

**NGHIÊN CỨU, XÂY DỰNG MÔ HÌNH MẠNG AN TOÀN CHO CÔNG TY CỔ PHẦN THƯƠNG MẠI HỒNG ANH**

**BÁO CÁO BÀI TẬP LỚN**

**HỌC PHẦN AN NINH MẠNG**

GVHD: T.s Phạm Văn Hiệp

Lớp: 20241IT6070001

Nhóm 8: Hoàng Hải Đăng - 2021606104

Dương Văn Trường - 2023600260

Trần Văn Hoàng - 2021607887

Lữ Sơn Trường - 2021601393

**Hà Nội 2024**

c

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

------------

# **LỜI MỞ ĐẦU**

An ninh mạng đã trở thành một lĩnh vực quan trọng và đa dạng trong lĩnh vực khoa học máy tính và công nghệ thông tin. Nó liên quan đến việc bảo vệ dữ liệu, ngăn chặn các cuộc tấn công mạng, quản lý danh sách truy câp,.... Được áp dụng trong tất cả các doanh nghiệp, cơ quan chính phủ, ngân hàng,...

Mạng không dây đang trở thành một phần quan trọng và không thể thiếu trong môi trường công nghiệp và doanh nghiệp ngày nay. Sự tiện lợi và tính linh hoạt của mạng không dây đã giúp nâng cao hiệu suất làm việc, tạo điều kiện thuận lợi cho làm việc từ xa, và cung cấp sự kết nối liền mạch. Tuy nhiên, với sự tiến bộ trong kỹ thuật, mạng không dây cũng mang theo các rủi ro bảo mật đáng kể, chẳng hạn như việc truy cập trái phép, đánh cắp dữ liệu và tấn công mạng. Vì vậy, việc xây dựng một mô hình mạng không dây an toàn là một nhiệm vụ quan trọng và không thể bỏ qua trong việc quản lý và bảo vệ dữ liệu của công ty.

Dưới sự hướng dẫn của TS. Phạm Văn Hiệp, bọn em đã hoàn thành đề tài. Mặc dù đã cố gắng hết sức nhưng nhóm chúng em cũng không thể tránh khỏi những sai sót trong quá trình làm bài. Vì vậy rất mong thầy thông cảm và chia sẻ ý kiến để nhóm chúng em có thể hoàn thiện đề tài.

Chúng em xin chân thành cảm ơn!

# **CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI**

* 1. **Tổng quan về An ninh mạng**
     1. **Khái niệm**

**An ninh mạng (Cybersecurity)** là tập hợp các biện pháp, công nghệ và quy trình được thiết kế để bảo vệ hệ thống, mạng lưới và dữ liệu khỏi các cuộc tấn công, truy cập trái phép, hoặc thiệt hại. An ninh mạng đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin số.



* + 1. **Mục tiêu chính của An ninh mạng**

Mục tiêu chính của an ninh mạng là bảo vệ thông tin và hệ thống khỏi các mối đe dọa và tấn công. Dưới đây là một số mục tiêu cụ thể:

* **Bảo mật thông tin:** Đảm bảo rằng thông tin nhạy cảm và quan trọng được bảo vệ khỏi truy cập trái phép và rò rỉ.
* **Tính toàn vẹn:** Đảm bảo rằng dữ liệu không bị thay đổi hoặc giả mạo trong quá trình lưu trữ hoặc truyền tải.
* **Tính sẵn sàng:** Đảm bảo rằng hệ thống và dịch vụ luôn sẵn sàng và hoạt động liên tục, không bị gián đoạn do các cuộc tấn công hoặc sự cố.
* **Xác thực:** Đảm bảo rằng người dùng và hệ thống được xác thực đúng cách để ngăn chặn truy cập trái phép.
* **Kiểm soát truy cập:** Đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên và thông tin quan trọng.
* **Bảo vệ chống lại các mối đe dọa:** Phát hiện và ngăn chặn các cuộc tấn công mạng, phần mềm độc hại, và các mối đe dọa khác.
* **Đảm bảo tuân thủ:** Đảm bảo rằng các hệ thống và quy trình tuân thủ các quy định và tiêu chuẩn an ninh mạng.
  + 1. **Các mối đe dọa trong An ninh mạng**

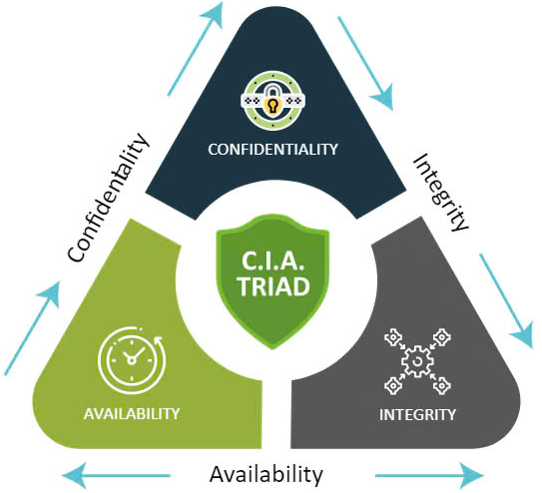
An ninh mạng được lập nên để chống lại những mối đe dọa ảnh hưởng đến người sử dụng như:

* **Malware:** Phần mềm độc hại như virus, worm, trojan...
* **Hacking:** Việc xâm nhập trái phép vào hệ thống máy tính.
* **Phishing:** Lừa đảo trực tuyến để đánh cắp thông tin cá nhân.
* **DDoS:** Tấn công từ chối dịch vụ để làm quá tải hệ thống.
* **Ransomware:** Mã độc mã hóa dữ liệu và đòi tiền chuộc.
* **Lỗ hổng bảo mật:** Các điểm yếu trong phần mềm, hệ điều hành...
  + 1. **Các biện pháp bảo vệ An ninh mạng**
* **Cập nhật phần mềm:** Luôn cập nhật các bản vá bảo mật mới nhất.
* **Sử dụng mật khẩu mạnh:** Tạo mật khẩu phức tạp và duy nhất cho mỗi tài khoản.
* **Xác thực hai yếu tố:** Thêm một lớp bảo mật bằng cách yêu cầu xác thực qua email, SMS hoặc ứng dụng.
* **Firewall:** Tường lửa giúp chặn các kết nối không đáng tin cậy.
* **Giải pháp bảo mật:** Sử dụng các phần mềm diệt virus, hệ thống phát hiện xâm nhập...
* **Đào tạo nhận thức:** Nâng cao nhận thức về an ninh mạng cho người dùng.
* **Sao lưu dữ liệu:** Thường xuyên sao lưu dữ liệu để phòng trường hợp bị mất dữ liệu.

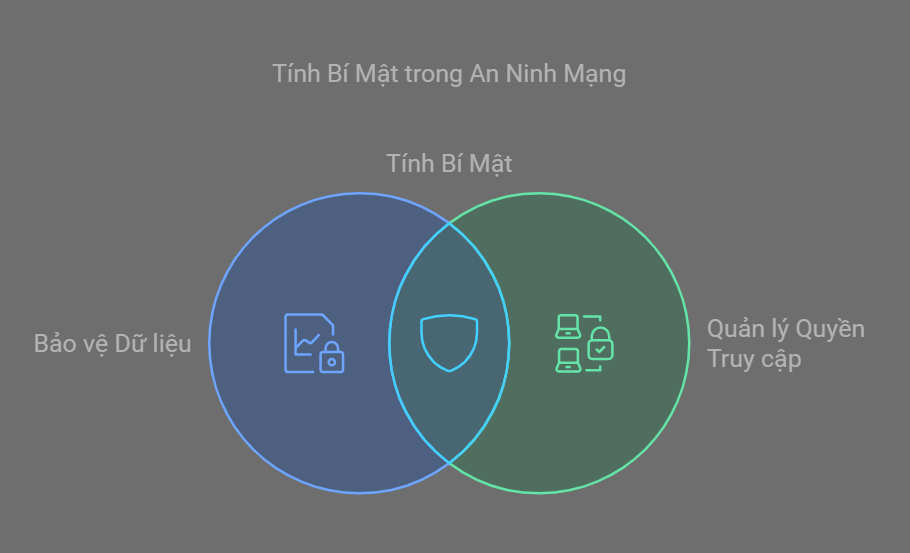
An ninh mạng là một lĩnh vực phức tạp và luôn thay đổi. Để bảo vệ bản thân và tổ chức trước các mối đe dọa, cần có sự kết hợp giữa các giải pháp công nghệ và các biện pháp quản lý.

* 1. **Các kiến thức cơ sở**
     1. **An toàn thông tin (Mô hình CIA)**

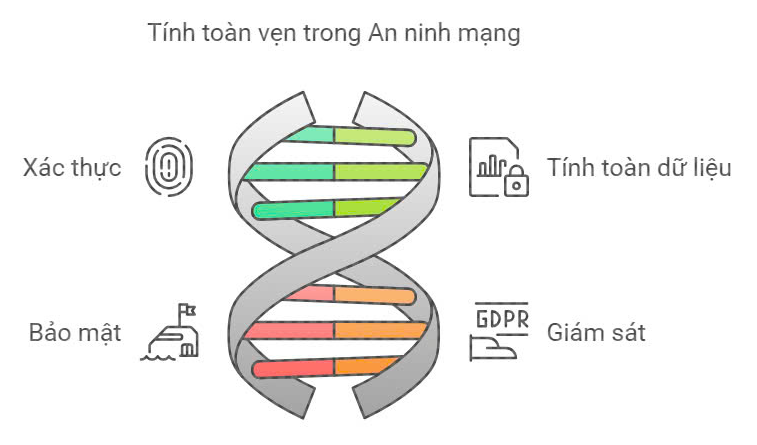
Mô hình bộ ba CIA gồm có: Confidentiality (tính bí mật), Integrity (tính toàn vẹn) và Availability (tính sẵn sàng). Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng. Bộ ba CIA cũng cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đói với các thực hiện an ninh. Mọi vi phạm bất kì một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.



* **Tính bí mật:** là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhảy cảm đó được che giấu với người dùng không được cấp phép. Gồm 2 nội dung là bí mật về dữ liệu và quyền riêng tư. Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.



* **Tính toàn vẹn:** Là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó Bảo đảm sự chính xác về dữ liệu và hệ thống.

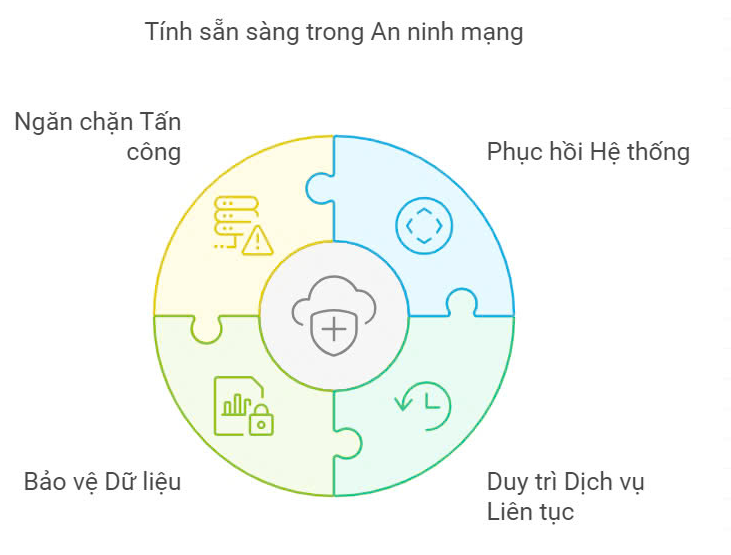


Có 3 mục đích chính của việc đảm bảo tính toàn vẹn:

* Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
* Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chú tâm của những người sử dụng được phép.
* Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

Tính toàn vẹn gồm có toàn vẹn về dữ liệu và toàn vẹn của hệ thống, trong đó:

* Toàn vẹn dữ liệu: Đảm bảo rằng dữ liệu và các chương trình chỉ được thay đổi theo bởi người được cấp quyền.
* Tính toàn vẹn của hệ thống: Đảm bảo rằng một hệ thống thực hiện chức năng dự kiến của nó một cách nguyên vẹn, không bị
* thao túng trái phép một cách có chủ ý hoặc vô ý.
* **Tính sẵn sàng:** Đảm bảo truy cập và sử dụng thông tin kịp thời và đáng tin cậy. Mất tính sẵn sàng là sự gián đoạn truy cập hoặc gián đoán sử dụng thông tin hoặc gián đoạn sử dụng hệ thống thông tin. Do đó, tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.



* + 1. **An toàn mạng máy tính**

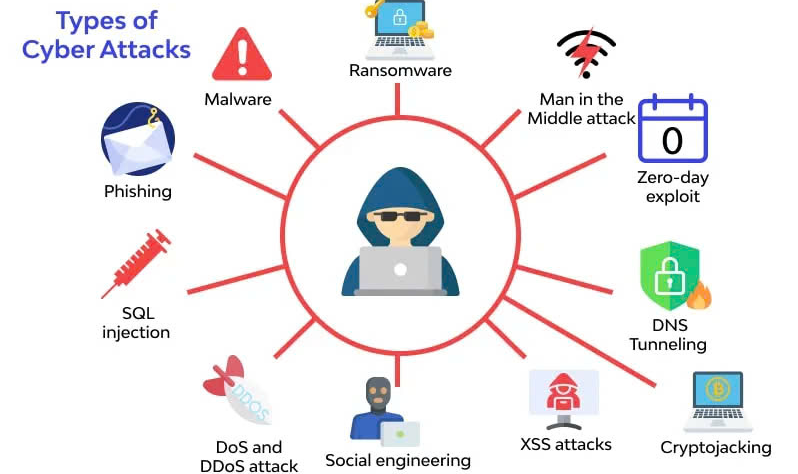
**An toàn mạng máy tính** (Network Security) là tập hợp các biện pháp, công nghệ, và quy trình được sử dụng để bảo vệ các hệ thống mạng máy tính khỏi các mối đe dọa, tấn công, và truy cập trái phép. Mục tiêu chính của an toàn mạng là đảm bảo tính **bảo mật**, **toàn vẹn**, và **khả dụng** của dữ liệu và tài nguyên trong hệ thống mạng

* **Các mối đe dọa mạng phổ biến:**
* **Malware (Phần mềm độc hại):** Gồm virus, sâu (worms), ransomware, spyware, adware.
* **Phishing (Lừa đảo):** Sử dụng email hoặc website giả mạo để đánh cắp thông tin nhạy cảm.
* **DDoS (Tấn công từ chối dịch vụ):** Làm tê liệt hệ thống bằng cách gửi lượng lớn yêu cầu đến máy chủ.
* **Man-in-the-Middle Attack:** Tấn công chặn thông tin giữa hai bên giao tiếp.
* **Zero-Day Exploits:** Lỗ hổng chưa được phát hiện hoặc chưa được vá trong phần mềm/hệ thống.
* **Các biện pháp bảo mật:**
* **Sử dụng tường lửa (Firewall):** Lọc và kiểm soát lưu lượng mạng ra vào.
* **Mã hóa (Encryption):** Bảo vệ dữ liệu bằng cách chuyển đổi thông tin sang dạng không thể đọc được.
* **Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS):** Phát hiện và phản ứng với các mối đe dọa.
* **Xác thực hai yếu tố (2FA):** Tăng cường bảo mật cho tài khoản.
* **Cập nhật và vá lỗi phần mềm:** Giảm nguy cơ bị tấn công qua các lỗ hổng.
  + 1. **Tấn công mạng**

**Tấn công mạng** (Cyber Attack) là hành động cố ý nhằm xâm nhập, làm gián đoạn, hoặc làm tổn hại đến các hệ thống máy tính, mạng lưới, hoặc dữ liệu. Các cuộc tấn công mạng thường do cá nhân, nhóm, hoặc tổ chức thực hiện với nhiều mục đích khác nhau như đánh cắp thông tin, phá hoại hệ thống, hoặc gây thiệt hại về tài chính và uy tín.

**Các loại tấn công mạng phổ biến:**

* Phishing: Lừa người dùng cung cấp thông tin cá nhân qua email giả mạo hoặc trang web giả.
* Malware: Sử dụng phần mềm độc hại như virus, worm, Trojan để xâm nhập và gây hại.
* SQL Injection: Tấn công vào cơ sở dữ liệu qua các lỗ hổng trên ứng dụng web.
* Man-in-the-Middle (MitM): Nghe lén hoặc can thiệp vào giao tiếp giữa hai bên.
* Zero-Day Exploits: Tấn công các lỗ hổng chưa được phát hiện hoặc vá lỗi.
* Brute Force Attack: Thử tất cả các tổ hợp mật khẩu để truy cập.



**Phòng chống tấn công mạng:**

* Cập nhật phần mềm thường xuyên để vá các lỗ hổng bảo mật.
* Sử dụng mật khẩu mạnh và kích hoạt xác thực hai yếu tố (2FA).
* Cảnh giác với email lạ và không nhấp vào các liên kết hoặc tải xuống tệp không rõ nguồn gốc.
* Cài đặt phần mềm chống virus và tường lửa (firewall).
* Sao lưu dữ liệu định kỳ để khôi phục trong trường hợp xảy ra sự cố.
  1. **Nội dung nghiên cứu**
     1. **Lý do chọn đề tài**

Trong bối cảnh ngày càng gia tăng các mối đe dọa về an ninh mạng, việc bảo vệ hệ thống thông tin của các doanh nghiệp, đặc biệt là các công ty cổ phần, là cực kỳ quan trọng. Công ty CP thương mại Hồng Anh, với sự phát triển nhanh chóng và mở rộng quy mô hoạt động, đối mặt với nhiều thách thức trong việc đảm bảo an toàn thông tin và bảo mật mạng. Việc xây dựng một mô hình mạng an toàn giúp giảm thiểu rủi ro từ các cuộc tấn công mạng, bảo vệ tài sản dữ liệu và uy tín của công ty.

Đề tài này sẽ giúp nâng cao nhận thức về an ninh mạng trong môi trường doanh nghiệp, đồng thời cung cấp những giải pháp cụ thể và hiệu quả nhằm bảo vệ thông tin và đảm bảo hoạt động ổn định của công ty trong dài hạn. Hơn nữa, việc nghiên cứu và xây dựng mô hình này cũng góp phần nâng cao kiến thức và kỹ năng thực tế về an ninh mạng trong bối cảnh công nghệ ngày càng phát triển.

Đề tài "Nghiên cứu, xây dựng mô hình mạng an toàn cho Công ty CP thương mại Hồng Anh" được chọn vì tính cấp thiết và tầm quan trọng của việc đảm bảo an ninh mạng trong môi trường doanh nghiệp hiện nay. Với sự phát triển mạnh mẽ của công nghệ thông tin và việc áp dụng các hệ thống mạng trong hầu hết các hoạt động kinh doanh, các công ty đang phải đối mặt với những nguy cơ tiềm ẩn liên quan đến bảo mật thông tin và an ninh mạng.

Trong đó, các công ty cổ phần (CP) thường có quy mô lớn và cấu trúc tổ chức phức tạp, điều này khiến cho việc bảo vệ thông tin trở thành một thách thức lớn hơn. Dữ liệu của công ty, từ các thông tin khách hàng, tài chính, cho đến các bí mật công nghệ đều là những mục tiêu hấp dẫn đối với các hacker và những kẻ tấn công mạng. Một lỗ hổng bảo mật dù nhỏ cũng có thể dẫn đến những thiệt hại nghiêm trọng về tài chính và uy tín của công ty. Vì vậy, xây dựng và triển khai một mô hình mạng an toàn không chỉ giúp giảm thiểu rủi ro từ các cuộc tấn công mạng, mà còn bảo vệ thông tin quan trọng, tạo dựng niềm tin cho khách hàng và đối tác.

Ngoài ra, công ty CP thương mại Hồng Anh, với sự phát triển không ngừng về quy mô và hệ thống thông tin, cũng cần phải thích ứng với các thách thức của môi trường mạng hiện đại, bao gồm các mối đe dọa từ phần mềm độc hại, tấn công DDoS (Distributed Denial of Service), lỗ hổng bảo mật trong phần mềm, và các rủi ro đến từ người dùng bên trong (insider threats). Việc triển khai một mô hình mạng an toàn sẽ giúp công ty chủ động phòng ngừa và ứng phó với các mối đe dọa này, tạo ra một môi trường làm việc và giao dịch an toàn cho cả nhân viên và khách hàng.

Bên cạnh đó, xây dựng mô hình mạng an toàn còn giúp công ty tuân thủ các yêu cầu pháp lý về bảo mật dữ liệu, đặc biệt là trong bối cảnh các quy định như GDPR (General Data Protection Regulation) tại châu Âu hay các luật bảo vệ dữ liệu cá nhân tại Việt Nam đang trở nên ngày càng nghiêm ngặt. Việc không tuân thủ các quy định này có thể dẫn đến các hậu quả nghiêm trọng, từ các khoản phạt tài chính cho đến việc mất uy tín và sự tin tưởng từ phía khách hàng.

Cuối cùng, đề tài này không chỉ mang lại giá trị thiết thực đối với công ty, mà còn giúp sinh viên có cơ hội nghiên cứu, tìm hiểu và áp dụng các kiến thức lý thuyết về an ninh mạng vào thực tiễn. Đây cũng là cơ hội để phát triển các kỹ năng thiết kế, triển khai và quản lý hệ thống mạng an toàn, từ đó đóng góp vào sự nghiệp phát triển bền vững của ngành công nghệ thông tin và an ninh mạng.

* + 1. **Mục tiêu nghiên cứu**

Mục tiêu chính của đề tài "Nghiên cứu và xây dựng mô hình mạng an toàn cho Công ty CP thương mại Hồng Anh" là thiết lập và triển khai một mô hình mạng an toàn hiệu quả, phù hợp với các yêu cầu đặc thù của công ty. Mô hình này sẽ sử dụng các phương pháp và công cụ an ninh mạng hiện đại, đảm bảo hệ thống thông tin của công ty luôn được bảo vệ khỏi các mối đe dọa từ bên ngoài và bên trong. Để đạt được mục tiêu này, các mục tiêu cụ thể sau sẽ được thực hiện:

* **Phân tích và đánh giá hiện trạng bảo mật của công ty:**

Xác định các nguy cơ tiềm ẩn và điểm yếu trong hệ thống mạng hiện tại của công ty: Phân tích chi tiết các lỗ hổng bảo mật, các mối đe dọa tiềm tàng từ các cuộc tấn công mạng, phần mềm độc hại, tấn công DDoS (Distributed Denial of Service), và các mối nguy hiểm đến từ các nhân viên hoặc người dùng bên trong công ty.

Đánh giá các biện pháp bảo mật hiện có của công ty: Xem xét hiệu quả của các giải pháp bảo mật hiện tại như tường lửa, mã hóa dữ liệu, và các hệ thống phát hiện và phòng chống xâm nhập (IDS/IPS), từ đó xác định các điểm cần cải thiện.

* **Xác định và đề xuất các yêu cầu bảo mật đặc thù của công ty:**

Nghiên cứu và đưa ra yêu cầu bảo mật cụ thể cho công ty: Dựa trên các yếu tố như quy mô công ty, loại hình hoạt động và dữ liệu quan trọng, xác định các yêu cầu bảo mật đặc biệt như bảo mật thông tin khách hàng, dữ liệu tài chính, và bảo mật các giao dịch trực tuyến.

Lựa chọn và đề xuất các biện pháp bảo mật tối ưu: Đưa ra các giải pháp bảo mật phù hợp với yêu cầu của công ty, bao gồm việc triển khai mã hóa, kiểm soát truy cập, và các biện pháp ngăn ngừa rủi ro bảo mật.

* **Thiết kế mô hình mạng an toàn cho công ty:**

Phát triển kiến trúc mạng an toàn tổng thể: Xây dựng mô hình mạng an toàn toàn diện bao gồm các thành phần cốt lõi như firewall, IDS/IPS, VPN (Virtual Private Network), các cổng bảo mật và các giải pháp kiểm soát truy cập.

Thiết kế mô hình bảo mật linh hoạt và mở rộng: Đảm bảo rằng mô hình mạng an toàn có khả năng mở rộng trong tương lai, đáp ứng sự phát triển của công ty. Thiết kế cấu trúc mạng sao cho dễ dàng thêm vào các thành phần bảo mật mới khi cần thiết.

Lựa chọn các công cụ bảo mật tiên tiến và phù hợp: Xác định các công cụ và giải pháp bảo mật phù hợp để triển khai trong mô hình mạng, như hệ thống giám sát an ninh mạng thời gian thực, phân tích lưu lượng mạng và các công cụ kiểm tra bảo mật.

* **Triển khai mô hình mạng an toàn trên môi trường mô phỏng:**

Sử dụng công cụ mô phỏng như Packet Tracer để triển khai mô hình mạng an toàn: Sử dụng Packet Tracer, một công cụ mô phỏng mạng mạnh mẽ, để tạo dựng và kiểm tra các thành phần trong mô hình mạng an toàn. Việc mô phỏng sẽ giúp kiểm tra khả năng tương tác giữa các thành phần bảo mật và xác nhận tính khả thi của mô hình.

Thiết lập và cấu hình các giải pháp bảo mật trong mô hình: Cấu hình firewall, IDS/IPS, VPN và các cơ chế bảo mật khác trong Packet Tracer để đảm bảo chúng hoạt động hiệu quả, bảo vệ hệ thống mạng khỏi các mối đe dọa tiềm ẩn.

* **Kiểm tra và xác nhận tính hiệu quả của các giải pháp bảo mật:**

Thực hiện các bài kiểm tra bảo mật để đánh giá hiệu quả của mô hình: Sử dụng các phương pháp kiểm tra như tấn công mô phỏng (penetration testing), đánh giá khả năng chống lại các mối đe dọa từ bên ngoài và bên trong, và kiểm tra khả năng phản ứng của hệ thống trước các sự cố an ninh.

Đo lường hiệu quả của các biện pháp bảo mật: Đánh giá các chỉ số về hiệu suất bảo mật, bao gồm thời gian phát hiện và phản ứng với sự cố, mức độ bảo vệ dữ liệu và hệ thống mạng, và mức độ giảm thiểu rủi ro an ninh.

* **Đề xuất các giải pháp duy trì và cập nhật hệ thống bảo mật lâu dài:**

Xây dựng kế hoạch bảo trì và cập nhật hệ thống bảo mật: Đảm bảo rằng hệ thống bảo mật được duy trì và cập nhật thường xuyên, theo dõi các mối đe dọa mới và thay đổi trong môi trường công nghệ.

Đào tạo nhân viên và nâng cao nhận thức về bảo mật: Đưa ra các chương trình đào tạo cho nhân viên về các biện pháp bảo mật cơ bản và các chính sách bảo mật nội bộ, giúp họ nhận thức được vai trò của mình trong việc bảo vệ hệ thống mạng.

* **Đảm bảo tuân thủ các tiêu chuẩn và quy định về bảo mật thông tin**:

Tuân thủ các quy định pháp lý và tiêu chuẩn quốc tế về bảo mật thông tin: Đảm bảo rằng mô hình bảo mật đáp ứng các yêu cầu pháp lý về bảo vệ dữ liệu cá nhân và bảo mật thông tin, như GDPR hoặc các quy định bảo mật trong nước.

# **CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU**

## **2.1. Khái niệm về mạng**

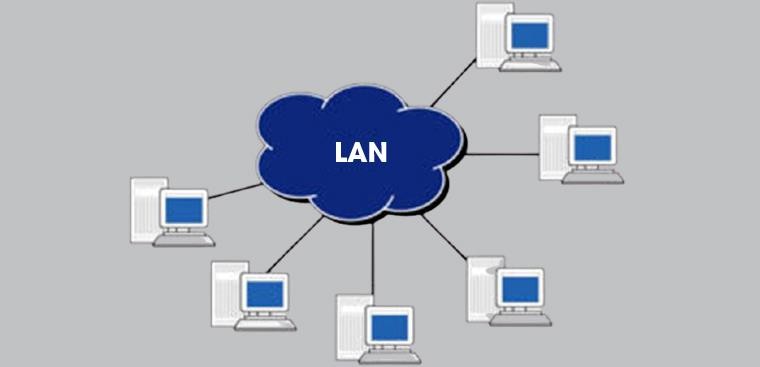
Mạng máy tính là một nhóm các máy tính và thiết bị ngoại vi kết nối với nhau thông qua các phương tiện truyền dẫn như cáp xoắn, cáp quang, sóng điện từ, tia hồng ngoại… để chia sẻ dữ liệu cho nhau. Dữ liệu truyền từ máy này sang máy khác đều là các bit nhị phân 0 và 1, sau khi biến đổi thành điện thế hoặc sóng điện từ, sẽ được truyền qua môi trường truyền dẫn bên dưới. Mạng máy tính có nhiều ích lợi:

* Tiết kiệm tài nguyên phần cứng
* Giúp trao đổi dễ dàng
* Chia sẻ ứng dụng
* Tập trung dữ liệu để bảo mật, sao lưu
* Sử dụng Internet,….

### **2.1.1. Các loại mạng máy tính thông dụng**

Mạng máy tính có nhiều loại, tùy thuộc vào vị trí địa lý, tốc độ đường truyền, tỉ lệ lỗi bit trên đường truyền, đường đi của dữ liệu trên mạng, dạng chuyển giao thông tin. Nhìn chung, các mạng máy tính có thể được phân biệt làm các loại sau:

1. Mạng cục bộ: Mạng LAN (Local Area Network – còn gọi là mạng cục bộ) là một nhóm các máy tính và thiết bị truyền thông mạng được kết nối với nhau trong một khu vực nhỏ như tòa nhà cao ốc, trường đại học, khu giải trí...

  
*Hình 2.1 Khái niệm về mạng LAN*

Mạng LAN có các đặc điểm sau:

• Băng thông lớn để có khả năng chạy các ứng dụng trực tuyến như xem phim, giải trí, hội thảo qua mạng.

• Kích thước mạng bị giới hạn bởi thiết bị.

• Chi phí thiết kế, lắp đặt mạng LAN rẻ.

• Quản trị đơn giản.

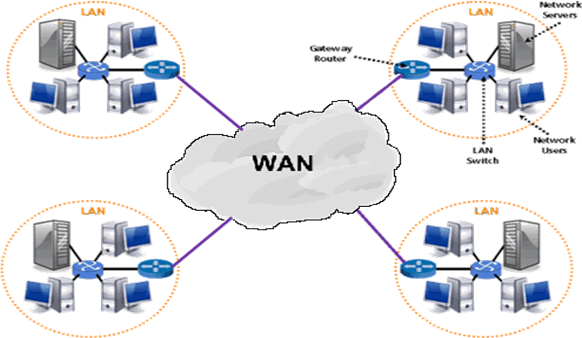
b) Mạng đô thị: Mạng đô thị MAN (Metropolitan Area Network) gần giống như mạng LAN nhưng giới hạn kích thước của nó là một thành phố hay một quốc gia. Mạng MAN kết nối các mạng LAN lại với nhau thông qua môi trường truyền dẫn và các phương thức truyền thông khác nhau. Mạng MAN có các đặc điểm sau:

• Băng thông ở mức trung bình, đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử, thương mại điện tử, các ứng dụng của các ngân hàng…

• Do MAN kết nối nhiều LAN nên việc quản trị sẽ gặp khó khăn hơn, đồng thời độ phức tạp cũng tăng theo.

• Chi phí các thiết bị MAN tương đối đắt tiền.

c) Mạng diện rộng: Mạng diện rộng WAN (Wide Area Network) có phạm vi bao phủ một vùng rộng lớn, có thể là quốc gia, lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu. Mạng WAN lớn nhất hiện nay là mạng Internet. Mạng WAN là tập hợp của nhiều mạng LAN và MAN được nối lại với nhau thông qua các phương tiện như vệ tinh, sóng vi ba, cáp quang, điện thoại ….



*Hình 2.2 Khái niệm về mạng WAN*

Mạng WAN có các đặc điểm sau:

• Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng online như e – mail, fpt, web….

• Phạm vi hoạt động không giới hạn.

• Do kết nối nhiều LAN và MAN với nhau nên mạng rất phức tạp và các tổ chức toàn cầu phải đứng ra quy định và quản lý.

• Chi phí cho các thiết bị và công nghệ WAN rất đắt Chú ý là việc phân biệt mạng thuộc loại LAN, MAN hay WAN chủ yếu dựa trên khoảng cách vật lý và chỉ máng tính chất ước lệ.

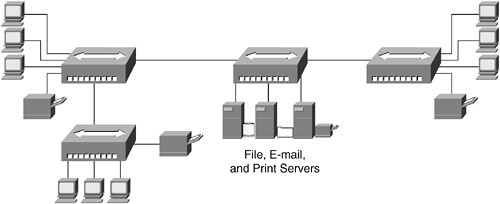
## **2.2. Các mạng máy tính phổ biến**

Các mô hình mạng máy tính phổ biến như mạng hình sao, mạng tuyến tính, mạng hình vòng và mạng kết hợp thường được sử dụng tùy thuộc vào yêu cầu cụ thể của tổ chức.

### **2.2.1. Mạng phẳng (Flat Network)**

**Mô tả:**

* Là mô hình mạng cơ bản, trong đó tất cả các thiết bị đều nằm trên một mạng logic duy nhất.
* Lưu lượng dữ liệu di chuyển tự do giữa các thiết bị mà không có phân đoạn cụ thể.



Hình : Mạng phẳng (Flat Network)

**Ưu điểm:**

* Đơn giản, dễ triển khai và quản lý.
* Chi phí thấp, không cần nhiều thiết bị hoặc cấu hình phức tạp.

**Nhược điểm:**

* Thiếu tính bảo mật: Một khi bị xâm nhập, toàn bộ mạng có thể bị ảnh hưởng.
* Không tối ưu cho doanh nghiệp lớn hoặc môi trường yêu cầu an ninh cao.

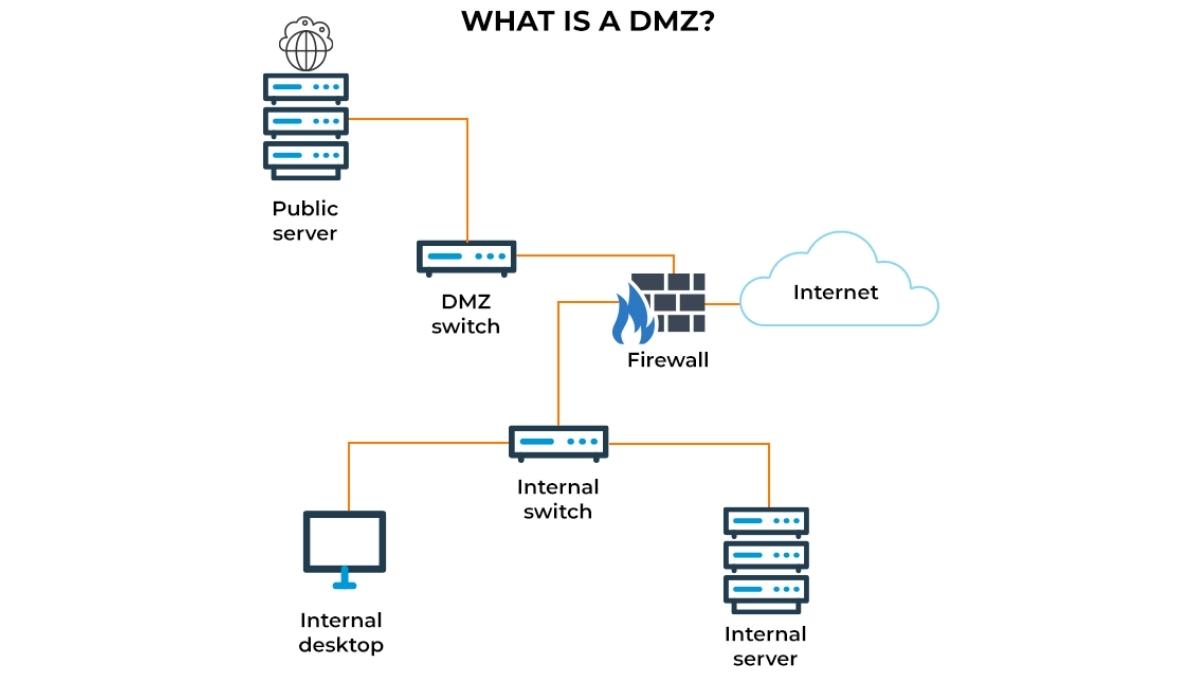
**Ứng dụng:**

* Phù hợp với doanh nghiệp nhỏ hoặc các phòng lab thử nghiệm không có yêu cầu bảo mật nghiêm ngặt.

### **2.2.2. Mạng DMZ (Demilitarized Zone)**

**Mô tả:**

* DMZ là vùng trung gian giữa mạng nội bộ (LAN) và mạng internet, nơi chứa các dịch vụ công khai như web server, mail server.
* Mô hình này thường sử dụng tường lửa để kiểm soát lưu lượng ra/vào giữa DMZ, LAN và internet.



Hình: Mạng DMZ

**Ưu điểm:**

* **Bảo mật dữ liệu nội bộ:** Giảm rủi ro từ các dịch vụ công khai bị tấn công.
* **Kiểm soát lưu lượng:** Các yêu cầu truy cập từ internet được kiểm tra trước khi đi vào LAN.

**Nhược điểm:**

* Tăng độ phức tạp trong thiết kế và quản lý.
* Cần đầu tư thêm thiết bị bảo mật và kỹ thuật quản trị.

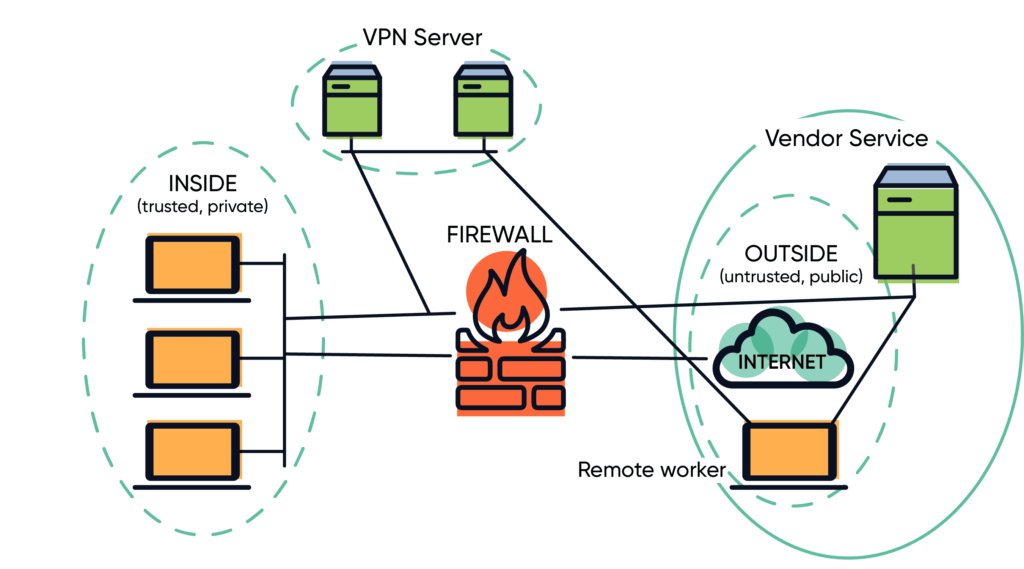
**Ứng dụng:**

* Các tổ chức cung cấp dịch vụ công khai như website thương mại điện tử, email công ty.

### **2.2.3. Mạng Zero Trust**

**Mô tả:**

* Triết lý "không tin tưởng bất kỳ ai" (dù là nội bộ hay bên ngoài).
* Mọi truy cập đều phải được xác thực, kiểm tra trước khi cấp quyền.



Hình: Mạng Zero Trust

**Thành phần chính:**

* **Xác thực đa yếu tố (MFA):** Kiểm tra danh tính qua nhiều lớp bảo mật.
* **Kiểm soát truy cập chi tiết:** Phân quyền người dùng dựa trên vai trò và trách nhiệm.
* **Giám sát liên tục:** Theo dõi hành vi người dùng và thiết bị.

**Ưu điểm:**

* Bảo vệ tối ưu ngay cả khi mạng nội bộ bị xâm nhập.
* Tăng cường khả năng đáp ứng với các mối đe dọa hiện đại.

**Nhược điểm:**

* Tăng độ phức tạp và chi phí triển khai.
* Đòi hỏi sự tích hợp chặt chẽ giữa các hệ thống bảo mật.

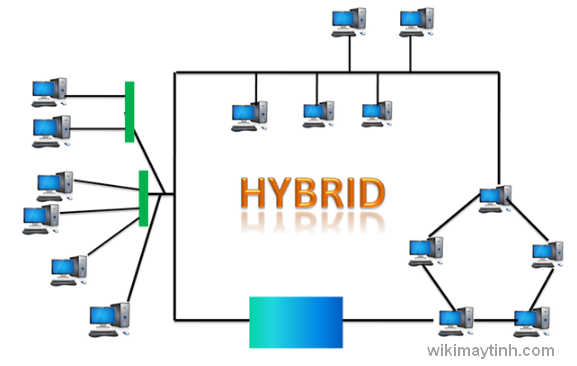
**Ứng dụng:**

* Phù hợp với doanh nghiệp lớn, đặc biệt trong lĩnh vực tài chính, y tế, và công nghệ.

### **2.2.4. Mạng hybrid (Kết hợp)**

**Mô tả:**

* Kết hợp ưu điểm của các mô hình mạng phẳng, phân tầng, DMZ và Zero Trust để tạo thành một hệ thống linh hoạt.
* Tùy thuộc vào yêu cầu thực tế, doanh nghiệp có thể kết hợp mạng phân tầng với DMZ hoặc tích hợp Zero Trust vào mạng hiện tại.



Hình: Mạng Hybrid

**Ưu điểm:**

* Linh hoạt và phù hợp với nhiều nhu cầu.
* Tận dụng được các công nghệ bảo mật tiên tiến mà không cần thay đổi toàn bộ hạ tầng mạng.

**Nhược điểm:**

* Chi phí và độ phức tạp cao.
* Yêu cầu đội ngũ kỹ thuật có năng lực cao.

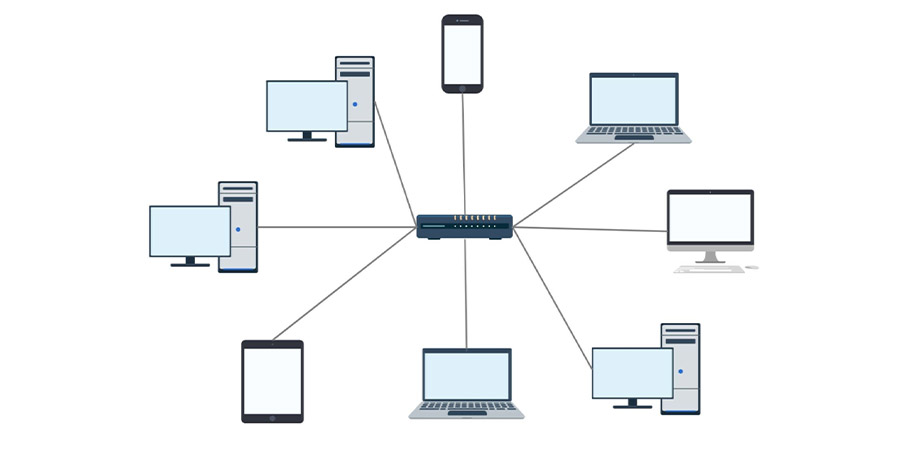
**Ứng dụng:**

* Doanh nghiệp lớn, có nhiều cơ sở và yêu cầu bảo mật đa dạng.

### **2.2.5. Mạng hình sao**

**Mô tả:**

Mô hình mạng hình sao kết nối tất cả các thiết bị đầu cuối (máy tính, máy in, camera...) đến một thiết bị trung tâm, thường là switch hoặc hub. Thiết bị trung tâm chịu trách nhiệm quản lý lưu lượng và điều phối giao tiếp giữa các thiết bị.  
Phù hợp cho môi trường mạng vừa và nhỏ với yêu cầu quản lý đơn giản và dễ mở rộng.



Hình: Mạng hình sao

**Ưu điểm:**

* Dễ dàng triển khai và quản lý.
* Khả năng mở rộng cao, chỉ cần bổ sung cổng kết nối vào thiết bị trung tâm.
* Giảm thiểu ảnh hưởng khi một thiết bị đầu cuối bị lỗi.
* Hiệu suất cao khi sử dụng switch, cho phép truyền dữ liệu trực tiếp giữa các thiết bị.

**Nhược điểm:**

* Phụ thuộc hoàn toàn vào thiết bị trung tâm: Nếu switch/hub gặp sự cố, toàn bộ mạng sẽ ngừng hoạt động.
* Chi phí cao hơn so với một số mô hình khác, do yêu cầu cáp riêng biệt cho từng thiết bị đầu cuối.
* Hạn chế số lượng kết nối tối đa dựa trên khả năng của thiết bị trung tâm.

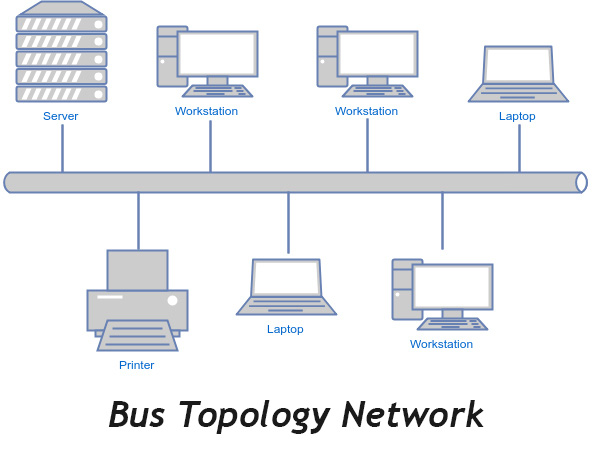
**Ứng dụng:**

* **Doanh nghiệp nhỏ và vừa:** Các văn phòng với số lượng thiết bị không quá lớn, cần quản lý đơn giản và hiệu quả.
* **Trường học và phòng lab:** Tổ chức các phòng máy tính hoặc thiết bị học tập có cấu trúc rõ ràng.
* **Hệ thống an ninh:** Kết nối camera giám sát, máy chủ lưu trữ, và các thiết bị khác thông qua switch trung tâm.

### **2.2.6. Mạng tuyến tính (Bus Network)**

**Mô tả:**

Mô hình mạng tuyến tính sử dụng một cáp chính (bus) làm đường truyền dữ liệu chính, nối tất cả các thiết bị đầu cuối (máy tính, máy in,...) với nhau. Mỗi thiết bị được kết nối thông qua một giao tiếp trên cáp chính và chia sẻ băng thông chung.



Hình: Mạng Bus

**Ưu điểm:**

* **Chi phí thấp:** Chỉ cần một cáp chính duy nhất để kết nối các thiết bị, giảm thiểu chi phí cáp và thiết bị phụ trợ.
* **Đơn giản trong cấu hình:** Dễ dàng triển khai và mở rộng bằng cách thêm thiết bị vào cáp chính.
* **Tương thích tốt:** Phù hợp cho các hệ thống mạng nhỏ, nơi số lượng thiết bị kết nối không lớn.

**Nhược điểm:**

* **Phụ thuộc vào cáp chính:** Nếu cáp chính bị hỏng, toàn bộ mạng sẽ ngừng hoạt động.
* **Hiệu suất thấp khi mở rộng:** Nhiều thiết bị chia sẻ cùng một băng thông, dẫn đến giảm hiệu suất khi có lưu lượng lớn.
* **Khó xác định lỗi:** Khi xảy ra sự cố, việc xác định vị trí lỗi trên cáp chính có thể mất nhiều thời gian.

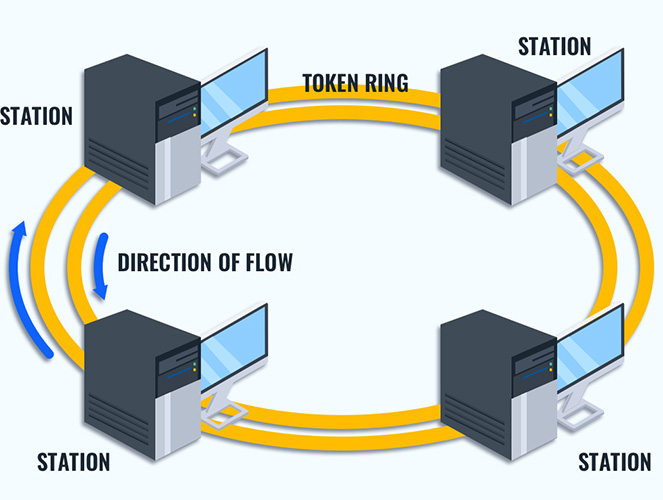
**Ứng dụng:**

* **Mạng nhỏ:** Phòng lab, phòng học hoặc các mạng thử nghiệm với số lượng thiết bị ít.
* **Kết nối tạm thời:** Dùng để kết nối các thiết bị trong các sự kiện hoặc triển lãm.
* **Hệ thống cũ:** Một số doanh nghiệp nhỏ vẫn sử dụng mô hình này trong mạng nội bộ truyền thống.

### **2.2.7. Mạng hình vòng (Ring Network)**

**Mô tả:**

Mô hình mạng hình vòng kết nối các thiết bị thành một vòng tròn, trong đó mỗi thiết bị được nối trực tiếp với hai thiết bị liền kề. Dữ liệu di chuyển theo một hướng cố định (chiều kim đồng hồ hoặc ngược chiều kim đồng hồ), qua từng thiết bị cho đến khi đến đích.



Hình: Mạng hình vòng

**Ưu điểm:**

* **Độ chính xác cao trong truyền dữ liệu:** Dữ liệu được truyền qua từng nút theo thứ tự, giảm khả năng va chạm.
* **Tiết kiệm tài nguyên:** Không cần thiết bị trung tâm như switch hoặc hub.
* **Tính đồng bộ:** Mỗi thiết bị hoạt động như một bộ lặp (repeater), đảm bảo tín hiệu được truyền đi mạnh mẽ và ổn định.

**Nhược điểm:**

* **Phụ thuộc vào từng nút:** Nếu một thiết bị trong vòng bị lỗi, toàn bộ mạng sẽ ngừng hoạt động, trừ khi có cơ chế dự phòng (dual-ring).
* **Khó mở rộng:** Thêm một thiết bị mới đòi hỏi phải gián đoạn mạng để kết nối.
* **Hiệu suất giảm khi lưu lượng lớn:** Mọi dữ liệu phải đi qua tất cả các thiết bị trung gian trước khi đến đích.

**Ứng dụng:**

* Hệ thống mạng nhỏ: Phù hợp cho các văn phòng hoặc tổ chức nhỏ với số lượng thiết bị giới hạn.
* Mạng cũ: Một số hệ thống mạng nội bộ truyền thống trong doanh nghiệp hoặc các cơ sở sản xuất nhỏ vẫn sử dụng.
* Mạng công nghiệp: Thường được sử dụng trong các hệ thống giám sát và điều khiển công nghiệp (SCADA), nơi tín hiệu cần được truyền tuần tự qua từng thiết bị.

## **2.3. Giới thiệu chung về mạng an toàn**

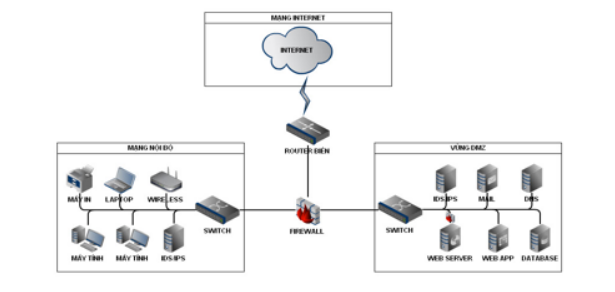
### **2.3.1. Khái niệm mô hình mạng an toàn**

Mô hình mạng an toàn là một cấu trúc tổ chức quan trọng để đảm bảo an toàn, bảo mật và tin cậy của hệ thống mạng trong tổ chức. Nó đặt ra các nguyên tắc cơ bản như phân biệt chức năng giữa các vùng mạng và thiết lập chính sách an toàn thông tin đặc biệt cho mỗi vùng. Việc tổ chức mô hình này đồng nghĩa với việc bảo vệ sự an toàn của hệ thống và các cổng thông tin điện tử, làm nền tảng cho việc xây dựng các hệ thống phòng thủ và bảo vệ. Đặc biệt, mô hình này có khả năng hiệu quả hạn chế các tấn công từ bên trong và bên ngoài, tạo ra một môi trường an toàn và ổn định cho hoạt động mạng của tổ chức.

### **2.3.2. Một số mô hình mạng phổ biến**

**Mô hình 1:**

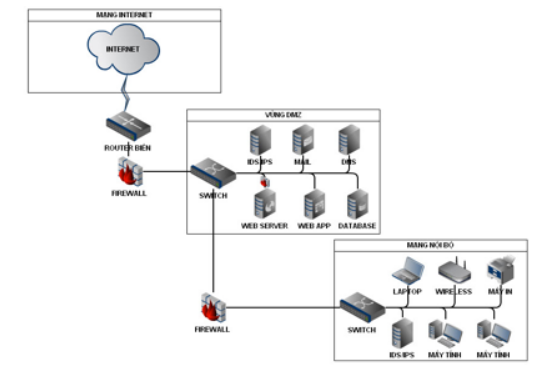
* Vùng mạng Internet, Local và DMZ được thiết kế tách biệt nhau
* Sơ đồ logic hệ thống mạng này cho phép người dùng có thể để firewall đặt giữa các vùng mạng.
* Firewall này có nhiệm vụ kiểm soát luồng dữ liệu giữa các vùng mạng với nhau và bảo vệ các vùng mạng khỏi các tấn công trái phép.



*Hình:*

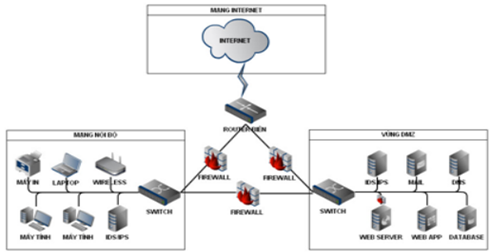
**Mô hình 2:**

* Sơ đồ thiết kế hệ thống mạng này bao gồm một firewall được đặt giữa mạng Internet và DMZ và một firewall giữa DMZ và vùng mạng nội bộ.
* Vùng mạng nội bộ nằm sâu bên trong và cách vùng mạng Internet bằng 2 lớp firewall.

  
*Hình:*

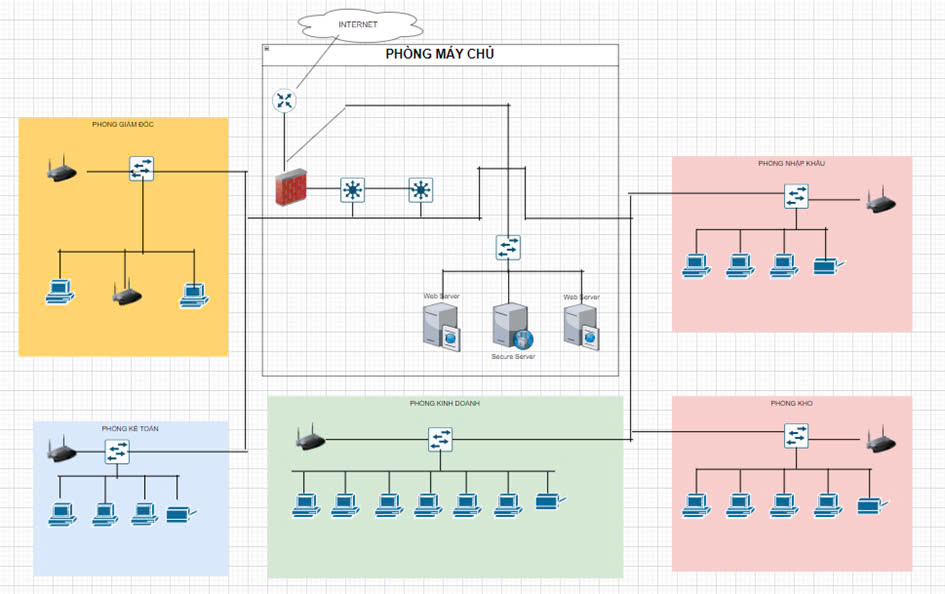
**Mô hình 3:**

* Firewall thứ nhất đặt giữa vùng mạng Internet và vùng mạng DMZ.
* Firewall thứ hai đặt giữa vùng mạng DMZ và vùng mạng nội bộ.
* Firewall thứ ba đặt giữa vùng mạng nội bộ và vùng mạng Internet.
* Các luồng dữ liệu giữa các vùng với nhau đều được kiểm soát bởi các firewall.



*Hình:*

## **2.4. Nghiên cứu mô hình mạng an toàn cho công ty cổ phần thương mại Hồng Anh**



### **2.4.1. Cấu trúc cơ bản Mô hình mạng của công ty cổ phần thương mại Hồng Anh**

Được thiết kế để đảm bảo an toàn thông tin và hiệu suất hoạt động tối ưu. Cấu trúc mạng bao gồm:

* Kết nối Internet được bảo vệ bởi một tường lửa (firewall) đặt tại cổng ra vào chính.
* Một vùng DMZ chứa các máy chủ quan trọng như web server và secure server để xử lý các giao dịch công khai.
* Các phòng ban khác nhau như Giám đốc, Kế toán, Kinh doanh, Nhập khẩu và Kho, mỗi phòng được kết nối qua các switch và router riêng biệt.
* Phòng máy chủ trung tâm chịu trách nhiệm quản lý toàn bộ dữ liệu và luồng thông tin trong hệ thống mạng.

### **2.4.2. Các thành phần chính**

Các thành phần chính trong mô hình mạng bao gồm:

*1. Kết nối với Internet:*

- Router 1941 ISP kết nối với địa chỉ mạng bên ngoài (8.0.0.0/8).

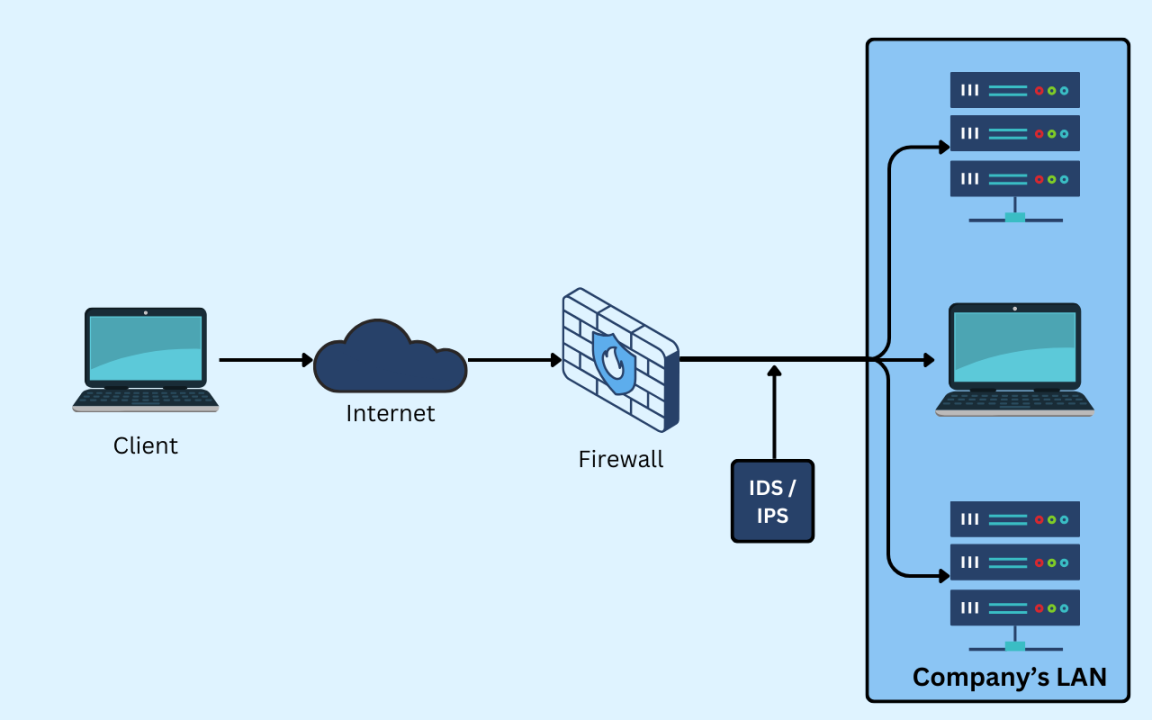
- Có tuyến đường kết nối tới máy chủ bên ngoài (ví dụ: Server-PT Google).

*2. Tường lửa và hệ thống phát hiện xâm nhập (Firewall & IDS/IPS)*

Tường lửa (Firewall) và Hệ thống phát hiện/cản phá xâm nhập (IDS/IPS) là hai yếu tố quan trọng trong bảo mật mạng, giúp bảo vệ hệ thống khỏi các mối đe dọa từ bên ngoài và bên trong. Cả hai cùng đóng vai trò ngăn chặn và phát hiện các cuộc tấn công mạng, bảo vệ dữ liệu và tài nguyên của doanh nghiệp.

Tường lửa là một thiết bị bảo mật mạng hoặc một phần mềm có chức năng giám sát và kiểm soát lưu lượng mạng giữa các mạng hoặc giữa mạng nội bộ và Internet. Nó dựa trên các quy tắc để quyết định xem lưu lượng mạng có được phép đi qua hay không, giúp bảo vệ hệ thống mạng khỏi các cuộc tấn công, truy cập trái phép và virus.

IDS (Intrusion Detection System) là hệ thống phát hiện xâm nhập, có nhiệm vụ giám sát lưu lượng mạng và phát hiện các hành vi bất thường, nguy hiểm. IPS (Intrusion Prevention System) là hệ thống cản phá xâm nhập, có nhiệm vụ không chỉ phát hiện mà còn ngăn chặn các cuộc tấn công trước khi chúng có thể gây hại cho hệ thống.



*Hình 2.4: Tường lửa và hệ thống phát hiện xâm nhập*

- Thiết bị bảo mật ASA (5506-X ASA) được triển khai để lọc luồng dữ liệu giữa mạng nội bộ và bên ngoài, giúp bảo vệ các tài nguyên nội bộ.

* Ưu điểm và lợi ích của Firewall & IDS/IPS:
* Bảo vệ mạng toàn diện: Kết hợp tường lửa và IDS/IPS giúp bảo vệ cả từ bên ngoài (tấn công từ Internet) và bên trong (tấn công nội bộ, phần mềm độc hại).
* Phát hiện và ngăn chặn tấn công hiệu quả: IDS giúp phát hiện các cuộc tấn công tinh vi, trong khi IPS có thể ngừng tấn công trước khi chúng gây thiệt hại.
* Giảm thiểu rủi ro: Cả hai công nghệ giúp bảo vệ hệ thống mạng khỏi các mối đe dọa mới và các cuộc tấn công tiềm ẩn.

*3. Switch Core:*

Hai switch chính (CoreSW1 và CoreSW2) đảm nhiệm việc kết nối và quản lý lưu lượng giữa các VLAN nội bộ, đảm bảo khả năng mở rộng và hiệu suất mạng.

*4. VLAN:*

Mạng được chia thành các VLAN để phân đoạn và cô lập lưu lượng:

- VLAN 10: Phòng giám đốc (192.168.10.0/24).

- VLAN 20: Kế toán (192.168.20.0/24).

- VLAN 30: Kinh doanh (192.168.30.0/24).

- VLAN 40: Kho (192.168.40.0/24).

- VLAN 50: Nhập khẩu (192.168.50.0/24).

*5. Các thiết bị kết nối trong VLAN:*

Máy in, PC, laptop, và các điểm truy cập (AccessPoint-PT) trong từng VLAN phục vụ công việc của từng bộ phận.

*6. Vùng DMZ (Demilitarized Zone):*

Bao gồm các server cung cấp dịch vụ công khai như:

- Server-PT WebDNS (192.168.2.3).

- Server-PT FTP (192.168.2.4).

- Server-PT Mail (2.2.2.2/24).

*7. Router nội bộ:*

Router 1941 thực hiện việc định tuyến và kết nối giữa các VLAN và kết nối ra ngoài Internet thông qua firewall.

*8. Cơ sở hạ tầng mạng:*

Sử dụng nhiều switch phân tán tại từng phòng ban (Switch24-PT) để kết nối các thiết bị trong cùng VLAN, đảm bảo hiệu suất và độ tin cậy.

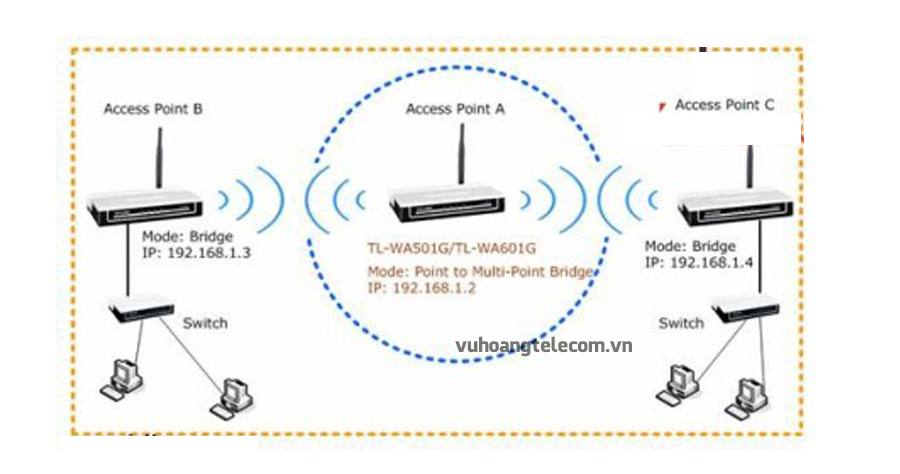
*9. Quản lý IP:*

Sử dụng địa chỉ IP phân bổ cụ thể cho từng VLAN với gateway đặt tại các Virtual IP trên firewall ASA.

*10. Access Point – PT*

Access Point là một thiết bị mạng có khả năng tạo ra WLAN, hay còn gọi là mạng không dây cục bộ. Access Point thường được dùng tại môi trường công sở, nhà hàng, tiệc cưới hay các tòa nhà lớn nhằm tạo ra không gian sử dụng mạng rộng rãi mà không làm suy giảm tốc độ của mạng.

Ngoài ra, Access Point còn khả năng chuyển đổi mạng có dây thành mạng không dây, từ đây mà các thiết bị có thể dễ dàng kết nối được. Có thể hiểu Access Point là một loại thiết bị thu phát WiFi. Tuy nhiên, không vì thế mà tính bảo mật trên không gian mạng bị suy giảm theo, điều này giúp bạn có thể yên tâm sử dụng thiết bị



*Hình 2.1: Mô hình điểm truy cập Access Point*

Một chức năng ưu việt của Access Point đó là khả năng liên kết các máy tính tại nơi làm việc, từ đó sẽ giúp việc kiểm soát và truyền tải dữ liệu trở nên đơn giản hơn.

Về cơ bản, Access Point có cách hoạt động tương tự như cổng chia mạng Switch, nhưng điểm đặc biệt là nó được trang bị thêm khả năng phát WiFi.

Bởi vì cấu tạo nhỏ gọn và cũng đơn giản, vậy nên Access Point có thể được gắn bất kỳ ở đâu, từ tường nhà cho đến trần nhà, mà không lo ảnh hưởng đến thẩm mỹ chung của không gian làm việc. Đồng thời, quá trình lắp đặt thiết bị cũng không quá phức tạp nên người dùng cũng không cần mất quá nhiều thời gian và công sức.

Về nguyên lý hoạt động, Access Point hoạt động theo 2 chế độ chính như sau:

Chế độ cầu nối Bridge Mode: Access Point đóng vai trò như là một cầu nối không dây thực hiện cùng lúc hai việc nhận và truyền tải tín hiệu. Các cầu nối sẽ kết nối hai hay nhiều đoạn mạng có dây để tạo thành một kết nối không dây hoàn chỉnh. Từ đó, mở rộng không gian tín hiệu Internet cho nhiều người dùng.

Chế độ lặp lại Repeater Mode: Với chế độ này, Access Point sẽ lặp lại tín hiệu từ Modem, Router và các Access Point khác có kết nối mạng có dây. Nhằm thiết lập một đường truyền mạng không dây để mở rộng phạm vi sử dụng mạng.

### **2.4.3. Cách thức hoạt động**

*1. Kết nối mạng tổng quan*

* Kết nối Internet:  
  Hệ thống được kết nối ra Internet thông qua Router 1941 và thiết bị định tuyến ASA 5506-X, cung cấp tường lửa và các tính năng bảo mật mạnh mẽ. Kết nối ra Internet thông qua dải địa chỉ IP công cộng (ví dụ: 209.165.202.0/29).
  + Router 1941: Quản lý giao tiếp với ISP (nhà cung cấp dịch vụ Internet) và kết nối tới mạng nội bộ.
  + ASA Firewall: Chịu trách nhiệm quản lý luồng dữ liệu vào/ra mạng, cung cấp chức năng bảo vệ khỏi các mối đe dọa bên ngoài như tấn công DDoS hoặc truy cập trái phép.
* DMZ(DeMilitarizedZone):  
  Một khu vực mạng riêng biệt (192.168.2.0/24) được thiết lập để lưu trữ các máy chủ công khai:
  + Server Web/DNS: Cung cấp dịch vụ web và DNS cho người dùng bên ngoài.
  + Server FTP: Lưu trữ dữ liệu cần chia sẻ qua giao thức FTP.

*2. Phân chia VLAN nội bộ*

Mạng nội bộ được phân thành các VLAN để cô lập lưu lượng và tăng cường bảo mật. Mỗi VLAN được định danh với dải địa chỉ IP riêng:

* VLAN 10 (192.168.10.0/24 - Ban Giám đốc):
  + Bao gồm các thiết bị: PC Giám đốc, PC Phó Giám đốc, máy in và laptop.
  + Các thiết bị được kết nối thông qua Switch và Access Point.
* VLAN 20 (192.168.20.0/24 - Kế toán):
  + Bao gồm PC Kế toán, máy in, và laptop.
  + Switch chịu trách nhiệm kết nối tất cả các thiết bị.
* VLAN 30 (192.168.30.0/24 - Kinh doanh):
  + Bao gồm PC trưởng phòng kinh doanh, các máy tính nhân viên, và máy in.
  + Hỗ trợ kết nối không dây qua Access Point.
* VLAN 40 (192.168.40.0/24 - Kho):
  + Bao gồm PC quản lý kho, nhân viên kho, máy in, và laptop.
* VLAN 50 (192.168.50.0/24 - Nhập khẩu):
  + Bao gồm PC quản lý mua hàng, nhân viên nhập khẩu, máy in, và thiết bị không dây.

*3. Thiết bị mạng cốt lõi*

* Switch Core1 và Core 2 (Cốt lõi): Hai thiết bị Switch cốt lõi (5500-24PS) chịu trách nhiệm kết nối các VLAN nội bộ với mạng tổng thể, đảm bảo dữ liệu truyền tải nhanh chóng và an toàn.
* Access Point:Cung cấp khả năng kết nối không dây cho các thiết bị di động như laptop và điện thoại thông minh.

*4. Các giải pháp bảo mật*

Hệ thống áp dụng nhiều lớp bảo mật như:

* Mã hóa dữ liệu: Sử dụng WPA2/WPA3 với mã hóa AES để bảo vệ dữ liệu trong quá trình truyền.
* Xác thực người dùng: Bao gồm mật khẩu mạnh và xác thực hai yếu tố (2FA).
* Tường lửa:
  + Tường lửa trên ASA và các Router giúp kiểm tra gói tin và ngăn chặn truy cập trái phép.
* Phát hiện và ngăn chặn xâm nhập (IDS/IPS): Giám sát lưu lượng mạng để phát hiện các hành vi bất thường.
* Bảo mật VPN:
  + Được triển khai để mã hóa dữ liệu khi nhân viên kết nối từ xa qua mạng công cộng.

*5. Cách thức hoạt động và truyền tải dữ liệu*

* Dữ liệu giữa các VLAN được truyền tải thông qua các Switch Core, được định tuyến qua Firewall để đảm bảo không có lưu lượng trái phép nào truy cập được vào hệ thống.
* Các kết nối ra Internet từ DMZ (như Web Server hoặc FTP) được giám sát chặt chẽ qua tường lửa ASA.

*6. Ưu điểm của mô hình*

* Bảo mật cao: Các lớp bảo mật như VLAN, Firewall, và IDS/IPS đảm bảo dữ liệu không bị xâm phạm.
* Phân quyền rõ ràng: Các bộ phận khác nhau được cách ly mạng qua VLAN, đảm bảo mỗi phòng ban chỉ truy cập được tài nguyên của mình.
* Khả năng mở rộng: Hệ thống hỗ trợ thêm thiết bị và mở rộng VLAN khi cần thiết.
* Hiệu suất cao: Switch Core đảm bảo băng thông và độ tin cậy cho các luồng dữ liệu nội bộ.

### **2.4.4. Ứng dụng**

Hệ thống đảm bảo an toàn cho các dữ liệu quan trọng như báo cáo tài chính, thông tin khách hàng, và đơn hàng.

Web Server cung cấp nền tảng thương mại điện tử ổn định và bảo mật cho khách hàng truy cập.

Hỗ trợ các hoạt động làm việc từ xa trong môi trường an toàn, giúp nâng cao hiệu quả làm việc của nhân viên.

Các giải pháp bảo mật tiên tiến như tường lửa, xác thực hai lớp, và IDS/IPS đảm bảo hệ thống hoạt động liên tục và ổn định trước các nguy cơ tấn công mạng.

### **2.5. Thực nghiệm mô hình mạng an toàn cho công ty cổ phần thương mại Hồng Anh**

* + 1. **Giới thiệu chung về Cisco Packet Tracer**
* **Khái niệm**

Cisco Packet Tracer là phần mềm mô phỏng mạng miễn phí được phát triển bởi Cisco Systems. Nó cho phép người dùng thiết kế, cấu hình và mô phỏng các mạng máy tính một cách trực quan và hiệu quả. Cisco Packet Tracer được sử dụng rộng rãi trong giáo dục, đào tạo, nghiên cứu, phát triển và quản trị mạng.

Ngoài ra phần mềm này cũng được sử dụng chủ yếu để dạy về các chứng chỉ quốc tế CCNA, CCENT. Cisco Packet Tracer được ra mắt lần đầu tiên vào năm 2006.Kể từ đó, nó đã được cập nhật liên tục với nhiều tính năng mới và cải tiến. Phiên bản mới nhất là Cisco Packet Tracer 8.2.2, được phát hành vào tháng 4 năm 2024.

1. **Các tính năng của Cisco Packet Tracer**

* Thiết bị không giới hạn: Người dùng có thể tạo và cấu hình một số lượng thiết bị mạng không giới hạn trong quá trình mô phỏng, rất tiện lợi khi thiết kế và thử nghiệm quy mô mạng phức tạp.
* Học trực tuyến: Packet Tracer đi kèm với nhiều tài nguyên giáo dục mạng hỗ trợ người dùng nắm vững các khái niệm và thiết bị mạng.
* Tùy chỉnh hoạt động người dùng: Phần mềm cho phép tạo và điều chỉnh các hoạt động học tập cho cá nhân hoặc nhóm, giúp giáo viên thiết kế bài học và bài tập phù hợp với nhu cầu của học sinh.
* Môi trường tương tác: Giao diện người dùng của Packet Tracer trực quan và dễ tương tác và theo dõi hiệu suất mạng mô phỏng.
* Trực quan hóa mạng: Packet Tracer cung cấp nhiều công cụ trực quan giúp người dùng theo dõi luồng dữ liệu, thông tin bảng định tuyến và chuyển mạch, cùng với hiệu suất mạng.
* Hai chế độ hoạt động: Chế độ thời gian thực cho phép tương tác với mạng như mạng thực tế, trong khi chế độ mô phỏng cho phép điều chỉnh tốc độ mô phỏng.
* Tự học theo nhịp độ: Packet Tracer hỗ trợ việc học tập và thực hành các kỹ năng mạng tương thích với tốc độ cá nhân của người dùng.
* Hỗ trợ nhiều giao thức mạng: Phần mềm hỗ trợ các giao thức mạng phổ biến như EGRP, [OSPF](https://vietnix.vn/giao-thuc-ospf-la-gi/), RIP, [ICMP](https://vietnix.vn/icmp-la-gi/), UDP, TCP và IP để người dùng thực hành.
* Hỗ trợ đa ngôn ngữ: Packet Tracer hỗ trợ nhiều ngôn ngữ, bao gồm tiếng Anh, tiếng Pháp, tiếng Đức, tiếng Trung Quốc và tiếng Nhật phù hợp với người dùng toàn cầu.

1. **Lợi ích của Cisco Packet Tracer**

Những lợi ích mà người dùng đạt được khi sử dụng Cisco Packet Tracer là:

* Kiểm tra mạng và phát hiện lỗi: Packet Tracer giúp bạn kiểm tra và phát hiện lỗi mạng dễ dàng, từ đó cải thiện kỹ năng sửa lỗi và tối ưu hóa mạng hiệu quả.
* Giảm chi phí: Vì là công cụ miễn phí, Packet Tracer giúp giảm đáng kể chi phí đào tạo mạng cho cả cá nhân và doanh nghiệp.
* Tiết kiệm thời gian: Khi dùng Packet Tracer, bạn có thể luyện tập thiết kế mạng mà không cần đến thiết bị thực tế, giúp tiết kiệm thời gian và tài nguyên.
* Thực hành trong môi trường an toàn: Phần mềm cung cấp môi trường ảo để thực hành và thử nghiệm các kỹ thuật mạng hiệu quả mà không cần thiết bị vật lý.
* Chuẩn bị cho kỳ thi chứng chỉ mạng: Packet Tracer là công cụ quan trọng để bạn luyện tập, kiểm tra kiến thức và chuẩn bị cho các chứng chỉ của Cisco như CCNA (Cisco Certified Network Associate) và [CCNP](https://vietnix.vn/ccnp-la-gi/) (Cisco Certified Network Professional).

1. **Ứng dụng thực tế của Cisco Packet Tracer**

Cisco Packet Tracer là một công cụ hữu ích với nhiều ứng dụng thực tế trong các lĩnh vực liên quan đến mạng máy tính và công nghệ thông tin. Trước hết, phần mềm này cho phép người dùng mô hình hóa mạng, giúp thiết kế và thử nghiệm mạng trước khi triển khai thực tế, đảm bảo hiệu suất hoạt động đáp ứng mong đợi. Ngoài ra, Cisco Packet Tracer hỗ trợ tìm hiểu và thử nghiệm các giao thức mạng, giúp người dùng hiểu sâu hơn về cách thức hoạt động của từng giao thức cụ thể. Đây cũng là lựa chọn lý tưởng cho việc nghiên cứu và phát triển các dự án mạng, tạo điều kiện phát triển ý tưởng cũng như thử nghiệm các giải pháp mạng phức tạp. Đặc biệt, công cụ này hỗ trợ hiệu quả cho hoạt động giảng dạy từ xa, giúp xây dựng bài giảng và tổ chức các hoạt động học tập trực tuyến liên quan đến mạng. Không chỉ dừng lại ở đó, Cisco Packet Tracer còn nổi bật với khả năng tạo môi trường thử nghiệm cho các ứng dụng và kịch bản IoT nhờ tích hợp thiết bị IoT. Thêm vào đó, phần mềm còn hỗ trợ tích hợp mã Python và tự động hóa mạng, tạo điều kiện phát triển các ứng dụng và kịch bản thử nghiệm một cách nhanh chóng và hiệu quả.

1. **Ứng dụng thực tiễn:**

Cisco Packet Tracer có thể được sử dụng trong:

Thiết kế và kiểm thử các mô hình mạng LAN/WAN.

Giảng dạy và học tập các khái niệm mạng.

Thực hành các kỹ năng cần thiết để thi chứng chỉ CCNA, CCNP.

Phân tích và xử lý lỗi mạng trước khi triển khai thực tế.

1. **Ví dụ về cách Cisco Packet Tracer hoạt động:**

Kịch bản: Kết nối hai máy tính thông qua router và switch

Mục tiêu: Mô phỏng một mạng đơn giản để kết nối hai máy tính qua một switch và một router. Đảm bảo hai máy tính có thể giao tiếp thông qua giao thức TCP/IP.

Các bước thiết lập trong Cisco Packet Tracer

*1. Thiết lập các thiết bị:*

* Kéo và thả một Router (ví dụ: Router1) vào không gian làm việc.
* Kéo và thả một Switch (ví dụ: Switch1) vào không gian làm việc.
* Kéo và thả hai PC (ví dụ: PC2 và PC3) vào không gian làm việc.

*2. Kết nối các thiết bị:*

* Kết nối PC2 với Switch1: Sử dụng cáp Ethernet (Copper Straight-Through) và kết nối PC2 đến một cổng bất kỳ trên Switch1.
* Kết nối PC3 với Switch1: Tương tự, kết nối PC3 đến một cổng bất kỳ trên Switch1 bằng cáp Ethernet.
* Kết nối Switch1 với Router1: Sử dụng cáp Ethernet, kết nối một cổng trên Switch1 với cổng FastEthernet0/0 trên Router1.

*3. Cấu hình địa chỉ IP cho các thiết bị:*

* PC2:
  + IP Address: 192.168.2.2
  + Subnet Mask: 255.255.255.0
  + Default Gateway: 192.168.2.1
* PC3:
  + IP Address: 192.168.2.3
  + Subnet Mask: 255.255.255.0
  + Default Gateway: 192.168.2.1
* Router1:
  + Truy cập cổng FastEthernet0/0 trên Router1 và cấu hình:
    - IP Address: 192.168.2.1
    - Subnet Mask: 255.255.255.0

*4. Kiểm tra kết nối:*

* Thực hiện lệnh ping:
  + Mở Command Prompt trên PC2 và nhập lệnh: ping 192.168.2.3
  + Nếu cấu hình chính xác, bạn sẽ nhận được phản hồi từ PC3 (Reply from 192.168.2.3).

*5. Giải thích hoạt động:*

* Khi PC2 gửi một gói tin đến PC3:
  + Switch1 sẽ nhận gói tin, kiểm tra địa chỉ MAC đích, và chuyển tiếp đến cổng tương ứng với PC3.
  + Nếu cấu hình IP, Subnet Mask, và Gateway chính xác, PC3 sẽ nhận và phản hồi lại gói tin.

1. *Kết quả:*

* Nếu lệnh ping thành công, bạn chứng minh được rằng PC2 có thể giao tiếp với PC3 thông qua switch và router.
  + 1. **Mục tiêu của hệ thống thực nghiệm:**

*1. Mục tiêu tổng quát của hệ thống*

Mục tiêu của hệ thống thực nghiệm là kiểm tra và đánh giá hiệu quả hoạt động của mô hình mạng an toàn được thiết kế, đảm bảo đáp ứng các yêu cầu về hiệu suất và bảo mật trước khi triển khai thực tế. Trước hết, hệ thống sẽ đánh giá hiệu suất mạng, xác định khả năng xử lý khi đối mặt với lưu lượng cao hoặc các tình huống giả lập thực tế. Đồng thời, các biện pháp bảo mật như tường lửa, VPN, IDS/IPS và phân vùng DMZ sẽ được kiểm tra để đảm bảo tính hiệu quả trong việc bảo vệ mạng. Bên cạnh đó, hệ thống thực nghiệm còn tập trung phân tích và phát hiện lỗ hổng, từ đó khắc phục các điểm yếu nhằm đảm bảo tính toàn vẹn trước khi triển khai trên quy mô lớn. Một mục tiêu quan trọng khác là kiểm tra khả năng mở rộng của hệ thống, đảm bảo thêm người dùng hoặc thiết bị mới mà không ảnh hưởng đến hiệu suất chung. Ngoài ra, hệ thống cung cấp môi trường thử nghiệm thực tế để đào tạo nhân sự IT, giúp họ làm quen và nâng cao kỹ năng quản trị mạng. Cuối cùng, thông qua các số liệu thu thập được, hệ thống sẽ đưa ra các khuyến nghị và đề xuất cải tiến nhằm hoàn thiện mô hình mạng trước khi chính thức đưa vào sử dụng.

1. *Yêu cầu bảo mật của Công ty CP Thương Mại Hồng Anh*

Hệ thống thực nghiệm được xây dựng nhằm đáp ứng các yêu cầu bảo mật và vận hành hiệu quả, đảm bảo an toàn cho toàn bộ tài nguyên mạng và các hoạt động nội bộ của công ty. Các mục tiêu cụ thể bao gồm:

1. *Đảm bảo xác thực và kiểm soát truy cập:*

Hệ thống triển khai cơ chế xác thực mạnh mẽ, cho phép chỉ những nhân viên và thiết bị được cấp quyền mới có thể truy cập vào mạng.

Ứng dụng các hình thức xác thực tiên tiến như 802.1X, RADIUS server, và xác thực đa yếu tố (MFA) nhằm ngăn chặn các truy cập trái phép từ bên ngoài.

1. *Bảo vệ dữ liệu truyền tải:*

Áp dụng các giao thức bảo mật hiện đại như WPA3 và AES-256 để mã hóa toàn bộ dữ liệu trong quá trình truyền tải qua mạng, giảm thiểu nguy cơ nghe lén hoặc đánh cắp dữ liệu.

Đảm bảo rằng các thông tin nhạy cảm được bảo vệ trong suốt quá trình vận hành của hệ thống.

1. *Phát hiện và ngăn chặn xâm nhập:*

Tích hợp hệ thống tường lửa (Firewall) và hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS) để giám sát, nhận diện và ngăn chặn các mối đe dọa như tấn công DoS/DDoS, truy cập trái phép hoặc khai thác lỗ hổng bảo mật.

Kịp thời phát hiện và xử lý các mối nguy nhằm bảo đảm sự ổn định của hệ thống.

1. *Bảo vệ thiết bị đầu cuối:*

Triển khai phần mềm bảo mật và chống virus trên tất cả các thiết bị đầu cuối như máy tính, laptop, điện thoại nhằm ngăn chặn các phần mềm độc hại.

Sử dụng các công cụ quản lý thiết bị đầu cuối (MDM hoặc Endpoint Security) để theo dõi, quản lý và đảm bảo các thiết bị này không trở thành nguồn lây nhiễm hoặc làm suy yếu hệ thống.

1. *Giám sát và quản lý bảo mật:*

Hệ thống được tích hợp công cụ giám sát theo thời gian thực, ghi nhận và phân tích các sự kiện, đưa ra cảnh báo khi phát hiện hành vi bất thường.

Sử dụng hệ thống SIEM (Security Information and Event Management) để quản lý và xử lý sự cố bảo mật nhanh chóng, giảm thiểu thiệt hại do các vấn đề bảo mật gây ra.

1. *Cập nhật và vá lỗi bảo mật thường xuyên:*

Duy trì việc cập nhật định kỳ firmware của các thiết bị mạng và phần mềm bảo mật để đảm bảo hệ thống không tồn tại các lỗ hổng bảo mật dễ bị khai thác.

Đảm bảo hệ thống luôn đáp ứng các tiêu chuẩn bảo mật hiện đại và sẵn sàng đối phó với các mối đe dọa mới. Những mục tiêu này nhằm xây dựng một hệ thống mạng mạnh mẽ, bảo mật và linh hoạt, hỗ trợ hoạt động kinh doanh của công ty một cách an toàn và hiệu quả.

1. *Các chỉ tiêu đánh giá thành công của hệ thống*

Các chỉ tiêu đánh giá thành công của hệ thống mạng tại Công ty Cổ phần Hồng Anh

Để đánh giá mức độ thành công của hệ thống mạng được thiết kế trong mô hình, các tiêu chí cụ thể bao gồm:

1. *Băng thông và hiệu suất*

* Tiêu chí:

Tốc độ kết nối trong hệ thống mạng đảm bảo đáp ứng yêu cầu sử dụng của từng bộ phận, với băng thông tối thiểu đạt từ 1 Gbps cho các kết nối nội bộ.

Độ trễ (latency) ở mức thấp, đảm bảo hiệu suất cho các dịch vụ quan trọng như truyền file lớn, họp trực tuyến và ứng dụng nội bộ.

Hệ thống chịu tải tốt với khả năng kết nối đồng thời cho nhiều thiết bị (trên 500 thiết bị trong toàn hệ thống).

* Đánh giá thành công:

Hệ thống mạng hoạt động ổn định, không xảy ra tình trạng nghẽn mạng hoặc gián đoạn khi nhiều bộ phận sử dụng đồng thời.

1. *Tính bảo mật*

* Tiêu chí:

Triển khai các cơ chế xác thực mạnh mẽ như RADIUS server và xác thực đa yếu tố (MFA) cho các thiết bị và người dùng.

Dữ liệu truyền tải được mã hóa bằng các giao thức tiên tiến như AES-256 và IPsec.

Tỷ lệ phát hiện và ngăn chặn các cuộc tấn công mạng (bao gồm xâm nhập trái phép và tấn công DoS/DDoS) đạt trên 95%.

Không xảy ra sự cố rò rỉ thông tin quan trọng trong quá trình triển khai và vận hành.

* Đánh giá thành công:

Không có vi phạm bảo mật nghiêm trọng xảy ra, hệ thống đảm bảo an toàn cho toàn bộ dữ liệu và hoạt động của công ty.

1. *Tính ổn định*

* Tiêu chí:

Độ sẵn sàng (uptime) của hệ thống đạt trên 99.9%, đảm bảo mạng luôn hoạt động liên tục.

Thời gian khắc phục sự cố không quá 15 phút với các vấn đề nhỏ và không quá 1 giờ với các vấn đề lớn.

* Đánh giá thành công:

Hệ thống hoạt động ổn định, không có tình trạng mất kết nối đột ngột hoặc ảnh hưởng đến các hoạt động kinh doanh.

1. *Khả năng mở rộng*

* Tiêu chí:

Dễ dàng mở rộng quy mô để hỗ trợ thêm các bộ phận, văn phòng, hoặc khu vực mới khi công ty phát triển.

Các nâng cấp phần cứng và phần mềm được thực hiện với chi phí hợp lý, không làm giảm hiệu suất mạng.

* Đánh giá thành công:

Hệ thống có khả năng mở rộng linh hoạt, đáp ứng đầy đủ các nhu cầu phát triển trong tương lai của công ty.

1. *Khả năng quản lý và giám sát*

* Tiêu chí:

Hệ thống cung cấp công cụ quản lý tập trung (Centralized Management) giúp giám sát toàn bộ hoạt động mạng và thiết bị trong thời gian thực.

Các cảnh báo bảo mật và báo cáo chi tiết được tự động gửi đến quản trị viên khi phát hiện sự cố hoặc hành vi bất thường.

* Đánh giá thành công:

Quản trị viên có thể nhanh chóng phát hiện và xử lý các vấn đề, duy trì tính ổn định và bảo mật của hệ thống mạng thông qua các công cụ giám sát.

*4. Liên hệ mục tiêu với các giải pháp thực tế hiện nay cho hệ thống mạng Công ty Cổ phần Hồng Anh*

*a. Xây dựng hệ thống mạng nội bộ an toàn*

Giải pháp bảo mật: Để bảo vệ an toàn cho mạng nội bộ của Công ty Cổ phần Hồng Anh, các giải pháp sau cần được triển khai:

* Mã hóa dữ liệu truyền tải: Sử dụng các giao thức mã hóa mạnh như IPsec hoặc AES-256 để bảo vệ dữ liệu khi truyền qua mạng nội bộ, đặc biệt là giữa các VLAN và khu vực DMZ.
* VPN (Virtual Private Network): Đảm bảo kết nối an toàn từ xa cho nhân viên truy cập hệ thống thông qua VPN, ngăn chặn các rủi ro từ môi trường bên ngoài.
* Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Tích hợp IDS/IPS vào hệ thống firewall (ASA 5506-X) để giám sát và ngăn chặn các mối đe dọa tiềm tàng, như tấn công DoS/DDoS hoặc khai thác lỗ hổng.
* Quản lý quyền truy cập: Sử dụng xác thực đa yếu tố (MFA) và RADIUS server để kiểm soát quyền truy cập vào từng VLAN, đảm bảo chỉ có người dùng hợp lệ được phép truy cập tài nguyên mạng.
* Tường lửa: Thiết lập firewall trên ASA và các gateway để lọc lưu lượng không mong muốn từ bên ngoài, ngăn ngừa tấn công vào các máy chủ trong vùng DMZ.

*b. Đảm bảo hiệu quả hoạt động*

Giải pháp tăng cường hiệu suất: Để đảm bảo hiệu suất của mạng và đáp ứng nhu cầu sử dụng lớn, các giải pháp sau cần được thực hiện:

* Mạng LAN tốc độ cao: Sử dụng switch core với chuẩn gigabit để đảm bảo tốc độ truyền tải dữ liệu nhanh giữa các VLAN và các bộ phận.
* Tối ưu hóa băng thông: Áp dụng các chính sách QoS (Quality of Service) để ưu tiên lưu lượng quan trọng như email nội bộ, họp trực tuyến hoặc truyền file.
* Mạng riêng ảo (VLAN): Phân chia mạng thành các VLAN (như VLAN 10, VLAN 20, VLAN 30...) để giảm thiểu xung đột lưu lượng và tăng khả năng quản lý mạng.
* Wi-Fi Mesh hoặc điểm truy cập mở rộng: Mở rộng vùng phủ sóng tại các văn phòng chi nhánh hoặc khu vực cần sử dụng Wi-Fi, đảm bảo kết nối ổn định và loại bỏ điểm chết.

*c. Tính ổn định và khả năng mở rộng*

Giải pháp tăng cường ổn định và khả năng mở rộng: Để đảm bảo hệ thống hoạt động ổn định và dễ dàng mở rộng, các giải pháp sau được khuyến nghị:

* Wi-Fi Mesh: Tích hợp hệ thống Wi-Fi Mesh tại các văn phòng lớn hoặc khu vực có nhiều tầng để tăng cường vùng phủ sóng mà không làm giảm hiệu suất mạng.
* Chuyển mạch tự động (Auto-switching): Tích hợp khả năng chuyển đổi giữa các kết nối mạng khi xảy ra sự cố để đảm bảo hệ thống luôn duy trì kết nối ổn định.
* Chia tải (Load Balancing): Sử dụng kỹ thuật chia tải trên các thiết bị mạng, đặc biệt tại switch core, để tối ưu hóa việc phân phối lưu lượng mạng.
* Quản lý tự động (SD-WAN): Triển khai SD-WAN để quản lý và tối ưu hóa kết nối giữa các văn phòng hoặc chi nhánh, đảm bảo hệ thống sẵn sàng cho sự phát triển trong tương lai.

*d. Khả năng quản lý và giám sát*

Giải pháp quản lý mạng: Để đảm bảo mạng được giám sát và quản lý hiệu quả, cần triển khai các công cụ:

* Giám sát thời gian thực: Sử dụng các công cụ giám sát như SolarWinds hoặc PRTG để theo dõi hiệu suất mạng và phát hiện sự cố kịp thời.
* Quản lý tập trung: Thiết lập hệ thống quản lý tập trung cho toàn bộ mạng nội bộ, từ các thiết bị trong VLAN đến vùng DMZ.
* Hệ thống SIEM: Áp dụng giải pháp SIEM để thu thập, phân tích và đưa ra cảnh báo về các sự kiện bảo mật, đảm bảo quản trị viên mạng phản ứng nhanh với các mối đe dọa tiềm tàng.

## **Thiết kế kịch bản chương trình**

1. *Mô tả chi tiết kịch bản mô phỏng*
   1. *Tổng quan về mạng*

* Mạng công ty này gồm 5 phòng làm việc (Giám đốc, Kế toán, Marketing, Nhân sự, IT) và 1 phòng máy chủ (chứa 3 server: DNS, Email, FTP). Mạng sử dụng các thiết bị cơ bản như router, switch, máy tính và máy chủ.
  1. *Các thành phần trong mạng*
* Phòng ban:
  + Giám đốc:
    - 1 máy tính để giám đốc làm việc.
    - 1 laptop để giám đốc làm việc khi cần.
  + Kế toán:
    - 10 máy tính và 4 laptop cho các kế toán viên.
    - 1 máy tính và 1 laptop cho kế toán trưởng.
  + Marketing:
    - 15 máy tính và 10 laptop cho các nhân viên sale, nhân viên quảng cáo.
    - 1 máy tính và 1 laptop cho trưởng phòng marketing.
  + Nhân sự:
    - 5 máy tính cho các nhân viên phòng nhân sự.
    - 1 máy tính và 1 laptop cho trưởng phòng nhân sự.
  + IT:
    - 10 máy tính và 20 laptop cho các nhân viên lập trình, 4 máy tính cho nhân viên kiểm thử, 2 máy tính và 1 laptop cho nhân viên hỗ trợ kĩ thuật.
    - 1 máy tính và 1 laptop cho trưởng phòng IT.
* Phòng máy chủ:
  + Gồm 3 server:
    - Server mail: Quản lý và lưu trữ email nội bộ của công ty.
    - Server FTP: Quản lý và cung cấp dịch vụ chia sẻ tệp tin qua giao thức FTP.
    - Server DNS: Cung cấp dịch vụ phân giải tên miền cho các máy tính trong mạng.
  1. *Thiết bị và kết nối*
* Router: Cung cấp kết nối Internet cho mạng nội bộ của công ty.
* Switch:
  + Mỗi phòng ban sẽ có một switch layer 2 để kết nối các thiết bị trong phòng.
  + Phòng máy chủ cũng dùng một switch layer 2 để kết nối các Server trong phòng.
  + Các switch thuộc các phòng ban sẽ được kết nối với một switch chính layer 3 chịu trách nhiệm cung cấp IP động cho các thiết bị và phân chia các VLAN cho các phòng.
* Access Point:
  + Mỗi phòng ban sẽ có một access point cung cấp Internet không dây cho các thiết bị không dây.

1. *Chi tiết cấu hình mạng*

* Kết nối Router với Switch:
  + Router sẽ kết nối trực tiếp đến một switch trung tâm, từ đó các phòng ban sẽ kết nối đến các switch của mình.
  + Các switch sẽ nối với nhau để tạo thành một mạng LAN liên tục.
* Cổng mạng của Router:
  + Cổng của router sẽ được cấu hình với địa chỉ IP 192.168.0.1 cho mạng LAN.
* Switches và Cấu Hình Mạng LAN:
  + Switch trong mỗi phòng:
    - Các switch trong mỗi phòng ban sẽ kết nối trực tiếp với switch trung tâm.
    - Ví dụ: Phòng Giám đốc sẽ có 1 switch nối với swith chính qua cổng FastEthernet hoặc GigabitEthernet.
  + Máy Tính trong các phòng:
    - Các máy tính trong các phòng sẽ được cấu hình với IP động. Các địa chỉ IP trong phòng ban có thể được phân bổ như sau:
      * Phòng giám đốc: 192.168.10.0/24 -> 192.168.10.254.
      * Phòng kế toán: 192.168.20.0/24 -> 192.168.20.254.
      * Phòng Kinh Doanh: 192.168.30.0/24 -> 192.168.30.254.
      * Phòng Kho: 192.168.40.0/24 -> 192.168.40.254.
      * Phòng Xuất nhập khẩu: 192.168.50.0/24 -> 192.168.50.254.
  + Máy chủ
    - Các máy chủ trong phòng sẽ được cấu hình với IP tĩnh. Các địa chỉ IP có thể được phân bổ như sau:
      * Server mail: 192.168.2.2.
      * Server FTP: 192.168.2.4.
      * Server DNS: 192.168.2.3.
      * Server Internet : 8.8.8.8.

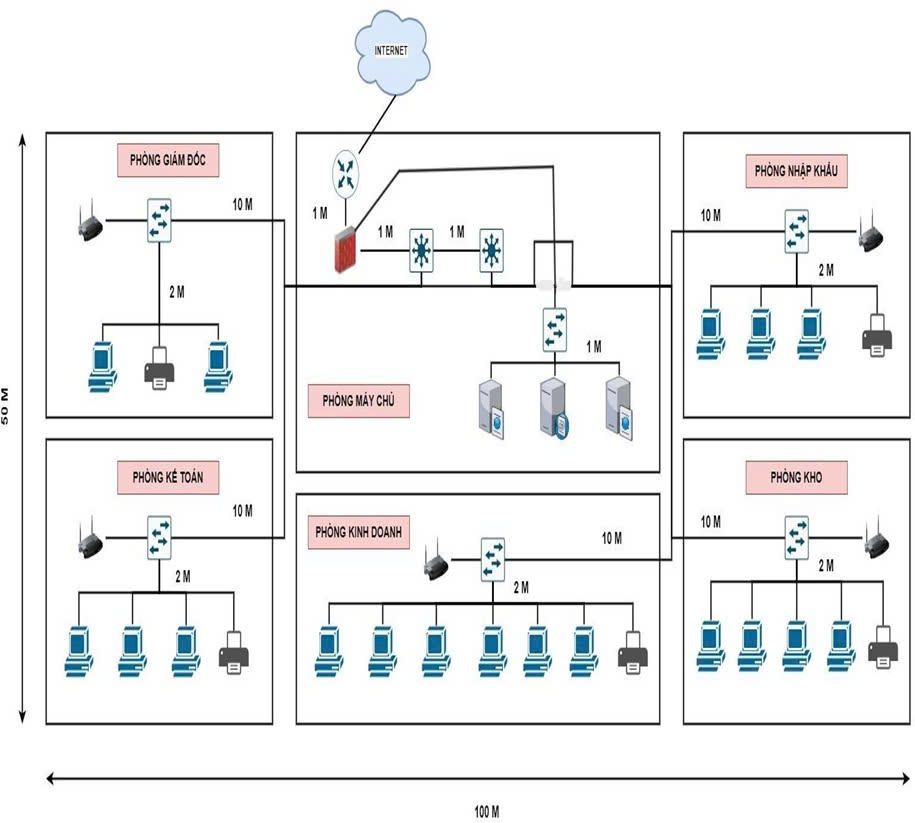
1. Chi tiết các dịch vụ

* Server mail:
  + Cấu hình Server Email: Máy chủ email sẽ cung cấp dịch vụ thư điện tử nội bộ cho tất cả các phòng ban. Các máy tính trong mạng sẽ được cấu hình để sử dụng máy chủ email này làm máy chủ gửi/nhận email.
* Server FTP:
  + Cấu hình FTP Server: Máy chủ FTP sẽ cung cấp dịch vụ chia sẻ tệp tin nội bộ. Các nhân viên trong công ty có thể lưu trữ và truy cập tài liệu từ các thư mục được chia sẻ trên FTP Server.
* Server DNS:
  + Cấu hình DNS: Máy chủ DNS sẽ chịu trách nhiệm phân giải các tên miền nội bộ (ví dụ: email.company.local, ftp.company.local) thành các địa chỉ IP cho các máy tính trong mạng và cung cấp dịch vụ HTTP nội bộ cho công ty.

1. *Các bước triển khai kịch bản*
   1. *Phân tích yêu cầu và lập kế hoạch.*

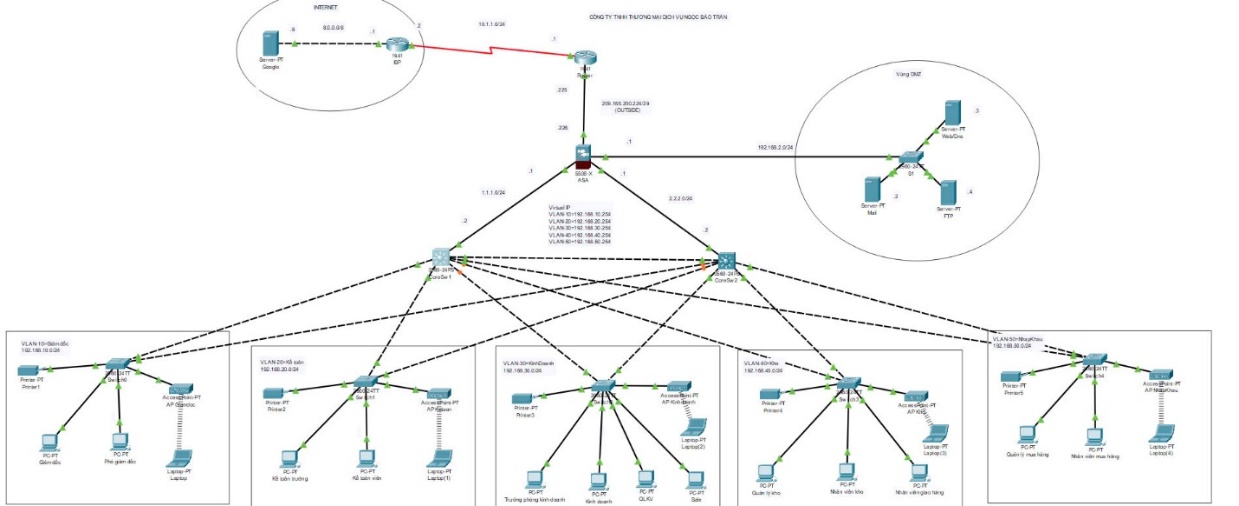
* Xác định mục tiêu của mô hình mạng.
* Liệt kê các thiết bị cần thiết.
* Lập sơ đồ mạng sơ bộ.
* Xác định các thông số cấu hình quan trọng.
  1. *Thiết lập topology vật lý.*
* Chọn và đặt các thiết bị mạng trên workspace.
* Kết nối các thiết bị bằng cáp phù hợp.
* Sắp xếp các thiết bị một cách logic và dễ nhìn.
* Đặt tên cho các thiết bị và interface.
  1. *Cấu hình cơ bản.*
* Cấu hình địa chỉ IP cho các interface.
* Thiết lập hostname và các thông số cơ bản
* Cấu hình VLAN cần thiết.
* Thiết lập các thông số không dây cơ bản.
  1. *Cấu hình routing*
* Chọn và cấu hình giao thức định tuyến phù hợp
* Thiết lập các route tĩnh nếu cần.
* Kiểm tra bảng định tuyến.
  1. *Cấu hình dịch vụ*
* Thiết lập DHCP server.
* Cấu hình DNS.
* Thiết lập các dịch vụ khác như web server, FTP,..
* Cấu hình NAT nếu cần.
  1. *Cấu hình báo mật*
* Thiết lập mật khẩu cho các thiết bị access point bằng WPA2-PSK.
* Cấu hình các phương thức xác thực.
  1. *Kiểm tra và tối ưu hóa*
* Thực hiện các lệnh ping và traceroute để kiểm tra kết nối.
* Tối ưu hóa các thông số cấu hình dựa trên kết quả test.
  1. *Tài liệu*
* Ghi chép lại các cấu hình đã thực hiện.
* Tạo sơ đồ mạng chi tiết.
* Lưu trữ file cấu hình.
* Tạo tài liệu hướng dẫn vận hành.

1. *Sơ đồ triển khai thiết kế mạng cho công ty*
2. *Sơ đồ vật lý*

****

Hình 2.5: Sơ đồ vật lý mạng công ty CP Hồng Anh

1. *Sơ đồ logic*

****

Hình 2.6: Sơ đồ logic hệ thống mạng công ty CP Hồng Anh

1. *Các thông số kĩ thuật cần thiết*

* Bảng địa chỉ IP cho các thiết bị

*Bảng 2.1: Thông số địa chỉ IP của các thiết bị*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thiết bị** | **Cổng** | **IP** | **Network mask** | **Default**  **gateway** |
| ISP | GigabitEthernet0/0 | 8.8.8.1 | 255.0.0.0 | N |
| Serial0/0/0 | 10.1.1.2 | 255.255.255.252 | N |
| Router | GigabitEthernet0/0 | 209.165.200.225 | 255.255.255.248 | N |
| Serial0/0/0 | 10.1.1.1 | 255.255.255.0 | N |
| Firewall ASA | GigabitEthernet1/1 | 209.165.200.226 | 255.255.255.248 | N |
| GigabitEthernet1/3 | 192.168.2.1 | 255.255.255.0 | N |
| GigabitEthernet1/4 | 2.2.2.1 | 255.255.255.0 | N |
| GigabitEthernet1/5 | 1.1.1.1 | 255.255.255.0 | N |
| CoreSw1 | GigabitEthernet0/2 | 1.1.1.2 | 255.255.255.0 | N |
| Vlan 10 | 192.168.10.1 | 255.255.255.0 | N |
| Vlan 20 | 192.168.20.1 | 255.255.255.0 | N |
| Vlan 30 | 192.168.30.1 | 255.255.255.0 | N |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Vlan 40 | 192.168.40.1 | 255.255.255.0 | N |
| Vlan 50 | 192.168.50.1 | 255.255.255.0 | N |
| CoreSw2 | GigabitEthernet0/1 | 2.2.2.2 | 255.255.255.0 | N |
| Vlan 10 | 192.168.10.2 | 255.255.255.0 | N |
| Vlan 20 | 192.168.20.2 | 255.255.255.0 | N |
| Vlan 30 | 192.168.30.2 | 255.255.255.0 | N |
| Vlan 40 | 192.168.40.2 | 255.255.255.0 | N |
| Vlan 50 | 192.168.50.2 | 255.255.255.0 | N |
| Mail | FastEthernet0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |
| Web/Dns | FastEthernet0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| FTP | FastEthernet0 | 192.168.2.4 | 255.255.255.0 | 192.168.2.1 |
| Google Server | FastEthernet0 | 8.8.8.8 | 255.0.0.0 | 8.8.8.1 |

* Kế hoạch phân bổ dải IP và chia VLAN

\* Phân bổ dải IP

*Bảng 2.2: Phân bổ dải IP cho các phòng ban*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phòng ban** | **IP** | **Network mask** | **Default gateway** | **DNS** |
| Phòng giám đốc | 192.168.10.31  → 192.168.10.254 | 255.255.255.0 | 192.168.10.254 | 209.165.200.227 |
| Phòng kế toán | 192.168.20.31  → 192.168.20.254 | 255.255.255.0 | 192.168.20.254 | 209.165.200.227 |
| Phòng kinh doanh | 192.168.30.31  → 192.168.30.254 | 255.255.255.0 | 192.168.30.254 | 209.165.200.227 |
| Phòng kho | 192.168.40.31  → 192.168.40.254 | 255.255.255.0 | 192.168.40.254 | 209.165.200.227 |
| Phòng nhập khẩu | 192.168.50.31  → 192.168.50.254 | 255.255.255.0 | 192.168.50.254 | 209.165.200.227 |

Thông tin VLAN

*Bảng 2.3: Thông tin cấu hình các VLAN*

|  |  |  |
| --- | --- | --- |
| **Vlan\_ID** | **Tên Vlan** | **Ghi chú** |
| 10 | Vlan 10 | Phòng giám đốc |
| 20 | Vlan 20 | Phòng kế toán |
| 30 | Vlan 30 | Phòng kinh doanh |
| 40 | Vlan 40 | Phòng kho |
| 50 | Vlan 50 | Phòng nhập khẩu |