ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN MÔN HỌC

THIẾT KẾ MẠNG

ĐỀ TÀI:

THIẾT LẬP HỆ THỐNG MẠNG CHO DOANH NGHIỆP

Giảng viên hướng dẫn: **ThS. Trần Thị Dung**

Lớp**: NT113.O11**

Học kỳ: **I**

Năm học: **2023-2024**

Nhóm thực hiện: **Nhóm 4**

STT	Họ và tên	MSSV
1	Nguyễn Trần Bảo Quốc	21520421
2	Trịnh Tấn Đạt	21520714
3	Nguyễn Thành Đăng	21520683

Thành phố Hồ Chí Minh, ngày 8 tháng 11 năm 2023

MỤC LỤC

1 GIỚI THIỆU TỔNG QUAN

1.1 Lời nói đầu

Báo cáo này nhằm trình bày một kế hoạch thiết kế mạng cho doanh nghiệp Outsource O-UIT. Với sự phát triển không ngừng của công nghệ thông tin và viễn thông, mạng máy tính đã trở thành một yếu tố quan trọng không thể thiếu trong hoạt động kinh doanh của các doanh nghiệp hiện đại. Việc xây dựng một hệ thống mạng hiệu quả và bảo mật đáng tin cậy là một trong những yếu tố quyết định đến sự thành công và sự phát triển của Outsource O-UIT.

Outsource O-UIT là một doanh nghiệp hoạt động trong lĩnh vực giải pháp và dịch vụ IT outsourcing, đáp ứng nhu cầu của các khách hàng trên toàn cầu. Với quy mô ngày càng lớn và mô hình hoạt động phức tạp, một hệ thống mạng vững chắc và linh hoạt là cực kỳ quan trọng để đảm bảo sự liên tục và hiệu suất cao trong các hoạt động kinh doanh của doanh nghiệp.

Báo cáo này sẽ tập trung vào việc thiết kế một mạng máy tính phù hợp cho Outsource O-UIT, bao gồm các yêu cầu kỹ thuật, cơ sở hạ tầng, bảo mật và quản lý. Nhóm đã tiến hành nghiên cứu cẩn thận về yêu cầu và môi trường hoạt động của Outsource O-UIT, từ đó đề xuất một kế hoạch thiết kế mạng chi tiết và khả thi.

1.2 Thuật ngữ sử dụng

PDC (Primary Domain Controller): Máy chủ miền chính là máy chủ chính trong một miền (domain) trong mô hình quản lý người dùng và tài nguyên mạng. Nhiệm vụ chính của PDC là duy trì cơ sở dữ liệu người dùng và quản lý các chính sách bảo mật trong miền.

ADC (Additional Domain Controller): Máy chủ miền bổ sung là máy chủ được sao chép từ PDC để cung cấp tính sẵn sàng và sự dự phòng cho hệ thống quản lý miền. ADC cũng có khả năng xử lý yêu cầu đăng nhập và truy cập người dùng trong miền.

AP (Access Point): Điểm truy cập là thiết bị không dây dùng để kết nối các thiết bị di động như máy tính, điện thoại di động hoặc máy tính bảng vào mạng không dây (Wi-Fi). AP chịu trách nhiệm phát sóng và nhận tín hiệu không dây để kết nối các thiết bị vào mạng.

TCP/IP (Transmission Control Protocol/Internet Protocol): Giao thức TCP/IP là một bộ các giao thức mạng được sử dụng rộng rãi trong môi trường Internet. Nó bao gồm giao thức TCP để quản lý việc truyền và nhận dữ liệu và giao thức IP để định tuyến và định địa chỉ cho các gói tin dữ liệu.

DHCP (Dynamic Host Configuration Protocol): Giao thức DHCP là giao thức tự động cấp phát địa chỉ IP và các thông số cấu hình mạng khác cho các thiết bị trong mạng. DHCP giúp tự động cấu hình và quản lý địa chỉ IP, subnet mask, gateway và DNS cho các máy tính và thiết bị kết nối vào mạng.

DNS (Domain Name System): Hệ thống tên miền (Domain Name System) là một hệ thống phân giải tên miền thành địa chỉ IP và ngược lại. DNS giúp chuyển đổi các tên miền (như example.com) sang địa chỉ IP tương ứng và ngược lại, giúp người dùng dễ dàng truy cập vào các tài nguyên mạng.

VLAN (Virtual Local Area Network): Mạng cục bộ ảo (Virtual Local Area Network) là một phương pháp để tạo ra các mạng ảo trên cùng một hạ tầng vật lý. VLAN cho phép tách biệt và quản lý lưu lượng mạng giữa các phân đoạn hoặc nhóm người dùng khác nhau mà không cần thay đổi cấu trúc vật lý của mạng.

VPN (Virtual Private Network): Mạng riêng ảo (Virtual Private Network) là một kết nối mạng an toàn và mã hóa được tạo ra trên mạng công cộng (như Internet) để tạo ra một mạng riêng tư. VPN cho phép truy cập an toàn vào mạng nội bộ từ xa và bảo mật thông tin truyền qua mạng.

OSPF (Open Shortest Path First): Giao thức OSPF là một giao thức định tuyến nội bộ được sử dụng trong mạng IP. OSPF sử dụng thuật toán Shortest Path First (SPF) để tìm đường đi ngắn nhất và tính toán bảng định tuyến cho các gói tin trong mạng.

SNMP (Simple Network Management Protocol): Giao thức SNMP là giao thức quản lý mạng đơn giản được sử dụng để giám sát và quản lý các thiết bị mạng trong một mạng. SNMP cho phép thu thập thông tin từ các thiết bị mạng, giám sát trạng thái và hiệu suất, và thực hiện các thao tác quản lý như cấu hình và khắc phục sự cố.

SSH (Secure Shell): SSH là một giao thức mạng được sử dụng để thiết lập kết nối mạng an toàn và mã hóa giữa hai thiết bị. Nó thường được sử dụng để truy cập từ xa vào các thiết bị mạng, như router hoặc máy chủ, và cung cấp một kênh kết nối bảo mật để truyền thông tin.

HSRP (Hot Standby Router Protocol): HSRP là một giao thức mạng được sử dụng để tạo ra một kịch bản chuyển đổi nguồn tài nguyên mạng chủ động (active/passive) giữa các router trong mạng. Mục đích chính của HSRP là đảm bảo tính sẵn sàng và độ tin cậy của mạng bằng cách cung cấp một router chủ động và một router dự phòng để đảm nhận các chức năng định tuyến và chuyển tiếp gói tin.

SWL3 (Switch Layer 3): SWL3 sử dụng để chỉ các switch có khả năng thực hiện các chức năng của một thiết bị chuyển mạch cấp 3 (Layer 3). SWL3 kết hợp cả chức năng của switch cấp 2 (Layer 2) và router cấp 3 (Layer 3) trong cùng một thiết bị.

NAT (Network Address Translation): Là một giao thức được sử dụng để chuyển đổi địa chỉ mạng trong mạng máy tính. Nó cho phép một thiết bị mạng, thường là một router hoặc firewall, thực hiện ánh xạ địa chỉ IP giữa hai miền mạng khác nhau.

LAP (Lightweight Access Point): LAP là một thuật ngữ thường được sử dụng trong các hệ thống mạng Wi-Fi để chỉ các điểm truy cập nhẹ (Lightweight Access Points). Các điểm truy cập nhẹ là các thiết bị mạng không dây được sử dụng để cung cấp kết nối mạng không dây cho các thiết bị di động như máy tính xách tay, điện thoại di động, máy tính bảng, v.v. LAP thường hoạt động dựa trên mô hình điểm truy cập và điểm truy cập sở hữu bởi một bộ điều khiển trung tâm, như một bộ điều khiển điểm truy cập (Access Point Controller) hoặc một bộ điều khiển trung tâm Wi-Fi (Wireless LAN Controller). Các LAP nhẹ thường có khả năng quản lý tập trung, quản lý cấu hình và cung cấp tính năng bảo mật cho mạng không dây.

WLC (Wireless LAN Controller): Là một thiết bị quản lý và điều khiển hệ thống mạng Wi-Fi, đặc biệt là quản lý các Access Point (AP) trong một mạng không dây.

2 PHÂN TÍCH YÊU CẦU

2.1 Thông tin được cung cấp

2.1.1 Hiện trạng công ty

Công ty Outsource O-UIT có 1 trụ sở chính tại Thủ Đức và một chi nhánh tại Quận 3. Trụ sở chính là một tòa nhà 5 tầng gồm Data Center và các văn phòng làm việc dành cho CEO, HR, Project manager, Technical Manager, Business Analyst, IT manager và các nhóm developer và tester cho các project thuộc thị trường nước ngoài. Chi nhánh tại Quận 3 là văn phòng làm việc của các nhóm developer và tester cho các project thuộc thị trường trong nước.

2.1.2 Yêu cầu từ khách hàng

Công ty cần thiết kế một mô hình hệ thống mạng cho trụ sở chính và chi nhánh với các yêu cầu cụ thể như sau:

Tại trụ sở chính:

- Developer và Tester chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop riêng để truy cập vào mạng của công ty.
- CEO, HR, Project manager, Technical Manager, Business Analyst, IT operation được sử dụng Laptop, truy cập vào hệ thống wifi nội bộ sử dụng tài khoản xác thực.
- Một hệ thống wifi public với đường kết nối Internet riêng.
- Hệ thống phần cứng để triển khai hệ thống server ảo phục vụ cho việc deploy các ứng dụng trong giai đoạn test.
- Sử dụng các dịch vụ Cloud để deploy các ứng dụng trong giai đoạn staging để khách hàng sử dụng thử trước khi đưa ra thực tế.

Tại chi nhánh:

- Developer và Tester chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop riêng để truy cập vào mạng của công ty.
- Sử dụng kết nối VPN site-to-site để truy cập server nội bộ và deploy ứng dụng lên hệ thống tại Data Center.
- Một hệ thống wifi với đường kết nối Internet riêng.

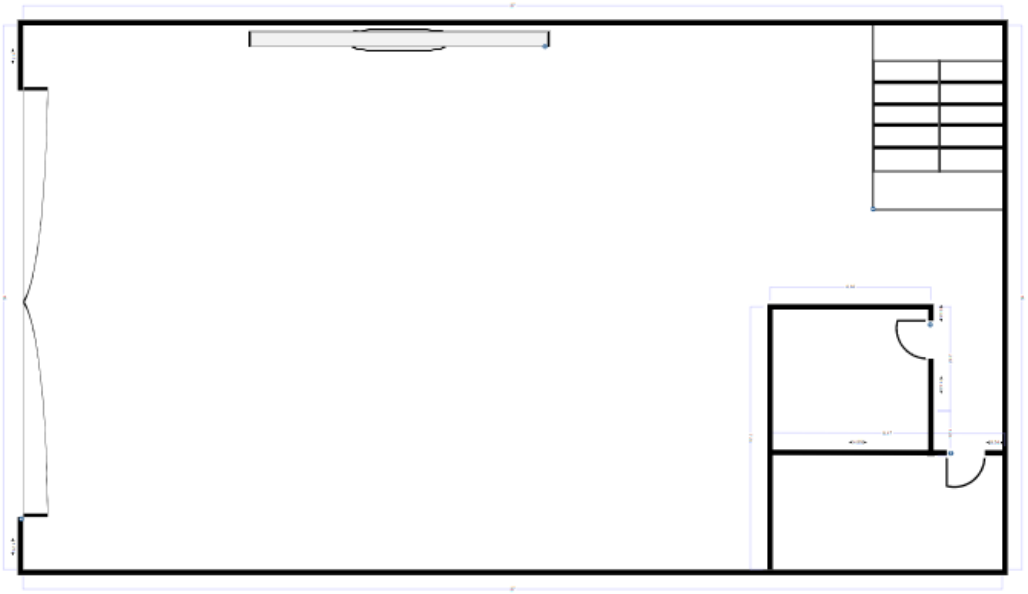
2.2 Thông tin khảo sát thực tế

2.2.1 Tại trụ sở chính

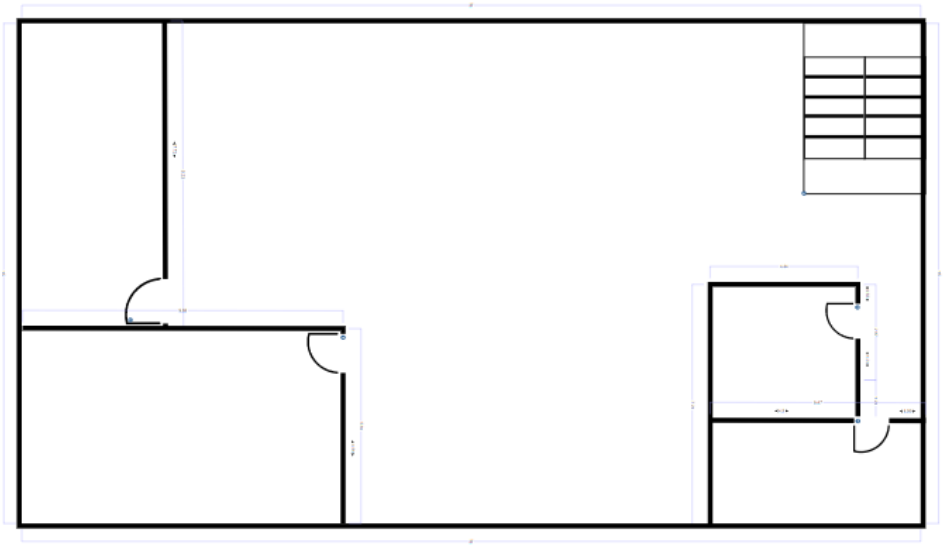
Trụ sở chính của tòa nhà bao gồm 5 tầng, với tổng cộng 47 nhân sự làm việc, bao gồm CEO. Mỗi tầng có diện tích 27m x 15m và chiều cao 4m. Tầng 2 và tầng 3 được chia thành 3 phòng, trong đó có 2 phòng nhỏ và 1 phòng lớn.

Vị trí của trụ sở được đặt ở một vị trí thông thoáng, phù hợp để xây dựng một trung tâm dữ liệu (data center). Hiện tại, chưa có hệ thống mạng được thiết lập bao gồm cả Data center.

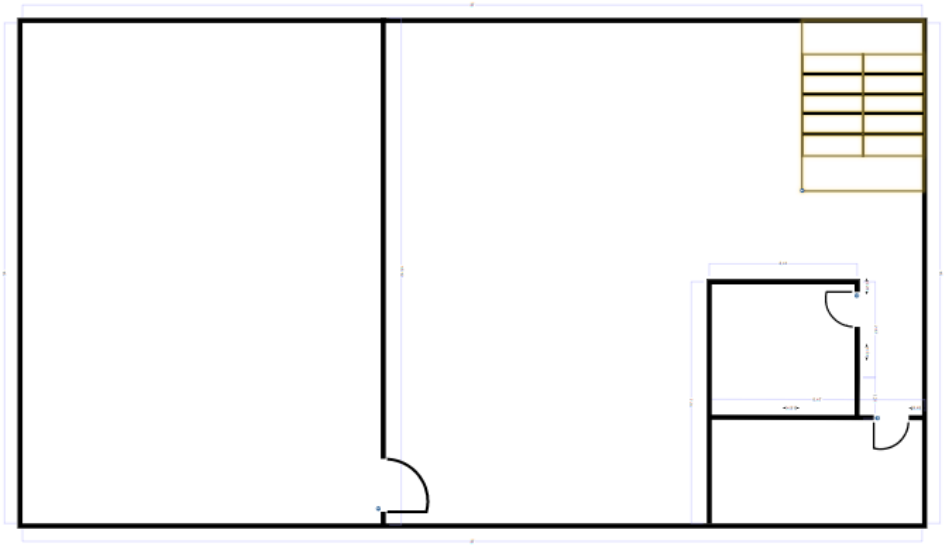
- **Sơ đồ tầng 1:**



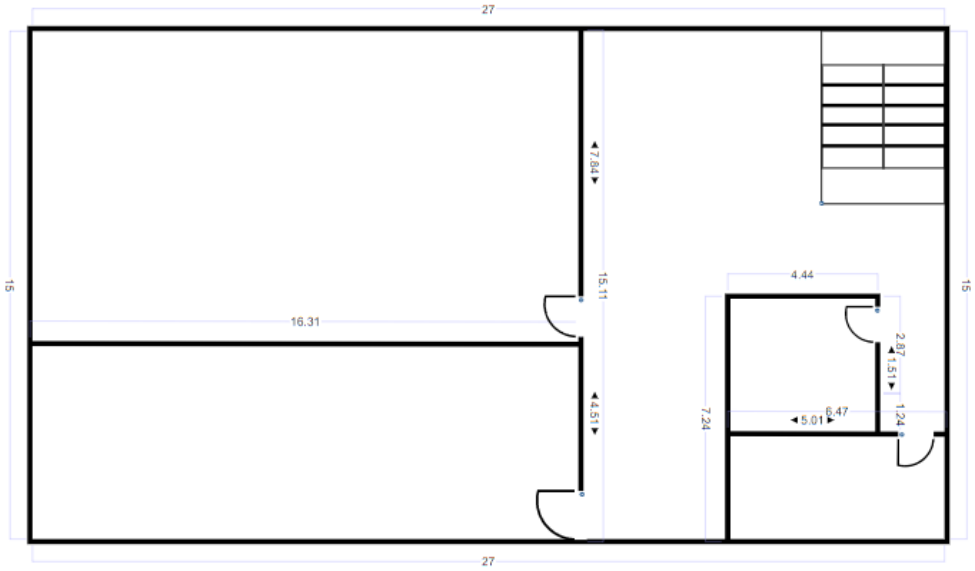
- **Sơ đồ tầng 2 và tầng 3:**



- **Sơ đồ tầng 4:**



- **Sơ đồ tầng 5:**



- **Nhân sự và nhu cầu:**

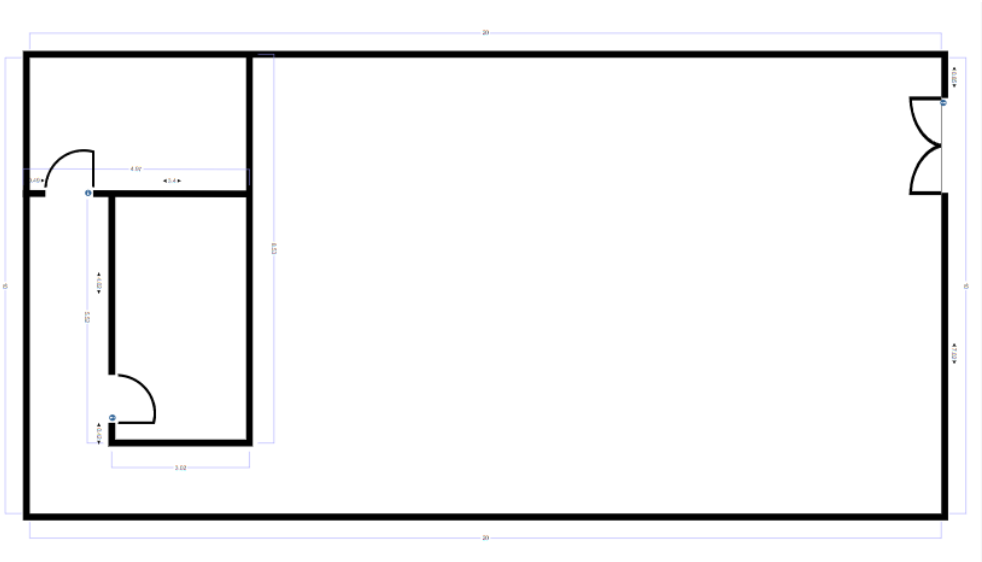
Tên nhóm	Số lượng	Ứng dụng / Thiết bị	Băng thông
Developer / Tester	26 / 6	Visual Studio Code, Web browser, Git, Docker, Microsoft Office, Microsoft Teams	20 Mbps
		Máy tính bàn	
HR Manager	2	Cflow, Microsoft Office, Web browser, Microsoft Teams	20 Mbps
		Máy tính bàn, laptop	
Project Manager	4	Web browser, Microsoft Office, Microsoft Teams, Git, Monday.com	20 Mbps
		Máy tính bàn, laptop	
Technical Manager	2	Web browser, Microsoft Office, Microsoft Teams, Monday.com	20 Mbps
		Máy tính bàn, laptop	
Business Analyst	4	Tableu, Oracle Netsuite, Web browser, Microsoft Office, Microsoft Teams	20 Mbps
		Máy tính bàn, laptop	
IT Operator	2	Zluri, Web browser	30 Mbps
		Máy tính bàn, laptop	
CEO	1	Web browser, Microsoft Office, Microsoft Teams.	20 Mbps

		Máy tính bàn, laptop	

2.2.2 Tại chi nhánh

Ở chi nhánh, văn phòng chỉ gồm 1 tầng, dành cho các nhân viên developer/tester, với tổng cộng 18 nhân viên làm việc. Kích thước của văn phòng này là 20m x 10m và chiều cao 4m và được chia thành 1 phòng lớn và 1 phòng nhỏ. Hiện tại, chưa có hệ thống mạng được thiết lập cho văn phòng này.

- **Sơ đồ văn phòng:**



- **Nhân sự và nhu cầu:**

Tên nhóm	Số lượng	Ứng dụng / Thiết bị	Băng thông
Developer / Tester	15 / 3	Visual Studio Code, Web browser, Git, Docker, Microsoft Office, Microsoft Teams	20 Mbps
		Máy tính bàn	

2.3 Yêu cầu chi tiết

2.3.1 Tại trụ sở chính

Tầng 1: Sảnh tiếp tân và không gian chung.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.

Tầng 2: Tầng làm việc cho phát triển sản phẩm. Phòng lớn là nơi làm việc cho Developer và Tester, hai phòng nhỏ khác dành cho Project Manager, Business Analyst và phòng họp.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.
- Mạng không dây khác là mạng nội bộ, trong đó chỉ cho phép Project Manager, HR, Business Analyst, Technical Manager, CEO và IT operator sử dụng các tài khoản xác thực để kết nối.

- Thiết lập hệ thống mạng có dây cho máy tính bàn có sẵn tại công ty kết nối với data center.

Tầng 3: Tiếp tục là tầng làm việc cho phát triển sản phẩm. Cũng giống như tầng 2, tầng này có phòng làm việc cho Developer và Tester, quy mô và vị trí nhân sự cũng tương đương.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.
- Mạng không dây khác là mạng nội bộ, trong đó chỉ cho phép Project Manager, HR, Business Analyst, Technical Manager, CEO và IT operator sử dụng các tài khoản xác thực để kết nối.
- Thiết lập hệ thống mạng có dây cho máy tính bàn có sẵn tại công ty kết nối với data center.

Tầng 4: Data center, nơi để đặt các thiết bị và hệ thống máy chủ. Tầng này được chọn để tránh ẩm mốc do độ ẩm cao và tránh nguy cơ ngập lụt do độ cao thấp. Ngoài ra, tầng này cũng được xem là dễ dàng quản lý an ninh. Đây là nơi làm việc của IT Operator.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.
- Mạng không dây khác là mạng nội bộ, trong đó chỉ cho phép IT operator sử dụng tài khoản xác thực riêng để kết nối.

Tầng 5: Tầng dành cho lãnh đạo và quản lý. Gồm hai phòng: HR Manager, Technical Manager và CEO. Các phòng này được sử dụng để làm việc và họp.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.
- Mạng không dây khác là mạng nội bộ, trong đó chỉ cho phép Project Manager, HR, Business Analyst, Technical Manager, CEO và IT operator sử dụng các tài khoản xác thực để kết nối

Data center: Hệ thống quản lý dữ liệu và hệ thống server ảo phục vụ cho việc deploy các ứng dụng trong giai đoạn test.

- Sử dụng 5 loại server phục vụ như cầu của khách hàng, bao gồm PDC, ADC, Web server, File server và Host server.
- PDC: Chịu trách nhiệm quản lý và duy trì các tài khoản người dùng, xác thực, và phân quyền truy cập trong một mạng.
  - Hệ điều hành: Đề xuất sử dụng hệ điều hành Windows Server 2019.
  - CPU: Đề xuất sử dụng CPU có hiệu năng cao, như Intel Xeon hoặc AMD EPYC, với ít nhất 8 lõi và tần số xung nhịp cao để xử lý các tác vụ cần thiết cho việc quản lý và xác thực tài khoản.
  - RAM: Đề xuất sử dụng ít nhất 16GB RAM để đảm bảo hiệu suất và xử lý đồng thời cho việc xác thực người dùng và quản lý tài khoản.
  - DISK: Sử dụng ổ cứng SSD hoặc ổ cứng SAS với dung lượng đủ để lưu trữ hệ điều hành và dữ liệu liên quan đến việc quản lý người dùng và tài khoản.
- ADC: Dự phòng, phân chia tải cho PDC.

- Hệ điều hành: Đề xuất sử dụng hệ điều hành Windows Server 2019.
- CPU: Sử dụng CPU tương tự như PDC, với ít nhất 8 lõi và tần số xung nhịp cao để xử lý các tác vụ quản lý tài khoản và sao lưu dữ liệu.
- RAM: Đề xuất sử dụng ít nhất 16GB RAM để đảm bảo hiệu suất và xử lý đồng thời cho việc sao lưu và đồng bộ dữ liệu từ PDC.
- DISK: Sử dụng ổ cứng SSD hoặc ổ cứng SAS với dung lượng đủ để lưu trữ hệ điều hành và dữ liệu liên quan đến việc sao lưu và đồng bộ dữ liệu.

- Web server: Trung tâm tác vụ về các dịch vụ Web của doanh nghiệp.
  - Hệ điều hành: Đề xuất sử dụng hệ điều hành Windows Server 2019.
  - CPU: Đề xuất sử dụng CPU có hiệu năng cao, như Intel Xeon hoặc AMD EPYC, với ít nhất 8 lõi và tần số xung nhịp cao để xử lý các yêu cầu HTTP và xử lý ứng dụng web.
  - RAM: Đề xuất sử dụng ít nhất 16GB RAM để đảm bảo hiệu suất và xử lý đồng thời cho việc chạy ứng dụng web và phục vụ yêu cầu từ khách hàng.
  - DISK: Sử dụng ổ cứng SSD hoặc ổ cứng SAS với dung lượng đủ để lưu trữ hệ điều hành, ứng dụng web và dữ liệu liên quan.
- File server: Nơi lưu trữ dữ liệu của doanh nghiệp.
  - Hệ điều hành: Đề xuất sử dụng hệ điều hành Windows Server 2019.
  - CPU: Sử dụng CPU tương tự như Web server, với ít nhất 8 lõi và tần số xung nhịp cao để xử lý các yêu cầu truy cập và quản lý tệp tin.
  - RAM: Đề xuất sử dụng ít nhất 16GB RAM để đảm bảo hiệu suất và xử lý đồng thời cho việc chia sẻ tệp tin và quản lý quyền truy cập.
  - DISK: Đề xuất sử dụng ổ cứng SAS hoặc ổ cứng RAID với dung lượng đủ để lưu trữ tệp tin, và cung cấp tốc độ truy cập nhanh và khả năng chịu lỗi.
- Host server: Hệ thống ảo hóa, phục vụ việc deploy ứng dụng trong giai đoạn test.
  - Đề xuất sử dụng hypervisor VMware vSphere.
  - CPU: Đề xuất sử dụng CPU có hiệu năng cao, với 16 lõi (core) và tần số xung nhịp cao để xử lý các tác vụ ảo hóa.
  - RAM: Đề xuất sử dụng RAM đủ lớn để chia sẻ cho các máy ảo và đảm bảo hiệu suất cao.
  - DISK: Sử dụng ổ cứng tốc độ cao và có dung lượng đủ để lưu trữ hệ điều hành, hypervisor và các máy ảo.

Cloud: Sử dụng dịch vụ Cloud để deploy các ứng dụng trong giai đoạn staging để khách hàng sử dụng thử trước khi đưa ra thực tế.

- Amazon Web Services (AWS):
  - Sử dụng Elastic Compute Cloud (EC2): Triển khai máy ảo EC2 để chạy các phiên bản staging của ứng dụng trên các máy ảo đám mây.

- Sử dụng Elastic Beanstalk: Elastic Beanstalk cung cấp một cách dễ dàng để triển khai ứng dụng web trên AWS. Tạo một môi trường staging trên Elastic Beanstalk để chạy và kiểm tra ứng dụng trước khi triển khai vào môi trường sản xuất.
- CPU: Hai lõi CPU có thể đáp ứng yêu cầu xử lý của ứng dụng staging.
- RAM: 4 GB RAM cho một ứng dụng vừa trong giai đoạn staging.
- Dung lượng ổ cứng: 50 GB dung lượng ổ cứng có thể đủ để lưu trữ ứng dụng và dữ liệu staging.
- Network Bandwidth: 100 Mbps có thể đáp ứng yêu cầu truy cập và giao tiếp của ứng dụng staging.

- Cấu hình dịch vụ Cloud có thể thay đổi để thích hợp yêu cầu của dự án trong giai đoạn staging.
- Sử dụng AWS S3 để phục vụ việc Backup server.

Wireless:

- Hệ thống mạng wifi Public sử dụng đường kết nối Internet riêng, độc lập với mạng nội bộ của công ty. Sử dụng cho tất cả các đối tượng có thông tin xác thực (mật khẩu).
- Hệ thống mạng wifi nội bộ sẽ được chia làm 2 vlan khác nhau, một mạng dùng riêng cho tầng 4 (nơi làm việc của IT operator) và mạng còn lại được sử cho tầng 2, tầng 3 và tầng 5 (chỉ lắp đặt AP này tại các phòng riêng của Project Manager, Business Analyst, HR Manager, Technical Manager và CEO). Trong đó, chỉ duy nhất mạng của vlan IT Operator được quyền root vào mạng của Data center.

Firewall và IPS: Đề xuất sử dụng thiết bị firewall phần cứng của FORTINET cho phát triển, triển khai các tính năng bảo mật và truy vết lưu lượng trong mạng.

2.3.2 Tại chi nhánh

Văn phòng làm việc cho phát triển sản phẩm. Phòng lớn là nơi làm việc cho Developer và Tester, phòng nhỏ dành cho các cuộc họp.

- Mạng không dây có thể được sử dụng để kết nối các thiết bị với Internet bằng cách yêu cầu thông tin xác thực (mật khẩu) đối với tất cả các đối tượng.
- Thiết lập hệ thống mạng có dây cho máy tính bàn có sẵn tại công ty kết nối với data center.
- Thiết lập hệ thống VPN tunnel cho phép truy cập server nội bộ và deploy ứng dụng lên hệ thống tại Data Center ở trụ sở chính.

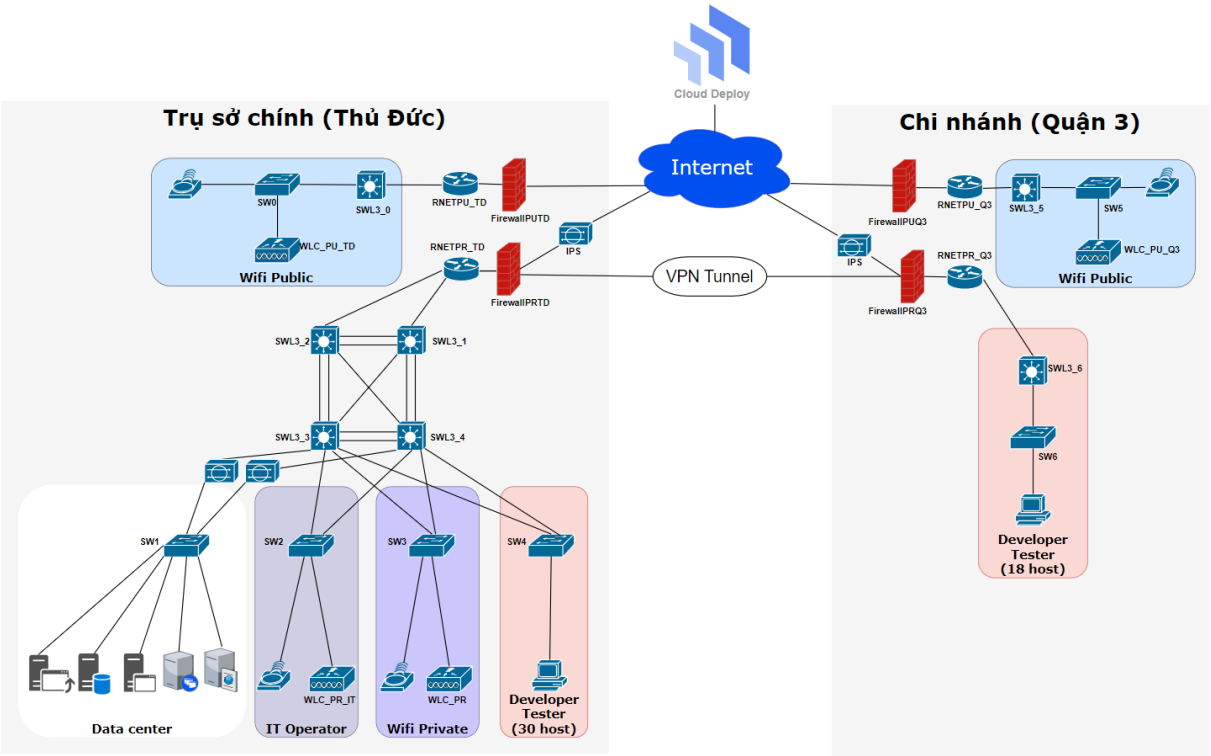
Wireless:

- Hệ thống mạng wifi Public sử dụng đường kết nối Internet riêng, độc lập với mạng nội bộ của công ty. Sử dụng cho tất cả các đối tượng có thông tin xác thực (mật khẩu).

3 THIẾT KẾ HỆ THỐNG MẠNG

3.1 Thiết kế mô hình mạng logic

3.1.1 Sơ đồ logic



Hình 1. Mô hình mạng logic

3.1.2 Giải thích sơ đồ

- **Tại trụ sở chính**, quy mô mạng được chia làm 5 phần:
  - Phần Wifi Public được kết nối độc lập với mạng nội bộ và cung cấp dịch vụ mạng cho khách hàng từ bên ngoài. Sử dụng Wireless Controller và Access Point (AP) để cung cấp kết nối Internet cho môi trường Wifi công cộng.
  - Phần Data center sử dụng mạng nội bộ của công ty và chứa các máy chủ quan trọng như PDC (Primary Domain Controller), ADC (Additional Domain Controller), File server và Web server. Các máy chủ này hỗ trợ các chức năng cốt lõi của công ty và được sử dụng để lưu trữ và chia sẻ dữ liệu, quản lý người dùng và cung cấp dịch vụ web.
  - Sử dụng IPS để theo dõi, truy vết lưu lượng mạng. Đặt IPS ở đường kết nối giữa Data center và SWL3 và tại đường kết nối ra Internet.
  - Phần Developer/Tester sử dụng mạng nội bộ của công ty và cung cấp dịch vụ mạng cho nhân viên công ty và nhóm Developer/Tester. Bao gồm mạng được cài đặc static trên máy tính PC của công ty.
  - Phần Wifi Private sử dụng mạng nội bộ và cung cấp dịch vụ cho HR Manager, Technical Manager, CEO và IT operator.
  - Phần IT Operator (không dây) sử dụng mạng nội bộ, chỉ cung cấp riêng cho IT operator.

- **Tại chi nhánh**, quy mô chỉ có 2 phần:
  - Phần Wifi Public được kết nối độc lập với mạng nội bộ và cung cấp dịch vụ mạng cho khách hàng từ bên ngoài. Sử dụng Wireless Controller và Access Point (AP) để cung cấp kết nối Internet cho môi trường Wifi công cộng.
  - Phần Developer/Tester sử dụng mạng nội bộ của công ty và cung cấp dịch vụ mạng cho nhân viên công ty và nhóm Developer/Tester. Bao gồm mạng được cài đặc static trên máy tính PC của công ty.
  - Sử dụng IPS để theo dõi, truy vết lưu lượng mạng. Đặt IPS tại đường kết nối ra Internet.
- **Kết nối trong mô hình**, có các phương tiện kết nối và thành phần mạng chính như sau:
  - Trong mạng nội bộ, các VLAN được phân chia thành các nhóm Developer/Tester, Data center, Wifi Private và IT Operator. Mặc dù Wifi Private và IT Operator có thể sử dụng cùng một mạng với Data center để đáp ứng yêu cầu của khách hàng, tuy nhiên, việc tách riêng một mạng cho các mạng này giúp dễ dàng quản lý, kiểm soát quyền truy cập và còn giúp khả năng mở rộng mạng một cách hiệu quả và dễ dàng hơn.
  - Kết nối ra ngoài Internet sử dụng Router kết hợp với một tường lửa (**Firewall**) để kết nối mạng nội bộ với Internet. Router được sử dụng để định tuyến các gói tin giữa mạng nội bộ và Internet, trong khi tường lửa bảo vệ mạng khỏi các mối đe dọa từ Internet.
  - Mạng nội bộ sử dụng các Switch Layer 3 (SWL3) để định tuyến lưu lượng mạng trong nội bộ, có sử dụng giao thức HSRP để tạo các đường đi dự phòng trong trường hợp xấu và còn giúp cân bằng tải trong hệ thống. Switch được sử dụng để chuyển mạch dữ liệu giữa các thiết bị trong mạng nội bộ.
  - Kết nối VPN giữa trụ sở chính và chi nhánh, thiết lập một VPN tunnel (đường hầm ảo riêng tư) giữa trụ sở chính và chi nhánh. VPN tunnel cho phép truyền dữ liệu an toàn và bảo mật giữa hai địa điểm, tạo thành một mạng nội bộ duy nhất.
  - Truy cập vào Cloud bên ngoài Internet, mạng nội bộ của trụ sở được cấu hình để cho phép truy cập vào Cloud từ bên ngoài Internet. Điều này cho phép nhân viên và hệ thống trong mạng nội bộ kết nối và sử dụng các dịch vụ và tài nguyên có sẵn trên Cloud.

3.1.3 Giao thức sử dụng và cấu hình cần có

Giao thức	Cấu hình cần có
IP	Thiết lập địa chỉ IP cho mỗi thiết bị trong mạng, đảm bảo chúng nằm trong cùng một phạm vi mạng (bao gồm IP cho các interface, mạng cho các VLAN). Cấu hình các thông số như subnet mask, gateway và DNS cho máy tính của công ty (ngoại trừ wifi thì mạng dây đều phải được cấu hình static).
DHCP	Cài đặt DHCP trong mạng để tự động cấp phát địa chỉ IP, subnetmask, gateway và DNS cho các thiết bị kết nối wifi (ADDS

	server sẽ quản lý DHCP cho wifi private, SWL3 sẽ quản lý DHCP cho wifi public).
DNS	Thiết lập hệ thống máy chủ DNS trên máy chủ ADDC server để chuyển đổi tên miền thành địa chỉ IP và ngược lại Cấu hình các bản ghi DNS cho các tên miền và địa chỉ IP tương ứng
VLAN	Cấu hình switch mạng để hỗ trợ VLAN và tạo các VLAN tương ứng với phân đoạn cho các nhóm người dùng được chỉ ra trên sơ đồ. Gán các cổng switch vào các VLAN tương ứng
VPN	Cài đặt một máy chủ VPN để tạo ra kết nối an toàn và mã hóa giữa trụ sợ và chi nhánh, giúp Developer/Tester ở chi nhánh có thể truy cập vào mạng nội bộ của trụ sở bằng VPN Site-to-Site (tunnel). Cấu hình các tham số VPN như phương thức mã hóa, chứng chỉ và quy tắc truy cập.
OSPF	Cấu hình OSPF trên các SWL3, router trong mạng, thiết lập các kết nối định tuyến.
SNMP	Cấu hình các thiết bị mạng để hỗ trợ SNMP và cung cấp thông tin quản lý. Thiết lập các thông số SNMP như cấu hình cộng đồng, phiên bản SNMP và quyền truy cập.
SSH	Cấu hình các thiết bị mạng để hỗ trợ SSH và thiết lập các thông tin xác thực trên mạng của VLAN Data center. Đảm bảo rằng các tài khoản và mật khẩu SSH đã được cấu hình và quản lý một cách an toàn.
HSRP	Cấu hình HSRP trên các SWL3 kết nối với nhau trong mạng để tạo ra một kịch bản chuyển đổi nguồn tài nguyên mạng chủ động (active/passive). Thiết lập các thông số HSRP như IP ảo, độ ưu tiên và thời gian chuyển đổi.
Giao thức không dây	Cấu hình các thiết bị mạng để hỗ trợ mạng không dây và thiết lập các thông tin xác thực WPA2-Enterprise trên mạng không dây của wifi private và xác thực WPA2 cho wifi public. Đảm bảo rằng các tài khoản và mật khẩu truy cập vào mạng không dây đã được cấu hình và quản lý trong ADDS server. Cấu hình Access Point (AP): Cấu hình các Access Point (AP) để phát sóng và quản lý mạng không dây. Điều này bao gồm thiết lập tên mạng (SSID), chế độ bảo mật, kênh phát sóng và các cấu hình mạng không dây khác.

NAT	Cấu hình NAT trên router để thực hiện chuyển đổi địa chỉ mạng (Network Address Translation) trong mạng nội bộ có thể đi ra Internet. Đảm bảo rằng các thiết lập NAT đã được cấu hình và quản lý một cách an toàn.

Cấu hình khác:

- Sử dụng kỹ thuật port-group để quản lý đường kết nối giữa các SWL3.
- Sử dụng kỹ thuật port-security để chặn các hành vi cố trình kết nối với phần cứng của hệ thống mà không được cho phép.
- Sử dụng ACL để ngăn quyền root hay truy cập vào cấu hình hệ thống (ngoại trừ IP của các IT operator).

3.2 Mô hình địa chỉ mạng

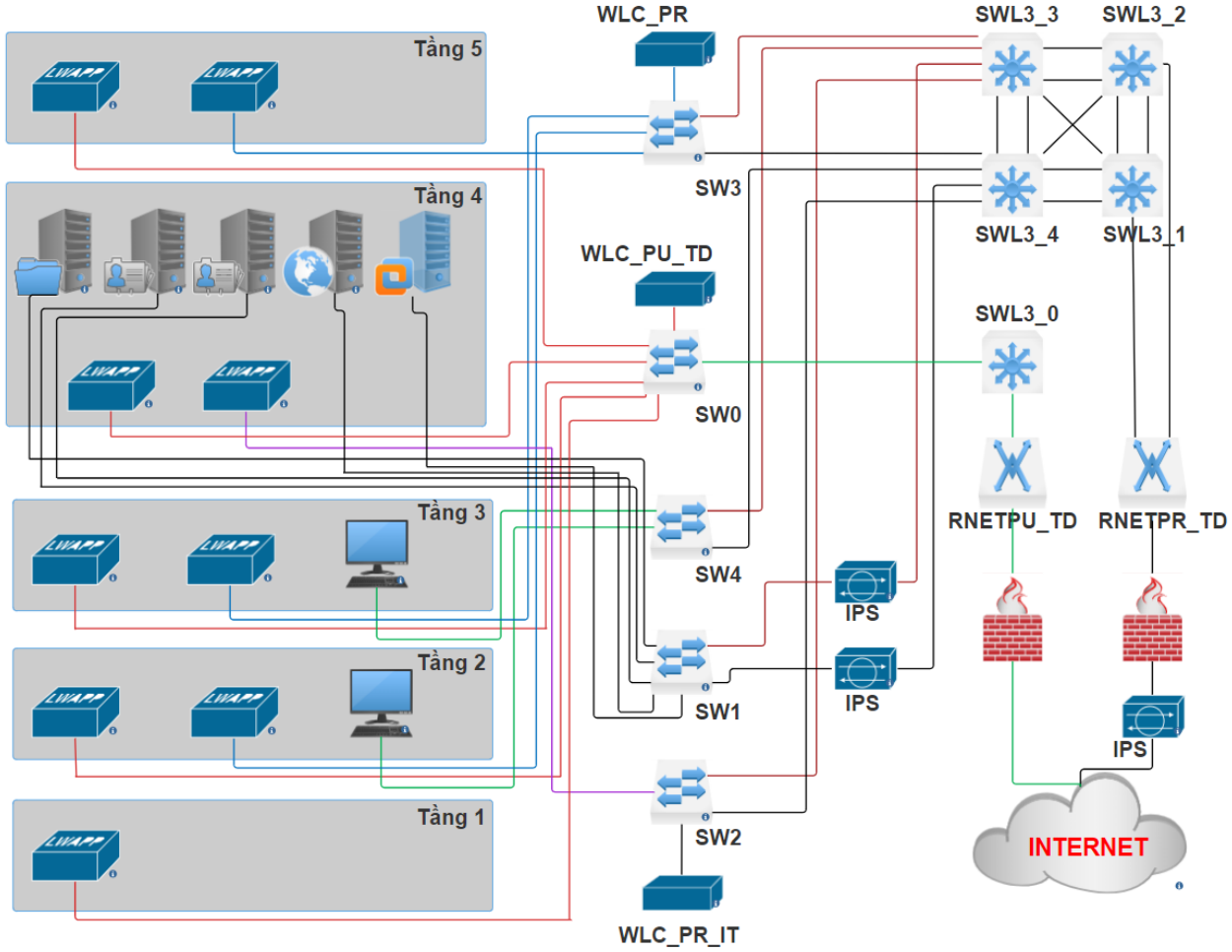
Vị trí	Đối tượng	VLAN	Mạng	Hosts
Trụ sở chính	Developer/Tester	DT	192.168.0.0/26	62
	Wifi Private	WPR	192.168.0.64/27	30
	Data center	DTC	192.168.0.96/29	6
	Wifi IT Operator	WPO	192.168.0.104/29	6
	Wifi Public	WP	172.20.0.0/24	254
Chi nhánh	Developer/Tester	DTQ3	192.168.1.0/27	30
	Wifi Public	WPQ3	172.20.1.0/24	254

3.3 Thiết kế sơ đồ vật lý của toàn bộ hệ thống mạng

3.3.1 Các thiết bị dùng trong hệ thống

3.3.1.1 Tại trụ sở chính

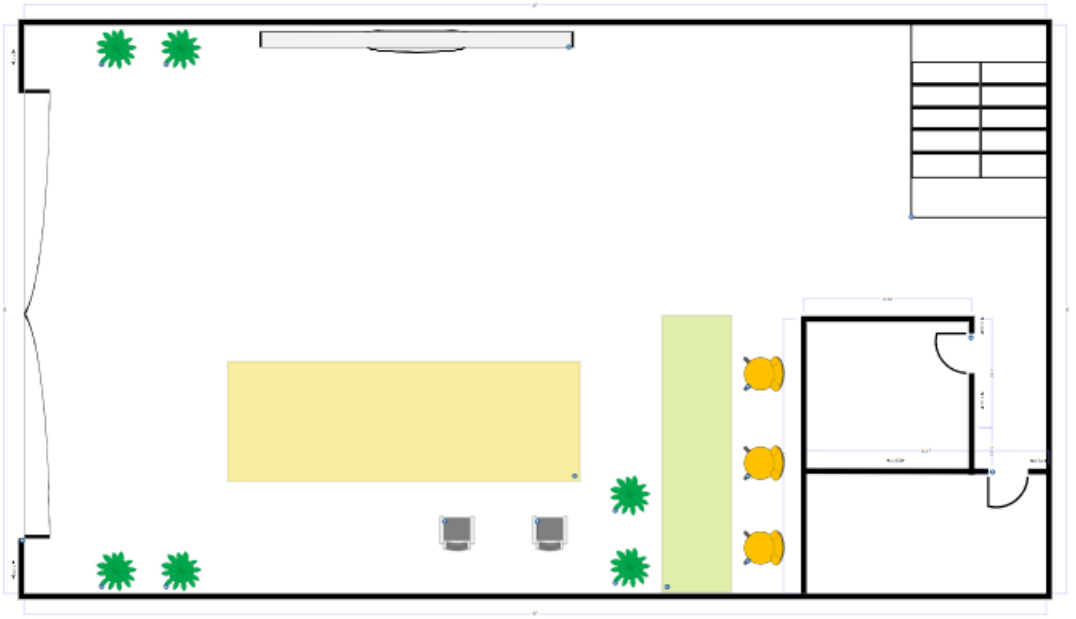
- **Mô hình vật lý:**

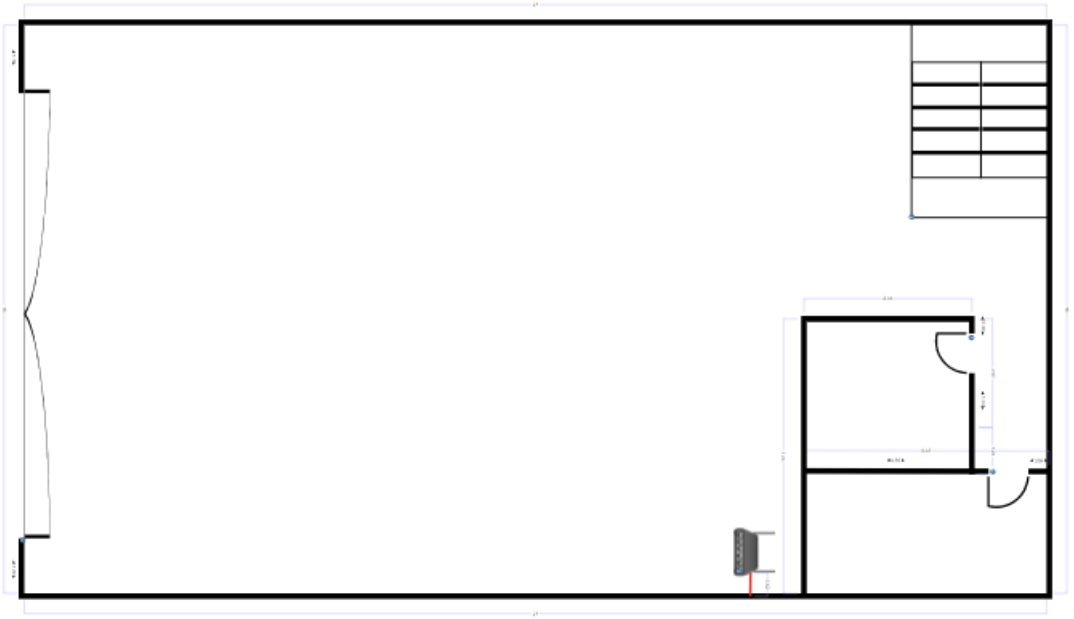


- **Chi tiết vị trí lắp đặt:**

Tầng 1:

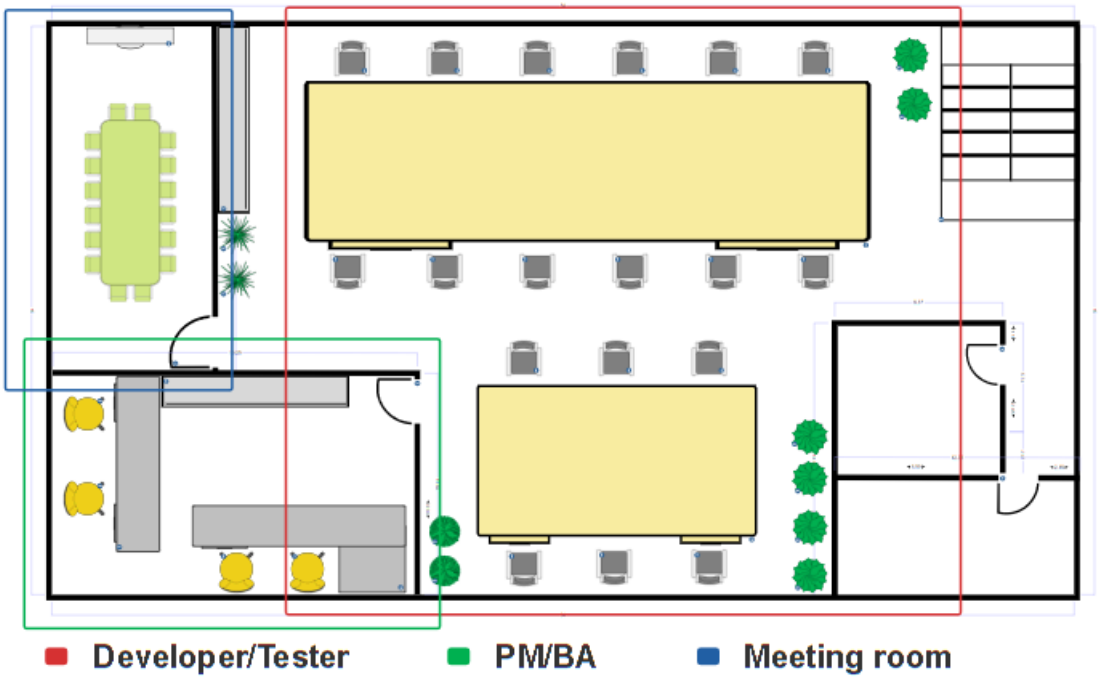
- Sử dụng một LAP, một cable RJ45 dài 20m (Nối tới Switch trên tầng Data center)
- LAP được đặt trên trần nhà để giảm bớt độ cản của vật thể xung quanh, tối ưu vùng tín hiệu. Vị trí cụ thể như sơ đồ bên dưới.

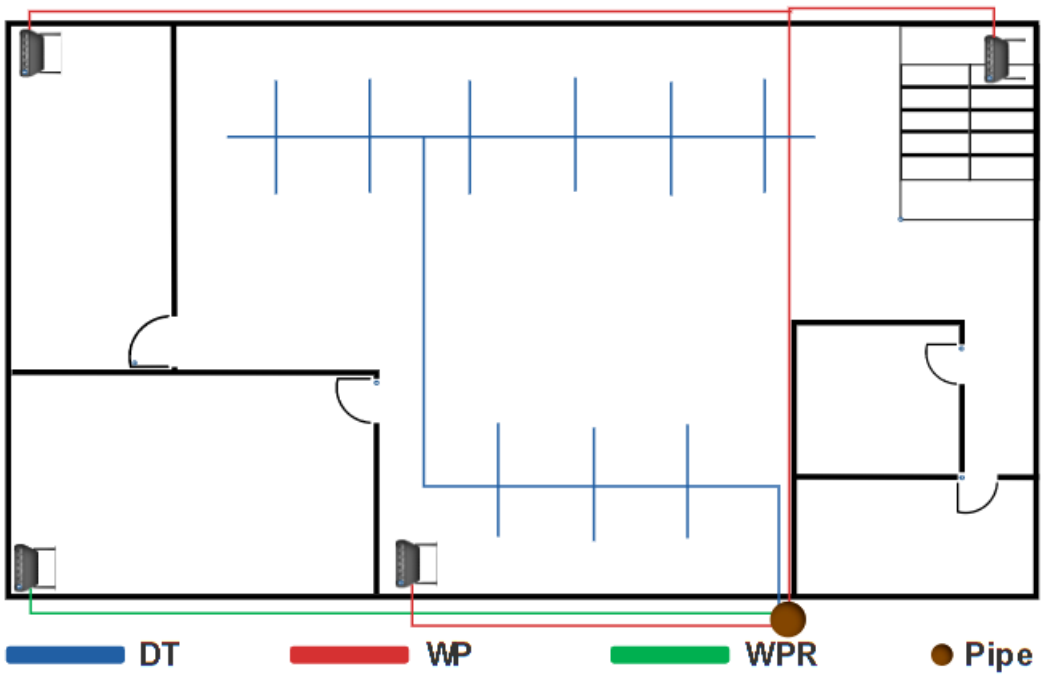




Tầng 2 và tầng 3:

- AP được đặt trên trần nhà để giảm bớt độ cản của vật thể xung quanh, tối ưu vùng tín hiệu. Tuy nhiên tại cầu thang thì chỉ có tầng 2 lắp đặt AP. Vị trí cụ thể như sơ đồ bên dưới.
- Tầng 2: Sử dụng 4 LAP bao gồm 3 LAP cho WP và 1 LAP cho WPR. Sử dụng 430m cable RJ45 (Sử dụng kết nối đơn lẻ giữa PC và SW tuy tốn tài nguyên hơn việc đặt thêm một SW khác nhưng cách này sẽ tối ưu được băng thông sử dụng cho từng PC, giảm thiểu sự chia sẻ).
- Tầng 3: Sử dụng 3 LAP bao gồm 2 LAP cho WP và 1 LAP cho WPR. Sử dụng 370m cable RJ45 (Sử dụng kết nối đơn lẻ giữa PC và SW tuy tốn tài nguyên hơn việc đặt thêm một SW khác nhưng cách này sẽ tối ưu được băng thông sử dụng cho từng PC, giảm thiểu sự chia sẻ).
- Sử dụng tổng là 32 bộ PC.

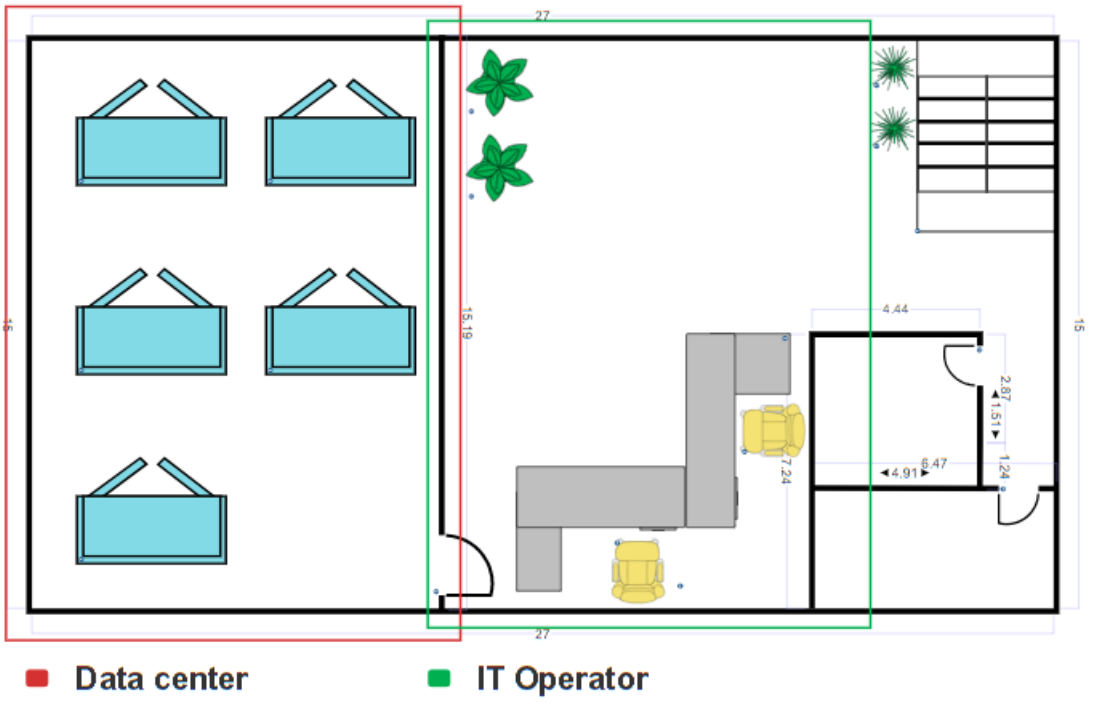


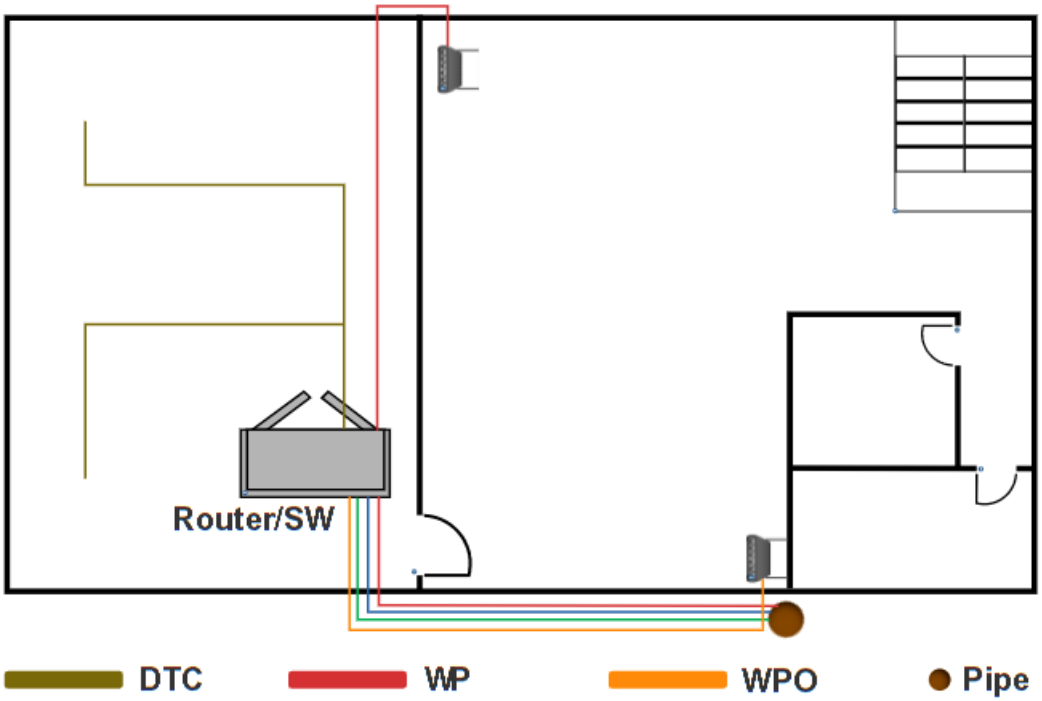


Tầng 4:

- LAP được đặt trên trần nhà để giảm bớt độ cản của vật thể xung quanh, tối ưu vùng tín hiệu. Vị trí cụ thể như sơ đồ bên dưới.
- Các thiết bị như Router, SW, SW3 được đặt tại cùng vị trí ở tầng này.
- Ở **Pipe** bao gồm các kết nối đã được chú thích thì còn bao gồm kết nối lục (WPR), xanh dương (DT).
- Sử dụng 2 LAP bao gồm 1 LAP cho WP và 1 LAP cho WPO. Sử dụng 35m cable RJ45.

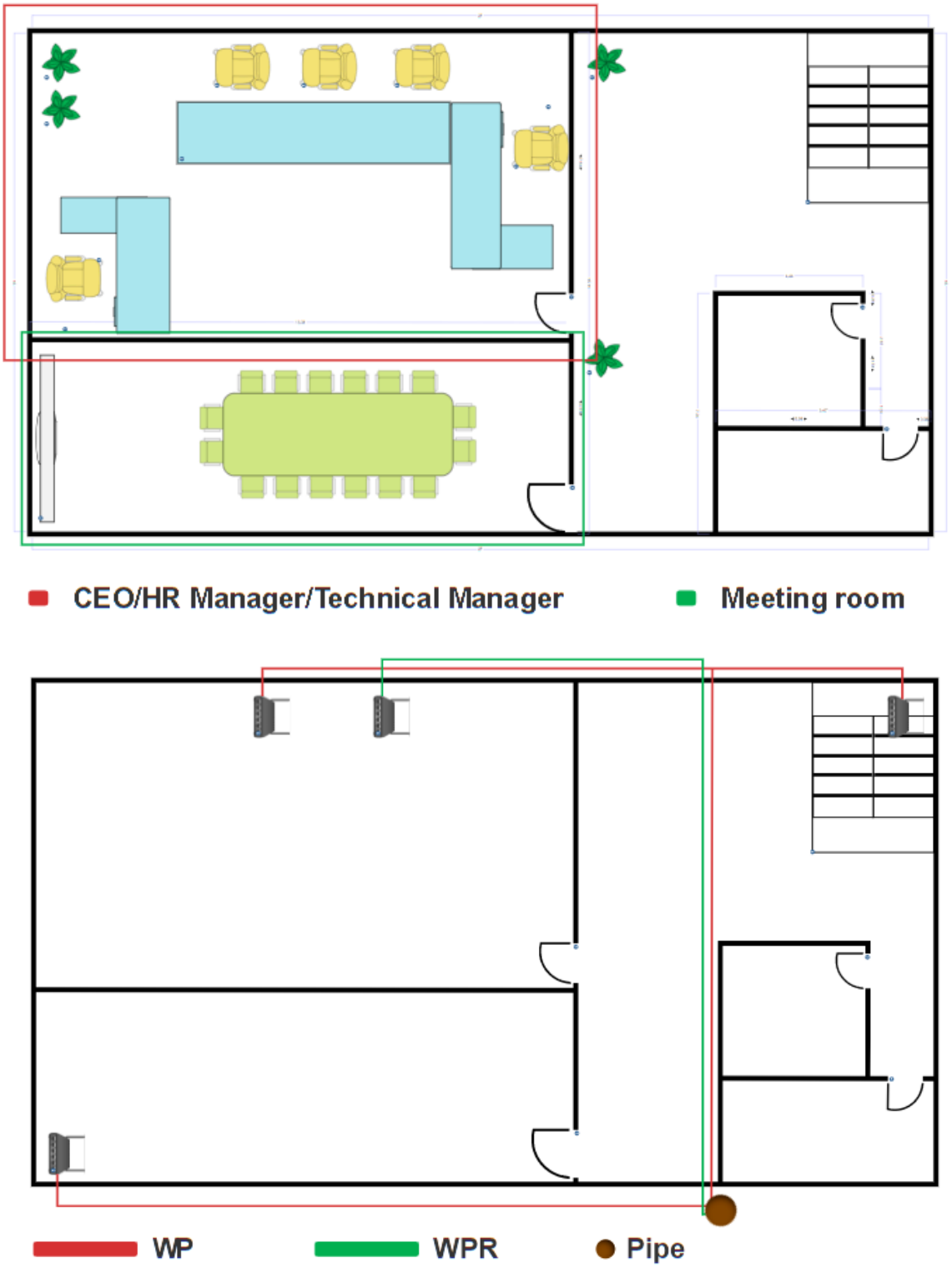
- Sử dụng 5 Server (đã mô tả trong phần phân tích), 5 Switch, 4 SwitchLayer3, 3 Wireless LAN Controller, 2 Router, 2 IPS và 2 Firewall.





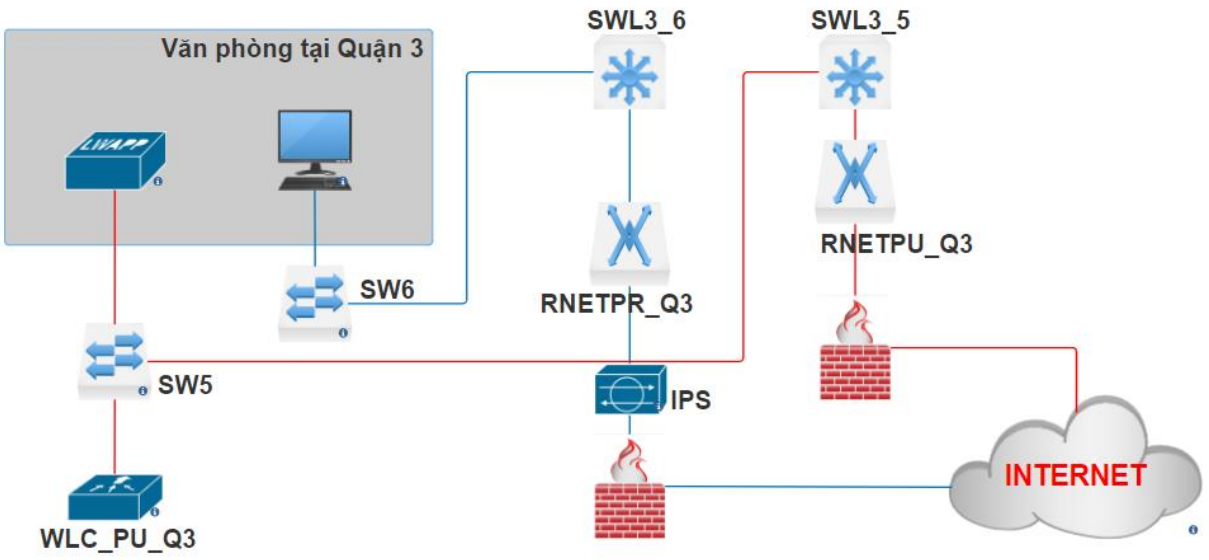
Tầng 5:

- LAP được đặt trên trần nhà để giảm bớt độ cản của vật thể xung quanh, tối ưu vùng tín hiệu. Vị trí cụ thể như sơ đồ bên dưới.
- Sử dụng 4 LAP bao gồm 3 LAP cho WP và 1 LAP cho WPR. Sử dụng 100m cable RJ45.

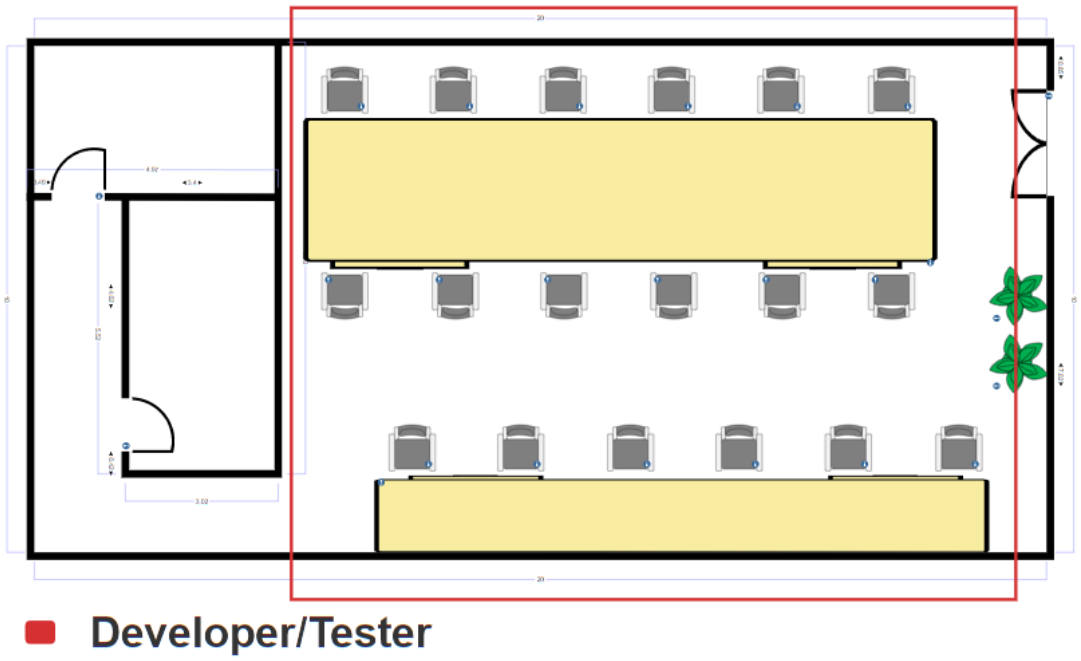


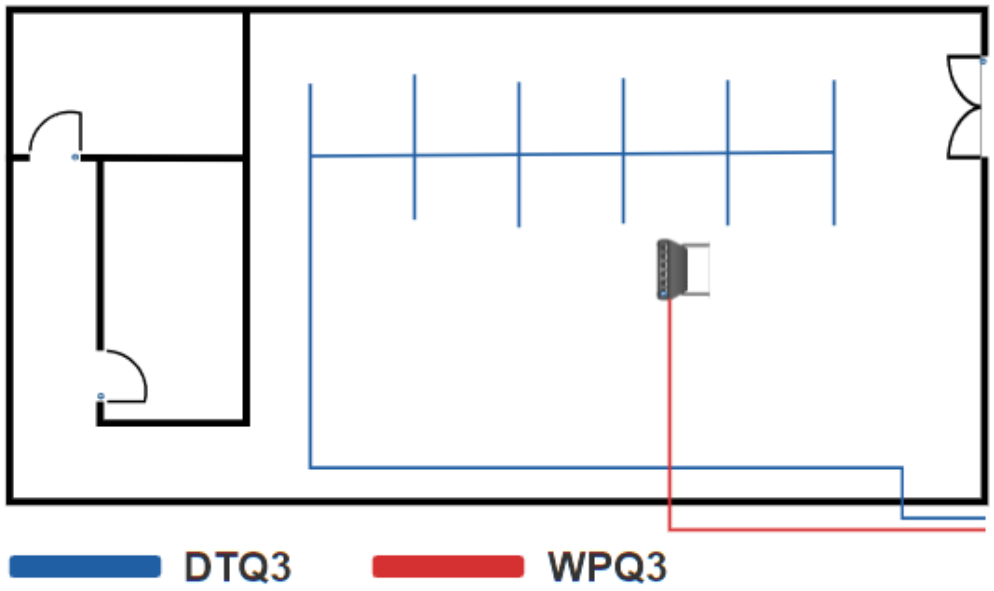
3.3.1.2 Tại chi nhánh

- **Mô hình vật lý:**



- **Chi tiết vị trí lắp đặt:**
  - LAP được đặt trên trần nhà để giảm bớt độ cản của vật thể xung quanh, tối ưu vùng tín hiệu. Vị trí cụ thể như sơ đồ bên dưới.
  - Sử dụng một LAP cho PUQ3, một cable RJ45 dài khoảng 200m.
  - Sử dụng 18 bộ PC.





3.3.2 Các dịch vụ cần thuê

Tại trụ sở chính:

- Dịch vụ cung cấp địa chỉ IP public: Dịch vụ này cung cấp một địa chỉ IP public duy nhất để kết nối mạng doanh nghiệp với Internet. Địa chỉ IP public cho phép các thiết bị trong mạng được truy cập từ bên ngoài và làm cho các dịch vụ của doanh nghiệp có thể tiếp cận được từ mạng công cộng.
- Dịch vụ tên miền: Dịch vụ này cung cấp tên miền duy nhất cho mạng doanh nghiệp. Tên miền cho phép xác định và truy cập các tài nguyên của mạng doanh nghiệp.
- Dịch vụ đường truyền Internet: Dịch vụ này cung cấp một kết nối Internet để kết nối mạng doanh nghiệp với Internet, trong đó đường truyền Internet với mạng nội bộ sử dụng 1200Mbps và đường truyền Internet của Wifi public là khoảng gần 1000Mbps.
- Dịch vụ Cloud (AWS): Dịch vụ Cloud như AWS (Amazon Web Services) cung cấp một loạt các tài nguyên và dịch vụ điện toán đám mây để lưu trữ dữ liệu, chạy ứng dụng và triển khai các dịch vụ trên nền tảng điện toán đám mây.
- Bản quyền phần mềm.

Tại chi nhánh:

- Dịch vụ đường truyền Internet: Dịch vụ này cung cấp một kết nối Internet để kết nối mạng doanh nghiệp với Internet.

4 CHI PHÍ CHO HỆ THỐNG

4.1 Chi phí cho thiết bị

- Chi phí được tính cho đến 11/2023 dựa trên nền tản **Amazon** và **eBay.**
- Trong mục đích tối ưu hóa chi phí, chúng ta đã sử dụng hai loại Router khác nhau để phục vụ các mục đích riêng biệt. Đối với RNETPU_TD, RNETPR_Q3 nhóm em đã chọn sử dụng Mikrotik RB3011UiAS-RM. Với khả năng tải lên đến 1Gbps, nó có thể đáp ứng nhu cầu kết nối của hơn 200 thiết bị một cách hiệu quả. Trong khi đó, để phục vụ các dịch vụ của doanh nghiệp ra bên ngoài, Router Mikrotik

CCR1009 cho RNETPR_TD là sự lựa chọn thích hợp. Với khả năng tải có băng lên vài Gbps, nó đáp ứng được yêu cầu cao về tốc độ và băng thông. Việc sử dụng hai loại Router khác nhau giúp tối ưu hóa chi phí mà không ảnh hưởng đến hiệu suất và khả năng phục vụ của hệ thống.

- Sử dụng hai loại Switch với số lượng cổng khác nhau. Loại đầu tiên có 10 cổng được sử dụng để kết nối với Data center và wifi công cộng. Loại thứ hai có 48 cổng và dùng cho các mạng còn lại trong hệ thống.
- Sử dụng Cloudkey Gen 2 Plus cho WLC. Mặc dù không phải là một WLC truyền thống, Cloudkey Gen 2 Plus cung cấp tính năng của một WLC và có nhiều ưu điểm. Nó có khả năng quản lý mạng không dây một cách dễ dàng và hiệu suất tốt. Đồng thời, giá thành của Cloudkey Gen 2 Plus cũng phù hợp ngân sách.
- Tại Data Center, các server được lựa chọn theo cấu hình tối thiểu đã đưa ra ở *mục 2.3.1*.
- Bảng chi phí không bao gồm PC. Sự lựa chọn PC là sự lựa chọn của doanh nghiệp.
- Các thiết bị khác đều được sử dụng bởi các hãng nổi tiếng trong lĩnh vực.

Vị trí	Thiết bị	Số lượng	Đơn giá ($)	Thành tiền ($)
Trụ sở chính	**Router** (RNETPU_TD) *Mikrotik RB3011UiAS-RM*	1	164,75	164,75
	Router (RNETPR_TD) *Router Mikrotik CCR1009*	1	984,99	984,99
	Switch (SW0, SW1) *TP-Link TL-SG108PE*	4	65,99	263,96
	Switch (SW2, SW3, SW4) *Switch TP-Link TL-SG1048 48Port*	1	209.99	209,99
	MultiSwitch *TRENDnet 10-Port*	5	229,99	1149,95
	Cable RJ45 *AMP cat5e UTP*	955m	0,33/1m	315,15
	Firewall *FortiGate 40F*	2	194,83	389,66
	IPS *IPS-4255-K9*	2	82,75	165,5
	LAP *Grandstream NETGEAR WiFi 6 Access Point (WAX214v2)*	14	89,99	1259,86

	WLC *CloudKey Gen 2 Plus*	3	189,99	569,97
	Server (service) *Dell PowerEdge R450*	4	3825,67	15302,68
	Host server *IBM 8205-E6B P740*	1	4495	4495
	PC	x	x	x
Tổng chi phí cho trụ sở:				**24.431,5**
Chi nhánh	**Router** (RNETPU_Q3, RNETPR_Q3) *Mikrotik RB3011UiAS-RM*	2	164,75	329.5
	Switch (SW5) *TP-Link TL-SG108PE*	1	65,99	65,99
	Switch (SW6) *Switch TP-Link TL-SG1048*	1	209.99	209,99
	MultiSwitch *TRENDnet 10-Port*	2	229,99	459,98
	Cable RJ45 *AMP cat5e UTP*	200m	0,33/1m	66
	Firewall *FortiGate 40F*	2	194,83	389,66
	IPS *IPS-4255-K9*	2	82,75	165,5
	LAP *Grandstream NETGEAR WiFi 6 Access Point (WAX214v2)*	1	89,99	89,99
	WLC *CloudKey Gen 2 Plus*	1	189,99	189,99
	PC	x	x	x
Tổng chi phí cho chi nhánh:				**1.966,6**

Tổng chi phí chi trả:	**26.398,1**
Tổng chi phí sau khi áp thuế VAT (10%):	**29.037,91**

Tổng chi phí chưa bao gồm chi phí phát sinh và bản quyền phần mềm.

Chi phí cho chi nhánh chưa bao gồm thuế 47.867.044 vnd.

Chi phí cho trụ sở chưa bao gồm thuế 594.662.710 vnd.

Chi phí cho chi nhánh và trụ sở sau thuế tương đương 706.782.729 vnd.

4.2 Chi phí cho dịch vụ

Chi phí được tính đến tháng 11/2023 dựa trên nhà cung cấp **FPT Telecom** (đường truyền Internet), **Inet** (tên miền), **AWS** (Cloud).

Các dịch vụ này đều đã được áp thuế VAT (10%).

Tại trụ sở chính:

- Sử dụng 3 đường truyền Super 400 của nhà mạng FPT để cung cấp tốc độ tải 1200Mbps cho mạng nội bộ. Đồng thời, sử dụng 3 đường truyền Super 300 để cung cấp tốc độ tải 900Mbps cho wifi public, và được hỗ trợ thiết bị load balance.
- Địa chỉ tĩnh được cung cấp tặng kèm với gói đường truyền mạng,
- Dịch vụ Cloud sử dụng với AWS EC2, với mục đích sử dụng các dịch vụ Cloud để deploy các ứng dụng trong giai đoạn staging để khách hàng sử dụng thử trước khi đưa ra thực tế thì điều này rất tốn kém khi thuê liên tục. Đồng thời quy mô các ứng dụng của khách hàng là khác nhau nên chi phí sử dụng Cloud cho mục đích này không được thống kê.
- Sử dụng dịch vụ AWS S3 để làm nới lưu trữ, backup server khi có sự cố.

Tại chi nhánh:

- Với quy mô ít hơn nên sử dụng 2 Super 300 cho wifi public và 2 Super 300 cho mạng nội bộ.

Vị trí	Dịch vụ	SL	Đơn giá (vnd)	Chi phí lắp đặt	Thành tiền (vnd)
Trụ sở chính	**Đường truyền Internet** *Super 400*	3	8.125.000/tháng	6.600.000/tháng	44.175.000/tháng
	Đường truyền Internet *Super 300*	3	1.410.000/tháng	3.300.000/tháng	14.130.000/tháng
	Tên miền	1	460.000/năm	x	460.000/năm

	.vn				
	Cloud *AWS EC2*	x	x	x	x
	Cloud *AWS S3 tiêu chuẩn*	1024GB	243/GB/tháng	x	248.832/tháng
	Hệ điều hành *Window Server 2019*	5	148.563	x	742.815
Tổng chi phí cho trụ sở (Không bao gồm Window Server):					**59.013.000/tháng**
Chi nhánh	**Đường truyền Internet** *Super 300*	4	1.410.000/tháng	3.300.000/tháng	18.840.000/tháng
Tổng chi phí:					**73.143.000/tháng**

Tổng chi phí chưa bao gồm bản quyền hệ điều hành và chưa bao gồm dịch vụ lắp đặt toàn bộ hệ thống.

Chi phí chi trả dịch vụ cho trụ sở 59.013.000vnd/tháng.

Chi phí chi trả dịch vụ cho chi nhánh 18.840.000/tháng.

Chi phí sau thuế tương đương 77.853.000vnd/tháng.

Tên phiên bản	Giá giờ theo nhu cầu	vCPU	Bộ nhớ	Lưu trữ	Hiệu năng mạng
g4dn.12xlarge	5,474 USD	48	192 GiB	SSD 900 GB NVMe	50 Gigabit
g4dn.16xlarge	6,089 USD	64	256 GiB	SSD 900 GB NVMe	50 Gigabit
g4dn.8xlarge	3,045 USD	32	128 GiB	SSD 900 GB NVMe	50 Gigabit
g4dn.4xlarge	1,685 USD	16	64 GiB	SSD 225 GB NVMe	Lên đến 25 Gigabit
g4dn.2xlarge	1,052 USD	8	32 GiB	SSD 225 GB NVMe	Lên đến 25 Gigabit
g4dn.xlarge	0,736 USD	4	16 GiB	SSD 125 GB NVMe	Lên đến 25 Gigabit
m5zn.2xlarge	0,826 USD	8	32 GiB	Chỉ EBS	Lên đến 25 Gigabit
t3a.xlarge	0,1888 USD	4	16 GiB	Chỉ EBS	Lên đến 5 Gigabit
r4.large	0,16 USD	2	15,25 GiB	Chỉ EBS	Lên đến 10 Gigabit
r4.8xlarge	2,56 USD	32	244 GiB	Chỉ EBS	10 Gigabit
t3a.2xlarge	0,3776 USD	8	32 GiB	Chỉ EBS	Lên đến 5 Gigabit
t4g.medium	0,0424 USD	2	4 GiB	Chỉ EBS	Lên đến 5 Gigabit
m6in.32xlarge	10,93248 USD	128	512 GiB	Chỉ EBS	200000 Megabit
m5.metal	5,76 USD	96	384 GiB	Chỉ EBS	25 Gigabit
r5b.2xlarge	0,712 USD	8	64 GiB	Chỉ EBS	Lên đến 10 Gigabit
r6g.2xlarge	0,4864 USD	8	64 GiB	Chỉ EBS	Lên đến 10 Gigabit
c6a.32xlarge	5,6448 USD	128	256 GiB	Chỉ EBS	50000 Megabit
m6i.2xlarge	0,48 USD	8	32 GiB	Chỉ EBS	Lên đến 12500 Megabit
c6in.2xlarge	0,5208 USD	8	16 GiB	Chỉ EBS	Lên đến 40000 Megabit
g5g.xlarge	0,5877 USD	4	8 GiB	Chỉ EBS	Lên đến 10 Gigabit

Hình 2. Bảng giá đề xuất dịch vụ EC2 (PAYG)

5 KẾT LUẬN

Mục tiêu	Tóm tắt nhu cầu	Giải pháp trong thiết kế	Mức độ đáp ứng
Developer và Tester chỉ được sử dụng máy bàn tại công ty,	Trụ sở chính: - Số lượng: 32 người.	Trụ sở chính: - Mạng: 192.168.0.0/26 cho 62 hosts.	- Số lượng: Đáp ứng (100%)

không được sử dụng laptop riêng để truy cập vào mạng của công ty (chi nhánh và trụ sở)	- Băng thông: 20Mbps/người. - Chỉ cho phép sử dụng máy bàn tại công ty. <u>Chi nhánh:</u> - Số lượng: 18 người. - Băng thông: 20Mbps/người. - Chỉ cho phép sử dụng máy bàn tại công ty.	- Chỉ sử dụng kết nối có dây cho các PC có sẵn. - Ba gói Super 400 cho tổng băng thông là 1200Mbps (Dư băng thông vì đã tính bao gồm các vị trí khác). - Router CR1009 có khả năng cung cấp hơn 1000Mps. - DHCP, VLAN, OSPF, HSRP, NAT. - Sử dụng SW 48port đủ cung cấp cho số lượng hosts. <u>Chi nhánh:</u> - Mạng: 192.168.1.0/27 cho 30 hosts. - Chỉ sử dụng kết nối có dây cho các PC có sẵn. - Hai gói Super 300 cho tổng băng thông là 600Mbps. - Router RB3011 có khả năng cung cấp 1000Mps. - DHCP, VLAN, OSPF, HSRP, NAT, VPN. - Sử dụng SW 48port đủ cung cấp cho số lượng hosts.	- Băng thông: Đáp ứng (100%) - Thiết bị: Đáp ứng khả năng yêu cầu. (100%) - Tính khả thi: Đáp ứng (100%) - Tính bảo mật: Đảm bảo (Do có sử dụng IPS, IDS và Firewall để giám sát lưu lượng mạng).
CEO, HR, Project manager, Technical Manager, Business Analyst, IT operation được sử dụng Laptop, truy cập vào hệ thống wifi nội bộ sử dụng tài khoản xác thực (trụ sở).	- Số lượng: 13 người (Bao gồm HR, BA, PM, CEO, TM gọi chung là nhóm đối tượng 1). - Băng thông: 20Mbps/người. - Số lượng: 1 người (Bao gồm IT Operator gọi chung là nhóm đối tượng 2). - Băng thông: 30Mbps/người. - Chỉ cho phép sử dụng máy bàn tại công ty. - Nhóm đối tượng 1 và đối tượng 2 đều sử dụng mạng không dây nội bộ để truy cập.	- Ba gói Super 400 cho tổng băng thông là 1200Mbps (Dư băng thông vì đã tính bao gồm các vị trí khác). - Sử dụng 2 SW 8 port cho kết nối WLC. - Sử dụng 6 LAP, 2 WLC. - Ngoài ra, có sử dụng PDC, ADC để quản lý Auth cho WPA2 Enterprise. <u>Đối tượng 1:</u> - Mạng: 192.168.0.64/27 cho 30 hosts. - DHCP, VLAN, OSPF, HSRP, giao thức không dây, NAT <u>Đối tượng 2:</u>	- Số lượng: Đáp ứng (100%) - Băng thông: Đáp ứng (100%) - Thiết bị: Đáp ứng khả năng yêu cầu. (100%) - Tính khả thi: Đáp ứng (100%) - Độ phủ song wifi: Đủ số lượng và đáp ứng nhu cầu (100%) - Tính bảo mật: Đảm bảo (Do có sử dụng IPS, IDS và Firewall để

		- Mạng: 192.168.0.104/29 cho 6 hosts. - DHCP, VLAN, OSPF, HSRP, giao thức không dây, NAT, VPN, SSH, SNMP.	giám sát lưu lượng mạng).
Một hệ thống wifi public với đường kết nối Internet riêng (chi nhánh và trụ sở).	- Sử dụng đường kết nối riêng. - Số lượng ~ 254 hosts. - Băng thông tối thiểu 4Mbps/hosts.	- Sử dụng 8 LAP, 1SW 10 port để điều khiển và kết nối LAP, 1 WLC. - Giao thức không dây, sử dụng bảo mật WPA2. - Ba gói Super300 cho tổng cung cấp 900Mbps. <u>Trụ sở chính:</u> - Mạng: 172.20.0.0/24 cho 254 hosts. <u>Chi nhánh:</u> - Mạng: 172.20.1.0/24 cho 254 hosts.	- Số lượng: Đáp ứng (100%) - Băng thông: Đáp ứng (100%) - Thiết bị: Đáp ứng khả năng yêu cầu. (100%) - Tính khả thi: Đáp ứng (100%) - Độ phủ song wifi: Đủ số lượng và đáp ứng nhu cầu (100%) - Tính bảo mật: Đảm bảo (Do có sử dụng IPS, IDS và Firewall để giám sát lưu lượng mạng).
Hệ thống phần cứng để triển khai hệ thống server ảo phục vụ cho việc deploy các ứng dụng trong giai đoạn test (trụ sở).	- Có host server riêng. - Sử dụng hypervisor VMware vSphere. - CPU: Đề xuất sử dụng CPU có hiệu năng cao, với 16 lõi (core) và tần số xung nhịp cao để xử lý các tác vụ ảo hóa. - RAM: Đề xuất sử dụng RAM đủ lớn để chia sẻ cho các máy ảo và đảm bảo hiệu suất cao. - DISK: Sử dụng ổ cứng tốc độ cao và có dung lượng đủ để lưu trữ hệ điều hành, hypervisor và các máy ảo	IBM 8205-E6B P740	- Số lượng: Đáp ứng (100%) - Thiết bị: Đáp ứng khả năng yêu cầu. (100%) - Tính khả thi: Đáp ứng (100%)
Sử dụng các dịch vụ Cloud để deploy các ứng dụng trong giai đoạn	- Đáp ứng được nhu cầu trong quá trình sử dụng, phát triển sản phẩm của công ty.	- Đưa ra giải pháp, phương án tối ưu cho doanh nghiệp lựa chọn, sử dụng dịch vụ một cách	Tương đối đáp ứng được yêu cầu của khách hàng.

staging để khách hàng sử dụng thử trước khi đưa ra thực tế (trụ sở).		hiệu quả nhất. Đề xuất giải pháp Pay as you go cho khách hàng. - Đưa ra bảng tham khảo giá của AWS.	
Sử dụng kết nối VPN site-to-site để truy cập server nội bộ và deploy ứng dụng lên hệ thống tại Data Center (chi nhánh)	- Thiết lập VPN site-to-site cho chi nhánh có thể kết nối vào mạng nội bộ của công ty.	- Thiết lập VPN trên firewall FortiGate 40F.	- Tính khả thi: Đáp ứng (100%)
Khả năng hoạt động của toàn bộ hệ thống.		- Hệ thống sử dụng các thiết bị IPS, IDS và Firewall đặt tại vị trí phù hợp cho khả năng giám sát mạng. - Khả năng dự phòng trong trường hợp gặp sự cố (HSRP). - Khả năng mở rộng cao khi sử dụng mô hình quản lý riêng lẻ các nhóm mục đích - Khả năng Backup dữ liệu.	Đáp ứng (100%)

Mục tiêu và yêu cầu	Kết quả	Đánh giá
Developer và Tester chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop riêng để truy cập vào mạng của công ty (chi nhánh và trụ sở)	✓	Đáp ứng được yêu cầu.
CEO, HR, Project manager, Technical Manager, Business Analyst, IT operation được sử dụng Laptop, truy cập vào hệ thống wifi nội bộ sử dụng tài khoản xác thực (trụ sở).	✓	Đáp ứng được yêu cầu, hệ thống mạng nội bộ riêng có sự phân tách giữa IT Operator và lãnh đạo (CEO, HR, Project manager, Technical Manager, Business Analyst) để tăng cường khả năng bảo mật cũng như quản lý).
Một hệ thống wifi public với đường kết nối Internet riêng (chi nhánh và trụ sở).	✓	Đáp ứng được yêu cầu, bên phần mạng nội bộ có sử dụng thiết bị IPS/IDS cho khả năng giám sát truy cập.
Hệ thống phần cứng để triển khai hệ thống server ảo phục vụ cho việc deploy	✓	Đáp ứng được yêu cầu.

các ứng dụng trong giai đoạn test (trụ sở).		
Sử dụng các dịch vụ Cloud để deploy các ứng dụng trong giai đoạn staging để khách hàng sử dụng thử trước khi đưa ra thực tế (trụ sở).	✓	Đưa ra giải pháp, phương án tối ưu cho doanh nghiệp lựa chọn, sử dụng dịch vụ một cách hiệu quả nhất.
Sử dụng kết nối VPN site-to-site để truy cập server nội bộ và deploy ứng dụng lên hệ thống tại Data Center (chi nhánh)	✓	Đáp ứng được yêu cầu.
Khả năng hoạt động của toàn bộ hệ thống.	Đảm bảo	Hệ thống sử dụng các thiết bị IPS, IDS và Firewall đặt tại vị trí phù hợp cho khả năng giám sát mạng. Đồng thời hệ thống còn cung cấp khả năng dự phòng trong trường hợp gặp sự cố (HSRP), khả năng mở rộng cao khi sử dụng mô hình quản lý riêng lẻ các nhóm mục đích và khả năng Backup dữ liệu.

Hệ thống mạng được thiết kế và triển khai bởi nhóm đã được đánh giá và phân tích dựa trên mục tiêu cung cấp. Nhóm em đã đáp ứng được toàn bộ yêu cầu mục tiêu và đồng thời mở rộng các tính năng thực tế để đáp ứng nhu cầu của doanh nghiệp.

Một trong những tính năng mở rộng quan trọng mà nhóm em đã đưa vào hệ thống mạng là việc sử dụng dịch vụ Cloud để lưu trữ dữ liệu sao lưu (backup). Bằng cách sử dụng Cloud, nhóm tạo ra một hệ thống lưu trữ linh hoạt và đáng tin cậy, cho phép doanh nghiệp sao lưu dữ liệu quan trọng và khôi phục nhanh chóng khi cần thiết. Việc sử dụng Cloud cũng giúp giảm rủi ro mất mát dữ liệu do sự cố hệ thống và cung cấp khả năng mở rộng linh hoạt theo nhu cầu của doanh nghiệp.

Thêm vào đó, bọn em đã tích hợp thiết bị IPS (Intrusion Prevention System) vào hệ thống mạng để theo dõi và bảo vệ lưu lượng mạng. Thiết bị IPS giám sát và phát hiện các hành vi xâm nhập, tấn công mạng và các mối đe dọa tiềm ẩn. Bằng cách theo dõi lưu lượng mạng và áp dụng các biện pháp bảo mật tự động, đảm bảo rằng hệ thống mạng của doanh nghiệp được bảo vệ một cách hiệu quả và giảm thiểu rủi ro liên quan đến an ninh mạng.

Tổng quan, hệ thống mạng do nhóm em thực hiện không chỉ đáp ứng được các yêu cầu mục tiêu ban đầu mà còn mở rộng ra nhiều tính năng thực tế, nhằm tối ưu hóa hiệu suất, bảo mật và khả năng mở rộng của mạng trong môi trường doanh nghiệp.

TÀI LIỆU THAM KHẢO

[1] AWS, "Giá theo nhu cầu của Amazon EC2," [Online]. Available: https://aws.amazon.com/vi/ec2/pricing/on-demand/.

[2] AWS, "Giá Amazon S3," [Online]. Available: https://aws.amazon.com/vi/s3/pricing/.

[3] "Tham khảo giá thiết bị," [Online]. Available: https://www.ebay.com/.

[4] F. Telecom, "Bảng giá cho thuê hoặc mua IP tĩnh FPT," [Online]. Available: https://fpttelecom.info.vn/cho-thue-ip-tinh-fpt/.

[5] Microsoft, "Giấy phép và giá cho Windows Server 2022," 2022. [Online]. Available: https://www.microsoft.com/vi-vn/windows-server/pricing.

[6] L. Cường, "Thiết kế hệ thống mạng nội bộ cho công ty," 21 April 2011. [Online]. Available: https://www.lecuong.info/2010/11/thiet-ke-mang-noi-bo-cty.html.

[7] N. L. Minh, "Giải pháp Wifi cho 200 người dùng phòng hội thảo, quán cafe, phòng học trực tuyến, khách sạn," 10 January 2023. [Online]. Available: https://viettuans.vn/giai-phap-wifi-200-nguoi-dung.