**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO BÀI TẬP**

Môn học: Thiết kế Mạng

Giáo viên hướng dẫn: ThS. Bùi Thanh Bình

Mã lớp: NT113.P22

|  |  |  |
| --- | --- | --- |
| Họ và tên | Mã số sinh viên | Email |
| Hồ Công Hiếu | 22520433 | 22520433@gm.uit.edu.vn |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | NĂM HỌC : 2024 - 2025 |  |

**MỤC LỤC**

[**LỜI CẢM ƠN 3**](#_Toc184752136)

[**1. Giới thiệu tổng quan: 4**](#_Toc184752137)

[**2. Các thông tin cơ bản về đề tài: 4**](#_Toc184752138)

[**3. Thiết kế hệ thống mạng: 5**](#_Toc184752139)

[3.1 Thiết kế mô hình mạng logic: 6](#_Toc184752140)

[3.2 Thiết kế sơ đồ vật lý cho toàn bộ hệ thống mạng. 6](#_Toc184752141)

[3.2.1 Sơ đồ vật lý: 6](#_Toc184752142)

[3.2.2 Các thiết bị dùng trong hệ thống: 10](#_Toc184752143)

[3.3.3 Các dịch vụ cần thuê: 10](#_Toc184752144)

[**3.3 Đặt địa chỉ IP cho hệ thống mạng và thiết bị. 11**](#_Toc184752145)

[**4. Các dịch vụ của hệ thống và chi phí hoạt động: 14**](#_Toc184752614)

[4.1 Các dịch vụ cung cấp: 14](#_Toc184752615)

[4.2 Chi phí cho toàn hệ thống: 15](#_Toc184752616)

[4.2.1 Chi phí cho thiết bị: 15](#_Toc184752617)

[4.2.2 Chi phí dịch vụ: 15](#_Toc184752618)

[**5. Kết luận: 15**](#_Toc184752619)

[5.1 Đánh giá hiệu suất và tính khả thi: 15](#_Toc184752620)

[5. 2 Hướng phát triển tương lai: 16](#_Toc184752621)

[**6. Tài liệu tham khảo 16**](#_Toc184752622)

# LỜI CẢM ƠN

Trước hết, nhóm chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến Thầy Th.S Bùi Thanh Bình, người đã luôn tận tình hướng dẫn, hỗ trợ và dành nhiều thời gian quý báu trong suốt quá trình thực hiện đề tài "Thiết lập hệ thống mạng cho công ty tài chính FastPay ".

Nhờ sự chỉ bảo tỉ mỉ, những ý kiến đóng góp quý báu và sự hỗ trợ tận tâm của Thầy, nhóm em đã có cơ hội áp dụng kiến thức lý thuyết vào thực tiễn, đồng thời nâng cao hiểu biết về cách triển khai và quản lý hệ thống mạng một cách bài bản. Đây là một hành trình đầy thử thách nhưng cũng rất bổ ích, giúp chúng em trưởng thành hơn cả về mặt chuyên môn lẫn kỹ năng làm việc.

Thầy không chỉ giúp em củng cố những kiến thức đã học mà còn truyền đạt thêm những kinh nghiệm thực tế vô cùng quý giá trong lĩnh vực quản trị mạng và triển khai hệ thống công nghệ thông tin. Những buổi trao đổi và góp ý từ Thầy đã mở ra cho em một cách nhìn mới, giúp em nhận thức sâu sắc hơn về tầm quan trọng của việc thiết kế hệ thống mạng đáp ứng đầy đủ các yêu cầu bảo mật, hiệu suất và khả năng mở rộng trong môi trường doanh nghiệp thực tế. Ngoài những kiến thức chuyên môn, em cũng học được từ Thầy thái độ nghiêm túc, tinh thần trách nhiệm và sự kiên trì – những yếu tố cần thiết để không chỉ hoàn thành đồ án này mà còn để phát triển bản thân trong hành trình sự nghiệp sau này.

Tuy nhiên, em nhận thấy rằng, với thời gian và kiến thức còn hạn chế, đồ án này chắc chắn không thể tránh khỏi một số thiếu sót. Các giải pháp được triển khai có thể chưa bao quát hết các tình huống thực tế phát sinh hoặc chưa tối ưu hoàn toàn về mặt hiệu suất và bảo mật. Nhóm em mong rằng sẽ nhận được thêm những ý kiến đóng góp quý báu từ Thầy để có thể hoàn thiện hơn những phần chưa đạt yêu cầu, đồng thời học hỏi thêm kinh nghiệm để áp dụng vào thực tế công việc sau này.

Một lần nữa, chúng em xin chân thành cảm ơn Thầy vì sự tận tâm và sự chỉ dẫn quý giá. Chúc Thầy luôn mạnh khỏe, tiếp tục thành công trong sự nghiệp giảng dạy và truyền cảm hứng cho các thế hệ sinh viên.

Trân trọng,

Nhóm 18.

# Giới thiệu tổng quan:

# Trong thời đại công nghệ số phát triển mạnh mẽ, ngành tài chính – ngân hàng đòi hỏi hệ thống hạ tầng mạng không chỉ đáp ứng hiệu suất cao mà còn phải đảm bảo các tiêu chuẩn bảo mật khắt khe và khả năng mở rộng linh hoạt. Đặc biệt với các công ty cung cấp dịch vụ thanh toán trực tuyến như FastPay, hạ tầng mạng đóng vai trò xương sống giúp đảm bảo hoạt động giao dịch liên tục, ổn định và an toàn.

# Công ty tài chính FastPay hiện có trụ sở chính đặt tại Quận 1, TP.HCM và hai chi nhánh tại Hà Nội và Đà Nẵng. Với đặc thù lĩnh vực hoạt động, hệ thống mạng của công ty cần phải:

# Hỗ trợ giao dịch trực tuyến có độ trễ thấp và độ sẵn sàng cao;

# Đảm bảo an toàn tuyệt đối cho dữ liệu tài chính nhạy cảm;

# Dễ dàng mở rộng khi phát triển thêm chi nhánh hoặc nâng cấp hệ thống.

# Đề tài "Thiết kế hệ thống mạng cho Công ty tài chính FastPay" được thực hiện nhằm xây dựng một mô hình mạng tối ưu, đảm bảo an toàn bảo mật, kết nối linh hoạt giữa các địa điểm và sẵn sàng tích hợp hạ tầng điện toán đám mây (Hybrid Cloud). Bên cạnh đó, đề tài cũng là cơ hội để nhóm vận dụng tổng hợp các kiến thức đã học về thiết kế mạng, bảo mật, kết nối VPN và giám sát hiệu suất hệ thống.

# Các thông tin cơ bản về đề tài:

**Phân tích yêu cầu khách hàng:**

* **Trụ sở chính – TP.Hồ Chí Minh:**

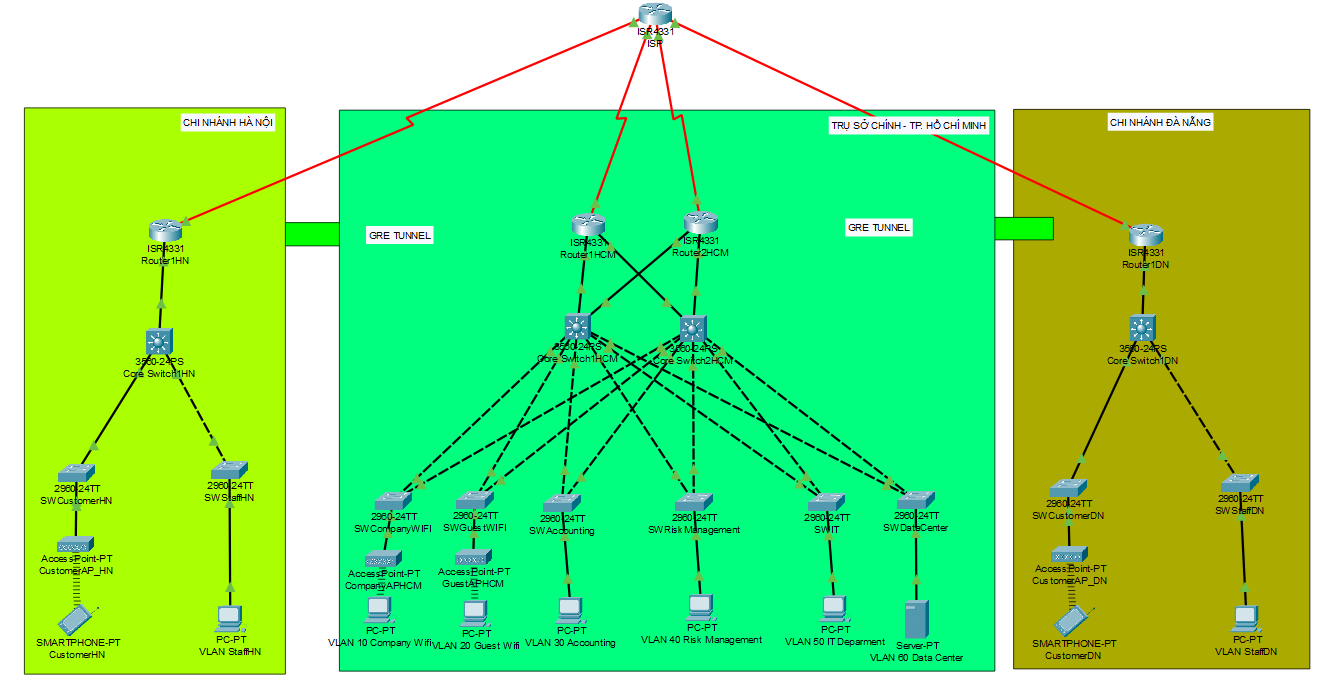
|  |  |
| --- | --- |
| **Yêu cầu** | **Nội dung** |
| Các thiết bị sử dụng | -Nhân viên các phòng ban như Kế toán, Quản lý Rủi ro, IT, và Data Center sẽ sử dụng máy bàn cố định trong mạng nội bộ tại công ty, kết nối qua các switch tương ứng với VLAN riêng. |
| Wifi nội bộ(VLAN10) | - Cung cấp hệ thống wifi nội bộ với khả năng xác thực người dùng (Sử dụng tài khoản xác thực).  - Wifi này dành cho các nhân viên của các phòng ban như Kế toán, Quản lý Rủi ro, IT và Data Center, kết nối với VLAN 10 (Company WiFi) qua Core Switch và các Switch của từng chi nhánh. - Zero Trust Security sẽ được áp dụng để chỉ cho phép các thiết bị và người dùng có quyền truy cập vào mạng nội bộ.. |
| Wifi công cộng(VLAN20) | - Cung cấp WiFi khách riêng biệt, cách ly hoàn toàn khỏi mạng nội bộ. - WiFi sẽ yêu cầu xác thực qua Captive Portal (một trang web mở ra khi kết nối vào WiFi) và có giới hạn băng thông để đảm bảo không ảnh hưởng đến mạng chính. - WiFi khách sẽ được kết nối với VLAN 20 và được phép truy cập Internet nhưng không có quyền truy cập vào các hệ thống nội bộ của công ty. |
| Bảo mật cao | - Áp dụng các công nghệ bảo mật như IDS/IPS, SIEM và Firewall Layer 7 để đảm bảo an toàn cho hệ thống mạng. - Cấu hình Zero Trust Security để không có thiết bị nào được phép truy cập mạng nội bộ mà không qua kiểm tra và xác thực. |
| Triển khai Hybrid Cloud | -Hệ thống giao dịch trực tuyến sẽ được triển khai trên nền tảng Hybrid Cloud (AWS/GCP), kết hợp giữa cơ sở hạ tầng tại chỗ và điện toán đám mây để nâng cao hiệu suất và khả năng mở rộng. |
| Đảm bảo kết nối mạng nội bộ | - Mạng nội bộ cần được thiết lập để đảm bảo việc kết nối giữa các phòng ban, các nhóm phát triển và tester, cũng như kết nối giữa các máy chủ và các ứng dụng nội bộ. |

* **Chi nhánh Đà Nẵng và Hà Nội:**

|  |  |
| --- | --- |
| **Yêu cầu** | **Nội dung** |
| Các thiết bị sử dụng | - Nhân viên chỉ được sử dụng máy bàn tại công ty, không được sử dụng laptop cá nhân để truy cập mạng công ty. |
| Kết nối VPN site-to-site | - Sử dụng kết nối VPN site-to-site để đảm bảo kết nối an toàn, bảo mật và ổn định giữa chi nhánh và trụ sở chính |
| Hệ thống bảo mật | - Cần các giải pháp bảo mật phù hợp để đảm bảo việc kết nối và truy cập giữa chi nhánh và trụ sở chính là an toàn, đặc biệt với việc sử dụng VPN site-to-site. |

# Thiết kế hệ thống mạng:

## **3.1 Thiết kế mô hình mạng logic:**



## **3.2 Thiết kế sơ đồ vật lý cho toàn bộ hệ thống mạng.**

### **3.2.1: Sơ đồ vật lý:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Loại thiết bị** | **Mẫu nhóm sản phẩm** | **Số cổng và các giao diện** | **Mô tả chức năng** | **Số lượng** | **Đơn giá** | **Thành tiền** |
| Router | Router Cisco ISR4331-AX/K9 | 3 cổng Gigabit Ethernet WAN/LAN (RJ45 và SFP)  2 khe NIM  1 khe SM-X  2 cổng USB  1 cổng Console và 1 cổng Aux | - Hỗ trợ thông lượng từ 100 Mbps đến 300 Mbps, phù hợp với các ứng dụng yêu cầu băng thông lớn.  - Hỗ trợ nhiều tính năng bảo mật như tường lửa, VPN, và quản lý mối đe dọa (với giấy phép nâng cấp).  - Tích hợp khả năng hỗ trợ VoIP, video, và dịch vụ mạng SD-WAN.  - Hỗ trợ các module NIM (Network Interface Module) và SM-X (Service Module), giúp mở rộng chức năng mạng theo nhu cầu.  - Cung cấp khả năng giám sát và cấu hình qua giao diện web hoặc giao diện dòng lệnh (CLI). | 4 | $2,360 | $9,440 |
| Switch  Layer3 | Cisco Catalyst C9200-48PB-A | 48 cổng RJ-45 tốc độ 1 Gbps hỗ trợ PoE+.  4 cổng uplink quang tốc độ 10 Gbps (SFP+). | - Cho phép cấp nguồn cho các thiết bị như camera IP, điện thoại IP, và điểm truy cập Wi-Fi mà không cần dây nguồn riêng.  - Tích hợp các biện pháp bảo vệ để đảm bảo tính toàn vẹn của phần cứng, phần mềm, và dữ liệu truyền qua switch.  - Hỗ trợ công nghệ StackWise-80, cho phép kết hợp nhiều switch thành một thực thể quản lý với băng thông xếp chồng 80 Gbps, tối đa 8 switch cùng loại trong một stack.  - Với 4 cổng uplink 10G, switch này đảm bảo hiệu suất kết nối giữa các tầng mạng.  - Chạy phần mềm Network Advantage, cung cấp các tính năng như định tuyến nâng cao (OSPF, EIGRP, BGP), QoS, và khả năng phân đoạn mạng (VLAN). | 4 | $6,927.90 | $27,711.6 |
| Switch  Layer 2 | Cisco Catalyst C1000-48FP-4G-L | 48 cổng PoE+ (10/100/1000 Mbps)  4 cổng SFP uplink (1G) | - Hỗ trợ chuẩn IEEE 802.3af/at (PoE+) với tổng công suất lên tới 740W, phù hợp để cấp nguồn cho các thiết bị như camera IP, điện thoại IP, và điểm truy cập không dây (AP).  - Hỗ trợ module quang Gigabit SFP (1G) để mở rộng băng thông và kết nối khoảng cách xa.  - Switch cung cấp khả năng chuyển tiếp ở tốc độ dây (wire-speed), đảm bảo hiệu suất cao trong môi trường nhiều thiết bị  - Hỗ trợ CLI (Command Line Interface) và giao diện web GUI thân thiện, giúp dễ dàng cấu hình và quản lý thiết bị. Có thể tích hợp với các công cụ quản lý mạng như CNA hoặc SNMP để giám sát và điều khiển từ xa.  - Tính năng Storm Control giới hạn lưu lượng Broadcast, Multicast và Unicast nhằm bảo vệ mạng khỏi các cơn bão lưu lượng.  - Phát hiện và ngăn chặn các vòng lặp trong mạng nhờ tính năng Spanning Tree Protocol (STP).  - Hỗ trợ kết nối với nguồn cấp điện dự phòng (RPS), đảm bảo hoạt động liên tục ngay cả khi nguồn chính gặp sự cố. | 10 | $3,832 | $38,320 |
| Access Point | Cisco AIR-AP2802I-I-K9 | 2 cổng Gigabit Ethernet  1 cổng Console  1 cổng USB 2.0  Kensington lock slot | - Tốc độ lý thuyết lên đến 5.2 Gbps, gấp 4 lần các thiết bị chuẩn 802.11ac Wave 1.  **-** Công nghệ MU-MIMO: Hỗ trợ 4x4 Multi-User Multiple Input Multiple Output, tăng cường hiệu suất và cho phép nhiều thiết bị kết nối đồng thời mà không giảm băng thông.  - Tối ưu hóa tín hiệu để tăng độ ổn định và hiệu năng cho thiết bị di động.  - Theo dõi và giảm thiểu nhiễu sóng không dây  - Flexible Radio Assignment tự động chuyển đổi tần số giữa 2.4 GHz và 5 GHz dựa trên môi trường sử dụng.  - Hỗ trợ chế độ giám sát an ninh không dây để phát hiện các mối đe dọa. | 4 | $1,355 | $5,420 |
| Tổng |  | | | | | $80,891.6 |

### 

### **3.2.2: Các thiết bị dùng trong hệ thống:**

* Router Cisco ISR4331-AX/K9
* Switch Layer 3 Cisco Catalyst C9200-48PB-A
* Switch Layer 2 Cisco Catalyst C1000-48FP-4G-L
* Access Point Cisco AIR-AP2802I-I-K9

### **3.2.3: Các dịch vụ cần thuê:**

* **Mạng nội bộ:** Lux800 (FPT Telecom): 1.000.000đ/ tháng
* **Mạng công cộng:** Lux 500 (FPT Telecom): 800.000đ/tháng

## **3.3 Đặt địa chỉ IP cho hệ thống mạng và thiết bị.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng chia IP cho trụ sở chính** | | | | |
| **Subnet** | **Size** | **Address** | **Subnet mask** | **Broadcast** |
| Company Wifi | 248 | 192.168.10.0/24 | 255.255.255.0 | 192.168.10.255 |
| Guest Wifi | 248 | 192.168.20.0/24 | 255.255.255.0 | 192.168.20.255 |
| Accounting | 248 | 192.168.30.0/24 | 255.255.255.0 | 192.168.30.255 |
| Risk Management | 248 | 192.168.40.0/24 | 255.255.255.0 | 192.168.40.255 |
| IT | 248 | 192.168.50.0/24 | 255.255.255.0 | 192.168.50.255 |
| Data Center | 248 | 192.168.60.0/24 | 255.255.255.0 | 192.168.60.255 |
| Core Switch 1 – Router 1 | 2 | 192.168.1.4/30 | 255.255.255.252 | 192.168.1.7 |
| Core Switch 1 – Router 2 | 2 | 192.168.1.16/30 | 255.255.255.252 | 192.168.2.19 |
| Core Switch 2 – Router 1 | 2 | 192.168.1.12/30 | 255.255.255.252 | 192.168.1.15 |
| Core Switch 2 – Router 2 | 2 | 192.168.1.8/30 | 255.255.255.252 | 192.168.1.11 |
| VPN Router 1 to HN | 248 | 192.168.250.0/24 | 255.255.255.0 | 192.168.250.255 |
| VPN Router 1 to DN | 248 | 192.168.253.0/24 | 255.255.255.0 | 192.168.253.255 |
| VPN Router 2 to HN | 248 | 192.168.252.0/24 | 255.255.255.0 | 192.168.252.255 |
| VPN Router 2 to DN | 248 | 192.168.251.0/24 | 255.255.255.0 | 192.168.251.255 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng chia IP cho chi nhánh Hà Nội** | | | | |
| **Subnet** | **Size** | **Address** | **Subnet mask** | **Broadcast** |
| Staff | 248 | 192.168.201.0/24 | 255.255.255.0 | 192.168.201.255 |
| Core Switch – Router | 2 | 192.168.200.0/30 | 255.255.255.252 | 192.168.200.3 |
| Customer | 248 | 192.168.202.0/24 | 255.255.255.0 | 192.168.202.255 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng chia IP cho chi nhánh Hà Nội** | | | | |
| **Subnet** | **Size** | **Address** | **Subnet mask** | **Broadcast** |
| Staff | 248 | 192.168.211.0/24 | 255.255.255.0 | 192.168.211.255 |
| Core Switch – Router | 2 | 192.168.210.0/30 | 255.255.255.252 | 192.168.210.3 |
| Customer | 248 | 192.168.212.0/24 | 255.255.255.0 | 192.168.212.255 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng đặt IP cho cơ sở chính** | | | | |
| **Device** | **Interface** | **Address** | **Subnet mask** | **Default Gateway** |
| **Router1HCM** | G0/0/0 | 192.168.1.6 | 255.255.255.252 | N/A |
| G0/0/1 | 192.168.1.13 | 255.255.255.252 | N/A |
| Se0/1/0 | 9.0.0.2 | 255.255.255.252 | N/A |
| Tunnel0 | 192.168.250.1 | 255.255.255.0 | N/A |
| Tunnel1 | 192.168.253.1 | 255.255.255.0 | N/A |
| **Router2HCM** | G0/0/0 | 192.168.1.10 | 255.255.255.252 | N/A |
| G0/0/1 | 192.168.1.17 | 255.255.255.252 | N/A |
| Se0/1/0 | 9.0.0.6 | 255.255.255.252 | N/A |
| Tunnel0 | 192.168.251.1 | 255.255.255.252 | N/A |
| Tunnel1 | 192.168.252.1 | 255.255.255.252 | N/A |
| **Core Switch1HCM** | Fa0/1 | 192.168.1.5 | 255.255.255.252 | N/A |
| Fa0/5 | 192.168.1.18 | 255.255.255.252 | N/A |
| VLAN10 (Company WiFi) | 192.168.10.1 | 255.255.255.0 | N/A |
| VLAN20 (Guest WiFi) | 192.168.20.1 | 255.255.255.0 | N/A |
| VLAN30(Accounting) | 192.168.30.1 | 255.255.255.0 | N/A |
| VLAN40 (Risk Management) | 192.168.40.1 | 255.255.255.0 | N/A |
| VLAN50 (IT Department) | 192.168.50.1 | 255.255.255.0 | N/A |
| VLAN60 (Data Center) | 192.168.60.1 | 255.255.255.0 | N/A |
| **CoreSW2Main** | Fa0/1 | 192.168.1.9 | 255.255.255.252 | N/A |
| Fa0/5 | 192.168.1.14 | 255.255.255.252 | N/A |
| VLAN10 (Company WiFi) | 192.168.10.2 | 255.255.255.0 | N/A |
| VLAN20 (Guest WiFi) | 192.168.20.2 | 255.255.255.0 | N/A |
| VLAN30 (Accounting) | 192.168.30.2 | 255.255.255.0 | N/A |
| VLAN40 (Risk Management) | 192.168.40.2 | 255.255.255.0 | N/A |
| VLAN50 (IT Department) | 192.168.50.2 | 255.255.255.0 | N/A |
| VLAN60 (Data Center) | 192.168.60.2 | 255.255.255.0 | N/A |
| **HSRP Virtual Gateway** | VLAN10 (Company WiFi) | 192.168.10.254 | 255.255.255.0 | N/A |
| VLAN20 (Guest WiFi) | 192.168.20.254 | 255.255.255.0 | N/A |
| VLAN30 (Accounting) | 192.168.30.254 | 255.255.255.0 | N/A |
| VLAN40 (Risk Management) | 192.168.40.254 | 255.255.255.0 | N/A |
| VLAN50 (IT Department) | 192.168.50.254 | 255.255.255.0 | N/A |
| VLAN60 (Data Center) | 192.168.60.254 | 255.255.255.0 | N/A |
| **Company Wifi PC** | NIC | DHCP (192.168.10.21-253) | 255.255.255.0 | 192.168.10.254 |
| **Guest Wifi PC** | NIC | DHCP (192.168.20.21-253) | 255.255.255.0 | 192.168.20.254 |
| **Accounting PC** | NIC | DHCP (192.168.30.21-253) | 255.255.255.0 | 192.168.30.254 |
| **Risk Mangagement PC** | NIC | DHCP (192.168.40.21-253) | 255.255.255.0 | 192.168.40.254 |
| **IT Department PC** | NIC | DHCP (192.168.50.21-253) | 255.255.255.0 | 192.168.50.254 |
| **Data Center** | NIC | DHCP (192.168.60.21-253) | 255.255.255.0 | 192.168.60.254 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng đặt IP cho chi nhánh Hà Nội** | | | | |
| **Device** | **Interface** | **Address** | **Subnet mask** | **Default Gateway** |
| **Router1HN** | G0/0/0 | 192.168.200.2 | 255.255.255.252 | N/A |
| S0/1/0 | 7.0.0.2 | 255.255.255.252 | N/A |
| Tunnel0 | 192.168.250.2 | 255.255.255.0 | N/A |
| Tunnel1 | 192.168.252.2 | 255.255.255.0 | N/A |
| **Core Switch1HN** | Fa0/1 | 192.168.200.1 | 255.255.255.252 | N/A |
| VLAN201 | 192.168.201.1 | 255.255.255.0 | 255.255.255.0 |
| VLAN202 | 192.168.202.1 | 255.255.255.0 | 255.255.255.0 |
| **Staff PC** | NIC | DHCP (192.168.201.21-253) | 255.255.255.0 | 192.168.201.1 |
| **Customer Smartphone** | NIC | DHCP(192.168.202.21-253) | 255.255.255.0 | 192.168.202.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bảng đặt IP cho chi nhánh Đà Nẵng** | | | | |
| **Device** | **Interface** | **Address** | **Subnet mask** | **Default Gateway** |
| **Router1DN** | G0/0/0 | 192.168.210.2 | 255.255.255.252 | N/A |
| S0/1/0 | 8.0.0.2 | 255.255.255.252 | N/A |
| Tunnel0 | 192.168.251.2 | 255.255.255.0 | N/A |
| Tunnel1 | 192.168.253.2 | 255.255.255.0 | N/A |
| **Core Switch1DN** | Fa0/1 | 192.168.210.1 | 255.255.255.252 | N/A |
| VLAN211 | 192.168.211.1 | 255.255.255.0 | N/A |
|  | VLAN212 | 192.168.212.1 | 255.255.255.0 | N/A |
| **Staff PC** | NIC | DHCP (192.168.211.21-253 | 255.255.255.0 | 192.168.211.1 |
| **Customer Smartphone** | NIC | DHCP (192.168.212.21-253 | 255.255.255.0 | 192.168.212.1 |

## **3.4 Thiết kế hệ thống Hybrid Cloud**

### **3.4.1 Mô hình tổng quát**

A screenshot of a computer

AI-generated content may be incorrect.

### **3.4.2 Thiết kế chi tiết AWS Cloud**

* Máy chủ ứng dụng: 5 EC2 instance loại t3.large (2 vCPU, 8GB RAM).
* Cơ sở dữ liệu: 2 instance db.r5.large (Multi-AZ) chạy PostgreSQL.
* Kết nối giữa trụ sở và AWS: sử dụng Direct Connect cung cấp đường truyền riêng 1Gbps kết nối trực tiếp từ trụ sở đến AWS, đảm bảo độ trễ thấp và băng thông ổn định
* Bảo mật: AWS WAF bảo vệ ứng dụng web, Security Groups và IAM kiểm soát truy cập.
* API: sử dụng AWS API Gateway để quản lý API, xác thực và uỷ quyền API.
* CDN (Content Delivery Network): sử dụng AWS CloudFront để phân phối nội dung nhanh chóng, giảm độ trễ cho người dùng cuối, tối ưu hóa hiệu suất.
* DNS: sử dụng AWS Route53 để quản lý và định tuyến.
* Lưu trữ nhật ký giao dịch, backup, tài liệu KYC và nội dung tĩnh của ứng dụng: sử dụng AWS S3 với độ bền cao (99.999999999%), khả năng mở rộng không giới hạn, và hỗ trợ các chính sách vòng đời tự động chuyển dữ liệu giữa các lớp lưu trữ (Standard → Standard-IA → Glacier) giúp tối ưu chi phí lưu trữ dài hạn cho dữ liệu tài chính.
* Load Balancer: Sử dụng AWS Application Load Balancer (ALB) để phân phối lưu lượng truy cập đến các EC2 instance, hỗ trợ kiểm tra sức khỏe máy chủ, chứng chỉ SSL/TLS và định tuyến theo nội dung.
* Giám sát: Sử dụng Amazon CloudWatch để theo dõi hiệu suất hệ thống, thiết lập cảnh báo tự động, thu thập logs và metric từ tất cả dịch vụ AWS, cho phép phân tích thời gian thực và cung cấp dashboard trực quan về hoạt động của hệ thống thanh toán.

### **3.4.3 Chi phí dịch vụ Cloud**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dịch vụ AWS** | **Cấu hình** | **Chi phí hàng tháng (USD)** | **Chi tiết** |
| AWS Direct Connect | Cổng kết nối 1Gbps  Chuyển dữ liệu ra (5TB/tháng) | $472 | $292 cho cổng kết nối  $180 cho chuyển dữ liệu |
| Amazon EC2 | 5 máy chủ t3.large (2 vCPU, 8GB RAM)  EBS Storage (100GB/máy chủ x 5) | $3,391 | $3,341 cho máy chủ  $50 cho lưu trữ |
| Application Load Balancer | 1 ALB  Xử lý dữ liệu (10TB/tháng) | $71.3 | $25.3 cho ALB  $46 cho xử lý dữ liệu |
| Amazon S3 | Lưu trữ Standard (1TB)  Requests và truyền dữ liệu | $43 | $23 cho lưu trữ  $20 cho requests và truyền dữ liệu |
| Amazon CloudWatch | CloudWatchGiám sát cơ bản  Log chi tiết (100GB)  Cảnh báo và dashboards | $60 | $0 cho giám sát cơ bản  $50 cho log chi tiết  $10 cho cảnh báo và dashboards |
| Amazon RDS (PostgreSQL) | 2 máy chủ db.r5.large (Multi-AZ)  Lưu trữ (500GB)  Backup và snapshot | $745.4 | $590.4 cho máy chủ  $115 cho lưu trữ  $40 cho backup |
| Amazon API Gateway | 50 triệu requests/tháng | $175 | $175 cho các requests API |
| Amazon CloudFront | Chuyển dữ liệu (10TB/tháng)  Requests (100 triệu/tháng) | $940 | $850 cho chuyển dữ liệu  $90 cho requests |
| AWS WAF | Quy tắc cơ bản  Xử lý requests (50 triệu/tháng) | $205 | $5 cho quy tắc cơ bản  $200 cho xử lý requests |
| Amazon Route 53 | Hosted zone  Truy vấn (10 triệu/tháng) | $5.5 | $0.5 cho hosted zone  $5 cho truy vấn |
| Tổng chi phí hàng tháng |  | $6,108.2 |  |

# Các dịch vụ của hệ thống và chi phí hoạt động:

## **4.1 Các dịch vụ cung cấp:**

* Ưu điểm:
* **Giá cả hợp lý**: Hệ thống được thiết kế với chi phí hợp lý, phù hợp với ngân sách của doanh nghiệp, tối ưu hóa chi phí triển khai và vận hành. Đây là một lợi thế lớn, đặc biệt cho các công ty có yêu cầu về ngân sách nhưng vẫn muốn đảm bảo chất lượng và hiệu quả của hệ thống mạng.
* **Hệ thống đầy đủ và hoàn chỉnh**: Hệ thống được xây dựng với đầy đủ tính năng và dịch vụ, đáp ứng các yêu cầu công việc và đảm bảo khả năng phục vụ cho cả trụ sở chính và các chi nhánh. Điều này chứng tỏ sự đầu tư kỹ lưỡng và tính thực tế trong việc thiết kế và triển khai hệ thống mạng.
* **Mô hình mạng đơn giản và dễ mở rộng**: Mô hình mạng được thiết kế với cấu trúc đơn giản nhưng hiệu quả, giúp việc quản lý, nâng cấp hoặc mở rộng hệ thống trở nên dễ dàng khi có nhu cầu phát triển kinh doanh. Điều này đảm bảo sự linh hoạt, thích ứng tốt với những thay đổi trong tương lai mà không cần tái xây dựng toàn bộ hệ thống.
* **Đảm bảo tính liên tục với đường truyền dự phòng**: Việc triển khai đường truyền dự phòng giúp duy trì tính liên tục và ổn định của hệ thống trong trường hợp xảy ra sự cố hoặc gián đoạn mạng. Đây là yếu tố quan trọng để đảm bảo các hoạt động kinh doanh không bị gián đoạn.
* Nhược điểm:
* **Khó khăn khi xử lý khối lượng dữ liệu lớn**: Hệ thống có thể gặp phải vấn đề hiệu suất khi phải xử lý khối lượng dữ liệu lớn hoặc khi có sự gia tăng đột biến số lượng người dùng, do chưa được tối ưu hóa hạ tầng máy ảo. Điều này có thể dẫn đến giảm hiệu quả hoạt động của hệ thống, đặc biệt khi gặp phải tình huống tải cao.
* **Giới hạn sử dụng thiết bị cá nhân tại chi nhánh**: Chính sách không cho phép nhân viên sử dụng thiết bị cá nhân để truy cập vào mạng công ty tại chi nhánh Hà Nội và Đà Nẵng có thể làm giảm sự linh hoạt trong công việc. Điều này đặc biệt bất tiện khi nhân viên cần làm việc từ xa hoặc cần truy cập nhanh chóng để xử lý các công việc khẩn cấp.
* **Cấu hình phức tạp và khó khắc phục sự cố**: Hệ thống với cấu hình phức tạp có thể gây khó khăn trong việc bảo trì và xử lý sự cố. Khi xảy ra lỗi, quá trình sửa chữa có thể tốn nhiều thời gian và yêu cầu đội ngũ kỹ thuật có trình độ chuyên môn cao, điều này có thể làm gián đoạn hoạt động kinh doanh nếu không được giải quyết kịp thời.

## **4.2 Chi phí cho toàn hệ thống:**

### **Chi phí cho thiết bị:**

* Chi phí đầu tư ban đầu cho các thiết bị cần thiết để triển khai toàn bộ hệ thống đã được nêu ở trên là 80,891.6 USD ~ 2,099,945.94VND. Con số này bao gồm các thiết bị phần cứng đã nêu trên. Tuy nhiên, mức chi phí này chưa bao gồm các chi phí phát sinh như phí lắp đặt, phí vận chuyển thiết bị, cũng như các vật tư phụ trợ như dây dẫn mạng hoặc các phụ kiện cần thiết khác. Doanh nghiệp cần dự trù thêm ngân sách cho các khoản này để đảm bảo hệ thống được triển khai một cách đầy đủ và hiệu quả.

### **Chi phí dịch vụ:**

* Chi phí dịch vụ để duy trì hệ thống mà doanh nghiệp cần chi trả hằng tháng cho dịch vụ Cloud là 6108.2 USD ~ 158.651.944 VND, cộng với chi phí mạng nội bộ và công cộng là 1.800.000 VND. Vậy tổng chi phí là 160.451.944 VND.

## **4.3 Giao thức, dịch vụ và cấu hình mạng đề xuất cho mô hình:**

* ACL:
  + Cấu hình ACL trong mô hình mạng có ý nghĩa quan trọng trong việc tăng cường bảo mật và kiểm soát lưu lượng. Nó cho phép quản lý các gói tin dựa trên tiêu chí như địa chỉ IP, giao thức, và cổng đích, giúp ngăn chặn hoặc cho phép truy cập theo yêu cầu. Đặc biệt, trong mạng chia VLAN, ACL đảm bảo tính bảo mật bằng cách kiểm soát việc giao tiếp giữa các VLAN. Ngoài ra, ACL còn đáp ứng nhu cầu tùy chỉnh bảo mật linh hoạt, phù hợp với các yêu cầu cụ thể của khách hàng, giúp bảo vệ tài nguyên mạng hiệu quả.
* HSRP:
  + Đóng vai trò quan trọng trong việc đảm bảo tính sẵn sàng cao và duy trì kết nối liên tục. HSRP cho phép cấu hình một nhóm các router hoạt động như một cổng mặc định ảo, trong đó một router đóng vai trò chính (active) và router khác ở chế độ dự phòng (standby). Khi router chính gặp sự cố, router dự phòng sẽ tự động tiếp quản, đảm bảo các thiết bị trong mạng vẫn có thể kết nối mà không bị gián đoạn. Điều này đặc biệt hữu ích trong các hệ thống yêu cầu độ tin cậy cao, giúp giảm thiểu thời gian ngừng hoạt động và cải thiện trải nghiệm người dùng.
* DHCP:
  + Tự động cấp phát địa chỉ IP và các thông số mạng như subnet mask, gateway mặc định và DNS cho các thiết bị đầu cuối. Điều này giúp giảm thiểu công việc cấu hình thủ công, hạn chế lỗi cấu hình, và tăng hiệu quả quản lý hệ thống. DHCP đặc biệt hữu ích trong các mạng lớn, nơi số lượng thiết bị kết nối thường xuyên thay đổi, đảm bảo mỗi thiết bị đều nhận được địa chỉ IP hợp lệ, đồng thời tối ưu hóa việc sử dụng tài nguyên địa chỉ IP.
* VPN:
  + Có ý nghĩa quan trọng trong việc bảo mật và kết nối từ xa. VPN tạo ra một kênh truyền dữ liệu an toàn qua mạng công cộng bằng cách mã hóa thông tin, đảm bảo dữ liệu không bị truy cập trái phép. Điều này đặc biệt hữu ích cho các doanh nghiệp có nhân viên làm việc từ xa hoặc cần kết nối giữa các chi nhánh, giúp họ truy cập tài nguyên nội bộ một cách an toàn. Ngoài ra, VPN còn hỗ trợ bảo vệ quyền riêng tư, tăng tính bảo mật và tối ưu hóa hiệu quả kết nối mạng.

# Kết luận:

## **5.1 Đánh giá hiệu suất và tính khả thi:**

Sau quá trình nghiên cứu, phân tích yêu cầu và thiết kế hệ thống mạng cho công ty FastPay, nhóm nhận thấy mô hình đề xuất có những ưu điểm nổi bật:

* **Hiệu suất cao & độ trễ thấp**: Phân chia VLAN hợp lý cho các phòng ban tại trụ sở chính (Kế toán, Quản lý rủi ro, IT) giúp tối ưu lưu lượng mạng nội bộ và hạn chế broadcast. Kết nối VPN Site-to-Site giữa trụ sở chính và chi nhánh được cấu hình ổn định, mã hóa mạnh (IPSec), đảm bảo kết nối an toàn và ít độ trễ khi truy cập dữ liệu từ xa.
* **Bảo mật chặt chẽ**: Áp dụng mô hình **Zero Trust Security** giúp kiểm soát chặt truy cập nội bộ, chỉ cho phép quyền truy cập tối thiểu cần thiết. Tích hợp các công nghệ bảo mật hiện đại như **IDS/IPS**, **Firewall Layer 7**, **SIEM** giúp phát hiện và ngăn chặn sớm các mối đe dọa tiềm ẩn.
  + Wi-Fi nội bộ và Wi-Fi khách được tách biệt hoàn toàn (Captive Portal), tránh nguy cơ rò rỉ thông tin.
* **Khả năng mở rộng linh hoạt:** Hệ thống sẵn sàng tích hợp hạ tầng Hybrid Cloud (AWS/GCP), thuận tiện mở rộng dịch vụ trực tuyến hoặc nâng cấp hạ tầng khi có nhu cầu. Các chi nhánh có thể dễ dàng kết nối bổ sung vào hệ thống qua VPN mà không cần thay đổi kiến trúc lõi..

## **5.2 Hướng phát triển tương lai:**

Để hệ thống mạng tiếp tục đáp ứng tốt sự phát triển không ngừng của FastPay, nhóm đề xuất một số hướng nâng cấp như sau:

* **Triển khai giám sát tập trung**: Sử dụng công cụ mã nguồn mở như **Zabbix** hoặc **Prometheus, Grafana** để giám sát toàn bộ hạ tầng (kết nối VPN, thiết bị mạng, hiệu suất dịch vụ), giúp phát hiện sự cố kịp thời và chủ động xử lý.
* **Tăng cường bảo mật tầng ứng dụng**: Tích hợp thêm **Web Application Firewall (WAF)** cho các dịch vụ thanh toán trực tuyến, kết hợp giải pháp **Multi-Factor Authentication (MFA)** để bảo vệ tài khoản quản trị quan trọng.
* **Nghiên cứu áp dụng SD-WAN**: Giải pháp này giúp tối ưu kết nối giữa các chi nhánh, tự động cân bằng tải đường truyền, giảm chi phí thuê kênh riêng (MPLS) trong dài hạn.
* **Tự động hóa triển khai hạ tầng (IaC)**: Ứng dụng **Terraform** hoặc **Ansible** để quản lý và triển khai hạ tầng một cách nhanh chóng, chính xác và nhất quán khi có nhu cầu mở rộng.

# Tài liệu tham khảo:

* [1] Cisco Systems, Inc., "Enterprise Campus 3.0 Architecture: Overview and Framework," Cisco Design Guide, 2020. [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html>
* [2] Cấu hình ACL: <https://www.youtube.com/watch?v=BXOJS3cJ3_A&t=197s>
* [3] GRE – VPN Tunnel: <https://www.youtube.com/watch?v=y_6eTs4rkvs&t=902s>
* [4] HSRP: <https://securityzone.vn/t/lab-13-cau-hinh-hsrp-cisco.182/>