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.P11

Thành viên trong nhóm:

22521340 – Phạm Hữu Thắng

22521328 – Lương Cao Thắng

22520071 – Phan Xuân Tuấn Anh

NĂM HỌC : 2024 – 2025

MỤC LỤC

1. Giới thiệu tổng quan:

Báo cáo này nhằm mục đích trình bày kế hoạch thiết kế hệ thống mạng cho Công ty tài chính FastPay có trụ sở chính tại Quận 1, TP.HCM và 2 chi nhánh tại Hà Nội và Đà Nẵng. Công ty cung cấp dịch vụ thanh toán trực tuyến, yêu cầu bảo mật cao, độ trễ thấp và khả năng mở rộng linh hoạt . Thiết kế mạng là một yếu tố quan trọng trong việc đảm bảo sự hoạt động hiệu quả của một tổ chức. Một hệ thống mạng tốt không chỉ giúp tăng cường giao tiếp giữa các phòng ban mà còn bảo vệ thông tin nhạy cảm và tối ưu hóa hiệu suất làm việc. Đồ án sẽ phân tích nhu cầu của công ty, xác định các thiết bị và công nghệ cần thiết, đồng thời đề xuất giải pháp mạng tối ưu.

2. Các thông tin cơ bản về đề tài:

2.1 Yêu cầu của khách hàng:

Trụ sở chính:

- Mạng nội bộ tách biệt: Nhóm Kế toán, Quản lý rủi ro, IT có VLAN riêng để đảm bảo an toàn dữ liệu.
- Bảo mật cao: Cấu hình Zero Trust Security, IDS/IPS, SIEM, Firewall Layer 7.
- Triển khai Hybrid Cloud: Sử dụng AWS/GCP để chạy hệ thống giao dịch trực tuyến.
- Wi-Fi công ty + Wi-Fi khách (tách biệt, sử dụng Captive Portal).
- Chi nhánh Hà Nội & Đà Nẵng:
- VPN Site-to-Site kết nối với Data Center tại trụ sở chính.
- Giám sát hiệu suất mạng bằng công cụ quản trị mạng (Công cụ mã nguồn mở) Sản phẩm đầu ra sơ đồ mạng logic & vật lý, sơ đồ VLAN, chi tiết các thiết bị mạng.
- Chính sách bảo mật chi tiết, giải pháp chống tấn công mạng.
- Kế hoạch triển khai theo PDIOO, kèm đánh giá hiệu suất.

2.2 Phân chia mạng thành các VLAN:

- Tại Trụ sở Chính:
  - VLAN 10: kế toán : Nhóm quản lý tài chính công ty
  - VLAN 20: RiskManagement: Nhóm quản lý rủi ro kiểm thử, đảm bảo chất lượng sản phẩm trước khi ra mắt.
  - VLAN 30: IT : Nhóm phát triển phần mềm, chịu trách nhiệm thiết kế và lập trình ứng dụng.
  - VLAN 40: Wifi-Guest : nhóm khách hàng
  - VLAN 50: Wifi-company: Quản lý mạng nội bộ công ty.
  - VLAN 60: Managenment : Quản lý công nghệ thông tin, giám sát hoạt động của hệ thống mạng.
- Tại Chi nhánh (Hà Nội và Đà Nẵng):
  - VLAN 10: kế toán : Nhóm quản lý tài chính công ty
  - VLAN 30: IT : Nhóm phát triển phần mềm, chịu trách nhiệm thiết kế và lập trình ứng dụng.
  - VLAN 40: Wifi-Guest : nhóm khách hàng
  - VLAN 50: Wifi-company: Quản lý mạng nội bộ công ty.

- Việc phân chia này không chỉ giúp quản lý lưu lượng mạng hiệu quả hơn mà còn tăng cường bảo mật, ngăn chặn việc truy cập trái phép giữa các phòng ban khác nhau.

2.3 Định tuyến giữa các VLAN (Inter-VLAN Routing):

- Mỗi VLAN cần có một gateway để định tuyến lưu lượng mạng giữa các VLAN. Việc cấu hình Inter-VLAN Routing có thể được thực hiện trên Switch Layer 3 hoặc Router. Điều này cho phép các VLAN giao tiếp với nhau một cách hiệu quả, đồng thời đảm bảo rằng lưu lượng mạng được quản lý tốt.
- Cấu hình Gateway: Mỗi VLAN sẽ có một địa chỉ IP riêng làm gateway, giúp định tuyến lưu lượng giữa các VLAN khác nhau.
- Thiết lập Routing Protocol: Sử dụng giao thức định tuyến OSPF để đảm bảo rằng các thông tin định tuyến được cập nhật kịp thời.

2.4 Kết nối VPN giữa Trụ sở Chính và Chi nhánh:

- Do Trụ sở Chính và Chi nhánh nằm ở hai vị trí địa lý khác nhau, việc thiết lập một VPN site-to-site sử dụng giao thức GRE làm nền tảng là rất quan trọng để tạo một đường hầm kết nối an toàn và hiệu quả qua Internet.
- Cấu hình GRE VPN giữa hai router tại mỗi địa điểm, đảm bảo truyền tải dữ liệu qua đường hầm GRE một cách đáng tin cậy. Có thể tích hợp với giao thức mã hóa như IPsec để bảo vệ dữ liệu khỏi các rủi ro an ninh mạng.
- Kiểm tra kết nối: Thực hiện các bài kiểm tra như ping, traceroute, và kiểm tra thông lượng để đảm bảo rằng kết nối GRE VPN hoạt động ổn định, đạt hiệu suất mong muốn và bảo mật tối đa.

2.5 Tính sẵn sàng cao với HSRP:

- Để đảm bảo tính khả dụng cao cho mạng, HSRP (Hot Standby Router Protocol) sẽ được sử dụng để tạo ra một gateway ảo cho các VLAN.
- Cấu hình HSRP: Thiết lập HSRP trên các router để tạo ra một IP ảo mà tất cả các VLAN sẽ sử dụng. Nếu router chính gặp sự cố, router dự phòng sẽ tự động thay thế mà không làm gián đoạn dịch vụ.
- Giám sát trạng thái: Theo dõi trạng thái của các router để phát hiện sớm các vấn đề và khắc phục kịp thời.

2.6 Phân bổ địa chỉ IP cho các thiết bị:

- Việc phân bổ địa chỉ IP cho các thiết bị trong các VLAN là rất quan trọng để đảm bảo rằng mọi thiết bị đều có thể kết nối và giao tiếp với nhau.
- Sử dụng địa chỉ IP riêng: Mỗi VLAN sẽ được cấp phát một dải địa chỉ IP riêng, giúp quản lý và phân loại thiết bị dễ dàng hơn.
- Cấu hình DHCP: Thiết lập DHCP server để tự động cấp phát địa chỉ IP cho các thiết bị người dùng trong các VLAN, đảm bảo rằng không có sự xung đột địa chỉ IP.

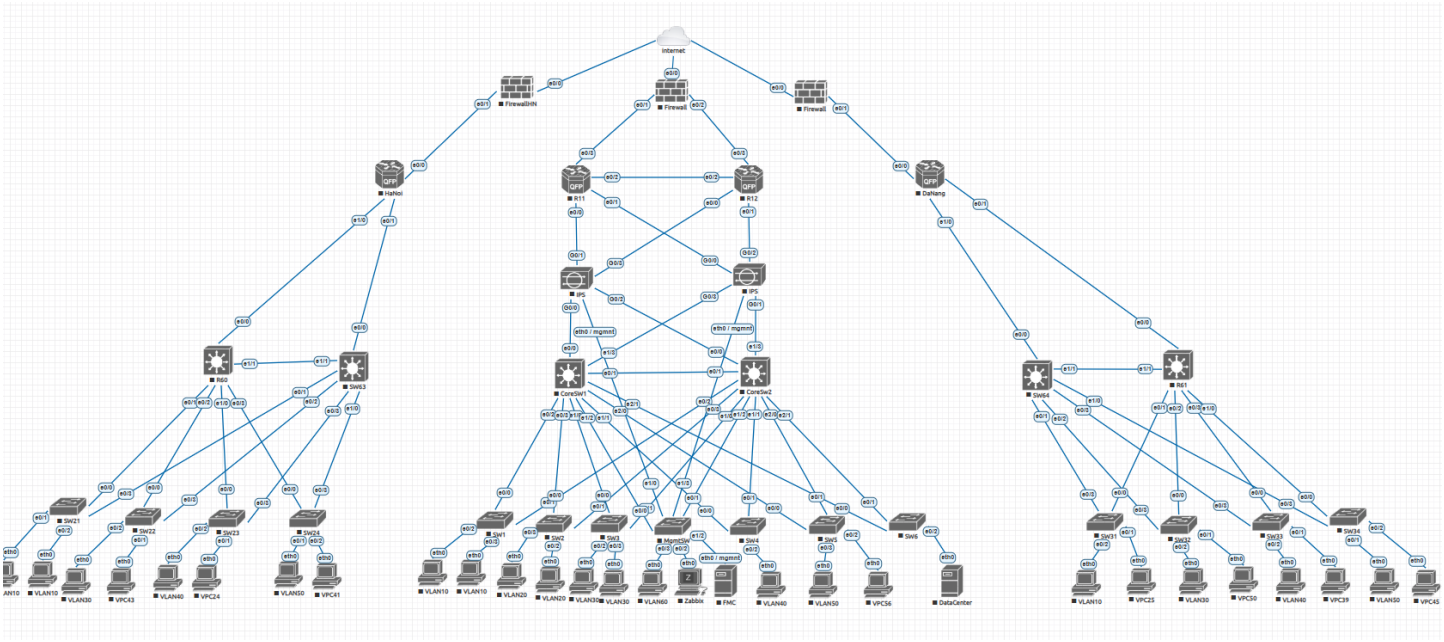
2.7 Quản lý mạng:

- Để duy trì an ninh và hiệu suất của mạng, việc quản lý và giám sát là rất cần thiết.

- Triển khai ACL (Access Control Lists): Sử dụng ACL để hạn chế truy cập giữa các VLAN không cần thiết, bảo vệ thông tin nhạy cảm và ngăn chặn các mối đe dọa từ bên ngoài.

3.Thiết kế hệ thống mạng:

3.1 Thiết kế mô hình mạng logic:



Mô hình mạng Top-Down gồm ba tầng: Core Layer, Distribution Layer, và Access Layer được lựa chọn trong thiết kế mạng nhờ tính cấu trúc chặt chẽ, khả năng mở rộng linh hoạt và hiệu quả trong quản lý.

- Khả năng mở rộng: Mô hình 3 lớp giúp mở rộng mạng một cách dễ dàng và có thể đáp ứng được nhu cầu gia tăng của người dùng hoặc dịch vụ.
- Hiệu suất tối ưu: Chia mạng thành các lớp giúp tối ưu hóa hiệu suất, giảm độ trễ và tải lên từng lớp.
- Quản lý và bảo mật dễ dàng: Việc phân tách các chức năng giúp dễ dàng áp dụng các chính sách bảo mật và quản lý mạng một cách tập trung và hiệu quả.
- Tính khả dụng cao: Sự phân tách giữa các lớp giúp tăng tính dự phòng và giảm thiểu sự cố hệ thống, cải thiện tính ổn định của mạng.
- Tối ưu hóa chi phí: Việc chia nhỏ các chức năng và phân phối lưu lượng giúp tối ưu hóa tài nguyên, giảm thiểu chi phí triển khai và duy trì mạng.

3.2 Thiết kế sơ đồ của toàn bộ hệ thống mạng:

3.2.1 Các thiết bị dùng trong hệ thống mạng:

- Router là thiết bị mạng đảm nhiệm vai trò định tuyến dữ liệu giữa các mạng khác nhau, ví dụ như giữa mạng LAN và WAN, hoặc giữa các mạng con trong một mạng nội bộ.
- Switch Layer 3 kết hợp chức năng của switch và router, giúp chuyển tiếp dữ liệu giữa các VLAN khác nhau và cung cấp khả năng định tuyến nội bộ trong mạng.

- Switch Layer 2 hoạt động trong phạm vi cùng một mạng con (LAN), chịu trách nhiệm chuyển tiếp các gói tin dựa trên địa chỉ MAC của các thiết bị.
- Server là thiết bị cung cấp các dịch vụ như lưu trữ, chia sẻ tài nguyên và ứng dụng cho các máy khách trong mạng, có thể là máy chủ web, email, hoặc cơ sở dữ liệu.
- Access Point (AP) là thiết bị mạng cho phép kết nối không dây giữa các thiết bị di động và mạng nội bộ, giúp mở rộng phạm vi và khả năng tiếp cận của mạng LAN không dây (Wi-Fi).

3.2.2 Các dịch vụ cần thuê:

Để đảm bảo rằng hệ thống mạng của Công ty tài chính hoạt động hiệu quả và đáp ứng được các yêu cầu giao dịch , công ty cần thuê một số dịch vụ thiết yếu. Các dịch vụ này không chỉ giúp tối ưu hóa hiệu suất mạng mà còn đảm bảo an toàn và bảo mật cho thông tin. Dưới đây là các dịch vụ cụ thể mà công ty cần xem xét:

a) Dịch vụ Internet

- Công ty cần thuê một dịch vụ Internet với băng thông rộng và tốc độ cao để đảm bảo rằng tất cả các hoạt động trực tuyến diễn ra mượt mà và không bị gián đoạn. Dịch vụ Internet này sẽ phục vụ cho nhiều mục đích khác nhau, bao gồm:
- Truy cập thông tin: Nhân viên cần truy cập vào các nguồn tài nguyên trực tuyến, bao gồm các ứng dụng đám mây, hệ thống quản lý dự án và các công cụ giao tiếp.
- Giao tiếp nội bộ và ngoại bộ: Việc sử dụng email, video call và các ứng dụng nhắn tin yêu cầu một kết nối Internet ổn định và nhanh chóng.
- Chạy các ứng dụng và dịch vụ trực tuyến: Nhiều ứng dụng mà công ty sử dụng có thể yêu cầu kết nối Internet liên tục để hoạt động hiệu quả.
- Việc lựa chọn nhà cung cấp dịch vụ Internet cần được thực hiện cẩn thận, với các tiêu chí như tốc độ, độ tin cậy và khả năng hỗ trợ kỹ thuật.

b) Dịch vụ VPN

- Để bảo vệ thông tin nhạy cảm khi truyền tải giữa trụ sở chính và chi nhánh, công ty cần thiết lập một dịch vụ VPN (Virtual Private Network). Dịch vụ VPN sẽ cung cấp một kết nối an toàn và mã hóa dữ liệu, giúp ngăn chặn các mối đe dọa từ bên ngoài. Lợi ích của dịch vụ VPN bao gồm:
- Bảo mật thông tin: Dữ liệu được mã hóa khi truyền qua Internet, giúp bảo vệ thông tin quan trọng khỏi các cuộc tấn công và rò rỉ dữ liệu.
- Kết nối an toàn giữa các địa điểm: VPN cho phép nhân viên làm việc từ xa hoặc kết nối từ chi nhánh đến trụ sở chính một cách an toàn, đảm bảo rằng thông tin luôn được bảo vệ.
- Truy cập vào các tài nguyên nội bộ: Nhân viên có thể truy cập vào các ứng dụng và tài nguyên nội bộ của công ty từ xa, tạo điều kiện thuận lợi cho việc làm việc linh hoạt.

c) Dịch vụ bảo trì và hỗ trợ kỹ thuật

- Để đảm bảo rằng hệ thống mạng luôn hoạt động hiệu quả và liên tục, công ty cần thuê dịch vụ bảo trì và hỗ trợ kỹ thuật. Dịch vụ này sẽ bao gồm:
- Bảo trì định kỳ: Thực hiện các công việc bảo trì định kỳ như cập nhật phần mềm, kiểm tra thiết bị và tối ưu hóa cấu hình để đảm bảo rằng hệ thống luôn hoạt động ở hiệu suất tối ưu.

- Hỗ trợ kỹ thuật: Cung cấp hỗ trợ kỹ thuật khi có sự cố xảy ra, giúp nhân viên nhanh chóng khắc phục vấn đề và giảm thiểu thời gian chết của hệ thống.
- Dịch vụ bảo trì và hỗ trợ kỹ thuật không chỉ giúp duy trì hoạt động của hệ thống mà còn cung cấp sự yên tâm cho công ty rằng mọi vấn đề sẽ được giải quyết một cách nhanh chóng và hiệu quả.

d) Dịch vụ giám sát và bảo mật

- Để đảm bảo rằng hệ thống luôn an toàn và ổn định, công ty cần có các thiết bị và đội ngủ giám sát cũng như triển khai các hệ thống giám sát và bảo mật
- Giám sát: kiểm tra lưu lượng các gói tin giữa các thiết bị trong mô hình mạng để kịp thời phát hiện sai sót hay điểm bất thường trong hệ thống,với hiệu suất tối đa
- Bảo mật: triển khai các biện pháp phòng thủ tránh các đối tượng cố tình xâm nhập hoặc các cuộc tấn công bằng mã độc để đánh cắp thông tin công ty cũng như khách hàng, đảm bảo an toàn và bảo mật cho hệ thống mạng của công ty

3.3 Địa chỉ IP của hệ thống mạng và thiết bị:

Đặt địa chỉ IP cho hệ thống mạng và thiết bị

Device	Interface	IP Address	Subnet Mask	Default Gateway
CoreSW1	Ethernet0/0	172.16.1.6	255.255.255.0	N/A
CoreSW1	Ethernet1/3	172.16.3.2	255.255.255.0	N/A
CoreSW1	Vlan10	10.10.10.2	255.255.255.0	10.10.10.1
CoreSW1	Vlan20	10.10.20.2	255.255.255.0	10.10.20.1
CoreSW1	Vlan30	10.10.30.2	255.255.255.0	10.10.30.1
CoreSW1	Vlan40	10.10.40.2	255.255.255.0	10.10.40.1
CoreSW1	Vlan50	10.10.50.2	255.255.255.0	10.10.50.1
CoreSW1	Vlan60	192.168.5.2	255.255.255.0	192.168.5.254
CoreSW2	Ethernet0/0	172.16.1.5	255.255.255.0	N/A
CoreSW2	Ethernet1/3	172.16.2.4	255.255.255.0	N/A
CoreSW2	Vlan10	10.10.10.3	255.255.255.0	10.10.10.1
CoreSW2	Vlan20	10.10.20.3	255.255.255.0	10.10.20.1
CoreSW2	Vlan30	10.10.30.3	255.255.255.0	10.10.30.1
CoreSW2	Vlan40	10.10.40.3	255.255.255.0	10.10.40.1
CoreSW2	Vlan50	10.10.50.3	255.255.255.0	10.10.50.1
CoreSW2	Vlan60	192.168.5.3	255.255.255.0	192.168.5.1
Switch (MgmtSW)	Vlan60	192.168.5.5	255.255.255.0	192.168.5.254
EdgeRouter	Ethernet0/0	172.16.1.1	255.255.255.0	N/A
EdgeRouter	Ethernet0/1	172.16.2.1	255.255.255.0	N/A
EdgeRouter	Ethernet0/2	192.168.10.1	255.255.255.0	N/A
EdgeRouter	Ethernet0/3	192.168.2.2	255.255.255.0	N/A
EdgeRouter	NVI0	172.16.1.1	255.255.255.0	N/A
R26	Ethernet0/0	172.16.1.2	255.255.255.0	172.16.1.1

R26	Ethernet0/1	172.16.2.2	255.255.255.0	172.16.2.1
R26	Ethernet0/2	192.168.10.2	255.255.255.0	192.168.10.1
R26	Ethernet0/3	192.168.3.2	255.255.255.0	192.168.3.1
ISP	Ethernet0/0	192.168.4.1	255.255.255.0	N/A
ISP	Ethernet0/1	192.168.1.133	255.255.255.0	N/A
ISP	Ethernet0/2	192.168.7.1	255.255.255.0	N/A
ISP	Ethernet0/3	192.168.6.1	255.255.255.0	N/A
ISP	NVI0	192.168.4.1	255.255.255.0	N/A
R59	Ethernet0/0	192.168.18.2	255.255.255.0	N/A

- Trụ sở chi nhánh Hà Nội:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R60	Ethernet0/0	192.168.20.2	255.255.255.0	192.168.20.1
R60	Vlan10	10.30.10.1	255.255.255.0	10.30.10.254
R60	Vlan30	10.30.30.1	255.255.255.0	10.30.30.254
R60	Vlan40	10.30.40.1	255.255.255.0	10.30.40.254
R60	Vlan50	10.30.50.1	255.255.255.0	10.30.50.254
SW63	Ethernet0/0	192.168.25.2	255.255.255.0	192.168.25.1
SW63	Vlan10	10.30.10.3	255.255.255.0	10.30.10.254
SW63	Vlan30	10.30.30.2	255.255.255.0	10.30.30.254
SW63	Vlan40	10.30.40.3	255.255.255.0	10.30.40.254
SW63	Vlan50	10.30.50.3	255.255.255.0	10.30.50.254
QFF_HaNoi Router	Ethernet0/0	192.168.13.2	255.255.255.0	N/A
QFF_HaNoi Router	Ethernet0/1	10.10.200.1	255.255.255.0	N/A
QFF_HaNoi Router	Ethernet1/0	192.168.20.1	255.255.255.0	N/A

- Trụ sở chi nhánh Đà Nẵng:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R61	Ethernet0/0	192.168.21.2	255.255.255.0	192.168.21.1
R61	Vlan10	10.20.10.1	255.255.255.0	10.20.10.254
R61	Vlan30	10.20.30.1	255.255.255.0	10.20.30.254
R61	Vlan40	10.20.40.1	255.255.255.0	10.20.40.254
R61	Vlan50	10.20.50.1	255.255.255.0	10.20.50.254
SW64	Ethernet0/0	192.168.26.2	255.255.255.0	192.168.26.1
SW64	Vlan10	10.20.10.3	255.255.255.0	10.20.10.254
SW64	Vlan30	10.20.30.3	255.255.255.0	10.20.30.254
SW64	Vlan40	10.20.40.3	255.255.255.0	10.20.40.254
SW64	Vlan50	10.20.50.3	255.255.255.0	10.20.50.254
QFF_DaNang Router	Ethernet0/0	192.168.12.2	255.255.255.0	N/A

QFF_DaNang Router	Ethernet0/1	192.168.21.1	255.255.255.0	N/A

- Cấu hình HSRP ở hai chi nhánh Hà Nội và Đà Nẵng:

VLAN	Virtual IP	Ưu tiên SW63	Trạng thái SW63	Thiết bị Active
10	10.30.10.1	90	Active (local)	SW63
20	10.30.20.1	90	Active (local)	SW63
30	10.30.30.1	110 (P)	Active (local)	SW63
40	10.30.40.1	110 (P)	Active (local)	SW63
50	10.30.50.1	110 (P)	Active (local)	SW63

VLAN	Virtual IP	Ưu tiên SW64	Trạng thái SW64	Thiết bị Active
10	10.20.10.1	90	Active (local)	SW64
20	10.20.20.1	90	Active (local)	SW64
30	10.20.30.1	110 (P)	Active (local)	SW64
40	10.20.40.1	110 (P)	Active (local)	SW64
50	10.20.50.1	110 (P)	Active (local)	SW64

4. Các dịch vụ cung cấp và chi phí cho toàn bộ hệ thống:

4.1 Các dịch vụ cung cấp:

4.1.1 Cấu hình HSRP cho SWLayer 3:

Mô tả: HSRP (Hot Standby Router Protocol) đã được thiết lập thành công tại hai chi nhánh, với một router hoạt động ở chế độ "Active" và router còn lại ở chế độ "Standby". Khi router chính gặp sự cố, router dự phòng sẽ tự động đảm nhận vai trò của nó.

Lợi ích:

- Tính sẵn sàng cao: Giúp duy trì kết nối liên tục cho người dùng, giảm thiểu thời gian ngừng hoạt động.
- Quản lý đơn giản: Người dùng chỉ cần biết địa chỉ IP ảo của HSRP, không cần nhớ địa chỉ IP của từng router.
- Tăng cường bảo mật: Kiểm soát lưu lượng và giảm nguy cơ tấn công từ chối dịch vụ (DoS).

4.1.2 Thiết lập VPN Tunnel:

Mô tả: VPN tunnel đã được cấu hình bằng GRE (Generic Routing Encapsulation) để tạo kết nối giữa các chi nhánh và trụ sở chính, cho phép truyền dữ liệu giữa các mạng với giao thức đóng gói linh hoạt. GRE có thể kết hợp với giao thức mã hóa như IPsec để đảm bảo tính bảo mật và an toàn thông tin.

Lợi ích:

- Kết nối linh hoạt: Hỗ trợ nhiều giao thức truyền tải, cho phép các mạng sử dụng các hệ thống khác nhau kết nối dễ dàng.

- Giảm chi phí: Cung cấp giải pháp kết nối hiệu quả qua Internet mà không cần đầu tư nhiều vào hạ tầng riêng.

4.1.3 Phân chia VLAN:

Mô tả: Các VLAN (Virtual Local Area Network) đã được thiết lập cho từng phòng ban, cho phép tách biệt lưu lượng mạng theo chức năng và nhu cầu sử dụng. Mỗi VLAN được cấu hình với các chính sách bảo mật riêng biệt, đảm bảo rằng thông tin nhạy cảm không bị truy cập bởi các phòng ban không liên quan.

Lợi ích:

- Tăng cường bảo mật: Giảm thiểu nguy cơ rò rỉ thông tin giữa các phòng ban, giúp bảo vệ dữ liệu nhạy cảm.
- Quản lý lưu lượng hiệu quả: Giúp tối ưu hóa băng thông và giảm tắc nghẽn mạng bằng cách phân chia lưu lượng theo từng nhóm người dùng.
- Dễ dàng mở rộng: Khi có nhu cầu mở rộng, việc thêm VLAN mới sẽ dễ dàng hơn mà không làm ảnh hưởng đến cấu trúc mạng hiện tại.

4.1.4 Cấu hình Wireless Router:

Mô tả: Wireless router đã được triển khai tại các khu vực làm việc chung và phòng họp, cung cấp kết nối không dây cho nhân viên.

Lợi ích:

- Tiện lợi cho người dùng: Nhân viên có thể kết nối với mạng một cách dễ dàng và linh hoạt, tăng cường năng suất làm việc.
- Khả năng mở rộng: Dễ dàng mở rộng mạng không dây khi cần thiết, đáp ứng nhu cầu sử dụng ngày càng tăng.

4.1.5 Cấu hình DHCP:

Mô Tả: Cấu hình DHCP (Dynamic Host Configuration Protocol) cho phép tự động cấp phát địa chỉ IP và thông tin mạng cho các thiết bị trong mạng. Điều này giúp giảm thiểu công sức quản lý địa chỉ IP thủ công và đảm bảo không có xung đột địa chỉ.

Lợi ích:

- Tiết kiệm thời gian: Giảm thiểu thời gian cấu hình địa chỉ IP cho từng thiết bị.
- Giảm xung đột địa chỉ IP: Tự động cấp phát địa chỉ IP duy nhất cho mỗi thiết bị.
- Dễ dàng quản lý: Cung cấp giao diện quản lý trung tâm cho việc theo dõi và điều chỉnh cấu hình.

4.1.6 Cấu hình OSPF:

Mô Tả: OSPF (Open Shortest Path First) đã được cấu hình để quản lý định tuyến giữa các router trong mạng, giúp tối ưu hóa đường đi của dữ liệu. OSPF sử dụng thuật toán Dijkstra để tìm đường đi ngắn nhất và tự động cập nhật thông tin định tuyến khi có sự thay đổi trong mạng.

Lợi ích:

- Hiệu quả và nhanh chóng: OSPF cung cấp khả năng định tuyến nhanh và chính xác hơn, phù hợp với các mạng lớn và phức tạp.
- Tối ưu hóa lưu lượng mạng: Giảm độ trễ và tăng hiệu suất tổng thể bằng cách định tuyến dữ liệu qua các đường đi tối ưu.

- Khả năng mở rộng tốt: Phù hợp với mạng có quy mô từ trung bình đến lớn.
- Tự động cập nhật: Các router tự động trao đổi và cập nhật thông tin định tuyến mà không cần quản lý thủ công.

4.1.7 Xây dựng hệ thống mạng đầy đủ:

Mô Tả: Xây dựng một hệ thống mạng đầy đủ tối ưu bằng cách sử dụng các thiết bị cùng hang, tích hợp tất cả các thành phần mạng, bao gồm router, switchlayer3, sw , wireless router và server, đảm bảo chúng hoạt động cùng nhau một cách hiệu quả.

Lợi ích: Tất cả thiết bị hoạt động hài hòa, giảm thiểu xung đột và tối ưu hóa hiệu suất.

4.1.8 Cấu hình NAT để ra Internet:

Mô tả: Network Address Translation (NAT) đã được cấu hình giữa core router và isp, thực hiện chuyển đổi giữa địa chỉ IP nội bộ trong công ty và địa chỉ mạng công cộng.

Lợi ích :

- Bảo mật: Giấu địa chỉ IP nội bộ, ngăn chặn truy cập từ bên ngoài.
- Tiết kiệm IP: Cho phép nhiều thiết bị sử dụng chung một địa chỉ IP công cộng.
- Quản lý dễ dàng: Giảm thiểu yêu cầu thay đổi cấu trúc mạng khi kết nối Internet.
- Mở rộng linh hoạt: Dễ dàng mở rộng mạng mà không cần thêm địa chỉ IP công cộng.
- Tăng hiệu quả: Giúp tối ưu hóa việc sử dụng các địa chỉ IP công cộng.

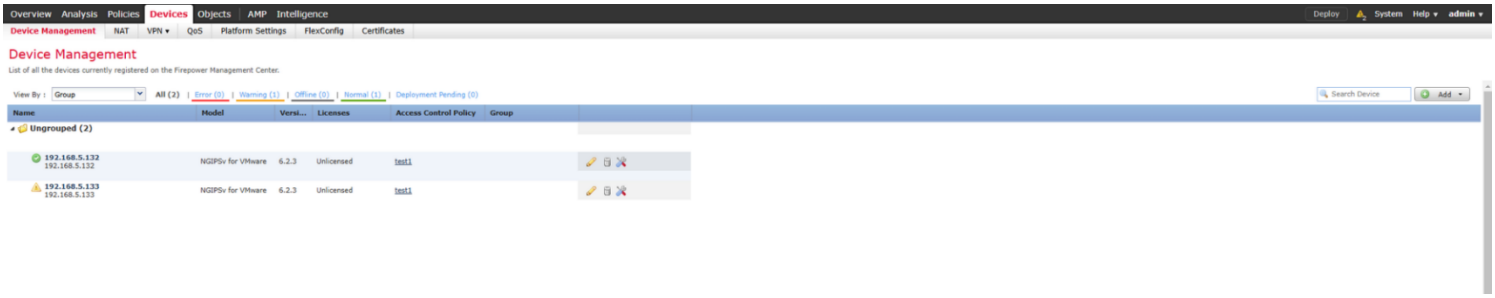
4.1.9 Cấu hình ACL:

Mô tả: ACL đã được cấu hình đã được cấu hình và áp dụng trên các interface vlan, mục đích là chỉ cho phép trao đổi nội bộ giữa các phòng ban với nhau, ngoài ra dev bên chi nhánh có thể giao tiếp tới dev bên trụ sở, tester bên chi nhánh cũng có thể giao tiếp với tester bên trụ sở. Tất cả developer và tester được truy cập đến hệ thông cloud và datacenter.

Lợi ích :

- Bảo mật: Hạn chế lưu lượng không cần thiết hạn chế truy cập trái phép.
- Hiệu quả mạng: Giảm thiểu xung đột lưu lượng không liên quan, tối ưu hóa tài nguyên mạng.
- Bảo vệ tài nguyên: Giới hạn quyền truy cập đến cloud và datacenter, chỉ cho phép các đối tượng đã xác định truy cập.

4.1.10 Quản lý thiết bị IDPS bằng FMC:



Thiết bị IDPS được quản lý tập trung bởi FMC (Firepower Management Center) thông qua giao diện eth0, bằng cách đăng ký FMC làm "manager" với lệnh show managers. Sau khi đăng ký thành công (Registration: Completed), FMC có thể cấu hình và cập nhật rule cho IDPS, bao gồm: thiết lập chính sách bảo mật (IPS, lọc ứng dụng, kiểm soát truy cập), cấu hình routing, NAT, VPN, và High Availability. Giao diện quản lý cần có kết nối IP đến FMC, đồng bộ thời gian (NTP) để đảm bảo đăng ký thành công và triển khai cấu hình chính xác.

4.2 Chi phí cho toàn hệ thống:

4.2.1 Chi phí cho thiết bị:

Loại thiết bị	Mẫu sản phẩm	Số lượng thiết bị	Đơn giá, ước tính	Số lượng và loại cổng giao tiếp	Mô tả, chức năng	Thành tiền
Core Switch	Cisco Catalyst 9500-48Y4C	6	400.000.000 đ	48x 25GE SFP28, 4x 100GE QSFP28	Core switch cao cấp, layer 3, hỗ trợ 100G, SD-Access	2.400.000.000 đ
Switch Phân Phối	Cisco Catalyst 9300X-48HX	15	300.000.000 đ	48x 10GE PoE (90W), 4x 25GE SFP28	Switch phân phối mạnh, multigigabit, 90W PoE, layer 3	4.500.000.000 đ
Server (cho VPC)	Dell PowerEdge R750	2	100,000,000 - 150,000,000	4x GE RJ45, 2x 10GE SFP+	Server mạnh mẽ, 2 CPU, 128GB RAM, chạy VPC và ứng dụng	200.000.000 đ
Router (QFP)	Cisco ASR 1002-HX	4	500.000.000	8x 10GE SFP+, 4x GE RJ45	Router hiệu suất cao, QFP tích hợp, 100Gbps throughput	2.000.000.000 đ
Firewall	FortiGate 200F	3	150.000.000 đ	16x GE RJ45, 8x GE SFP, 2x 10GE SFP+	Gateway bảo mật, firewall, VPN, IPS	450.000.000
Management Center	Cisco Firepower Management	1	300.000.000	4x GE RJ45, 2x 10GE SFP+	Trung tâm quản lý bảo mật, giám sát	300.000.000 đ

	Center (FMC) 1600				và cấu hình Firepower	
Tổng cộng					**9.850.000.000 đ**	

4.2.2 Chi phí cho dịch vụ:

STT	Dịch vụ	Đơn giá	Số lượng	Băng thông trong nước/ quốc tế	Thành tiền
1	Gói cước F300 PLUS	9.900.000 đ /tháng	1	600Mbps / 30Mbps	6.600.000 đ/tháng
2	Gói cước VIP200 Internet Viettel cho khách	800.000 đ/tháng	2	200Mbps/ 5Mbps	1.600.000 đ/tháng
3	Microsoft Azure Virtual Machines: Standard F4s_v2	2.500.000 đ/tháng	1	--	3.000.000 đ/tháng
Thành tiền					11.200.000 đ/tháng

5. Triển khai mô hình giám sát Zabbix:

- Cài đặt và cấu hình SNMP trên các thiết bị mạng
- Cấu hình SNMP Agent trên router và switch

+ Router:

```
net>enable
net#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
net(config)#snmp
net(config)#snmp-s
net(config)#snmp-server com
net(config)#snmp-server community public ro
net(config)#snmp-server community public rw
net(config)#snmp-se
net(config)#snmp-server host
net(config)#snmp-server host 192.168.2.6 ve
net(config)#snmp-server host 192.168.2.6 version 2c public
net(config)#
```

+ Switch 1 :

```
Switch(config)#snmp-server community public ro
Switch(config)#snmp-server community public rw
Switch(config)#snm
Switch(config)#snmp-
Switch(config)#snmp-server ho
Switch(config)#snmp-server host 192.168.2.6 ve
Switch(config)#snmp-server host 192.168.2.6 version 2c public
Switch(config)#
```

+ Tương tự cho switch 2:

- Cấu hình SNMP Trap để gửi cảnh báo

```
net(config)#snmp-server enable traps
net(config)#^Z
net#
Nov 10 07:20:42.207: %SYS-5-CONFIG_I: Configured from console by console
net#debug snmp packets
SNMP packet debugging is on
net#
```

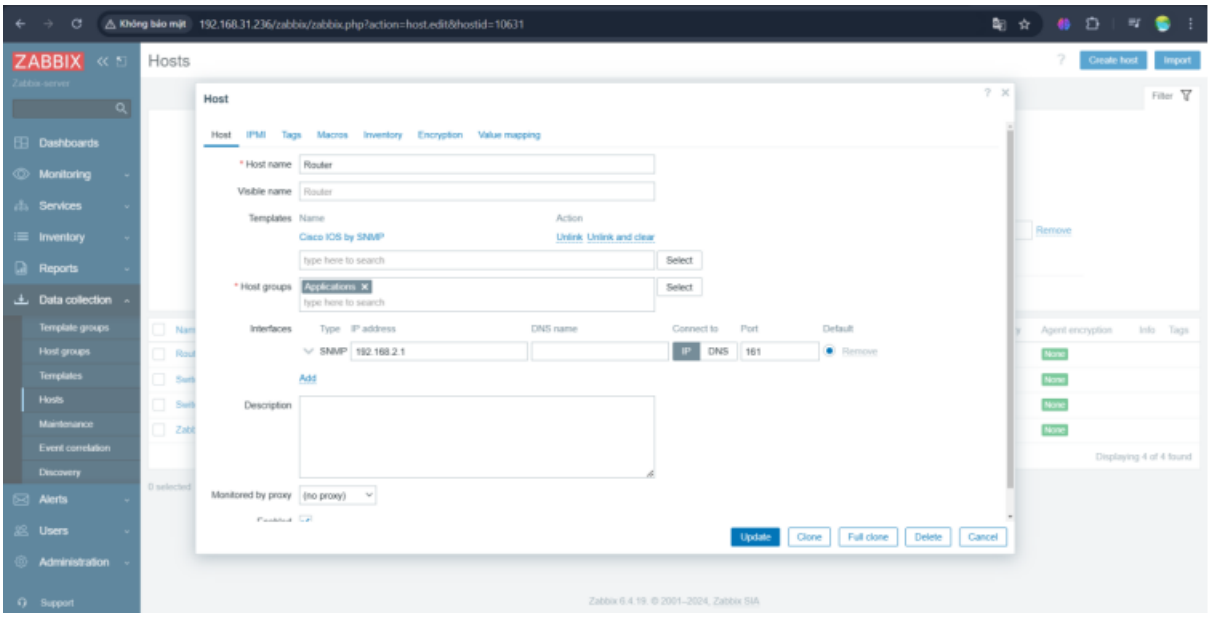
- Cấu hình Zabbix Server để nhận dữ liệu SNMP
- Cấu hình host trong Zabbix

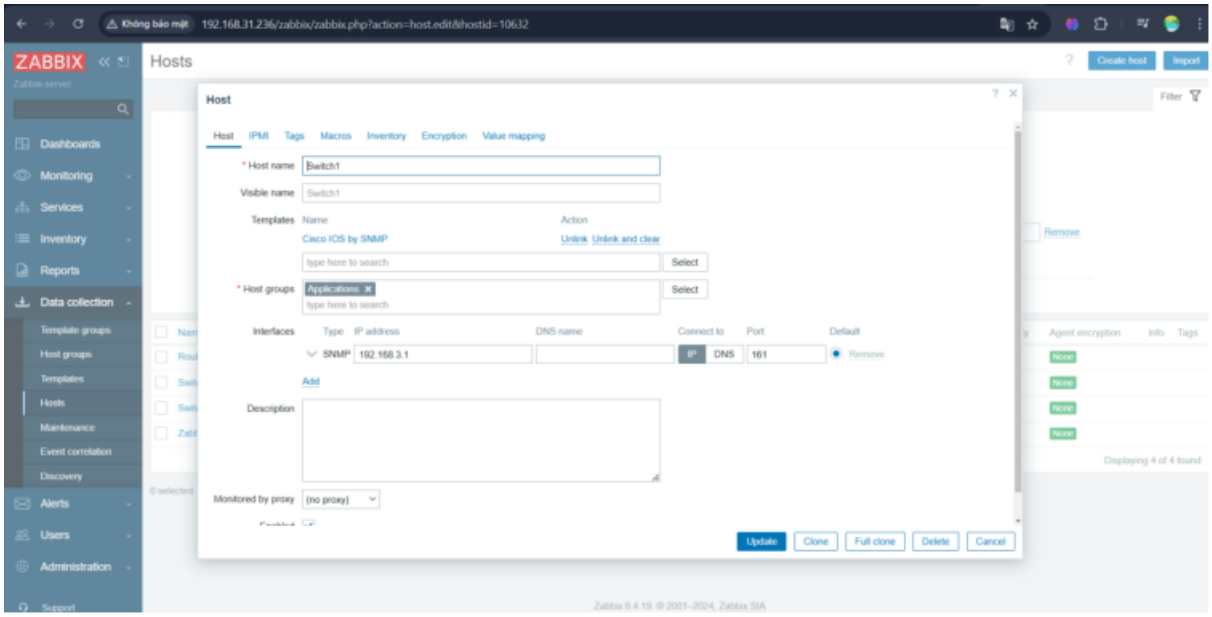
Bước 1: Thêm thiết bị mạng vào Zabbix

- Truy cập Zabbix Web Interface.
- Điều hướng đến mục Configuration > Hosts và chọn Create Host.
- Nhập tên của thiết bị, địa chỉ IP và chọn SNMP Interface để chỉ định giao thức SNMP.

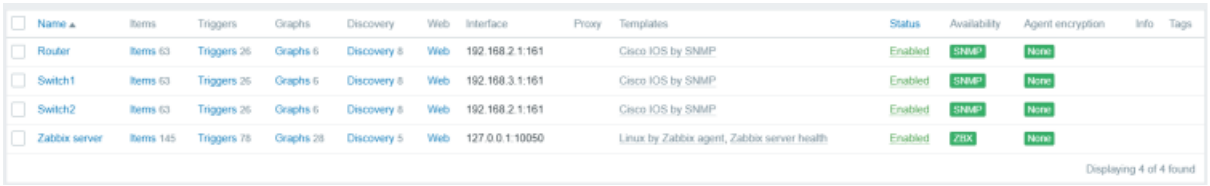
Bước 2: Thiết lập SNMP version và Community string

- Trong tab SNMP của host, chọn phiên bản SNMPv2
- Ở phần SNMP community ta ghi public





- Đợi khoảng tầm 2 phút thì các host sẽ được cập nhật Accept thành công như sau:



6. Kết luận:

Kết quả đạt được: Thiết kế hệ thống mạng cho công ty tài chính FastPay, đáp ứng các yêu cầu bảo mật cao, độ trễ thấp, và khả năng mở rộng linh hoạt. Hệ thống triển khai tại trụ sở chính (TP.HCM) và chi nhánh (Hà Nội, Đà Nẵng) với:

- Mạng nội bộ tách biệt: VLAN10 (Kế toán), VLAN20 (Quản lý rủi ro), VLAN30 (IT), VLAN40 (Data Center), VLAN50 (Wi-Fi) được cấu hình rõ ràng, đảm bảo an toàn dữ liệu.
- Bảo mật: Áp dụng Zero Trust Security, Firewall1, Firewall2 (Layer 7), IPS, và FMC (quản lý Firewall, IPS) để bảo vệ hệ thống trước mối đe dọa từ Internet, nội bộ, và chi nhánh.
- Kết nối: VPN Site-to-Site giữa chi nhánh và Data Center.

Hạn chế:

- Quản lý bảo mật hạn chế: FMC chỉ quản lý Firewall và IPS, không có chức năng SIEM đầy đủ để phân tích log toàn diện, dẫn đến khả năng bỏ sót các mối đe dọa phức tạp (như APT).
- Giám sát chi nhánh: Zabbix chưa tối ưu cho việc giám sát chi tiết tại chi nhánh, có thể chậm phát hiện sự cố từ xa.
- Hiệu suất Wi-Fi: Wi-Fi khách (VLAN50) chưa có cơ chế kiểm soát băng thông, dễ gây quá tải khi số lượng thiết bị tăng.

Phát triển trong tương lai:

- Nâng cấp FMC: Triển khai FMC với đầy đủ tính năng SIEM để phân tích log toàn mạng, tích hợp với Zabbix, và phát hiện mối đe dọa nâng cao.
- Tăng cường giám sát chi nhánh: Mở rộng Zabbix bằng cách thêm agent tại chi nhánh (Hà Nội, Đà Nẵng) để giám sát chi tiết hơn.
- Tối ưu Wi-Fi: Cấu hình QoS cho Wi-Fi khách (VLAN50) để kiểm soát băng thông, đảm bảo hiệu suất khi mở rộng số lượng người dùng.
- Tự động hóa bảo mật: Áp dụng AI/ML vào IPS để tự động phát hiện và phản ứng với các mối đe dọa.

Các nguồn tài liệu tham khảo:

[1] CNTT SHOP, "Hướng dẫn cấu hình GRE VPN Tunnel over IPSEC Trên Router Cisco," *YouTube*, Jan. 13, 2022. https://www.youtube.com/watch?v=qW0B5ueOPGw (accessed Dec. 01, 2024).
[2] Gurutech Networking Training, "CCNA DAY 49: Configure HSRP with Multiple VLANs | HSRP with Inter-VLAN Routing Configuration," *YouTube*, Jun. 21, 2023. https://www.youtube.com/watch?v=9-JY_On0-vY (accessed Jun. 02, 2024).
[3] "Tự thực hành Wireless miễn phí với Cisco Packet Tracer," *Quantrimang.com*, Dec. 09, 2011. https://quantrimang.com/cong-nghe/tu-thuc-hanh-wireless-mien-phi-84141
[4] "Configuring a LAN with DHCP and VLANs [Support]," *Cisco*. https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/dhcpvlan.htm
[5] cnttshop, "Lê Văn Tuấn," *Cnttshop.vn*, 2023. https://cnttshop.vn/blogs/cisco/huong-dan-cau-hinh-access-list-tren-cisco-voi-lab-cu-the (accessed Dec. 10, 2024).