**BÁO CÁO LAB CUỐI KỲ**

Môn: Mạng máy tính nâng cao

MSSV: 23162006 – Họ tên: Nguyễn Gia Bảo

MỤC LỤC

Mục lục

[1) Giới thiệu/Mô tả vấn đề của bài toán 1](#_Toc210601349)

[2) Topology 1](#_Toc210601350)

[3) Mục tiêu 2](#_Toc210601351)

[3.1) Mục tiêu Câu 1 2](#_Toc210601352)

[3.2) Mục tiêu Câu 2 3](#_Toc210601353)

[4) Kịch bản 3](#_Toc210601354)

[5) Thực hiện (Câu 1) 4](#_Toc210601355)

[5.1) Cấu hình cơ bản 4](#_Toc210601356)

[5.2) Cấu hình bảo mật 20](#_Toc210601357)

[5.3) VPN Site-to-Site (IPSec) 32](#_Toc210601358)

[6) Kiểm tra kết quả (Câu 1) 34](#_Toc210601359)

[7) Thực hiện (Câu 2) 41](#_Toc210601360)

[8) Kiểm tra kết quả (Câu 2) 46](#_Toc210601361)

[9) Kết luận/Phân tích 48](#_Toc210601362)

[9.1) Kết luận Câu 1 48](#_Toc210601363)

[9.2) Kết luận Câu 2 48](#_Toc210601364)

[10) Giải pháp 49](#_Toc210601365)

# 1) Giới thiệu/Mô tả vấn đề của bài toán

Trong hệ thống mạng doanh nghiệp, việc phân chia VLAN, triển khai các dịch vụ mạng, bảo mật và kết nối chi nhánh là nhu cầu quan trọng.

Hệ thống phải đáp ứng các yêu cầu:

+ Người dùng nội bộ có thể truy cập Internet.

+ Dịch vụ Web, Email công bố ra ngoài.

+ Các chi nhánh kết nối an toàn qua VPN.

+ Bảo mật hạ tầng với Port Security, ACL, DHCP Snooping, Firewall, Radius.

+ Đảm bảo hiệu suất với EtherChannel, cân bằng tải và DMZ.

# 2) Topology

Hệ thống được thiết kế với 2 site: HQ và Branch.

+ HQ: CoreSW, DistSW, AccessSW, Firewall, các server (Web, Email, DNS, DHCP, Radius).

+ Branch: CoreSW, DistSW, AccessSW, DHCP server.

+ DMZ: chứa Web Server, Email Server, App Server.

+ VPN Site-to-Site kết nối HQ và Branch.

+ Người dùng nội bộ truy cập Internet qua NAT Overload.

+ Người dùng ngoài Internet truy cập dịch vụ qua Static NAT.

A computer screen shot of a diagram

AI-generated content may be incorrect.

# 3) Mục tiêu

## 3.1) Mục tiêu Câu 1

Hệ thống mạng nội bộ và chi nhánh cần đạt được các mục tiêu sau:

Phân chia VLAN theo từng phòng ban để tách biệt lưu lượng.

Sử dụng VTP và Trunk để quản lý VLAN và truyền VLAN giữa các switch.

Cấu hình EtherChannel nhằm tăng băng thông và đảm bảo dự phòng đường truyền.

Cấu hình định tuyến động (RIPv2) để các mạng nội bộ liên lạc được với nhau.

NAT Overload cho phép toàn bộ người dùng nội bộ truy cập Internet.

Static NAT để công bố Web Server và Email Server ra ngoài Internet với IP public.

Thực hiện các cơ chế bảo mật: Hardening switch, Port Security, ACL, DHCP Snooping.

Cho phép truy cập thiết bị bằng SSH thay vì Telnet.

Kết nối HQ – Branch bằng VPN Site-to-Site để truyền dữ liệu an toàn.

## 3.2) Mục tiêu Câu 2

Thiết kế lại hệ thống để nâng cao bảo mật và tính chuyên nghiệp:

WiFi dành cho nhân viên và khách chỉ được phép ra Internet, không truy cập vào mạng nội bộ.

Khu vực quản trị được gom lại trong một mạng quản trị riêng, chỉ subnet này mới có thể SSH vào các thiết bị.

Bổ sung Database Server và Application Server để chạy các ứng dụng nội bộ, triển khai mô hình 3-tier (Web – App – DB).

DMZ được thiết kế thêm cơ chế bảo mật chặt chẽ và cân bằng tải cho Web/App Server, giúp tăng hiệu suất và độ tin cậy.

# 4) Kịch bản

Người dùng các VLAN nội bộ HQ/Branch truy cập Internet qua NAT Overload.

Người dùng ngoài Internet truy cập Web (4.4.4.4) và Email (5.5.5.5).

VPN HQ – Branch đảm bảo liên lạc bảo mật.

Port Security hạn chế thiết bị trái phép.

DHCP Snooping chống DHCP giả.

ACL giới hạn quyền truy cập theo phòng ban.

Firewall quản lý dịch vụ truy cập Internet.

WiFi HQ chứng thực Radius.

WiFi Guest chỉ được ra Internet, không vào mạng nội bộ.

Database và Application Server phục vụ ứng dụng nội bộ.

DMZ bảo mật và cân bằng tải dịch vụ công bố ra ngoài.

# 5) Thực hiện (Câu 1)

## 5.1) Cấu hình cơ bản

**Trên CoreSw:**

Thực hiện gán các port nối giữa DistSw và CoreSw vào chung 1 channel-group

A computer screen shot of a program

AI-generated content may be incorrect.

A screen shot of a computer code

AI-generated content may be incorrect.

Gán địa chỉ ip cho port nối tới ServerSw 🡪 default gateway

A close up of a computer screen

AI-generated content may be incorrect.

Cấu hình Ethernet từ CoreSw đến DistSw1 và DistSw2:

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Cấu hình địa chỉ IP cho port nối tới khu vực quản trị và ip helper-address đến địa chỉ DHCP Server để các thiết bị trong mạng có thể xin địa chỉ ip từ DHCP Server 🡪 default gateway

A computer screen shot of a program

AI-generated content may be incorrect.

Cấu hình địa chỉ IP cho port nối tới khu vực VP TNTT và ip helper-address đến địa chỉ DHCP Server để các thiết bị trong mạng có thể xin địa chỉ ip từ DHCP Server 🡪 default gateway

A screenshot of a computer program

AI-generated content may be incorrect.

Cấu hình địa chỉ IP cho port nối tới firewall

A black text on a white background

AI-generated content may be incorrect.

Định tuyến các mạng:

A screenshot of a computer program

AI-generated content may be incorrect.

* Định tuyến đến mạng 0.0.0.0 0.0.0.0 để khi gửi gói tin đến địa chỉ không biết gói tin sẽ gửi đến địa chỉ được chỉ, cấu hình định tuyến này giúp cho có thể gửi gói tin đến Branch

**Trên DistSw1:**

Khởi tạo các vlan tương ứng với các phòng ban thuộc building 2 sau đó gán địa chỉ ip cho từng port đó 🡪 Default gateway

A screenshot of a computer code

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Cấu hình ethernet từ DistSw1 đến CoreSw và các AccessSw: cho các port nối giữa CoreSW và DistSw1 vào chung 1 channel-group và gán địa chỉ cho port-channel đó

A screen shot of a computer

AI-generated content may be incorrect.

Sau đó gán các port nối giữa DistSw1 và AccessSw vào chung 1 channel-group mỗi AccessSw là 1 phòng ban nên sẽ gán VLAN khác nhau. Đồng thở chuyển port-channel sang mode trunk và cho phép VLAN đi qua

A screenshot of a computer program

AI-generated content may be incorrect.

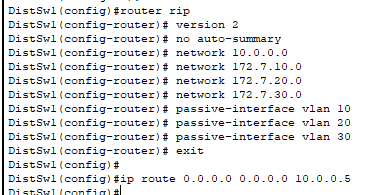
A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

Cấu hình định tuyến bằng phương thức RIPv2



* Sử dụng thêm passive-interface vlan 10/20/30 để vẫn quảng bá mạng vào trong bảng định tuyến RIP nhưng không gửi bản tin RIP ra các interface đó nữa.
* Định tuyến đến mạng 0.0.0.0 0.0.0.0 để khi gửi gói tin đến địa chỉ không biết gói tin sẽ gửi đến địa chỉ được chỉ, cấu hình định tuyến này giúp cho có thể gửi gói tin đến Branch

**Trên DistSw2:**

Khởi tạo các vlan tương ứng với các phòng ban thuộc building 2 sau đó gán địa chỉ ip cho từng port đó 🡪 Default gateway

A close up of text

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Cấu hình ethernet từ DistSw2 đến CoreSw và các AccessSw: cho các port nối giữa CoreSW và DistSw2 vào chung 1 channel-group và gán địa chỉ cho port-channel đó

A screenshot of a computer program

AI-generated content may be incorrect.

Tương tự, trên DistSw2 ta gán các port nối giữa DistSw2 và AccessSw vào chung 1 channel-group, mỗi AccessSw là 1 phòng ban nên sẽ gán từng port-channel vào VLAN khác nhau. Đồng thở mở chuyển port-channel sang mode trunk và cho phép VLAN đi qua

A screenshot of a computer program

AI-generated content may be incorrect.

Cấu hình định tuyến bằng phương thức RIPv2

A screenshot of a computer program

AI-generated content may be incorrect.

* Sử dụng thêm passive-interface vlan 10/20/30 để vẫn quảng bá mạng vào trong bảng định tuyến RIP nhưng không gửi bản tin RIP ra các interface đó nữa.
* Định tuyến đến mạng 0.0.0.0 0.0.0.0 để khi gửi gói tin đến địa chỉ không biết gói tin sẽ gửi đến địa chỉ được chỉ, cấu hình định tuyến này giúp cho có thể gửi gói tin đến Branch

**Trên AccessSw1:**

Khởi tạo Vlan 10 tương ứng với phòng ban 1 của building 2 và gán vlan 10 vào port kết nối với các PC-client:





Cấu hình ethernet: cho các port nối giữa CoreSW và DistSw2 vào chung 1 channel-group và cho phép vlan 10 đi qua

A screenshot of a computer program

AI-generated content may be incorrect.

🡪 Tương tự cấu hình trên các AccessSw khác

**Trên ServerSw:**

Khởi tạo vlan 100 và cấu hình các port nối tới DHCP Server và DNS Server chuyển sang mode access, và access tới vlan 100

A white background with black text

AI-generated content may be incorrect.

Sau đó gán địa chỉ ip cho vlan 100 🡪 default gateway



Cấu hình đặt địa chỉ ip cho port nối tới CoreSw

A black text on a white background

AI-generated content may be incorrect.

Cấu hình định tuyến bằng phương thức RIPv2

A screenshot of a computer program

AI-generated content may be incorrect.

* Sử dụng thêm passive-interface vlan 100 để vẫn quảng bá mạng vào trong bảng định tuyến RIP nhưng không gửi bản tin RIP ra các interface đó nữa.

**Trên DHCP Server**

Đặt địa chỉ ip cho Server

A screenshot of a computer

AI-generated content may be incorrect.

Bật dịch vụ DHCP lên và tạo các pool để cấp phát địa chỉ IP

A screenshot of a computer

AI-generated content may be incorrect.

**Trên DNS Server:**

Đặt địa chỉ ip cho DNS server:

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó bật dịch vụ DNS lên thêm các tên miền để server phân giải

A screenshot of a computer

AI-generated content may be incorrect.

**Trên Firewall:**

Gán địa chỉ IP cho các port nối đến các thiết bị:

A screenshot of a computer program

AI-generated content may be incorrect.

Thực hiện định tuyến bằng phương thức RIPv2

A computer code with numbers and symbols

AI-generated content may be incorrect.

**Trên Web\_Server:**

Đặt địa chỉ ip cho web server:

A screenshot of a computer

AI-generated content may be incorrect.

Bật dịch vụ HTTP:

A screenshot of a computer

AI-generated content may be incorrect.

**Trên Email Server**

Đặt địa chỉ ip cho Email Server

A screenshot of a computer

AI-generated content may be incorrect.

Bật dịch vụ email, set domain và add thêm user

A screenshot of a computer

AI-generated content may be incorrect.

**Trên CoreSw thuộc Branch:**

Gán địa chỉ ip cho các port nối đến các thiết bị 🡪 default gateway. Sau đó ip helper-address đến DHCP Server (Branch) để các thiết bị trong từng mạng có thể nhận cấp phát ip động

A screenshot of a computer

AI-generated content may be incorrect.

Cấu hình định tuyến bằng phương thức RIPv2

A computer code with black text

AI-generated content may be incorrect.

**Trên Firewall (Branch):**

Thực hiện cấu hình địa chỉ ip cho các port nối đến các thiết bị

A screenshot of a computer code

AI-generated content may be incorrect.

Thực hiện định tuyến bằng phương thức RIPv2

A screenshot of a computer code

AI-generated content may be incorrect.

**Trên Router HQ:**

Cấu hình địa chỉ ip cho các port nối đến các thiết bị🡪 default gateway. Đồng thời cấu hình cổng nat inside và outside

A screenshot of a computer program

AI-generated content may be incorrect.

Cấu hình Static NAT, với IP public cho Web server là 4.4.4.4 và Email Server là 5.5.5.5



Cấu hình PAT cho phép người dùng bên trong ra ngoài Internet

A screenshot of a computer code

AI-generated content may be incorrect.

**Trên Router BR (Branch):**

Cấu hình địa chỉ ip cho các port nối đến các thiết bị🡪 default gateway. Đồng thời cấu hình cổng nat inside và outside

A screenshot of a computer code

AI-generated content may be incorrect.

Cấu hình định tuyến bằng phương thức RIPv2

A close up of a white background

AI-generated content may be incorrect.

Cấu hình PAT cho phép người dùng bên trong ra ngoài Internet

A white background with black text

AI-generated content may be incorrect.

**Trên ISP Router:**

Cấu hình địa chỉ ip trên các port nối tới các thiết bị

A screenshot of a computer program

AI-generated content may be incorrect.

Thực hiện định tuyến bằng phương thức RIPv2 và static routing đến WebServer, EmailServer, và 2 mạng bên trong local

A screenshot of a computer program

AI-generated content may be incorrect.

## 5.2) Cấu hình bảo mật

**Trên CoreSw:**

Bật dịch vụ ssh và cấu hình ACL chỉ cho phép các thiết bị thuộc khu vực quản trị mới có thể truy cập từ xa đến thiết bị

A group of black text

AI-generated content may be incorrect.

A white screen with black text

AI-generated content may be incorrect.

Cấu hình ACL để chặn các truy cập từ phòng ban thuộc VLAN 10 đến khu vực quản trị

A close-up of a computer code

AI-generated content may be incorrect.

**Trên DistSw1:**

Bật dịch vụ ssh và cấu hình ACL chỉ cho phép các thiết bị thuộc khu vực quản trị mới có thể truy cập từ xa đến thiết bị

A white background with black text

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

**Trên AccessSw1:**

Cấu hình Hardening: shutdown tất cả các port, chỉ bật các port khi sử dụng



Bật dịch vụ ssh và cấu hình ACL chỉ cho phép các thiết bị thuộc khu vực quản trị mới có thể truy cập từ xa đến thiết bị

**A screenshot of a computer code

AI-generated content may be incorrect.**

Cấu hình port-security để Sw chỉ nhận 1 địa chỉ MAC của 1 thiết bị nối vào trên các cổng, nếu thay thiết bị khác vào thì sẽ shutdown

A screen shot of a computer

AI-generated content may be incorrect.

A close up of a white background

AI-generated content may be incorrect.

Trên Server Switch:

Cấu hình DHCP Snooping để tránh DHCP giả cung cấp ip cho người dùng trong mạng

A black text on a white background

AI-generated content may be incorrect.

Trên các Switch: Cấu hình DHCP Snooping để tránh DHCP giả cung cấp ip cho người dùng trong mạng

A black text on a white background

AI-generated content may be incorrect.

A black text on a white background

AI-generated content may be incorrect.

A close up of text

AI-generated content may be incorrect.

A black text on a white background

AI-generated content may be incorrect.

🡪 Tương tự trên các Switch khác

**Trên Firewall:**

Cấu hình ACL để các máy ở VLAN20 chỉ được truy cập ra ngoài bằng dịch vụ PING và dịch vụ FTP còn các máy tính khác trong mạng truy cập được tất cả các dịch vụ bên ngoài Internet

A screenshot of a computer code

AI-generated content may be incorrect.

**Mạng Wifi:**

Thêm radius server ở khu vực quản trị

A computer network diagram with a computer and a computer server

AI-generated content may be incorrect.

Đặt địa chỉ IP cho Radius Server

A screenshot of a computer

AI-generated content may be incorrect.

Bật dịch vụ AAA và thêm tài khoản và cấu hình

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó trên Wireless Router ở building 3: Cấu hình cho Wireless Router:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Trên PC client: thay module WMP300N vào để có thể kết nối không dây

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Vào PC Wireless:

A screenshot of a computer

AI-generated content may be incorrect.

Chọn profile 🡪 tạo mới (New)

A screenshot of a computer

AI-generated content may be incorrect.

Đặt tên profile

A screenshot of a computer

AI-generated content may be incorrect.

Nhập SSID của wireless:

A screenshot of a computer

AI-generated content may be incorrect.

Nhấn next:

A screenshot of a computer

AI-generated content may be incorrect.

Chọn WPA2-Enterprise mới có thể dùng mạng wifi được tạo trên radius

A screenshot of a computer security message

AI-generated content may be incorrect.

Nhập username và pass đã tạo ở radius server

A screen shot of a computer security

AI-generated content may be incorrect.

Hoàn tất nhấn save:

A screenshot of a computer

AI-generated content may be incorrect.

Nhấn vào profile vừa tạo và ấn connect:

A screenshot of a computer

AI-generated content may be incorrect.

Kết nối thành công:

A screenshot of a computer

AI-generated content may be incorrect.

A computer network diagram with a router

AI-generated content may be incorrect.

## 5.3) VPN Site-to-Site (IPSec)

**Trên Router HQ:** tiến hành cấu hình VPN Site to site

A screenshot of a computer program

AI-generated content may be incorrect.

Trên Router BR (Branch): cấu hình vpn site to site

A screenshot of a computer program

AI-generated content may be incorrect.

# 6) Kiểm tra kết quả (Câu 1)

Ping giữa các VLAN trong HQ và Branch.

Ping từ PC ở HQ thuộc Vlan 10:

A computer screen shot of a computer

AI-generated content may be incorrect.

Ping từ PC ở Branch thuộc vlan 10:

A computer screen shot of a computer program

AI-generated content may be incorrect.

Ping HQ ↔ Branch qua VPN (kiểm tra encapsulation/decapsulation): Kiểm tra bằng lệnh

**show crypto isakmp sa**

A black text on a white background

AI-generated content may be incorrect.

**show crypto ipsec sa**

A close up of a computer code

AI-generated content may be incorrect.

A screen shot of a computer code

AI-generated content may be incorrect.

* pkts encaps (gói tin đã được mã hóa gửi đi)
* pkts decaps (gói tin nhận được và giải mã thành công)
* 2 con số này tăng khi bạn ping giữa 2 LAN 🡪 VPN hoạt động

Ping từ PC nội bộ ra Internet (NAT Overload).

A computer screen shot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

Truy cập Web/Email Server từ Internet.

A computer screen shot of a black screen

AI-generated content may be incorrect.

Kiểm tra Port Security bằng cách cắm thiết bị lạ.

A diagram of a computer network

AI-generated content may be incorrect.

SSH chỉ cho phép từ VLAN quản trị.

* Thử ssh từ PC thuộc vlan

A computer screen shot of a computer

AI-generated content may be incorrect.

* Bị chặn
* Thử ssh từ admin

A computer screen shot of a black screen

AI-generated content may be incorrect.

* Thành công

VLAN20 chỉ ra ngoài bằng Ping/FTP.

Thử ping ra ngoài

A screenshot of a computer program

AI-generated content may be incorrect.

Thử tìm kiếm tới địa chỉ web server ngoài mạng trên web browser

A screenshot of a computer program

AI-generated content may be incorrect.

Ping được

A screenshot of a computer

AI-generated content may be incorrect.

Nhưng không tìm kiếm trang web được

WiFi HQ kết nối thành công khi chứng thực Radius.

A diagram of a router

AI-generated content may be incorrect.

# 7) Thực hiện (Câu 2)

WiFi tách biệt: VLAN riêng cho WiFi Guest/Staff, ACL/Firewall chỉ cho ra Internet, chặn toàn bộ vào mạng nội bộ.

Sử dụng WirelessRouter để triển khai wifi cho toàn bộ hệ thống (cả nhân viên và khách)

Trên CoreSw cấu hình địa chỉ ip cho port nối đến 2 WirelessRouter (Nhân viên và khác hàng) và đồng thời ip helper-address đến địa chỉ DHCP Server

A white background with black text

AI-generated content may be incorrect.

A black text on a white background

AI-generated content may be incorrect.

A white screen with black text

AI-generated content may be incorrect.

Trên Wireless Router Staff:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Tắt DHCP để lấy trực tiếp từ DHCP Server ở khu vực Internal Server

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

Trên Wireless Router Guest:

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

Trên máy laptop sẽ hiển thị:

A screenshot of a computer

AI-generated content may be incorrect.

Connect và nhập mật khẩu của mạng Staff hoặc Guest

Trên DHCP Server tạo 2 pool mới để cấp IP cho mạng Staff và Guest

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó trên các Laptop đã kết nối tới mạng Staff và Guest thử xin địa chỉ IP DHCP cấp

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Trên CoreSw tạo ACL để chỉ cho phép Wifi đi thẳng ra Internet chứ không truy cập hệ thống nội bộ được

A white background with black text

AI-generated content may be incorrect.

Bảo mật DMZ

* NAT tĩnh public ↔ private cho Web/DNS.
* ACL/Zone-Based Firewall trên biên: chỉ cho TCP 80/443 tới Web, UDP/TCP 53 tới DNS; deny mọi chiều DMZ→Inside (chỉ cho phép log/backup cần thiết)

A screen shot of a computer code

AI-generated content may be incorrect.



# 8) Kiểm tra kết quả (Câu 2)

WiFi Guest ra được Internet, không truy cập mạng nội bộ.

A computer screen shot of a computer program

AI-generated content may be incorrect.

WiFi Staff xác thực Radius thành công, chỉ ra Internet.

A screenshot of a computer program

AI-generated content may be incorrect.

# 9) Kết luận/Phân tích

## 9.1) Kết luận Câu 1

Sau khi cấu hình và kiểm tra, hệ thống ở Câu 1 đã đảm bảo:

* VLAN phân tách lưu lượng rõ ràng, tăng tính bảo mật.
* EtherChannel giúp tăng băng thông và dự phòng đường truyền.
* NAT Overload cho phép người dùng nội bộ truy cập Internet, trong khi Static NAT công bố Web/Email server ra ngoài ổn định.
* ACL, Port Security, DHCP Snooping ngăn chặn được các truy cập trái phép và DHCP giả.
* Firewall kiểm soát dịch vụ truy cập chi tiết.
* VPN Site-to-Site giúp HQ và Branch liên lạc an toàn, đảm bảo tính riêng tư dữ liệu.

## 9.2) Kết luận Câu 2

Sau khi thiết kế lại hệ thống theo yêu cầu mới, ta có:

* WiFi được tách biệt hoàn toàn với mạng nội bộ, giảm nguy cơ truy cập trái phép từ bên ngoài.
* Khu vực quản trị tập trung trong một subnet riêng, dễ dàng kiểm soát và bảo vệ thiết bị mạng.
* Database và Application Server được bổ sung, triển khai theo mô hình 3-tier, đảm bảo an toàn dữ liệu và dễ dàng mở rộng ứng dụng.
* DMZ được củng cố với giải pháp bảo mật và cân bằng tải, đảm bảo dịch vụ Web/App hoạt động ổn định, có khả năng chịu tải cao và dự phòng khi một server gặp sự cố.

# 10) Giải pháp

Bổ sung HSRP/VRRP dự phòng gateway.

Tích hợp IDS/IPS để phát hiện và ngăn chặn tấn công.

Sử dụng AAA (Radius/TACACS+) quản lý người dùng tập trung.

Mở rộng VPN sang MPLS nếu nhiều chi nhánh.