TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

DIỆP TRƯƠNG KHÁNH BĂNG - 52200238

NGUYỄN NGỌC QUỲNH NHƯ - 52200281

NGUYỄN TẤN ĐẠT - 52200285

LÊ NHỰT HÀO - 52200258

THIẾT KẾ MẠNG CHO HỆ THỐNG NGÂN HÀNG NHỎ VỚI YÊU CẦU BẢO MẬT CAO

BÁO CÁO CUỐI KỲ
MẠNG MÁY TÍNH NÂNG CAO

THÀNH PHỐ HỒ CHÍ MINH, 2025

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

DIỆP TRƯƠNG KHÁNH BĂNG - 52200238

NGUYỄN NGỌC QUỲNH NHƯ - 52200281

NGUYỄN TẤN ĐẠT - 52200285

LÊ NHỰT HÀO - 52200258

THIẾT KẾ MẠNG CHO HỆ THỐNG NGÂN HÀNG NHỎ VỚI YÊU CẦU BẢO MẬT CAO

BÁO CÁO CUỐI KỲ
MẠNG MÁY TÍNH NÂNG CAO

Người hướng dẫn

TS. TRƯƠNG ĐÌNH TÚ

THÀNH PHỐ HỒ CHÍ MINH, 2025

LỜI CẢM ƠN

Chúng em xin chân thành bày tỏ sự biết ơn sâu sắc và lòng kính trọng đến TS. TRƯƠNG ĐÌNH TÚ, thầy là người hướng dẫn chúng em trong dự án lần này. Trong quá trình học tập và làm việc, thầy đã truyền đạt cho chúng em vô vàn kiến thức hay và bổ ích, giúp chúng em có được cơ sở lý thuyết vững vàng để em có thể hoàn thành dự án này.

Tuy nhiên, vì sự hiểu biết còn hạn chế của chúng em, bài báo cáo còn nhiều sai sót và chưa chỉnh chu như chúng em mong muốn. Chúng em rất mong nhận được nhận xét và đánh giá của thầy cổ để có thể rút kinh nghiệm cũng như sửa chữa lỗi sai của bản thân.

Chúng em xin kính chúc quý thầy, quý cô và quý nhà trường luôn mạnh khỏe, hạnh phúc và ngày một thành công hơn trong sự nghiệp trồng người của mình.

Chúng em xin chân thành cảm ơn!

TP.Hồ Chí Minh, Ngày 22 tháng 11 năm 2025.
Tác giả
(ký và ghi rõ họ tên)

Diệp Trương Khánh Băng

Nguyễn Ngọc Quỳnh Như

Lê Nhựt Hào

Nguyễn Tấn Đạt

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Nhóm chúng em xin cam đoan đây là công trình nghiên cứu của riêng chúng em và được sự hướng dẫn khoa học của TS. TRƯƠNG ĐÌNH TÚ. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong báo cáo còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào nhóm chúng em xin hoàn toàn chịu trách nhiệm về nội dung Báo cáo của mình. Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do chúng em gây ra trong quá trình thực hiện (nếu có).

TP.Hồ Chí Minh, Ngày 22 tháng 11 năm 2025.
Tác giả
(ký và ghi rõ họ tên)

Diệp Trương Khánh Băng

Nguyễn Ngọc Quỳnh Như

Lê Nhựt Hào

Nguyễn Tấn Đạt

THIẾT KẾ MẠNG CHO HỆ THỐNG NGÂN HÀNG NHỎ VỚI YÊU CẦU BẢO MẬT CAO

TÓM TẮT

- **Vấn đề nghiên cứu:**

  Báo cáo gồm 5 chương

  - Chương 1 - Mục tiêu và phạm vi dự án
  - Chương 2 - Thiết kế sơ đồ mạng
  - Chương 3 - Cấu hình chi tiết
  - Chương 4 - Kiểm thử và kết quả thực nghiệm
  - Chương 5 - Kết luận và hướng phát triển

  Hệ thống mạng được thiết kế theo mô hình chuẩn của một ngân hàng quy mô nhỏ, trong đó yếu tố bảo mật và phân tách vùng dữ liệu được đặt lên hàng đầu. Toàn bộ kiến trúc được chia thành ba khu vực độc lập: Internal, DMZ, và External, đảm bảo các dịch vụ nhạy cảm như Database và Web Server được đặt trong vùng DMZ trung gian, tách biệt khỏi mạng nội bộ và Internet.

  Các router, switch L3 và tường lửa ASA được cấu hình đồng bộ nhằm thực thi các chính sách bảo mật doanh nghiệp, bao gồm: phân tách VLAN, định tuyến OSPF, NAT, DHCP Snooping, Port Security và HSRP. Đặc biệt, hệ thống triển khai Extended ACL để giới hạn truy cập vào cơ sở dữ liệu, chỉ cho phép những subnet hoặc máy chủ được cấp quyền mới có thể kết nối đến DB Server trong DMZ.

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

CHƯƠNG 1 - MỤC TIÊU VÀ PHẠM VI DỰ ÁN

1.1 Mục tiêu dự án

Dự án thực hiện xây dựng một hệ thống mạng cho ngân hàng nhỏ, bảo vệ dữ liệu nhạy cảm trong lĩnh vực ngân hàng, tài chính yêu cầu tính bảo mật cao.

Mục tiêu cụ thể bao gồm:

- Xây dựng mô hình ba vùng: External - DMZ - Internal.
- Tách biệt hoàn toàn Web Server, DNS, FTP trong DMZ để giảm rủi ro bảo mật.
- Cấu hình Extended ACL để kiểm soát truy cập Database.
- Kích hoạt Syslog và SNMP để giám sát hoạt động router, switch, server.
- Cấu hình VPN Remote Access để nhân viên truy cập từ bên ngoài.
- Kiểm thử khả năng chống truy cập trái phép và báo cáo log giám sát.

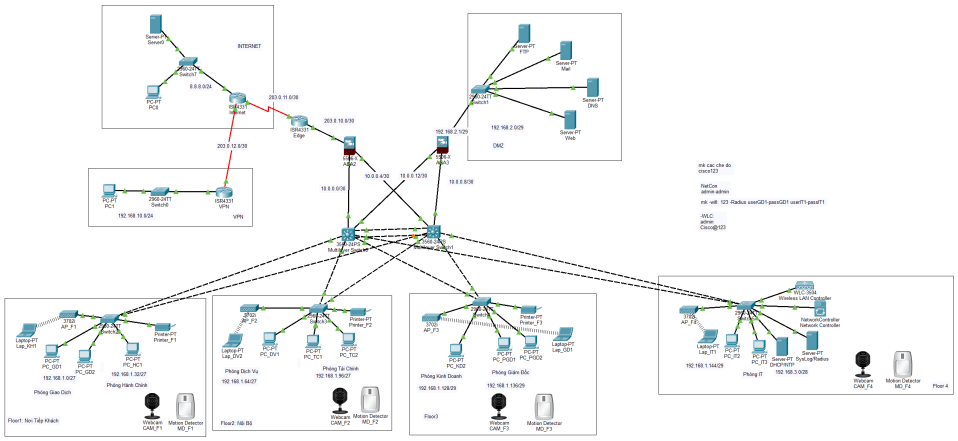
1.2 Phạm vi dự án

Phạm vi dự án bao gồm các phần sau:

- Thiết kế sơ đồ mạng (Topology): phân chia rõ ràng 3 khu vực Internal, DMZ và External; xác định vị trí của Web Server và Database trong DMZ.
- Cấu hình chi tiết: cấu hình định tuyến (routing), địa chỉ IP, VLAN cần thiết để đảm bảo kết nối giữa các khu vực mạng.
- Phân vùng bảo mật: cấu hình Extended ACL để kiểm soát truy cập, giới hạn truy cập vào Database.
- Hệ thống giám sát: cấu hình Syslog và SNMP trên router và switch để thu thập dữ liệu và giám sát trạng thái mạng.
- Truy cập từ xa: cấu hình VPN Remote Access để nhân viên kết nối từ xa an toàn vào mạng nội bộ của ngân hàng.
- Kiểm thử và báo cáo: Thực hiện kiểm thử khả năng chống truy cập trái phép từ bên ngoài và báo cáo log giám sát thu thập được từ Syslog.

CHƯƠNG 2 - THIẾT KẾ SƠ ĐỒ MẠNG

2.1 Sơ đồ mạng tổng quan



Hình 2.1 Sơ đồ tổng quan hệ thống

2.2 Phân vùng khu vực mạng

Mô hình hệ thống mạng được phân chia theo 3 khu vực chính: External - DMZ - Internal. Mỗi khu vực có vai trò và dải địa chỉ IP riêng, các khu vực kết nối tập trung về Core Switch để kiểm soát lưu lượng và áp dụng ACL.

2.2.1 Khu vực External

External là vùng đại diện cho mạng công cộng, Internet và các nguồn truy cập từ bên ngoài vào ngân hàng.

Thiết bị:

- Router Internet **(Internet)**: nhà cung cấp dịch vụ Internet, gửi truy cập từ bên ngoài vào Edge Router, dùng để kiểm thử truy cập Web từ Internet.
- External Switch **(Switch7)**: kết nối router ISP với các thiết bị Internet mô phỏng.
- PC **(PC0)** : mô phỏng người dùng ngoài ngân hàng truy cập Web Server, dùng để kiểm thử chống truy cập trái phép.
- External Server **(Server0)**: cung cấp dịch vụ công cộng ngoài Internet.
- Edge Router **(Edge)**: cổng vào chính của ngân hàng từ Internet, thực hiện NAT/PAT, ACL để kiểm soát lưu lượng và bảo vệ mạng, chuyển tiếp kết nối hợp lệ xuống DMZ qua Firewall.

- External Firewall (**ASA2**): kiểm soát toàn bộ lưu lượng từ Edge Router trước khi vào hệ thống nội bộ, tạo lớp bảo vệ đầu tiên trước DMZ và Internal.

2.2.2 Khu vực DMZ

DMZ là vùng chứa các dịch vụ công cộng mà ngân hàng cung cấp. DMZ nằm sau ASA Firewall nhằm tách biệt hoàn toàn với Internal.

Thiết bị:

- 4 Server cung cấp các dịch vụ:
  - **Web Server**: cung cấp dịch vụ web công cộng.
  - **DNS Server**: phân giải tên miền cho các dịch vụ của ngân hàng.
  - **Mail Server**: xử lý email đến từ bên ngoài.
  - **FTP Server**: lưu trữ file, tài liệu công khai.
- DMZ Switch **(Switch1)**: kết nối toàn bộ server trong DMZ với Firewall và Core Switch
- DMZ Firewall **(ASA3)**: phân tách hoàn toàn DMZ với Internal, chặn Internal truy cập DMZ ngoại trừ dịch vụ được cho phpes, là lớp phòng thủ thứ 2 sau External Firewall.

2.2.3 Khu vực Internal

Internal là khu vực nội bộ của ngân hàng, gồm 4 tầng. Mỗi tầng có router, switch và thiết bị riêng. Đây là vùng chứa dữ liệu, giao dịch và hoạt động của nhân viên.

Ngoài ra hệ thống còn mở rộng khu vực VPN Remote dùng để cho nhân viên làm việc từ xa kết nối vào mạng nội bộ của ngân hàng.

Thiết bị trung tâm:

- Core Switch **(Multilayer Switch0, Multilayer Switch1)**: kết nối tất cả các khu vực, định tuyến nội bộ giữa các tầng, phòng ban; áp dụng ACL nội bộ để bảo vệ dữ liệu ngân hàng.
- Internal Server (đặt tại phòng IT): cung cấp các dịch vụ nội bộ
  - **RADIUS Server**: xác thực người dùng WiFi.
  - **DHCP Server**: cấp IP động cho thiết bị nội bộ. ‘
  - **Syslog Server**: thu thập log từ router, switch, firewall để giám sát hệ thống.
- **Wireless LAN Controller** (đặt tại phòng IT): điều khiển toàn bộ Access Point trong ngân hàng, xác thực người dùng thông qua RADIUS, quản lý chất lượng mạng không dây.

- **Network Controller** (đặt tại phòng IT): máy chủ quản lý mạng/ IoT nội bộ, hỗ trợ kiểm soát và giám sát thiết bị.

Thiết bị theo từng tầng:

- Floor 1 - Phòng giao dịch, phòng hành chính: Nơi tiếp khách
  - Switch Floor 1 (**Switch2**): kết nối các thiết bị của tầng 1.
  - Access Point (**AP_F1**): cung cấp WiFi cho tầng 1.
  - Thiết bị người dùng (**PC_GD1, PC_GD2, PC_HC1, Lap_KH1, Printer_F1**): thiết bị làm việc của các phòng ban
  - Thiết bị IoT (**CAM_F1, MD_F1**): camera và cảm biến chuyển động để giám sát an ninh nội bộ tầng 1.
- Floor 2 - Phòng dịch vụ, phòng tài chính : Nội bộ
  - Switch Floor 2 **(Switch3)**: kết nối các thiết bị của tầng 2.
  - Access Point **(AP_F2)**: cung cấp WiFi cho tầng 2.
  - Thiết bị người dùng **(Lap_DV2, PC_DV1, PC_TC1, PC_TC2, Printer_F2)**: thiết bị làm việc của các phòng ban.
  - Thiết bị IoT **(CAM_F2, MD_F2)**: camera và cảm biến chuyển động để giám sát an ninh nội bộ tầng 2.
- Floor 3 - Phòng kinh doanh, phòng giám đốc
  - Switch Floor 3 **(Switch4)**: kết nối các thiết bị của tầng 3.
  - Access Point **(AP_F3)**: cung cấp WiFi cho tầng 3.
  - Thiết bị người dùng **(PC_KD2, PC_PGD1, PC_PGD2, Lap_GD1, Printer_F3)**: thiết bị làm việc của các phòng ban.
  - Thiết bị IoT **(CAM_F3, MD_F3)**: camera và cảm biến chuyển động để giám sát an ninh nội bộ tầng 3.
- Floor 4 - Phòng IT
  - Switch Floor 4 **(Switch5)**: kết nối các thiết bị của tầng 4.
  - Access Point (**AP_F4)**: cung cấp WiFi cho tầng 4.
  - Thiết bị người dùng **(Lap_IT1, PC_IT2, PC_IT3)**: thiết bị làm việc của phòng ban.
  - Thiết bị IoT **(CAM_F4, MD_F4)**: camera và cảm biến chuyển động để giám sát an ninh nội bộ tầng 4.
  - **RADIUS/DHCP/Syslog Server.**
  - **Wireless LAN Controller.**
  - **Network Controller.**

Khu vực VPN Remote:

- Router VPN **(VPN)** : xác thực người dùng VPN.
- Switch VPN **(Switch0)**: kết nối Router VPN với thiết bị kiểm thử.
- PC VPN client **(PC1)**: thiết bị kiểm thử việc kết nối VPN từ xa.

2.3 Phân chia địa chỉ IP

2.3.1 Thông tin kết nối port trong hệ thống

No	**Source Device**	**Source Interface**	**Destination Device**	**Destination Interface**	**Protocol**	**Trunk/VLAN**
1	Internet Router	S0/1/0	Edge Router	S0/1/0	Serial	WAN
2	Internet Router	S0/1/1	VPN Router	S0/1/1	Serial	WAN
3	Edge Router	Gi0/0/0	ASA2 External	Gi1/3	Ethernet	L3 link
4	ASA2 External	Gi1/1	Core SW1	Fa0/1	Ethernet	Trunk
5	ASA2 External	Gi1/2	Core SW2	Fa0/2	Ethernet	Trunk
6	ASA3 DMZ	Gi1/1	Core SW1	Fa0/1	Ethernet	Trunk
7	ASA3 DMZ	Gi1/2	Core SW2	Fa0/2	Ethernet	Trunk
8	Core SW1	Gi0/1	Core SW2	Gi0/1	Ethernet	Trunk
9	Core SW1	Gi0/2	Core SW2	Gi0/2	Ethernet	Trunk
10	Core SW1	Fa0/3	SW_F1	Fa0/1	Ethernet	Trunk
11	Core SW1	Fa0/4	SW_F2	Fa0/1	Ethernet	Trunk
12	Core SW1	Fa0/5	SW_F3	Fa0/1	Ethernet	Trunk
13	Core SW1	Fa0/6	SW_F4	Fa0/1	Ethernet	Trunk
14	Core SW2	Fa0/3	SW_F1	Fa0/2	Ethernet	Trunk
15	Core SW2	Fa0/4	SW_F2	Fa0/2	Ethernet	Trunk
16	Core SW2	Fa0/5	SW_F3	Fa0/2	Ethernet	Trunk
17	Core SW2	Fa0/6	SW_F4	Fa0/2	Ethernet	Trunk
18	SW_VPN	Gi0/0/0	VPN Router	Fa0/1	Ethernet	N/A

Bảng 2.1 Thông tin kết nối port

2.3.2 Thông tin VLAN & Interface VLAN trong hệ thống

VLAN ID	**Tên VLAN**	**Subnet**	**Default Gateway**
10	GiaoDich	192.168.1.0/27	192.168.1.1
11	HanhChinh	192.168.1.32/27	192.168.1.33
20	DichVu	192.168.1.64/27	192.168.1.65
21	TaiChinh	192.168.1.96/27	192.168.1.97
30	KinhDoanh	192.168.1.128/29	192.168.1.129
31	GiamDoc	192.168.1.136/29	192.168.1.137
32	KyThuat	192.168.1.144/29	192.168.1.145
33	QuanLy	192.168.3.0/28	192.168.3.1
40	DMZ	192.168.2.0/29	192.168.2.1

Bảng 2.2 Thông tin VLAN

2.3.3 Thông tin IP Management

Thiết bị	Interface	VLAN	IP address	Subnet Mask	Gateway
Core SW1	VLAN33	33	192.168.3.7	255.255.255.240	192.168.3.1
Core SW2	VLAN33	33	192.168.3.8	255.255.255.240	192.168.3.1
SW_F1	VLAN33	33	192.168.3.9	255.255.255.240	192.168.3.1
SW_F2	VLAN33	33	192.168.3.10	255.255.255.240	192.168.3.1
SW_F3	VLAN33	33	192.168.3.11	255.255.255.240	192.168.3.1
SW_F4	VLAN33	33	192.168.3.12	255.255.255.240	192.168.3.1
Wireless LAN Controller	Mgmt	33	192.168.3.6	255.255.255.240	192.168.3.1
Network Controller	Mgmt	33	192.168.3.5	255.255.255.240	192.168.3.1
DHCP/NTP Server	NIC	33	192.168.3.3	255.255.255.240	192.168.3.1
Syslog/Radius Server	NIC	33	192.168.3.4	255.255.255.240	192.168.3.1

Bảng 2.3 Thông tin IP Management

CHƯƠNG 3 - CẤU HÌNH CHI TIẾT

3.1 Phân chia VLAN và gán cổng

Dựa trên kế hoạch phân chia VLAN theo các phòng ban, từ đó dữ liệu giao dịch, tài chính sẽ không lẫn với hành chính hay marketing… VLAN sẽ được tạo trên Switch Layer 2, 3.

- VLAN 10 - Giao Dịch
- VLAN 11 - Hành Chính
- VLAN 20 – Dịch Vụ
- VLAN 21 – Tài Chính
- VLAN 30 – Kinh Doanh
- VLAN 31 - Giám Đốc
- VLAN 32 - Kỹ Thuật
- VLAN 33 - Quản Lý
- VLAN 40 - DMZ

Trên các Switch L2 VLAN được tạo và gán cho từng port theo phòng ban, không cho phép người dùng cắm trunk giả mạo để chiếm quyền VLAN khác:

nterface f0/3
switchport mode access
switchport access vlan 10

Cấu hình trunk: dùng để cho phép các VLAN cần thiết đi qua:

interface range f0/1-2
switchport mode trunk
switchport trunk allowed vlan 10,11,20,21,30,31,32,33,40

Cấu hình port Security: chống giả mạo, ghi nhận học các MAC thật và ngăn chặn các MAC lạ tấn công, ngăn tấn công “MAC flooding”:

switchport port-security
switchport port-security mac-address sticky

Cấu hình DHCP Snooping: lọc DHCP Server giả mạo, bảo vệ khách hàng và nhân viên khỏi các cuộc tấn công:

ip dhcp snooping vlan 10-11
ip dhcp snooping

3.2 Switch L3 - Định tuyến nội bộ và dự phòng

Trong mô hình mạng, Switch L3 có vai trò như Core Switch dùng để xử lý các đường đi nội bộ và các giao thức quan trọng.

3.2.1 Bật IP Routing

Cho phép Switch L3 hoạt động như Router

Hỗ trợ Inter-VLAN Routing

ip routing

3.2.2 Interface VLAN (SVI)

Trong mô hình, mỗi VLAN đều được tạo một **SVI (interface VLAN)** trên Switch L3.

Router giữa các VLAN (inter-VLAN routing) chỉ hoạt động khi mỗi VLAN có gateway.

HSRP tạo ra một "gateway ảo" (virtual IP). Đây là một thành phần rất quan trọng khi xây dựng trong mạng ngân hàng vì nó đòi hỏi tính sẵn sàng cực kì cao. Lợi ích HSRP mang lại như nếu một Switch L3 đang làm gateway bị chết thì mạng sẽ không bị gián đoạn, và người dùng vẫn đi ra ngoài Internet được. Vì thế nếu không có HSRP thì một sự cố nhỏ cũng có thể dẫn đến tình trạng downtime như mất giao dịch, thiệt hại về mặt tài chính...

interface Vlan10
ip address 192.168.1.2 255.255.255.224
standby 10 ip 192.168.1.1

3.2.3 DHCP Relay

Chuyển tiếp gói DHCP đến DHCP Server trung tâm

Cho phép 1 server cấp IP cho nhiều VLAN.

ip helper-address 192.168.1.154

3.2.4 OSPF Routing

OSPF là giao thức định tuyến ổn định: Hoạt động tốt trong mạng ngân hàng lớn, nhiều VLAN, nhiều router, giảm lỗi.

Có tính hội tụ cao: Khi mạng thay đổi, OSPF cập nhật định tuyến nhanh → hạn chế downtime.

router ospf 1
network 192.168.1.0 0.0.0.255 area 0

3.3 Router – Kết nối WAN, OSPF, VPN, NAT

3.3.1 Router Internet

Giả lập ISP của ngân hàng

Cung cấp đường đi ra Internet

interface g0/0/0
ip address 8.8.8.1 255.255.255.0

3.3.2 Router Edge – VPN, NAT

AAA Authentication cho VPN: Cung cấp tài khoản nội bộ cho nhân viên truy cập từ xa. Chỉ người đã đăng ký trong hệ thống mới đăng nhập được
aaa authentication login UserVPN local
username uservpn secret ciscovpn

Cấu hình ISAKMP (Phase 1): Tạo phiên VPN an toàn. AES-256 → mức mã hóa cấp doanh nghiệp
crypto isakmp policy 100
encr aes 256
authentication pre-share

Cấu hình IPSec (Phase 2): Mã hóa dữ liệu truyền qua VPN. Đảm bảo không ai nghe lén.
crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac

IP Pool cho VPN: Khi nhân viên kết nối VPN → được cấp IP riêng. Tách biệt khỏi mạng nội bộ để dễ quản lý và log.
ip local pool PoolVPN 192.168.100.10 192.168.100.50

3.4 Firewall ASA – Chia vùng mạng và bảo mật DMZ

ASA được dùng để tách **Internal – DMZ – External.**

3.4.1 Phân vùng bảo mật

Internal (100): mức tin cậy cao nhất

DMZ: mức trung gian

External: Internet (0) – không tin cậy

ASA tự động chặn traffic từ thấp → cao

nameif inside1
security-level 100

nameif dmz
security-level 75

nameif outside
security-level 0

3.4.2 Dynamic NAT

Giấu IP thật của hệ thống ngân hàng.

object network INTERNAL
nat (inside,outside) dynamic interface

3.4.3 ACL bảo vệ Database trong DMZ

Chặn toàn bộ truy cập từ các mạng nội bộ không được phép

Chỉ mở đúng những port cần thiết (DNS, HTTP, Mail. . .)

Đảm bảo database không bị truy cập trái phép

access-list DMZ extended deny ip 192.168.1.0 255.255.255.224 object WEB

3.4.4 Kiểm tra traffic (Inspection)

Ngăn tấn công thay đổi gói DNS

Kiểm tra FTP control-data để chống giả mạo

Theo dõi ICMP để phát hiện scan mạng

inspect dns
inspect ftp
inspect icmp

3.5 Syslog và SNMP – Giám sát toàn hệ thống

3.5.1 Log và syslog

Tập trung log từ Switch, Router, Firewall

Ghi lại vi phạm:

- Port-security
- DHCP Snooping
- Đăng nhập VPN sai
- OSPF down/up

Dùng để theo dõi khi có sự cố.

logging trap debugging
logging 192.168.3.4

3.5.2 SNMP – Network Monitoring

Theo dõi trạng thái thiết bị: CPU, RAM, interface

Gửi cảnh báo khi link down hoặc traffic bất thường

snmp-server community read RO
snmp-server community write RW

CHƯƠNG 4 - KIỂM THỬ VÀ KẾT QUẢ THỰC NGHIỆM

4.1 Kiểm thử kết nối cơ bản (Ping)

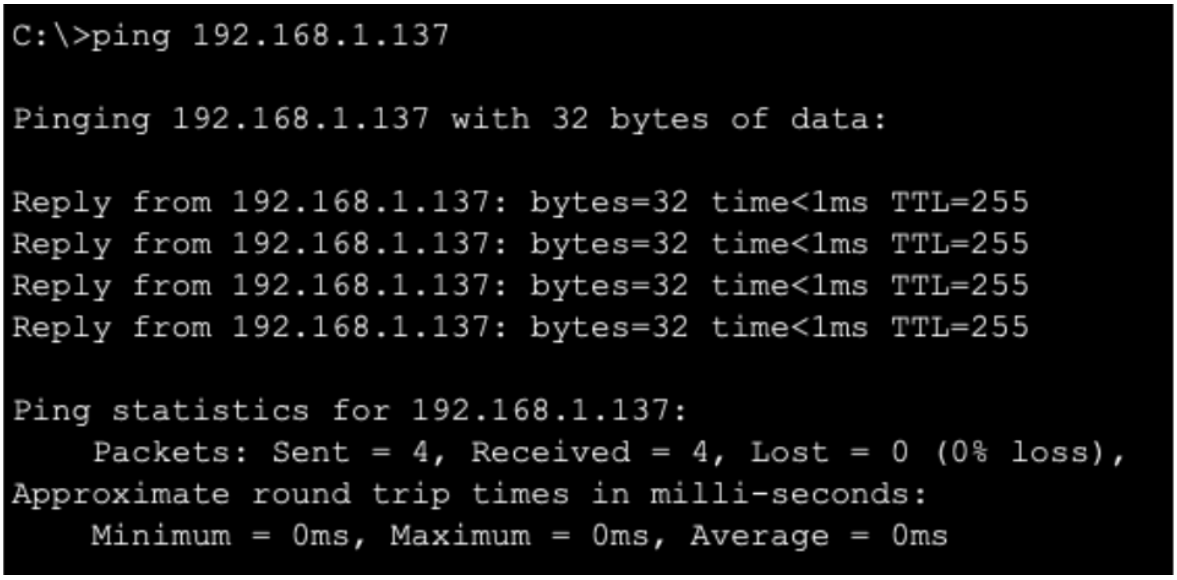
Kiểm chứng Switch L3 và OSPF hoạt động đúng, các VLAN giao tiếp qua SVI.

Ping đến gateway của chính VLAN đó: kiểm tra SVI hoạt động, kiểm tra trunk và access port cấu hình đúng. (Hình 4.1)

Kiểm thử ping đến VLAN khác (Inter-VLAN Routing): chức năng Inter-VLAN Routing hoạt động, Kiểm tra OSPF đã quảng bá các mạng con. (Hình 4.2)

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:D3FF:FE72:C7AD
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.71
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                                 192.168.1.65

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time=5ms TTL=255

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

Hình 4.1 Ping từ PCDV1 đến gateway



Hình 4.2 Ping từ PCDV1 đến VLAN khác (ping đến VLAN 31 Giám đốc)

4.2 Kiểm thử OSPF

Xác minh các Router/Switch L3 đã thiết lập quan hệ láng giềng (neighbors).

Kết quả mong đợi

- FULL/DR
- FULL/BDR
- FULL/ -

=> OSPF adjacency đã hình thành.

Router đã trao đổi LSAs.

Mạng đã sẵn sàng định tuyến.

```
Switch#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.2           1   FULL/DR         00:00:32    192.168.1.35    Vlan11
1.1.1.2           1   FULL/DR         00:00:32    192.168.1.67    Vlan20
1.1.1.2           1   FULL/DR         00:00:32    192.168.1.99    Vlan21
1.1.1.2           1   EXSTART/DR      00:00:32    192.168.1.129   Vlan30
1.1.1.2           1   EXSTART/DR      00:00:32    192.168.1.137   Vlan31
1.1.1.2           1   EXSTART/DR      00:00:32    192.168.1.145   Vlan32
1.1.1.2           1   EXSTART/DR      00:00:32    192.168.3.1     Vlan33
203.0.10.2        1   FULL/DR         00:00:32    10.0.0.1        FastEthernet0/1
192.168.2.1       1   FULL/DR         00:00:31    10.0.0.13       FastEthernet0/2
```

Hình 4.3 Kiểm tra Neighbor OSPF

Kiểm tra bảng định tuyến OSPF

Mục tiêu: Xác minh các mạng VLAN và DMZ đã được quảng bá.

Ý nghĩa:

- Các mạng từ Switch Layer3 hoặc ASA quảng bá đã được học qua OSPF.
- Định tuyến động đang hoạt động.

```
Switch#show ip route ospf
     8.0.0.0/24 is subnetted, 1 subnets
O       8.8.8.0 [110/67] via 10.0.0.1, 00:41:13, FastEthernet0/1
     10.0.0.0/30 is subnetted, 4 subnets
O       10.0.0.4 [110/2] via 10.0.0.1, 00:41:13, FastEthernet0/1
                 [110/2] via 192.168.1.35, 00:41:13, Vlan11
                 [110/2] via 192.168.1.67, 00:41:13, Vlan20
                 [110/2] via 192.168.1.99, 00:41:13, Vlan21
O       10.0.0.8 [110/2] via 10.0.0.13, 04:17:09, FastEthernet0/2
                 [110/2] via 192.168.1.35, 04:17:09, Vlan11
                 [110/2] via 192.168.1.67, 04:17:09, Vlan20
                 [110/2] via 192.168.1.99, 04:17:09, Vlan21
     192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
O       192.168.1.0 [110/2] via 192.168.1.35, 04:17:09, Vlan11
                    [110/2] via 192.168.1.67, 04:17:09, Vlan20
                    [110/2] via 192.168.1.99, 04:17:09, Vlan21
     192.168.2.0/29 is subnetted, 1 subnets
O       192.168.2.0 [110/2] via 10.0.0.13, 04:17:09, FastEthernet0/2
O    192.168.10.0 [110/131] via 10.0.0.1, 00:41:13, FastEthernet0/1
     203.0.10.0/30 is subnetted, 1 subnets
O       203.0.10.0 [110/2] via 10.0.0.1, 00:41:13, FastEthernet0/1
     203.0.11.0/30 is subnetted, 1 subnets
O       203.0.11.0 [110/66] via 10.0.0.1, 00:41:13, FastEthernet0/1
     203.0.12.0/30 is subnetted, 1 subnets
O       203.0.12.0 [110/130] via 10.0.0.1, 00:41:13, FastEthernet0/1
```

Hình 4.4 Kiểm tra bảng định tuyến OSPF

Kiểm tra LSA sẽ thấy:

- Router-LSA
- Network-LSA
- Summary-LSA
- External-LSA

Ý nghĩa: Chứng minh hệ thống:

- Đang trao đổi LSAs
- Đang duy trì topology OSPF
- Đang hoạt động đúng chuẩn doanh nghiệp

```
Switch#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
203.0.12.2      203.0.12.2      116         0x80000004 0x00e81b 3
203.0.12.1      203.0.12.1      115         0x80000006 0x002616 5
203.0.11.2      203.0.11.2      86          0x80000005 0x0014b9 3
192.168.2.1     192.168.2.1     81          0x80000006 0x00d2ca 3
1.1.1.2         1.1.1.2         76          0x80000010 0x0028b9 10
1.1.1.1         1.1.1.1         61          0x8000000f 0x001e26 9
203.0.10.2      203.0.10.2      56          0x80000007 0x002478 3

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.67    1.1.1.2         86          0x80000001 0x005c44
192.168.1.99    1.1.1.2         86          0x80000002 0x001966
10.0.0.9        192.168.2.1     81          0x80000001 0x00610a
10.0.0.5        203.0.10.2      81          0x80000001 0x008711
203.0.10.1      203.0.11.2      86          0x80000001 0x00f605
10.0.0.13       192.168.2.1     81          0x80000002 0x003136
192.168.1.35    1.1.1.2         81          0x80000003 0x009925
10.0.0.1        203.0.10.2      56          0x80000002 0x00a7f4
```

Hình 4.5 Kiểm tra LSA

CHƯƠNG 5 - KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Chương cuối cùng tóm tắt kết quả và đưa ra những gợi ý cho tương lai.

5.1 Kết luận

5.1.1 Hoàn thiện phân đoạn mạng theo mô hình 3 lớp (External – DMZ – Internal)

Internal gồm 8 VLAN: Giao Dịch, Hành Chính, Dịch vụ, Tài chính, Kinh doanh, Giám đốc, Kỹ thuật, Quản lý.

DMZ hoạt động độc lập tại VLAN 40, có kết nối bảo vệ qua ASA2.

External mô phỏng Internet kết nối vào Edge Router và ASA1.

5.1.2 Hoàn thiện DMZ với firewall

Hệ thống DMZ gồm các server Web, DNS, Mail, FTP được bảo vệ bởi ACL chi tiết trên ASA2.

Hệ thống đã đạt được:

- Chặn hoàn toàn truy cập từ các VLAN không được phép (deny strict)
- Chỉ mở cổng phù hợp cho dịch vụ (DNS eq domain, HTTP/HTTPS, FTP. . .)
- Kiểm tra gói tin.

Kết quả: → DMZ được cô lập hiệu quả, chống truy cập trái phép từ nội bộ và Internet.

5.1.3 Hoàn thiện Edge Security với ASA1

Trên ASA1 (gateway ra Internet):

- NAT động cho toàn bộ mạng nội bộ
- ACL chống spoofing
- Chính sách kiểm tra gói tin

Kết quả: → Người dùng từ xa có thể truy cập an toàn vào hệ thống qua VPN, bảo đảm tính bảo mật của ngân hàng.

5.2 Hướng phát triển

5.2.1 Triển khai thật trên toàn bộ khuôn viên ngân hàng

Chuyển mô hình mô phỏng sang môi trường thực tế:

Sử dụng switch Cisco Catalyst series mới (9300/9400)

Sử dụng firewall thế hệ mới (ASA-X hoặc FirePower)

Kết nối WAN thực tế tại các chi nhánh

5.2.2 Áp dụng giám sát tự động (Network Monitoring và Automation)

Đề xuất:

Triển khai SNMP + Syslog server + SIEM

Tích hợp phần mềm giám sát

Tự động hóa backup cấu hình switch/firewall

Tự động phát hiện bất thường mạng

5.2.3 Ứng dụng mở rộng cho Smart City hoặc Smart Campus

Dựa trên mô hình phân lớp mạng hiện tại, ta có thể phát triển cho:

Hệ thống tòa nhà thông minh (IoT + security)

Khu dân cư/công viên/campus

Quản lý camera giám sát, cảm biến, tự động hóa

TÀI LIỆU THAM KHẢO

[1] Cisco Networking Academy, *Module 1: Single-Area OSPFv2 Concepts*, Enterprise Networking, Security, and Automation v7.0, Cisco Systems, 2016.

[2] Cisco Networking Academy, *Module 4: ACL Concepts*, Enterprise Networking, Security, and Automation v7.0, Cisco Systems, 2016.

[3] Cisco Networking Academy, *Packet Tracer 8.2 Official Lab Manual*, Cisco Press, 2023.