

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



CAO NGUYỄN KỲ DUYÊN – 51900491
HOÀNG PHÚC THIÊN AN – 51900644

**TÌM HIỂU VÀ XÂY DỰNG HỆ THỐNG
BẢO MẬT CHO CÔNG TY SẢN XUẤT
THỰC PHẨM GREENFEED**

DỰ ÁN CÔNG NGHỆ THÔNG TIN 2

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG
DỮ LIỆU**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024

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



CAO NGUYỄN KỲ DUYÊN – 51900491
HOÀNG PHÚC THIÊN AN – 51900644

**TÌM HIỂU VÀ XÂY DỰNG HỆ
THỐNG BẢO MẬT CHO CÔNG TY
SẢN XUẤT THỰC PHẨM
GREENFEED**

DỰ ÁN CÔNG NGHỆ THÔNG TIN 2

**MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG
DỮ LIỆU**

Người hướng dẫn

TS. Bùi Quy Anh

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024

LỜI CẢM ƠN

Nhóm xin chân thành cảm ơn đến thầy Bùi Quy Anh đã giúp đỡ, hướng dẫn và dùu dắt chúng em trong quá trình tìm hiểu cho dự án CNTT 2. Nhờ như vậy, nhóm có thể thực hiện đồ án này một cách tốt nhất và có thể đạt được một kết quả tốt nhất.

Và chúng em cũng xin chân thành cảm ơn đến quý thầy cô trong khoa Công nghệ thông tin đã truyền đạt những kiến thức quý báu giúp em có thể hoàn thành tốt được bài báo cáo này. Khoa đã luôn sẵn sàng chia sẻ các kiến thức bổ ích cũng như chia sẻ các kinh nghiệm tham khảo tài liệu, giúp ích không chỉ cho việc thực hiện và hoàn thành đề tài nghiên cứu mà còn giúp ích cho việc học tập và rèn luyện trong quá trình thực hành tại trường Đại học Tôn Đức Thắng.

Nhóm chúng em xin chân thành cảm ơn!

TP. Hồ Chí Minh, ngày 20 tháng 3 năm 2024

Tác giả

(Ký tên và ghi rõ họ tên)

Cao Nguyễn Kỳ Duyên

Hoàng Phúc Thiên An

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH

TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Nhóm xin cam đoan đây là công trình nghiên cứu của riêng nhóm và được sự hướng dẫn khoa học của TS Bùi Quy Anh. 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 Dự án 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 tôi xin hoàn toàn chịu trách nhiệm về nội dung Dự án của mình. Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 20 tháng 3 năm 2024

Tác giả

(Ký tên và ghi rõ họ tên)

Cao Nguyễn Kỳ Duyên

Hoàng Phúc Thiên An

TRIỂN KHAI HỆ THỐNG MẠNG DOANH NGHIỆP

TÓM TẮT

Dựa vào mô hình hệ thống mạng doanh nghiệp, dự án này sẽ triển khai trên 2 site với trụ sở chính ở miền Nam và 1 chi nhánh nằm ở miền Bắc. Cả hai site đều sẽ được thiết kế riêng biệt với đầy đủ các phòng chức năng tương ứng. Đối với các thiết bị Switch và Router và khu vực Server sẽ phân vùng địa chỉ IP tĩnh sử dụng kỹ thuật chia VLSM để đảm bảo tiết kiệm và có khả năng mở rộng. Đối với các phòng chức năng sẽ được gán VLAN để có thể dễ quản lý, đồng thời mỗi client sẽ nhận địa chỉ động từ Server DHCP.

Các Switch Layer 2 sẽ được bảo mật bằng phương pháp Network Access Control thông qua xác thực bằng Radius Server. Trên các Switch Layer 3 sẽ được cài đặt bảo mật với ACL, Firewall được xây dựng thêm hệ thống IDS/IPS bằng mã nguồn mở Snort. Cấu hình một số phương thức chống lặp và dự phòng cùng với cấu hình đường hầm VPN-IPSec. Cuối cùng xây dựng hệ thống Zabbix để giám sát toàn bộ hệ thống mạng nội bộ.

Ngoài ra sẽ tự động hóa cấu hình các thiết bị bằng Ansible, sử dụng github làm công cụ quản lý code.

DEPLOYMENT OF ENTERPRISE NETWORK SYSTEM

ABSTRACT

Based on the enterprise network system model, this project will be deployed across two sites, with the main headquarters located in the South and a branch office in the North. Both sites will be designed separately with all corresponding functional departments. Switches, routers, and server areas will be allocated static IP addresses using VLSM (Variable Length Subnet Masking) to ensure efficiency and scalability. VLANs will be assigned to functional departments for easier management, and each client will receive a dynamic IP address from a DHCP server.

Layer 2 switches will be secured using Network Access Control (NAC) with Radius Server authentication. Layer 3 switches will have security measures in place, including Access Control Lists (ACLs) and a firewall. An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) will be implemented using the open-source Snort. Various redundancy and failover mechanisms will be configured, along with the setup of IPSec VPN tunnels. Lastly, a Zabbix system will be established for comprehensive monitoring of the entire internal network.

Additionally, automation of device configurations will be achieved using Ansible, and GitHub will be utilized as a code management tool.

MỤC LỤC

DANH MỤC HÌNH VẼ	viii
DANH MỤC BẢNG BIỂU	xv
DANH MỤC CÁC CHỮ VIẾT TẮT.....	xvi
CHƯƠNG 1. GIỚI THIỆU VÀ KHẢO SÁT	1
1.1 Giới thiệu đê tài.....	1
1.2 Khảo sát thực tế.....	1
1.3 Mô tả đê tài.....	3
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT.....	4
2.1 Tự động hóa	4
2.1.1 <i>Ansible</i>	4
2.1.2 <i>SSH</i>	5
2.2 Quản lý hệ thống	7
2.2.1 <i>VLAN</i>	7
2.2.2 <i>OSPF</i>	10
2.2.3 <i>SNMP</i>	13
2.3 Tính dự phòng trong hệ thống.....	15
2.3.1 <i>Ethernet Channel</i>	15
2.3.2 <i>Spanning Tree</i>	16
2.3.3 <i>VRRP</i>	18
2.4 Máy chủ.....	20
2.4.1 <i>DNS</i> và <i>Alternative DNS</i>	20
2.4.2 <i>Active Directory Domain Service</i>	21

2.4.3 <i>DHCP</i>	23
2.4.4 <i>ADCS và NPAS</i>	24
2.4.5 <i>FTP Server</i>	26
2.4.6 <i>Group Policy Management</i>	28
2.5 Bảo mật trong hệ thống	29
2.5.1 <i>Network Access Control</i>	29
2.5.2 <i>Access Control List</i>	31
2.5.3 <i>Firewall</i>	32
2.5.4 <i>VPN – IPSec</i>	33
2.5.5 <i>NAT</i>	35
2.5.6 <i>IDS/IPS</i> với <i>Snort</i>	35
CHƯƠNG 3. MÔ HÌNH VÀ THÔNG TIN CẤU HÌNH HỆ THỐNG	39
3.1 Sơ đồ luận lý	39
3.2 Thông tin kết nối port trong hệ thống	42
3.3 Thông tin VLAN, Interface VLAN trong hệ thống	46
3.4 Thông tin thiết kế quy hoạch địa chỉ IP Planning	48
CHƯƠNG 4. CẤU HÌNH HẠ TẦNG.....	51
4.1 Cấu hình cơ bản cho các Router ISP	51
4.2 SSH Access	52
4.3 Cài đặt Ansible	54
4.4 Cấu hình Interface cho các thiết bị	57
4.5 Cấu hình VLAN	59
4.6 Cấu hình Spanning Tree	63

4.7 Cấu hình HSRP	64
4.8 Cấu hình định tuyến động OSPF.....	66
4.9 Access Control List	69
4.10 Network Access Control	76
4.11 SNMP	77
4.12 Cấu hình Server.....	78
4.12.1 Primary DNS Server và Alternative DNS	78
4.12.2 Active Directory Domain Service	86
4.12.3 DHCP Server	90
4.12.4 ADCS và NPAS	92
4.12.5 FTP Server.....	103
4.13 Firewall	108
4.13.1 VPN - IPsec	113
4.13.2 NAT	116
4.13.3 IDS/IPS với Snort.....	117
4.14 Zabbix	122
CHƯƠNG 5. KẾT LUẬN.....	129
5.1 Kết quả đạt được	129
5.2 Hạn chế và hướng phát triển	129
TÀI LIỆU THAM KHẢO	130

DANH MỤC HÌNH VẼ

Hình 1.2.1: Quá trình hình thành và phát triển của GreenFeed	2
<i>Hình 2.1.1.1[12]: Cấu trúc quản lý trên máy Ansible</i>	<i>4</i>
Hình 2.1.2.1: Cơ chế hoạt động của SSH	6
Hình 2.2.2.1: Một số OSPF Concept	12
<i>Hình 2.2.3[11]: Cơ chế hoạt động của SNMP</i>	<i>14</i>
Hình 2.3.1.1[9]: Công nghệ Ethernet Channel.....	15
Hình 2.3.3: Ví dụ về VRRP	18
Hình 2.4.7.1: Mở GPO	28
Hình 2.4.7.2: Hai Policy mặc định của hệ thống	28
Hình 3.1.1: Sơ đồ luận lý khu vực Internet.....	39
Hình 3.1.2: Sơ đồ luận lý khu vực miền Nam.....	40
Hình 3.1.3: Khu vực miền Bắc.....	41
Hình 3.1.4: Sơ đồ tổng quát	42
Hình 4.1: Cấu hình NAT router ISP_R5	51
Hình 4.2: Cấu hình interface cho R1 và áp rule NAT vào interface.....	52
Hình 4.2.1: Cấu hình SSH Access cho Core 1	53
Hình 4.3.1: Tạo cây thư mục	56
Hình 4.3.2: Ví dụ cho cách tạo cây thư mục	56
Hình 4.4.1: Set interface vào thiết bị Distribution 1 bằng Ansible	58
Hình 4.6.1: Cấu hình STP trên Distribution 1 bằng Ansible	63
Hình 4.7.1: Cấu hình HSRP cho Distribution 1 bằng Ansible.....	64
Hình 4.7.2: Cấu hình HSRP cho Distribution 1 bằng Ansible.....	65

Hình 4.7.3: Shutdown cổng nối tới Switch vẫn có thể ping internet bình thường....	65
Hình 4.7.4: Shutdown cổng nối tới Core 1 vẫn có thể ping internet bình thường	66
Hình 4.8.1: Các đường mạng ở các interface của Core 1	67
Hình 4.9.1: Rule cho phép các phòng ban kết nối vào vùng Server thông qua port 53	70
Hình 4.9.2: Từ chối mọi gói tin DNS TCP và UDP đến bất kỳ đích nào (địa chỉ đích và cổng 53).	70
Hình 4.9.3: Thiết lập Rule chỉ cho phòng ban IT remote desktop đến Server.....	71
Hình 4.9.4: Thiết lập rule cho phép phòng ban IT có thể telnet và SSH đến tất cả các thiết bị.....	71
Hình 4.9.5: Áp dụng các rule lên các interface theo chiều out	72
Hình 4.9.6: Cấu hình ACL telnet và SSH cho các thiết bị.....	72
Hình 4.9.7: Các máy client chỉ có thể ping bằng domain thông qua DNS server nội bộ	73
Hình 4.9.8: Các phòng ban chức năng không phải phòng ban IT sẽ không thể SSH vào mọi thiết bị.....	73
Hình 4.9.9: Phòng ban IT ở HO có thể SSH vào các thiết bị HO.....	74
Hình 4.9.10: Phòng ban IT ở site HO có thể SSH vào các thiết bị ở site miền Bắc.	74
Hình 4.9.11: Phòng ban IT ở site miền Bắc chỉ có thể SSH vào các thiết bị ở Miền Bắc nhưng không thể SSH vào các thiết bị ở site HO	75
Hình 4.9.12: Phòng ban IT ở site HO có thể Remote Desktop vào Server.....	75
Hình 4.9.13: Các phòng ban chức năng khác sẽ không thể remote desktop vào Server	76
Hình 4.10.1: Cấu hình xác thực 802.1x trên các thiết bị Switch	76
Hình 4.10.2: Cấu hình Authentication 802.1x trên các thiết bị Switch Access	77

Hình 4.11.1: Cấu hình SMNP cho các Switch	78
Hình 4.12.1.1: Set IP cho Server.....	79
Hình 4.12.1.2: Install DNS Server ở mục add Role and Feature	79
Hình 4.12.1.3: Sau khi đã cài đặt thành công DNS Server, tiến hành vào DNS Manager để cấu hình	80
Hình 4.12.1.4: Nhập đường mạng của DNS Server.....	81
Hình 4.12.1.5: Tương tự Tạo Zone mới ở vùng Forward	81
Hình 4.12.1.6: Tạo bản ghi A và CNAME cho domain của Web Server.....	82
Hình 4.12.1.7: Để thực hiện phân giải tên miền các địa chỉ ở bên ngoài mạng LAN ta sẽ cài đặt DNS recursive	83
Hình 4.12.1.8: Mở CMD -> Nhập lệnh net stop dns && net start dns để khởi động lại dịch vụ DNS	83
Hình 4.12.1.9: Sử dụng Server trên để cấu hình DNS Alternative	84
Hình 4.12.1.10: Tạo Zone cho Forward Lookup Zone	84
Hình 4.12.1.11: Tạo Zone cho Reverse Lookup Zone.....	85
Hình 4.12.1.12: Vào DNS Primary => Properties	85
Hình 4.12.1.13: Cấu hình backup trên cả hai server DNS	86
Hình 4.12.1.14: Khi dịch vụ DNS trên máy Primary tắt thì hệ thống sẽ tự động trỏ đến DNS backup.	86
Hình 4.12.2.1: Install ADDS	87
Hình 4.12.2.2.: Thêm domain và password backup là 2024@gf.....	87
Hình 4.12.2.3: Quản lý ADDS	88
Hình 4.12.2.4: Tạo OU đại diện cho 2 site	88
Hình 4.12.2.5: Tạo Group cho các phòng ban	89

Hình 4.12.2.6: Tạo Users	89
Hình 4.12.2.7: Thêm các user vào các nhóm phòng ban	90
Hình 4.12.3.1: Sau khi đã cài đặt vào DHCP Manager	90
Hình 4.12.3.2: Chọn New Scope để tạo VLAN	91
Hình 4.12.3.3 : Tạo pool VLAN	91
Hình 4.12.3.4: Nhập thông số cho VLAN	92
Hình 4.12.4.1: Cài đặt dịch vụ	92
Hình 4.12.4.2: Cấu hình AD CS	93
Hình 4.12.4.3: Chọn Certification Authority và chọn type là Enterprise CA.....	93
Hình 4.12.4.4: Tạo Pollicy cho phép bật Services Wired AutoConfig.....	94
Hình 4.12.4.5: Tạo Pollicy cho phép bật IEE 802.1X	94
Hình 4.12.4.6: Cập nhật Policy	95
Hình 4.12.4.1.1: Vào giao diện quản lý và cấu hình Radius Server theo chuẩn 802.1X	95
Hình 4.12.4.1.2: Tạo network policy cho phòng ban IT	96
Hình 4.12.4.1.3: Tạo network policy cho phòng ban IT	96
Hình 4.12.4.1.4: Tạo network policy cho phòng ban IT	97
Hình 4.12.4.1.5: Tạo network policy cho phòng ban IT	97
Hình 4.12.4.1.6: Tạo các network policy tương tự cho các phòng ban còn lại	98
Hình 4.12.4.1.7: Bật dịch vụ Wired	98
Hình 4.12.4.1.8: Cấu hình Properties của Ethernet Connection	99
Hình 4.12.4.1.9: Thực hiện join domain	99
Hình 4.12.4.1.10: Máy client sau khi join domain thành công	100

Hình 4.12.4.1.11: Máy client sau khi join domain thành công	101
Hình 4.12.4.2.1: Tạo Policy cho phép phòng IT có thể truy cập vào	102
Hình 4.15.4.2.2: Cấu hình phương thức xác thực	102
Hình 4.15.4.2.3: Phòng ban IT có thể SSH vào thiết bị trong hệ thống	103
Hình 4.12.5.1: Cài đặt FTP ở mục IIS	103
Hình 4.12.5.2: Cấu hình truy cập có tài khoản	104
Hình 4.12.5.3: Tạo Folder chứa file cho từng phòng ban và set quyền cho các role nhất định.....	104
Hình 4.12.5.4: Disable inheritance trong phần Advanced Sharing.....	105
Hình 4.12.5.5: Share các folder riêng cho từng phòng ban phù hợp	105
Hình 4.12.5.6: Thiết lập các quyền truy cập trên dịch vụ FTP	106
Hình 4.12.5.7: Truy cập dịch vụ FTP bằng tài khoản của Admin	107
Hình 4.12.5.8: Sử dụng tài khoản của phòng ban Kế toán để truy cập FTP	107
Hình 4.12.5.9: Sử dụng tài khoản của phòng ban HR để truy cập vào FTP	108
Hình 4.13.1: Sử dụng Firewall pfSense cho hệ thống	108
Hình 4.13.2: Cấu hình IP cho WAN Zone	109
Hình 4.13.3: Tương tự cấu hình IP cho LAN zone.....	109
Hình 4.13.4: Hai Firewall hoạt động song song	110
Hình 4.13.5: Cài đặt IP gateway ảo trên hai Firewall	110
Hình 4.13.6: Thiết lập Firewall là master và Firewall 2 là backup.....	111
Hình 4.13.7: Cài đặt gói FRR để cấu hình OSPF	111
Hình 4.13.8: Cấu hình OSPF cho Firewall	112
Hình 4.13.9: Add Area cho các interface và bật gói tin FRR	112

Hình 4.13.10: Gói tin sẽ ưu tiên đi qua Firewall 1.....	113
Hình 4.13.1.1: Tạo hai tunnel trên hai Firewall ở HO	114
Hình 4.13.1.2: Tạo Phase 1 cho Firewall	114
Hình 4.13.1.3: Tạo Phase 2 cho Firewall	115
Hình 4.13.1.4: Set rule cho Interface của các tunnel và IPSec có thể đi qua Firewall	115
Hình 4.13.2: Kết nối tunnel trên Firewall	116
Hình 4.13.3: Chỉ thực hiện NAT trên interface WAN.....	116
Hình 4.13.4: Các phòng ban ở 2 site có thể kết nối thông được với nhau	117
Hình 4.13.3.1: Cài đặt package Snort cho Firewall	117
Hình 4.13.3.2: Nhập code đã đăng ký từ trang chủ Snort vào Global Setting.....	118
Hình 4.13.3.3: Tiếp tục cấu hình Snort	118
Hình 4.13.3.4: Update rules	119
Hình 4.13.3.5: Alert phát hiện hành vi scan port	120
Hình 4.13.3.6: Hệ thống sẽ block ip này với hành vi scan port	120
Hình 4.13.3.7: Log thể hiện mục tiêu đã down.....	121
Hình 4.13.3.8: Sử dụng công cụ Hight Orbit ION Canon để tấn công DoS/DoS.	121
Hình 4.13.3.9: Alert và Block IP.....	122
Hình 4.14.1: Tạo Discovery Rule để phát hiện các thiết bị mạng có trong nội bộ.	123
Hình 4.14.2: Tạo Action Discovery	123
Hình 4.14.3: Thêm các host cần monitor vào Zabbix	124
Hình 4.14.4: Add Mail cho server.....	125
Hình 4.14.5: Thêm Email của Admin	125

Hình 4.14.6: Tạo các Triggers cần thông báo qua Email.....	126
Hình 4.14.7: Gửi tin nhắn đến các Email trong nhóm Admin khi có sự cố.....	127
Hình 4.14.8: Email thông báo khi có sự cố.....	127
Hình 4.14.9: Dashboard của Zabbix	128

DANH MỤC BẢNG BIỂU

Bảng 1.2.2 Các thiết bị được sử dụng trong mô hình	2
Bảng 2.1.2: Ưu nhược điểm của SSH	6
Bảng 3.2: Bảng thông tin kết nối port trong hệ thống.....	46
Bảng 3.3.1: Bảng thông tin VLAN HO	47
Bảng 3.3.2: Bảng thông tin VLAN Miền Bắc.....	48
Bảng 3.4.1 Bảng thông tin IP khu vực Server miền Nam.....	48
Bảng 3.4.2 Bảng thông tin IP	50

DANH MỤC CÁC CHỮ VIẾT TẮT

VLAN	Virtual Local Area Network
SSH	Secure Shell
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
OSPF	Open Shortest Path First
VRRP	Virtual Router Redundancy Protocol
HSRP	Hot Standby Router Protocol
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
SNMP	Simple Network Monitoring Protocol
SMTP	Simple Mail Transfer Protocol
ACL	Access Control List
VPN	Virtual Private Network
NAT	Network Address Translation

STP	Spanning Tree Protocol
NPAS	Network Policy Access Services
NAC	Network Access Control
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
AD DS	Active Directory Domain Services
AD CS	Active Directory Certificate Services

CHƯƠNG 1. GIỚI THIỆU VÀ KHẢO SÁT

Ở chương này sẽ trình bày khái quát về thông tin doanh nghiệp cũng như việc khảo sát thực tế quy mô hạ tầng từ đó có thể lên kế hoạch triển khai lắp đặt hệ thống mạng cho doanh nghiệp.

1.1 Giới thiệu đề tài

Ngành công nghệ thông tin đã và đang có nhiều thay đổi to lớn và tác động sâu sắc vào cuộc sống cũng như cách sống của mỗi chúng ta. Có thể thấy, chúng ta dường như không thể cách xa được các thiết bị điện tử chẳng hạn như máy tính hay điện thoại,... Nó đã trở nên vô cùng quan trọng trong các công việc hàng ngày từ học tập cũng như công việc. Và để đáp ứng các nhu cầu trong việc giao tiếp, gửi tin nội bộ, tìm kiếm thông tin,... trong các doanh nghiệp hay trường học thì việc triển khai một hạ tầng mạng với các chức năng và bảo mật là vô cùng cần thiết cho một doanh nghiệp để tránh các cuộc tấn công nội bộ với những hậu quả vô cùng nghiêm trọng.

Do đó, mục đích của bài báo cáo này là nghiên cứu, phân tích những đặc điểm của hệ thống mạng, những kỹ thuật tấn công hệ thống mạng để từ đó đưa ra những giải pháp an ninh, bảo mật dựa trên các tiêu chí dựa trên hai khía cạnh: đảm bảo an toàn dữ liệu và toàn vẹn dữ liệu.

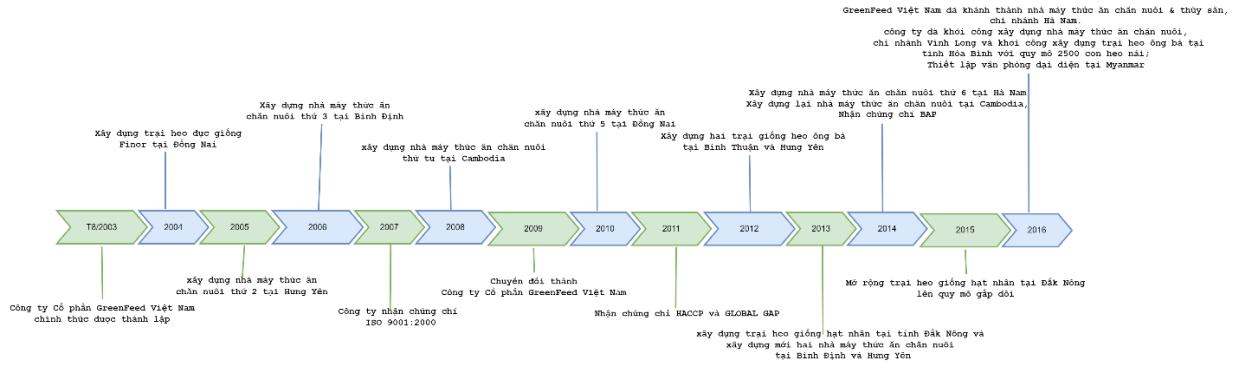
1.2 Khảo sát thực tế

GreenFeed VN có tên đầy đủ là Công ty Cổ phần GreenFeed Việt Nam, tiền thân là Công ty trách nhiệm hữu hạn GreenFeed Việt Nam, được thành lập vào năm 2003 với tầm nhìn đưa thương hiệu GreenFeed VN dẫn đầu trong ngành thực phẩm.

Với khởi đầu trong ngành thức ăn chăn nuôi và sản xuất thức ăn cho gia súc, gia cầm, thủy sản. Hiện nay, GREENFEED trở thành Tập đoàn hàng đầu trong lĩnh vực Nông nghiệp - Thực phẩm với 12 nhà máy, 29 trang trại cùng hoạt động sản xuất kinh doanh tại Việt Nam và khu vực Đông Nam Á. Những nhà máy này được trang bị công nghệ sản xuất từ Mỹ và Châu u, công suất mỗi năm là 2 triệu tấn sản phẩm đạt tiêu chuẩn ISO 22.000, HACCP, GLOBAL GAP, BAP. Toàn hệ thống hoạt động

một cách chuyên nghiệp bằng việc ứng dụng giải pháp hoạch định nguồn lực doanh nghiệp (ERP).

Quá trình hình thành và phát triển của GreenFeed



Hình 1.2.1: Quá trình hình thành và phát triển của GreenFeed

Dựa vào những quan sát, nghiên cứu và học tập ở đây, em đã có ý tưởng về việc triển khai và bảo mật hệ thống mạng doanh nghiệp trong ngành sản xuất. Tuy nhiên để đơn giản hóa trong quá trình nghiên cứu và triển khai, cùng với kinh nghiệm hạn chế của mình, dự án này sẽ tập trung xây dựng một hệ thống mạng nhỏ hơn chỉ với 2 site.

Đối với hệ thống mạng trên, những thiết bị cần thiết để sử dụng sẽ bao gồm những thiết bị sau:

STT	Thiết bị	Hãng/OS	Số lượng
1	Multilayer Switch	Cisco	6
2	Switch Access	Cisco	8
3	Laptop, PC		Theo thực tế
4	Server	Windows	2
5	Ansible	Linux	1
6	Zabbix	Linux	1
7	Firewall	pfSense	3

Bảng 1.2.2 Các thiết bị được sử dụng trong mô hình

1.3 Mô tả đề tài

Một công ty sản xuất có một cơ sở chính tại miền Nam và một chi nhánh tại miền Bắc, với sự phân bổ cụ thể các phòng ban như sau:

Tại văn phòng miền Nam:

- Tầng 1: Lễ tân và phục vụ khách hàng
- Tầng 2: Nhân sự, bộ phận Marketing và Kế toán
- Tầng 3: Phòng IT
- Tầng 4: Kiểm toán, truyền thông và phát triển bền vững
- Tầng 5: Phòng của Giám đốc và Phó giám đốc

Tại văn phòng miền Bắc, sẽ có một chuỗi nhà máy sản xuất riêng và với các phòng ban sau:

- Khu văn phòng với các phòng ban Kế toán, IT, Quản lý, phòng họp,...
- Khu nhà máy sản xuất sẽ do bộ phận Tự động hóa quản lý

Xây dựng một hệ thống mạng có dây, với việc phân chia các nhóm làm việc thành các VLAN riêng biệt. Mỗi nhân viên sẽ có một tài khoản email để liên lạc và làm việc trong mạng nội bộ.

Sử dụng phần mềm giả lập EVE-NG để triển khai trong đó các máy chủ sẽ bao gồm các vai trò như DHCP, Mail, DNS, FTP và Radius.

Để đảm bảo an ninh mạng, hệ thống cũng sẽ cấu hình tường lửa, IDS/IPS dựa trên mã nguồn mở Snort và ACLs. Ngoài ra chỉ cho một số đội nhất định ở phòng IT mới được phép truy cập vào thiết bị mạng. Hệ thống cũng sẽ sử dụng tường lửa để ngăn ngừa tấn công từ internet bên ngoài cũng như thiết lập các chính sách bảo mật cho công ty. Sử dụng giải pháp Network Access Control để linh hoạt cho user kết nối vào mạng và bảo mật hệ thống.

Để đảm bảo tính sẵn sàng của hạ tầng, hệ thống cũng sẽ được cấu hình ethernet channel, spanning tree và HSRP để tạo các đường dự phòng khi có sự cố và truyền thông sẽ không bị gián đoạn. Tự động hóa cấu hình các thiết bị bằng Ansible, sử dụng github làm công cụ quản lý code.

CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

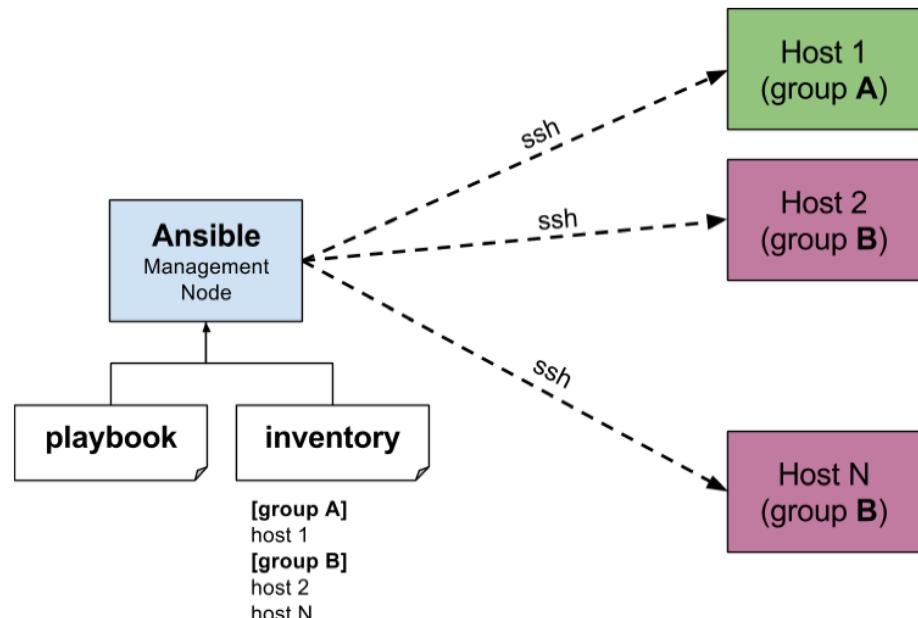
Cơ sở lý thuyết là tiên đề để áp dụng các kỹ thuật vào việc cấu hình, vận hành hệ thống mạng. Sau đây là các lý thuyết mà nhóm đã học và tìm hiểu thêm để vận dụng vào việc xây dựng mô hình hệ thống mạng cho doanh nghiệp.

2.1 Tự động hóa

Tự động hóa trong hệ thống mạng là quá trình sử dụng các công cụ để tự động hóa các tác vụ, quy trình và quản lý mạng một cách hiệu quả. Mục tiêu của tự động hóa là tăng tính linh hoạt và hiệu suất của hệ thống. Một số công cụ thường được sử dụng như là: Ansible, Puppet hoặc Chef để tự động hóa quá trình cấu hình và triển khai thiết bị mạng.

2.1.1 Ansible

Ansible là một công cụ mã nguồn mở được thiết kế để tự động hóa các nhiệm vụ bao gồm triển khai, quản lý cấu hình và xử lý các tác vụ lặp đi lặp lại trên hệ thống, từ đó giúp giảm thiểu thời gian thao tác trên từng server được cài đặt.



[Hình 2.1.1.1^{\[12\]}](#): Cấu trúc quản lý trên máy Ansible

Một số thuật ngữ thường dùng trong Ansible:

- **Playbook:** Là file chứa thông tin những server cần quản lý, thường nằm tại đường dẫn /etc/ansible/hosts
- **Task:** Một block để ghi lại những tác vụ cần thực hiện trong playbook đó.
- **Role:** Là một tập playbook đã được định nghĩa để thực thi một tác vụ nhất định.
- **Module:** Một mã thực thi cụ thể được gọi trong một tssk để thực hiện các công việc cụ thể. Hiện nay Ansible có khá nhiều module có sẵn.
- **Inventory:** Là file chứa thông tin những server cần quản lý, thường được nằm tại đường dẫn /etc/ansible/hosts.
- **Play:** Quá trình thực thi một playbook
- **Handler:** Được sử dụng để kích hoạt những thay đổi của dịch vụ như start, stop service.

Để chạy file playbook trên Ansible, chúng ta sẽ sử dụng câu lệnh:

```
ansible-playbook -i <inventory_file><playbook_file.yml>
```

Trong đó:

- <inventory_file>: là file inventory.ini
- <playbook_file.yml> là file playbook muốn thực thi.

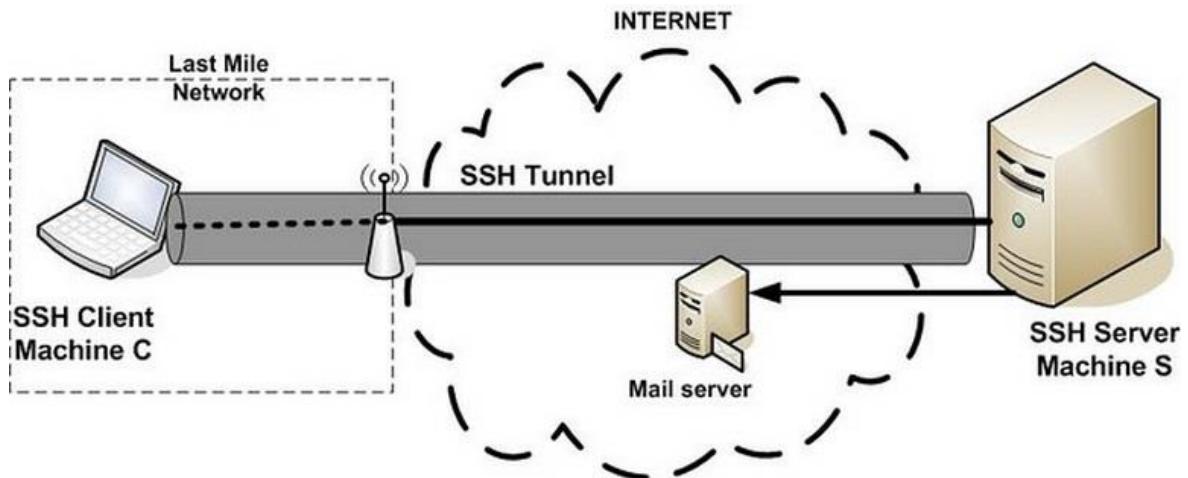
2.1.2 SSH

SSH là một giao thức truyền thông dựa trên văn bản tương tự telnet nhưng an toàn hơn bởi vì các gói tin truyền qua SSH đều sẽ được mã hóa để tránh việc bị tấn công hoặc nghe trộm trong quá trình gói tin được truyền đi.

Các bước để cấu hình SSH

- Bật dịch vụ SSH trên các thiết bị
- Cấu hình xác thực SSH
- Cấu hình quyền truy cập SSH

Khi triển khai SSH thì hệ thống sẽ hỗ trợ cả giao thức ứng dụng, sử dụng cho trình giả lập Terminal hoặc truyền file. Trong thực tế, SSH còn được sử dụng để phát triển tunnel bảo mật cho các giao thức ứng dụng.



Hình 2.1.2.1: Cơ chế hoạt động của SSH

Ưu điểm	Nhược điểm
<ul style="list-style-type: none"> - Bảo mật cao - Không gửi mật khẩu trong văn bản thông thường - Mã hóa dữ liệu đường truyền - Hỗ trợ nhiều phương tiện truyền thông - Giao thức độc lập - Quản lý Phiên an toàn - Khả năng xác định địa chỉ IP cố định 	<ul style="list-style-type: none"> - Cần kết nối mạng - Khó sử dụng đối với người mới - Đòi hỏi kỹ thuật nâng cao khi cấu hình - Khó khắc phục lỗi trong trường hợp sự cố

Bảng 2.1.2: Ưu nhược điểm của SSH

Một số kỹ thuật mã hóa trong SSH:

Mã hóa Symmetric Encryption: Là một phương thức mã hóa ứng dụng secret key theo hai chiều, giải mã tin cho Host và Client, trong đó host và client có nhiệm vụ tạo Key secret.

Mã hóa Asymmetric Encryption: là phương thức dùng 2 khóa riêng biệt để phục vụ mã hóa và giải mã. Bao gồm public key sẽ công khai trên tất cả thành phần liên quan và private key luôn tuyệt mật và không chia sẻ cho bất kỳ bên thứ ba nào.

Mã hóa Hashing: là phương thức sử dụng phổ biến trong Secure Shell Connection nhưng khác với hai loại mã hóa kia thì hashing không sử dụng vào mục đích giải mã.

2.2 Quản lý hệ thống

2.2.1 VLAN

VLAN (Virtual Local Area Network) là một mạng LAN ảo với mục đích làm nhỏ khu vực quảng bá, có thể giúp các quản trị viên dễ quản lý và giúp giảm thiểu chi phí hơn. Mỗi VLAN sẽ có 1 địa chỉ riêng và sẽ góp phần mang lại hiệu suất tốt hơn.

Một số loại VLAN:

- Default VLAN: các VLAN mặc định thường thuộc VLAN 1
- Default Native VLAN
- Default Management VLAN
- Data VLAN: phân tách lưu lượng do người dùng tạo ra (thường gọi là VLAN của người dùng)
- Management VLAN
- Voice VLAN:
 - Lưu lượng voice IP
 - Băng thông đảm bảo cho chất lượng hội thoại
 - Mức độ ưu tiên hơn so với mạng khác
 - Độ trễ thấp

Các bước cài đặt VLAN

1. Tạo VLAN (Đặt VLAN ID, đặt tên VLAN)
2. Gán VLAN cho port (VLAN membership)

Với trạng thái Access port thì chỉ cho 1 VLAN đi qua, cho nên để mang traffic của nhiều VLAN đi qua 1 link vật lý duy nhất, chúng ta có **Trunk**.

Ban đầu khi gói tin được đóng gói, sẽ không có bất kỳ thông tin nào về VLAN của gói tin đó. Và khi gói tin đi vào đường link trunk thì quá trình Trunk Encapsulation sẽ diễn ra.

Vậy Trunk Encapsulation là gì?

Đây là quá trình đóng gói những thông tin cần thiết để phân biệt các traffic của các VLAN khác nhau qua một liên kết vật lý duy nhất.

Hiện nay Trunk Encapsulation có hai chuẩn phổ biến là ISL (Inter-Switch Link) của Cisco và 802.1Q của IEEE.

ISL: Mỗi frame Ethernet sẽ được bọc trong một header ISL chứa thông tin về VLAN ID và các thông tin khác. Header này sẽ được thêm vào trước frame gốc và sau đó được gửi qua link trunk.

802.1q: Được sử dụng rộng rãi và được hỗ trợ nhiều thiết bị, VLAN ID được thêm vào frame Ethernet dưới dạng TAG 802.1Q. TAG này nằm giữa header Ethernet và dữ liệu của frame.

Nói qua một chút về VLAN TAG, đây là 802.1Q header được đóng vào Ethernet Frame chứa thông tin về VLAN ID để phân biệt các Frame khi đi qua trunk, và các Header sẽ bị gỡ đi ra khỏi link trunk ở đầu kia.

Khi thiết lập một liên kết trunk trên một thiết bị mang, quan trọng nhất là đảm bảo cả hai đầu liên kết đều sử dụng cùng một giao thức trunk encapsulation.

Sau khi đã chọn giao thức trunk encapsulation, chúng ta cần xác định mode trunk. Có hai mode trunk phổ biến:

❖ Static trunk: Mode on

Đây là trunk tĩnh do admin gán cho nhóm trunk. Các thành viên không trao đổi dữ liệu LACP và đây là loại trunk mặc định. Đường trunk tĩnh không yêu cầu hệ thống partner tổng hợp các cổng thành viên của nó

❖ DTP (Dynamic Trunk): Dynamic auto, Dynamic Desirable

Giao thức này sẽ tự động đàm phán để trở thành trunk link. Có hai mode trong giao thức này:

Dynamic auto: Nó sẽ trở thành port trunk dựa trên những DTP request từ neighbor switch.

Dynamic Desirable: Dạng port này sẽ thực hiện quá trình tương tác với neighbor switch thông qua DTP. Và port này sẽ trở thành trunk nếu port của switch neighbor của nó đã trở thành port trunk.

❖ **Tham số dùng để thiết lập trunk:**

switchport trunk encapsulation dot1q: Đóng gói theo chuẩn 802.1q và thông tin VLAN sẽ được thêm vào frame Ethernet sử dụng thẻ 802.1q để phân biệt giữa các VLAN.

switchport mode trunk: Đặt chế độ hoạt động thành mode trunk.

❖ **Sau khi thiết lập trunk, có hai tham số vận hành trên link trunk:**

- + VLAN allowed: Default Allow All trên 1 số dòng Switch Cisco
- + Native VLAN: Chứa các untag traffic.

❖ **Ngoài ra trong môi trường triển khai có một số yếu tố quan trọng khác:**

- VOICE VLAN: Dành riêng cho voice traffic để đánh dấu voice traffic => Cần phải có QoS để phân loại là đánh dấu.
- Inter VLAN: Định tuyến VLAN

❖ **Trong mô hình triển khai, quá trình cấu hình cần thực hiện ở 3 phía**

- + PC: Đặt IP và trả default gateway về VLAN tương ứng
- + Network trung gian (Switch): Chia VLAN và trunk về gateway và allow các VLAN cần thiết.

+Default gateway: Địa chỉ IP Gateway của VLAN để đi sang lớp mạng khác

2.2.2 OSPF

OSPF với tên gọi đầy đủ là Open Shortest Path First, đây là một giao thức dùng để định tuyến động sử dụng thuật toán Dijkstra để tìm ra đường đi ngắn nhất giữa các thiết bị định tuyến.

❖ **Một số ưu điểm của OSPF:**

- Độ hội tụ nhanh hơn RIP
- Quy mô triển khai lớn hơn
- Có thể chia các vùng định tuyến thành các area để dễ kiểm soát và quản lý traffic
- Network Segment và Link State giúp OSPF có thể xây dựng bảng định tuyến chi tiết và chính xác.

Trong OSPF, cost là một yếu tố quan trọng quyết định đường đi tối ưu. Quy tắc cơ bản là đường đi có cost thấp nhất (tức là băng thông cao nhất) được coi là đường đi tối ưu.

Cost của một đường đi được tính bằng cách ly băng thông tham chiếu (Reference Bandwidth) chia cho băng thông của đường đi đó.

Đơn vị của cost là stable và băng thông tham chiếu thường được thiết lập mặc định là 100Mbps.

Đường đi với cost thấp nhất sẽ được chọn làm đường đi chính. Nếu có nhiều đường đi có cost bằng nhau, OSPF có thể thực hiện load balancing giữa chúng, được gọi là Equal Cost (Path) Load Balancing.

Load Balancing xảy ra khi các đường đi có Administrative Distance (AD) và Metric (cost) bằng nhau, trong trường hợp này, các gói dữ liệu sẽ được phân phối đều giữa các đường đi tương đồng.

Một số cost trong interface:

Giga Ethernet interface 1gbps = 1 cost

fast ethernet interface = 1 cost

Ethernet interface 10mbps = 10 cost

DSL1 (1544 Mbps) = 64 cost

DSL2 (768 Kbps)= 133 cost

❖ Router chạy OSPF có 5 loại packet sau:

- Hello Packet: Là các gói mà các router sẽ dùng để gửi cho nhau để xác định xem các thiết bị lân cận của nó còn hoạt động hay không
- Database Description Packet
- Link-state request packet (Yêu cầu những thông tin còn thiếu)
- Link-state update packet (Chứa thông tin cập nhật về LSAs)
- Link-state acknowledgment packet (Xác nhận việc gửi thành công 1 gói tin link-state)

Mục đích: Khám phá các router lân cận, láng giềng với nó. Dùng 5 gói này để trao đổi thông tin với nhau với mục đích duy trì mạng ổn định.

❖ 3 loại OSPF Database

- Neighbor table: Lưu các thông tin về router lân cận sau khi đã trao đổi gói hello, được cập nhật khi các router thiết lập Adjacency.
- Link-state Database: Lưu trữ thông tin chi tiết về các LSAs mà router nhận được.
- Forwarding database: Dùng để xây dựng bảng forward để lựa chọn đường đi.

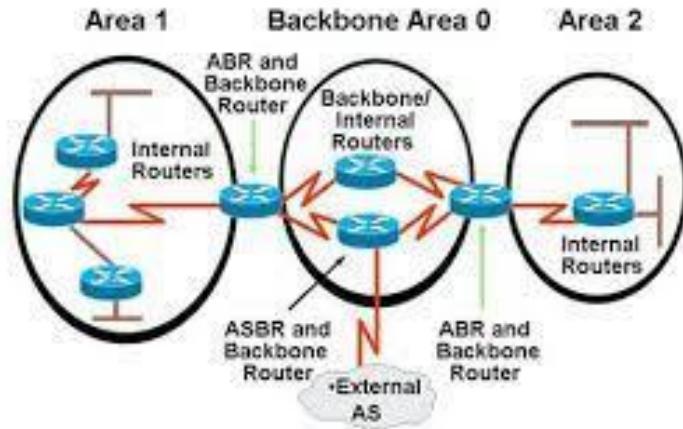
❖ Các bước của thuật toán OSPF

1. Thiết lập các vùng lân cận: Gửi gói hello đến tất cả interface
2. Trao đổi thông tin quảng bá lẫn nhau: Trao đổi các LSA để cập nhật thông tin định tuyến
3. Xây dựng 1 database: Từ các LSAs nhận được, router xây dựng thành link-state Database
4. Thực thi thuật toán SPF để tìm đường đi (Shortest Path First)
5. Chọn đường đi ngắn nhất: Dựa trên kết quả của thuật toán SPF, router sẽ chọn đường đi tối ưu.

OSPF thường chia mạng thành các vùng giúp quản lý mạng một cách hiệu quả.

Có hai loại vùng chính:

- o single area: Các router ở cùng 1 vùng (tốt nhất là area 0)
- o multi area: Phân cấp các vùng, các router phải kết nối với backbone area 0



Hình 2.2.2.1: Một số OSPF Concept

Trong OSPF, việc bầu chọn DR(Designated Router) và BDR(Backup Designated Router) rất quan trọng để tránh mạng bị flood LSAs. Quy tắc bầu chọn theo thứ tự như sau:

1. Priority cao nhất (0-255)
2. Router-ID cao nhất
3. IP address cao nhất của loopback hoặc Active Interface: Nếu priority và router-id đều giống nhau, thì router có IP address cao nhất của loopback hoặc active interface sẽ được chọn làm DR hoặc BDR. IP loopback thường được ưu tiên hơn các interface khác.

❖ Một số trạng thái hoạt động của OSPF

1. Down: Không có gói hello được nhận
2. Init State: Gửi gói hello, router sẽ set trường Active Neigbor trong bản tin Hello gửi ra = Router-id và chuyển vào trạng thái hai chiều
3. Two-way state: 2 router song hành với nhau và bắt đầu trao đổi thông tin liên kết, trong giai đoạn này router thường bầu chọn DR và BDR.
4. Exstart State: Trên mạng point to point, 2 router sẽ quyết định router nào là Master/Slave sau khi hoàn thành trao đổi gói BDR.

5. Exchange: Thực hiện trao đổi thông tin

6. Loading State: LSR và LSU được sử dụng để có thông tin bổ sung, nếu không có thay đổi thì chuyển sang full state

7. Full state: Ở trạng thái này, các router đã có đầy đủ thông tin về database của nhau. Các router tiếp tục gửi gói tin hello để tìm kiếm hàng xóm mới và duy trì kết nối với hàng xóm cũ, khi có thông tin về LSA mới, router sẽ thực hiện cập nhật cho hàng xóm thông qua LS update.

2.2.3 SNMP

SNMP, hay Simple Network Management Protocol, là một giao thức ứng dụng được IAB định nghĩa trong RFC1157 để trao đổi thông tin quản lý giữa các thiết bị mạng, phát triển như một phần của mạng TCP/IP.

SNMP là một trong những giao thức mạng được sử dụng phổ biến để quản lý và giám sát các thành phần mạng. Hầu hết các thiết bị mạng được trang bị SNMP Agent, các agent này cần được kích hoạt và cấu hình để có thể giao tiếp với các công cụ giám sát mạng hoặc hệ thống quản lý mạng.

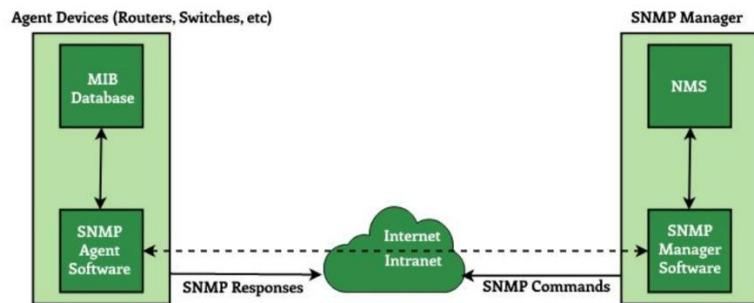
❖ Các thành phần của SNMP

SNMP Manager: Là hệ thống trung tâm dùng để giám sát và quản lý các thiết bị mạng. Nó có khả năng truy cập và điều khiển thông tin từ SNMP Agent trên các thiết bị mạng.

SNMP Agent: Là phần mềm chạy trên các thiết bị mạng, cho phép các thiết bị này trao đổi thông tin với các client thông qua giao thức SNMP. Thông thường, SNMP Agent chứa thông tin về trạng thái hoạt động của thiết bị như CPU, bộ nhớ, băng thông, và tình trạng kết nối.

❖ Cơ chế hoạt động:

SNMP Architecture



Hình 2.2.3^[11]: Cơ chế hoạt động của SNMP

- SNMP sử dụng một số lệnh cơ bản để giao tiếp giữa manager và agent.
- GET: Yêu cầu thông tin bất cứ lúc nào.
- SET: Điều khiển thiết bị từ xa.
- TRAP: Là thông điệp phổ biến nhất, dùng để thông báo cho SNMP Manager về các sự kiện quan trọng như lỗi mạng hoặc cảnh báo mạng.
- INFORM: Một loại thông điệp khác dùng để thông báo cho SNMP về các sự kiện quan trọng như khắc phục lỗi mạng hoặc báo cáo tình trạng mạng.
- SNMPWALK: Nhận tất cả dữ liệu.

Trong quá trình hoạt động, SNMP Manager tạo yêu cầu và chuyển đến SNMP Agent, sau đó xác thực và xử lý yêu cầu trước khi trả kết quả về cho SNMP Manager thông qua PDU Response. Dữ liệu được tổ chức theo MIB (Management Information Base) và được truyền qua giao thức SNMP.

❖ Mối liên hệ giữa SNMP và Zabbix

SNMP và Zabbix là hai công nghệ được sử dụng phổ biến trong việc giám sát mạng. Trong đó, Zabbix có khả năng sử dụng SNMP để thu thập thông tin từ các thiết bị mạng. Bên cạnh đó, SNMP cung cấp dữ liệu thô cho Zabbix để xử lý và phân tích, từ đó Zabbix sử dụng để tạo báo cáo, đồ thị và cảnh báo.

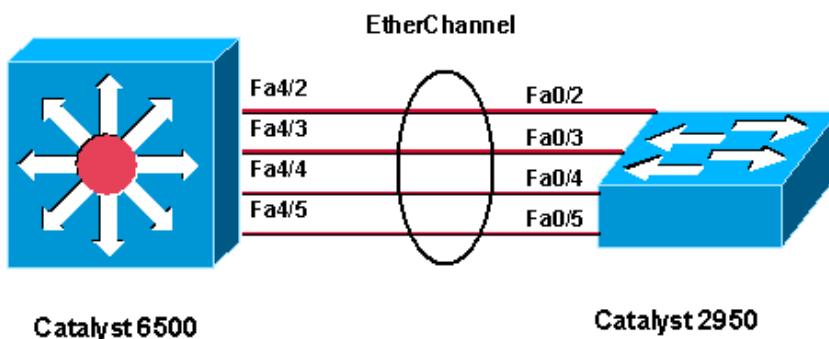
❖ **Sự kết hợp SNMP và Zabbix đã mang lại một số lợi ích:**

- Giám sát toàn diện: Zabbix có thể thu thập dữ liệu từ nhiều thiết bị mạng bằng SNMP.
- Khả năng mở rộng: Zabbix có thể hỗ trợ nhiều thiết bị và mạng lớn.
- Linh hoạt: Zabbix có thể được cấu hình để giám sát các thông số cụ thể.
- Dễ sử dụng: Zabbix có giao diện web trực quan để quản lý và giám sát.

2.3 Tính dự phòng trong hệ thống

2.3.1 Ethernet Channel

EtherChannel là một kỹ thuật nhóm hai hay nhiều đường kết nối truyền tải dữ liệu vật lý thành một đường ảo duy nhất có Port ảo thậm chí cả MAC ảo nhằm mục đích tăng tốc độ truyền dữ liệu và tăng khả năng dự phòng cho hệ thống. Nếu một trong các link thuộc EtherChannel bị down thì traffic sẽ tự động được chuyển sang link khác trong channel chỉ trong vòng vài milliseconds. Khi link up trở lại thì traffic được phân bổ lại như cũ.



Hình 2.3.1.1^[9]: Công nghệ Ethernet Channel

❖ **EthernetChannel bao gồm hai loại giao thức:**

LACP (Link Aggregation Control Protocol): Đây là giao thức theo chuẩn quốc tế IEEE 802.3ad và có thể dùng được cho hầu hết các thiết bị thuộc các hãng khác nhau, LACP hỗ trợ ghép tối đa 16 link logical (8 port Active – 8 port Passive).

- Có 3 chế độ
 - On: mode cấu hình tĩnh, nhưng thường không được dùng vì có thể dẫn đến khả năng loop cao và bị STP Block.
 - Active: mode tự động thương lượng với thiết bị đối tác
 - Passive: mode bị động – Chờ được thương lượng

PagP (Port Aggregation Protocol): là giao thức độc quyền của Cisco và chỉ hỗ trợ ghép tối đa 8 link vật lý thành 1 link luận lý.

Tương tự cũng có ba chế độ như LACP

❖ Để cấu hình Ethernet Channel ta sử dụng câu lệnh sau:

LACP

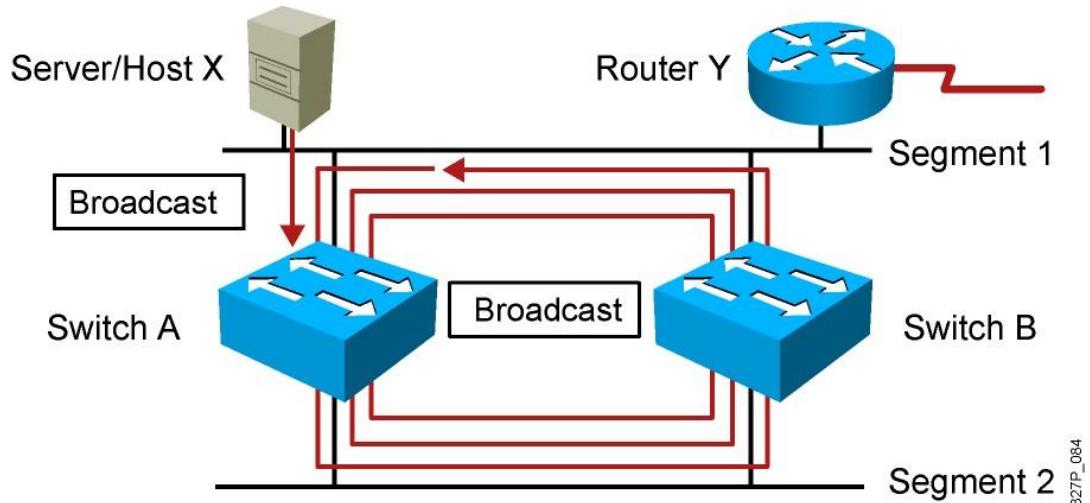
```
interface range GigabitEthernet0/1 - 2
channel-protocol lacp
channel-group 1 mode active/passive/desirable
```

PAgP

```
interface range GigabitEthernet0/1 - 2
channel-group 1 mode desirable/auto
```

2.3.2 Spanning Tree

Spanning Tree Protocol(STP) là một giao thức được sử dụng để ngăn chặn vòng lặp trong các mạng có cấu trúc cây. Mục tiêu chính của STP là đảm bảo rằng chỉ có một đường dẫn hoạt động giữa các thiết bị mạng, tránh tình trạng lặp.



Hình 2.3.2.1^[10]: Giao thức STP

Như hình trên ta có thể thấy hai switch được kết nối theo vòng khép kín và xảy ra hiện tượng lặp. Do đó, IEEE đưa ra chuẩn 802.1D (STP) để chống lặp theo cơ chế block 1 port. Và để tìm ra block port sẽ cần phải trải qua các bước:

- Bầu chọn Root Switch: Mỗi Switch trong mạng sẽ có địa chỉ MAC và Default Priority. Root Bridge sẽ dành cho Switch có Priority và địa chỉ MAC thấp nhất.
- Bầu chọn Root port: Mỗi cổng trên mỗi switch sẽ tính toán chi phí đường dẫn (Path cost) đến Root Bridge. Và cổng có path cost thấp nhất đến Root Bridge sẽ được chọn làm Root Port.
- Bầu chọn Designated port: Trên mỗi segment của mạng, một switch được chọn làm Designated Bridge và một cổng trên switch này được chọn làm Designated Port – cổng có chiều dài đường dẫn ngắn nhất đến Root Bridge trên segment đó.
- Port còn lại là Altermated port

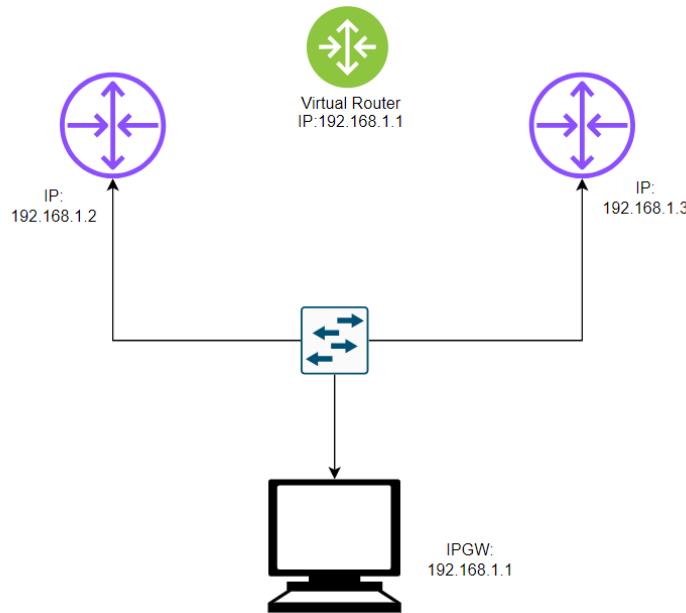
Nguyên tắc tính tổng path-cost: tính từ Root-Switch → switch đang muốn tính:

- Đi ra: không cộng
- Đi vào: cộng cost

2.3.3 VRRP

VRRP – Virtual Router Redundancy Protocol, là một giao thức được dùng để dự phòng cho các router hoặc gateway. Mục tiêu của VRRP là duy trì một địa chỉ IP và một MAC address ảo nhằm đảm bảo rằng mạng vẫn hoạt động khi một trong những hai Switch gặp sự cố.

HSRP, hay còn gọi là Hot Standby Router Protocol, cũng có công dụng tương tự VRRP nhưng HSRP là giao thức riêng của các thiết bị Cisco, trong khi đó VRRP lại là giao thức quốc tế có thể chạy trên nhiều sản phẩm của nhiều nhà sản xuất khác nhau.



Hình 2.3.3: Ví dụ về VRRP

Giả sử chúng ta có một topology đơn giản như sau với 2 router chạy song song, thì nhiệm vụ của VRRP sẽ là chọn một Router làm nhiệm vụ Master và một router là Backup, và cũng tương tự như HSRP, router có priority cao nhất sẽ được chỉ định làm Master. Ngoài ra, chúng ta cũng cần thiết lập một địa chỉ IP gateway ảo cho hai Router với cùng một IP 192.168.1.1.

Giá trị mặc định của VRRP cho hello-timer là 1 giây và hold-timer là 3 giây. Hello-timer là thời gian giữa các gói tin hello được gửi đi và hold-timer là thời gian mà một router sẽ chờ trước khi xác định rằng router kia không còn hoạt động.

❖ Cơ chế bầu chọn Master/Backup của VRRP

- Priority (default 100): Router nào có priority cao hơn sẽ được bầu chọn làm Master.
- Nếu hai router có cùng Priority, thì router có địa chỉ IP cao hơn sẽ được bầu chọn làm Master.
- Preempt (mặc định sẽ không bật): Nếu bật preempt thì router Master ban đầu (có priority cao hơn, IP cao hơn) sẽ chiếm lại quyền Master khi nó quay trở lại.

Giả sử nếu muốn R0 đóng vai trò Master, chúng ta sẽ đặt priority của R0 là 110 và R1 là 90, từ đó R0 sẽ đứng lên và đóng vai trò Master.

Về cơ bản, các host trong LAN sẽ dùng ARP để lấy MAC của default gateway (ở đây là Virtual IP) và MAC của Virtual sẽ được lưu trong bảng ARP và tất cả những gói tin nào đi ra ngoài thì đều có MAC đích là MAC của Virtual IP.

Router nào là Router Master sẽ chiếm quyền sử dụng thông tin của Virtual Router để trả lời lại ARP Request từ client. Switch cũng đồng thời học Virtual MAC trên cổng nối với Router Master.

❖ Khi Router Master down:

- Virtual Mac sẽ bị loại bỏ
- Router Backup sẽ chờ gói hello từ Master trong khoảng thời gian Holdtime
- Khi hết Holdtime mà không nhận được gói Hello thì Router Backup sẽ mặc định cho rằng Master đã down và Router backup sẽ chiếm quyền Master.
- Thông tin về gateway trên client là không thay đổi nhưng switch sẽ update entry trên cổng kết nối với router mới trở thành Master.

Quá trình chuyển đổi từ Master sang Backup sẽ diễn ra tự động và không ảnh hưởng đến kết nối của các host trong mạng LAN. Sau khi chuyển đổi, Router Backup sẽ sử dụng Virtual MAC và IP Address của router Master.

❖ Hạn chế của VRRP

- Lãng phí tài nguyên: VRRP sử dụng cơ chế Master/Backup tức là chỉ dùng 1 thiết bị, nếu thiết bị Master không lỗi thì thiết bị Backup sẽ không bao giờ sử dụng.
⇒ Để khắc phục điểm yếu này, ta có thể chia vai trò Master ra nếu có nhiều group.
- Khả năng phát hiện lỗi: Chỉ phát hiện lỗi ở phần LAN, nếu đứt đường truyền ở uplink hoặc sâu trong mạng ISP thì Master Router mất mạng nhưng vẫn giữ quyền Master.
- Hiệu suất: Có thể ảnh hưởng đến hiệu suất mạng do việc trao đổi thông tin hello và các hoạt động dự phòng.

2.4 Máy chủ

2.4.1 DNS và Alternative DNS

DNS - Domain Name System là một hệ thống phân giải tên miền bao gồm cả TCP/IP. DNS là then chốt trong việc duyệt web, mail,... Mỗi thiết bị kết nối với Internet có một địa chỉ IP duy nhất để xác định trong hệ thống mạng, tuy nhiên nó rất khó nhớ. Vì vậy, DNS sẽ giúp phân giải các địa chỉ IP trên thành những tên miền dễ nhớ (chẳng hạn như *google.com*).

- **Phân giải tên miền:** Khi bạn nhập một tên miền vào trình duyệt web, trình duyệt sẽ gửi một truy vấn đến máy chủ DNS. Máy chủ DNS sẽ tìm kiếm bản ghi DNS cho tên miền đó và trả về địa chỉ IP tương ứng.
- **Các loại bản ghi DNS:** Có nhiều loại bản ghi DNS khác nhau, mỗi loại cung cấp một loại thông tin khác nhau về tên miền. Các loại bản ghi DNS phổ biến bao gồm A, AAAA, CNAME, MX và NS.
- **Máy chủ DNS:** Máy chủ DNS là máy tính lưu trữ thông tin về các bản ghi DNS. Máy chủ DNS được tổ chức theo hệ thống phân cấp, với các máy chủ DNS cấp cao nhất lưu trữ thông tin về các tên miền cấp cao

nhất (như .com, .net, .org) và các máy chủ DNS cấp thấp hơn lưu trữ thông tin về các tên miền phụ.

Alternative DNS hay còn gọi là DNS thay thế, là một thuật ngữ mà người ta sử dụng để ám chỉ các dịch vụ DNS khác nhau mà người dùng có thể sử dụng thay vì sử dụng DNS mặc định được cấu hình bởi nhà cung cấp dịch vụ Internet (ISP). Sử dụng Alternative DNS có thể mang lại một số lợi ích như:

- **Tăng tốc độ truy cập:** Alternative DNS có thể có cơ sở hạ tầng mạng tốt hơn và ít bị tắc nghẽn hơn so với máy chủ DNS của ISP, dẫn đến tốc độ truy cập trang web nhanh hơn.
- **Tăng cường bảo mật:** Alternative DNS có thể cung cấp các tính năng bảo mật bổ sung như mã hóa DNS, giúp bảo vệ bạn khỏi các cuộc tấn công lừa đảo và theo dõi.
- **Bỏ chặn nội dung:** Một số Alternative DNS có thể giúp bạn bỏ chặn các trang web bị chặn bởi ISP hoặc chính phủ.

2.4.2 Active Directory Domain Service

Active Directory Domain Service (AD DS) là dịch vụ thư mục cho phép quản trị viễn mạng quản lý tập trung các tài nguyên mạng, bao gồm người dùng, máy tính, nhóm, thiết bị và các dịch vụ. AD DS được sử dụng rộng rãi trong các môi trường Windows Server và là một phần quan trọng của cơ sở hạ tầng CNTT cho nhiều tổ chức.

❖ **Dưới đây là một số khái niệm cơ bản về AD DS:**

- **Domain:** Là tập hợp các đối tượng (người dùng, máy tính, nhóm, v.v.) chia sẻ cùng một cơ sở dữ liệu AD DS và chính sách bảo mật.
- **Forest:** Là tập hợp các domain được liên kết với nhau bằng mối quan hệ tin cậy.
- **Tree:** Là tập hợp các domain được liên kết với nhau theo cấu trúc phân cấp.

- **Schema:** Là tập hợp các định nghĩa cho các đối tượng và thuộc tính có thể được lưu trữ trong AD DS.
 - **Global Catalog:** Là bản sao đầy đủ của tất cả các đối tượng trong một forest.
 - **Domain Controller:** Là máy chủ lưu trữ cơ sở dữ liệu AD DS và cung cấp dịch vụ xác thực, ủy quyền và quản lý cho các đối tượng trong domain.
- ❖ **AD DS cung cấp một số lợi ích cho các tổ chức, bao gồm:**
- **Quản lý tập trung:** Cho phép quản trị viên quản lý tất cả các tài nguyên mạng từ một vị trí trung tâm.
 - **Bảo mật nâng cao:** Cung cấp các tính năng bảo mật mạnh mẽ để bảo vệ tài nguyên mạng khỏi truy cập trái phép.
 - **Khả năng mở rộng:** Có thể mở rộng để hỗ trợ số lượng lớn người dùng, máy tính và các thiết bị.
 - **Tích hợp:** Tích hợp với nhiều ứng dụng và dịch vụ khác nhau.
- ❖ **Dưới đây là một số trường hợp sử dụng phổ biến của AD DS:**
- **Xác thực người dùng:** Cho phép người dùng đăng nhập vào mạng và truy cập các tài nguyên mạng.
 - **Ủy quyền truy cập:** Cho phép quản trị viên kiểm soát người dùng nào có thể truy cập các tài nguyên mạng nào.
 - **Quản lý nhóm:** Cho phép quản trị viên tạo và quản lý các nhóm người dùng để đơn giản hóa việc quản lý quyền truy cập.
 - **Quản lý máy tính:** Cho phép quản trị viên cài đặt phần mềm, cập nhật và vá lỗi cho các máy tính trong mạng.
 - **Khôi phục dữ liệu:** Cho phép quản trị viên khôi phục dữ liệu bị mất hoặc bị hỏng.

2.4.3 DHCP

Dynamic Host Configuration Protocol - DHCP là giao thức mạng được sử dụng để tự động cấp phát địa chỉ IP cho các thiết bị trên mạng.

Máy chủ DHCP: Máy chủ DHCP là máy chủ lưu trữ một pool địa chỉ IP và chịu trách nhiệm cấp phát địa chỉ IP cho các thiết bị yêu cầu.

Cấu hình DHCP: Quản trị viên mạng có thể cấu hình máy chủ DHCP để xác định phạm vi địa chỉ IP, thời gian thuê địa chỉ IP và các tùy chọn khác.

❖ **Quá trình cấp phát địa chỉ IP:**

- Khi một thiết bị khởi động, nó sẽ gửi một gói tin **DHCP DISCOVER** để tìm kiếm máy chủ DHCP.
- Máy chủ DHCP sẽ trả lời bằng một gói tin **DHCP OFFER**, cung cấp một địa chỉ IP cho thiết bị.
- Thiết bị sẽ gửi một gói tin **DHCP REQUEST** để chấp nhận địa chỉ IP.
- Máy chủ DHCP sẽ xác nhận địa chỉ IP cho thiết bị.

Cổng DHCP là cổng UDP 67 được sử dụng bởi máy chủ DHCP và các thiết bị để giao tiếp với nhau. Khi một thiết bị khởi động, nó sẽ gửi một gói tin DHCP DISCOVER trên cổng 67 để tìm kiếm máy chủ DHCP. Máy chủ DHCP sẽ trả lời bằng một gói tin DHCP OFFER, cũng được gửi trên cổng 67. Thiết bị sau đó sẽ gửi một gói tin DHCP REQUEST để chấp nhận địa chỉ IP, cũng được gửi trên cổng 67.

❖ **Lợi ích của DHCP:**

- **Tự động hóa:** DHCP tự động hóa quá trình cấp phát địa chỉ IP, giúp giảm bớt gánh nặng cho quản trị viên mạng.
- **Hiệu quả:** DHCP giúp sử dụng hiệu quả pool địa chỉ IP bằng cách thu hồi địa chỉ IP không sử dụng.
- **Khả năng mở rộng:** DHCP có thể hỗ trợ số lượng lớn thiết bị trên mạng.

❖ **Nhược điểm của DHCP:**

- **Phụ thuộc vào máy chủ:** Mạng phụ thuộc vào máy chủ DHCP để cấp phát địa chỉ IP. Nếu máy chủ DHCP gặp sự cố, các thiết bị sẽ không thể truy cập mạng.
- **Bảo mật:** DHCP có thể là mục tiêu tấn công mạng.

2.4.4 ADCS và NPAS

AD CS – Active Directory Certificate Services là dịch vụ cung cấp cơ sở hạ tầng cho phép tổ chức phát hành, quản lý và thu hồi chứng chỉ số hóa. Chứng chỉ số hóa được sử dụng để xác thực người dùng, máy tính và thiết bị, cũng như mã hóa dữ liệu và bảo mật giao tiếp.

❖ **Thành phần:**

- **Máy chủ ADCS:** Máy chủ lưu trữ cơ sở dữ liệu chứng chỉ và cung cấp các dịch vụ ADCS.
- **Cơ sở dữ liệu chứng chỉ:** Lưu trữ thông tin về các chứng chỉ được phát hành bởi ADCS.
- **Chính sách cấp phát chứng chỉ:** Xác định các quy tắc và điều kiện cho việc phát hành chứng chỉ.
- **Gói đăng ký chứng chỉ:** Định nghĩa các thuộc tính và cài đặt cho các chứng chỉ được phát hành.
- **Cơ quan đăng ký chứng chỉ:** Chịu trách nhiệm phát hành và quản lý chứng chỉ.

❖ **Quá trình hoạt động:**

- **Yêu cầu chứng chỉ:** Người dùng hoặc thiết bị yêu cầu chứng chỉ từ ADCS.
- **Xác thực:** ADCS xác thực danh tính của người dùng hoặc thiết bị.
- **Cấp phát chứng chỉ:** ADCS phát hành chứng chỉ cho người dùng hoặc thiết bị.

- **Lưu trữ chứng chỉ:** Chứng chỉ được lưu trữ trên máy chủ ADCS hoặc trong kho lưu trữ chứng chỉ.
- **Quản lý chứng chỉ:** ADCS cung cấp các công cụ để quản lý vòng đời của chứng chỉ, bao gồm gia hạn, thu hồi và phân phối.

❖ **Lợi ích:**

- **Tăng cường bảo mật:** ADCS giúp bảo vệ tổ chức khỏi các cuộc tấn công mạng bằng cách cung cấp xác thực mạnh mẽ và mã hóa dữ liệu.
- **Tuân thủ quy định:** ADCS có thể giúp tổ chức tuân thủ các quy định yêu cầu xác thực mạnh mẽ và mã hóa dữ liệu.
- **Tăng hiệu quả:** ADCS có thể giúp tổ chức tự động hóa các quy trình quản lý chứng chỉ.

❖ **NPAS là dịch vụ cung cấp các tính năng bảo mật và truy cập mạng, bao gồm:**

- **Mạng riêng ảo (VPN):** NPAS cho phép người dùng truy cập mạng an toàn từ xa.
- **Mạng Wi-Fi được bảo vệ:** NPAS cho phép tổ chức triển khai mạng Wi-Fi an toàn với xác thực và mã hóa dữ liệu.
- **Quản lý truy cập mạng (NAC):** NPAS cho phép tổ chức kiểm soát truy cập vào mạng dựa trên danh tính người dùng và trạng thái thiết bị.

❖ **Thành phần:**

- **Máy chủ NPAS:** Máy chủ lưu trữ các dịch vụ NPAS.
- **Cơ sở dữ liệu NPS:** Lưu trữ thông tin về người dùng, thiết bị, chính sách và cấu hình NPAS.
- **Chính sách mạng:** Xác định các quy tắc và điều kiện cho phép truy cập mạng.

- **Máy chủ RADIUS:** Cung cấp dịch vụ xác thực và ủy quyền cho các thiết bị truy cập mạng.

❖ **Quá trình hoạt động:**

- **Yêu cầu truy cập mạng:** Người dùng hoặc thiết bị yêu cầu truy cập mạng.
- **Xác thực:** NPAS xác thực danh tính của người dùng hoặc thiết bị.
- **Ủy quyền:** NPAS xác định xem người dùng hoặc thiết bị có được phép truy cập mạng hay không.
- **Cấp quyền truy cập:** NPAS cấp quyền truy cập mạng cho người dùng hoặc thiết bị.

❖ **Lợi ích:**

- **Tăng cường bảo mật:** NPAS giúp bảo vệ tổ chức khỏi các cuộc tấn công mạng bằng cách cung cấp xác thực mạnh mẽ, mã hóa dữ liệu và kiểm soát truy cập mạng.
- **Tăng hiệu quả:** NPAS có thể giúp tổ chức tự động hóa các quy trình quản lý truy cập mạng.
- **Tuân thủ quy định:** NPAS có thể giúp tổ chức tuân thủ các quy định yêu cầu xác thực mạnh mẽ và kiểm soát truy cập mạng.

2.4.5 FTP Server

Dịch vụ FTP (File Transfer Protocol) là một dịch vụ mạng cho phép người dùng truyền tải tập tin giữa máy tính và máy chủ FTP. Dịch vụ này sử dụng giao thức FTP để truyền tải dữ liệu.

Giao thức FTP (File Transfer Protocol) là một giao thức mạng được sử dụng để truyền tải tập tin giữa máy tính và máy chủ FTP. Giao thức này hoạt động dựa trên mô hình client-server, trong đó máy tính được gọi là client sẽ kết nối với máy chủ FTP để truyền tải tập tin.

❖ **Cách thức hoạt động của FTP:**

- **Kết nối:** Client sẽ kết nối với máy chủ FTP bằng cách sử dụng cổng **21** (cổng FTP mặc định).
- **Xác thực:** Client sẽ cung cấp tên đăng nhập và mật khẩu để xác thực với máy chủ FTP.
- **Truyền tải tập tin:** Sau khi xác thực thành công, client có thể truyền tải tập tin lên hoặc tải tập tin xuống từ máy chủ FTP.
- **Kết thúc:** Khi việc truyền tải tập tin hoàn tất, client sẽ ngắt kết nối với máy chủ FTP.

❖ **Các loại FTP:**

- **FTP Plain:** Đây là loại FTP cơ bản nhất, không sử dụng mã hóa dữ liệu.
- **FTP over SSL (FTPS):** Loại FTP này sử dụng mã hóa SSL để bảo mật dữ liệu truyền tải.
- **FTP over SSH (SFTP):** Loại FTP này sử dụng SSH để bảo mật dữ liệu truyền tải.

❖ **Lợi ích của FTP:**

- **Dễ sử dụng:** FTP là một giao thức đơn giản và dễ sử dụng.
- **Khả năng tương thích:** FTP được hỗ trợ bởi hầu hết các hệ điều hành và máy tính.
- **Hiệu quả:** FTP có thể truyền tải tập tin dung lượng lớn một cách hiệu quả.

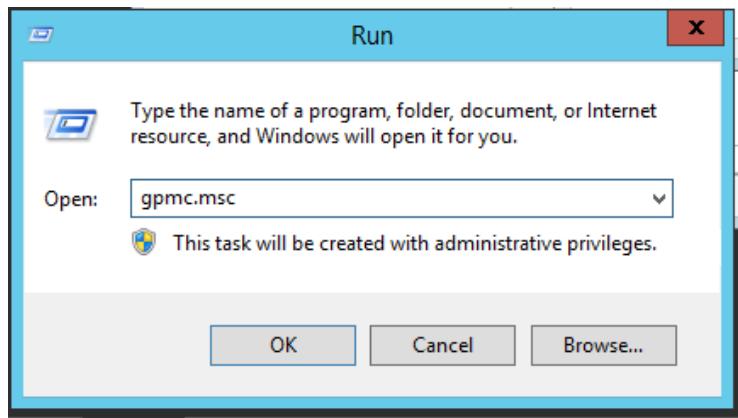
❖ **Nhược điểm của FTP:**

- **Bảo mật:** FTP Plain không sử dụng mã hóa dữ liệu, do đó không an toàn để truyền tải dữ liệu nhạy cảm.
- **Tốc độ:** Tốc độ truyền tải tập tin của FTP có thể bị ảnh hưởng bởi nhiều yếu tố, như băng thông mạng và độ trễ.

2.4.6 Group Policy Management

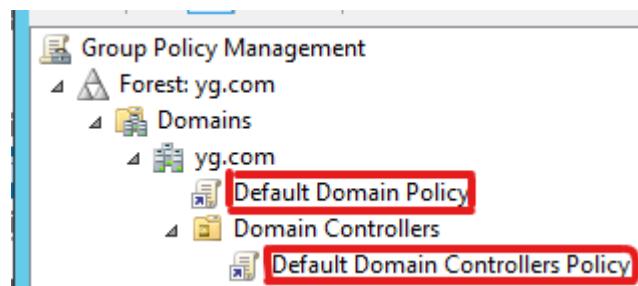
Group Policy là tập hợp các rules nhằm kiểm soát môi trường làm việc của nhân viên trong môi trường Domain. Group Policy giúp kiểm soát được user có thể làm gì và không được làm gì trên hệ thống máy tính.

Để mở GPO, chúng ta sẽ sử dụng tổ hợp phím Windows + R để mở hộp thoại Run và nhập lệnh gpmc.msc



Hình 2.4.7.1: Mở GPO

Trong GPO sẽ có 2 chính sách mặc định là Default Domain Controller Policy (áp dụng cho DC), Default Domain Policy(Áp dụng cho toàn hệ thống).



Hình 2.4.7.2: Hai Policy mặc định của hệ thống

Trong cùng 1 OU nếu áp chung 2 policy (không Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn. Nếu áp chung 2 policy (cả 2 policy đều Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn. Nếu áp chung 2 policy (1 policy Enforce và 1 policy không Enforce) thì policy Enforce sẽ có độ ưu tiên cao hơn.

2.5 Bảo mật trong hệ thống

2.5.1 Network Access Control

Network Access Control (NAC) là một hệ thống quản lý và kiểm soát quyền truy cập vào mạng, nhằm bảo vệ mạng khỏi các truy cập trái phép và các mối đe dọa an ninh mạng. NAC hoạt động bằng cách xác định, ủy quyền và kiểm soát các thiết bị và người dùng truy cập vào mạng.

❖ Lợi ích của NAC:

- **Tăng cường bảo mật:** NAC giúp bảo vệ mạng khỏi các truy cập trái phép, các cuộc tấn công mạng và các phần mềm độc hại.
- **Tuân thủ quy định:** NAC giúp tổ chức tuân thủ các quy định về bảo mật dữ liệu và an ninh mạng.
- **Giảm chi phí:** NAC giúp giảm chi phí cho việc bảo mật mạng bằng cách tự động hóa các quy trình quản lý truy cập và ngăn chặn các vi phạm an ninh mạng.

❖ Cách thức hoạt động của NAC:

- Xác định: NAC sử dụng các phương pháp khác nhau để xác định các thiết bị và người dùng truy cập vào mạng, bao gồm:
- Địa chỉ MAC: NAC có thể xác định các thiết bị dựa trên địa chỉ MAC duy nhất của chúng.
- Chứng chỉ: NAC có thể xác định các thiết bị và người dùng dựa trên các chứng chỉ số hóa.
- Tên miền và mật khẩu: NAC có thể xác định người dùng dựa trên tên miền và mật khẩu của họ.
- Ủy quyền: Sau khi xác định được thiết bị hoặc người dùng, NAC sẽ ủy quyền cho họ truy cập vào mạng dựa trên các chính sách được định nghĩa. Các chính sách này có thể dựa trên:
 - Loại thiết bị

- Nhóm người dùng
- Vị trí truy cập
- Mức độ bảo mật của thiết bị
- Kiểm soát: NAC có thể kiểm soát quyền truy cập của các thiết bị và người dùng vào mạng bằng cách:
 - Cấp quyền truy cập đầy đủ
 - Cấp quyền truy cập hạn chế
 - Chặn truy cập

❖ **Các thành phần chính của NAC:**

- **Máy chủ NAC:** Máy chủ NAC là trung tâm của hệ thống NAC. Máy chủ NAC lưu trữ các chính sách truy cập, thông tin về thiết bị và người dùng, và các bản ghi nhật ký.
- **Thiết bị NAC:** Thiết bị NAC là các thiết bị được sử dụng để thực thi các chính sách NAC. Các thiết bị NAC có thể bao gồm:
 - Bộ định tuyến
 - Bộ chuyển mạch
 - Tường lửa
- **Phần mềm NAC:** Phần mềm NAC là phần mềm được cài đặt trên máy chủ NAC để quản lý và điều khiển hệ thống NAC.

❖ **Các loại NAC:**

- **NAC dựa trên mạng:** Loại NAC này sử dụng các thiết bị mạng để thực thi các chính sách NAC.
- **NAC dựa trên máy chủ:** Loại NAC này sử dụng phần mềm NAC được cài đặt trên máy chủ để thực thi các chính sách NAC.
- **NAC dựa trên đám mây:** Loại NAC này sử dụng dịch vụ đám mây để thực thi các chính sách NAC.

2.5.2 Access Control List

Access Control List (ACL) là một danh sách các quy tắc được sử dụng để kiểm soát quyền truy cập vào các tài nguyên mạng, chẳng hạn như tập tin, thư mục, máy tính và mạng. ACL xác định các đối tượng nào được phép truy cập vào tài nguyên và loại truy cập nào được phép (ví dụ: đọc, ghi, thực thi).

❖ **Lợi ích của ACL:**

- **Tăng cường bảo mật:** ACL giúp bảo vệ các tài nguyên mạng khỏi truy cập trái phép.
- **Kiểm soát chi tiết:** ACL cho phép bạn kiểm soát chi tiết ai có thể truy cập vào tài nguyên và loại truy cập nào được phép.
- **Tuân thủ quy định:** ACL có thể giúp bạn tuân thủ các quy định về bảo mật dữ liệu.

❖ **Cách thức hoạt động của ACL:**

- **Xác định đối tượng:** Khi một người dùng hoặc thiết bị truy cập vào một tài nguyên mạng, ACL sẽ xác định đối tượng đó là ai.
- **Kiểm tra quyền truy cập:** ACL sẽ kiểm tra xem đối tượng đó có được phép truy cập vào tài nguyên hay không.
- **Cho phép hoặc từ chối truy cập:** Nếu đối tượng được phép truy cập vào tài nguyên, ACL sẽ cho phép truy cập. Nếu đối tượng không được phép truy cập vào tài nguyên, ACL sẽ từ chối truy cập.

Có hai loại ACL chính: ACL standard và ACL extended.

❖ **ACL Standard**

Cấu trúc: Gồm các mục (entry) xác định địa chỉ IP nguồn và loại truy cập được phép (cho phép hoặc từ chối).

Tính năng:

- Chỉ kiểm soát dựa trên địa chỉ IP nguồn.
- Không hỗ trợ các giao thức cụ thể hoặc cổng TCP/UDP.
- Dễ cấu hình và quản lý.

Ứng dụng: Thích hợp cho các mạng đơn giản hoặc để kiểm soát truy cập cơ bản.

❖ **ACL Extended:**

Cấu trúc: Gồm các mục (entry) xác định địa chỉ IP nguồn, địa chỉ IP đích, giao thức, cổng TCP/UDP và loại truy cập được phép.

Tính năng:

- Kiểm soát dựa trên địa chỉ IP nguồn, địa chỉ IP đích, giao thức và cổng TCP/UDP.
- Hỗ trợ nhiều giao thức mạng và ứng dụng.
- Cung cấp khả năng kiểm soát chi tiết hơn.

Ứng dụng: Thích hợp cho các mạng phức tạp hoặc yêu cầu kiểm soát truy cập chi tiết.

2.5.3 Firewall

Tường lửa (firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát lưu lượng truy cập vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào cản giữa mạng an toàn và mạng không an toàn.

❖ **Các loại tường lửa:**

- **Tường lửa lọc gói tin:** Loại tường lửa này kiểm tra các gói tin mạng dựa trên các tiêu chí như địa chỉ IP, cổng và giao thức.
- **Tường lửa cấp ứng dụng:** Loại tường lửa này kiểm tra các ứng dụng đang tạo ra lưu lượng truy cập mạng.
- **Tường lửa trạng thái:** Loại tường lửa này theo dõi trạng thái của các kết nối mạng và chỉ cho phép lưu lượng truy cập hợp lệ.

❖ **Chức năng chính:**

- **Kiểm soát truy cập:** Cho phép hoặc từ chối lưu lượng truy cập dựa trên các quy tắc được định nghĩa.

- **Bảo vệ khỏi các cuộc tấn công mạng:** Ngăn chặn các truy cập trái phép và các cuộc tấn công mạng.
- **Giám sát mạng:** Theo dõi lưu lượng truy cập mạng và ghi lại các hoạt động đáng ngờ.
- **Quản lý truy cập từ xa:** Cho phép người dùng truy cập vào mạng từ xa một cách an toàn.

❖ **Lợi ích:**

- **Tăng cường bảo mật:** Giúp bảo vệ mạng khỏi các truy cập trái phép và các cuộc tấn công mạng.
- **Tuân thủ quy định:** Giúp tổ chức tuân thủ các quy định về bảo mật dữ liệu.
- **Giảm chi phí:** Giúp giảm chi phí cho việc bảo mật mạng bằng cách ngăn chặn các vi phạm an ninh mạng.

Tường lửa là một công cụ quan trọng để bảo vệ mạng khỏi các truy cập trái phép và các cuộc tấn công mạng. Tường lửa có nhiều lợi ích như tăng cường bảo mật, tuân thủ quy định và giảm chi phí. Tường lửa hoạt động bằng cách kiểm soát lưu lượng truy cập vào, ra khỏi hệ thống dựa trên các quy tắc được định nghĩa.

2.5.4 VPN – IPSec

VPN (Virtual Private Network) là mạng riêng ảo được tạo ra trên mạng Internet công cộng, cho phép người dùng truy cập vào mạng riêng một cách an toàn từ xa.

IPSec (Internet Protocol Security) là một tập hợp các giao thức bảo mật được sử dụng để bảo vệ dữ liệu truyền tải trên mạng IP. IPSec thường được sử dụng kết hợp với VPN để cung cấp bảo mật cho kết nối VPN.

❖ **Lợi ích của VPN - IPSec:**

- **Bảo mật:** IPSec mã hóa dữ liệu truyền tải giữa hai điểm, giúp bảo vệ dữ liệu khỏi bị đánh cắp hoặc nghe lén.

- **Xác thực:** IPSec xác thực người dùng và thiết bị trước khi cho phép truy cập vào mạng VPN.
- **Tính toàn vẹn dữ liệu:** IPSec đảm bảo rằng dữ liệu truyền tải không bị thay đổi trong quá trình truyền.
- **Quyền riêng tư:** IPSec che giấu địa chỉ IP của người dùng, giúp bảo vệ quyền riêng tư của họ.

❖ **Quy trình kết nối VPN - IPSec:**

- **Khởi tạo kết nối:** Người dùng khởi tạo kết nối VPN với máy chủ VPN bằng cách sử dụng phần mềm VPN hoặc giao diện web.
- **Xác thực:** Máy chủ VPN xác thực người dùng và thiết bị bằng cách sử dụng các phương thức xác thực như tên người dùng và mật khẩu, mã thông báo bảo mật hoặc chứng chỉ kỹ thuật số.
- **Thỏa thuận:** Máy chủ VPN và máy khách VPN thỏa thuận về các thông số bảo mật cho kết nối VPN, bao gồm thuật toán mã hóa, độ dài khóa và chế độ ESP (Encapsulating Security Payload).
- **Thiết lập đường hầm:** Máy chủ VPN và máy khách VPN thiết lập đường hầm IPSec để truyền tải dữ liệu an toàn.
- **Truyền tải dữ liệu:** Dữ liệu được truyền tải giữa máy chủ VPN và máy khách VPN qua đường hầm IPSec được mã hóa.
- **Giải mã dữ liệu:** Dữ liệu được giải mã tại điểm đến.
- **Kết thúc kết nối:** Người dùng kết thúc kết nối VPN bằng cách sử dụng phần mềm VPN hoặc giao diện web.

❖ **Các giai đoạn của quy trình IPSec:**

- Giai đoạn 1 (IKE - Internet Key Exchange):
 - Giai đoạn này thiết lập các khóa bảo mật được sử dụng để mã hóa dữ liệu trong đường hầm IPSec.
 - Giai đoạn 1 sử dụng các giao thức IKEv1 hoặc IKEv2 để trao đổi khóa.
- Giai đoạn 2 (ESP - Encapsulating Security Payload):

- Giai đoạn này mã hóa dữ liệu và thêm thông tin tiêu đề để bảo vệ tính toàn vẹn dữ liệu.
- Giai đoạn 2 sử dụng các thuật toán mã hóa như AES (Advanced Encryption Standard) và SHA (Secure Hash Algorithm) để bảo mật dữ liệu.

❖ **Các loại VPN - IPSec:**

- Site-to-site VPN: Loại VPN này kết nối hai mạng riêng với nhau.
- Remote-access VPN: Loại VPN này cho phép người dùng truy cập vào mạng riêng từ xa.

2.5.5 NAT

NAT, với tên đầy đủ của Network Address Translation. Đây là một kỹ thuật dùng để chuyển đổi địa chỉ IP. NAT giúp chuyển đổi các IP private thành các IP public khi các gói tin từ LAN ra ngoài Internet và ngược lại sẽ chuyển đổi các IP public thành private khi nhận các gói tin từ Internet. Chức năng chính của việc dùng NAT là bảo tồn không gian địa chỉ public.

❖ NAT sẽ thường có 3 loại chính:

- Static NAT: Đây đơn giản là một loại NAT ánh xạ 1-1 (Inside Local – Inside Global)
- Dynamic NAT: Sử dụng 1 pool địa chỉ public và gán địa chỉ theo (firstcome, firstserved basis)
- PAT (Port Address Translation): - Ánh xạ nhiều địa chỉ IP private thành 1 Ipv4 public
 - Dùng số cổng nguồn để xác định NAT

Sử dụng TCP port number khác nhau

2.5.6 IDS/IPS với Snort

Hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS) là những công cụ quan trọng để bảo vệ mạng khỏi các cuộc tấn công mạng. Snort là một công cụ mã nguồn mở phổ biến được sử dụng để triển khai IDS/IPS.

IDS: Phát hiện các hành vi đáng ngờ trên mạng và cảnh báo người quản trị hệ thống.

IPS: Phát hiện và ngăn chặn các hành vi đáng ngờ trên mạng.

❖ **Có hai loại IDS/IPS chính:**

- IDS dựa trên mạng: Giám sát lưu lượng truy cập mạng để phát hiện các hành vi đáng ngờ.
- IDS dựa trên host: Giám sát các hoạt động trên máy tính để phát hiện các hành vi đáng ngờ.

Snort là một IDS/IPS dựa trên mạng sử dụng các quy tắc để phát hiện các hành vi đáng ngờ. Snort có thể được sử dụng để:

- Phát hiện các cuộc tấn công mạng phổ biến như quét cổng, tấn công DoS và tấn công SQL injection.
- Phát hiện các hành vi bất thường có thể là dấu hiệu của một cuộc tấn công mạng.
- Ghi lại các hoạt động mạng để phân tích sau này.

❖ **Cách thức hoạt động của Snort:**

- **Thu thập gói tin:** Snort thu thập các gói tin mạng bằng cách sử dụng promiscuous mode.
- **Phân tích gói tin:** Snort phân tích các gói tin để tìm kiếm các mẫu phù hợp với các quy tắc được định nghĩa.
- **Báo động:** Nếu Snort tìm thấy một mẫu phù hợp với một quy tắc, nó sẽ tạo ra một báo động.
- **Phản hồi:** Người quản trị hệ thống có thể xem xét báo động và thực hiện các hành động thích hợp.

❖ **Lợi ích của việc sử dụng Snort:**

- **Mã nguồn mở:** Miễn phí và có thể được tùy chỉnh để đáp ứng nhu cầu cụ thể.
- **Phổ biến:** Có nhiều tài liệu và cộng đồng hỗ trợ.
- **Hiệu quả:** Có thể phát hiện nhiều loại tấn công mạng.

❖ **Hạn chế của việc sử dụng Snort:**

- **Có thể tạo ra nhiều báo động giả:** Cần được cấu hình cẩn thận để giảm thiểu báo động giả.
- **Có thể ảnh hưởng đến hiệu suất mạng:** Cần được cấu hình cẩn thận để không ảnh hưởng đến hiệu suất mạng.

 **Ví dụ về tấn công DoS:**

Tấn công DoS (Denial-of-Service) là một loại tấn công mạng nhằm làm cho hệ thống hoặc dịch vụ không thể sử dụng được bằng cách làm quá tải tài nguyên của hệ thống.

Snort có thể được sử dụng để ngăn chặn các cuộc tấn công DoS bằng cách sử dụng các **signature**. **Signature** là một tập hợp các quy tắc được sử dụng để xác định các mẫu lưu lượng truy cập mạng có thể là dấu hiệu của một cuộc tấn công DoS.

Ví dụ về signature để ngăn chặn tấn công DoS của Snort:

```
alert tcp $EXTERNAL_NET any -> $INTERNAL_NET any (msg:"SYNflood";
sid:10001; rev:1;)
```

alert tcp: Signature này áp dụng cho các gói tin TCP.

\$EXTERNAL_NET any: Gói tin đến từ bất kỳ địa chỉ IP nào bên ngoài mạng nội bộ.

=> **\$INTERNAL_NET any**: Gói tin đến bất kỳ địa chỉ IP nào trong mạng nội bộ.

(msg:"SYNflood"; sid:10001; rev:1;):

msg:"SYNflood": Thông báo cảnh báo "SYN flood".

sid:10001: Mã ID duy nhất cho signature này.

rev:1: Phiên bản của signature này.

Khi Snort nhận được một gói tin TCP phù hợp với signature này, nó sẽ tạo ra một báo động. Người quản trị hệ thống có thể xem xét báo động và thực hiện các hành động thích hợp, chẳng hạn như chặn địa chỉ IP nguồn của gói tin.

Ngoài ra, Snort còn có các signature khác để ngăn chặn các loại tấn công DoS khác, chẳng hạn như tấn công Ping of Death và tấn công Smurf.

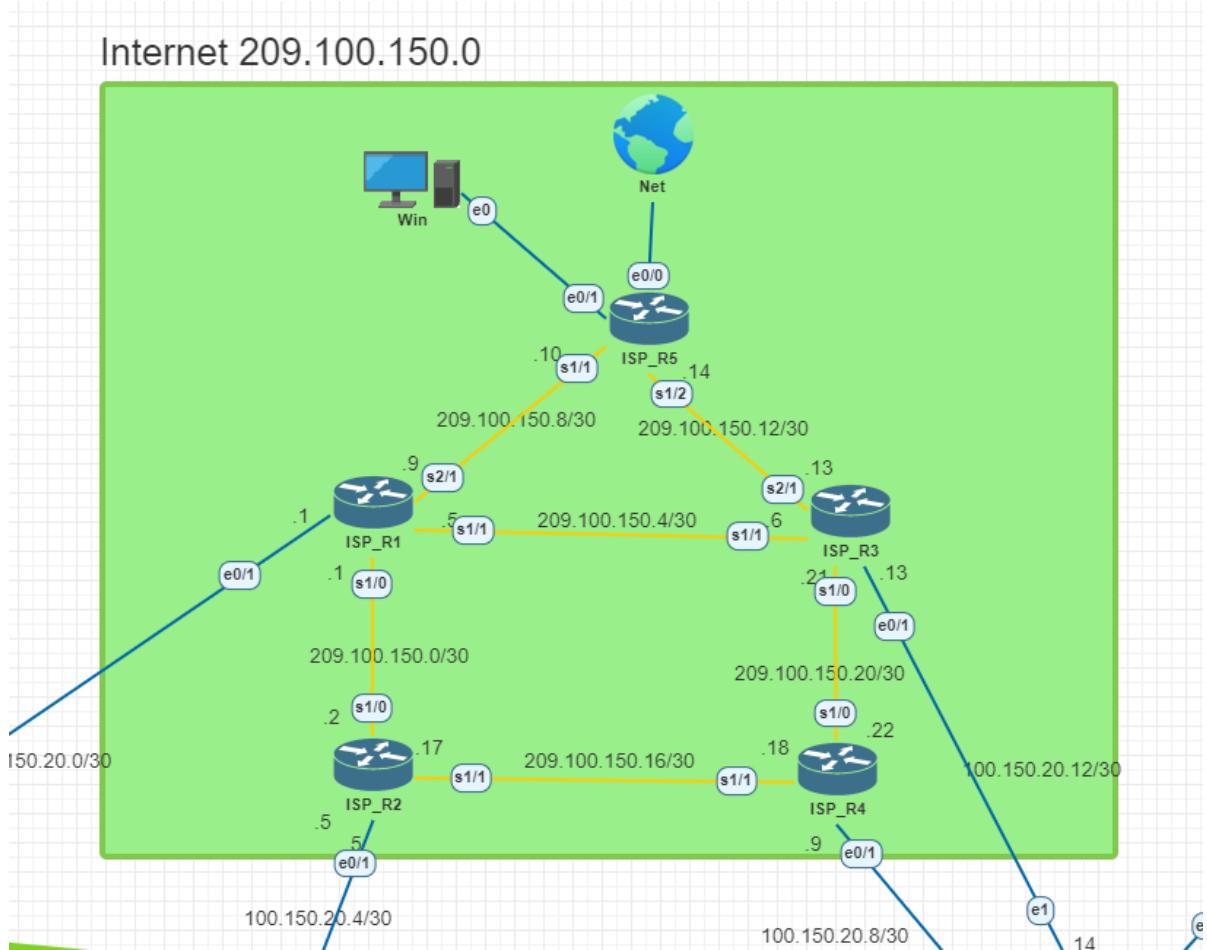
Snort là một công cụ hiệu quả để ngăn chặn các cuộc tấn công DoS bằng cách sử dụng các signature. Snort có nhiều signature để ngăn chặn các loại tấn công DoS khác nhau.

CHƯƠNG 3. MÔ HÌNH VÀ THÔNG TIN CẤU HÌNH HỆ THỐNG

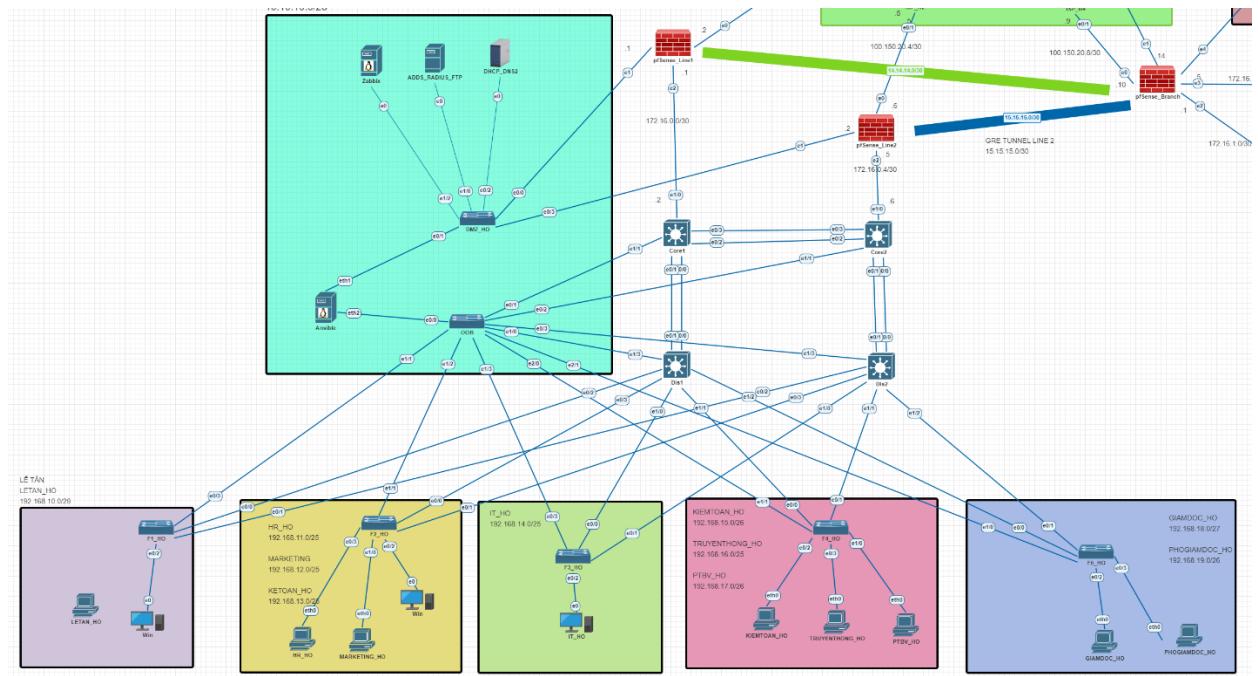
Dựa trên khảo sát, nhóm tiến hành dựng mô hình hệ thống trên lab. Quy hoạch địa chỉ IP cho các phòng ban, các dịch vụ server cần thiết.

3.1 Sơ đồ luận lý

Ở đây chúng ta sẽ giả định 5 router ISP trên sẽ đóng vai trò giả định như là nhà cung cấp dịch vụ internet để kết nối vào hệ thống mạng WAN. Sử dụng hai kênh truyền internet để đảm bảo tính ổn định và tính dự phòng.



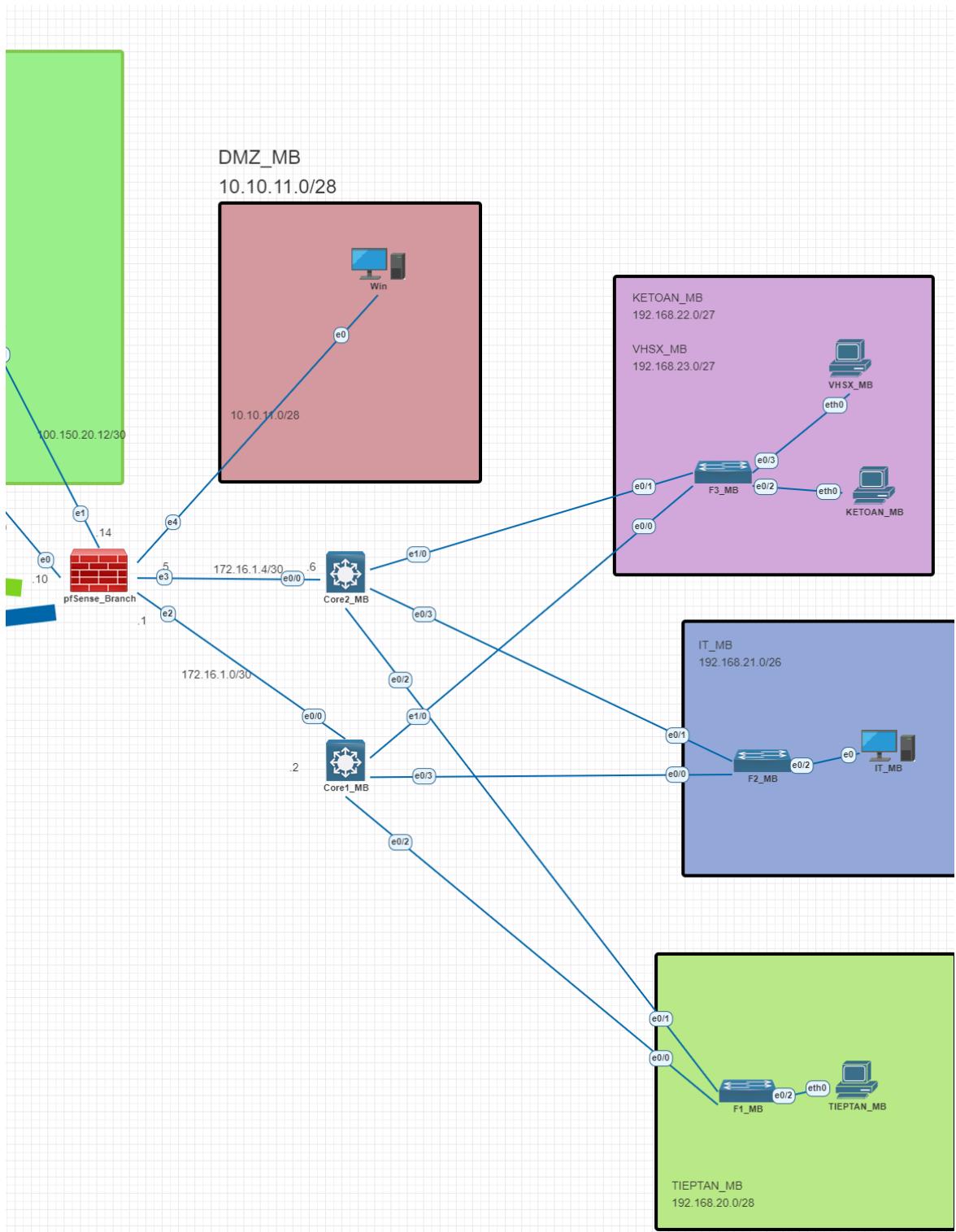
Hình 3.1.1: Sơ đồ luận lý khu vực Internet



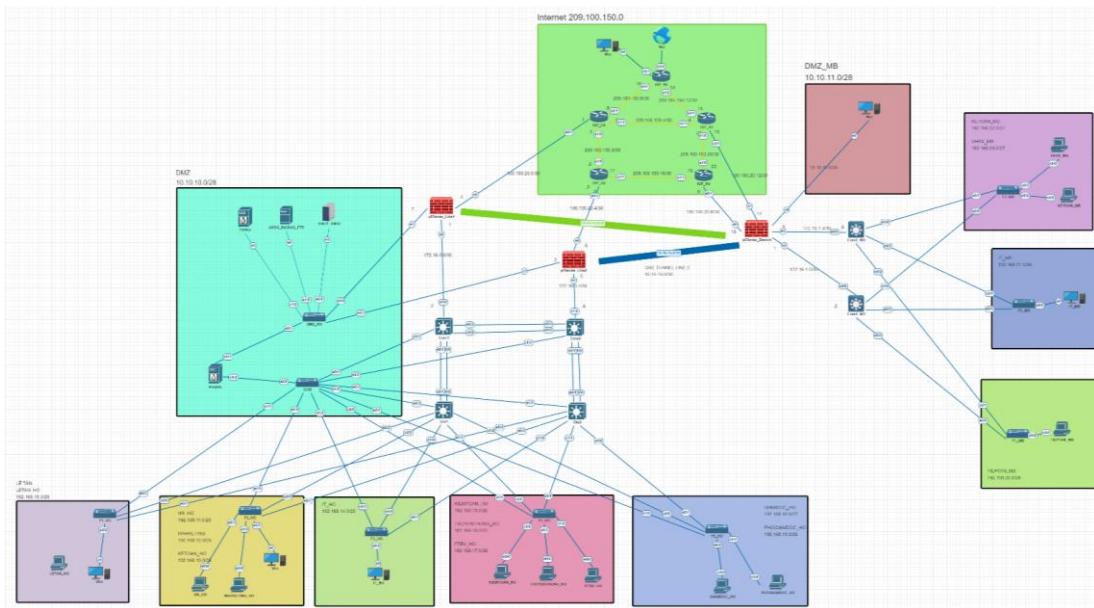
Hình 3.1.2: Sơ đồ luận lý khu vực miền Nam

Trong đó, chúng ta sẽ sử dụng tường lửa để đạt được mục đích HA (High Availability) và cân bằng tải. Khu vực LAN sẽ được cấu hình bằng mô hình ba lớp với lớp Core, Distribution và Access. Các máy chủ dịch vụ sẽ được đặt ở vùng DMZ, switch OOB(Out of band) sẽ đóng vai trò kết nối các thiết bị mạng với Ansible nhằm tạo ra một đường quản lý và cấu hình riêng biệt, không chia sẻ dữ liệu với traffic in-band. Điều này sẽ giúp đơn giản hóa triển khai tự động hóa cấu hình và quản lý, cung cấp một kênh dự phòng và đảm bảo tính ổn định của hệ thống.

Ở lớp Access sẽ là nơi để chia các VLAN cho các phòng ban trong LAN, trong sơ đồ này sẽ bao gồm 5 tầng với các tầng sẽ có một hoặc nhiều phòng ban.



Hình 3.1.3: Khu vực miền Bắc



Hình 3.1.4: Sơ đồ tổng quát

3.2 Thông tin kết nối port trong hệ thống

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
HO				
DHCP_MAIL_DNS2 to DMZ_HO	e0	e0/2	Ethernet	
ADDS_RADIUS to DMZ_HO	e0	e1/1	Ethernet	
Zabbix to DMZ_HO	e1	e1/2	Ethernet	
Router Firewall to Switch DMZ	e0/2	e0/0	Ethernet	
Ansible to DMZ_HO	e1	e0/1	Ethernet	
Ansible to OOB	e2	e0/0	Ethernet	
Win to DMZ_HO	e0	e1/0	Ethernet	

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
pSense_Line1 to DMZ_HO	e1	e0/0	Ethernet	
pSense_Line1 to Core1	E2	E1/0	Ethernet	
pSense_Line1 to pSense_Line2	E3	E3	Ethernet	
pSense_Line1 to ISP_R1	E0	E0/1	Ethernet	
pSense_Line2 to DMZ_HO	e1	e0/3	Ethernet	
pSense_Line2 to Core2	E2	E1/0	Ethernet	
pSense_Line2 to ISP_R2	E0	E0/1	Ethernet	
Core1 to OOB	E1/1	E0/1	Ethernet	
Core1 to Core 2	Port-channel 2 (e0/2-3)	Port-channel 2 (e0/2-3)	Ethernet	Port-channel
Core1 to Dis1	Port-channel 1 (e0/0-1)	Port-channel 1 (e0/0-1)	Ethernet	Port-channel
Core2 to OOB	E1/1	E0/2	Ethernet	
Core2 to Dis2	Port-channel 1 (e0/0-1)	Port-channel 1 (e0/0-1)	Ethernet	Port-channel
Dis1 to F1_HO	E0/2	e0/0	Ethernet	Trunking
Dis1 to F2_HO	E0/3	e0/0	Ethernet	Trunking
Dis1 to F3_HO	E1/0	e0/0	Ethernet	Trunking
Dis1 to F4_HO	E1/1	e0/0	Ethernet	Trunking
Dis1 to F5_HO	E1/2	e0/0	Ethernet	Trunking
Dis2 to F1_HO	E0/2	e0/1	Ethernet	Trunking

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
Dis2 to F2_HO	E0/3	e0/1	Ethernet	Trunking
Dis2 to F3_HO	E1/0	e0/1	Ethernet	Trunking
Dis2 to F4_HO	E1/1	e0/1	Ethernet	Trunking
Dis2 to F5_HO	E1/2	e0/1	Ethernet	Trunking
F1_HO to LETAN_HO	e0/2	e0	Ethernet	VLAN
F2_HO to HR_HO	e0/2	e0	Ethernet	VLAN
F2_HO to MARKETING_HO	e0/3	e0	Ethernet	VLAN
F2_HO to KETOAN_HO	e1/0	e0	Ethernet	VLAN
F3_HO to IT_HO	e0/2	e0	Ethernet	VLAN
F4_HO to KIEMTOAN_HO	e0/2	e0	Ethernet	VLAN
F4_HO to TRUYENTHONG_HO	e0/3	e0	Ethernet	VLAN
F4_HO to PTBV_HO	e1/0	e0	Ethernet	VLAN
F5_HO to GIAMDOC_HO	e0/2	e0	Ethernet	VLAN
F5_HO to PHOGIAMDOC_HO	e0/3	e0	Ethernet	VLAN
Dis1 to OOB	E2/0	E1/0	Ethernet	
Dis2 to OOB	E1/3	E0/3	Ethernet	
F1_HO to OOB	E0/3	E1/1	Ethernet	
F2_HO to OOB	E1/1	E1/2	Ethernet	
F3_HO to OOB	E0/3	E1/3	Ethernet	
F4_HO to OOB	E1/1	E2/0	Ethernet	

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
F5_HO to OOB	E1/0	E2/1	Ethernet	
Miền Bắc				
pSense_Branch to ISP_R4				
DMZ_MB to ADDS_MB	E0/1	E0	Ethernet	
Core_MB to Dis1_MB	Port-channel1(e0/0-1)	Port-channel1(e0/0-1)		
Core_MB to Dis2_MB	Port-channel2(e0/2-3)	Port-channel1(e0/0-1)		
Dis1_MB to F1_MB	E0/2	E0/0		Trunking
Dis1_MB to F2_MB	E0/3	E0/0		Trunking
Dis1_MB to F3_MB	E1/0	E0/0		Trunking
Dis2_MB to F1_MB	E0/2	E0/1		Trunking
Dis2_MB to F2_MB	E0/3	E0/1		Trunking
Dis2_MB to F3_MB	E1/0	E0/1		Trunking
F1_MB to TIEPTAN_MB	E0/2	E0		VLAN
F2_MB to IT_MB	E0/2	E0		VLAN
F3_MB to VHSX_MB	E0/2	E0		VLAN
F3_MB to KETOAN_MB	E0/3	E0		VLAN
Internet				
ISP_R1 to ISP_R2	S1/0	S1/0	Serial	

Source to destination	Source Interface	Destination Interface	Protocol	Trunking/VLAN
ISP_R1 to ISP_R3	S1/1	S1/1	Serial	
ISP_R1 to ISP_R4	S1/2	S1/2	Serial	
ISP_R2 to ISP_R3	S1/2	S1/2	Serial	
ISP_R2 to ISP_R4	S1/1	S1/1	Serial	
ISP_R3 to ISP_R4	S1/0	S1/0	Serial	
ISP_R1 to Net	E0/0		Ethernet	
ISP_R3 to Net	E0/0		Ethernet	

Bảng 3.2: Bảng thông tin kết nối port trong hệ thống

3.3 Thông tin VLAN, Interface VLAN trong hệ thống

📍 Khu vực miền Nam

PHÒNG BAN	VLAN ID	NAME	IP SIZE	IP ADDRESS	IP RANGE
LỄ TÂN	10	LETAN_HO	14	192.168.10.1/28	192.168.10.1 - 192.168.10.14
NHÂN SỰ	11	HR_HO	80	192.168.11.1/25	192.168.11.1 - 192.168.11.126
MARKETING	12	MARKETING_HO	80	192.168.12.1/25	192.168.12.1 - 192.168.12.126
KẾ TOÁN	13	KETOAN_HO	100	192.168.14.1/25	192.168.14.1 - 192.168.14.126
IT	14	IT_HO	90	192.168.14.1/25	192.168.14.1 - 192.168.14.126
KIỂM TOÁN	15	KIEMTOAN_HO	60	192.168.15.1/26	192.168.15.1 - 192.168.15.62

PHÒNG BAN	VLAN ID	NAME	IP SIZE	IP ADDRESS	IP RANGE
TRUYỀN THÔNG	16	TRUYENTHONG_HO	80	192.168.16.1/25	192.168.16.1 - 192.168.16.126
PHÁT TRIỂN BỀN VỮNG	17	PTBV_HO	40	192.168.17.1/26	192.168.17.1 - 192.168.17.62
GIÁM ĐỐC	18	GIAMDOC_HO	30	192.168.18.1/27	192.168.18.1 - 192.168.18.30
PHÓ GIÁM ĐỐC	19	PHOGIAMDOC_HO	40	192.168.19.1/26	192.168.19.1 - 192.168.19.62
Management	1	Management	30	172.10.1.1/27	172.10.1.1 - 172.10.1.30

Bảng 3.3.1: Bảng thông tin VLAN HO

 Khu vực miền Bắc

PHÒNG BAN	VLAN ID	NAME	IP SIZE	IP ADDRESS	IP RANGE
TIẾP TÂN	20	TIEPTAN_MB	10	172.168.20.1/28	172.168.20.1 - 172.168.20.14
IT	21	IT_MB	40	172.168.21.1/26	172.168.21.1 - 172.168.21.126
KẾ TOÁN	22	KETOAN_MB	20	172.168.22.1/27	172.168.22.1 - 172.168.22.30
VẬN HÀNH SẢN XUẤT	23	VHSX_MB	30	172.168.23.1/27	172.168.23.1 - 172.168.23.30

PHÒNG BAN	VLAN ID	NAME	IP SIZE	IP ADDRESS	IP RANGE
Management_MB	99	Management_MB	30	172.10.2.1/27	172.10.2.1-172.10.2.30

Bảng 3.3.2: Bảng thông tin VLAN Miền Bắc

3.4 Thông tin thiết kế quy hoạch địa chỉ IP Planning

SERVER	IPV4	GATEWAY	NETWORK
ADDS_Radius	10.10.10.4/28	10.10.10.3	10.10.10.0
Ansible	10.10.10.10/28	10.10.10.3	10.10.10.0
Zabbix	10.10.10.12/28	10.10.10.3	10.10.10.0
DHCP	10.10.10.5/28	10.10.10.3	10.10.10.0

Bảng 3.4.1 Bảng thông tin IP khu vực Server miền Nam

STT	Devices	Interface	Ipv4	Network
1	ISP_R1	s1/0	209.100.150.1	209.100.150.0
		s1/1	209.100.150.5	209.100.150.4
		s1/2	209.100.150.9	209.100.150.8
		e0/1	100.150.20.1	100.150.20.0

STT	Devices	Interface	Ipv4	Network
2	ISP_R2	s1/0	209.100.150.2	209.100.150.0
		s1/1	209.100.150.17	209.100.150.16
		s1/2	209.100.150.13	209.100.150.12
		e0/1	100.150.20.5	100.150.20.4
3	ISP_R3	s1/0	209.100.150.21	209.100.150.20
		s1/1	209.100.150.6	209.100.150.4
		s1/2	209.100.150.14	209.100.150.12
4	ISP_R4	s1/0	209.100.150.22	209.100.150.20
		s1/1	209.100.150.18	209.100.150.16
		s1/2	209.100.150.10	209.100.150.8
		e0/0	100.150.20.9	100.150.20.8
5	FW1	port1	10.10.10.1	10.10.10.0
		port2	100.150.20.2	100.150.20.0
		port3	172.16.0.2	172.16.0.0
		port4	15.15.15.1	15.15.15.0
6	FW2	port1	10.10.10.2	10.10.10.0
		port2	100.150.20.6	100.150.20.4
		port3	172.16.0.5	172.16.0.4
		port4	15.15.15.2	15.15.15.0
7	FW3	port1	172.16.0.29	172.16.0.28
		port2	100.150.20.10	100.150.20.8

STT	Devices	Interface	Ipv4	Network
		port3	10.10.11.1	10.10.11.0
		port4		
8	Core1	e1/0	172.16.0.1	172.16.0.0
		portchannel1	172.16.0.10	172.16.0.8
		portchannel2	172.16.0.13	172.16.0.12
9	Core2	e1/0	172.16.0.6	172.16.0.4
		portchannel1	172.16.0.18	172.16.0.16
		portchannel2	172.16.0.14	172.16.0.12
10	Dis1	portchannel1	172.16.0.9	172.16.0.8
11	Dis2	port channel1	172.16.0.17	172.16.0.16
13	Core1_MB	E0/0	172.16.1.2	172.16.1.0
14	Core2_MB	E0/0	172.16.1.6	172.16.1.4

Bảng 3.4.2 Bảng thông tin IP

CHƯƠNG 4. CẤU HÌNH HẠ TẦNG

Trong đồ án này, nhóm triển khai hệ thống trong môi trường ảo EVE-NG, một số chú ý trong việc sử dụng image các thiết bị khi triển khai hệ thống:

Đối với các thiết bị Router: Sử dụng image L3-ADVANTERPRISEK9-M15.2-M5.3.bin

Đối với các thiết bị Switch Layer 2: Sử dụng image L2-ADVENTERPRISEK9-M-15.2-20150703.bin

Đối với các thiết bị Switch Layer 3: Sử dụng image L2-ADVENTERPRISEK9-M-15.2-IRON-20151103.bin

Sử dụng winserver-S2016-x64-rev2 cho các máy chủ dịch vụ.

Sử dụng pfsense-CE-2.7.2-RELEASE cho thiết bị tường lửa.

Ở chương này sẽ đi vào chi tiết tất cả các bước cấu hình hệ thống từ khi bắt đầu đến khi hoàn tất.

4.1 Cấu hình cơ bản cho các Router ISP

```

ISP_R5

hostname ISP_R5
access-list 1 permit any
ip nat inside source list 1 interface e0/0
overload
int e0/0
ip add dhcp
ip nat out
no shut
exit
int s1/2
ip add 209.100.150.14 255.255.255.252
ip ospf 209 area 1
ip nat in
no shut
ex
int s1/1
ip add 209.100.150.10 255.255.255.252
ip ospf 209 area 1
ip nat in
no shut
ex
router ospf 209
passive-interface e0/0
net 209.100.150.12 0.0.0.3 area 1
net 209.100.150.8 0.0.0.3 area 1
default-information originate
exit

```

Interface e0/0 là interface hướng về internet => Sẽ lấy IP DHCP từ máy ảo EVE-NG

Cấu hình IP, NAT và định tuyến cho 2 interface hướng về LAN

Quảng bá DF Route vào OSPF cho các máy trong lab có thể ra internet

Hình 4.1: Cấu hình NAT router ISP_R5

```

ISP_R1

hostname ISP_R1
int s1/0
ip add 209.100.150.1 255.255.255.252
ip ospf 209 area 1
no shut
exit
int s1/1
ip add 209.100.150.5 255.255.255.252
ip ospf 209 area 1
no shut
exit
int s2/1
ip add 209.100.150.9 255.255.255.252
ip ospf 209 area 1
no shut
exit
int e0/1
ip add 100.150.20.1 255.255.255.252
no shut
exit
router ospf 209
net 209.100.150.0 0.0.0.3 area 1
net 209.100.150.4 0.0.0.3 area 1
net 209.100.150.8 0.0.0.3 area 1
net 100.150.20.1 0.0.0.3 area 1
passive-interface e0/1
exit

```

Cấu hình IP,
định tuyến cho
Router ISP

Hình 4.2: Cấu hình interface cho R1 và áp rule NAT vào interface

Tương tự cấu hình cho R2, R3 và R4 với IP dựa vào bảng 3.3.

Sau khi đã đảm bảo khu vực internet đã thông với nhau, chúng ta sẽ sử dụng thiết bị Ansible để tự động hóa các quá trình cấu hình bằng code.

4.2 SSH Access

Để Ansible có thể truy cập đến các thiết bị trong hệ thống để tiến hành cấu hình auto thì bước đầu tiên chúng ta cần phải cấu hình SSH cho tất cả các thiết bị trong hệ thống. Ở đây chúng ta sẽ sử dụng VLAN quản lý để quản lý các thiết bị, trong đó:

VLAN 1: VLAN quản lý ở site HO với network 172.10.1.0/27

VLAN 99: VLAN quản lý ở site Miền Bắc với network 172.10.2.0/27

Cấu hình SSH cho các thiết bị Switch và Router có trong hệ thống:

```

1 hostname Core1
2 enable secret level 15 2023@InFraGF
3 banner motd "KHONG PHAN SU MIEN VAO"
4 service password-encryption
5 ip domain-name gf.com
6 no ip domain-lookup
7 crypto key generate rsa general-keys modulus 1024
8 username adminlocalHO secret 2023@InFraGF
9 ip ssh ver 2
10 line vty 0 4
11 login local
12 transport input SSH
13 exit
14 do wr
15 interface vlan 1
16 description Management
17 ip add 172.10.1.2 255.255.255.224
18 no shut
19 exit
20 do write

```

Hình 4.2.1: Cấu hình SSH Access cho Core 1

Cài đặt tương tự đối với các thiết bị còn lại với IP VLAN 1 tương ứng

- Core2 : 172.10.1.3
- Dis1: 172.10.1.4
- Dis2: 172.10.1.5
- F1_HO: 172.0.1.6
- F2_HO: 172.0.1.7
- F3_HO: 172.0.1.8
- F4_HO: 172.0.1.9
- F5_HO: 172.0.1.10

Sau khi đã cấu hình SSH cho tất cả các thiết bị, chúng ta sẽ ssh từ Ansible vào các thiết bị để generate key mới.

4.3 Cài đặt Ansible

Ansible là một công cụ mã nguồn mở dùng để tự động hóa cấu hình và quản lý máy chủ. Nó là một công cụ thuộc dạng "Infrastructure as Code" (IaC), giúp tự động hóa quá trình triển khai và quản lý hạ tầng hệ thống.

Cài đặt Ansible Server:

```
apt-get update
apt-get upgrade
python3 -m pip install --user ansible
pip install paramiko
pip install ansible-pylibssh
```

Mở tập tin cấu hình với trình soạn thảo văn bản, ví dụ:

```
nano ~/.bashrc
```

Thêm dòng sau vào cuối tập tin:

```
export PATH=$PATH:~/local/bin
```

Lưu tập tin và tái tải cấu hình:

```
source ~/.bashrc
```

```
ansible-galaxy collection install cisco.ios
```

Trước khi bắt đầu cấu hình, phải đảm bảo rằng Ansible có thể SSH thành công đến thiết bị và đã generate khóa mới thì mới bắt đầu cấu hình.

Sử dụng câu lệnh: **ssh adminlocalHO@172.10.1.4** để ssh vào thiết bị.

Với:

adminlocalHO: username đăng nhập vào thiết bị

172.10.1.4: là địa chỉ của VLAN quản lý dùng để quản lý các thiết bị trong hệ thống.

Sau khi đã ssh thành công đến các thiết bị thì chúng ta sẽ tạo file trên Ansible hoặc có thể tải source code lên github và clone code về máy.

Đối với tạo thủ công, chúng ta sẽ dùng lệnh **nano temfile.yml** để tạo file mới, sau đó copy code lưu lại.

Đối với cách clone code từ github, chúng ta sẽ sử dụng câu lệnh: git clone [url] Tiếp theo sẽ là các file cần thiết để cấu hình thiết bị, bao gồm file inventory.ini và pass.yml

Xác định Inventory:

Tạo một file inventory để xác định các thiết bị cần cấu hình.

[CORE]

Core1 ansible_host=172.10.1.2

Core2 ansible_host=172.10.1.3

[DIS]

Dis1 ansible_host=172.10.1.4

Dis2 ansible_host=172.10.1.5

[Access]

F1_HO ansible_host=172.10.1.6

F2_HO ansible_host=172.10.1.7

F3_HO ansible_host=172.10.1.8

F4_HO ansible_host=172.10.1.9

F5_HO ansible_host=172.10.1.10

[all:vars]

ansible_ssh_type=paramiko

ansible_network_os=ios

ansible_connection=network_cli

ansible_become="yes"

ansible_become_method="enable"

File inventory trên sẽ bao gồm các thông số như `ansible_host` để gán địa chỉ IP cho các thiết bị tương ứng.

[CORE] [DIS] [Access] chứa các thiết bị switch tương ứng.

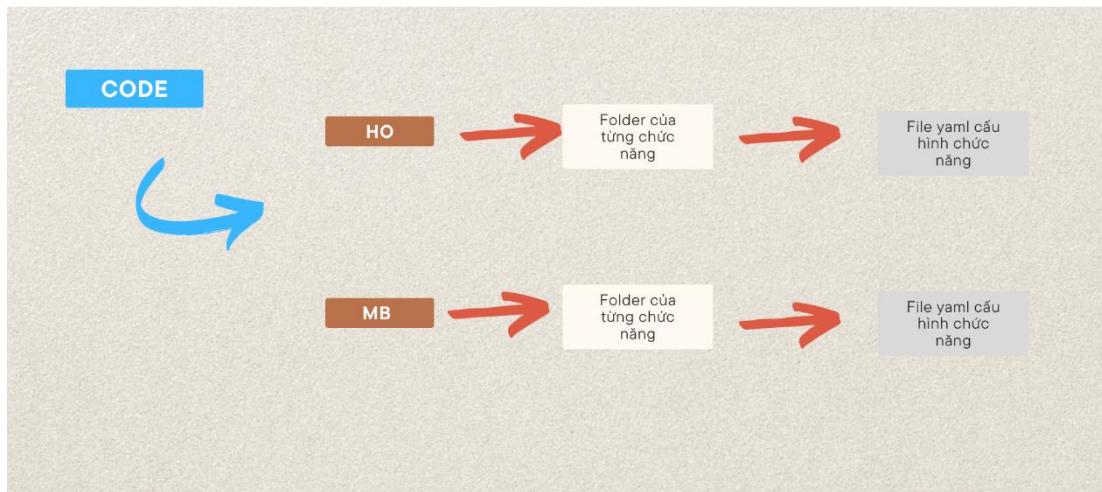
ansible_connection=network_cli: `network_cli` là phương thức kết nối đến thiết bị thông qua SSH

`ansible_become="yes"` và `ansible_become_method="enable"` enable là cho phép ansible có thể vào privilege mode trước khi thực thi các task.

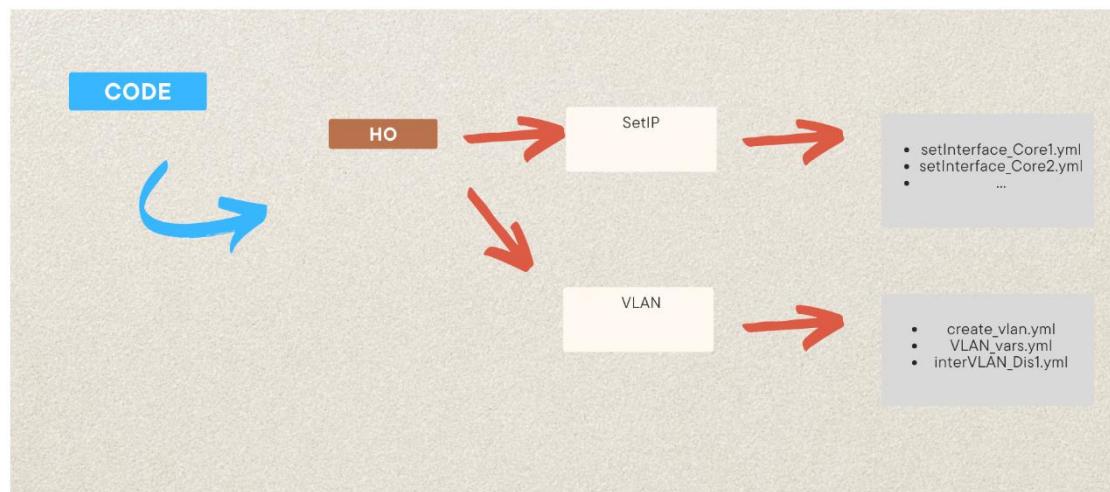
`ansible_network_os=ios`: `ios` ở đây do dùng các thiết bị của Cisco nên khai báo như vậy.

Tạo Playbook:

Tạo cây thư mục với cấu trúc như sau:



Hình 4.3.1: Tạo cây thư mục



Hình 4.3.2: Ví dụ cho cách tạo cây thư mục

Trong đó các file .yml sẽ là các playbook để xác định các nhiệm vụ mà chúng ta muốn thực hiện cấu hình trên máy chủ.

- Một số thông số trong file yml thường sẽ bao gồm các thông số như sau:
 - ``name`` : Đặt tên cho playbook
 - ``hosts`` : Chỉ định playbook sẽ chạy trên thiết bị nào.
 - ``gather_facts: no`` : Tắt chức năng tự động thu thập thông tin từ host trước khi chạy các task (**Khi thực hiện playbook sẽ tự động lấy thông tin của host**)
 - ``var_files: -pass.yml`` : Đọc các biến từ tệp pass.yml
- Trong mục ``task``:
 - ``name``: Đặt tên cho task
 - ``ios_config``: Các lệnh để cấu hình các chức năng

4.4 Cấu hình Interface cho các thiết bị

Giữa các Switch Core và Distribution, chúng ta sẽ nối thêm một dây và sử dụng kỹ thuật Ethernet Channel để tạo ra một liên kết có băng thông lớn hơn so với việc sử dụng một đường kết nối duy nhất.

Dựa vào bảng IP đã chia và sử dụng kỹ thuật VLSM, chúng ta sẽ gán các IP đó vào các thiết bị Switch và Router thông qua code.

```

1 ---
2 - name: Set IP and Interface configurations on Dis1
3   hosts: Dis1
4   gather_facts: no
5   vars_files:
6     - pass.yml
7   tasks:
8     - name: Configure interface range Ethernet0/0-1
9       cisco.ios.ios_config:
10      lines:
11        - no switchport
12        - channel-group 1 mode on
13        - no shutdown
14      parents: "{{ item }}"
15      with_items:
16        - interface Ethernet0/0
17        - interface Ethernet0/1
18
19
20     - name: Configure interface Port-channel1
21       cisco.ios.ios_config:
22      lines:
23        - no switchport
24        - ip address 172.16.0.9 255.255.255.252
25        - do wr
26      parents: interface Port-channel1

```

Đặt tên Playbook

Chỉ định playbook sẽ chạy trên thiết bị nào

chạy vòng lặp qua list interface e0/0-1 và áp các dòng lệnh trên vào để tạo channel group

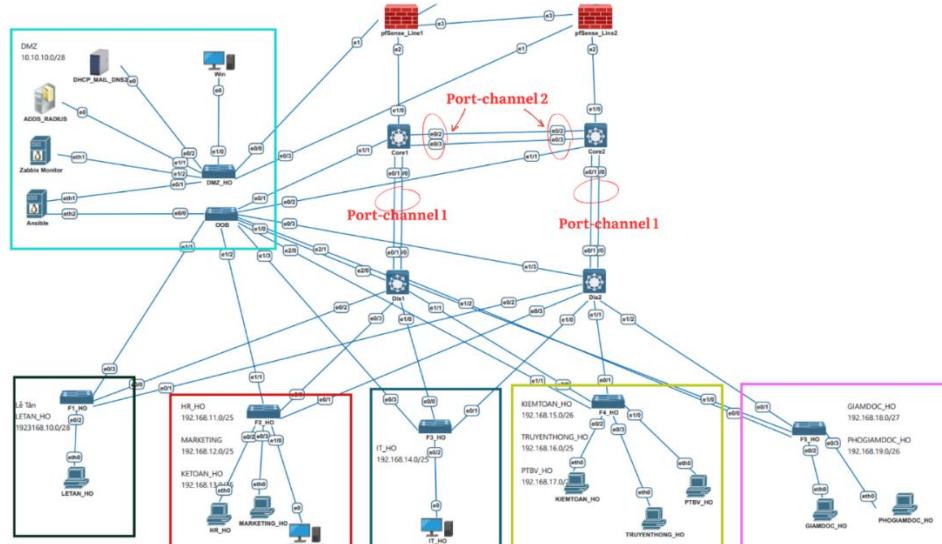
Add IP vào port channel 1

Hình 4.4.1: Set interface vào thiết bị Distribution 1 bằng Ansible

Để chạy code cấu hình trên vào các thiết bị, sử dụng câu lệnh:

`ansible-playbook -i inventory_file playbook.yml`

Cấu hình tương tự cho các thiết bị còn lại với các thông số như bảng 3.3



4.5 Cấu hình VLAN

Ở khu vực miền Nam và miền Bắc, chúng ta sẽ có 2 Switch Distribution và các Switch Access ở các tầng, chúng ta sẽ sử dụng Ansible để chạy cấu hình.

Bước đầu tiên, sau khi đảm bảo Ansible có thể SSH đến các thiết bị Switch, chúng ta cần tạo một file VLAN_vars.yml chứa các thông số cần thiết:

❖ **VLAN_vars.yml**

vlans:

- *vlan_id: 1 #VLAN id*

department: Management # Tên VLAN

subnetmask: 255.255.255.224 #subnet mask của vlan

- *vlan_id: 10*

department: LETAN_HO

subnetmask: 255.255.255.240

Tương tự đối với các VLAN còn lại

...

dis_Trunking_interfaces: # Các interface can trunking ở switch

Distribution

- *e0/2*

- *e0/3*

- *e1/0*

- *e1/1*

- *e1/2*

switch Access

- *e0/0*

- *e0/1*

F1_Access_interfaces: # Các interface access của các switch access

- *e0/2*

- *e0/3*

...

...

...

Tương tự cho các Switch access còn lại

Sau khi đã có các thông số cần thiết ở file VLAN_vars.yml, chúng ta sẽ bắt đầu tạo VLAN với đoạn code sau:

❖ **create_vlan.yml**

```
---
- name: Create VLANs on DIS and Access devices
  hosts: DIS:Access => Thực hiện tạo VLAN trên tt cả các thiết bị ở
        lớp Distribution và lớp access đã được khai báo ở file inventory.ini
  gather_facts: no
  vars_files:
    - pass.yml
    - VLAN_vars.yml
  tasks:
    - name: Create VLANs on DIS and Access devices
      ios_vlans: => Sử dụng module ios_vlans để tạo VLAN trên các
                    thiết bị
      vlan_id: "{{ item.vlan_id }}"
      name: "{{ item.department }}"
      state: merged
      config:
        - name: "{{ item.department }}"
      with_items: "{{ vlans }}" => Sử dụng vòng lặp để lặp qua các
                    danh sách ở biến vlans từ file VLAN_vars.yml
      when:      inventory_hostname      in      groups['DIS']      or
              inventory_hostname in groups['Access'] => Chỉ thực hiện task trên các thiết
                    bị DIS hoặc Access
```

```

- name: Save configuration => Lưu cấu hình
  ios_command:
    commands:
      - "write"

```

Sau khi đã tạo VLAN database, chúng ta sẽ thực hiện cấu hình interface VLAN trên hai thiết bị Switch Distribution 1 và Distribution 2 và cấu hình trunking và access cho các Switch Access

Chúng ta đã cấu hình ở DHCP Server và chừa ra các dãy địa chỉ từ **.1 - .3** không cấp cho các máy client, và chúng ta sẽ sử dụng nó để cấp interface VLAN cho hai thiết bị Distribution, trong đó Switch Distribution 1 sẽ là active của VLAN từ 10 đến 14 với IP bắt đầu từ **.2** và các VLAN từ 15 đến 19 sẽ là standby với IP từ **.3**. Ngược lại với Distribution 2 sẽ là standby của VLAN 10 đến 14 và active của VLAN 15 đến 19.

Sau khi đã cấu hình interface VLAN, chúng ta sẽ sử dụng câu lệnh ip helper-address để chuyển tiếp các yêu cầu DHCP từ VLAN đó tới máy chủ DHCP.

Đối với **Switch Distribution** sẽ cấu hình như sau:

```

❖ interVLAN._Dis1.yml

---
- name: Configure SVIs and IP addresses
  hosts: Dis1
  gather_facts: no
  vars_files:
    - pass.yml
    - VLAN_vars.yml
  tasks:
    - name: Configure SVI for VLANs 10 to 14
      ios_config:
        lines:
          - interface Vlan {{ item.vlan_id }}

```

```

- description {{ item.department }}
- ip address 192.168.{{ item.vlan_id }}.2 {{ item.subnetmask }}
- ip helper-address 10.10.10.5
- no shut

with_items: "{{ vlans }}" # Sử dụng vòng lặp để lặp qua các danh sách từ biến vlans trong file VLAN_vars.yml và cấu hình interface vlan .2 cho vlan 10-14

when: item.vlan_id >= 10 and item.vlan_id <= 14
- name: Configure SVI for VLANs 15 to 19

ios_config:

lines:
- interface Vlan {{ item.vlan_id }}
- description {{ item.department }}
- ip address 192.168.{{ item.vlan_id }}.3 {{ item.subnetmask }}
- ip helper-address 10.10.10.5
- no shut

with_items: "{{ vlans }}" # Sử dụng vòng lặp để lặp qua các danh sách từ biến vlans trong file VLAN_vars.yml và cấu hình interface vlan .3 cho vlan 15-19

when: item.vlan_id >= 15 and item.vlan_id <= 19
- name: Configure trunk interfaces

ios_config: # Cấu hình trunk cho các interface trong đó: trunk native vlan 1 dùng để gán các vlan không có thông tin vlan ở header sẽ được coi là thuộc vlan 1

lines:
- interface {{ item }}
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk native vlan 1

```

```

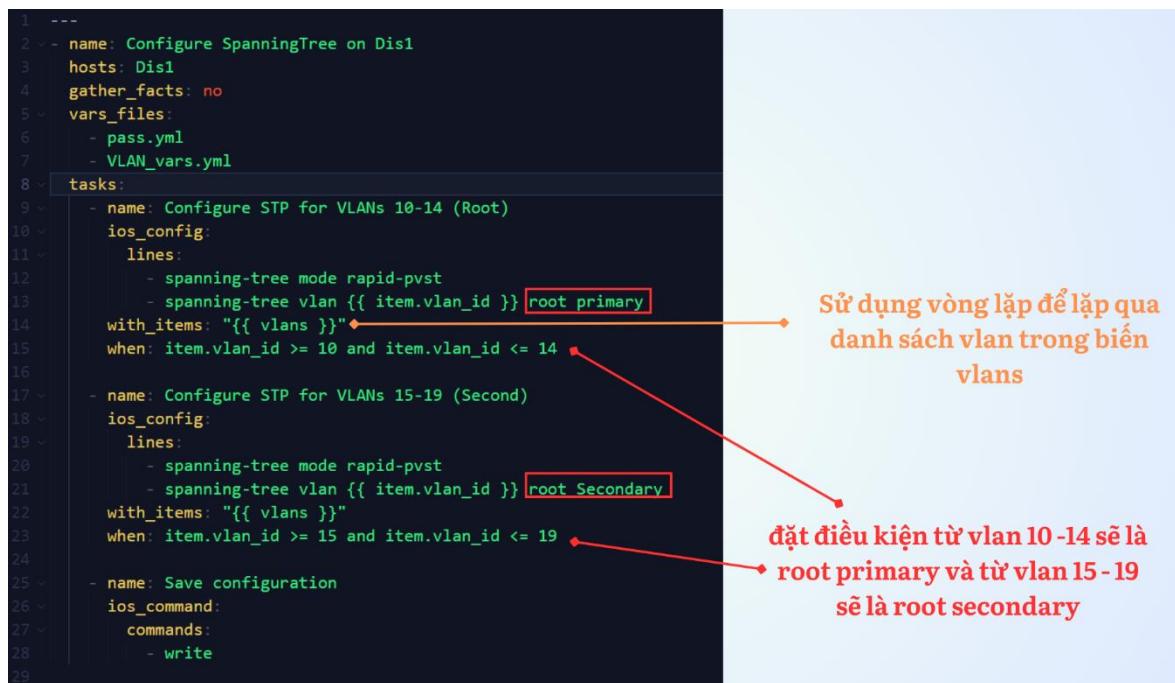
    with_items: "{{ dis_Trunking_interfaces }}"
- name: Save configuration
  ios_command:
    commands:
      - write

```

Cấu hình tương tự interface vlan cho Dis2, với VLAN 10-14: .3 và 15-19: .2. Các Switch Access sẽ cấu hình trunk và access cho các interface đã khai báo ở file vars.

4.6 Cấu hình Spanning Tree

Cấu hình Spanning tree trên Switch Distribution 1 với các VLAN từ 10 đến 14 sẽ là root và VLAN từ 15 đến 19 sẽ là secondary. Cấu hình ngược lại đối với Switch Distribution 2.



```

1 ---
2   - name: Configure SpanningTree on Dis1
3     hosts: Dis1
4     gather_facts: no
5     vars_files:
6       - pass.yml
7       - VLAN_vars.yml
8     tasks:
9       - name: Configure STP for VLANs 10-14 (Root)
10      ios_config:
11        lines:
12          - spanning-tree mode rapid-pvst
13          - spanning-tree vlan {{ item.vlan_id }} root primary
14      with_items: "{{ vlans }}"
15      when: item.vlan_id >= 10 and item.vlan_id <= 14
16
17     - name: Configure STP for VLANs 15-19 (Second)
18      ios_config:
19        lines:
20          - spanning-tree mode rapid-pvst
21          - spanning-tree vlan {{ item.vlan_id }} root Secondary
22      with_items: "{{ vlans }}"
23      when: item.vlan_id >= 15 and item.vlan_id <= 19
24
25     - name: Save configuration
26       ios_command:
27         commands:
28           - write

```

Sử dụng vòng lặp để lặp qua danh sách vlan trong biến vlans

đặt điều kiện từ vlan 10-14 sẽ là root primary và từ vlan 15-19 sẽ là root secondary

Hình 4.6.1: Cấu hình STP trên Distribution 1 bằng Ansible

Cấu hình mode rapid-pvst cho các switch access và cấu hình Dis 2 ngược lại so với Dis 1.

4.7 Cấu hình HSRP

Chúng ta sẽ tạo các standby ở các VLAN trên các switch Distribution với mục đích là để khi một con Switch Distribution bị hỏng, Switch còn lại sẽ đứng lên thay thế Switch chính. Chúng ta sẽ đặt standby ở Switch Distribution với priority là 110, đóng vai trò active và priority ở Switch Distribution 2 là 90, đóng vai trò dự phòng.

```

1  ---
2  - name: Configure HSRP on Dis1 for VLANs 10-14 (Active)
3  hosts: Dis1
4  gather_facts: no
5  vars_files:
6    - pass.yml
7    - VLAN_vars.yml
8  tasks:
9    - name: Configure IP SLA for Internet Check
10   ios_config:
11     lines:
12       - ip sla 1
13       - icmp-echo 8.8.8.8 source-interface Port-Channel1
14       - frequency 5
15       - ip sla schedule 1 life forever start-time now
16
17    - name: Configure HSRP for VLANs 10-14
18    ios_config:
19      lines:
20        - interface Vlan {{ item.vlan_id }}
21        - standby {{ item.vlan_id }} ip 192.168.{{ item.vlan_id }}.1
22        - standby {{ item.vlan_id }} priority 110
23        - standby {{ item.vlan_id }} preempt
24        - standby {{ item.vlan_id }} track 1 decrement 50
25    with_items: "{{ vlans }}"
26    when: item.vlan_id >= 10 and item.vlan_id <= 14

```

Cấu hình IP SLA để kiểm tra kết nối internet thông qua việc ping địa chỉ ip 8.8.8.8 từ interface portchannel 1

}

Chạy vòng lặp từ vlan 10-14 và đặt ip ảo là .1 với độ ưu tiên là 110, mode preempt chiếm quyền active và track khi switch bị down thì priority sẽ giảm đi 50, lúc này Dis1 sẽ trở thành standby và Dis2 sẽ trở thành active

}

Hình 4.7.1: Cấu hình HSRP cho Distribution 1 bằng Ansible

```

28     - name: Configure HSRP for VLANs 15-19 (Backup)
29     ios_config:
30       lines:
31         - interface Vlan {{ item.vlan_id }}
32         - standby {{ item.vlan_id }} ip 192.168.{{ item.vlan_id }}.1
33         - standby {{ item.vlan_id }} priority 90
34         - standby {{ item.vlan_id }} track 1 decrement 50
35     with_items: "{{ vlans }}"
36     when: item.vlan_id >= 15 and item.vlan_id <= 19
37
38     - name: Configure HSRP for VLANs Management
39     ios_config:
40       lines:
41         - interface Vlan 1
42         - standby 1 ip 172.10.1.1
43         - standby 1 priority 110
44         - standby 1 preempt
45         - standby 1 track 1 decrement 50
46
47     - name: Save configuration
48     ios_command:
49       commands:
50         - write

```

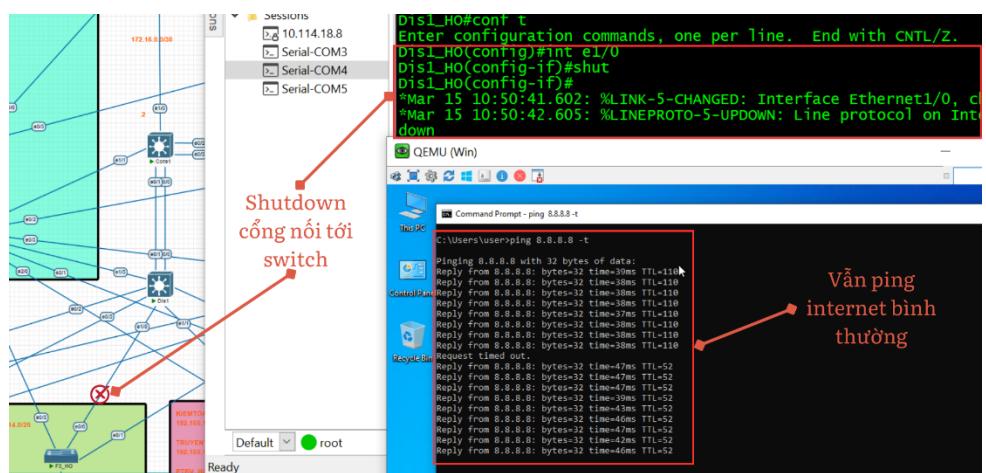
Tương tự các bước trên nhưng priority ở vlan 15-19 sẽ là 90

Cấu hình hsrp cho vlan quản lý là active

Hình 4.7.2: Cấu hình HSRP cho Distribution 1 bằng Ansible

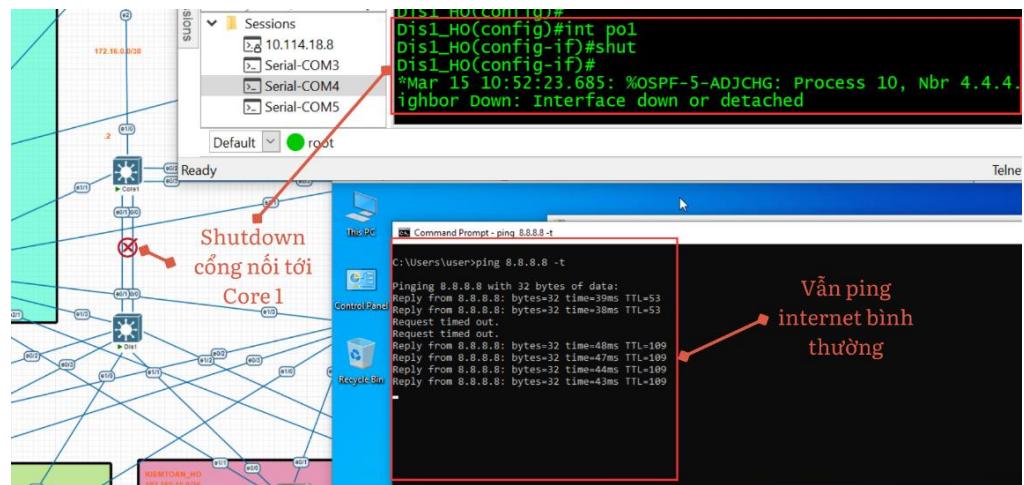
Cấu hình ngược lại với Dis 1 trên Switch Dis2.

Tiến hành kiểm thử với trường hợp link giữa switch access và switch distribution 1 bị down, khi này với lệnh ping tới địa chỉ dns Google là 8.8.8.8 thì kết quả nhận được là sẽ bị rớt 1 gói khi link bị down ngay tức thì lưu lượng sẽ chuyển qua switch distribution 2 do lúc này đã chuyển từ standby lên active và vẫn đi được internet bình thường như hình 4.7.3.



Hình 4.7.3: Shutdown cổng nối tới Switch vẫn có thể ping internet bình thường

Tiếp tục với trường đầu nối giữa switch distribution 1 với switch core 1 bị down, lúc này do có cấu hình Track IP SLA nên giá trị Priority của distribution 1 sẽ bị giảm từ đó distribution 2 sẽ chuyển từ mode standby lên active. Lưu lượng chỉ bị rót 1 đến 2 gói tin khi switch tính toán lại priority và chuyển mode trong HSRP sau đó đường đi internet vẫn thông bình thường như hình 4.7.4.



Hình 4.7.4: Shutdown cổng nối tới Core 1 vẫn có thể ping internet bình thường

4.8 Cấu hình định tuyến động OSPF

=> Process-id của ospf sẽ là 10

Các Router-id của từng thiết bị sẽ là

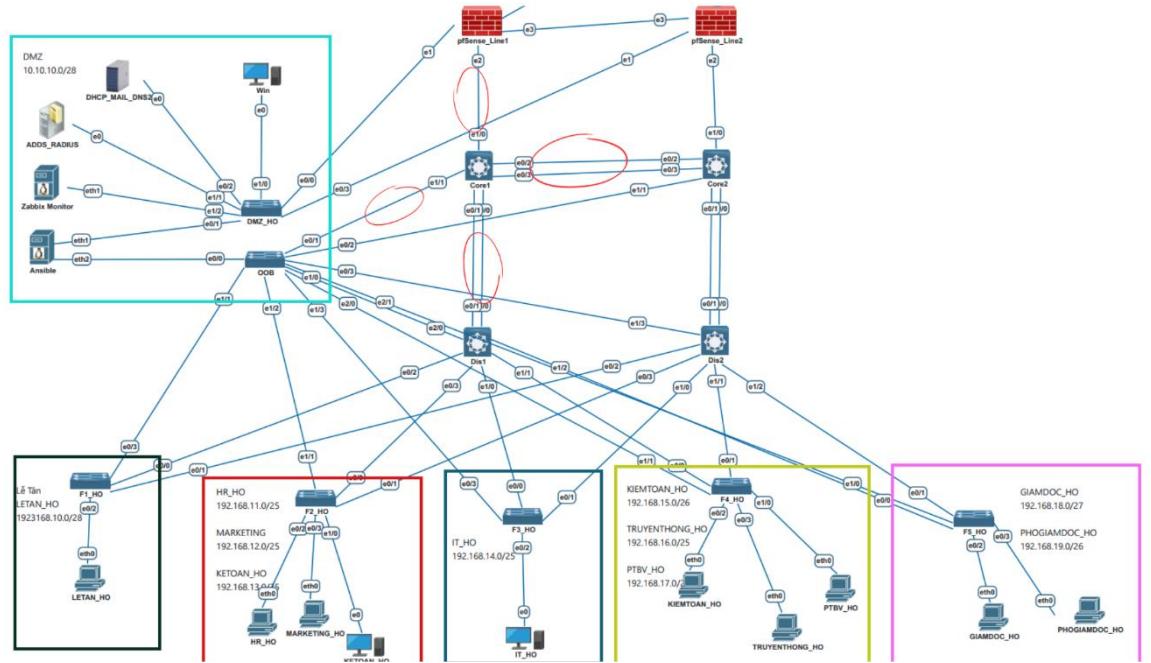
Dis1: 1.1.1.1

Dis2: 2.2.2.2

Core1: 4.4.4.4

Core2: 3.3.3.3

Cách cấu hình OSPF bao gồm các bước sau:



Hình 4.8.1: Các đường mạng ở các interface của Core 1

Tương tự với các chức năng trước đó, đầu tiên chúng ta sẽ tạo file OSPF_vars.yml chứa các thông số cần thiết.

❖ OSPF_vars.yml

dis_interfaces:

- int po 1
- int vlan 1
- int vlan 10
- ...
- int vlan 19

dis_passive_interfaces:

- e0/2
- e0/3
- e1/0
- e1/1
- e1/2

core_interfaces:

- *int po 1*
- *int po 2*
- *int e1/0*

Sau đó tiến hành định tuyến:

❖ **OSPF_Core1.yml**

```

- name: Configure OSPF Core1
hosts: Core1
gather_facts: no
vars_files:
  - OSPF_vars.yml
  - pass.yml
tasks:
  - name: Enable routing
    ios_config:
      lines:
        - ip routing
  - name: Enable OSPF process 10
    ios_config:
      lines: # Cấu hình ospf trên core 1
        - router ospf 10 # process id
        - router-id 4.4.4.4 # router-id
        - net 172.16.0.0 0.0.0.3 area 0
        - net 172.16.0.8 0.0.0.3 area 0
        - net 172.16.0.12 0.0.0.3 area 0
  - name: Enable OSPF on interfaces
    ios_config:

```

*lines: # Sử dụng vòng lặp chạy danh sách từ biến core_interface
để áp ospf vào các interface*

- "{{ item }}"
- ip ospf 10 area 0

with_items: "{{ core_interfaces }}"

- name: Save configuration
- cisco.ios.ios_command:
- commands:
- write

Thực hiện tương tự với các thiết bị còn lại.

4.9 Access Control List

Một số kịch bản cho các rule ACL:

Các phòng chức năng có thể sử dụng các dịch vụ FTP, Mail

Chỉ được sử dụng DNS nội bộ, khi tự ý thay đổi qua IP DNS khác như 8.8.8.8 của Google thì không sử dụng được giao thức này.

Phòng IT và Ansible có thể telnet và ssh vào các thiết bị mạng, Remote Desktop đến Server kể cả ở khu vực miền Bắc.

Ở khu vực miền Bắc, thì phòng IT tại khu vực này chỉ được phép truy cập các thiết bị nội bộ còn các thiết bị ở HO thì không được phép.

Chúng ta sẽ cấu hình ACL ở Switch Distribute thông qua Ansible, với cấu hình như sau:

```

--+
  name: Set ACL
  hosts: DIS
  gather_facts: no
  vars_files:
    - pass.yml
  tasks:
    - name: Define access control lists
      cisco.ios.ios_acls:
        config:
          - afi: ipv4
            acls:
              - name: 110
                aces:
                  - grant: permit
                    protocol: udp
                    source:
                      address: any
                    destination:
                      address: 10.10.10.0
                      wildcard_bits: 0.0.0.15
                    port_protocol:
                      eq: 53

```

```

- grant: permit
  protocol: tcp
  source:
    address: any
  destination:
    address: 10.10.10.0
    wildcard_bits: 0.0.0.15
    port_protocol:
      eq: 53

```

Cho phép gửi và nhận gói tin DNS
 UDP và TCP từ bất kỳ nguồn nào
 đến đích là mạng 10.10.10.0/28
 (10.10.10.0 đến 10.10.10.15) trên cổng
 53.

Hình 4.9.1: Rule cho phép các phòng ban kết nối vào vùng Server thông qua port 53

```

- grant: deny
  protocol: tcp
  source:
    address: any
  destination:
    address: any
    port_protocol:
      eq: 53
- grant: deny
  protocol: udp
  source:
    address: any
  destination:
    address: any
    port_protocol:
      eq: 53

```

Hình 4.9.2: Từ chối mọi gói tin DNS TCP và UDP đến bất kỳ đích nào (địa chỉ đích và cổng 53).

```

- grant: permit
  protocol: tcp
  source:
    address: 192.168.14.0
    wildcard_bits: 0.0.0.127
  destination:
    address: any
    port_protocol:
      eq: 3389
- grant: deny
  protocol: tcp
  source:
    address: any
  destination:
    address: 10.10.10.0
    wildcard_bits: 0.0.0.15
    port_protocol:
      eq: 3389

```

Cho phép truy cập RDP (Remote Desktop Protocol) từ mạng của phòng ban IT đến bất kỳ đích nào trên cổng 3389:

Từ chối truy cập RDP từ bất kỳ nguồn nào đến mạng DMZ trên cổng 3389

Hình 4.9.3: Thiết lập Rule chỉ cho phòng ban IT remote desktop đến Server

```

grant: permit
protocol: tcp
source:
  address: 192.168.14.0
  wildcard_bits: 0.0.0.127
destination:
  address: any
  port_protocol:
    eq: 22
- grant: permit
  protocol: tcp
  source:
    address: 192.168.14.0
    wildcard_bits: 0.0.0.127
  destination:
    address: any
    port_protocol:
      eq: 23
- grant: permit
  protocol: tcp
  source:
    host: 172.10.1.30
  destination:
    address: any
    port_protocol:
      eq: 22
- grant: permit
  protocol: tcp
  source:
    host: 172.10.1.30
  destination:
    address: any
    port_protocol:
      eq: 23

```

Cho phép truy cập SSH và telnet từ mạng phòng ban IT đến bất kỳ đích nào.

Cho phép truy cập SSH và telnet từ host 172.10.1.30 đến bất kỳ đích nào

Deny any any

Hình 4.9.4: Thiết lập rule cho phép phòng ban IT có thể telnet và SSH đến tất cả các thiết bị

```

- name: Apply ACL to interfaces
  cisco.ios.ios_acl_interfaces:
    config:
      - name: "{{ item }}"
        access_groups:
          - afi : "ipv4"
            acls:
              - name: 110
                direction: out
        state: merged
    with_items:
      - "ethernet0/0"
      - "ethernet0/1"
      - "Port-channel1"

```

Hình 4.9.5: Áp dụng các rule lên các interface theo chiều out

Với việc kiểm soát truy cập vào thiết bị thì ACL sẽ được áp lên toàn bộ các thị mạng (không chỉ riêng switch distribution)

```

config:
  acl:
    - name: SSH_Telnet
      acl_type: standard
      aces:
        - grant: permit
          source:
            host: "172.10.1.30"
        - grant: permit
          source:
            host: "10.10.10.10"
        - grant: permit
          source:
            address: "192.168.14.0"
            wildcard_bits: "0.0.0.127"
  state: replaced

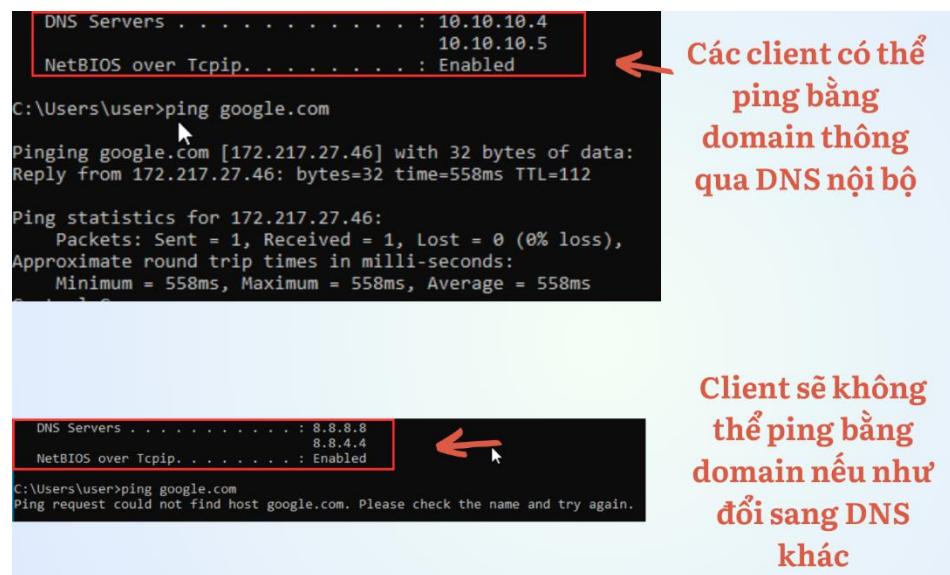
- name: Apply ACL to vty 0 4
  cisco.ios.ios_config:
    lines:
      - access-class SSH_Telnet in
    parents: "line vty 0 4"

```

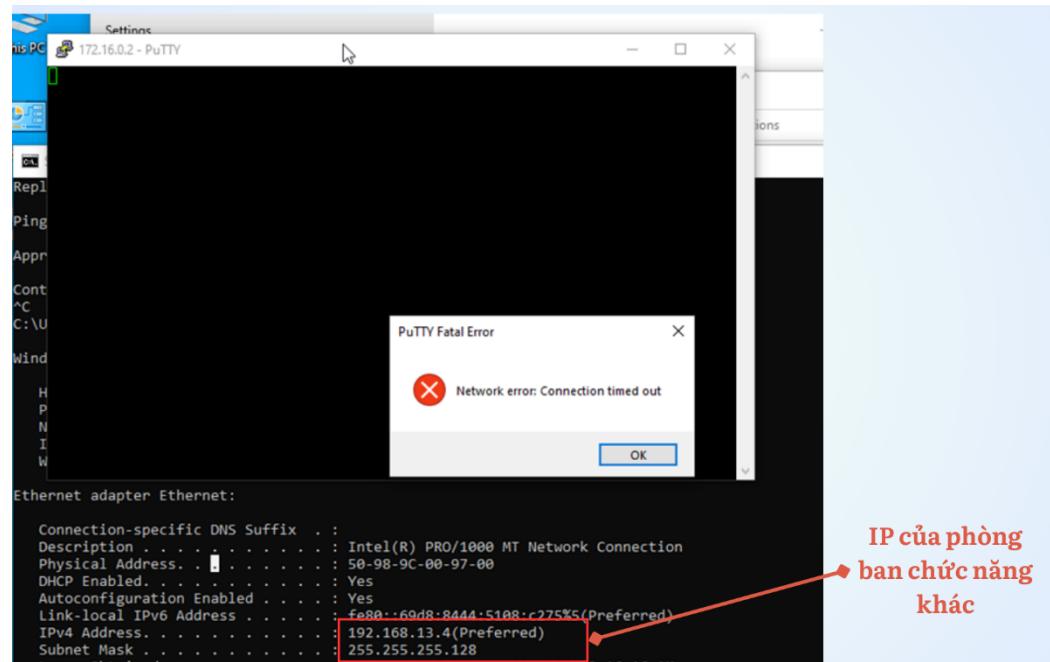
Cho phép truy cập từ host
172.10.1.30, 10.10.10.10.
và cho phép truy cập từ mạng của
phòng ban IT.

Apply ACL vào line vty 0 4

Hình 4.9.6: Cấu hình ACL telnet và SSH cho các thiết bị



Hình 4.9.7: Các máy client chỉ có thể ping bằng domain thông qua DNS server nội bộ



Hình 4.9.8: Các phòng ban chức năng không phải phòng ban IT sẽ không thể SSH vào mọi thiết bị

172.16.0.2 - PuTTY

```

login as: adminlocalHO
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
KHONG PHAN SU MIEN VAOCorel>

```

Select Command Prompt

```
C:\Users\user>ipconfig
```

```
Windows IP Configuration
```

Ethernet adapter Ethernet:

```

Connection-specific DNS Suffix . . . .
Link-local IPv6 Address . . . . . : fe80::698:8444%5
IPv4 Address. . . . . : 192.168.14.4
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 192.168.14.1

```

phòng IT ở HO
có thể SSH vào
thiết bị Corel

IP của phòng
ban IT ở site HO

Hình 4.9.9: Phòng ban IT ở HO có thể SSH vào các thiết bị HO

172.16.1.2 - PuTTY

```

login as: duyen.cnk
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
KHONG PHAN SU MIEN VAO
Corel_MB>

```

Command Prompt

```
C:\Users\user>ipconfig
```

```
Windows IP Configuration
```

Ethernet adapter Ethernet:

```

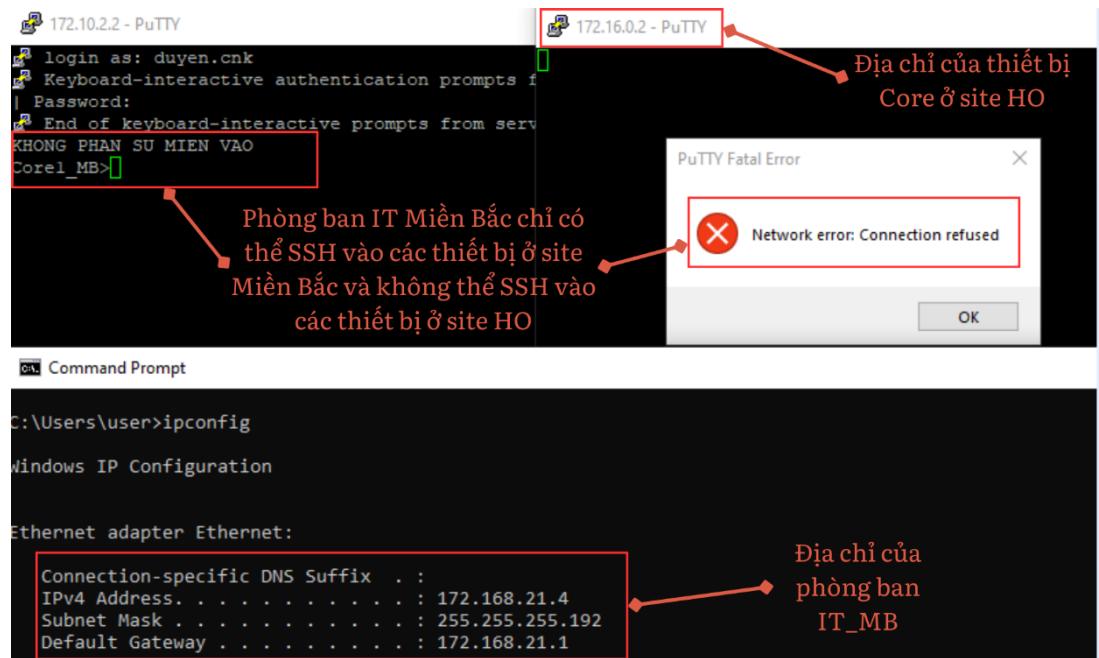
Connection-specific DNS Suffix . . .
IPv4 Address. . . . . : 192.168.14.5
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 192.168.14.1

```

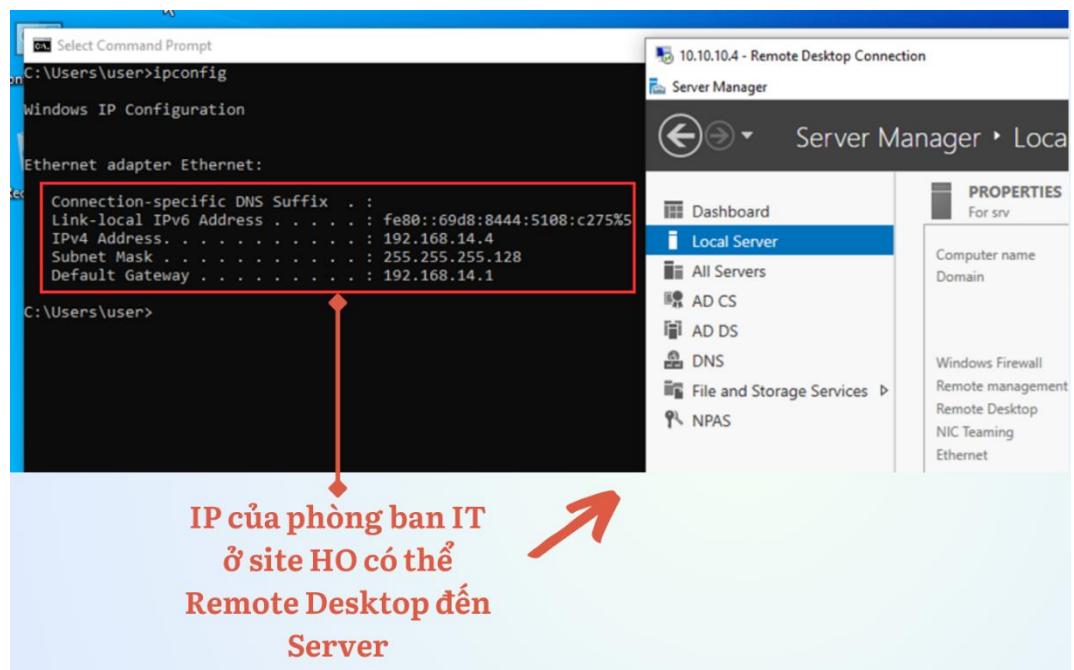
Phòng ban IT có thể SSH
vào các thiết bị ở site
Miền Bắc

Địa chỉ của
phòng ban
IT_HO

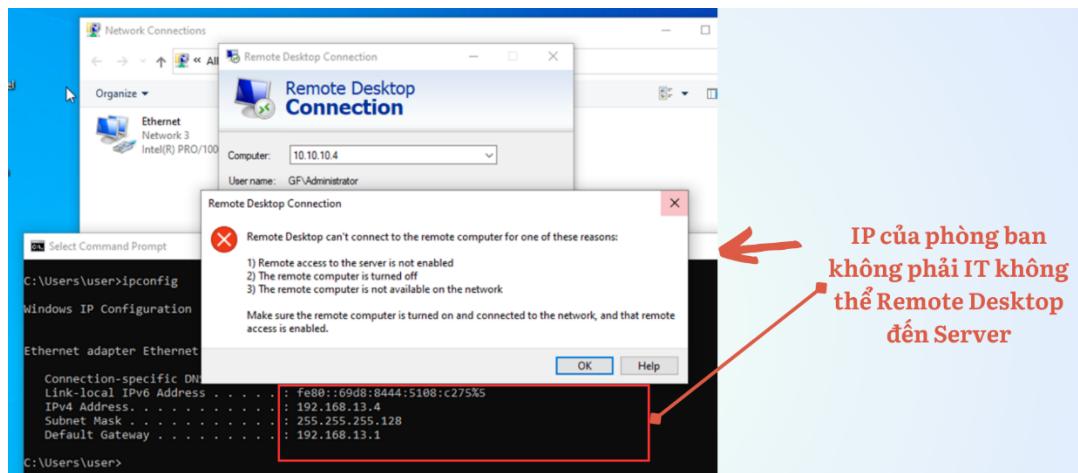
Hình 4.9.10: Phòng ban IT ở site HO có thể SSH vào các thiết bị ở site miền Bắc



Hình 4.9.11: Phòng ban IT ở site miền Bắc chỉ có thể SSH vào các thiết bị ở Miền Bắc nhưng không thể SSH vào các thiết bị ở site HO



Hình 4.9.12: Phòng ban IT ở site HO có thể Remote Desktop vào Server



Hình 4.9.13: Các phòng ban chức năng khác sẽ không thể remote desktop vào Server

4.10 Network Access Control

Để tăng cường bảo mật mạng bằng cách kiểm soát và quản lý quyền truy cập của các thiết bị và người dùng trong doanh nghiệp, chúng ta cần cấu hình NAC nhằm mục đích ngăn chặn sự truy cập trái phép bằng cách bật chế độ xác thực, các client muốn sử dụng thiết bị trong doanh nghiệp cần phải xác thực bằng tài khoản do doanh nghiệp cung cấp, để tránh việc người lạ sử dụng trái phép các thiết bị của doanh nghiệp.

Chúng ta sẽ cấu hình trên các thiết bị Switch như sau:

```

- name: Configure Login Device With Authentication 802.1x
  hosts: [CORE:DIS:Access]
  gather_facts: no
  vars_files:
    - pass.yml
  tasks:
    - name: Enable Authentication 802.1x
      ios_config:
        lines:
          - aaa new-model
          - aaa authentication login default group radius local
          - aaa authorization exec default group radius local
          - radius server WINSERVER
          - address ipv4 10.10.10.4
          - key "{{keyAAA}}"

    - name: Apply to vty 0 4
      cisco.ios.ios_config:
        lines:
          - login authentication default
        parents: "line vty 0 4"

    - name: Save configuration
      cisco.ios.ios_command:
        commands:
          - write

```

Bên phải code có các chú thích:

- Bật chế độ AAA
- Xác định cấu hình xác thực radius cho quá trình login, nếu máy chủ Radius không phản hồi, quá trình xác thực này sẽ chuyển sang xác thực local
- Xác định cấu hình phân quyền thực thi tương tự như xác thực đăng nhập
- Xác định rằng quá trình đăng nhập trên line vty 0 4

Hình 4.10.1: Cấu hình xác thực 802.1x trên các thiết bị Switch

Tiếp tục kích hoạt các cài đặt cơ bản để hỗ trợ xác thực 802.1x trên các switch access với từng interface cụ thể:

```

tasks:
  - name: Enable Authentication 802.1x
    ios_config:
      lines:
        - aaa authorization network default group radius
        - dot1x system-auth-control
        - aaa authentication dot1x default group radius

```

Bật xác thực 802.1x

kiểm soát port auto để xác định trạng thái port dựa trên kết quả xác thực.

Cho phép nhiều thiết bị kết nối đến cổng được xác thực.

Chọn phương thức xác thực là pae

Cấu hình xác thực trên F1_HO với tất cả các interface trừ interface nối với Switch OOB (e0/3)

Cấu hình tương tự với các Switch còn lại

Hình 4.10.2: Cấu hình Authentication 802.1x trên các thiết bị Switch Access

Sau khi đã chạy cấu hình trên, chúng ta sẽ cấu hình NPAS trên Server Radius sau đó. Mục đích của việc này sẽ giúp kiểm soát quyền truy cập vào mạng, cung cấp một lớp bảo vệ bổ sung để ngăn chặn sự truy cập trái phép và bảo vệ mạng khỏi các mối đe dọa từ các thiết bị không an toàn.

4.11 SNMP

SNMP là giao thức quan trọng trong việc quản lý mạng vì nó sẽ cung cấp các chức năng cho việc giám sát và quản lý các thiết bị mạng, cụ thể hơn là Zabbix sẽ sử dụng SNMP để thu thập thông tin từ các thiết bị mạng có trong hệ thống.

```

- name: Configure SNMP on network devices
  hosts: [CORE:DIS:Access]
  gather_facts: no
  vars_files:
    - pass.yml

  tasks:
    - name: Configure SNMP community and traps
      cisco.ios.ios_config:
        lines:
          - snmp-server community GreenFeedCompanySNMP ro
          - snmp-server enable traps snmp
          - snmp-server host 10.10.10.12 version 2c GreenFeedCompanySNMP udp-port 162

    - name: Save configuration
      cisco.ios.ios_command:
        commands:
          - write

```

Hình 4.11.1: Cấu hình SMNP cho các Switch

Đoạn code trên sẽ khai báo giá trị *community* có tên là “*GreenFeedCompanySNMP*” với quyền read only, sau đó sẽ bật chức năng gửi các sự kiện SNMP traps để cho phép các thiết bị gửi các thông báo SNMP traps khi có sự cố xảy ra. Host 10.10.10.12 chính là máy chủ Zabbix của hệ thống, Zabbix sau khi được thiết lập sẽ có thể nhận các traps từ thiết bị và xác định các thông số liên quan.

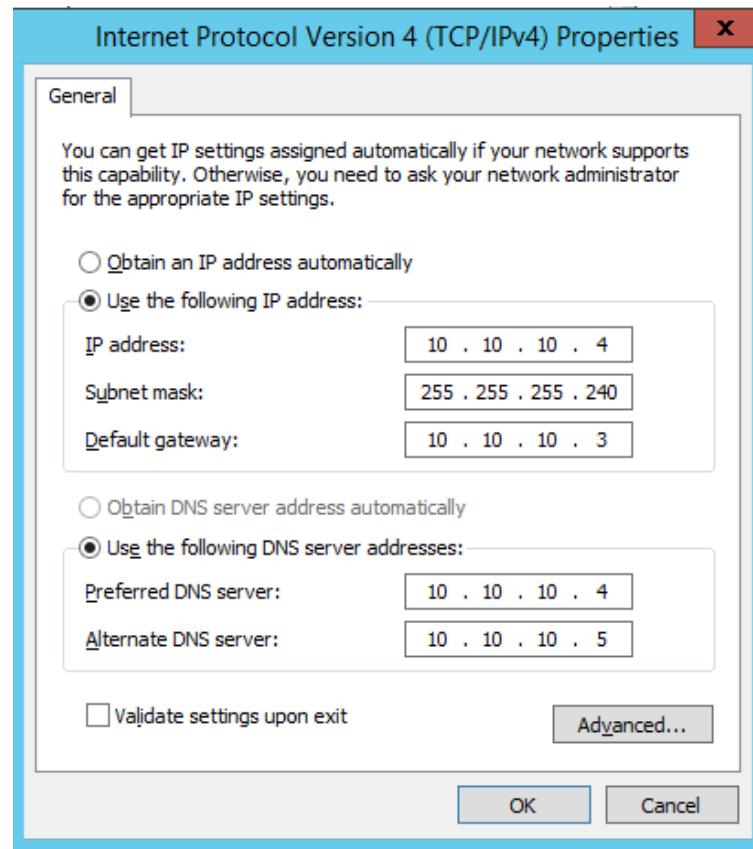
4.12 Cấu hình Server

4.12.1 Primary DNS Server và Alternative DNS

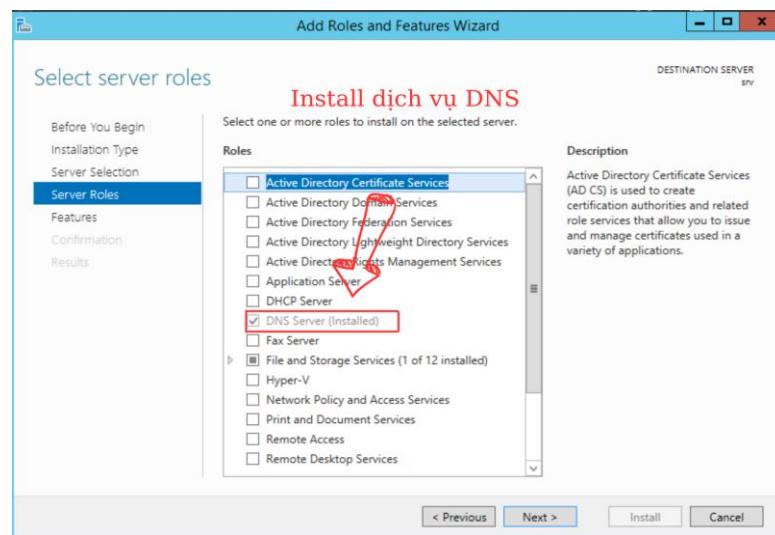
❖ Primary DNS Server

Trong đồ án này, hệ thống mạng của chúng ta sẽ có hai site bao gồm site chính là head office và chi nhánh ở miền Bắc, cho nên chúng ta sẽ sử dụng 2 server và cấu hình các dịch vụ trên 2 server này.

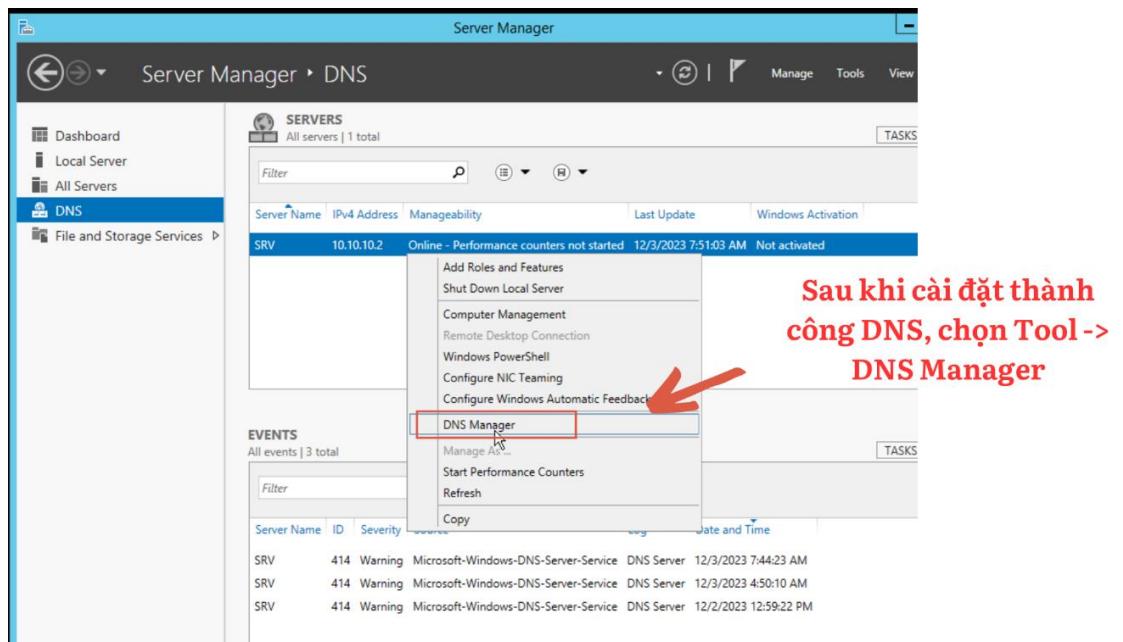
Sau khi khởi động Server, chúng ta cần gán địa chỉ IP cho thiết bị



Hình 4.12.1.1: Set IP cho Server



Hình 4.12.1.2: Install DNS Server ở mục add Role and Feature

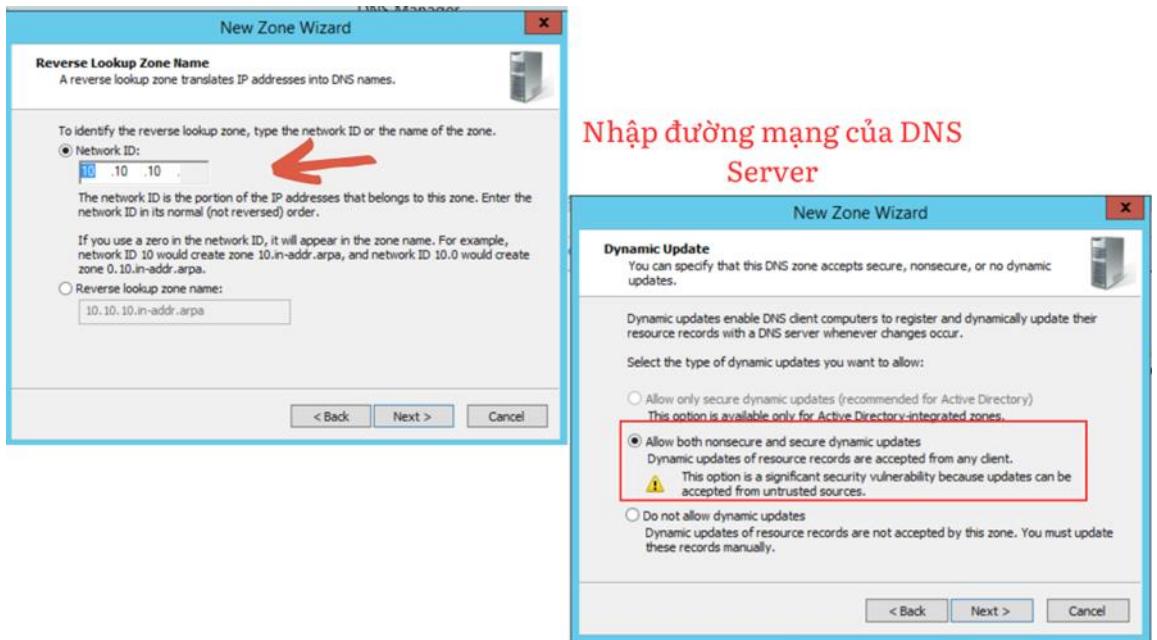


Hình 4.12.1.3: Sau khi đã cài đặt thành công DNS Server, tiến hành vào DNS Manager để cấu hình

Chúng ta sẽ cần chú ý đến hai mục là Forward Lookup Zones và Reverse Lookup Zone. Đây là hai vùng có trách nhiệm giúp cho máy chủ DNS chuyển đổi giữa địa chỉ IP và tên miền và ngược lại.

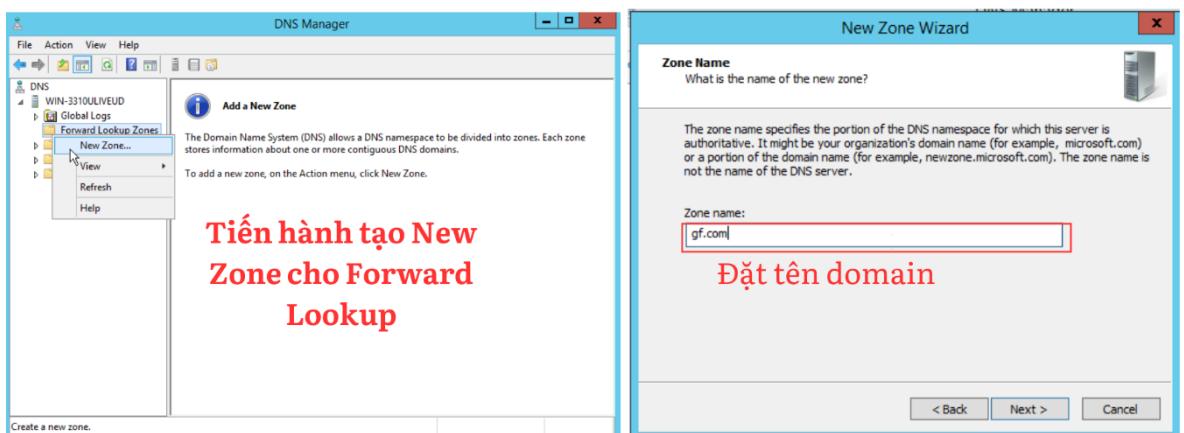
Đối với Forward Lookup Zone: được sử dụng để chuyển đổi tên miền thành địa chỉ IP. Khi một máy client truy cập một tên miền bất kỳ, máy chủ DNS sẽ tra cứu trong vùng này để xác định IP tương ứng với tên miền đó.

Đối với Reverse Lookup Zone: được sử dụng để chuyển đổi ngược lại từ IP về tên miền. Khi một máy client nhập địa chỉ IP trên thanh tìm kiếm, máy chủ DNS sẽ tra cứu trong Reverse Lookup Zone để xác định tên miền tương ứng.



Hình 4.12.1.4: Nhập đường mạng của DNS Server

Nhập dải mạng của Server sử dụng sau đó chọn **Allow both nonsecure and secure dynamic updates** để cập nhật tự động từ các máy khách DNS mà không yêu cầu xác thực hoặc chỉ yêu cầu xác thực an toàn.



Hình 4.12.1.5: Tương tự Tạo Zone mới ở vùng Forward

Ta sẽ có một số bản ghi cơ bản mà chúng ta sẽ gặp sau khi tạo zone name

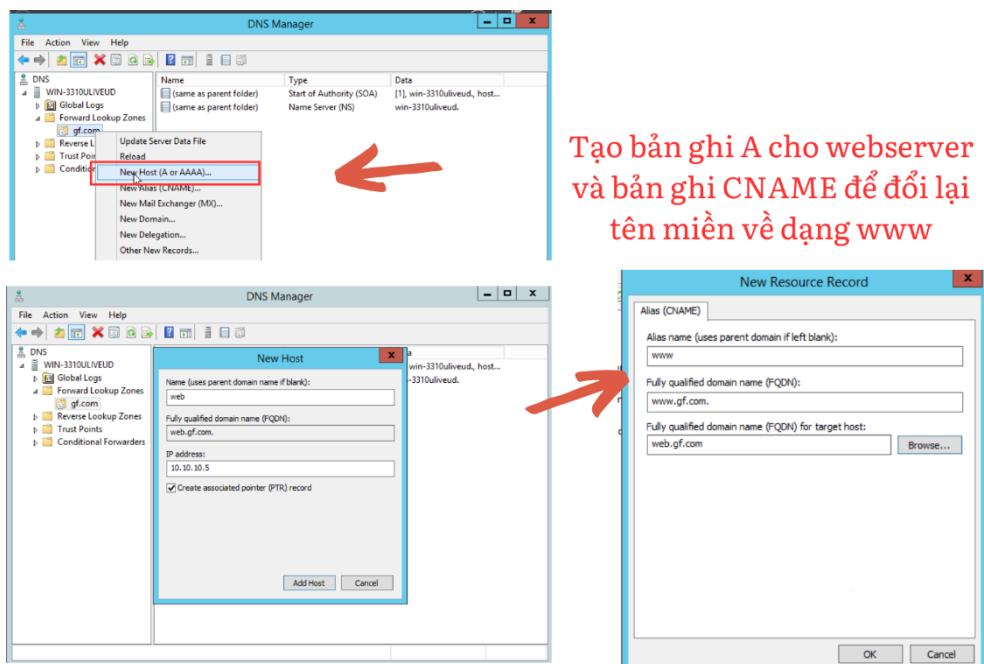
- Bản ghi A và AAAA: đây là hai bản ghi dùng để ánh xạ một tên miền với A là địa chỉ IPv4 và AAAA là địa chỉ IPv6

Ví dụ: ta có một domain web.gf.com với bản ghi A: 10.10.10.5

- Bản ghi CNAME: đây là bản ghi được sử dụng để tạo ra một bản định danh chính thức cho một tên miền

Ví dụ: Ta có web.gf.com là tên miền mặc định của trang web và chúng ta muốn đổi cấu trúc của tên miền thành: www.gf.com thì chúng ta sẽ sử dụng bản ghi CNAME để thực hiện điều đó.

- Bản ghi MX(Mail Exchange Record): Đây là bản ghi dùng để xác định máy chủ email chấp nhận thư điện tử cho một tên miền cụ thể

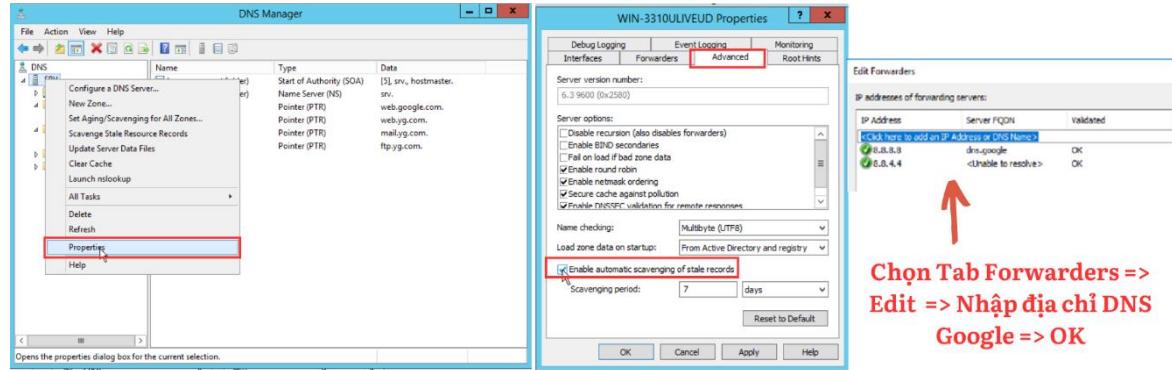


Hình 4.12.1.6: Tạo bản ghi A và CNAME cho domain của Web Server

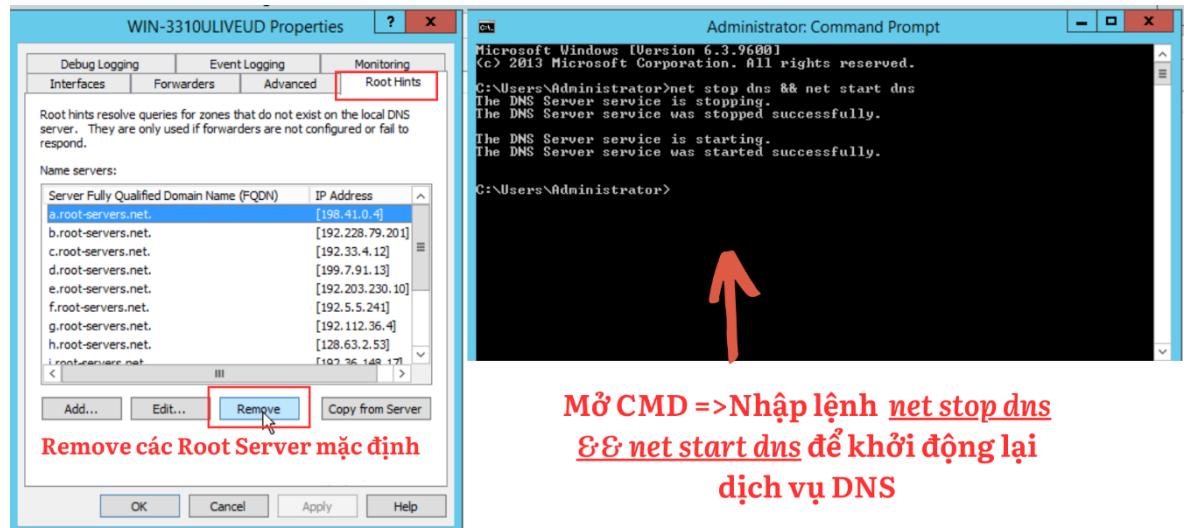
Thực hiện cài đặt DNS recursive

- Chọn **Properties** tại Server đang chạy dịch vụ DNS.
- Tại tab **Advanced**, tích chọn **Enable automatic scavenging of stale record** để tự động loại bỏ các bản ghi DNS không còn được sử dụng ("stale records"). Điều này giúp giữ cho cơ sở dữ liệu DNS sạch sẽ và hiệu quả hơn bằng cách loại bỏ các bản ghi không còn cần thiết.

- Tại tab **Forwarders**, chọn **Edit** và nhập địa chỉ DNS Google sau đó chọn **OK**.



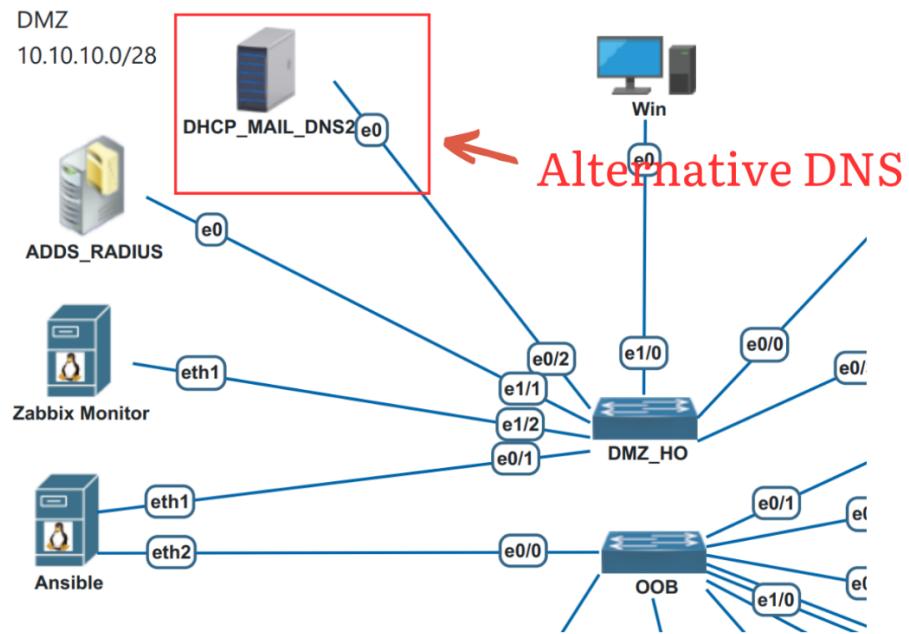
Hình 4.12.1.7: Để thực hiện phân giải tên miền các địa chỉ ở bên ngoài mạng LAN ta sẽ cài đặt DNS recursive



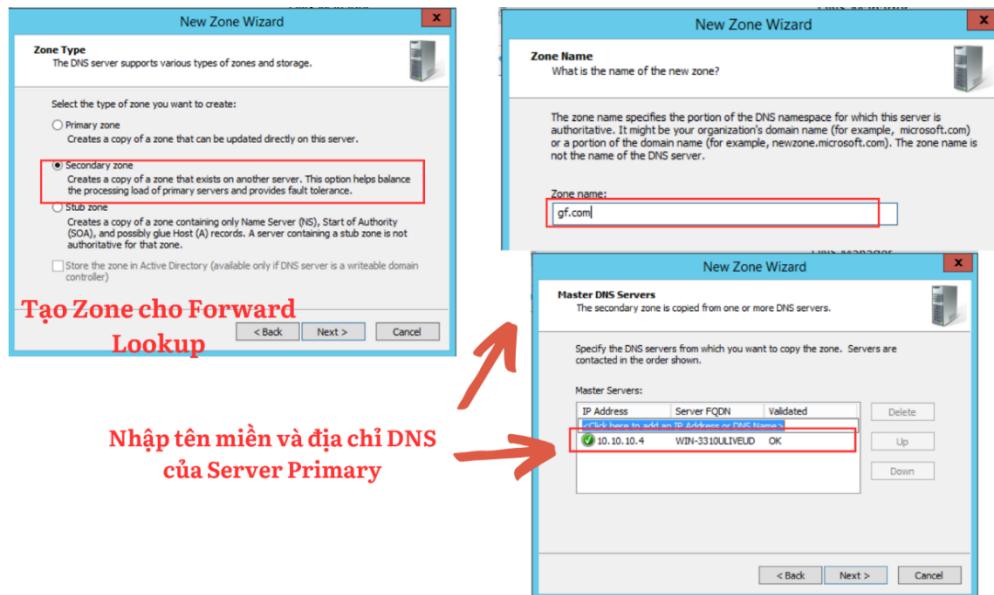
Hình 4.12.1.8: Mở CMD -> Nhập lệnh **net stop dns && net start dns** để khởi động lại dịch vụ DNS

❖ Alternative DNS

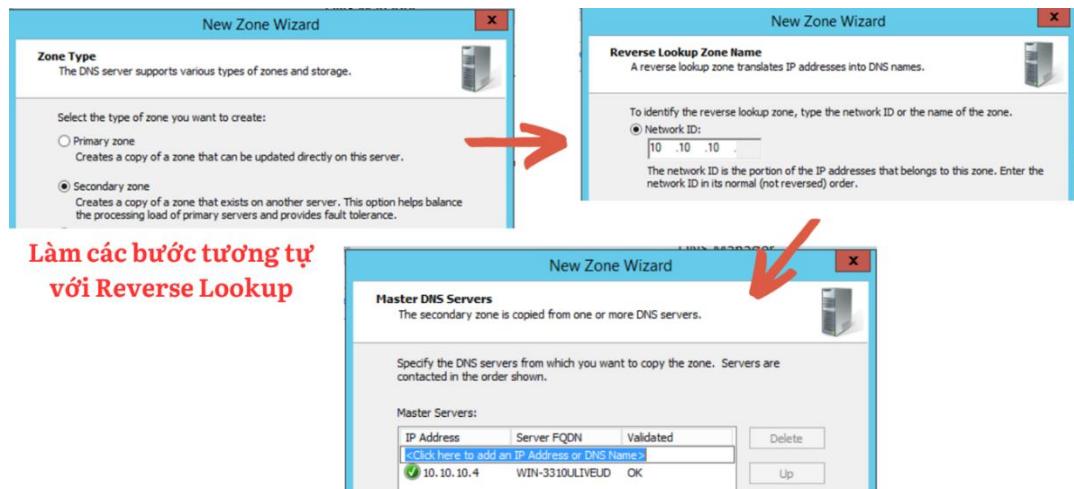
Các bước cấu hình DNS Alternative



Hình 4.12.1.9: Sử dụng Server trên để cấu hình DNS Alternative

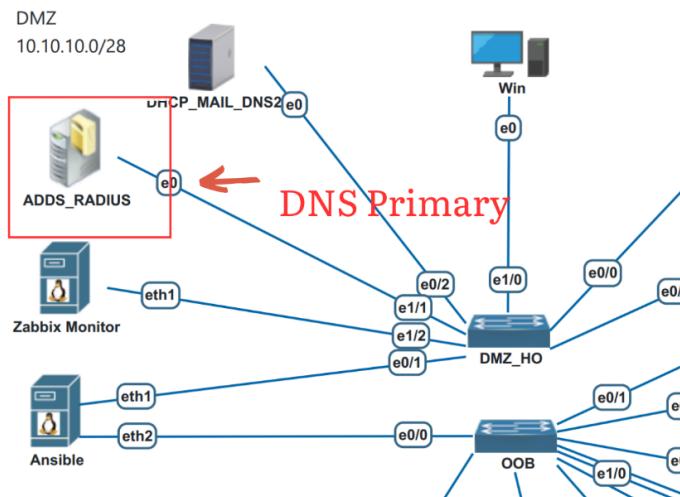


Hình 4.12.1.10: Tạo Zone cho Forward Lookup Zone

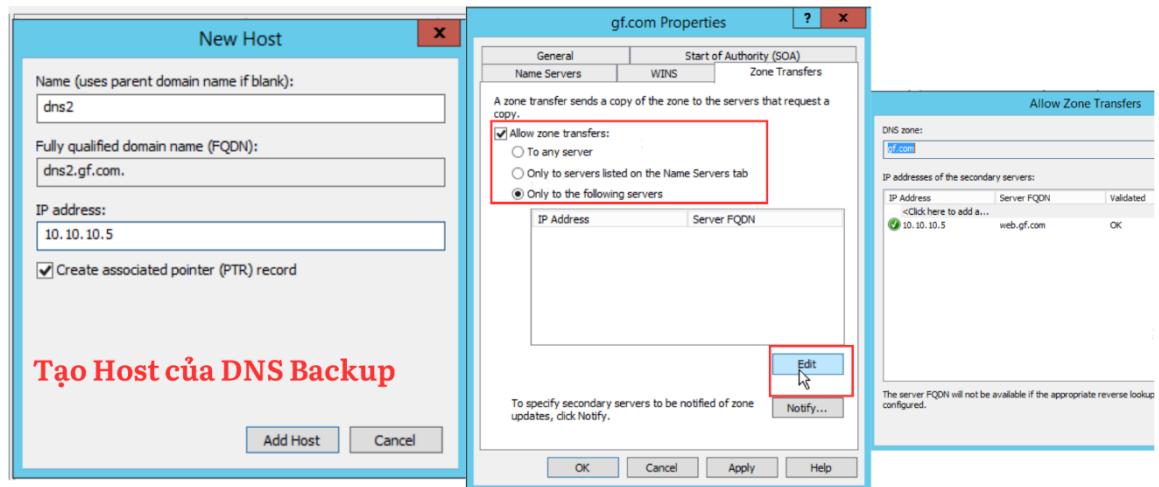


Hình 4.12.1.11: Tạo Zone cho Reverse Lookup Zone

Sang DNS Primary cấu hình:



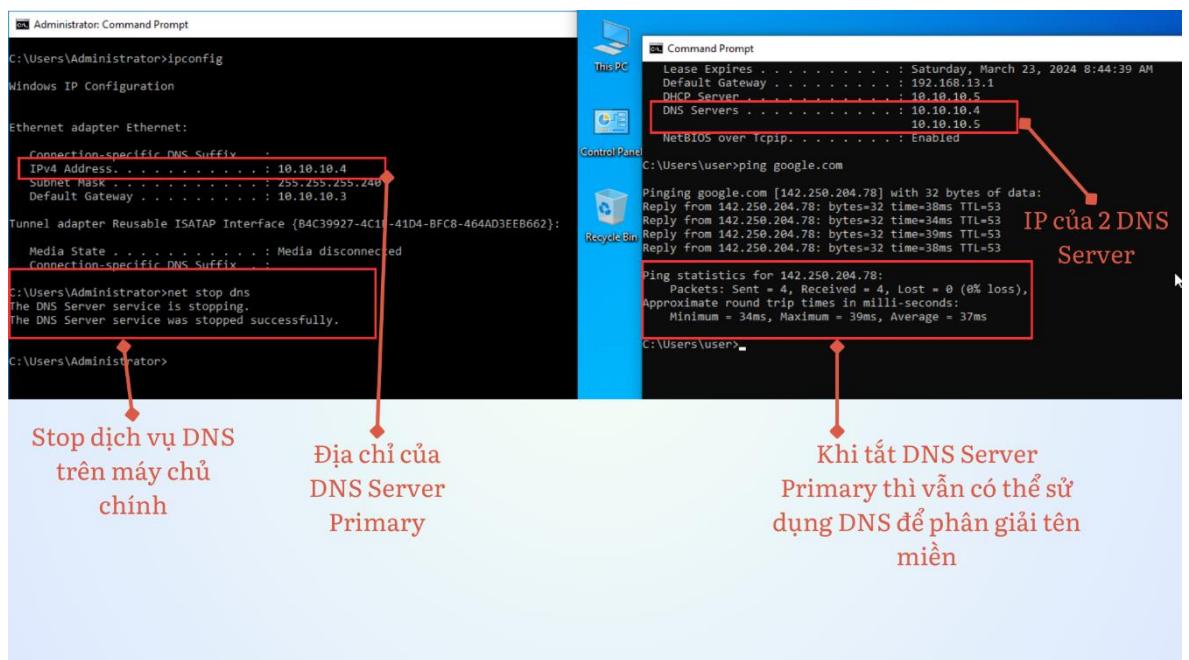
Hình 4.12.1.12: Vào DNS Primary => Properties



Thực hiện tương tự với Reverse Lookup và trên Server Backup

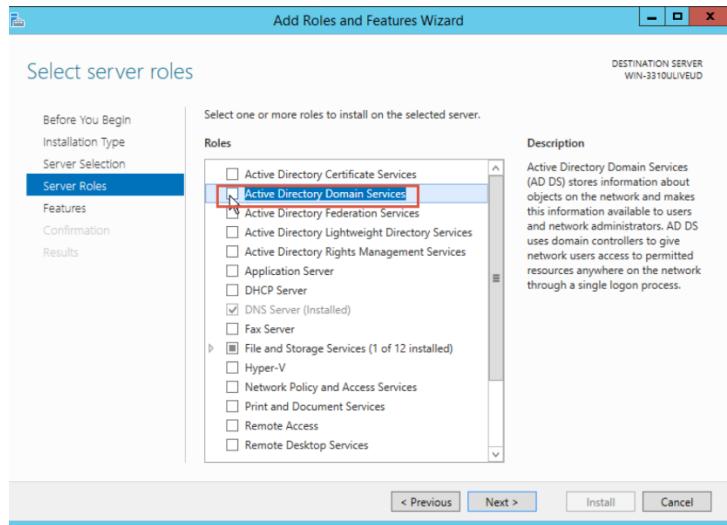
Hình 4.12.1.13: Cấu hình backup trên cả hai server DNS

Sau khi đã cấu hình xong hai dịch vụ trên, chúng ta sẽ thử tắt dịch vụ DNS trên Primary DNS Server (IP 10.10.10.4). Và sau khi tắt dịch vụ DNS thì hệ thống sẽ tự động trỏ đến DNS backup Server và vẫn có thể phân giải tên miền bình thường như hình 4.12.1.14.

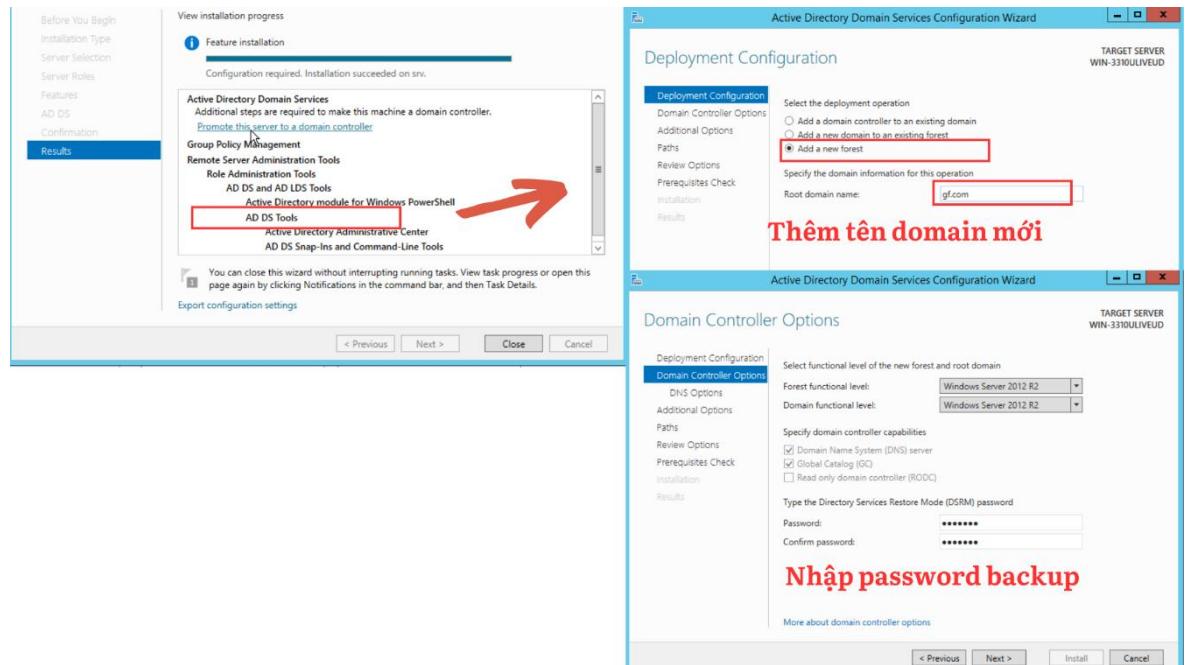


Hình 4.12.1.14: Khi dịch vụ DNS trên máy Primary tắt thì hệ thống sẽ tự động trỏ đến DNS backup.

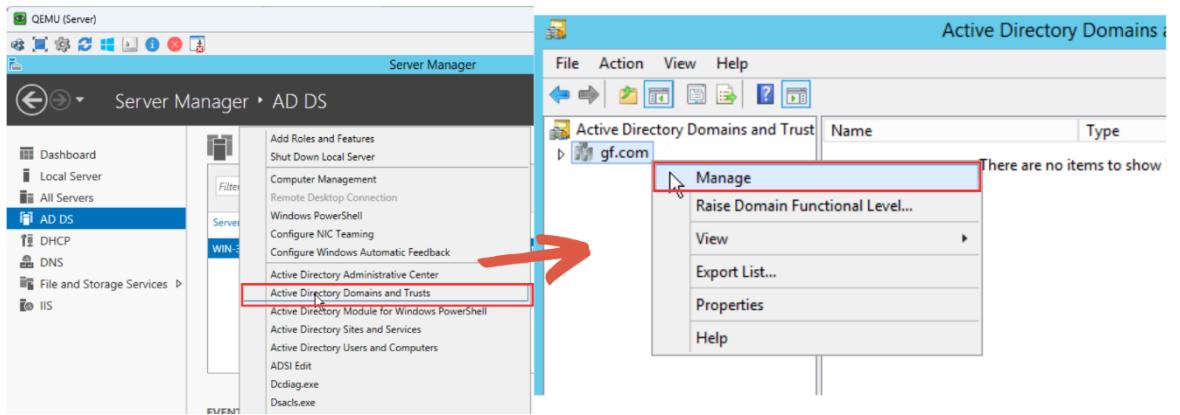
4.12.2 Active Directory Domain Service



Hình 4.12.2.1: Install ADDS

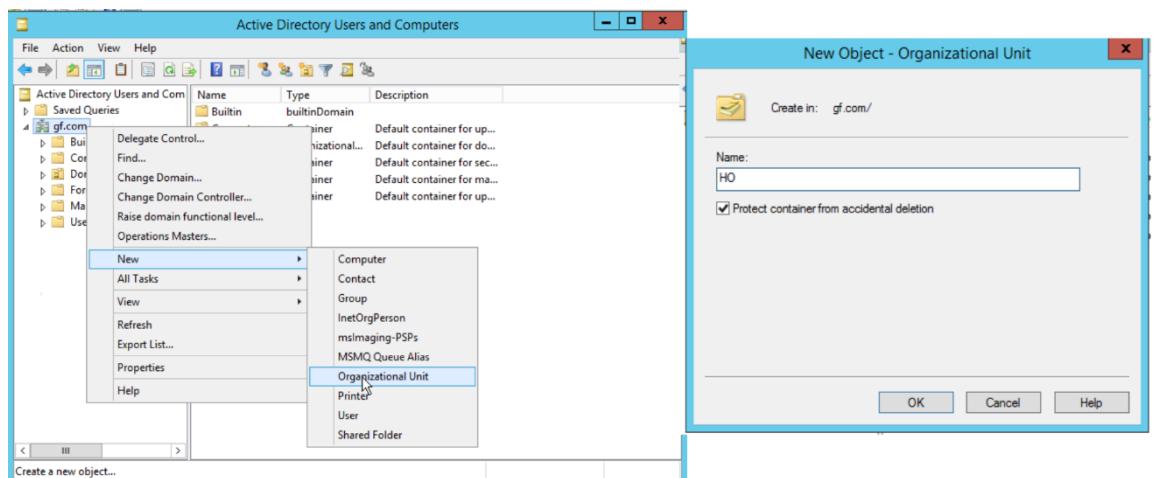


Hình 4.12.2.2.: Thêm domain và password backup là 2024@gf



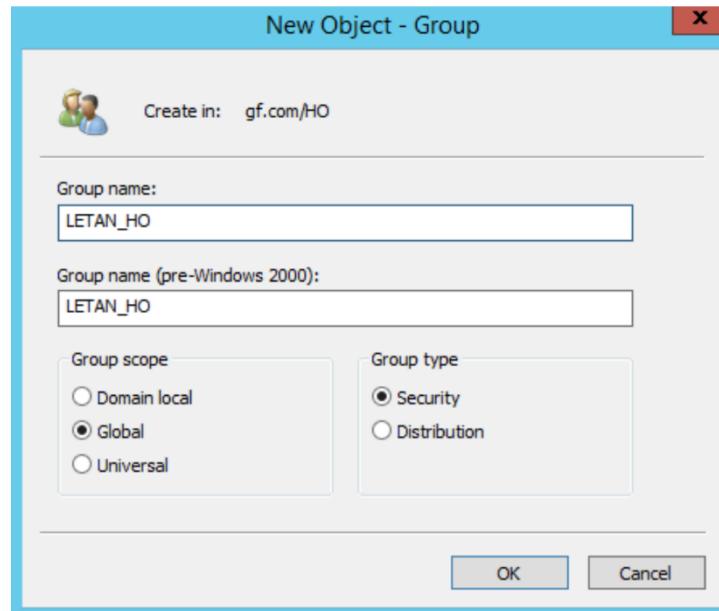
Vào mục ADD and Trusts và tiến hành quản lý AD

Hình 4.12.2.3: Quản lý ADDS



Tạo hai OU đại diện cho site Head Office
và site Branch

Hình 4.12.2.4: Tạo OU đại diện cho 2 site



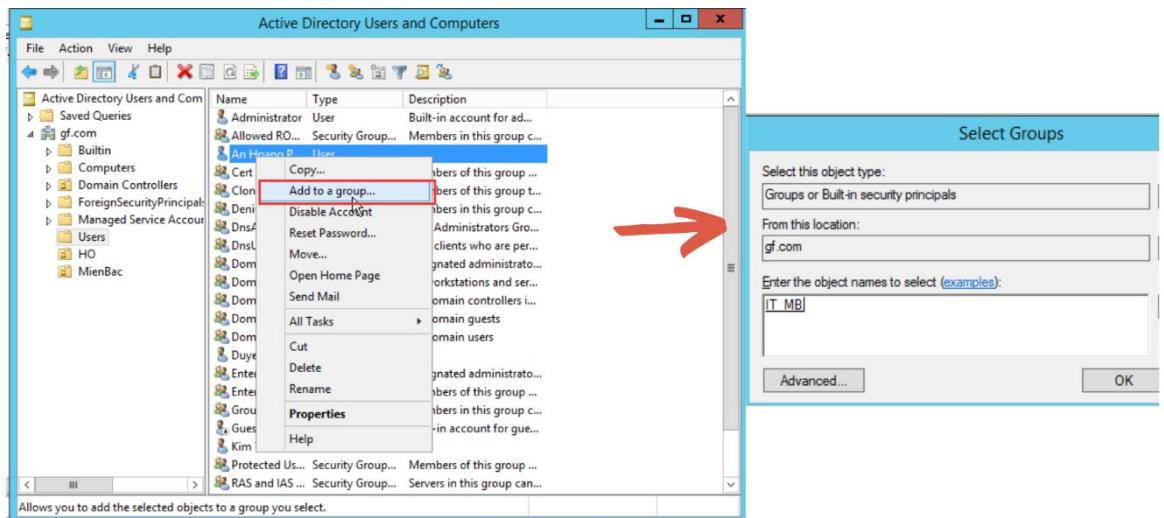
Sau khi đã tạo các OU, tiếp tục tạo các Group cho các phòng ban

Hình 4.12.2.5: Tạo Group cho các phòng ban

The screenshot displays the 'Active Directory Users and Computers' interface. On the left, a context menu is open over a list of objects, with 'New' selected. A submenu appears, showing options like Computer, Contact, Group, and User, with 'User' being highlighted. On the right, there are two separate 'New Object - User' dialog boxes. Both dialog boxes have 'Create in: gf.com/Users' at the top. The first dialog has 'First name: An', 'Last name: Hoang Phuc Thien', and 'User logon name: an.hpt'. The second dialog has 'First name: Duyen', 'Last name: Cao Nguyen Ky', and 'User logon name: duyen.cnk'. Both dialogs also have fields for 'Initials' and 'Full name'.

Hình 4.12.2.6: Tạo Users

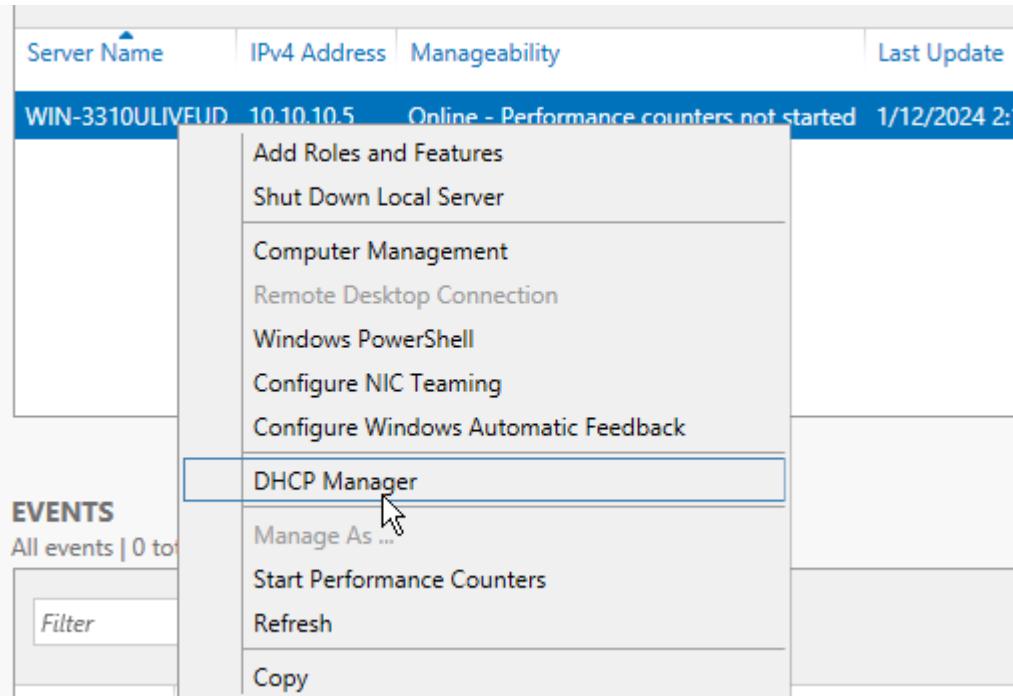
Sau khi đã tạo xong các User, chúng ta sẽ thêm các user đó vào các phòng ban phù hợp.



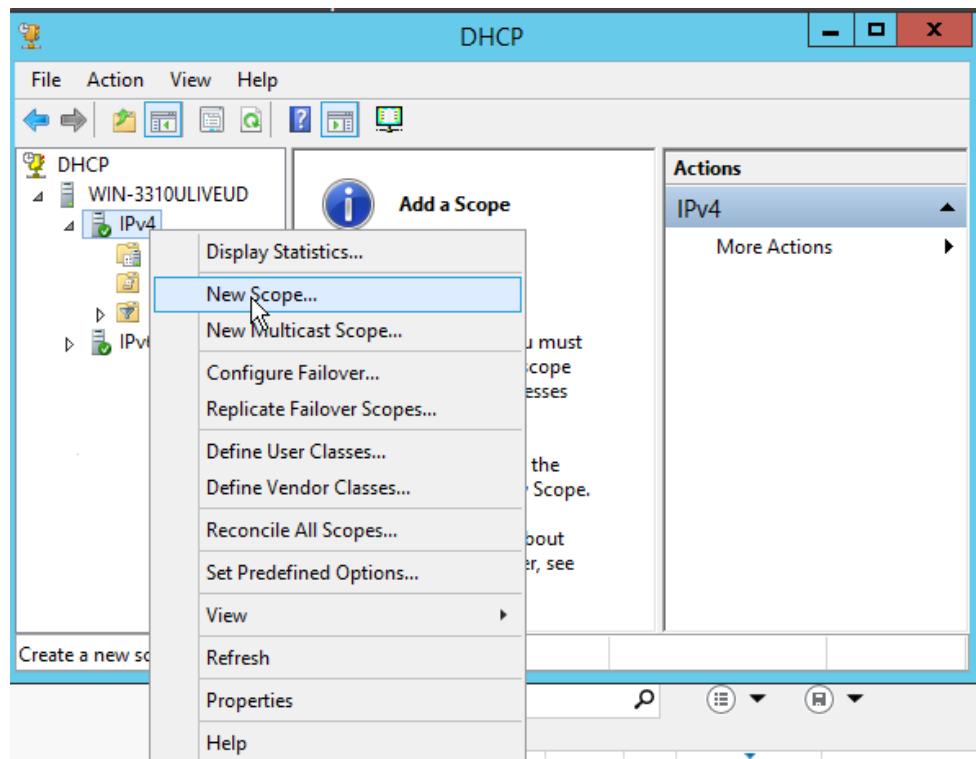
Hình 4.12.2.7: Thêm các user vào các nhóm phòng ban

4.12.3 DHCP Server

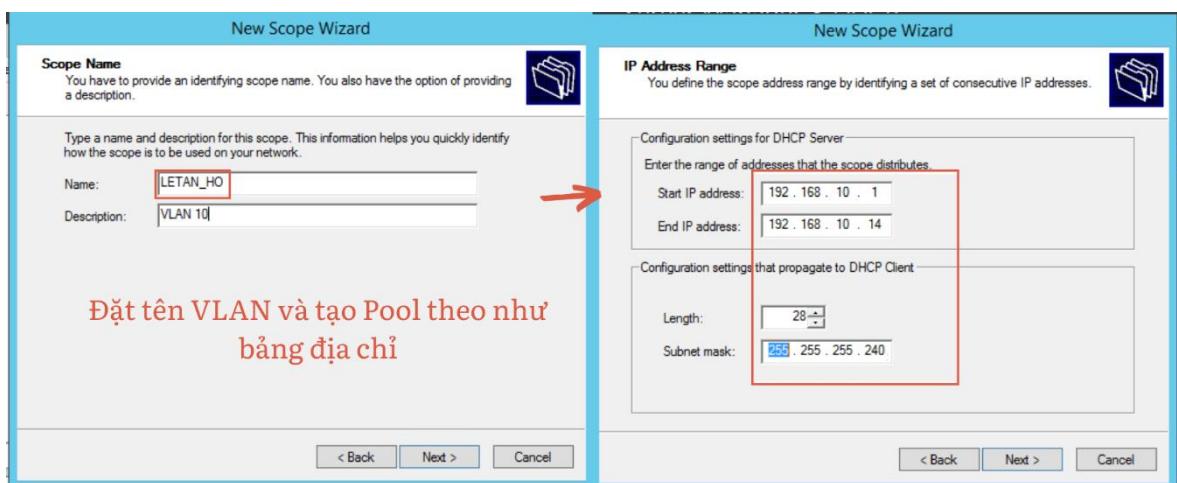
Tương tự các bước cài đặt các dịch vụ trước đó, chúng ta sẽ add Role DHCP trên DHCP Server



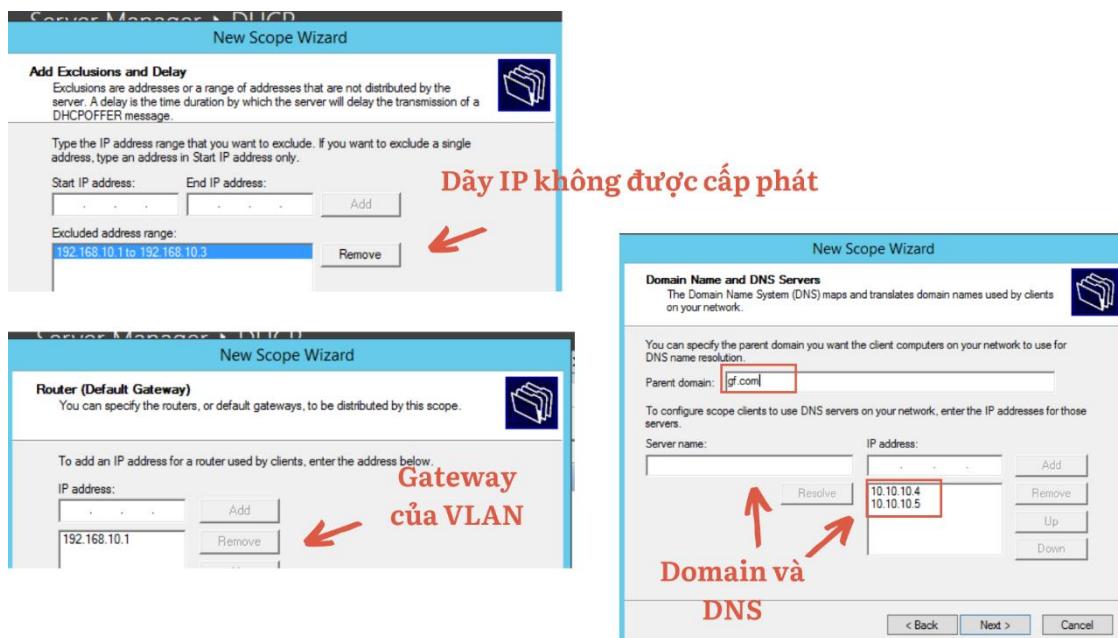
Hình 4.12.3.1: Sau khi đã cài đặt vào DHCP Manager



Hình 4.12.3.2: Chọn New Scope để tạo VLAN



Hình 4.12.3.3 : Tạo pool VLAN

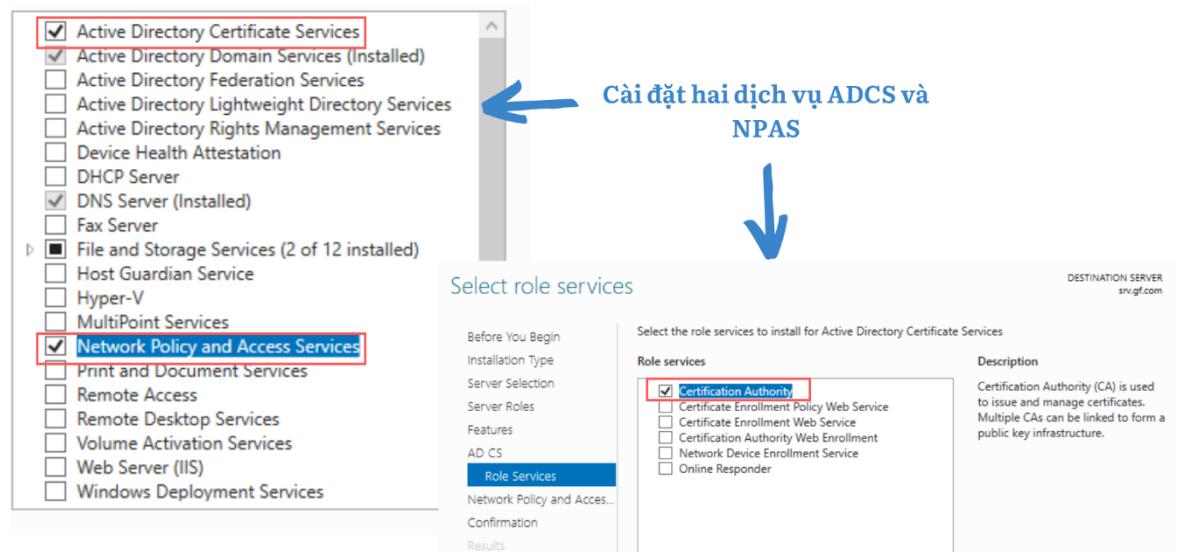


Hình 4.12.3.4: Nhập thông số cho VLAN

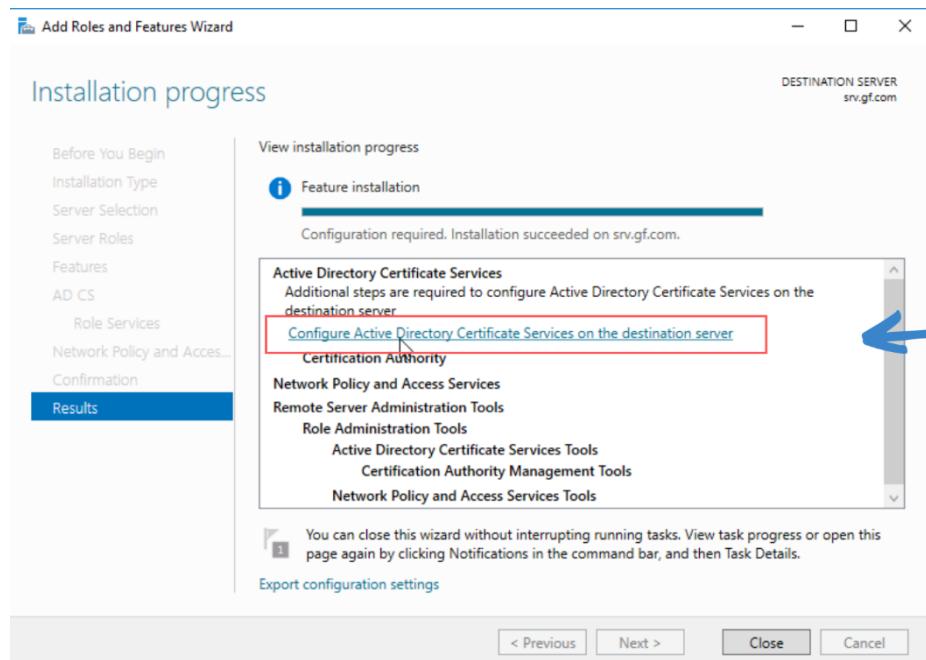
Tạo các pool VLAN còn lại ở hai site tương tự các bước trên.

4.12.4 ADCS và NPAS

Ở dự án này, nhóm sử dụng hai dịch vụ trên để cấu hình xác thực thông qua Radius Server.

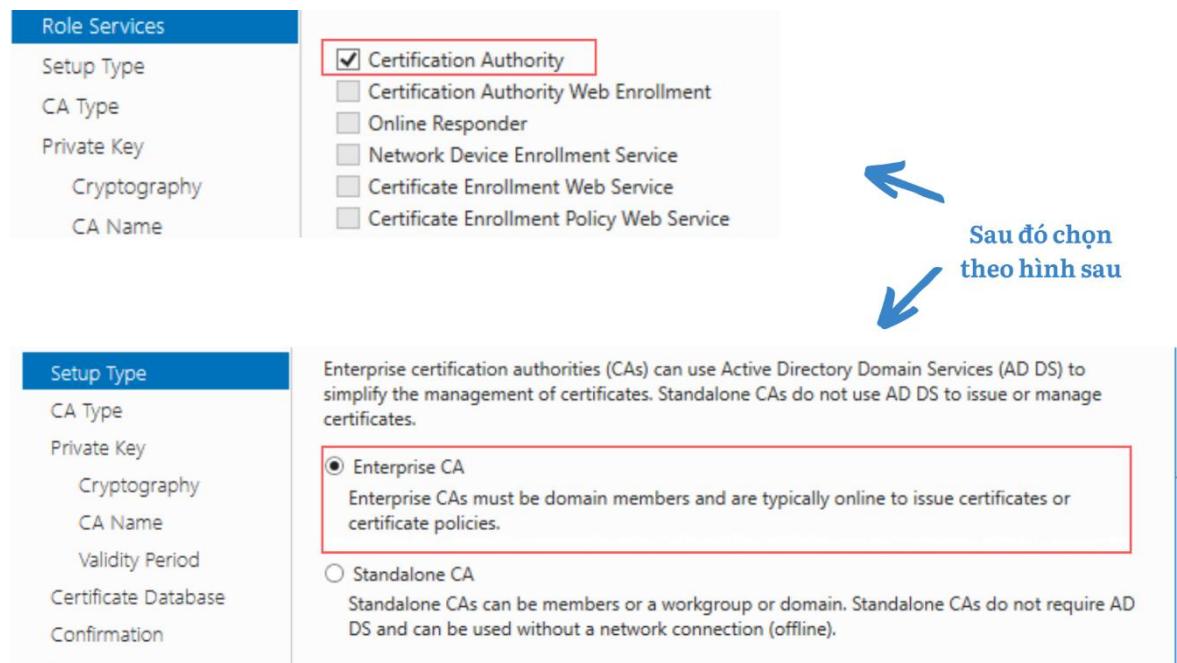


Hình 4.12.4.1: Cài đặt dịch vụ

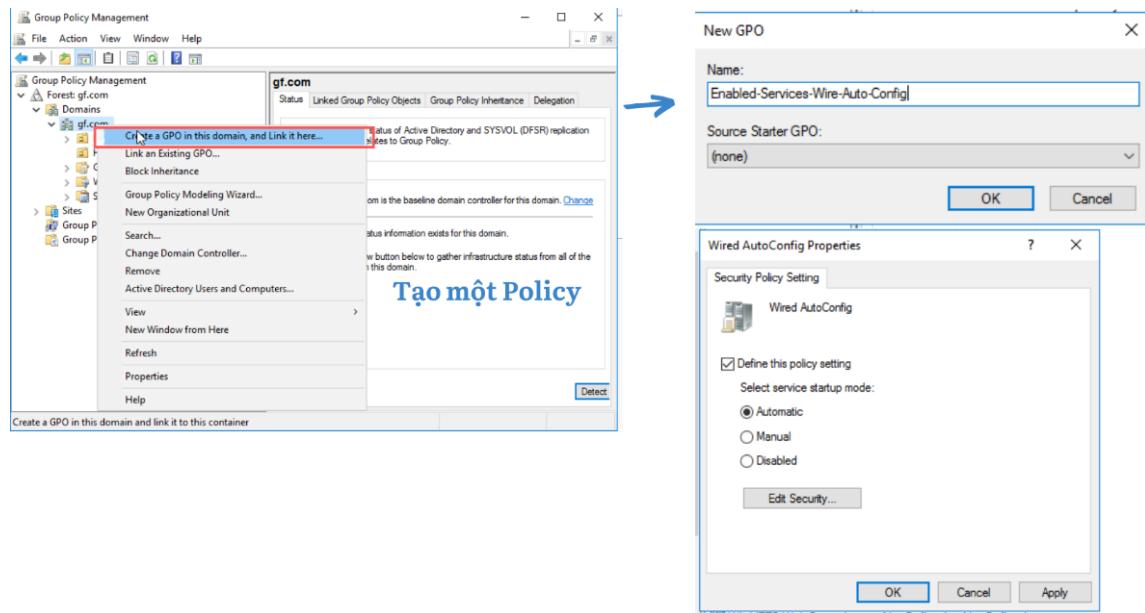


Đến giai đoạn
Result -> chọn
Cấu hình
ADCS

Hình 4.12.4.2: Cấu hình AD CS

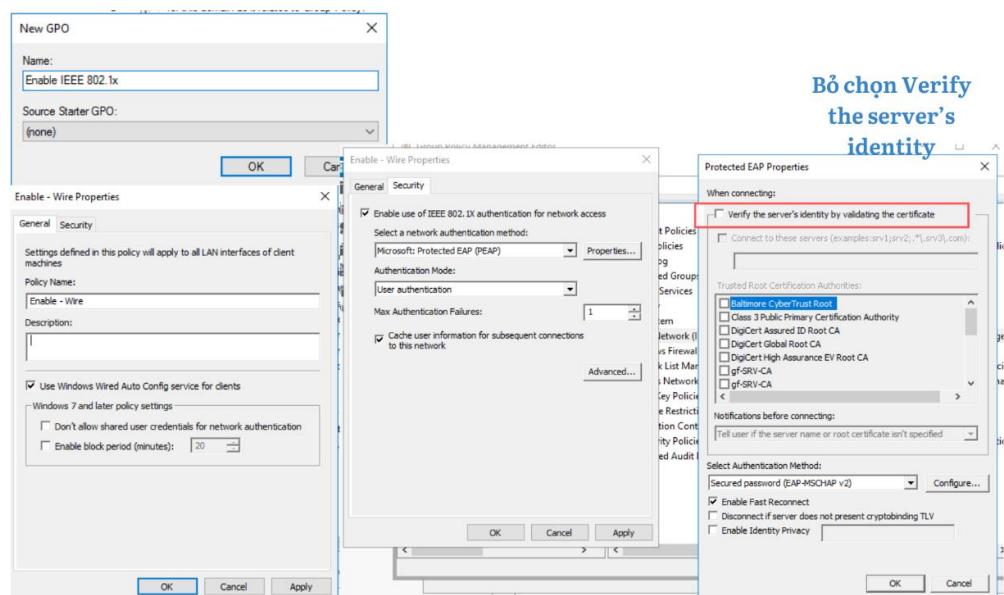


Hình 4.12.4.3: Chọn Certification Authority và chọn type là Enterprise CA



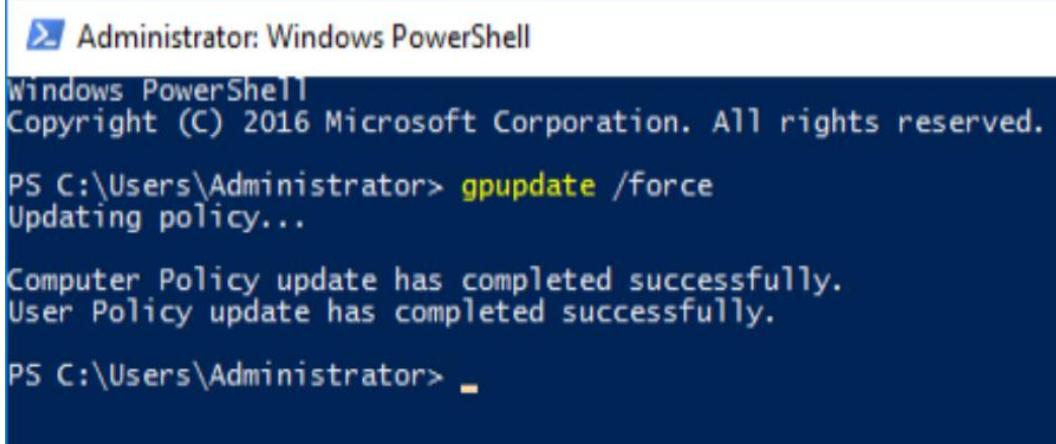
Hình 4.12.4.4: Tạo Pollicy cho phép bật Services Wired AutoConfig

Tại hộp thoại Group Policy Management Editor → ta click vào → Computer Configuration → Policies>→ Setting → Security Setting → System Services → click chuột phải vào Wired AutoConfig chọn Properties.



Hình 4.12.4.5: Tạo Pollicy cho phép bật IEE 802.1X

Hộp thoại Group Policy Management Editor xuất hiện bạn click chọn Computer Configuration → Policies → Windows Setting → Security Settings → Wire Network → click chuột phải chọn Create A New Wired Network Policy for Windows Vista and Later Releases.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

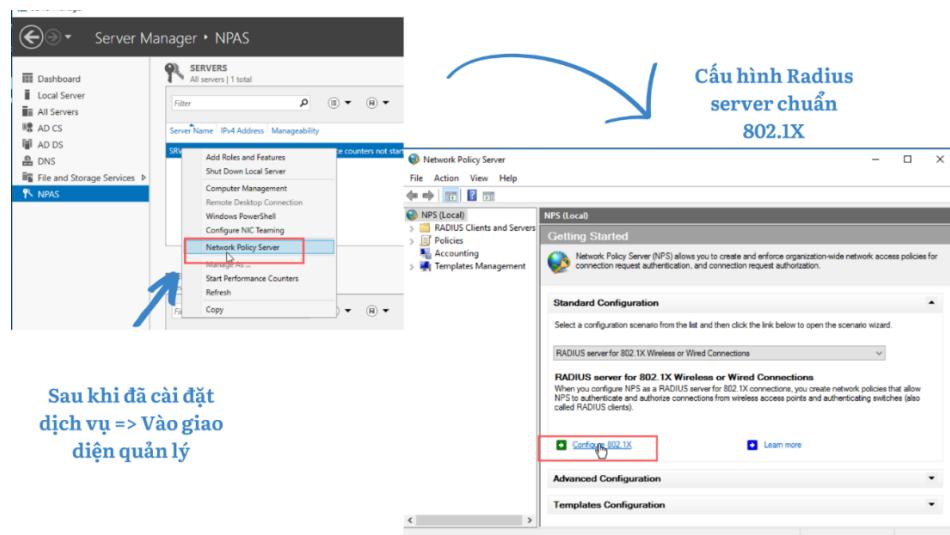
PS C:\Users\Administrator>

```

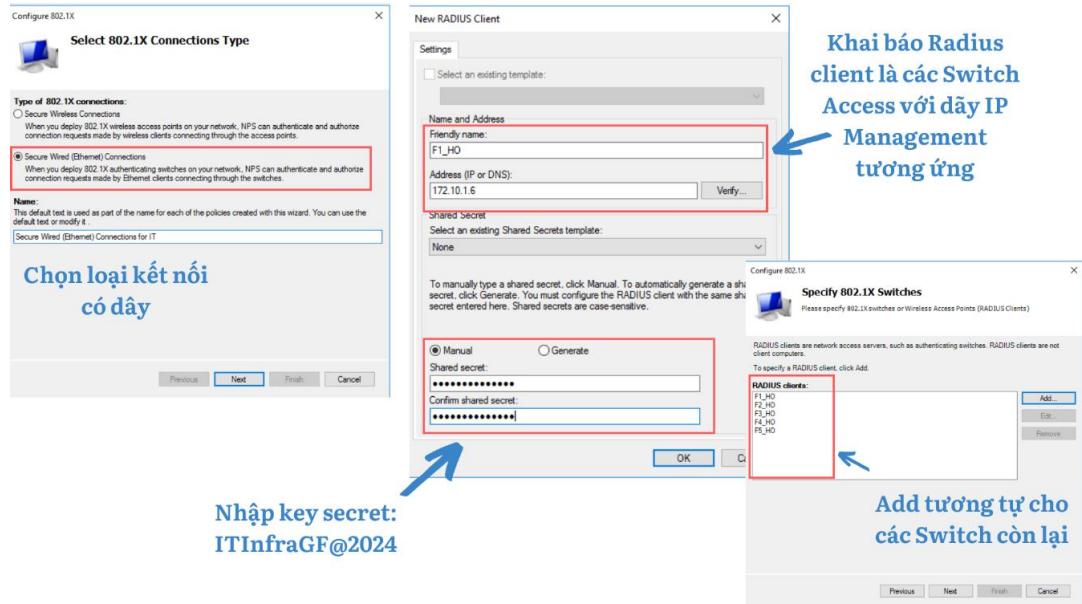
Hình 4.12.4.6: Cập nhật Policy

4.12.4.1 Xác thực truy cập vào mạng doanh nghiệp

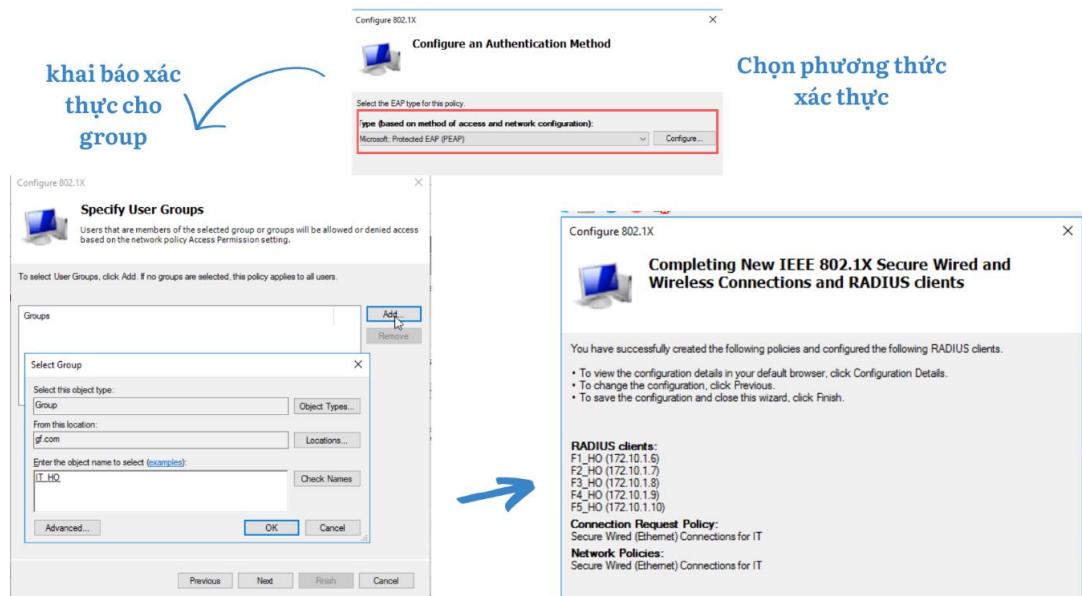
Thiết lập các chính sách truy cập vào mạng nội bộ thông qua dịch vụ Network Policy and Access Services làm Radius server. Các bước thực hiện làm theo như các hình chú thích sau đây:



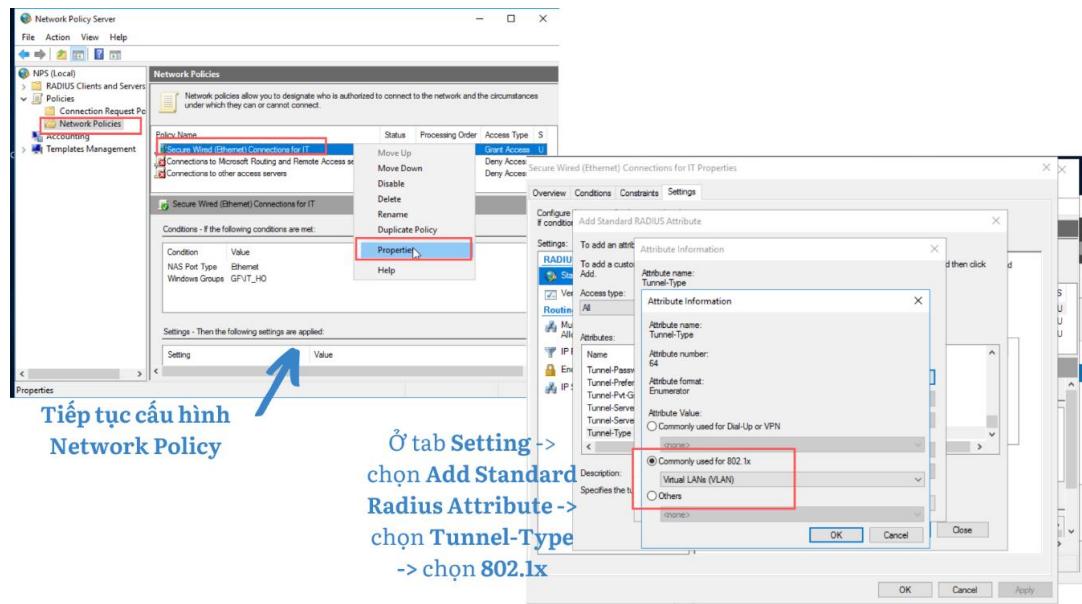
Hình 4.12.4.1.1: Vào giao diện quản lý và cấu hình Radius Server theo chuẩn 802.1X



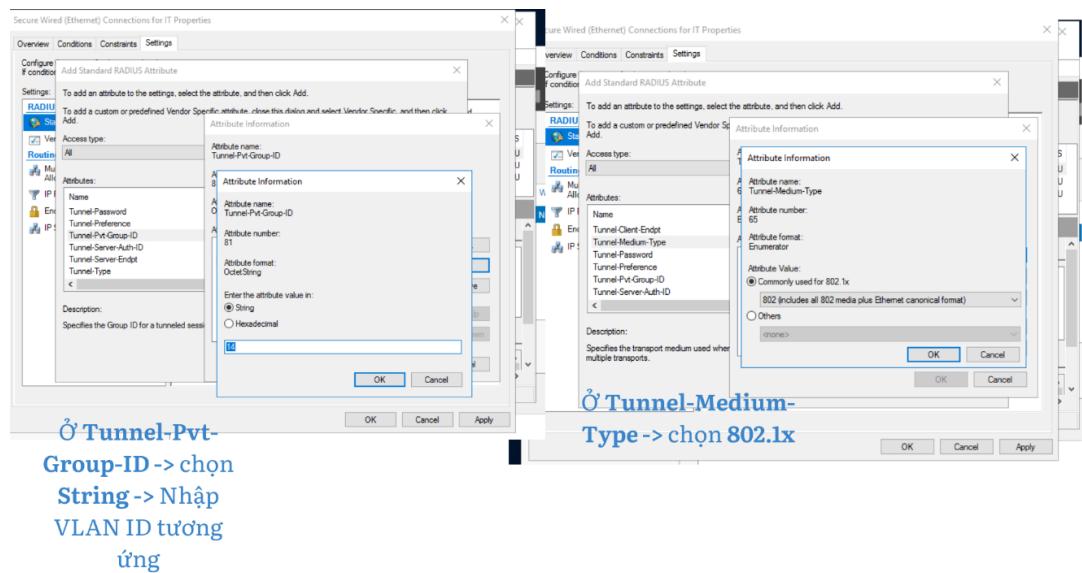
Hình 4.12.4.1.2: Tạo network policy cho phòng ban IT



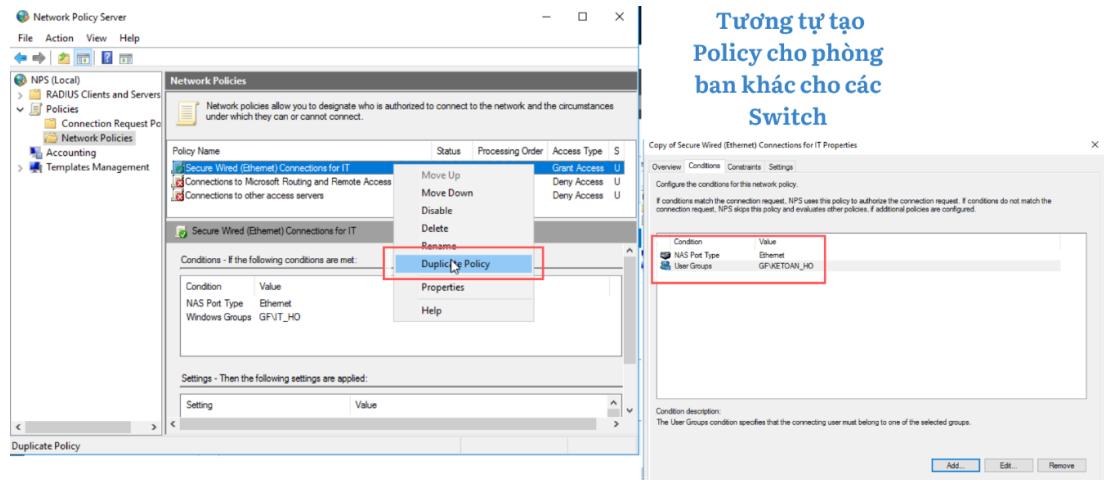
Hình 4.12.4.1.3: Tạo network policy cho phòng ban IT



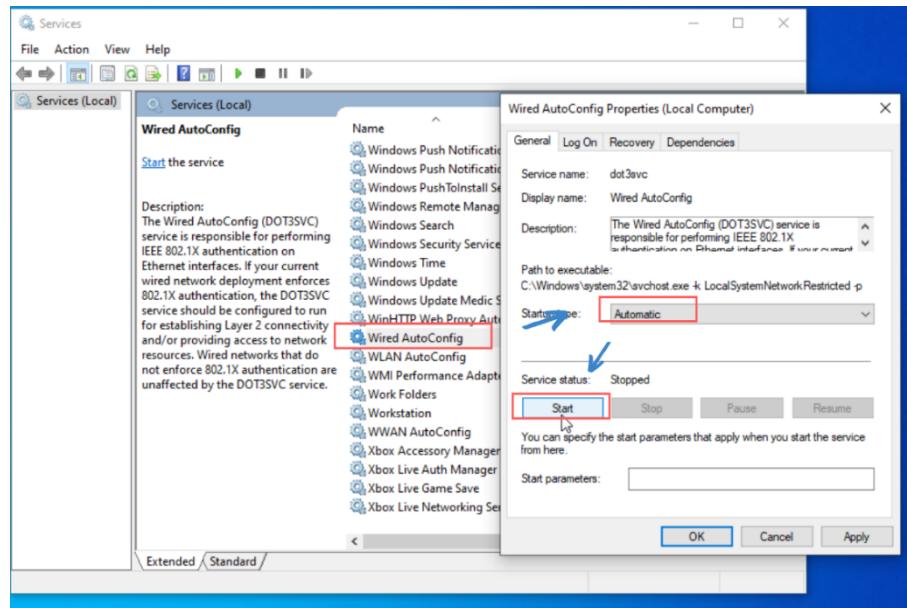
Hình 4.12.4.1.4: Tạo network policy cho phòng ban IT



Hình 4.12.4.1.5: Tạo network policy cho phòng ban IT

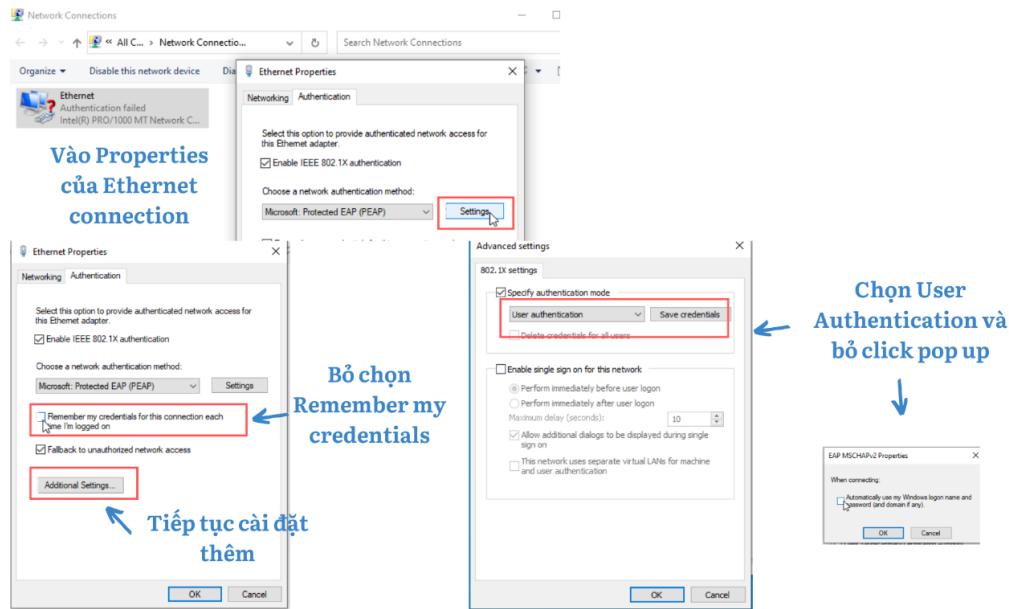


Hình 4.12.4.1.6: Tạo các network policy tương tự cho các phòng ban còn lại

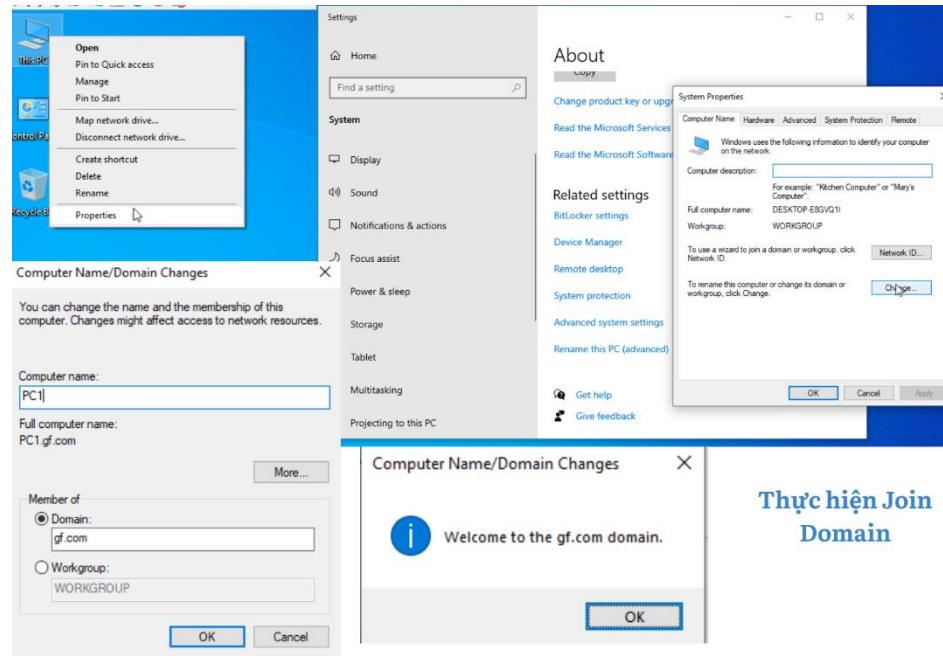


Vào Services và
bật dịch vụ
Wired Auto
Config

Hình 4.12.4.1.7: Bật dịch vụ Wired AutoConfig



Hình 4.12.4.1.8: Cấu hình Properties của Ethernet Connection



Hình 4.12.4.1.9: Thực hiện join domain

Sau khi đã join domain thành công, thiết bị sẽ tự động restart và yêu cầu người dùng đăng nhập lại.

Khi cắm bất kỳ máy tính vào Switch, người dùng sẽ đăng nhập tài khoản do công ty cung cấp, ở đây Switch đóng vai trò trung gian người xác thực, sau khi Radius

server xác thực xong thì Switch sẽ access vlan tương ứng với nhóm chứa tài khoản đó.

Ví dụ dưới đây là tài khoản thuộc nhóm IT thì port e0/2 sẽ được access VLAN 14 và PC này sẽ nhận IP thuộc VLAN 14.

The screenshot shows a Windows desktop environment. On the left, there is a user profile picture and the name 'Duyen Cao Nguyen Ky'. On the right, there is a terminal window with the following content:

```

Password: F1_HO#sh vlan
VLAN Name          Status   Ports
----  -----
1    default        active   Et0/3
10   LETAN_HO      active
11   HR_HO         active
12   MARKETING_HO  active
13   KETOAN_HO     active
14   IT_HO          active   Et0/2
15   KIEMTOAN_HO   active
16   TRUYENTHONG_HO active
17   PTBV_HO        active
18   GIAMDOC_HO    active
19   PHOGIAMDOC_HO active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default   act/unsup

C:\Users\duyen.cnk>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . : gf.com
  IPv4 Address . . . . . : 192.168.14.6
  Subnet Mask . . . . . : 255.255.255.128
  Default Gateway . . . . . : 192.168.14.1
  
```

A red box highlights the row for VLAN 14 (IT_HO) in the terminal output. Another red box highlights the IP configuration details for the Ethernet adapter.

Khi sử dụng account của VLAN của phòng IT logon vào máy tính tầng 1, Switch sẽ tự động xác thực thông qua Radius Server và tự động access VLAN tương ứng

Hình 4.12.4.1.10: Máy client sau khi join domain thành công

Một trường hợp khác khi thay đổi người dùng sang nhóm Kế toán thì tương tự máy tính người dùng sẽ được cấp IP thuộc VLAN 13.

```
F1_H0#sh vlan
VLAN Name Status Ports
1 default active Et0/3
10 LETAN_HO active
11 HR_HO active
12 MARKETING_HO active
13 KETOAN_HO active Et0/2
14 IT_HO active
15 KIEMTOAN_HO active
16 TRUYENTHONG_HO active
17 PTBV_HO active
18 GIAMDOC_HO active
19 PHOGIAMDOC_HO active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp B

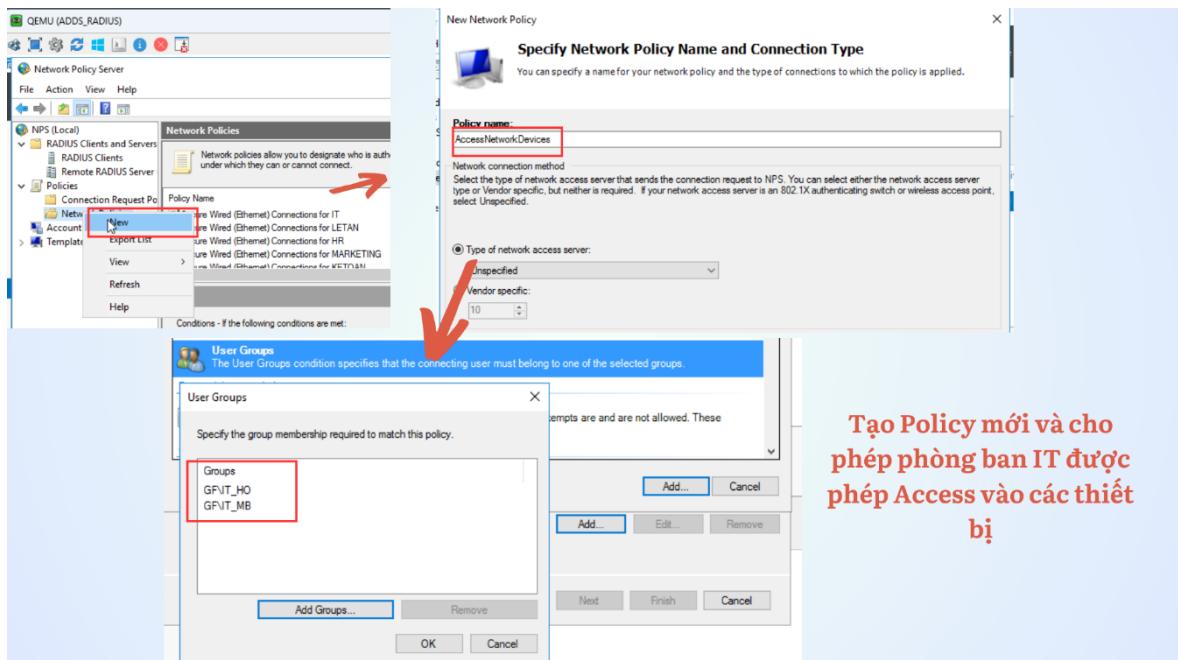
```

Tương tự khi sử dụng account của VLAN khác đăng nhập vào thiết bị đó thì Switch sẽ tự động access sang VLAN tương ứng

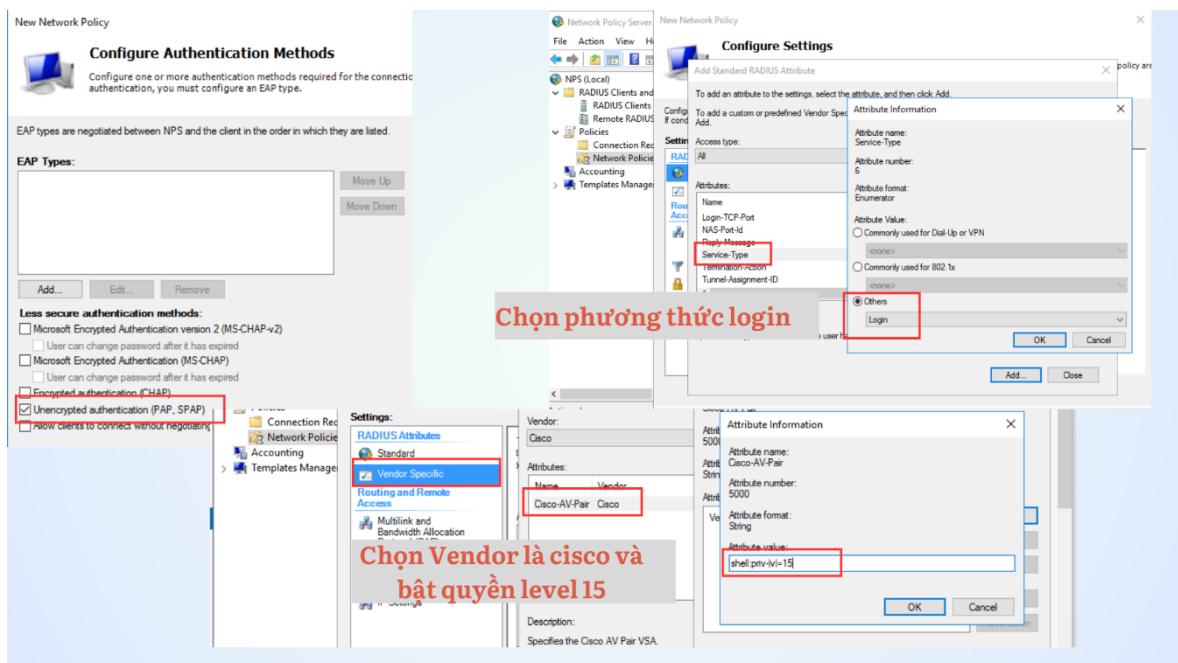
Hình 4.12.4.1.11: Máy client sau khi join domain thành công

4.12.4.2 Xác thực truy cập vào thiết bị network

Ở mục 4.10 chúng ta đã cấu hình Network Access Control cho các thiết bị Switch, ở phần này, chúng ta sẽ tiếp tục thiết lập các Policy trên Radius Server để cho phép và không cho phép những phòng ban chức năng truy cập vào các thiết bị của doanh nghiệp.



Hình 4.12.4.2.1: Tạo Policy cho phép phòng IT có thể truy cập vào



Hình 4.15.4.2.2: Cấu hình phương thức xác thực

Sau khi đã cấu hình xong Policy, các phòng ban chức năng khác ngoại trừ phòng ban IT sẽ không thể ssh đến các thiết bị.

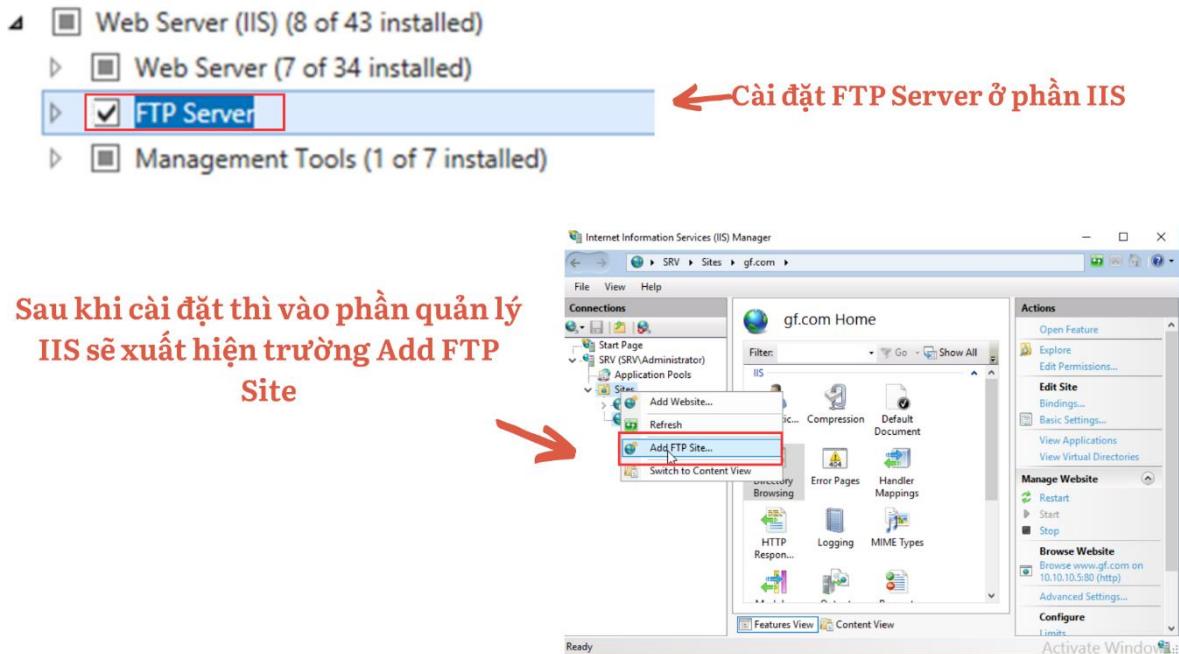
```
duyen.cnk@172.10.1.6's password:
KHONG PHAN SU MIEN VAO
F1_HO>█
```

Hình 4.15.4.2.3: Phòng ban IT có thẻ SSH vào thiết bị trong hệ thống

4.12.5 FTP Server

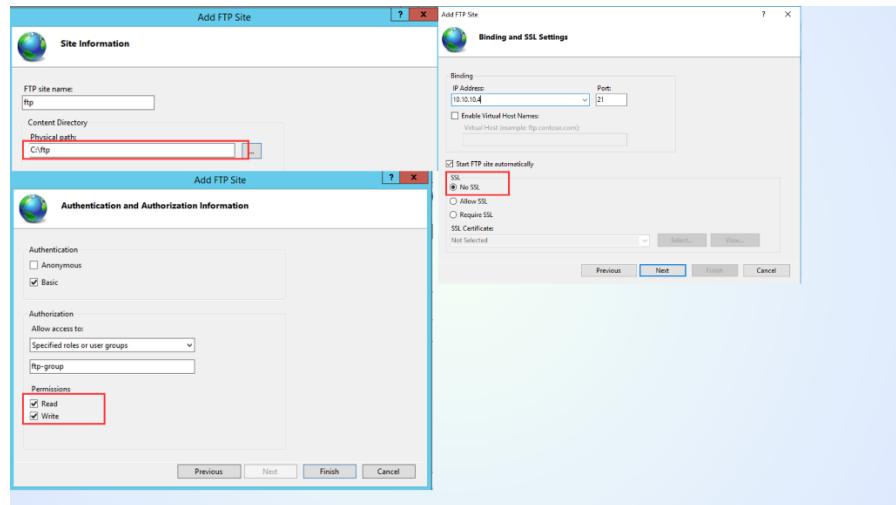
FTP server – File Transfer Protocol là một loại phần mềm hoặc dịch vụ trên mạng được sử dụng để lưu trữ và quản lý các tập tin và thư mục và cho phép người dùng truy cập và truyền tải chúng qua mạng Internet. FTP server thường được sử dụng để chia sẻ và truyền tải tệp tin và dữ liệu giữa các máy tính trên mạng, đặc biệt là trong các doanh nghiệp.

Đối với dịch vụ FTP sẽ nằm trong Webserver, chúng ta sẽ chọn vào Webserver, sau đó chọn FTP Server.



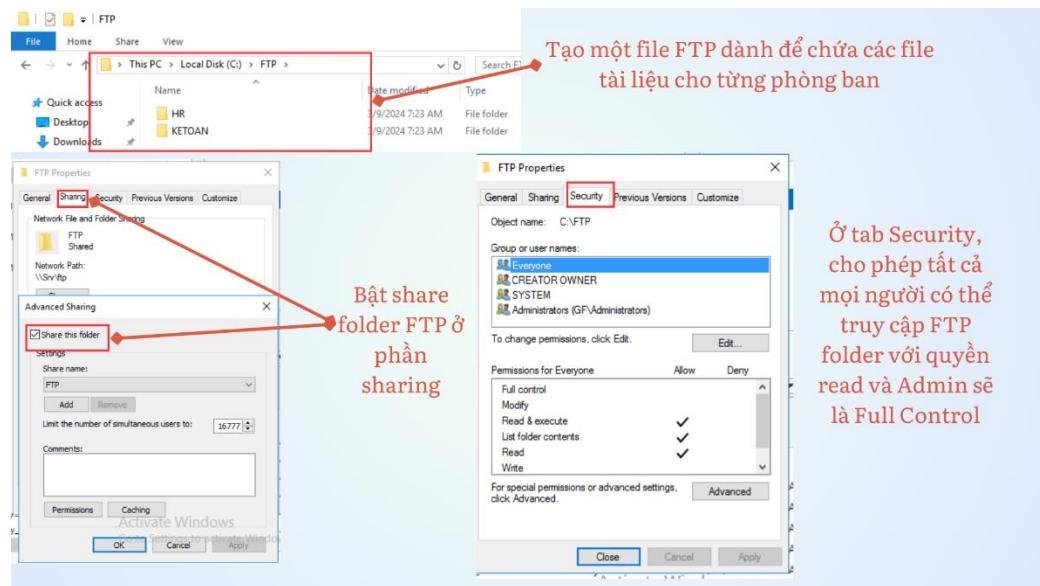
Hình 4.12.5.1: Cài đặt FTP ở mục IIS

Sau khi đã cài đặt thành công FTP vào máy chủ, chúng ta sẽ tiến hành xây dựng FTP cho phép người dùng có tài khoản mới được truy cập. Tài khoản này sẽ được tạo trên Server File Service.



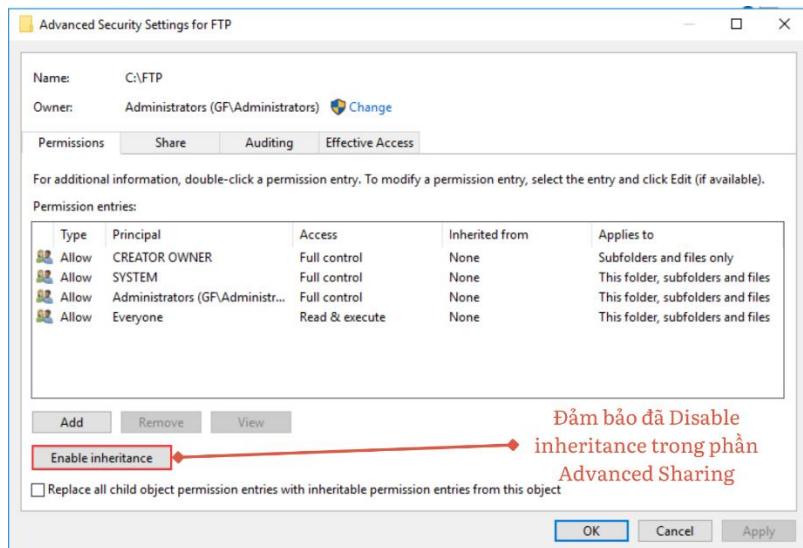
Hình 4.12.5.2: Cấu hình truy cập có tài khoản

Sau khi đã tạo thành công dịch vụ FTP, chúng ta sẽ tạo các folder chứa các tập tin dành cho từng phòng ban.



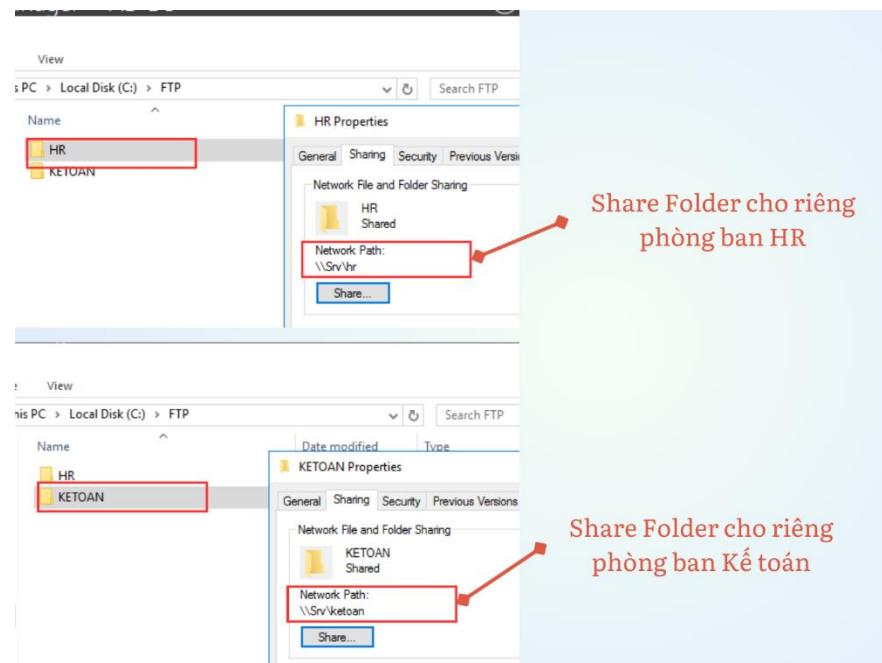
Hình 4.12.5.3: Tạo Folder chứa file cho từng phòng ban và set quyền cho các role nhất định

Ở hình 4.12.5.3, việc đầu tiên chúng ta cần share folder FTP cho tất cả các phòng ban có thể truy cập vào folder chứa file, tuy nhiên thì ngoài Admin ra thì tất cả user sẽ chỉ có quyền Read.



Hình 4.12.5.4: Disable inheritance trong phần Advanced Sharing

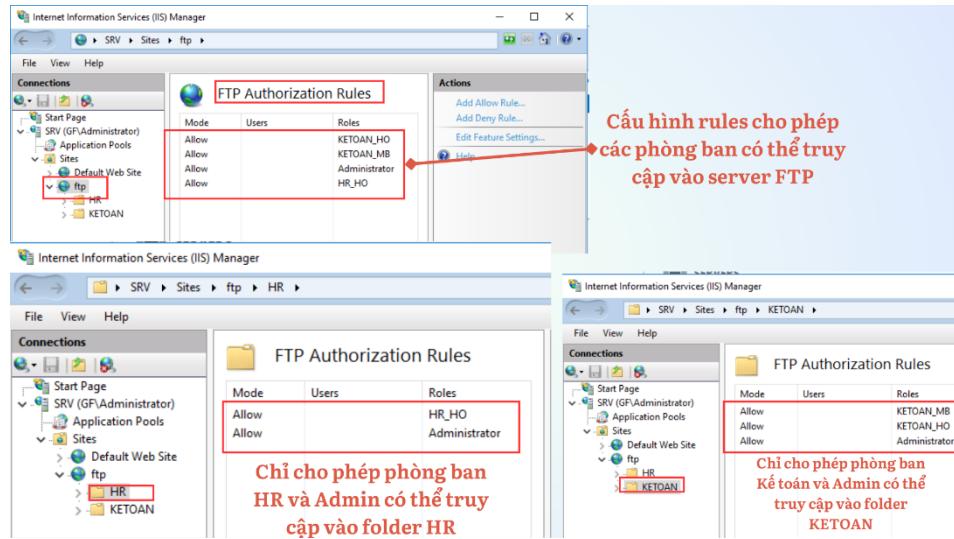
Ngoài ra, cần phải đảm bảo đã tắt Inheritance trong mục Advanced Sharing cho thư mục FTP để có thể custom theo rule của chúng ta.



Hình 4.12.5.5: Share các folder riêng cho từng phòng ban phù hợp

Ở các Folder dành cho từng phòng ban, chúng ta cần phải thiết lập quyền truy cập cho từng phòng ban nhất định. Giả sử, chúng ta có thư mục HR và KETOAN, thì chúng ta sẽ chỉ share riêng cho phòng ban HR và Kế toán truy cập vào.

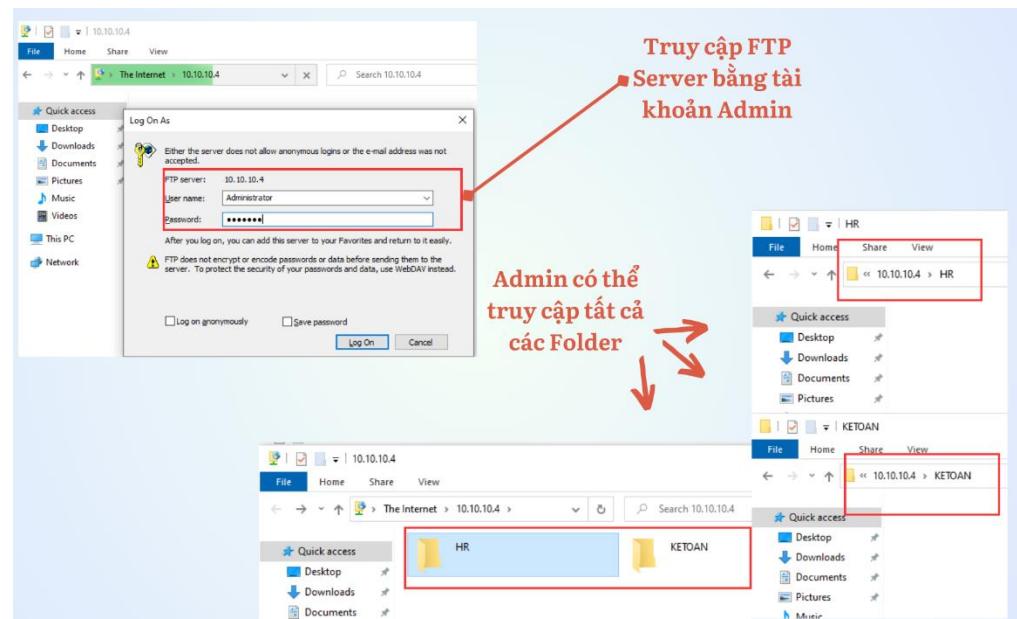
Sau khi đã hoàn thành thiết lập quyền trên các thư mục, chúng ta sẽ tiếp tục thiết lập quyền truy cập cho các phòng ban trên dịch vụ FTP.



Hình 4.12.5.6: Thiết lập các quyền truy cập trên dịch vụ FTP

Hình 4.12.5.6 có thể thấy rằng, ở dịch vụ FTP, chúng ta sẽ cho phép tất cả các phòng ban kể cả Admin có thể truy cập vào. Tuy nhiên ở thư mục HR thì chỉ có phòng ban HR và Admin có thể truy cập, điều này cũng thực hiện tương tự với phòng ban Kế toán.

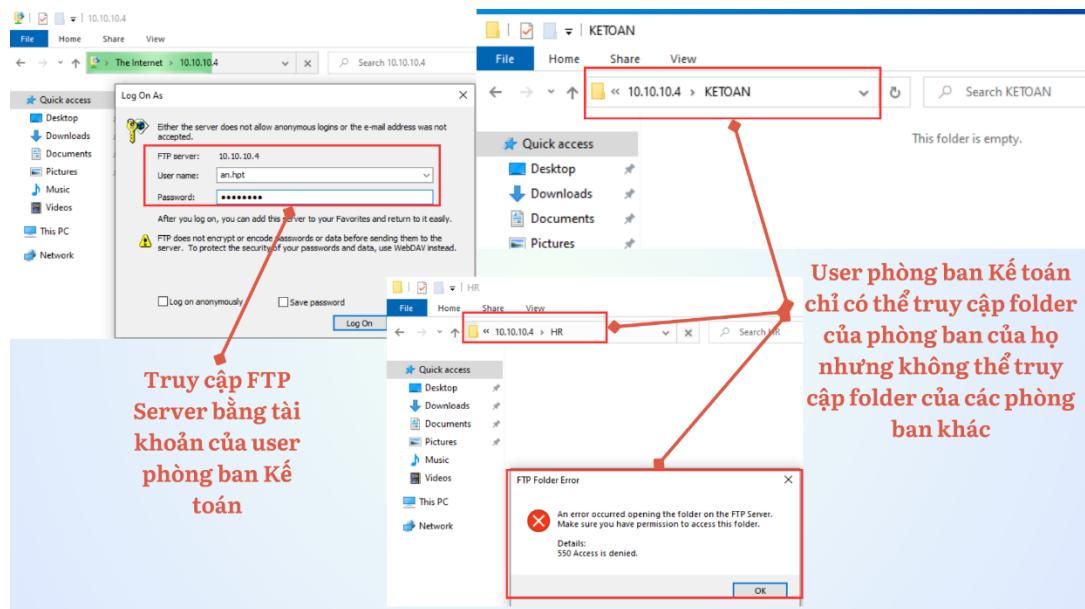
Sau khi hoàn thành tất cả cấu hình cho dịch vụ, chúng ta sẽ thực hiện kiểm thử truy cập vào dịch vụ FTP trên từng Account.



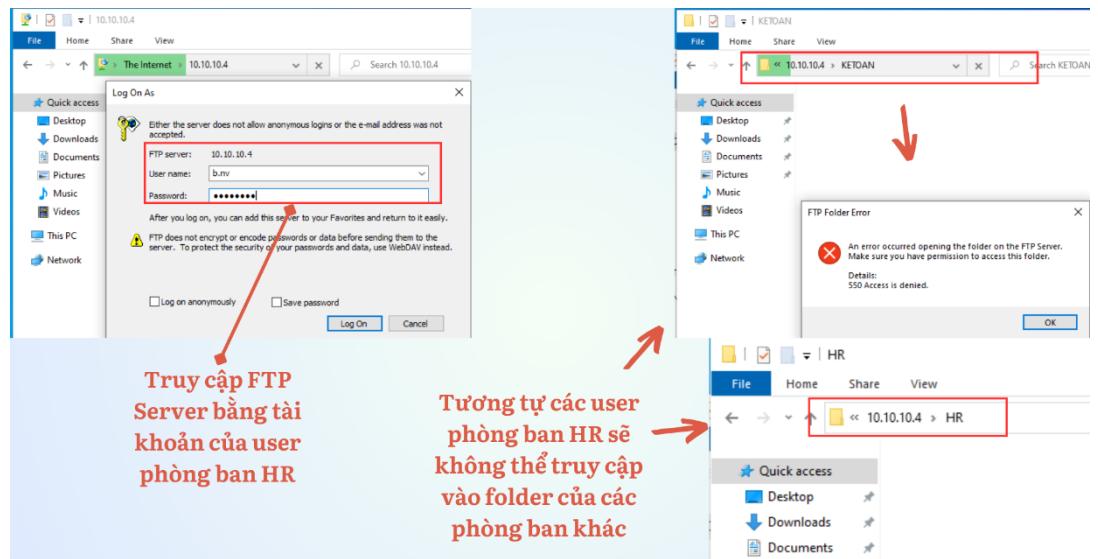
Hình 4.12.5.7: Truy cập dịch vụ FTP bằng tài khoản của Admin

Sử dụng tài khoản của Admin truy cập vào dịch vụ FTP, với quyền Full Control, ta có thể thấy Admin có thể vào được tất cả folder các phòng ban.

Tương tự sử dụng hai tài khoản của phòng ban HR và Kế toán để truy cập:



Hình 4.12.5.8: Sử dụng tài khoản của phòng ban Kế toán để truy cập FTP

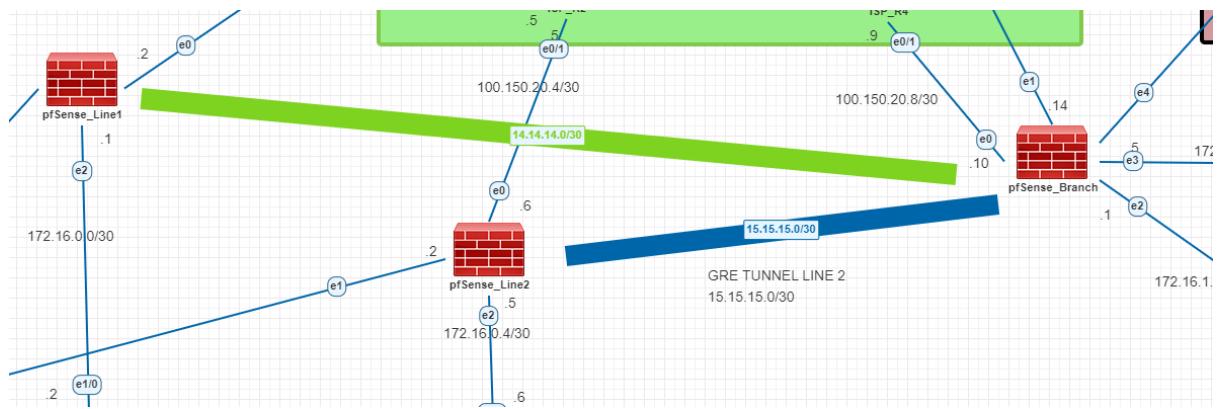


Hình 4.12.5.9: Sử dụng tài khoản của phòng ban HR để truy cập vào FTP

Dựa vào hình 4.12.5.8 và 4.12.5.9 chúng ta có thể thấy phòng ban Kế toán chỉ có thể truy cập vào thư mục của phòng ban của họ và không thể truy cập vào thư mục của phòng ban khác và điều này cũng tương tự đối với phòng ban HR và những phòng ban còn lại.

4.13 Firewall

Hệ thống này sẽ sử dụng Firewall pfSense để bảo mật, trong đó sẽ có 2 Firewall ở trụ sở chính để luôn đảm bảo tính sẵn sàng và một Firewall ở site chi nhánh.



Hình 4.13.1: Sử dụng Firewall pfSense cho hệ thống

Bước đầu tiên khi bắt đầu cấu hình Firewall, chúng ta cần cấu hình một số lệnh cấu hình cơ bản cho các Zone cần thiết.

```

** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense_LINE1 **

WAN (wan)      → vtne0          → v4: 100.150.20.2/24
LAN (lan)      → vtne1          → v4: 10.10.10.1/24
OPT1 (opt1)    → vtne2          →
OPT2 (opt2)    → vtne3          →

0) Logout (SSH only)         9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM

Enter an option: 2

Available interfaces:
1 - WAN (vtne0 - static)
2 - LAN (vtne1 - static)
3 - OPT1 (vtne2)
4 - OPT2 (vtne3)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 100.150.20.6

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 30

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 100.150.20.5

Should this gateway be set as the default gateway? (y/n) y

Configure IPv6 address WAN interface via DHCP? (y/n) n

```

Giao diện console của Firewall

Các Option để cấu hình

Lựa chọn Option Set Interface và lựa chọn WAN Zone

Hình 4.13.2: Cấu hình IP cho WAN Zone

```

Available interfaces:
1 - WAN (vtne0 - static)
2 - LAN (vtne1 - static)
3 - OPT1 (vtne2)
4 - OPT2 (vtne3)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 28

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD ...
Disabling IPv6 DHCPD ...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD ...

The IPv4 LAN address has been set to 10.10.10.2/28
You can now access the webConfigurator by opening the following URL in your web browser:
http://10.10.10.2/

```

Tương tự cấu hình interface cho zone LAN

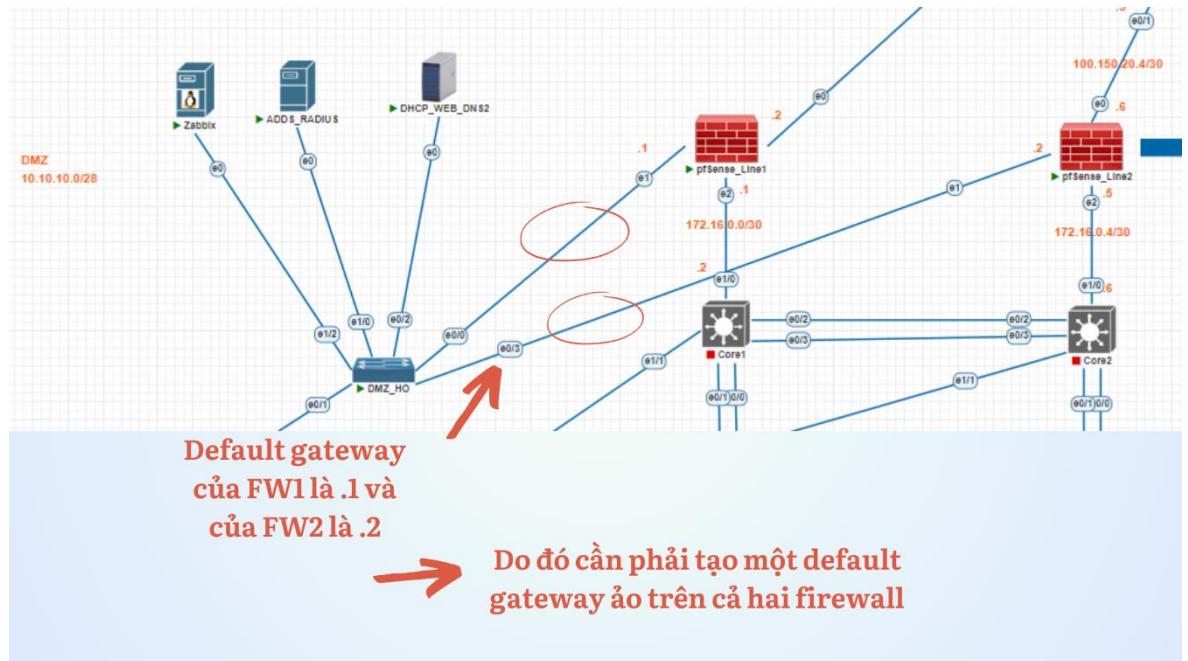
Đường link để cấu hình firewall bằng giao diện

Hình 4.13.3: Tương tự cấu hình IP cho LAN zone

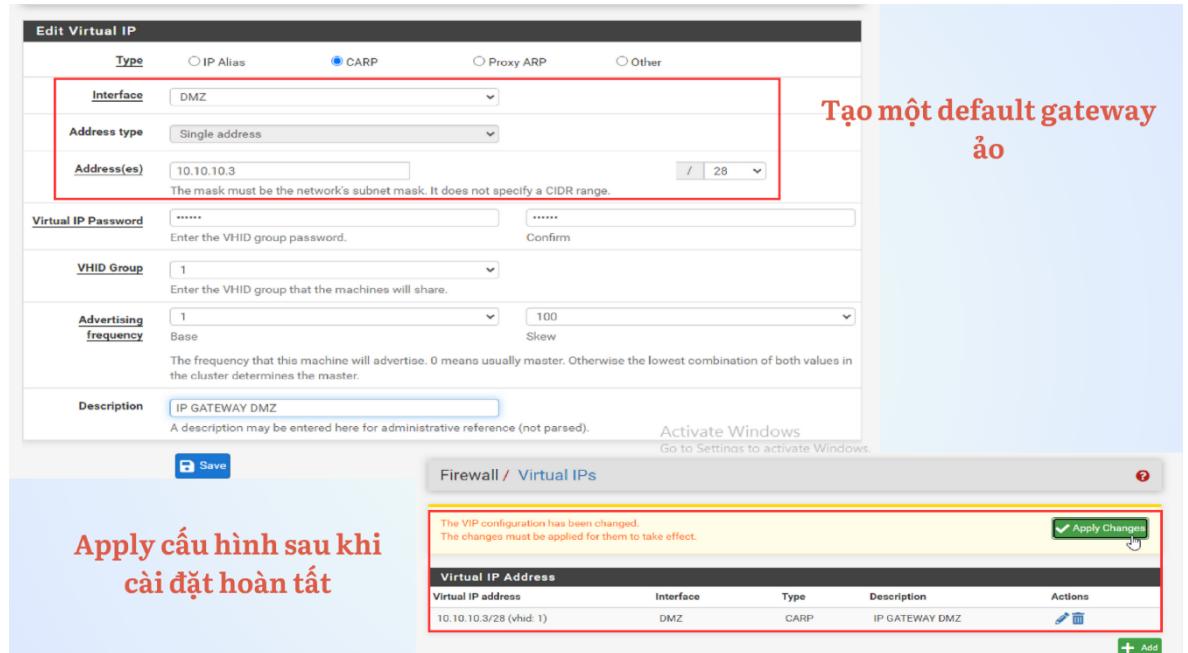
Thực hiện tương tự ở Firewall thứ 2, sau khi đã cấu hình xong, chúng ta sẽ có đường link để có thể truy cập và cấu hình thông qua giao diện.

Ở trụ sở chính, chúng ta sẽ có hai Firewall kết nối với vùng DMZ, với line kết nối với Firewall 1 có địa chỉ 10.10.10.1 và Firewall 2 là 10.10.10.2. Để đảm bảo tính

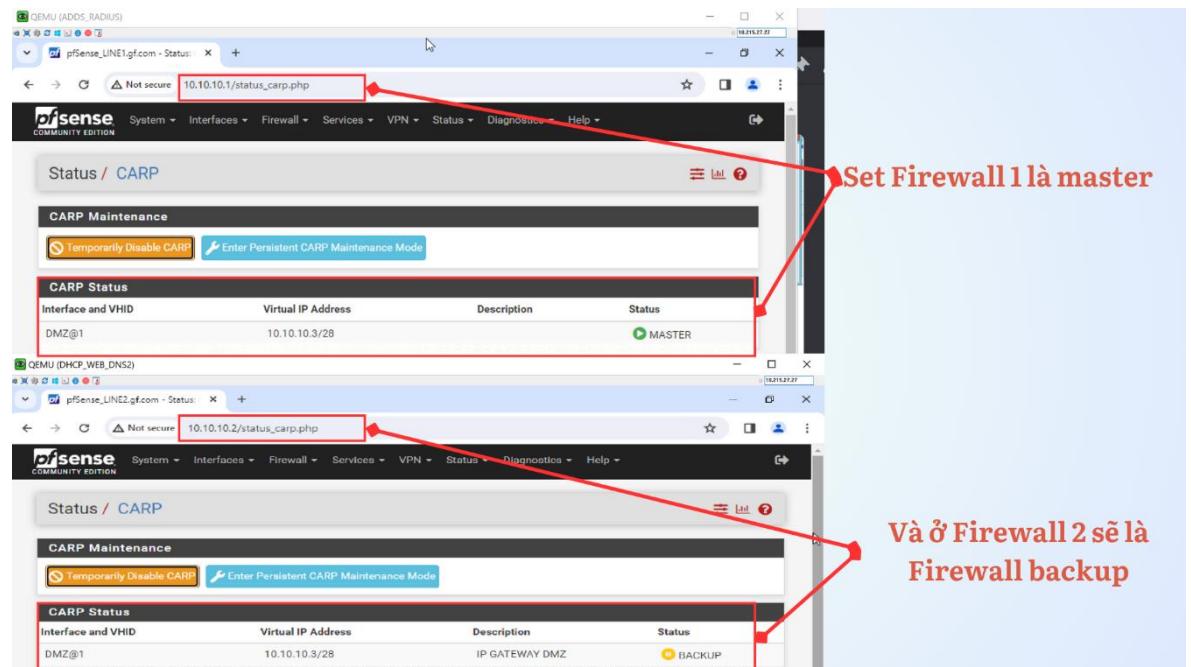
sẵn sàng và khả năng chịu lỗi trong môi trường mạng khi có hai Firewall hoạt động song song, bước đầu tiên chúng ta cần tạo một IP default gateway ảo với địa chỉ IP là 10.10.10.3.



Hình 4.13.4: Hai Firewall hoạt động song song



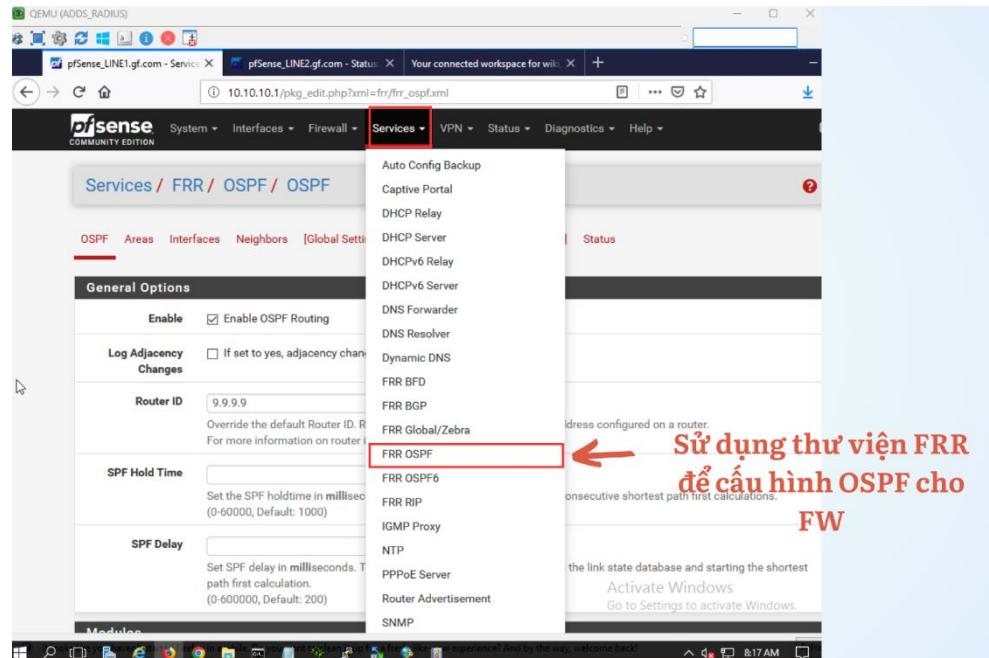
Hình 4.13.5: Cài đặt IP gateway ảo trên hai Firewall



Hình 4.13.6: Thiết lập Firewall là master và Firewall 2 là backup

Tương tự các bước cấu hình cơ bản, chúng ta cần cấu hình định tuyến động cho Firewall để các đường mạng đảm bảo kết nối đến internet.

Để cấu hình OSPF ở Firewall, chúng ta cần cài package FRR:



Hình 4.13.7: Cài đặt gói FRR để cấu hình OSPF

Bật OSPF

Area ở dạng IPv4

Redistribute default route để có thể quảng bá IP để các client biết đường đi ra internet

Hình 4.13.8: Cấu hình OSPF cho Firewall

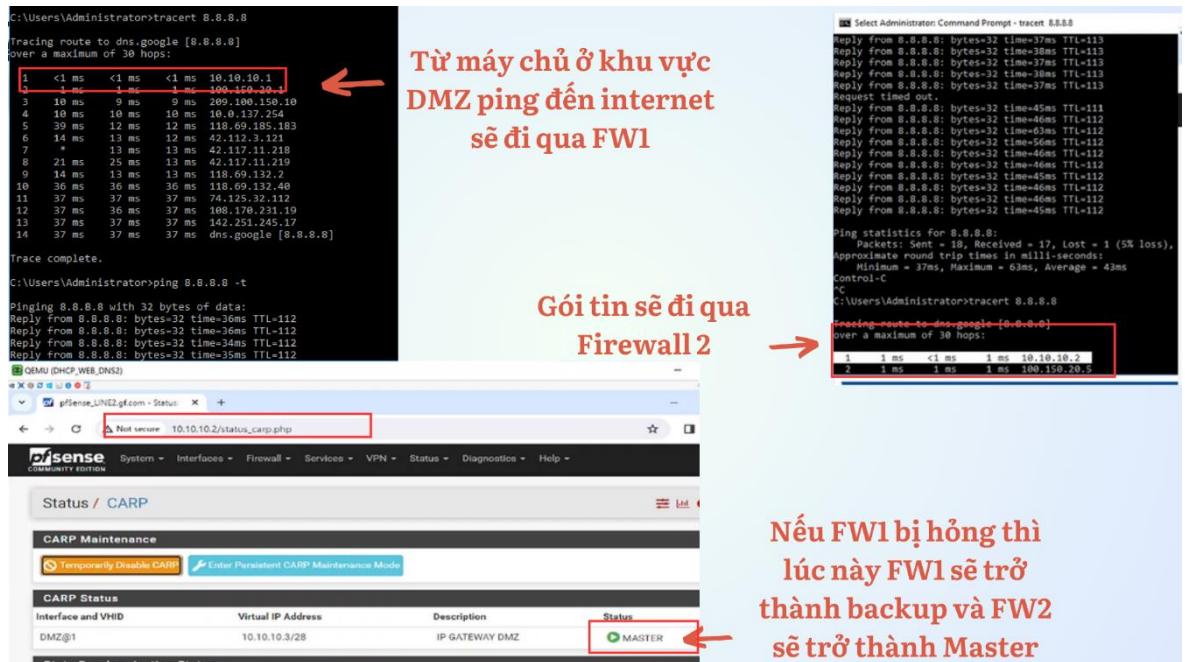
Add area của các interface tương ứng

Sau khi cấu hình xong ở OSPF, lưu ý bật gói tin FRR ở Global Settings

Status OSPF sau khi đã cấu hình thành công

Hình 4.13.9: Add Area cho các interface và bật gói tin FRR

Sau khi các đường mạng đã thông nhau, chúng ta sẽ kiểm tra đường đi của các gói tin để chắc chắn rằng tính sẵn sàng của Firewall đang hoạt động.

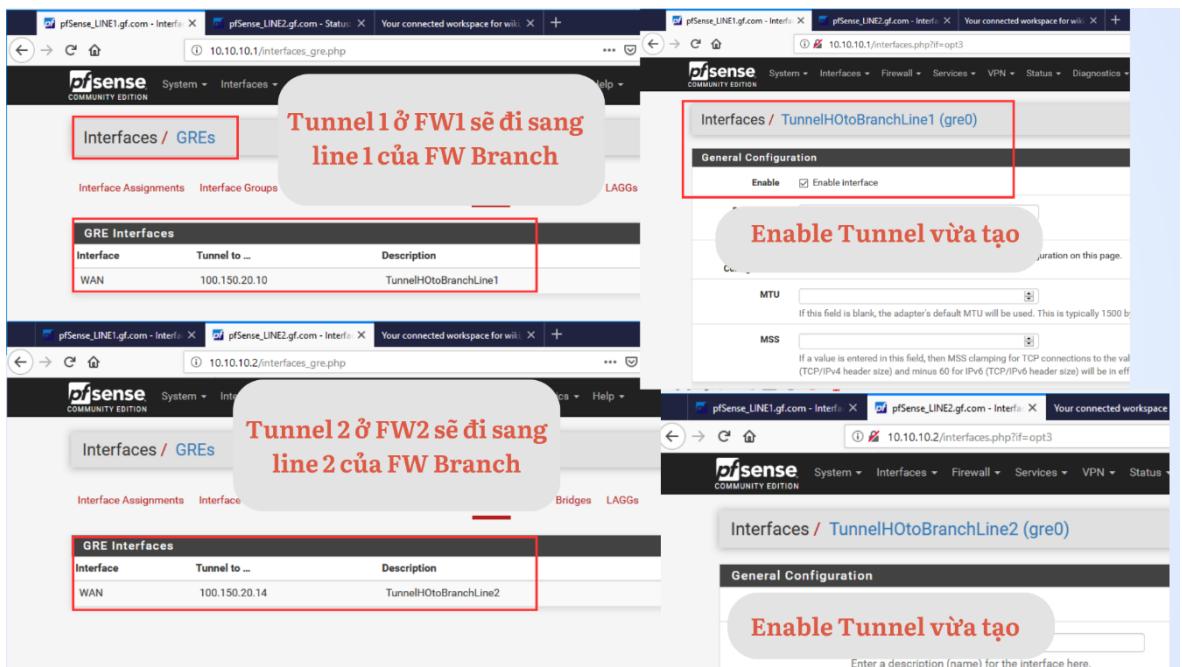


Hình 4.13.10: Gói tin sẽ ưu tiên đi qua Firewall 1

4.13.1 VPN - IPSec

Để hai khu vực có thể kết nối với nhau, chúng ta sẽ sử dụng VPN để tạo một mạng riêng ảo, tất cả các VLAN và mạng trong công ty sẽ gửi tin cho nhau thông qua Tunnel và các gói tin đi qua Tunnel này sẽ được mã hóa bằng IPSec.

Chúng ta sẽ tạo cấu hình chức năng này trên 3 Firewall. Trong đó, chúng ta sẽ có 2 tunnel, đi từ Firewall 1 đến Firewall chi nhánh sẽ là line 1 với IP của tunnel là 14.14.14.0/30 và line 2 sẽ từ Firewall 2 đến Firewall chi nhánh với IP 15.15.15.0/30



Hình 4.13.1.1: Tạo hai tunnel trên hai Firewall ở HO

Tương tự tạo 2 tunnel ở Firewall chi nhánh.

Sau khi hai tunnel đã được tạo thành công giữa hai chi nhánh, chúng ta sẽ edit các phase IPSec cho cả ba Firewall. Đối với Phase 1, chúng ta cần thiết lập kenh an toàn giữa hai Firewall để thực hiện trao đổi thông tin và khóa cho việc thiết lập kết nối an toàn. Đối với Phase 2, chúng ta sẽ quyết định lưu lượng nào được phép đi qua.

The screenshot shows the 'Edit Phase 1' configuration page for a tunnel named 'TunnelH0toBranchLine1'.

Vào phần IPSec để tạo Phase 1 (Enter Phase 1 IPSec settings to create)

General Information

- Description: TunnelH0toBranchLine1
- Disabled:

IKE Endpoint Configuration

- Key Exchange version: IKEv2
- Internet Protocol: IPv4
- Interface: **Remote Gateway** (highlighted with a red box) - Value: 14.14.14.2

Phase 1 Proposal (Authentication)

- Authentication Method: Mutual PSK
- My identifier: My IP address
- Peer identifier: Peer IP address
- Pre-Shared Key: GreenFeedCompanyNetworkVPN (highlighted with a red box)

Tạo Key và chọn độ dài mã hóa 256 bit (Create key and select 256-bit encryption strength)

Phase 1 Proposal (Encryption Algorithm)

- Encryption Algorithm: AES
- Key length: 256 bits
- Hash: SHA256
- DH Group: 14 (2048 bit)

Hình 4.13.1.2: Tạo Phase 1 cho Firewall

Ở hình trên, chúng ta sẽ tạo Phase 1 với đường đi từ HO đến site Miền Bắc

ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	TUNNELBRANCHTOHOLINE1 14.14.14.1	Mutual PSK	AES (256 bits)	SHA256	14 (2048 bit)	TunnelBranchtoHOLine1	
1	tunnel	DMZ	10.10.10.0/28	ESP	AES (256 bits), AES256-GCM (auto)	SHA256	DMZBranchtoDMZHO	
2	tunnel	DMZ	172.10.2.0/27	ESP	AES (256 bits), AES256-GCM (auto)	SHA256	DMZtoBranchNetworkDevices	
3	tunnel	DMZ	172.16.1.0/30	ESP	AES (256 bits), AES256-GCM (auto)	SHA256	DMZtoBranchNetworkLAN1	
4	tunnel	DMZ	172.16.1.4/30	ESP	AES (256 bits), AES256-GCM (auto)	SHA256	DMZtoBranchNetworkLAN2	

Các subnet remote ở Miền Bắc

Ở phase 2 sẽ cấu hình cho các rule để các lưu lượng có thể đi qua chặng hạn như lưu lượng DMZ ở HO đến DMZ ở Miền Bắc hoặc DMZ đến các thiết bị ở Miền Bắc

Hình 4.13.1.3: Tạo Phase 2 cho Firewall

Với Phase 2, chúng ta sẽ cho phép các lưu lượng từ mạng DMZ ở site HO đến mạng DMZ, các thiết bị và hai đường mạng LAN ở site Miền Bắc.

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped.

Disabled: Disable this rule

Set this option to disable this rule without removing it from the list.

Interface: **TUNNELHOTOBANCHLINE1**

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped.

Disabled: Disable this rule

Set this option to disable this rule without removing it from the list.

Interface: **IPsec**

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Set rules cho interface tunnel và IPSec có thể đi qua tường lửa

Hình 4.13.1.4: Set rule cho Interface của các tunnel và IPSec có thể đi qua Firewall

Sau khi đã hoàn thành các bước thiết lập VPN-IPSec, tiến hành kết nối giữa hai khu vực.

Tunnel kết nối thành công

Hình 4.13.2: Kết nối tunnel trên Firewall

4.13.2 NAT

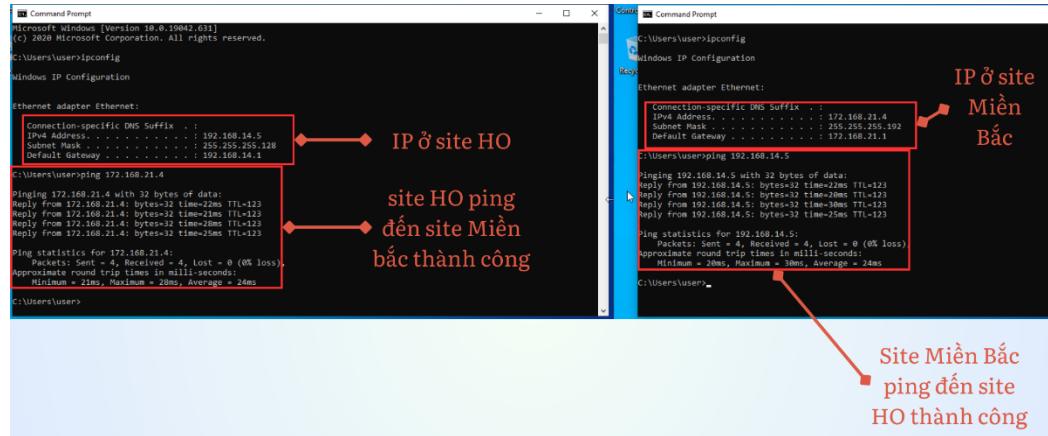
Ở phần trên, chúng ta đã cấu hình VPN cho mạng nội bộ để có thể đi qua các tunnel và đảm bảo được tính an toàn và bảo mật. Ngoài ra, NAT cũng là một phương pháp cần thiết cho tính bảo mật để có thể ẩn địa chỉ IP nội bộ trong doanh nghiệp khỏi Internet giúp bảo vệ các thiết bị trong mạng khỏi các cuộc tấn công mạng từ bên ngoài. Khi này các client gửi gói tin cho nhau qua hai site sẽ đi qua đường VPN, và khi client muốn truy cập ra ngoài internet, chúng ta sẽ sử dụng NAT.

NAT thủ công cho Firewall

Không NAT trên Tunnel và IPSec

Chỉ thực hiện NAT trên Interface WAN

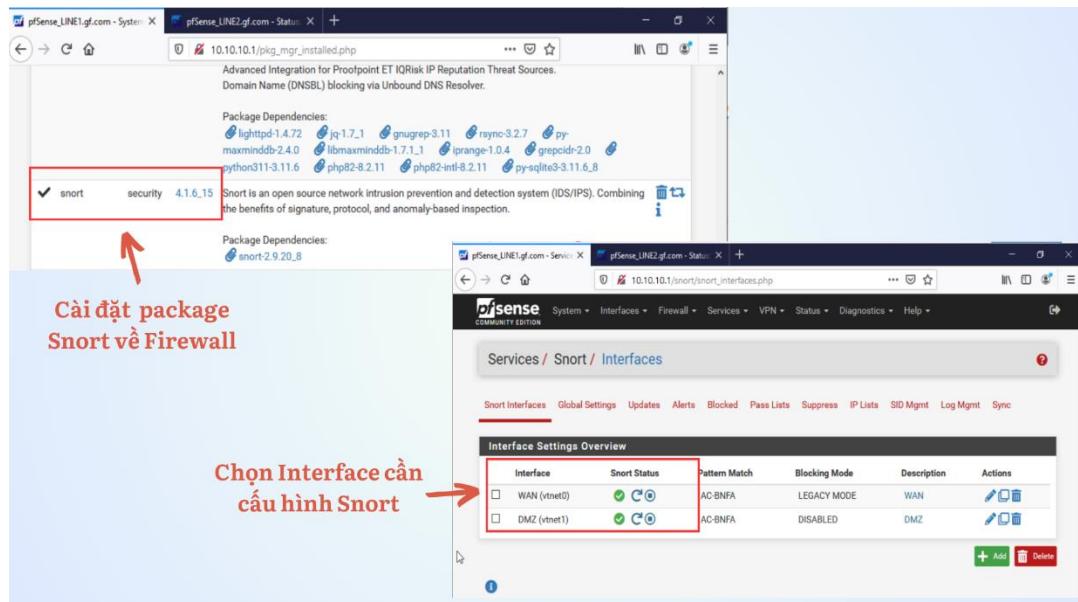
Hình 4.13.3: Chỉ thực hiện NAT trên interface WAN
Tiến hành kiểm tra kết nối giữa 2 client ở 2 khu vực.



Hình 4.13.4: Các phòng ban ở 2 site có thể kết nối thông qua công cụ mã nguồn mở Snort.

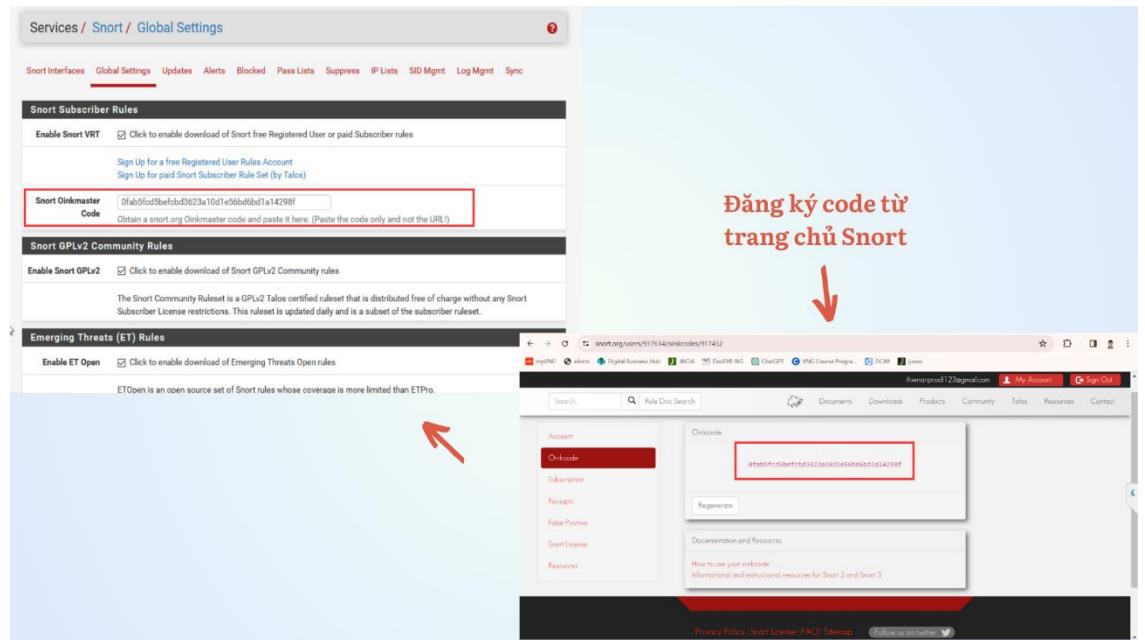
4.13.3 IDS/IPS với Snort

Xây dựng hệ thống phát hiện và chống xâm nhập mạng thông qua công cụ mã nguồn mở Snort. Tiến hành cài đặt gói Snort trên firewall theo các bước ở hình sau:

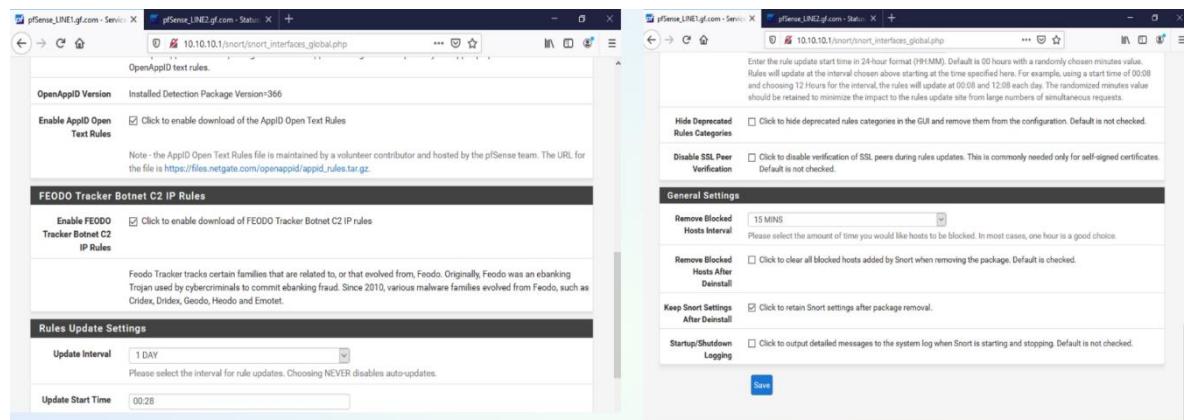


Hình 4.13.3.1: Cài đặt package Snort cho Firewall

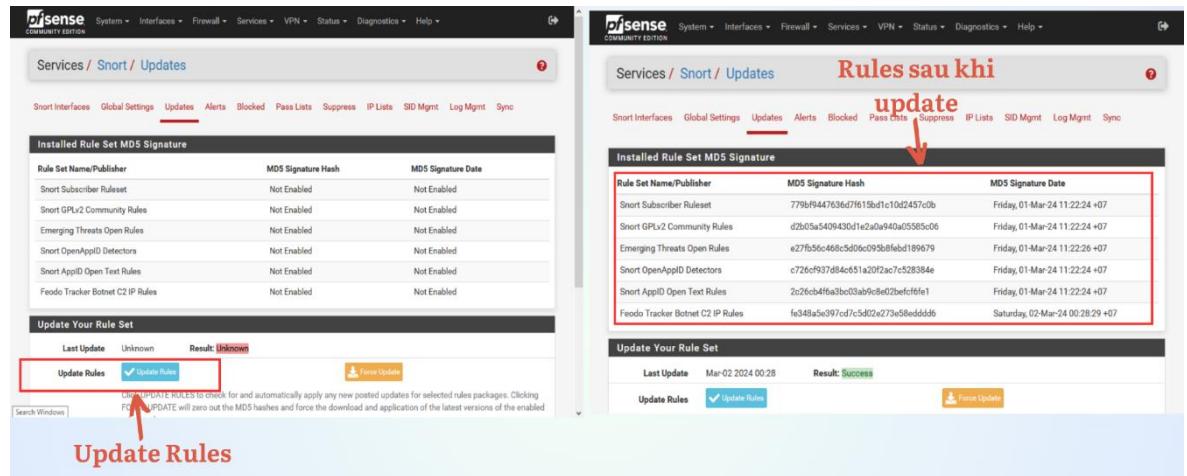
Ở bước này, ta sẽ điền code đã đăng ký từ trang chủ Snort, với đoạn code này chứng minh ta đã có tài khoản của snort và thiết bị sẽ tiến hành tải xuống các bộ luật, các đặc điểm để có thể phát hiện xâm nhập và chống tấn công.



Hình 4.13.3.2: Nhập code đã đăng ký từ trang chủ Snort vào Global Setting



Hình 4.13.3.3: Tiếp tục cấu hình Snort



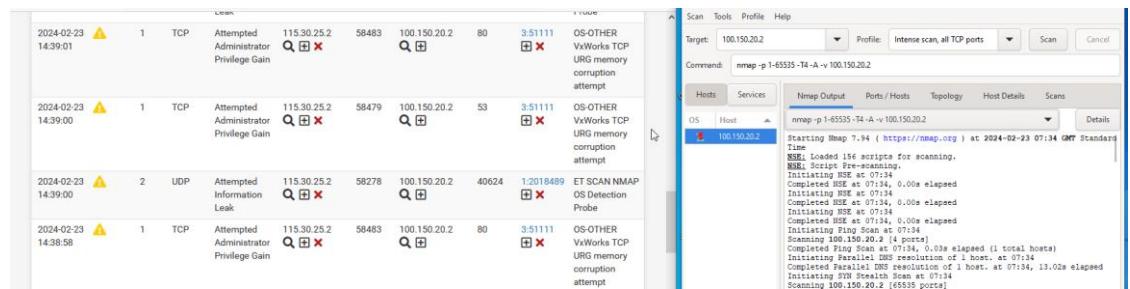
Hình 4.13.3.4: Update rules

Khi tiến hành sử dụng công cụ Nmap scanport từ 1 máy bên ngoài internet, quét các port với mục tiêu là ip public của line 1 thì với cấu hình snort trên firewall đã hiển thị alert hành động này.

Signature sau đây có thể được thiết kế để phát hiện các tấn công scan port bằng Nmap dựa trên cấu trúc và hành vi của các gói tin trong quá trình quét.

alert tcp any any -> any any (msg:"Potential Nmap port scan detected"; flags:S; dsize:0; detection_filter: track by_src, count 5, seconds 10; sid:1000001;)

- alert tcp any any -> any any: Xác định phát hiện cho các gói TCP từ bất kỳ nguồn hoặc đích.
- (msg:"Potential Nmap port scan detected";): Hiển thị thông điệp cảnh báo khi tấn công được phát hiện.
- flags:S: Xác định rằng gói tin có cờ SYN được đặt, một trong các cờ thường được sử dụng trong quá trình scan port.
- dsize:0: Điều kiện độ dài dữ liệu gói tin là 0, ngữ ý rằng nó là một gói tin SYN.
- detection_filter: track by_src, count 5, seconds 10;: Lọc phát hiện để chỉ báo cáo khi có ít nhất 5 gói tin cùng loại từ cùng một nguồn trong 10 giây.
- sid:1000001: Mã định danh cho signature.



Hình 4.13.3.5: Alert phát hiện hành vi scan port

The screenshot shows the 'Services / Snort / Blocked Hosts' configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has tabs for Snort Interfaces, Global Settings, Updates, Alerts, Blocked (which is selected), Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync.

The 'Blocked Hosts and Log View Settings' section contains the following controls:

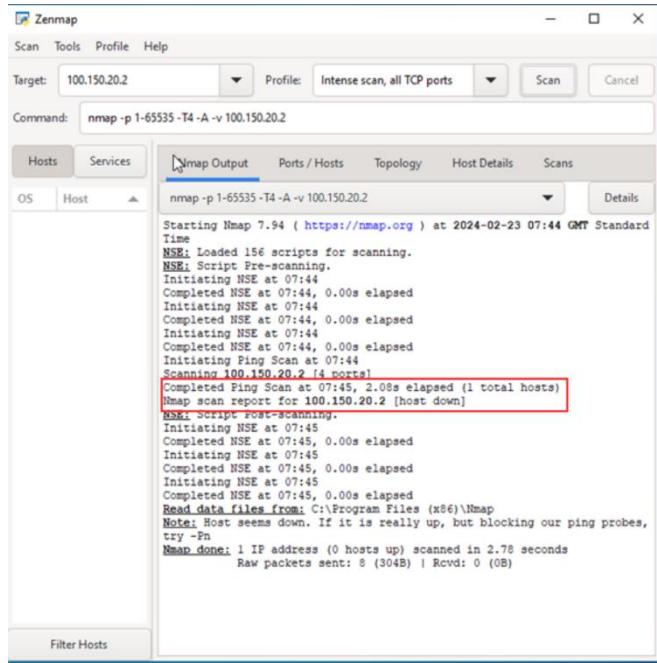
- Blocked Hosts:** A green 'Download' button and a red 'Clear' button. Below them is the text "All blocked hosts will be saved".
- Refresh and Log View:** A blue 'Save' button and a checkbox 'Refresh' (checked) with the subtext "Default is ON".
- Number of blocked entries to view:** A dropdown menu set to 500, with the subtext "Number of blocked entries to view. Default is 500".

The 'Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)' table lists one entry:

#	IP	Alert Descriptions and Event Times	Remove
1	115.30.25.2	ET SCAN NMAP OS Detection Probe – 2024-02-23 14:39:02 OS-OTHER VxWorks TCP URG memory corruption attempt – 2024-02-23 14:39:02	X

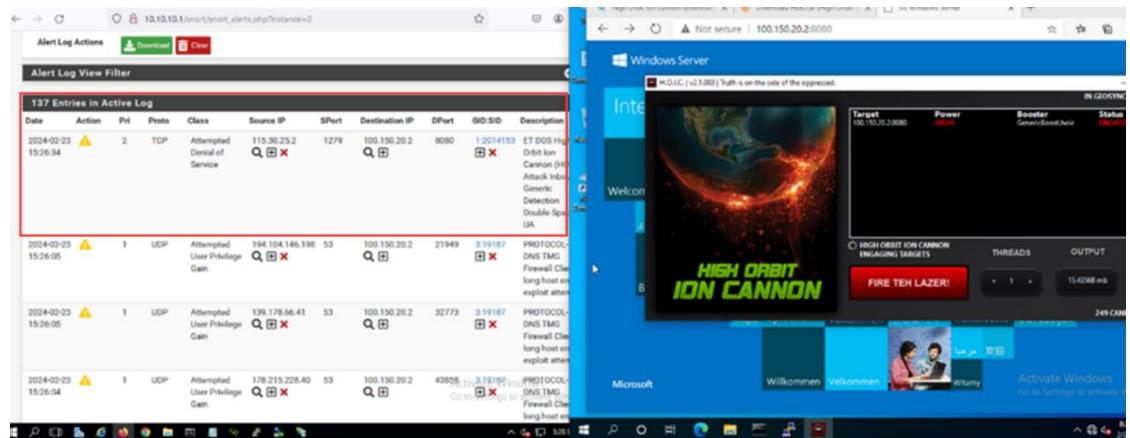
Hình 4.13.3.6: Hệ thống sẽ block ip này với hành vi scan port

Tiến hành scan port lại lần nữa tại máy attacker thì đã không thành công, log thẻ hiện mục tiêu đã down nhưng đây là do hệ thống IDS/IPS trên firewall block ip của máy attacker từ bước trên.



Hình 4.13.3.7: Log thẻ hiện mục tiêu đã down

Sử dụng công cụ Hight Orbit ION Canon để tấn công DoS/DDoS với mục tiêu là Web server của công ty đã được nat port ra public để cho người dùng truy cập web.



Hình 4.13.3.8: Sử dụng công cụ Hight Orbit ION Canon để tấn công DoS/DDoS

Khi tấn công thì IDS/IPS đã phát hiện ra traffic cao và nhận diện đây là tấn công DoS từ công cụ HOIC nên đã hiển thị alert và block luôn lại IP attacker này.

Signature sau có thể được thiết kế để phát hiện các gói tin TCP có kích thước và nội dung phù hợp với các giao thức và hành vi tấn công từ công cụ Hight Orbit ION Canon

```
alert tcp any any -> any 8080 (msg:"Potential Hight Orbit ION Canon DoS attack detected"; dsize:0; flags: S; detection_filter: track by_src, count 10, seconds 5; sid:1000002;)
```

- alert tcp any any -> any 8080: Xác định phát hiện cho các gói TCP từ bất kỳ nguồn hoặc đích trên cổng 8080.
- (msg:"Potential Hight Orbit ION Canon DoS attack detected";): Hiển thị thông điệp cảnh báo khi tấn công được phát hiện.
- dsize:0: Điều kiện độ dài dữ liệu gói tin là 0, ngụ ý rằng đây là gói tin SYN, một trong các loại gói tin mà công cụ Hight Orbit ION Canon thường sử dụng trong tấn công DoS.
- flags: S: Xác định rằng gói tin có cờ SYN được đặt.
- detection_filter: track by_src, count 10, seconds 5;: Lọc phát hiện để chỉ báo cáo khi có ít nhất 10 gói tin SYN từ cùng một nguồn trong 5 giây.
- sid:1000002: Mã định danh cho signature.

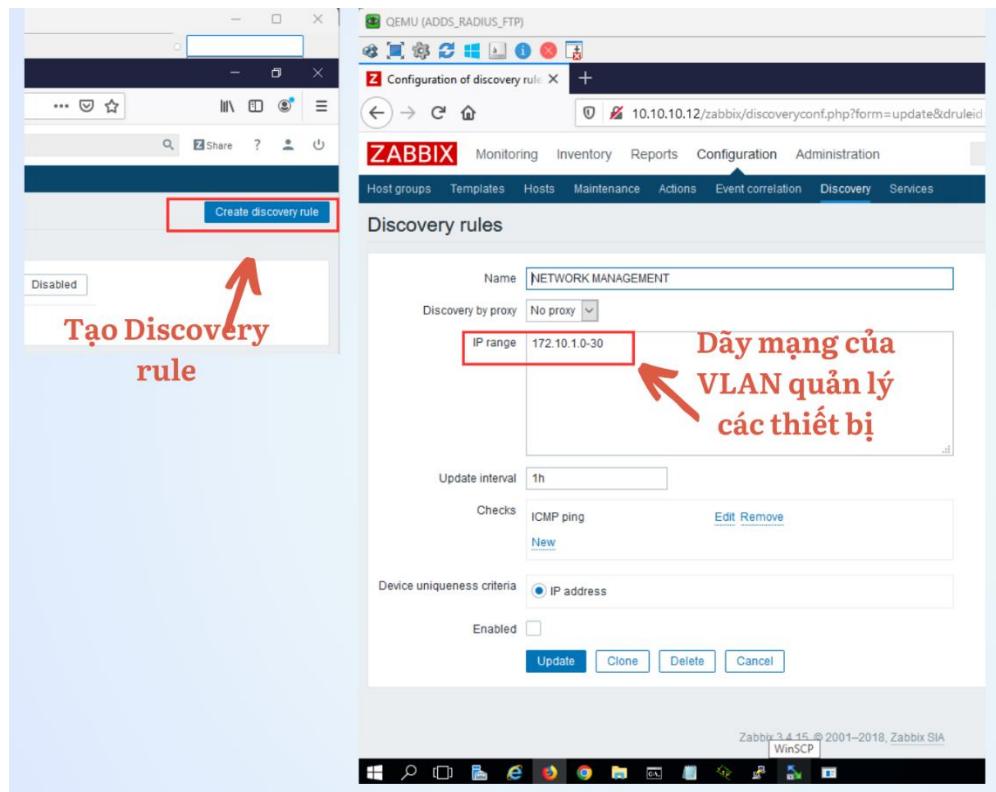
4	115.30.25.2	ET SCAN NMAP OS Detection Probe -- 2024-02-23 14:39:02 OS-OTHER VxWorks TCP URG memory corruption attempt -- 2024-02-23 15:07:46 (spo_bo) Back Orifice Client Traffic detected -- 2024-02-23 15:31:44 ET DOS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA -- 2024-02-23 15:26:34
---	-------------	---

Hình 4.13.3.9: Alert và Block IP

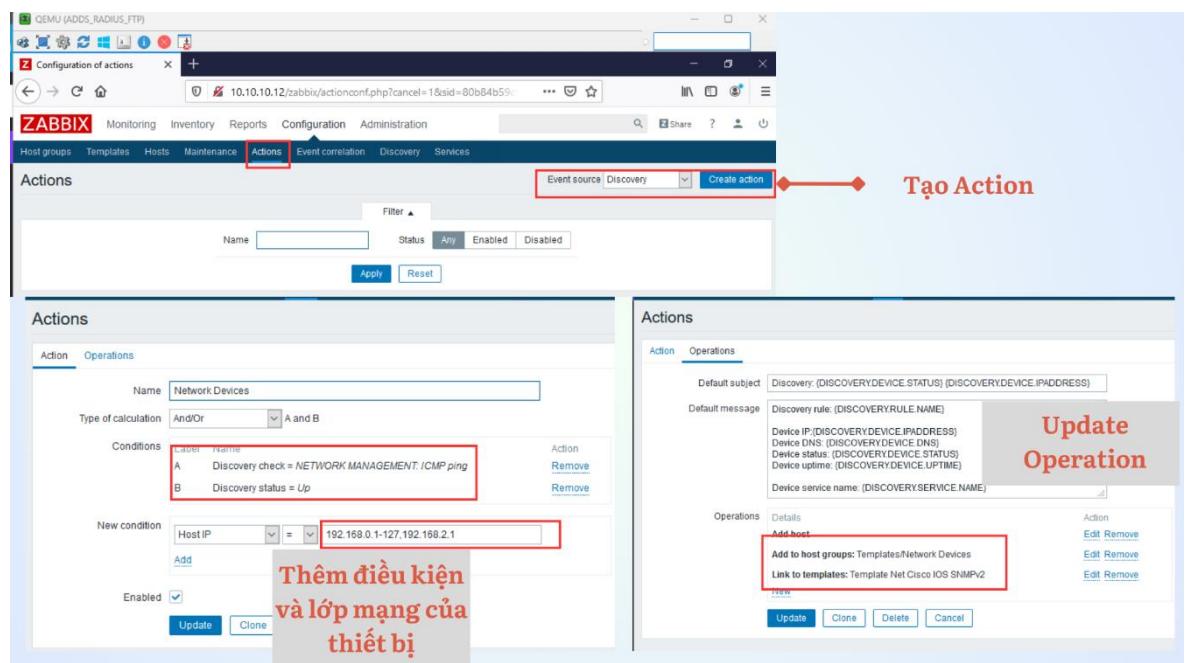
4.14 Zabbix

Phần cuối cùng trong hệ thống mạng của chúng ta sẽ là xây dựng một hệ thống giám sát bằng Zabbix để giám sát các thiết bị mạng từ đó có thể xử lý những sự cố kịp thời.

Bước đầu tiên, tạo discovery và trigger để thêm thiết bị có trong hệ thống mạng nội bộ vào server Zabbix.

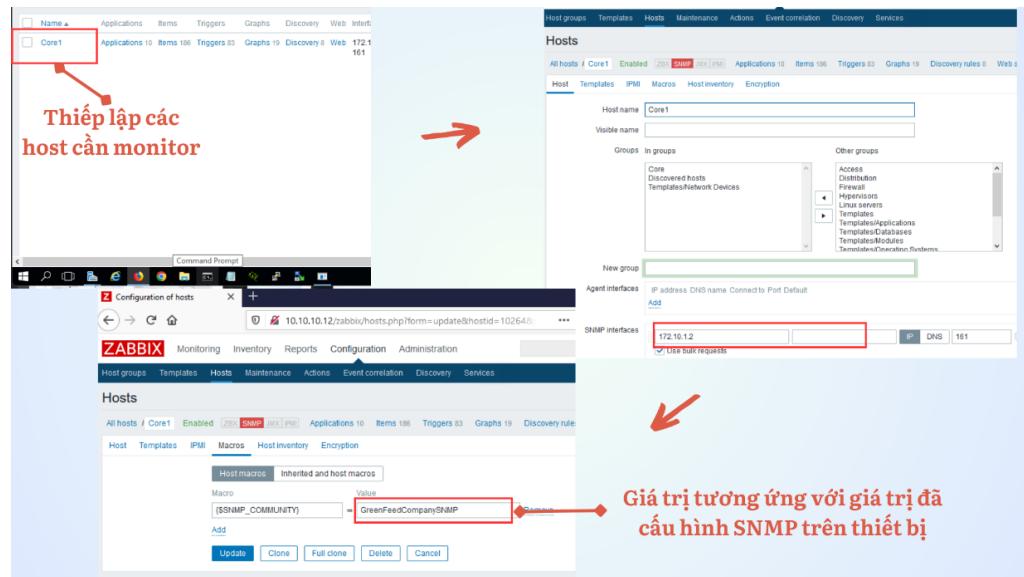


Hình 4.14.1: Tạo Discovery Rule để phát hiện các thiết bị mạng có trong nội bộ



Hình 4.14.2: Tạo Action Discovery

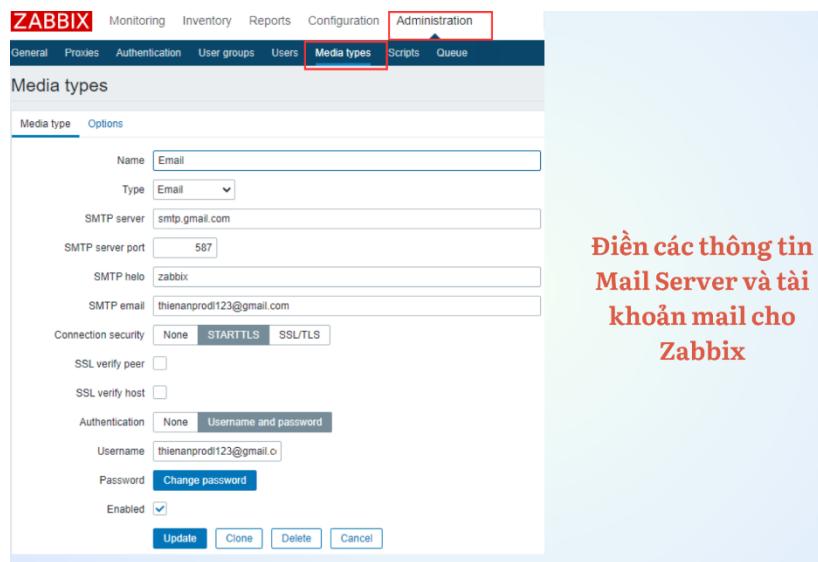
Thiết lập các thiết bị đã được thêm vào zabbix, quan trọng nhất là giá trị **SNMP_Community String** tương ứng với khi cấu hình trên thiết bị mạng.



Hình 4.14.3: Thêm các host cần monitor vào Zabbix

Tiến hành cấu hình mail server và các địa chỉ email cần thiết để người quản trị nhận được thông báo kịp thời khi có sự cố bất thường xảy ra.

Tại màn hình chính, ta chọn mục **Administration → Media types**, lúc này sẽ phải điền các giá trị thông số của mail server mà người quản trị sử dụng để áp dụng cho server zabbix dùng nó để gửi email thông báo. Ở đây nhóm kiểm thử sử dụng bằng mail server của Google, với các giá trị mà mail server Google đưa ra ta sẽ phải điền đúng vào từng mục thiết lập trên zabbix như **SMTP Server**, **SMTP Port**, địa chỉ email bao gồm cả thông tin đăng nhập của email này trên Gmail.



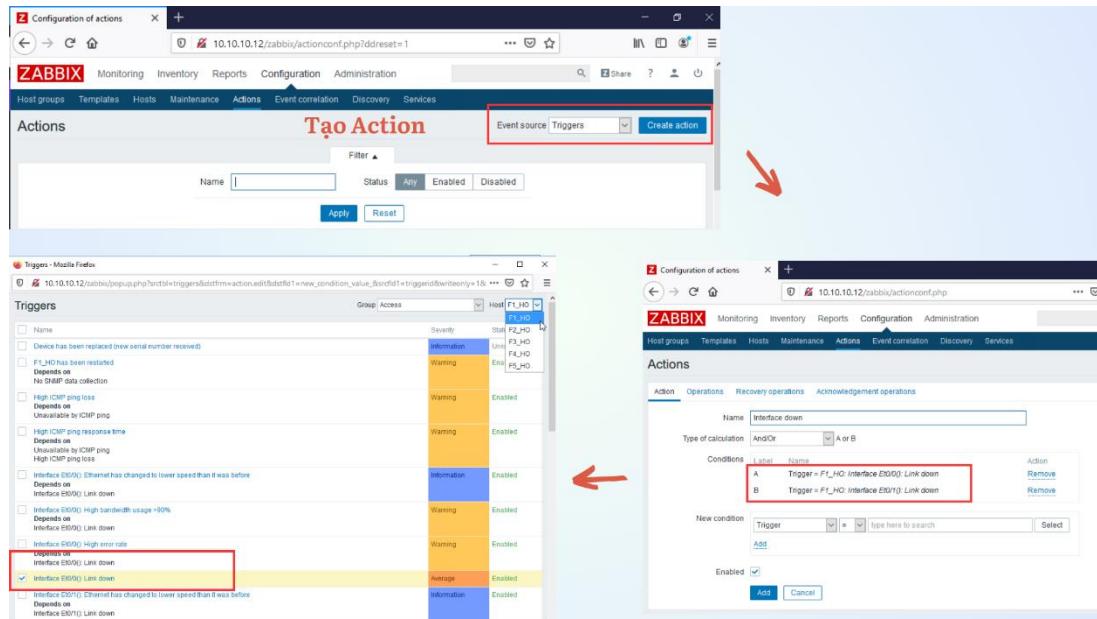
Hình 4.14.4: Add Mail cho server

Sau khi đã thêm email cho zabbix, ta tiến hành thiết lập email người được nhận thông báo. Mục **Administration → Users**, chọn user cần thiết lập (ở đây là Admin) ta chọn kiểu thông tin liên lạc với người nhận là Email sau đó điền thông tin email của người này, cuối cùng là chọn **Enabled**. Kết quả được như hình 4.14.5.

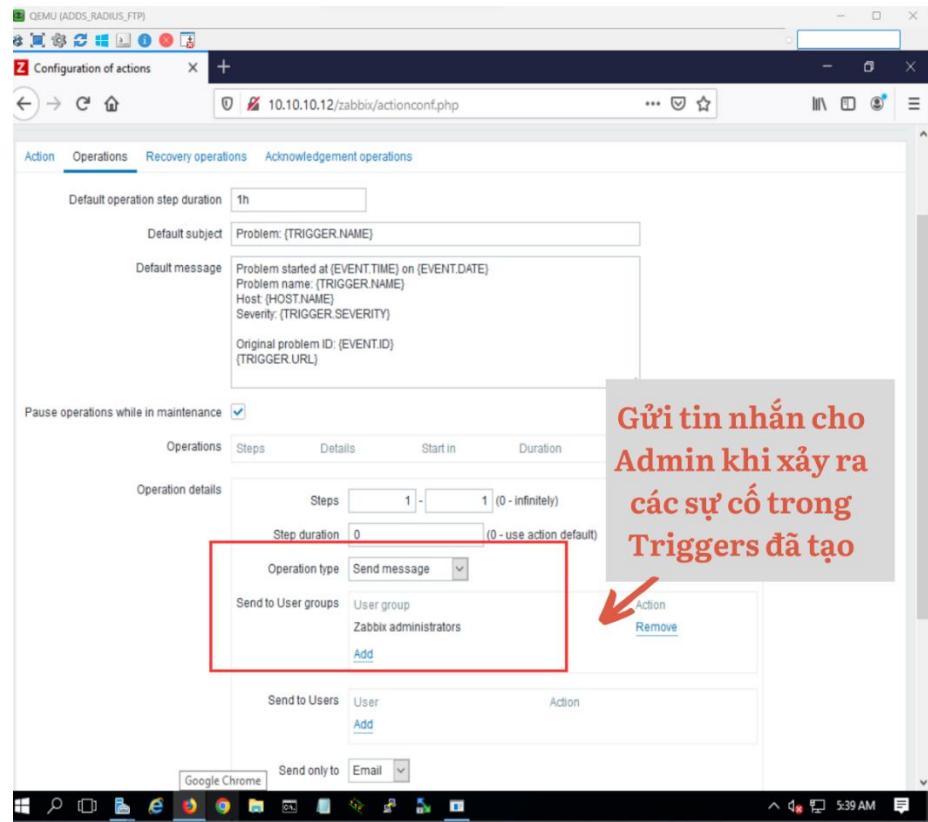
Thêm Email thông
báo

Hình 4.14.5: Thêm Email của Admin

Tiến hành tạo Actions với mục đích dựa trên triggers mà có những hành động cụ thể như là gửi email thông báo đến người quản trị. Tại mục **Configuration → Action**, chọn nguồn sự kiện là Triggers với ví dụ sự kiện là Interface của switch bị down hoặc switch khởi động lại, điều kiện Triggers xảy ra thì sẽ thiết lập hành động gửi email thông báo như hình 4.14.6 và 4.14.7.

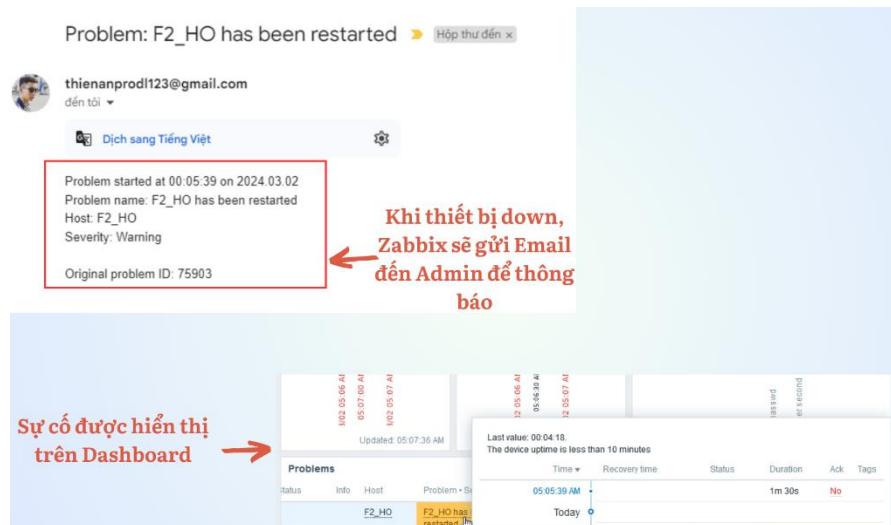


Hình 4.14.6: Tạo các Triggers cần thông báo qua Email



Hình 4.14.7: Gửi tin nhắn đến các Email trong nhóm Admin khi có sự cố

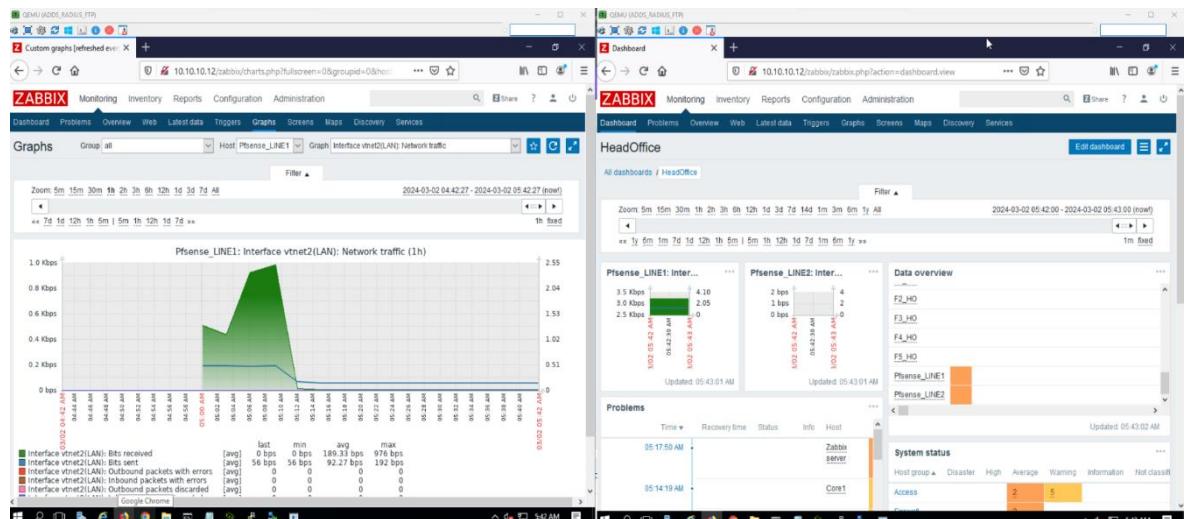
Tiến hành kiểm thử với ví dụ xảy ra sự cố switch F2_HO down và khởi động lại, lúc này người quản trị đã nhận được email thông báo kịp thời từ zabbix.



Hình 4.14.8: Email thông báo khi có sự cố

Tại màn hình chính, ta có thể tùy biến dashboard để theo dõi lưu lượng, trạng thái thiết bị, các vấn đề phát sinh xảy ra.

Như ở hình 4.14.9, ta có thể theo dõi được lưu lượng đi qua interface Vtnet2 trên firewall thông qua biểu đồ lưu lượng, ví dụ vùng xanh lá hiển thị được lưu lượng tăng cao trong khoảng thời gian nhất định, sau đó trở về lại bình thường (có thể lúc này có nhiều user sử dụng hoặc có thể có user đang tải phần mềm, sử dụng ứng dụng tiêu tốn nhiều băng thông). Bên phải hình là một dashboard khác thể hiện các thông tin cơ bản của hệ thống mà người quản trị cần theo dõi như trạng thái của nhóm thiết bị **Access**, **Core**, **Firewall**; sự cố xảy ra lúc nào tại thiết bị gì và đã được khắc phục hay chưa; biểu đồ thu nhỏ lưu lượng của interface tại hai firewall hướng ra internet.



Hình 4.14.9: Dashboard của Zabbix

CHƯƠNG 5. KẾT LUẬN

5.1 Kết quả đạt được

Trong quá trình triển khai mô hình hệ thống mạng doanh nghiệp, em đã tập trung vào những cấu hình thiết yếu cần có để hệ thống mạng trở nên an toàn, linh hoạt và hiệu quả.

Bằng cách áp dụng các biện pháp bảo mật như xác thực Radius, VPN, Firewall, ACL để bảo vệ mạng khỏi các cuộc tấn công mạng và đảm bảo tính toàn vẹn của dữ liệu. Ngoài ra, hệ thống cũng áp dụng các phương pháp dự phòng, chống lặp và tăng băng thông để giúp trải nghiệm của người dùng trở nên hiệu quả hơn.

5.2 Hạn chế và hướng phát triển

Hệ thống mạng trên vẫn còn một số nhược điểm và nếu có thể, em sẽ phát triển thêm một số tính năng mới để có thể nâng cao hiệu suất và sự linh hoạt chặng hạn như:

- Thay vì chỉ để riêng một phòng ban IT, thì chúng ta nên chia team IT ra nhiều team hơn để có thể dễ dàng quản lý và việc đặt rule sẽ không bao quát cho cả một team IT mà sẽ chia nhỏ ra theo các chức năng của từng team.
- Để dễ dàng hơn cho việc mở rộng hệ thống cho sau này, em nghĩ thay vì cấu hình trên từng Firewall, chúng ta nên chuyển đổi theo hướng cài đặt một Firewall chính, sau đó khi cần mở rộng sẽ đẩy các rule từ Firewall chính xuống các Firewall chi nhánh, như vậy sẽ tiết kiệm nhiều thời gian và có tính hiệu quả hơn.
- Ngoài việc xác thực bằng account để truy cập vào mạng thì có thể xác thực bằng địa chỉ MAC của mỗi thiết bị.
- Để phòng chống thất thoát dữ liệu trong doanh nghiệp, chúng ta có thể xây dựng thêm một số ứng dụng như DLP (Data Loss Prevention) để ngăn chặn việc dữ liệu nội bộ của doanh nghiệp bị thất thoát ra ngoài hoặc sử dụng Fasoo để mã hóa và bảo mật các tập tin của doanh nghiệp.

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Anh, T. T. (2022, September 28). [Tư hoc MCSA MCSE 2016]-Lab 4-Câu hình DHCP Server và Backup Restore - ITFORVN. ITFORVN. <https://itforvn.com/tu-hoc-mcsa-mcse-2016-lab-4-cau-hinh-dhcp-server-va-backup-restore/>
- [2] Câu hình HSRP CISCO. (n.d.). Https://Securityzone.Vn/. Retrieved May 27, 2022, from <https://securityzone.vn/t/lab-13-cau-hinh-hsrp-cisco.182/>
- [3] Hoàng, L. B. (2017, April 1). Hướng dẫn cài đặt DNS trên Windows Server 2012. sinhvientot.net. <https://sinhvientot.net/huong-dan-cai-dat-dns-tren-windows-server-2012/>
- [4] Phong T. (2020, June 24). Hướng dẫn cài đặt DHCP Role trong Windows Server 2012. Quantrimang.com. <https://quanzimang.com/cong-nghe/huong-dan-cai-dat-dhcp-role-trong-windows-server-2012-154329>
- [5] Van Cuong, T. (2024, February 28). High Available for pfsense. Viblo. <https://viblo.asia/p/high-available-for-pfsense-0bDM6wy2G2X4>
- [6] Phạm, H. (2013, November 8). Group Policy – Windows Server 2012 R2. Phạm Đinh Huy. <https://huypd.wordpress.com/2013/11/08/group-policy-windows-server-2012-r2-part-1/#:~:text=Enforced%20%3A%20th%C6%B0%E1%BB%9Dng%20%C4%91%C6%BB%E1%BB%A3c%20c%E1%BA%A5u%20h%C3%ACnh,h%C3%ACnh%20B%lock%20Inheritance%20cho%20OU.>
- [7] Lab: Quản lý và triển khai tự động hạ tầng mạng dùng Ansible (Phần 1) -. (n.d.). <https://vnpro.vn/thu-vien/lab-quan-ly-va-trien-khai-tu-dong-ha-tang-mang-dung-ansible-phan-1-4148.html>
- [8] Đại học trực tuyến FUNiX. (2023, July 5). Cách cài đặt và cấu hình Zabbix trên Ubuntu/Debian. Học Trực Tuyến CNTT, Học Lập Trình Từ Cơ Bản Đến Nâng Cao. <https://funix.edu.vn/chia-se-kien-thuc/cach-cai-dat-va-cau-hinh-zabbix-tren-ubuntu-debian/>

- [9] Anh, N. H. (2024, March 12). Tổng quan về Công nghệ EtherChannel. Viblo. <https://viblo.asia/p/tong-quan-ve-cong-nghe-etherchannel-vyDZOWAdZwj>
- [10] TÌM HIỂU VỀ GIAO THÚC SPANNING TREE PROTOCOL .. (n.d.). <https://vnpro.vn/thu-vien/tim-hieu-ve-giao-thuc-spanning-tree-protocol-3115.html>
- [11] VietTuanS. (n.d.). SNMP là gì? Cơ chế hoạt động của giao thức SNMP. Việt Tuân - Phân Phối Thiết Bị Mạng, Wifi, Thiết Bị Lưu Trữ NAS. <https://viettuan.svn/snmp-la-gi>
- [12] Tuấn, D. A. (2024, March 13). (Phần 1) Tìm hiểu về Ansible. Viblo. <https://viblo.asia/p/phan-1-tim-hieu-ve-ansible-4dbZNxv85YM>

Tiếng Anh

- [13] Cisco.IOS — Ansible Community Documentation. (n.d.). <https://docs.ansible.com/ansible/latest/collections/cisco/ios/index.html>
- [14] Installing Ansible — Ansible Community Documentation. (n.d.). https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html#installing-and-upgrading-ansible-with-pip
- [15] Getting started with Ansible — Ansible Community Documentation. (n.d.). https://docs.ansible.com/ansible/latest/getting_started/index.html