

Bộ Giáo Dục Và Đào Tạo
Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh
Khoa Công Nghệ Thông Tin



MÔN HỌC : ĐỒ ÁN MẠNG

**ĐỀ TÀI: XÂY DỰNG HỆ THỐNG MẠNG CHO
VIỆN GIÁO DỤC QUỐC TẾ HUFLIT**

Giáo Viên Hướng Dẫn : TS/ThS Đỗ Phi Hưng

Thành Viên :

1. Nguyễn Công Khanh – MSSV: 22DH111558
2. Nguyễn Thị Kim Doanh – MSSV: 22DH110511
3. Nguyễn Võ Anh Khoa – MSSV: 22DH111682

Tp. Hồ Chí Minh, Ngày 30 tháng 10 năm 2024

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin gửi lời cảm ơn chân thành tới Trường Đại học Ngoại ngữ - Tin học Thành phố Hồ Chí Minh và sau là khoa Công nghệ Thông tin đã tạo điều kiện cho chúng em được tiếp cận với môn Đồ án mạng.

Đặc biệt nhóm em xin gửi lời cảm ơn sâu sắc tới thầy Đỗ Phi Hưng là giảng viên hướng dẫn của nhóm em. Trong suốt thời gian qua Thầy đã dành nhiều thời gian và công sức để chỉ bảo, hỗ trợ và đánh giá nội dung của đề tài một cách khách quan và chính xác. Những ý kiến đóng góp của Thầy đã giúp nhóm em hoàn thiện hơn về sản phẩm của mình.

Nhóm em cũng xin gửi lời cảm ơn đến các bạn sinh viên khác đã giúp đỡ và chia sẻ kinh nghiệm trong quá trình làm việc nhóm để có thể ngày một hoàn thiện hơn.

Bài báo cáo đề tài môn Đồ án mạng thực hiện trong khoảng thời gian 2 tháng. Vì lượng kiến thức của chúng em còn nhiều hạn chế nên không tránh khỏi những thiếu sót, chúng em rất mong nhận được những ý kiến đóng góp quý báu từ Thầy để tiếp thu kiến thức lĩnh vực này được hoàn chỉnh hơn, học hỏi thêm nhiều kinh nghiệm, đồng thời có điều kiện bổ sung, nâng cao trình độ để hành trang tốt hơn trong công việc sau này.

Cuối cùng, nhóm em xin được phép thay mặt các thành viên trong nhóm xin được gửi lời chúc sức khỏe và thành công đến với Thầy và các bạn sinh viên.

Chúc Thầy luôn có thật nhiều niềm vui, sức khỏe, chúc cho Thầy luôn vững tin và thành công trên sự nghiệp trồng người.

NHẬN XÉT CỦA GIẢNG VIÊN

BẢNG PHÂN CÔNG CÔNG VIỆC

Tên thành viên	Công việc	Mức độ hoàn thành
Nguyễn Công Khanh	Bảng phân hoạch IP	100%
Nguyễn Thị Kim Doanh	Sơ đồ logic, viết báo cáo	100%
Nguyễn Võ Anh Khoa	Sơ đồ vật lý	100%

Bảng 1. Bảng phân công công việc.

MỤC LỤC

ĐỀ TÀI: XÂY DỰNG HỆ THỐNG MẠNG CHO VIỆN GIÁO DỤC QUỐC TẾ HUFLIT	i
LỜI CẢM ƠN	2
NHẬN XÉT CỦA GIẢNG VIÊN.....	3
BẢNG PHÂN CÔNG CÔNG VIỆC	4
MÔ TẢ ĐỒ ÁN	7
CHƯƠNG 1: NETWORK OPERATING SYSTEM (NOS)	8
1. Đánh giá các loại NOS:.....	9
1.1. So sánh và đánh giá các loại NOS (windows, linux, macos, ...):.....	9
1.2. Lựa chọn NOS phù hợp với dự án:.....	13
1.3. Các dịch vụ mạng cần triển khai (network services: Domain Controller, DNS, DHCP, ...):.....	14
2. Khả năng dự phòng:	16
2.1. Các hệ thống lưu trữ tập trung:	16
2.2. Các kiểu backup, RAID:	18
2.3. Các dịch vụ tường lửa:	20
2.4. Các hệ thống phát hiện xâm nhập:	21
2.5. Các hệ thống giám sát mạng:	23
CHƯƠNG 2: LÊN KẾ HOẠCH TRIỂN KHAI.....	26
1. Thiết kế hệ thống:	26
1.1. Chọn các phần mềm cần triển khai và chức năng (File, Backup, Firewall, IDS, ...):.....	26
1.2. Thiết bị cần có:.....	27
1.3. Physical topology, Logical topology và IP Table:.....	28
2. Đánh giá và kiểm chứng kế hoạch:	31
CHƯƠNG 3: TRIỂN KHAI	32
1. Triển khai setup hệ thống:	32

1.1. Domain Controller:	32
1.2. DNS:	34
1.3. DHCP:.....	35
1.4. Backup DHCP:.....	36
2. Cấu hình và test lỗi:	37
2.1. Router:	37
2.2. Fortigate:	37
2.3. Switch layer 3:.....	38
3. Đánh giá kết quả thực hiện:	40
3.1. Đã làm được những gì?	40
3.2. Chưa làm được những gì?	40
3.3. Điểm hạn chế:.....	40
CHƯƠNG 4: QUẢN TRỊ HỆ THỐNG.....	41
1. Đánh giá và lựa chọn network monitoring tool (SNMP, PRTG, ...):.....	41
2. Các báo cáo nhận được:	41
CHƯƠNG 5: REFERENCES LIST	42
DANH MỤC HÌNH ẢNH	43
DANH MỤC BẢNG BIỂU	44

MÔ TẢ ĐỒ ÁN

Bạn là kỹ sư Network của Công ty Hudo, chuyên các giải pháp Mạng công nghệ cao, có các chi nhánh ở các thành phố HCM, HN, DN, CT.

Công ty vừa có hợp đồng triển khai mạng cho Viện Giáo Dục Quốc Tế HUFLIT. Cụ thể như sau:

Nhân sự: 400 sinh viên, 30 giảng viên, 20 nhân viên marketing và giáo vụ, 5 quản lý cao cấp bao gồm giám đốc chương trình và quản lý đào tạo, 3 nhân viên quản trị mạng.

Thiết bị: 60 máy tính cho phòng Lab, 35 máy tính cho nhân viên, 3 máy in, chưa tính số lượng Server.

Tòa nhà: gồm 4 tầng, máy tính và máy in đặt ở tầng trệt, ngoại trừ phòng thực hành IT: 1 phòng ở tầng 1 và 1 phòng khác ở tầng 2 và tầng 3.

Viện Giáo Dục yêu cầu triển khai hệ thống Mạng đáp ứng số người dùng như trên, lưu trữ tập trung, có khả năng Backup và Restore dữ liệu, phủ sóng Wifi toàn bộ 4 tầng, có hệ thống tường lửa bảo mật, phát hiện xâm nhập, giám sát hệ thống mạng.

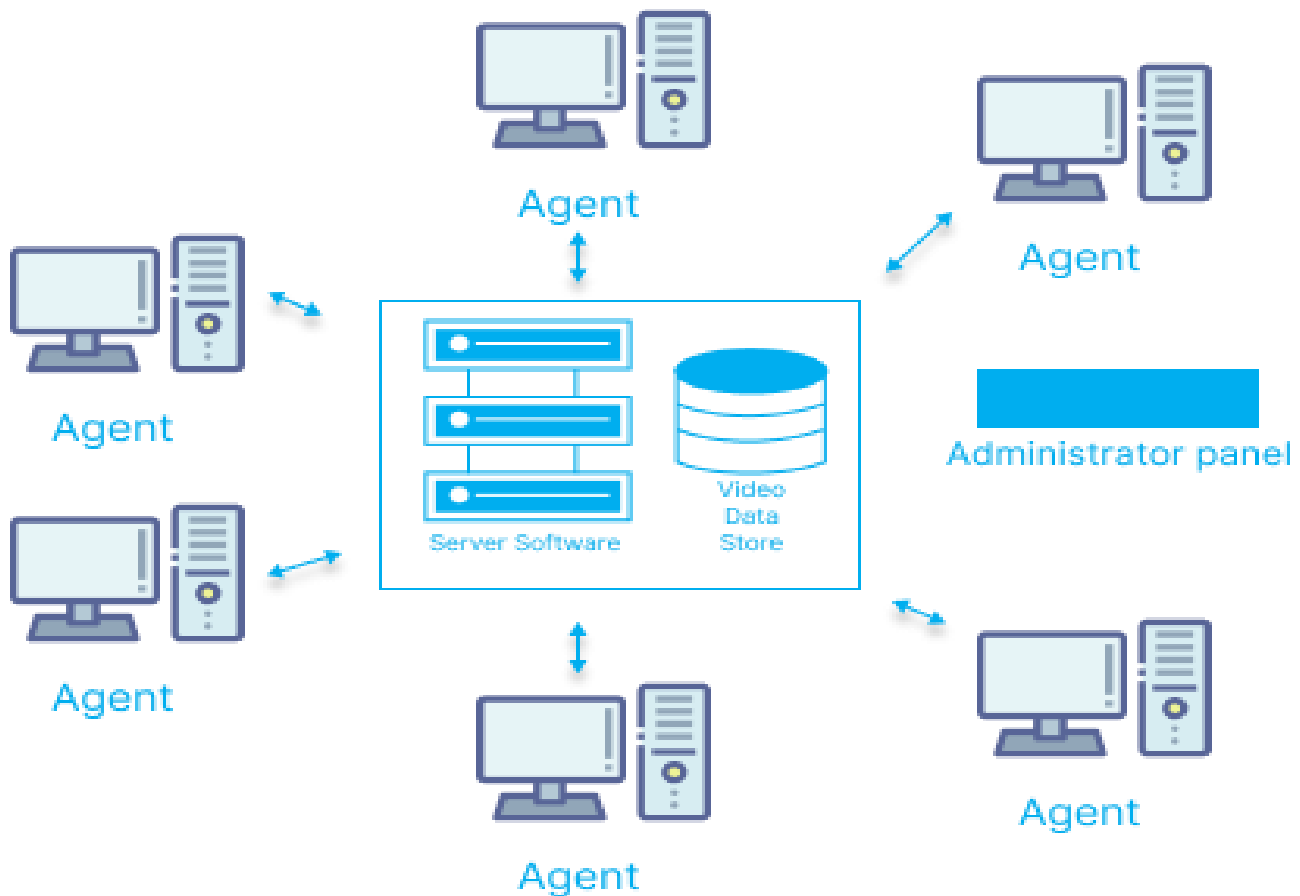
Nhiệm vụ đầu tiên mà CEO Hung yêu cầu là tìm hiểu và lựa chọn mô hình phù hợp với dự án, sau đó gửi báo cáo.

CEO Hung rất vui vì nhận được báo cáo đầu tiên của các bạn, ông yêu cầu nhóm dự án lên kế hoạch và triển khai cụ thể như sau:

CHƯƠNG 1: NETWORK OPERATING SYSTEM (NOS)

Hệ điều hành mạng (NOS) là một hệ điều hành đặc biệt, được thiết kế để quản lý và điều khiển các thiết bị trong một mạng máy tính. Nó đóng vai trò như một cầu nối, giúp các máy tính, máy chủ, thiết bị ngoại vi và các nguồn lực khác có thể giao tiếp và chia sẻ thông tin với nhau một cách hiệu quả. NOS thường được sử dụng trong các mạng LAN (Local Area Network) hoặc WAN (Wide Area Network).

Network Operating System



Hình 1. Network Operating System.

1. Đánh giá các loại NOS:

1.1. So sánh và đánh giá các loại NOS (windows, linux, macos, ...):

1.1.1. Windows Server (Microsoft):

- Là hệ điều hành mạng phổ biến của Microsoft, được sử dụng trong các doanh nghiệp vừa và lớn để quản lý các tài nguyên mạng, cung cấp dịch vụ như Active Directory, quản lý tệp tin, dịch vụ web, và các ứng dụng máy chủ.
- Tính năng chính: quản lý tập trung thông qua Active Directory; hỗ trợ ảo hóa với Hyper-V; quản lý máy in, máy chủ email và cơ sở dữ liệu; hỗ trợ các giao thức mạng như SMB, RDP, FTP, ...
- Các phiên bản: Windows Server 2019, Windows Server 2022, ...

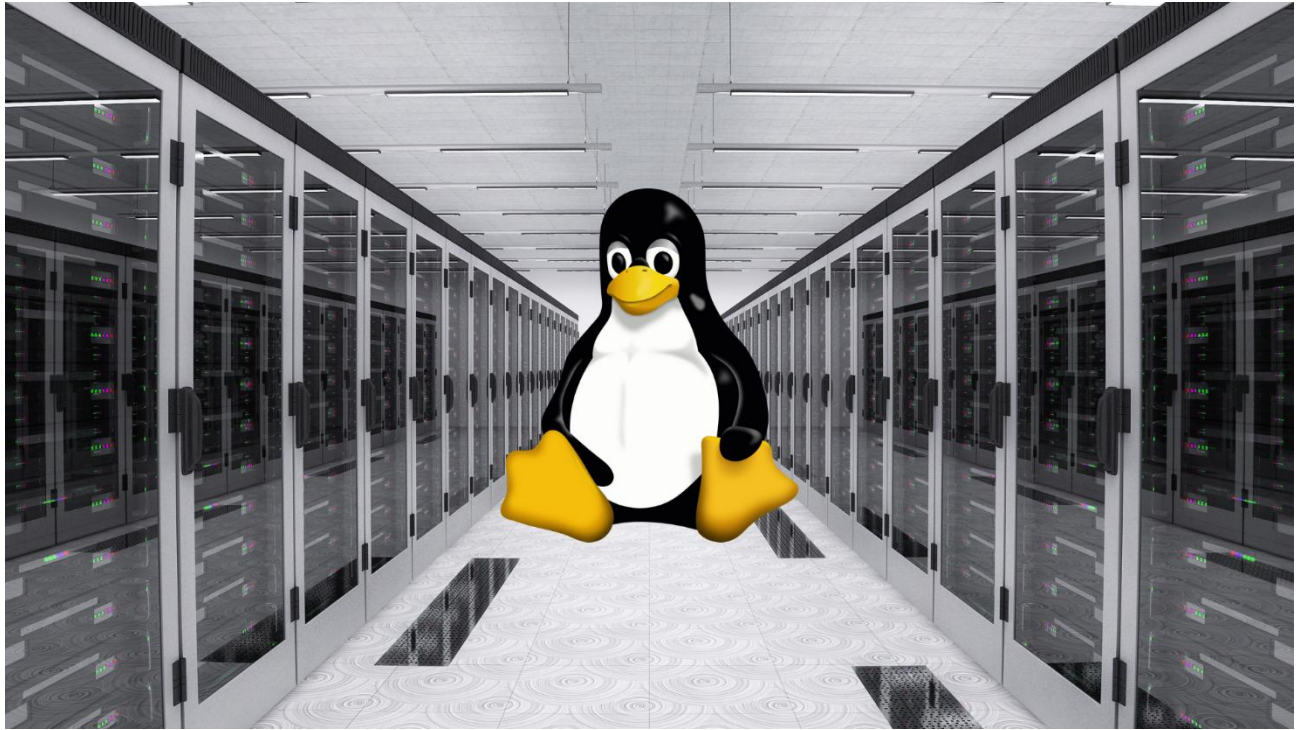


Hình 2. Window Server.

1.1.2. Linux (Server Distros):

- Có nhiều bản phân phối (distributions) khác nhau, được sử dụng như hệ điều hành mạng mã nguồn mở. Linux có tính ổn định, bảo mật cao và dễ tùy chỉnh, thích hợp cho cả các doanh nghiệp nhỏ, trung tâm dữ liệu lớn và dịch vụ đám mây.

- Tính năng chính: hỗ trợ nhiều giao thức mạng (NFS, SMB, FTP, SSH); tính ổn định và bảo mật cao; khả năng ảo hóa mạnh mẽ (KVM, Docker, LXC); dễ dàng cấu hình và mở rộng, rất phổ biến trong các hệ thống máy chủ web, ...
- Các phiên bản: Ubuntu Server, CentOS, Debian, ...



Hình 3. Linux Server.

1.1.3. MacOS (Apple):

- Không phải là một hệ điều hành mạng phổ biến như Windows Server hay Linux trong môi trường doanh nghiệp, nhưng được sử dụng trong một số môi trường đặc biệt, như các hệ thống thiết kế đồ họa hoặc lập trình, với khả năng kết nối mạng cơ bản và hỗ trợ chia sẻ tài nguyên.
- Tính năng chính: tích hợp chặt chẽ với các sản phẩm của Apple (như iCloud, Handoff, AirDrop); hỗ trợ dịch vụ chia sẻ tệp qua mạng, in ấn qua mạng và sử dụng Bonjour để tự động phát hiện các dịch vụ trong mạng; hỗ trợ giao thức mạng SMB và AFP (Apple Filing Protocol).



Hình 4. MacOS Server.

1.1.4. Cisco IOS (Internetwork Operating System):

- Là hệ điều hành mạng của Cisco, được sử dụng để quản lý và cấu hình các thiết bị mạng như router và switch. Cisco IOS rất mạnh trong các ứng dụng doanh nghiệp lớn và môi trường mạng phức tạp.
- Tính năng chính: hỗ trợ nhiều giao thức định tuyến (OSPF, BGP, EIGRP) và dịch vụ mạng như NAT, VPN, QoS; quản lý thiết bị mạng từ xa qua giao diện dòng lệnh (CLI); bảo mật cao với các tính năng firewall, access control list (ACL) và hệ thống phát hiện lệnh xâm nhập (IPS/IDS); khả năng ảo hóa và tạo các mạng ảo với Cisco SD-WAN.



Hình 5. Cisco IOS.

1.1.5. So sánh giữa các loại NOS:

	Windows Server	Linux	MacOS Server	Cisco IOS
Giao diện	Thân thiện	Phức tạp	Thân thiện	Dòng lệnh
Chi phí	Cao	Miễn phí	Cao	Bao gồm trong thiết bị
Linh hoạt	Trung bình	Cao	Trung bình	Cao
Bảo mật	Tốt	Tốt	Rất tốt	Rất tốt
Ứng dụng	Doanh nghiệp vừa và nhỏ	Doanh nghiệp lớn, dịch vụ	Môi trường Apple	Mạng lớn, phức tạp



Hình 6. So sánh các loại NOS.

1.1.6. Đánh giá các loại NOS:

- Windows Server: Được sử dụng trong các doanh nghiệp với khả năng quản lý tập trung, thích hợp cho các dịch vụ như email, quản lý file, và máy chủ web.
- Linux: Phù hợp với các tổ chức muốn có hệ điều hành mã nguồn mở, bảo mật cao, và khả năng tùy chỉnh, thường được sử dụng trong các máy chủ web và dịch vụ đám mây.
- MacOS: Thường không được dùng trong môi trường doanh nghiệp lớn với vai trò hệ điều hành mạng, nhưng có các tính năng kết nối mạng và chia sẻ tài nguyên cơ bản trong hệ sinh thái Apple.
- Cisco IOS: Hệ điều hành chuyên về thiết bị mạng như router và switch, rất phổ biến trong môi trường mạng doanh nghiệp và các nhà cung cấp dịch vụ.

1.2. Lựa chọn NOS phù hợp với dự án:

Windows Server là NOS phù hợp nhất với dự án với 1 số lý do sau:

- Tính tương thích cao: tích hợp tốt các ứng dụng văn phòng, giúp dễ dàng quản lý và chia sẻ dữ liệu; phần lớn các phần cứng hỗ trợ Windows, giúp quá trình cài đặt và cấu hình đơn giản hơn.

- Giao diện thân thiện, dễ sử dụng: giao diện được thiết kế trực quan, giúp người dùng dễ dàng nắm bắt và thực hiện các tác vụ; có nhiều tài liệu hướng dẫn, cộng đồng người dùng lớn, giúp giải quyết các vấn đề phát sinh nhanh chóng.
- Bảo mật: cung cấp nhiều tính năng bảo mật như tường lửa tích hợp, xác thực đa yếu tố; thường xuyên phát hành các bản cập nhật bảo mật để vá các lỗ hổng tiềm ẩn.
- Tích hợp các tác vụ: Active Directory, Exchange Server, SharePoint, SQL Server.
- Hỗ trợ từ Microsoft: cung cấp các dịch vụ hỗ trợ kỹ thuật; cộng đồng người dùng Windows Server lớn mạnh có thể tìm kiếm sự trợ giúp và chia sẻ kinh nghiệm.

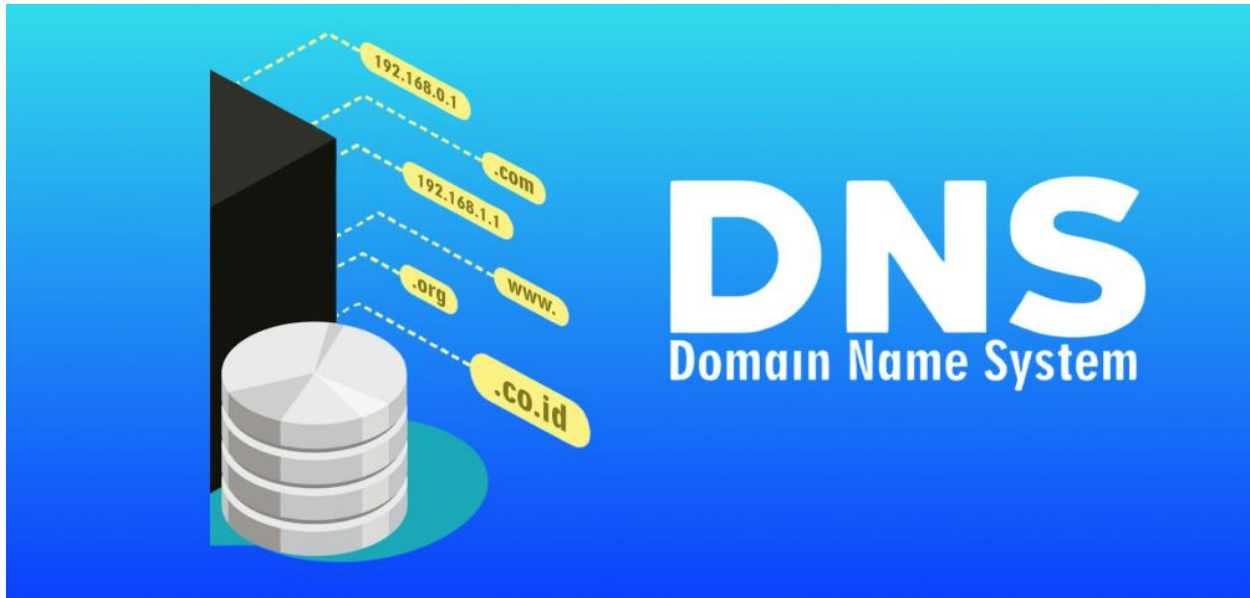
1.3. Các dịch vụ mạng cần triển khai (network services: Domain Controller, DNS, DHCP, ...):

- Domain Controller là một máy chủ trong hệ thống mạng dùng để quản lý bảo mật, xác thực người dùng, và kiểm soát các tài nguyên trong một domain (miền) của mạng máy tính, đặc biệt trong các hệ thống sử dụng Active Directory (AD) của Microsoft. Đóng vai trò quan trọng trong việc xác định danh tính và quyền truy cập của người dùng và thiết bị vào các tài nguyên mạng.



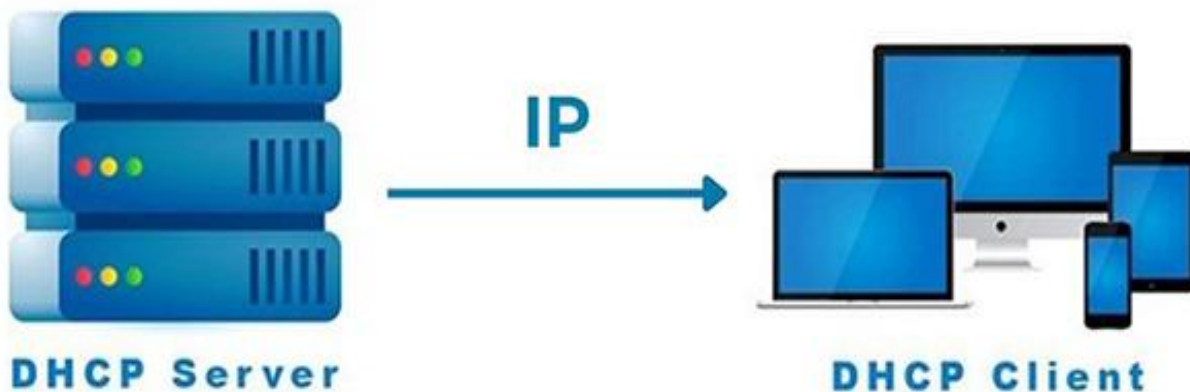
Hình 7. Domain Controller.

- DNS (Domain Name System) là một hệ thống phân giải tên miền, đóng vai trò là “sổ địa chỉ”, giúp chuyển đổi các tên miền dễ nhớ thành các địa chỉ IP mà máy tính có thể hiểu và sử dụng để liên lạc với nhau trên mạng Internet. Làm cho việc truy cập Internet trở nên dễ dàng và thuận tiện hơn rất nhiều mà không cần phải hiểu biết quá nhiều về cấu trúc mạng.



Hình 8. Domain Name System.

- DHCP (Dynamic Host Configuration Protocol) là một giao thức mạng rất quan trọng, có nhiệm vụ tự động cấp phát địa chỉ IP và các thông tin cấu hình mạng khác cho các thiết bị trong mạng khi chúng kết nối vào mạng. Giúp đơn giản hóa việc quản lý mạng và đảm bảo hoạt động mạng hiệu quả.



Hình 9. Dynamic Host Configuration Protocol.

- Backup là một quá trình quan trọng để đảm bảo tính toàn vẹn và khả năng phục hồi của dữ liệu trên máy chủ. Khi thực hiện sao lưu, sẽ tạo ra một bản sao chính xác của hệ thống hoặc dữ liệu của mình tại một thời điểm cụ thể, giúp khôi phục lại dữ liệu trong trường hợp xảy ra sự cố như mất điện, hỏng hóc phần cứng, tấn công mạng hoặc lỗi phần mềm.



Hình 10. Backup.

2. Khả năng dự phòng:

2.1. Các hệ thống lưu trữ tập trung:

Là một giải pháp trong đó các dữ liệu và tài nguyên lưu trữ được quản lý từ một vị trí trung tâm, thay vì phân tán dữ liệu trên nhiều thiết bị hoặc máy chủ khác nhau. Các hệ thống này giúp dễ dàng quản lý, bảo mật, và chia sẻ dữ liệu giữa các người dùng và ứng dụng khác nhau trong mạng.



Hình 11. Các hệ thống lưu trữ tập trung.

2.1.1. NAS (Network Attached Storage):

- Đặc điểm: Là một thiết bị chuyên dụng để lưu trữ dữ liệu và được kết nối trực tiếp vào mạng LAN. NAS thường được sử dụng cho các doanh nghiệp nhỏ và vừa.
- Ưu điểm: Dễ cài đặt, sử dụng, chi phí hợp lý.
- Nhược điểm: Khả năng mở rộng hạn chế hơn so với các hệ thống khác.

2.1.2. SAN (Storage Area Network):

- Đặc điểm: Là một mạng riêng dành riêng cho việc lưu trữ dữ liệu, cung cấp hiệu năng cao và khả năng mở rộng lớn. SAN thường được sử dụng trong các môi trường doanh nghiệp lớn.
- Ưu điểm: Hiệu năng cao, khả năng mở rộng lớn, bảo mật tốt.
- Nhược điểm: Chi phí đầu tư cao, phức tạp trong cài đặt và quản lý.

2.1.3. DAS (Direct Attached Storage):

- Đặc điểm: Lưu trữ kết nối trực tiếp với máy chủ mà không cần qua mạng, do đó không thể chia sẻ dữ liệu cho các thiết bị khác một cách dễ dàng. DAS thường được sử dụng cho các doanh nghiệp nhỏ và vừa.
- Ưu điểm: Hiệu năng cao, đơn giản, chi phí thấp.

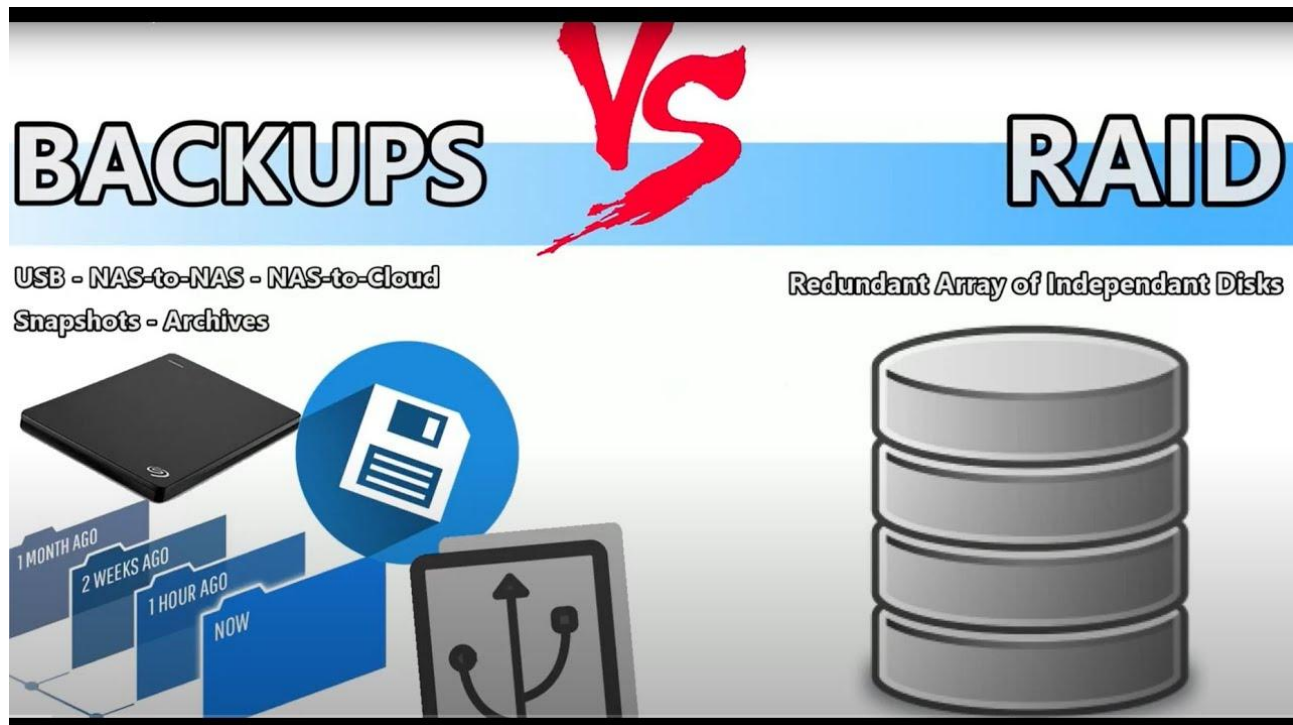
- Nhược điểm: Không có khả năng chia sẻ dữ liệu, không thể mở rộng linh hoạt.

2.1.4. Cloud Storage:

- Đặc điểm: Lưu trữ dữ liệu trên các máy chủ của bên thứ ba thông qua internet.
- Ưu điểm: Linh hoạt, dễ sử dụng, chi phí thấp, không cần quản lý hạ tầng.
- Nhược điểm: Phụ thuộc vào nhà cung cấp dịch vụ, có thể gặp vấn đề về tốc độ kết nối nếu đường truyền không ổn định.

2.2. Các kiểu backup, RAID:

Sao lưu dữ liệu là một quá trình quan trọng để bảo vệ thông tin khỏi mất mát do các sự cố như hỏng hóc phần cứng, lỗi phần mềm, tấn công mạng, thiên tai, ... Dưới đây là một số kiểu sao lưu phổ biến:



Hình 12. Các kiểu backup, RAID.

2.2.1. Các kiểu backup:

Sao lưu dữ liệu là một quá trình quan trọng để bảo vệ thông tin khỏi mất mát do các sự cố như hỏng hóc phần cứng, lỗi phần mềm, tấn công mạng, thiên tai, ... Dưới đây là một số kiểu sao lưu phổ biến:

2.2.1.1. Sao lưu toàn bộ (Full Backup):

- Sao lưu toàn bộ dữ liệu của hệ thống vào một điểm phục hồi duy nhất.
- Ưu điểm: Đảm bảo khôi phục dữ liệu một cách nhanh chóng và dễ dàng.

- Nhược điểm: Mất nhiều thời gian và dung lượng lưu trữ, đặc biệt đối với các hệ thống có lượng dữ liệu lớn.

2.2.1.2. Sao lưu tăng dần (Incremental Backup):

- Sao lưu tăng dần (Incremental Backup): Chỉ sao lưu những thay đổi so với bản sao lưu toàn bộ gần nhất.
- Ưu điểm: Tiết kiệm thời gian và dung lượng lưu trữ so với sao lưu toàn bộ.
- Nhược điểm: Để khôi phục dữ liệu cần phải có bản sao lưu toàn bộ và tất cả các bản sao lưu tăng dần sau đó.

2.2.1.3. Sao lưu khác biệt (Differential Backup):

- Sao lưu tất cả những thay đổi kể từ lần sao lưu toàn bộ gần nhất.
- Ưu điểm: Khôi phục dữ liệu nhanh hơn so với sao lưu tăng dần vì chỉ cần hai bản sao lưu (toàn bộ và khác biệt).
- Nhược điểm: Vẫn tốn nhiều dung lượng lưu trữ hơn so với sao lưu tăng dần.

2.2.1.4. Sao lưu tổng hợp (Synthetic Full Backup):

- Tạo một bản sao lưu toàn bộ mới dựa trên bản sao lưu toàn bộ cũ nhất và các bản sao lưu tăng dần hoặc khác biệt.
- Ưu điểm: Giúp giảm thiểu thời gian thực hiện sao lưu toàn bộ đầy đủ.
- Nhược điểm: Cần có quy trình quản lý sao lưu phức tạp hơn.

2.2.2. Các kiểu RAID:

RAID (Redundant Array of Independent Disks) là mảng dư thừa các đĩa độc lập. Là một công nghệ sử dụng nhiều ổ đĩa cứng để tăng hiệu suất, độ tin cậy và khả năng mở rộng cho hệ thống lưu trữ. Dưới đây là một số cấp độ RAID phổ biến:

2.2.2.1. RAID 0 (Striping):

- Ưu điểm: Tốc độ đọc/ghi rất cao nhờ phân chia dữ liệu đều lên các ổ đĩa.
- Nhược điểm: Không có khả năng phục hồi dữ liệu khi một ổ đĩa bị hỏng.
- Ứng dụng: Các hệ thống cần tốc độ cao như máy chủ cơ sở dữ liệu, render video.

2.2.2.2. RAID 1 (Mirroring):

- Ưu điểm: Bảo vệ dữ liệu cao nhờ sao chép dữ liệu giống hệt nhau lên các ổ đĩa.
- Nhược điểm: Tốn nhiều dung lượng ổ đĩa.
- Ứng dụng: Các hệ thống yêu cầu độ tin cậy cao như máy chủ, máy chủ lưu trữ.

2.2.2.3. RAID 5 (Striping with Parity):

- Ưu điểm: Kết hợp giữa hiệu suất và bảo vệ dữ liệu, sử dụng bit chẵn lẻ để phục hồi dữ liệu khi một ổ đĩa bị hỏng.
- Nhược điểm: Tốc độ viết chậm hơn so với RAID 0, khả năng phục hồi dữ liệu chậm hơn so với RAID 1 khi nhiều ổ đĩa bị hỏng cùng lúc.
- Ứng dụng: Phổ biến nhất, thích hợp cho hầu hết các hệ thống máy chủ.

2.2.2.4. RAID 6 (Double Parity):

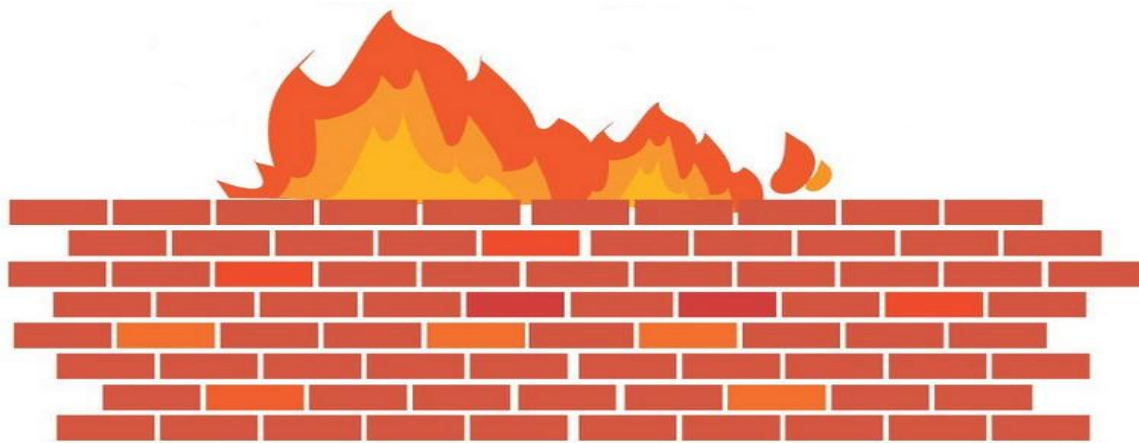
- Ưu điểm: Bảo vệ dữ liệu cao hơn RAID 5, có thể phục hồi dữ liệu khi hai ổ đĩa bị hỏng.
- Nhược điểm: Tốn nhiều dung lượng ổ đĩa hơn RAID 5.
- Ứng dụng: Các hệ thống yêu cầu độ tin cậy rất cao, như các trung tâm dữ liệu lớn.

2.2.2.5. RAID 10 (RAID 1 + 0):

- Ưu điểm: Kết hợp giữa RAID 0 và RAID 1, mang lại hiệu suất cao và khả năng bảo vệ dữ liệu tốt.
- Nhược điểm: Tốn nhiều dung lượng ổ đĩa.
- Ứng dụng: Các hệ thống cần cả hiệu suất cao và độ tin cậy, như máy chủ cơ sở dữ liệu, máy chủ ứng dụng.

2.3. Các dịch vụ tường lửa:

Tường lửa là một hệ thống bảo mật mạng đóng vai trò như một hàng rào bảo vệ, kiểm soát và giám sát lưu lượng mạng đi vào và đi ra khỏi một mạng riêng. Tường lửa hoạt động dựa trên các quy tắc được cấu hình sẵn để cho phép hoặc chặn các loại giao tiếp mạng nhất định. Dưới đây là một số dịch vụ tường lửa phổ biến:



Hình 13. Các loại tường lửa.

2.3.1. Tường lửa phần cứng (Hardware Firewall):

- Đặc điểm: Là một thiết bị vật lý chuyên dụng, được cài đặt trên một máy chủ hoặc thiết bị mạng riêng biệt.
- Ưu điểm: Hiệu suất cao, khả năng xử lý lưu lượng lớn, linh hoạt trong cấu hình.
- Nhược điểm: Chi phí đầu tư ban đầu cao, cần nhân viên kỹ thuật để cài đặt và quản lý.

2.3.2. Tường lửa phần mềm (Software Firewall):

- Đặc điểm: Được cài đặt trực tiếp trên hệ điều hành của một máy tính hoặc máy chủ.
- Ưu điểm: Dễ cài đặt và quản lý, chi phí thấp hơn so với tường lửa phần cứng.
- Nhược điểm: Hiệu suất có thể bị ảnh hưởng bởi các chương trình khác chạy trên cùng một máy

2.3.3. Tường lửa mạng (Network Firewall):

- Đặc điểm: Được triển khai ở mức độ mạng để bảo vệ toàn bộ hệ thống mạng và kiểm soát lưu lượng truy cập.
- Ưu điểm: Bảo vệ toàn bộ hệ thống mạng, hiệu quả trong việc kiểm soát truy cập từ xa hoặc giữa các phân đoạn mạng.
- Nhược điểm: Cấu hình và quản lý phức tạp, cần chuyên môn kỹ thuật cao.

2.3.4. Tường lửa đám mây (Cloud Firewall):

- Đặc điểm: Là một dịch vụ tường lửa được cung cấp qua Internet.
- Ưu điểm: Dễ sử dụng, không cần đầu tư phần cứng, dễ dàng mở rộng.
- Nhược điểm: Phụ thuộc vào nhà cung cấp dịch vụ, có thể gặp vấn đề về độ ổn định khi kết nối mạng kém.

2.4. Các hệ thống phát hiện xâm nhập:

IDS (Intrusion Detection System) là công nghệ giúp theo dõi và phân tích lưu lượng mạng hoặc hệ thống để phát hiện các hoạt động bất thường hoặc các dấu hiệu của một cuộc tấn công. IDS đóng vai trò quan trọng trong việc bảo vệ mạng và dữ liệu khỏi các hành vi xâm nhập bất hợp pháp. Dưới đây là các loại hệ thống phát hiện xâm nhập phổ biến:



Hình 14. Network Intrusion Detection System.

2.4.1. NIDS (Network Intrusion Detection System):

- NIDS giám sát lưu lượng mạng đến và đi qua một mạng cụ thể. Hệ thống này phân tích tất cả các gói tin để tìm kiếm các mẫu hoặc hành vi bất thường, cảnh báo khi phát hiện sự xâm nhập tiềm năng. Phù hợp cho các mạng lớn, nơi lưu lượng cần được giám sát toàn diện, như trong các doanh nghiệp hoặc tổ chức.
- Ưu điểm: Phát hiện các mối đe dọa trước khi chúng xâm nhập vào hệ thống, giám sát lưu lượng trên toàn bộ mạng, bảo vệ nhiều hệ thống trong cùng một thời gian.
- Nhược điểm: Khó phát hiện các tấn công được mã hóa hoặc lưu lượng qua VPN, có thể bỏ sót các cuộc tấn công diễn ra trong hệ thống nội bộ.

2.4.2. HIDS (Host-based Intrusion Detection System):

- HIDS được cài đặt trên các máy chủ hoặc thiết bị cá nhân để theo dõi và phân tích các hoạt động trong hệ điều hành, nhật ký hệ thống, và các tệp tin để phát hiện sự xâm nhập. Phù hợp cho các máy chủ, thiết bị cá nhân quan trọng hoặc có chứa dữ liệu nhạy cảm cần bảo vệ chi tiết.
- Ưu điểm: Có thể phát hiện các hành vi xâm nhập ngay trên máy chủ hoặc thiết bị, giám sát tệp tin, nhật ký và các quá trình hệ thống một cách chi tiết.

- Nhược điểm: Chỉ bảo vệ được thiết bị đã cài đặt hệ thống HIDS, có thể không phát hiện được các cuộc tấn công ở cấp độ mạng.

2.4.3. Signature-based IDS:

- Sử dụng các chữ ký (signatures) – các mẫu hoặc dấu hiệu đã biết về các cuộc tấn công trước đó để phát hiện các cuộc xâm nhập. Khi một hoạt động khớp với một chữ ký trong cơ sở dữ liệu, IDS sẽ cảnh báo. Phù hợp cho các môi trường cần phát hiện nhanh các mối đe dọa đã biết, chẳng hạn như hệ thống tài chính hoặc cơ sở dữ liệu lớn.
- Ưu điểm: Hiệu quả trong việc phát hiện các cuộc tấn công đã biết, ít gây ra báo động giả.
- Nhược điểm: Không thể phát hiện các cuộc tấn công mới hoặc chưa có chữ ký, yêu cầu cập nhật thường xuyên cơ sở dữ liệu chữ ký.

2.4.4. Anomaly-based IDS:

- IDS dựa trên bất thường phát hiện sự xâm nhập bằng cách thiết lập một đường cơ sở của hoạt động bình thường và sau đó giám sát hệ thống hoặc mạng để phát hiện các hoạt động bất thường so với đường cơ sở. Phù hợp cho các môi trường yêu cầu giám sát toàn diện và có khả năng phát hiện các mối đe dọa tiềm ẩn chưa biết trước.
- Ưu điểm: Có thể phát hiện các cuộc tấn công mới hoặc chưa biết, linh hoạt trong việc nhận diện các hành vi khác thường, không cần dựa vào chữ ký.
- Nhược điểm: Thường có nhiều báo động giả, vì một hoạt động không quen thuộc cũng có thể là hợp lệ, cần thời gian để thiết lập đường cơ sở chuẩn.

2.5. Các hệ thống giám sát mạng:

Hệ thống giám sát mạng (Network Monitoring Systems - NMS) là những công cụ và giải pháp giúp theo dõi, phân tích và quản lý hiệu suất của mạng, đảm bảo rằng các thiết bị và dịch vụ mạng hoạt động ổn định. Dưới đây là các loại hệ thống giám sát mạng phổ biến và công cụ tương ứng:



Hình 15. Network Monitoring System.

2.5.1. Giám sát hiệu suất mạng:

- Theo dõi hiệu suất hoạt động của các thiết bị mạng (router, switch, server) và các ứng dụng chạy trên mạng. Cung cấp thông tin về độ trễ, băng thông, tình trạng kết nối và khả năng sử dụng tài nguyên.
- Công cụ phổ biến: SolarWinds Network Performance Monitor, PRTG Network Monitor, Nagios.

2.5.2. Giám sát lưu lượng mạng:

- Phân tích và theo dõi lưu lượng dữ liệu đi qua mạng để phát hiện các hoạt động bất thường, xác định nguồn gốc lưu lượng và tối ưu hóa băng thông.
- Công cụ phổ biến: Wireshark, NetFlow Analyzer, sFlow.

2.5.3. Giám sát bảo mật mạng:

- Theo dõi các sự kiện bảo mật và phát hiện các hành vi đáng ngờ trong mạng. NSM giúp phát hiện các cuộc tấn công mạng và các mối đe dọa bảo mật.
- Công cụ phổ biến: Snort, Suricata, Zeek (Bro).

2.5.4. Giám sát trạng thái thiết bị:

- Theo dõi trạng thái hoạt động của các thiết bị mạng như router, switch và firewall, cung cấp thông tin về tình trạng hoạt động và hiệu suất của chúng.
- Công cụ phổ biến: Zabbix, Observium, ManageEngine OpManager.

2.5.5. Giám sát ứng dụng mạng:

- Theo dõi hiệu suất của các ứng dụng hoạt động trên mạng, giúp đảm bảo rằng chúng hoạt động ổn định và không gặp sự cố.
- Công cụ phổ biến: AppDynamics, Dynatrace, New Relic.

2.5.6. Giám sát từ xa:

- Chức năng: Giám sát và quản lý các thiết bị từ xa, thường được sử dụng bởi các nhà cung cấp dịch vụ quản lý IT.
- Công cụ phổ biến: ConnectWise Automate, Kaseya VSA, NinjaRMM.

2.5.7. Giám sát đám mây:

- Chức năng: Theo dõi hiệu suất và tình trạng của các dịch vụ và tài nguyên trên nền tảng đám mây.
- Công cụ phổ biến: Amazon CloudWatch, Azure Monitor, Google Cloud Operations.

2.5.8. Hệ thống giám sát tập trung:

- Chức năng: Quản lý và giám sát tất cả các thiết bị và dịch vụ mạng từ một giao diện duy nhất, tích hợp dữ liệu từ nhiều nguồn khác nhau.
- Công cụ phổ biến: Nagios XI, PRTG Network Monitor.

CHƯƠNG 2: LÊN KẾ HOẠCH TRIỂN KHAI

1. Thiết kế hệ thống:

1.1. Chọn các phần mềm cần triển khai và chức năng (File, Backup, Firewall, IDS, ...)

- File: NFS (Network File System) là một hệ thống giao thức chia sẻ file phát triển bởi Sun Microsystems từ năm 1984, cho phép một người dùng trên một máy tính khách truy cập tới hệ thống file chia sẻ thông qua một mạng máy tính giống như truy cập trực tiếp trên ổ cứng.
- Backup: Sync (Remote Sync) là một công cụ hữu hiệu để sao lưu và đồng bộ dữ liệu trên Linux. Với câu lệnh rsync bạn có thể sao lưu và đồng bộ dữ liệu remote từ các máy sử dụng hệ điều hành Linux một cách dễ dàng và thuận tiện. Trong bài viết này sẽ hướng dẫn bạn 10 công dụng hữu ích của rsync để truyền tải dữ liệu remote và local trên hệ điều hành Linux. Bạn không cần chạy rsync với quyền root.
- Firewall:
 - o Squid là một phần mềm proxy server mã nguồn mở được sử dụng để tạo ra một bộ đệm (cache) cho các yêu cầu web từ các máy tính trong mạng nội bộ. Nó cho phép cải thiện hiệu suất mạng bằng cách lưu trữ các tài nguyên web cục bộ và cung cấp chúng cho các máy tính trong mạng mà không cần tải lại từ máy chủ ngoại bên. Squid cũng có khả năng kiểm soát truy cập internet bằng cách thiết lập quy tắc và chính sách, cho phép quản trị viên mạng quản lý và giám sát việc sử dụng internet của người dùng.
 - o Iptables là một công cụ quản lý tường lửa được tích hợp sẵn trong hệ thống Linux. Nó cho phép bạn tạo, cấu hình và kiểm soát các luật tường lửa để lọc lưu lượng mạng trên máy tính Linux. Iptables hoạt động ở mức gói tin, cho phép bạn quyết định xem một gói tin cụ thể có được chấp nhận, từ chối hoặc chuyển hướng qua các cổng khác. Iptables rất mạnh mẽ và linh hoạt, cho phép bạn xác định các quy tắc dựa trên địa chỉ IP, cổng, giao thức và nhiều thuộc tính khác.
- IDS: Snort là phần mềm IDS được phát triển bởi Martin Roesch dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời. Với kiến

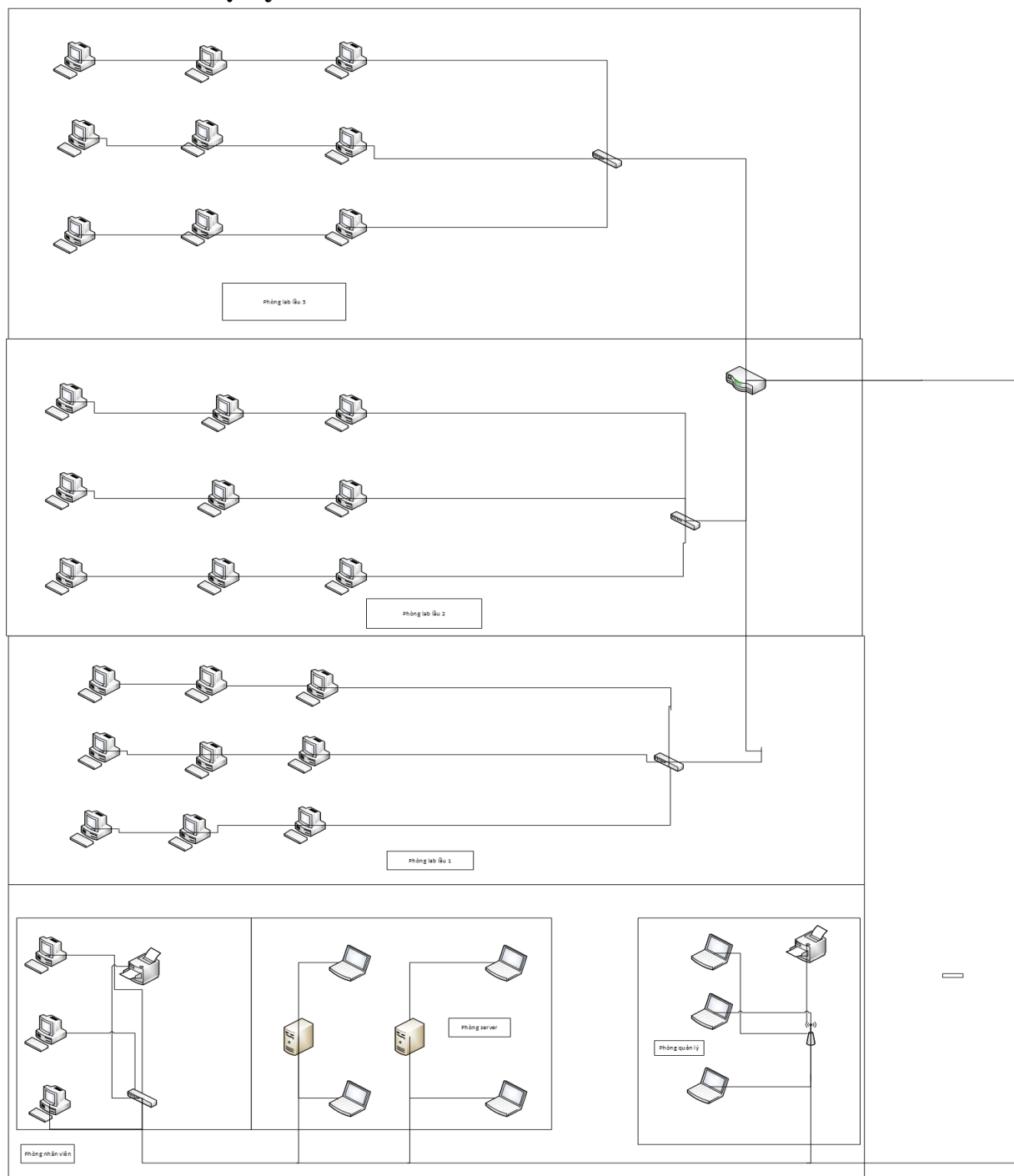
trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình. Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris. Bên cạnh việc có thể hoạt động như một ứng dụng bắt gói tin thông thường, Snort còn được cấu hình để chạy như một NIDS.

1.2. Thiết bị cần có:

- Tầng trệt:
 - 3 máy in.
 - 35 máy tính cho nhân viên marketing & giáo vụ, giảng viên.
 - 5 máy tính cho quản lý cấp cao.
 - 2 máy server.
 - 3 switch layer 2.
 - 1 router.
 - 1 firewall.
 - 1 máy cho nhân viên quản trị mạng.
 - 1 switch layer 3.
 - 1 accesspoint.
- Tầng 1:
 - 20 máy tính cho phòng lab.
 - 1 switch layer 2.
 - 1 accesspoint.
- Tầng 2:
 - 20 máy tính cho phòng lab.
 - 1 switch layer 2.
 - 1 accesspoint.
- Tầng 3:
 - 20 máy tính cho phòng lab.
 - 1 switch layer 2.
 - 1 accesspoint.

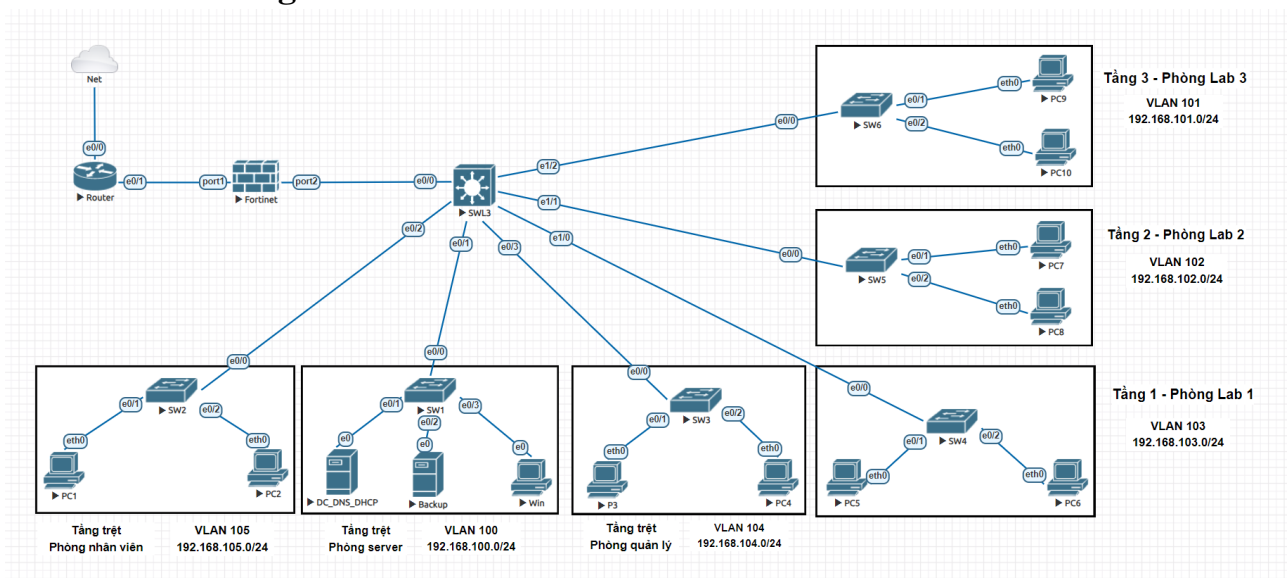
1.3. Physical topology, Logical topology và IP Table:

1.3.1. Sơ đồ vật lý:



Hình 16. Sơ đồ vật lý.

1.3.2. Sơ đồ logic:



Hình 17. Sơ đồ logic.

1.3.3. Bảng phân hoạch IP:

Ta sử dụng lớp mạng 192.168.90.0/24 để chia IP cho các thiết bị. Dự tính như sau:

- Tầng trệt: Có 3 lớp mạng cho phòng nhân viên, phòng quản lý và phòng Server. Phòng nhân viên có 35 máy và 3 máy in, phòng quản lý có 5 máy và phòng Server có 1 máy Domain, 1 máy Backup và một số máy pc. Phòng nhân viên sử dụng lớp mạng: 192.168.105.0, phòng quản lý sử dụng lớp mạng: 192.168.104.0 và phòng Server sử dụng lớp mạng: 192.168.100.0.
- Phòng thực hành IT có 60 máy chia đều cho 3 phòng:
 - o Tầng 1 sử dụng lớp mạng 192.168.103.0 cho phòng thực hành IT 1 gồm 20 máy. Các IP còn dư không được sử dụng dùng để dự phòng mở rộng cho sau này.
 - o Tầng 2 sử dụng lớp mạng 192.168.102.0 cho phòng thực hành IT 2 gồm 20 máy. Các IP còn dư không được sử dụng dùng để dự phòng mở rộng cho sau này.
 - o Tầng 3 sử dụng lớp mạng 192.168.101.0 cho phòng thực hành IT 3 gồm 20 máy. Các IP còn dư không được sử dụng dùng để dự phòng mở rộng cho sau này.

Floor	Interface	Network	Usable Range	Broadcast	Subnet mask
Ground floor	VLAN 100	192.168.100.0/24	192.168.100.100 192.168.100.254	192.168.100.255	255.255.255.0
	VLAN 104	192.168.104.0/24	192.168.104.100 192.168.104.254	192.168.104.255	255.255.255.0
	VLAN 105	192.168.105.0/24	192.168.105.100 192.168.105.254	192.168.105.255	255.255.255.0
1 st floor	20 máy tính phòng thực hành IT 1	192.168.103.0/24	192.168.103.100 192.168.103.254	192.168.103.255	255.255.255.0
2 nd floor	20 máy tính phòng thực hành IT 2	192.168.102.0/24	192.168.102.100 192.168.102.254	192.168.102.255	255.255.255.0
3 rd floor	20 máy tính phòng thực hành IT 3	192.168.101.0/24	192.168.101.100 192.168.101.254	192.168.101.255	255.255.255.0

Bảng 2. Bảng phân hoạch IP.

STT	Devices	Interface	IP	Routing		Notes
				Destination	Gateway	
1	Net		192.168.79.160/24			
2	R1	E0/0	192.168.79.167/24	0.0.0.0/0	192.168.79.160/24	DHCP từ ISP
		E0/1	192.168.2.112/24			
3	FW	Port1	192.168.2.111/24	0.0.0.0/0	192.168.2.112/24	
		Port 2	192.168.15.1/30	192.168.90.0/24	192.168.15.2/30	
			192.168.15.1/30	192.168.100.0/24		
			192.168.15.1/30	192.168.101.0/24		
			192.168.15.1/30	192.168.102.0/24		

			192.168.15.1/30	192.168.103.0/24		
			192.168.15.1/30	192.168.104.0/24		
			192.168.15.1/30	192.168.105.0/24		
4	SWL3 (Core Switch)	E0/0	192.168.15.2/30	0.0.0.0/0	192.168.15.2/30	
		Interface VLAN 100	192.168.100.10/24			
		Interface VLAN 101	192.168.101.0/24			
		Interface VLAN 102	192.168.102.0/24			
		Interface VLAN 103	192.168.103.0/24			
		Interface VLAN 104	192.168.104.0/24			
		Interface VLAN 105	192.168.105.0/24			
5	DC Server	E0	192.168.100.10/24		192.168.110.1/24	Domain Controller, DNS Server, DHCP Server
6	SAN Server	E0	192.168.100.12/24			
7	IDS-IPS Server	E0	192.168.100.13/24			

Bảng 3. Bảng quy hoạch địa chỉ IP của thiết bị mạng.

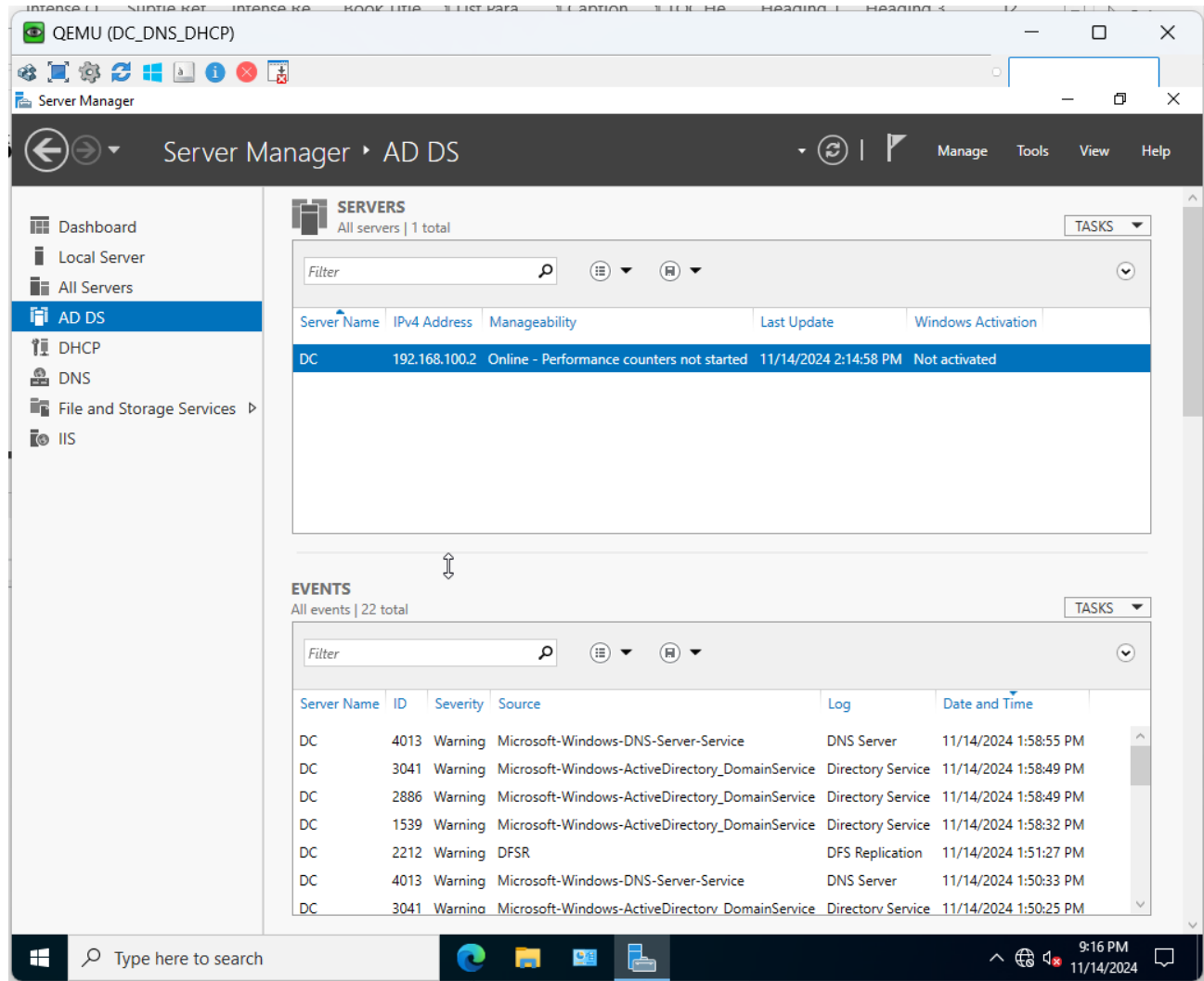
Sau những dự kiến và kế hoạch tham khảo trên của chúng em, cũng như tìm hiểu và khảo sát qua phần lý thuyết, chúng em được sự hướng dẫn của thầy Đỗ Phi Hưng triển khai và thực hiện dự án của mình trên hệ thống giả lập EVE-NG.

2. Đánh giá và kiểm chứng kế hoạch:

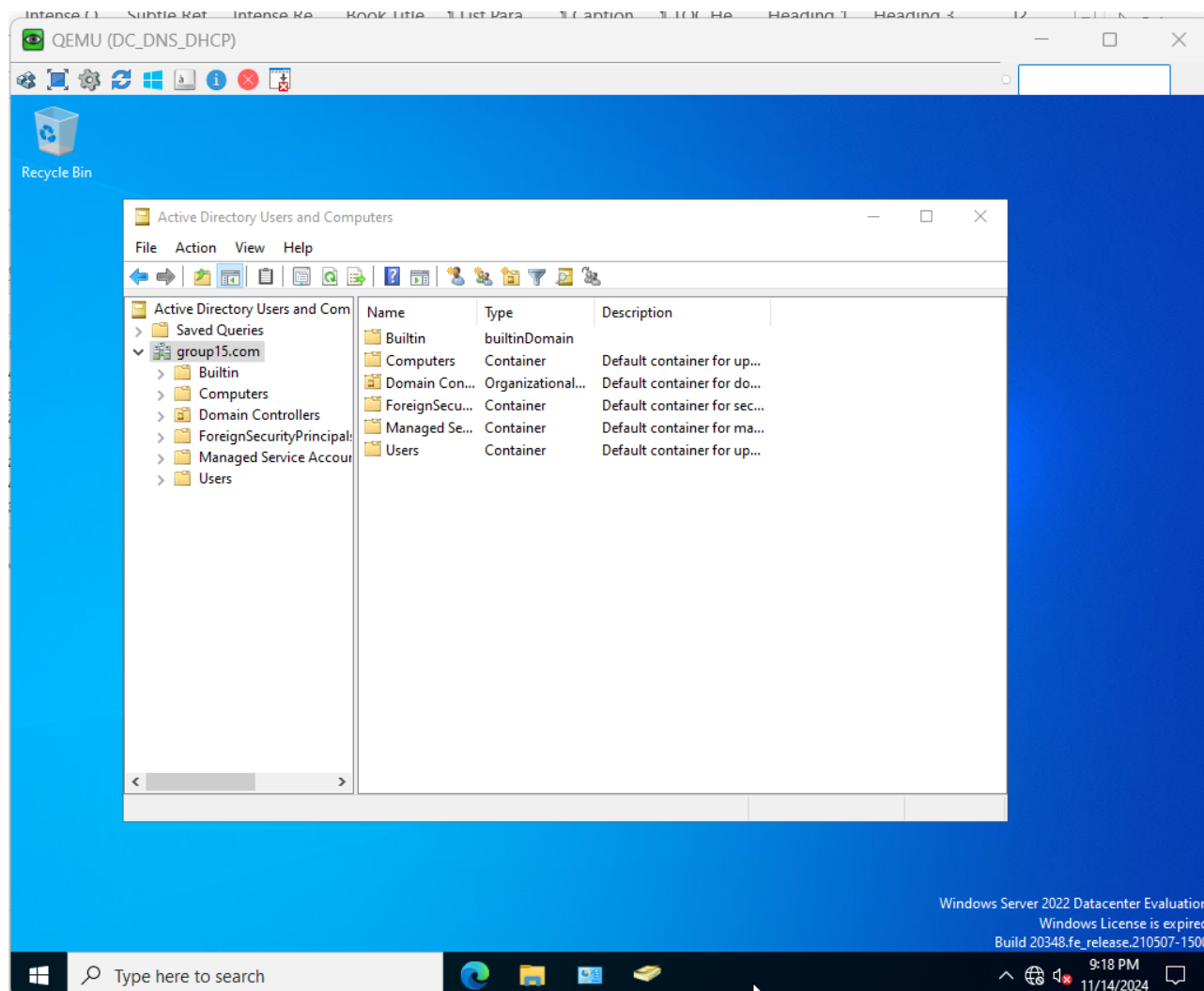
CHƯƠNG 3: TRIỂN KHAI

1. Triển khai setup hệ thống:

1.1. Domain Controller:

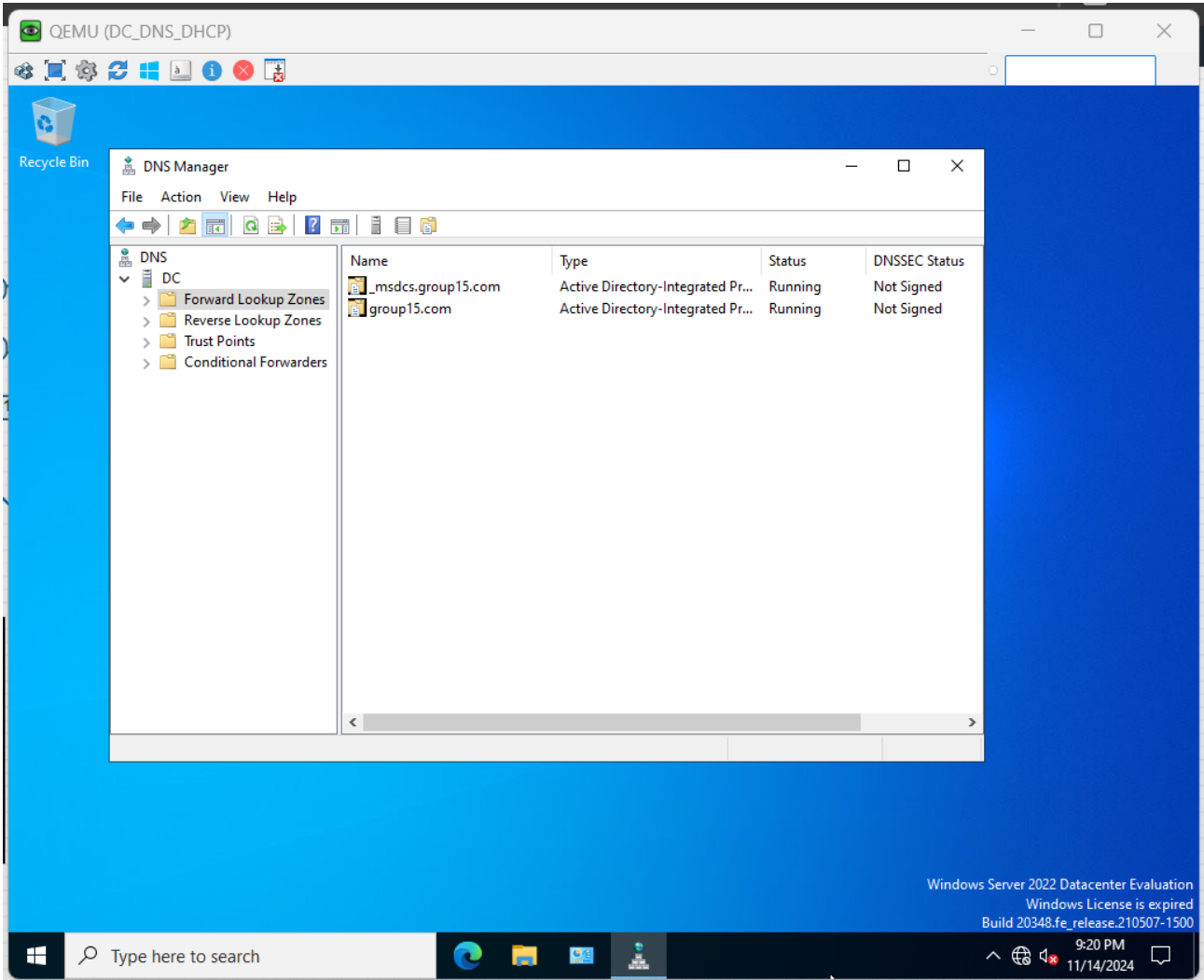


Hình 18. Domain Controller_1.



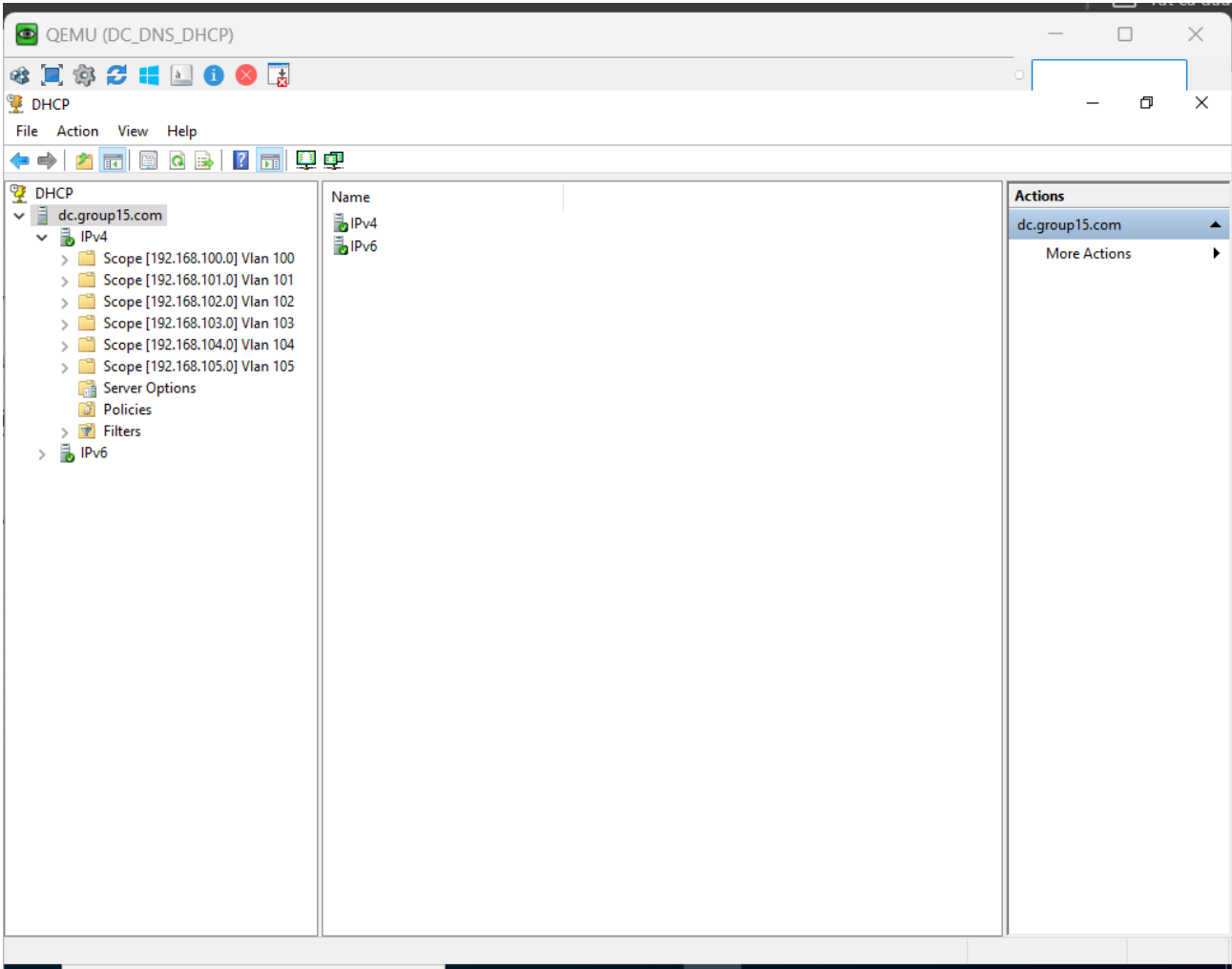
Hình 19. Domain Controller_2.

1.2. DNS:



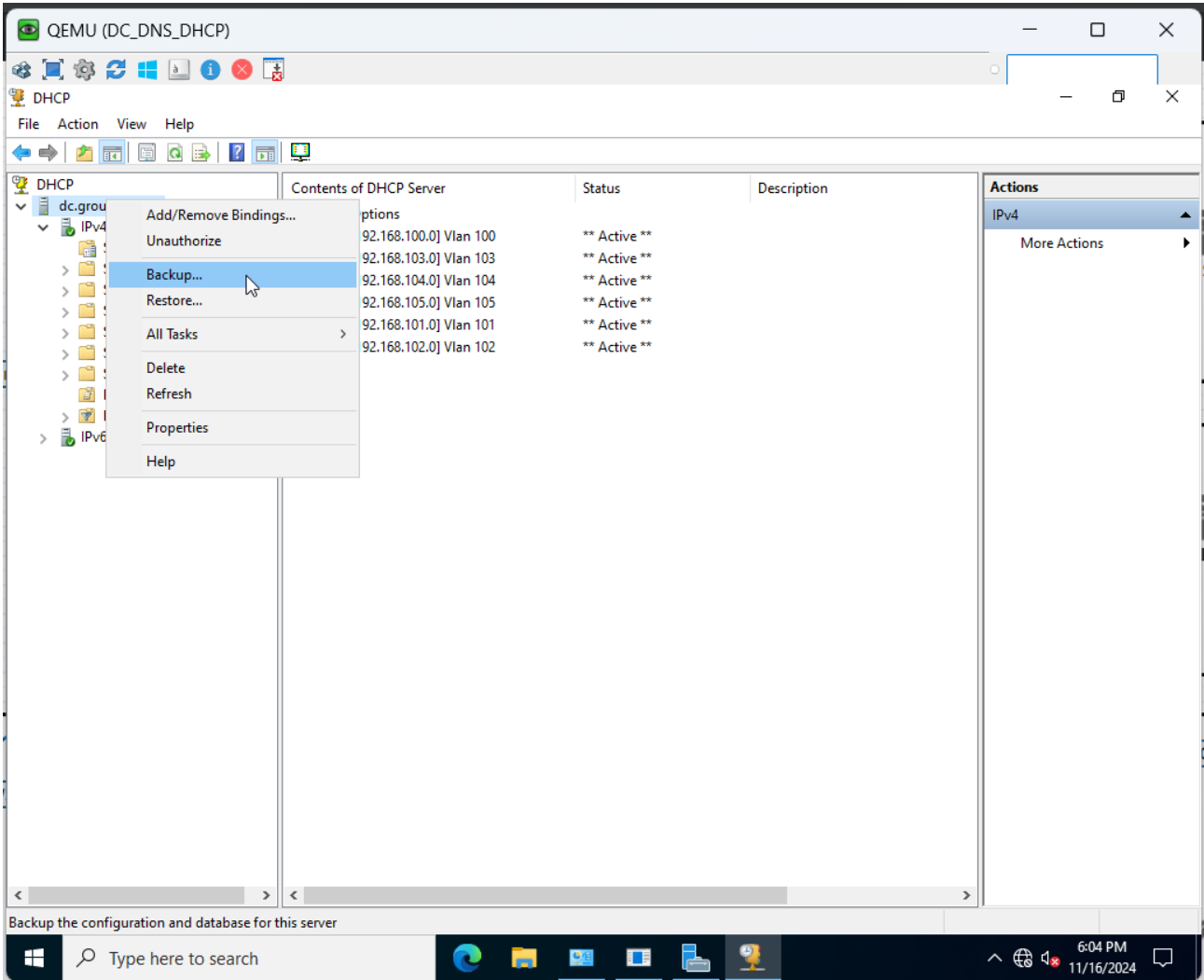
Hình 20. DNS.

1.3. DHCP:



Hình 21. DHCP server.

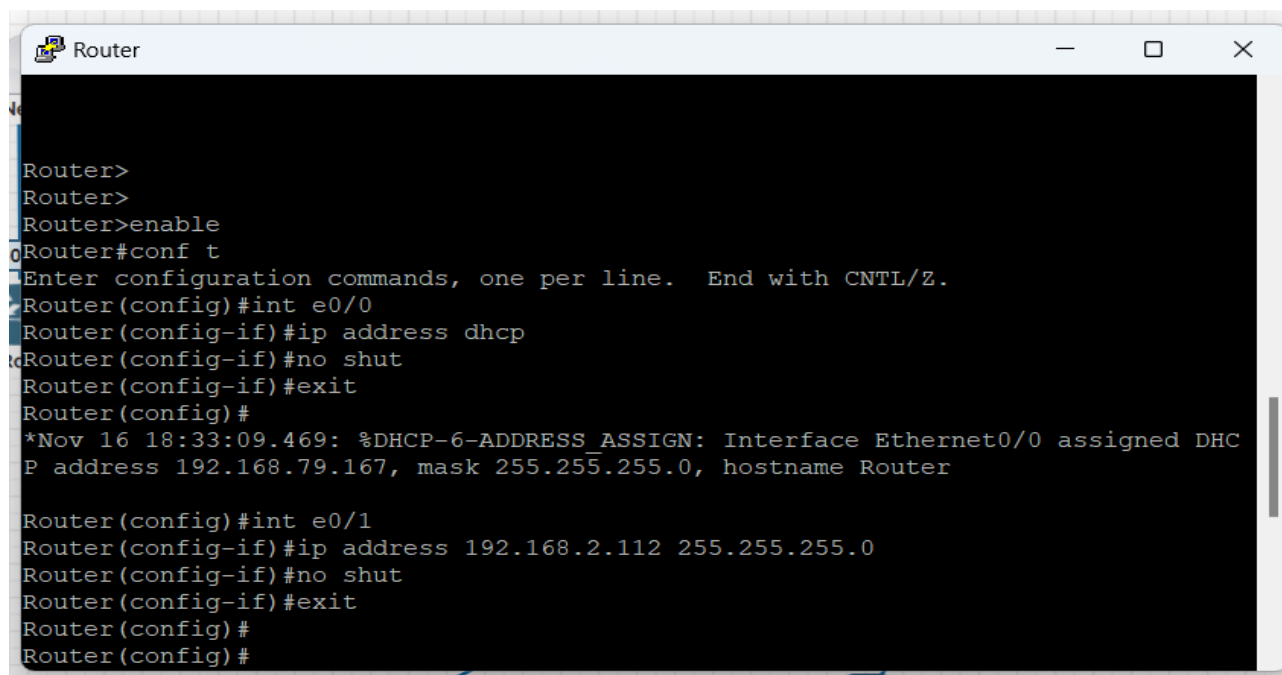
1.4. Backup DHCP:



Hình 22. Backup DHCP.

2. Cấu hình và test lỗi:

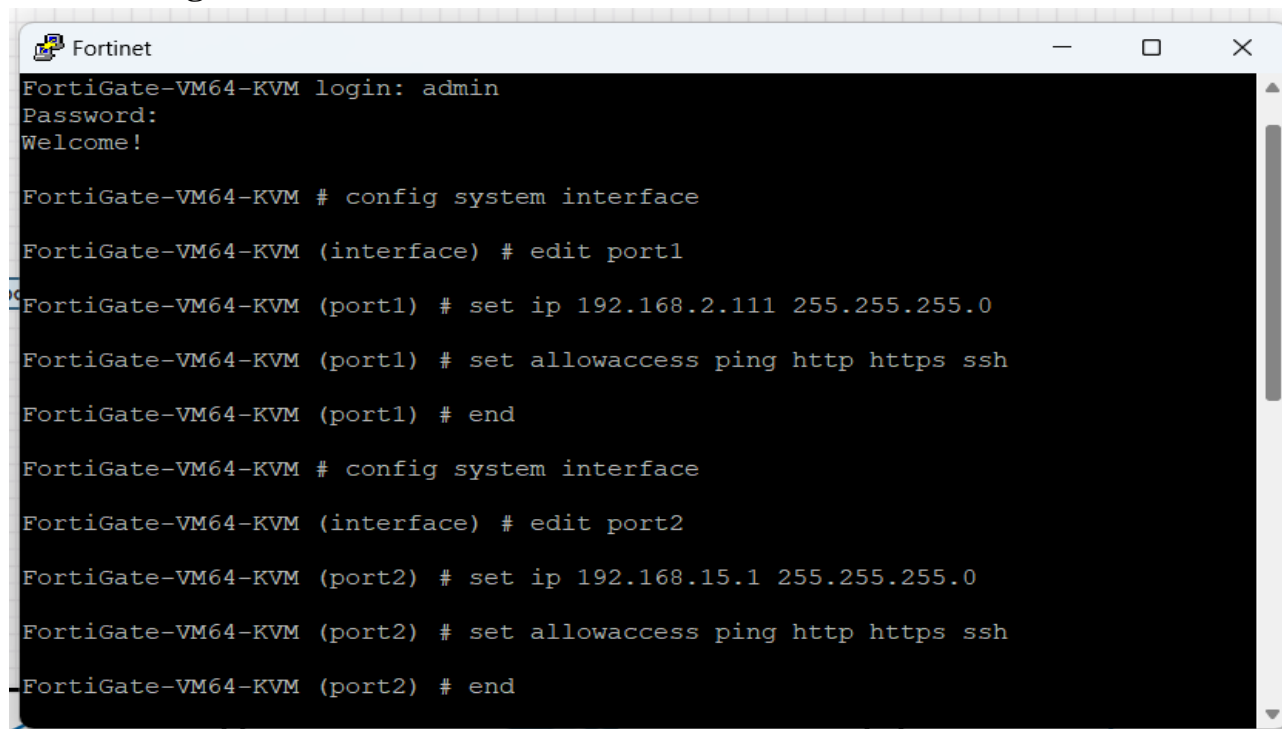
2.1. Router:

A screenshot of a terminal window titled "Router". The terminal shows a sequence of commands and their outputs. The user enters "enable" to enter privileged mode, then "conf t" to enter configuration mode. They configure interface e0/0 with DHCP and interface e0/1 with a static IP address. A system message indicates that the DHCP address 192.168.79.167 has been assigned to interface Ethernet0/0.

```
Router>
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int e0/0
Router(config-if)#ip address dhcp
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
*Nov 16 18:33:09.469: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.79.167, mask 255.255.255.0, hostname Router
Router(config)#int e0/1
Router(config-if)#ip address 192.168.2.112 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)#
```

Hình 23. Cấu hình router.

2.2. Fortigate:

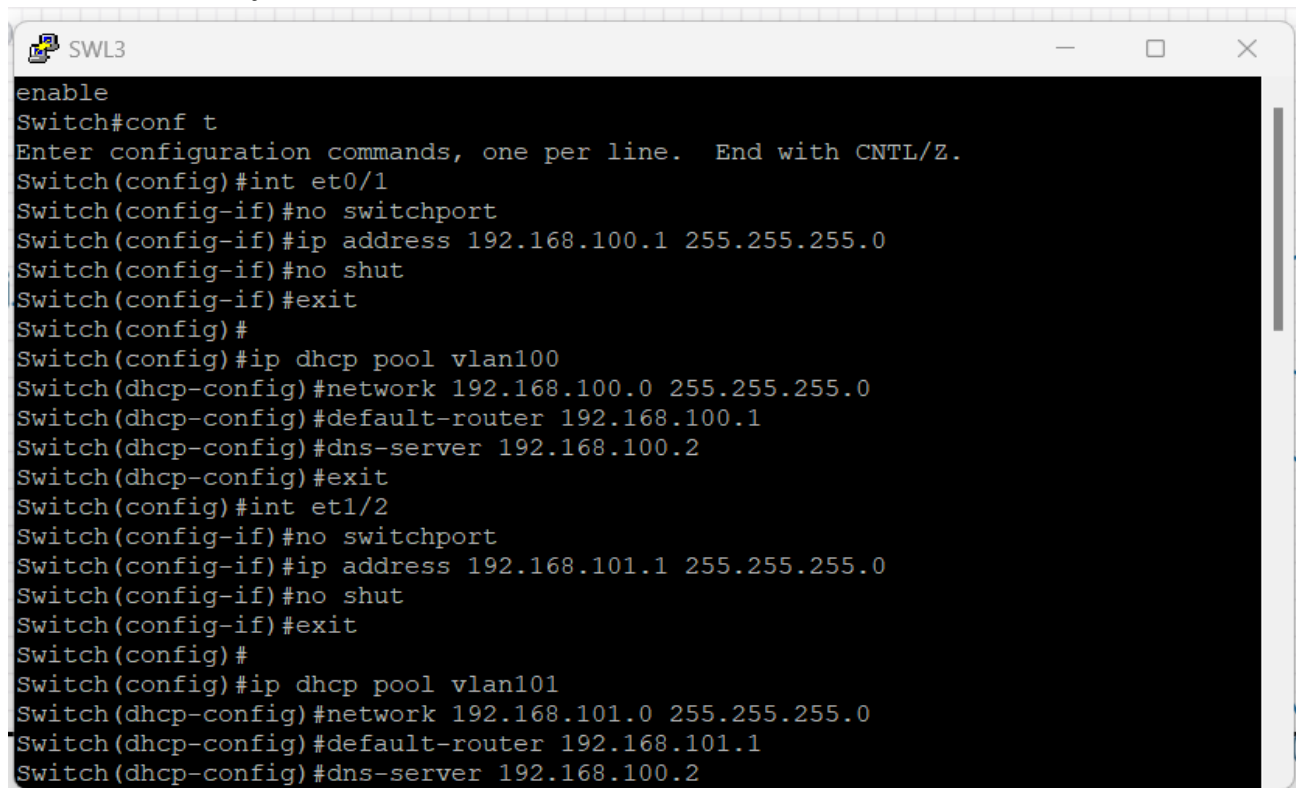
A screenshot of a terminal window titled "Fortinet". The terminal shows the login process for "FortiGate-VM64-KVM" with the username "admin". After logging in, the user enters configuration mode and configures two interfaces, port1 and port2, with static IP addresses and allows access to ping, http, https, and ssh.

```
FortiGate-VM64-KVM login: admin
Password:
Welcome!

FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set ip 192.168.2.111 255.255.255.0
FortiGate-VM64-KVM (port1) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port1) # end
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set ip 192.168.15.1 255.255.255.0
FortiGate-VM64-KVM (port2) # set allowaccess ping http https ssh
FortiGate-VM64-KVM (port2) # end
```

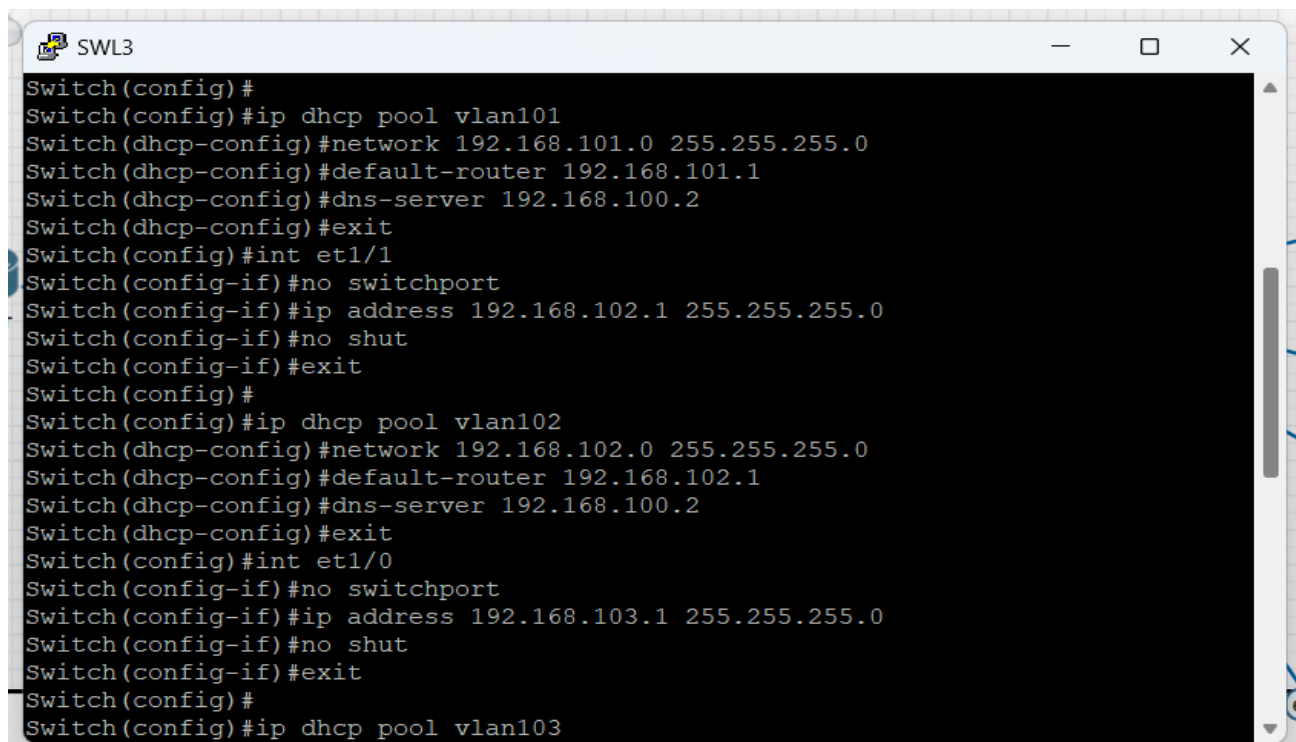
Hình 24. Cấu hình firewall fortigate.

2.3. Switch layer 3:



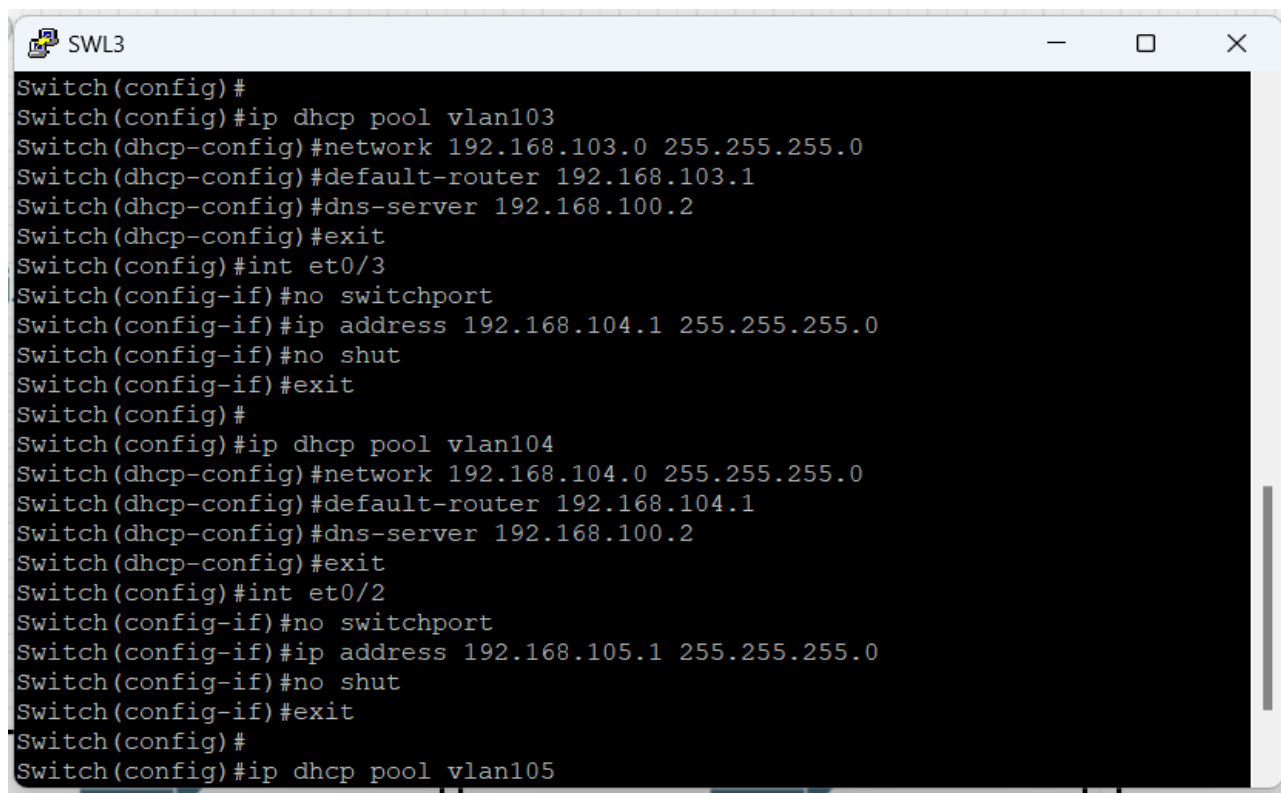
```
enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int et0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.100.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan100
Switch(dhcp-config)#network 192.168.100.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.100.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#int et1/2
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.101.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan101
Switch(dhcp-config)#network 192.168.101.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.101.1
Switch(dhcp-config)#dns-server 192.168.100.2
```

Hình 25. Cấu hình switch layer 3 1.



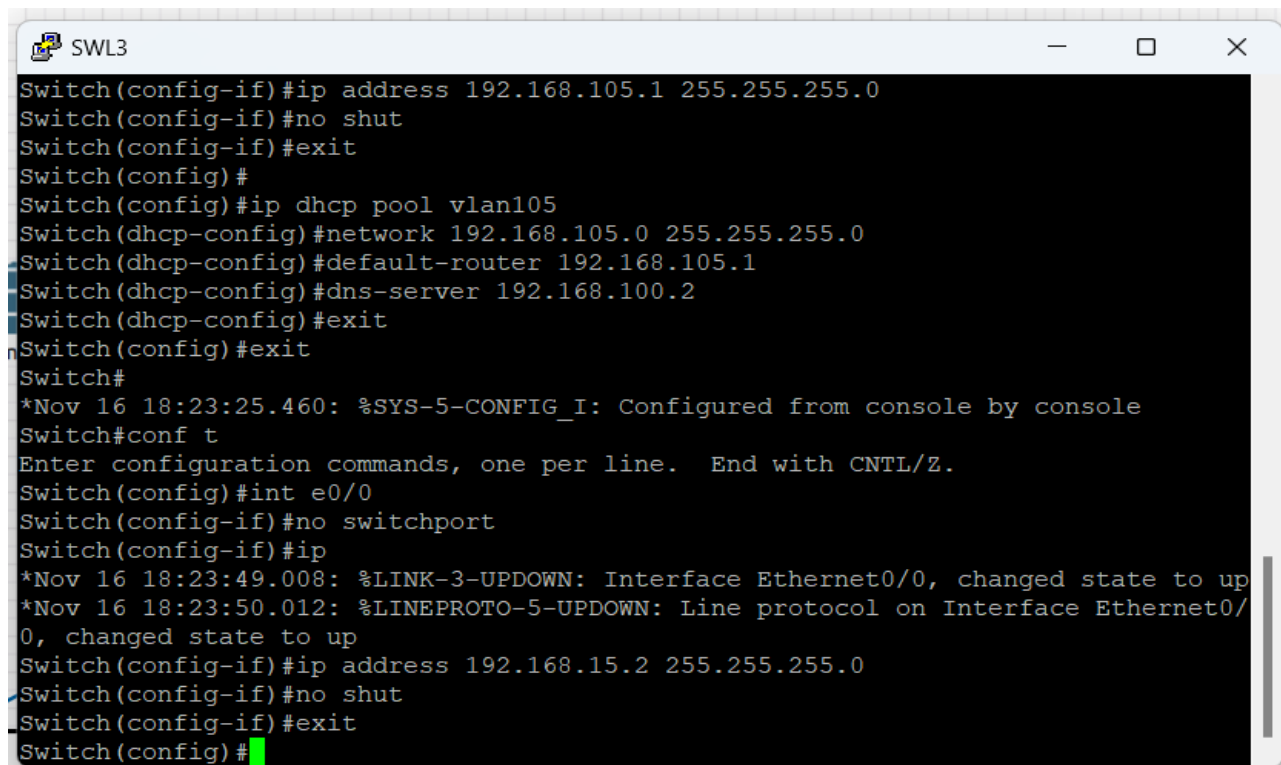
```
Switch(config)#
Switch(config)#ip dhcp pool vlan101
Switch(dhcp-config)#network 192.168.101.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.101.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#int et1/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.102.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan102
Switch(dhcp-config)#network 192.168.102.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.102.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#int et1/0
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.103.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan103
```

Hình 26. Cấu hình switch layer 3 2.



```
Switch(config)#
Switch(config)#ip dhcp pool vlan103
Switch(dhcp-config)#network 192.168.103.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.103.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#int et0/3
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.104.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan104
Switch(dhcp-config)#network 192.168.104.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.104.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#int et0/2
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.105.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan105
```

Hình 27. Cấu hình switch layer 3 3.



```
Switch(config-if)#ip address 192.168.105.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip dhcp pool vlan105
Switch(dhcp-config)#network 192.168.105.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.105.1
Switch(dhcp-config)#dns-server 192.168.100.2
Switch(dhcp-config)#exit
Switch(config)#exit
Switch#
*Nov 16 18:23:25.460: %SYS-5-CONFIG_I: Configured from console by console
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int e0/0
Switch(config-if)#no switchport
Switch(config-if)#ip
*Nov 16 18:23:49.008: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Nov 16 18:23:50.012: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch(config-if)#ip address 192.168.15.2 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
```

Hình 28. Cấu hình switch layer 3 4.

3. Đánh giá kết quả thực hiện:

3.1. Đã làm được những gì?

- Nắm vững kiến thức cơ bản về xây dựng mô hình hệ thống mạng nhỏ, cách thức hoạt động.
- Có kỹ năng thực hành công việc triển khai các dịch vụ mạng: Domain controller, DNS, DHCP server, Backup DHCP.

3.2. Chưa làm được những gì?

- Kinh nghiệm thực tế: chưa có cơ hội áp dụng kiến thức và kỹ năng trên các hệ thống phức tạp.
- Áp dụng toàn diện: chưa thể áp dụng đầy đủ các giải pháp, biện pháp trong một dự án thực tế.
- Kỹ thuật nâng cao: File store, backup, firewall, IDS, giám sát mạng.

3.3. Điểm hạn chế:

- Chưa có đủ thời gian để nghiên cứu và áp dụng các kỹ thuật nâng cao.

CHƯƠNG 4: QUẢN TRỊ HỆ THỐNG

1. Đánh giá và lựa chọn network monitoring tool (SNMP, PRTG, ...):

- PRTG Network Monitor của Paessler là một công cụ toàn diện để giám sát các thiết bị mạng, lưu lượng, hiệu suất và các ứng dụng.
- Một trong những điểm mạnh của PRTG Network Monitor là khả năng sử dụng tuyệt vời. Nó có thể được cài đặt chỉ với cài cú nhấp chuột và giống như hầu hết các công cụ chuyên nghiệp, có tính năng tự động phát hiện để quét mạng và tự động thêm các phần tử vào thiết lập giám sát. Công cụ này không chỉ đi kèm với giao diện web thân thiện với người dùng mà còn đi kèm với ứng dụng dành cho máy tính bàn cũng như dành cho các thiết bị di động. Điều này làm cho việc giám sát mạng khi đang di chuyển thuận tiện hơn.

2. Các báo cáo nhận được:

- Đánh giá các loại NOS.
- Domain Controller.
- DNS server.
- DHCP.
- Backup DHCP.
- Cấu Hình Test lỗi

CHƯƠNG 5: REFERENCES LIST

- Giáo trình, tài liệu khoa Công nghệ thông tin, Đại học Ngoại ngữ - Tin học thành phố Hồ Chí Minh.
- <https://s.net.vn/PXkg>
- <https://s.net.vn/2Y0S>
- <https://s.net.vn/LW1L>
- <https://s.net.vn/VAnK>
- <https://s.net.vn/8DjL>
- <https://s.net.vn/CMaR>
- <https://s.net.vn/lAmK>

DANH MỤC HÌNH ẢNH

Hình 1. Network Operating System.	8
Hình 2. Window Server.	9
Hình 3. Linux Server.	10
Hình 4. MacOS Server.	11
Hình 5. Cisco IOS.	12
Hình 6. So sánh các loại NOS.	13
Hình 7. Domain Controller.	14
Hình 8. Domain Name System.	15
Hình 9. Dynamic Host Configuration Protocol.	15
Hình 10. Backup.	16
Hình 11. Các hệ thống lưu trữ tập trung.	17
Hình 12. Các kiểu backup, RAID.	18
Hình 13. Các loại tường lửa.	20
Hình 14. Network Intrusion Detection System.	22
Hình 15. Network Monitoring System.	24
Hình 16. Sơ đồ vật lý.	28
Hình 17. Sơ đồ logic.	29
Hình 18. Domain Controller_1.	32
Hình 19. Domain Controller_2.	33
Hình 20. DNS.	34
Hình 21. DHCP server.	35
Hình 22. Backup DHCP.	36
Hình 23. Cấu hình router.	37
Hình 24. Cấu hình firewall fortigate.	37
Hình 25. Cấu hình switch layer 3 1.	38
Hình 26. Cấu hình switch layer 3 2.	38
Hình 27. Cấu hình switch layer 3 3.	39
Hình 28. Cấu hình switch layer 3 4.	39

DANH MỤC BẢNG BIỂU

Bảng 1. Bảng phân công công việc.	4
Bảng 2. Bảng phân hoạch IP.	30
Bảng 3. Bảng quy hoạch địa chỉ IP của thiết bị mạng.	31