

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 : Th.S.Đỗ Phi Hưng**


**Thành Viên : Nguyễn Tiến Quỳnh – 21DH112859**

**Nguyễn Lê Cang – 21DH113502**


**Lê Minh Thiện – 21DH113373**

*Tp. Hồ chí minh, Ngày 22 tháng 11 năm 2023*

## PHIẾU CHẤM ĐIỂM MÔN THI VĂN ĐÁP

 Điểm phần trình bày – Điểm hệ 10

	CBCT1	CBCT2
Họ tên CBCT	<div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div>Chữ ký: .....</div>	<div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div>Chữ ký: .....</div>
Điểm	<div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div>Bằng chữ: .....</div>	<div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 1.2em; margin-bottom: 5px;"></div> <div>Bằng chữ: .....</div>
Nhận xét	<div>1. Quyền báo cáo: .....điểm(3đ)</div> <div>2. Sơ đồ vật lý, logical, IP table: .....điểm(1đ)</div> <div>3. Dịch vụ quản trị mạng (DC,DHCP,DNS): .....điểm(2đ)</div> <div>4. File storage &amp; backup:.....điểm(2đ)</div> <div>5. Firewall: .....điểm(1đ)</div> <div>6. IDS: .....điểm(1đ)</div> <div>7. Giám sát mạng: .....điểm(1đ)</div> <div>8. Dự phòng, clustering: .....điểm(+đ)</div>	<div>1. Quyền báo cáo: .....điểm(3đ)</div> <div>2. Sơ đồ vật lý, logical, IP table: .....điểm(1đ)</div> <div>3. Dịch vụ quản trị mạng (DC,DHCP,DNS): .....điểm(2đ)</div> <div>4. File storage &amp; backup:.....điểm(2đ)</div> <div>5. Firewall: .....điểm(1đ)</div> <div>6. IDS: .....điểm(1đ)</div> <div>7. Giám sát mạng: .....điểm(1đ)</div> <div>8. Dự phòng, clustering: .....điểm(+đ)</div>

 Điểm quá trình – Điểm hệ 10

Họ tên CBCT: .....

 Điểm tổng kết: .....(Bằng chữ:.....)

## LỜI MỞ ĐẦU

Trong thời đại hiện đại, sự phát triển của công nghệ thông tin và viễn thông đang đặt ra nhiều thách thức và cơ hội mới đối với các tổ chức giáo dục trên khắp thế giới. Việc tận dụng ưu điểm của hệ thống mạng để cải thiện quy trình quản lý, giao tiếp và hỗ trợ giáo dục đã trở thành một phần quan trọng trong việc nâng cao chất lượng đào tạo và tạo ra môi trường học tập hiệu quả.

Đồ án này sẽ tập trung vào việc xây dựng hệ thống mạng cho một viện giáo dục quốc tế, nơi mà sự liên kết, giao tiếp và quản lý thông tin đóng vai trò quan trọng trong việc đáp ứng nhu cầu đa dạng của cộng đồng học thuật và hỗ trợ quá trình giảng dạy.

Chúng ta sẽ đi sâu vào các khía cạnh kỹ thuật và quản lý của hệ thống mạng, từ việc thiết kế cơ sở hạ tầng đến triển khai các giải pháp an toàn thông tin và quản lý tài nguyên mạng hiệu quả. Ngoài ra, chúng ta cũng sẽ nghiên cứu cách mà hệ thống mạng có thể hỗ trợ việc giao tiếp giữa giáo viên, học sinh và bảng quản trị, tạo điều kiện cho sự hợp tác và chia sẻ thông tin một cách linh hoạt.

Với những thách thức liên quan đến an ninh, hiệu suất và tích hợp hệ thống, đồ án này sẽ đề xuất và thảo luận về các giải pháp tiên tiến nhằm tối ưu hóa quá trình học tập và quản lý trong môi trường giáo dục quốc tế. Hy vọng rằng kết quả của đồ án sẽ mang lại những đóng góp quan trọng và giúp hiện thực hóa một hệ thống mạng đồng bộ, linh hoạt và bảo mật cho viện giáo dục của chúng ta.

Chân thành cảm ơn sự quan tâm và hỗ trợ của các bạn trong quá trình thực hiện đồ án này.

## LỜI CẢM ƠN

Chúng em xin bày tỏ lòng biết ơn sâu sắc đến Thầy Đỗ Phi Hưng, người đã đồng hành và hỗ trợ chúng em suốt quá trình thực hiện đồ án môn học "Đồ án Mạng". Sự chuyên nghiệp, tận tâm và kiến thức sâu rộng của Thầy không chỉ là nguồn động lực lớn mà còn là nguồn cảm hứng quan trọng giúp chúng em vượt qua những thử thách trong quá trình nghiên cứu và triển khai.

Chúng em trân trọng những hướng dẫn chi tiết, những ý kiến đóng góp sáng tạo và những lời khuyên quý báu mà Thầy đã chia sẻ. Nhờ có sự hỗ trợ của Thầy, chúng em đã có cơ hội học hỏi và phát triển kỹ năng một cách toàn diện trong lĩnh vực mạng.

Chúng em cũng xin bày tỏ lòng biết ơn đến sự tận tâm và giáo dục của Thầy, đã giúp chúng em hiểu rõ hơn về những vấn đề phức tạp trong xây dựng hệ thống mạng. Thầy không chỉ là người hướng dẫn mà còn là người đồng đội, luôn sẵn sàng chia sẻ kiến thức và kinh nghiệm.

Chúng em tự hào được là sinh viên của thầy và hy vọng sẽ tiếp tục học hỏi từ những kiến thức quý báu mà thầy chia sẻ. Một lần nữa, chân thành cảm ơn thầy Đỗ Phi Hưng vì những sự đóng góp lớn lao của mình trong việc truyền đạt và giảng dạy những kiến thức và kỹ năng cần thiết cho chúng em trong lĩnh vực này.

## MỤC LỤC

<b>LỜI MỞ ĐẦU .....</b>	<b>3</b>
<b>LỜI CẢM ƠN .....</b>	<b>4</b>
<b>MỤC LỤC .....</b>	<b>5</b>
<b>DOANH MỤC HÌNH ẢNH.....</b>	<b>7</b>
<b>MÔ TẢ ĐỀ TÀI.....</b>	<b>9</b>
<b>I. Network operating System: .....</b>	<b>10</b>
1. Đánh giá các loại NOS:.....	10
1.1. So sánh và đánh giá các loại NOS: .....	10
1.2. Lựa chọn NOS phù hợp với dự án: .....	11
1.3. Các dịch vụ Mạng cần triển khai:.....	11
2. Khả năng dự phòng, phục hồi hệ thống hoạt động liên tục: .....	13
2.1. Các hệ thống lưu trữ tập trung: .....	13
2.2. Các kiểu backup, Raid:.....	20
2.3. Các dịch vụ tường lửa: .....	24
2.4. Các hệ thống phát hiện xâm nhập và phần mềm:.....	26
2.5. Các hệ thống giám sát Mạng và phần mềm: .....	34
<b>II. Lên kế hoạch triển khai: .....</b>	<b>39</b>
1. Thiết kế hệ thống:.....	39
1.1. Chọn các phần mềm cần triển khai và chức năng: .....	39
1.2. Thiết bị cần có: .....	43
1.3. Logic topology: .....	44
1.4. Physical topology: .....	44
1.5. IP Table: .....	45
2. Đánh giá và kiểm chứng kế hoạch: .....	46
<b>III. Triển khai: .....</b>	<b>46</b>
1. Triển khai setup hệ thống:.....	46
1.1. Cấu hình ADDS: .....	46
1.2. Cấu hình DHCP:.....	47

1.3	Cấu hình DNS: .....	50
1.4	Backup:.....	51
1.5	Giám sát mạng:.....	53
2.	Đánh giá kết quả thực hiện: .....	57
IV.	Quản trị hệ thống:.....	57
1.	Đánh giá và lựa chọn Network monitoring tool (SNMP, PRTG...), chọn giải pháp (giám sát được lưu lượng,...):.....	57
2.	Các báo cáo nhận được: .....	58
V.	Kết luận: .....	58

## DOANH MỤC HÌNH ẢNH

Hình 1 .....	14
Hình 2 .....	16
Hình 3 .....	18
Hình 4 .....	20
Hình 5 .....	22
Hình 6 .....	25
Hình 7 .....	26
Hình 8 .....	28
Hình 9 .....	29
Hình 10 .....	30
Hình 11 .....	30
Hình 12 .....	31
Hình 13 .....	31
Hình 14 .....	32
Hình 15 .....	32
Hình 16 .....	33
Hình 17 .....	33
Hình 18 .....	35
Hình 19 .....	36
Hình 20 .....	37
Hình 21 .....	37
Hình 22 .....	44
Hình 23 .....	45
Hình 24 .....	47
Hình 25 .....	47
Hình 26 .....	48
Hình 27 .....	48
Hình 28 .....	49
Hình 29 .....	49
Hình 30 .....	50
Hình 31 .....	50
Hình 32 .....	51
Hình 33 .....	51
Hình 34 .....	52
Hình 35 .....	52
Hình 36 .....	53
Hình 37 .....	53

Hình 38 .....	54
Hình 39 .....	54
Hình 40 .....	55
Hình 41 .....	55
Hình 42 .....	56
Hình 43 .....	56
Hình 44 .....	57



## MÔ TẢ ĐỀ TÀI

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.

*You are employed as a Network Engineer by Hudo Networking Limited, a high-tech networking solution development company, which have branches in Ho Chi Minh City, Hanoi, Da Nang and Can Tho.*

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

*The company has been contracted to implement a networking project from HUFLIT educational institute. The specification of the project is given below:*

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.

*People: 400 students, 30 teachers, 20 marketing and administration staff, 5 higher managers including the head of academics and the programme manager, 3 computer network administrators.*

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 3 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.

*Resources: 50 student lab computers, 35 staff computers, 3 printers*

*Building: 3 floors, all computers and printers are on the ground floor apart from the IT labs – one lab located on the first floor and another located on the 2-3 floor*

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 3 tầng, có hệ thống tường lửa bảo mật, phát hiện xâm nhập, giám sát hệ thống Mạng.

## I. Network operating System:

### 1. Đánh giá các loại NOS:

#### 1.1. So sánh và đánh giá các loại NOS:

##### 1.1.1. Hiệu năng và ổn định:

- Windows Server: Windows Server thường được biết đến với hiệu năng và ổn định tốt, đặc biệt trong môi trường doanh nghiệp. Microsoft thường cung cấp các bản vá bảo mật và hỗ trợ dài hạn.
- Linux: Linux nổi tiếng với hiệu năng ổn định và cao cấp, đặc biệt là các phiên bản như CentOS và Ubuntu Server. Hệ điều hành này thường miễn phí và có cộng đồng hỗ trợ mạnh mẽ.
- MacOS Server: MacOS Server thích hợp cho môi trường chuyên dụng của Apple, nhưng nó không phải lựa chọn phù hợp cho hầu hết môi trường doanh nghiệp.

##### 1.1.2. Giá cả:

- Windows Server: Windows Server có giá cả cao hơn và thường đòi hỏi các giấy phép trả phí. Điều này có thể là một yếu tố quyết định đối với các doanh nghiệp có nguồn tài chính hạn chế.
- Linux: Linux thường là lựa chọn chi phí hiệu quả, với nhiều phiên bản miễn phí và các tùy chọn hỗ trợ thương mại. CentOS và Ubuntu Server đều là sự lựa chọn phổ biến và tiết kiệm chi phí.
- MacOS Server: MacOS Server có chi phí cài đặt ban đầu, và sau đó có các dịch vụ phụ phí. Điều này có thể là lựa chọn nếu tổ chức sử dụng sản phẩm và dịch vụ của Apple.

##### 1.1.3. Tích hợp ứng dụng và sự phát triển:

- Windows Server: Windows Server tích hợp tốt với các ứng dụng và dịch vụ Microsoft như Active Directory và Exchange. Microsoft cung cấp công cụ phát triển mạnh mẽ cho các ứng dụng doanh nghiệp.
- Linux: Linux là một môi trường phát triển mạnh mẽ với nhiều tùy chọn phát triển ứng dụng và tích hợp với nhiều ứng dụng mã nguồn mở.
- MacOS Server: MacOS Server được thiết kế chủ yếu cho môi trường Apple, vì vậy tích hợp tốt với các sản phẩm và dịch vụ của Apple.

##### 1.1.4. Hỗ trợ và cộng đồng:

- Windows Server: Microsoft cung cấp hỗ trợ dài hạn và có cộng đồng lớn. Tuy nhiên, hỗ trợ có thể đắt đỏ.
- Linux: Linux có cộng đồng lớn, hỗ trợ dựa trên cộng đồng, và nhiều tài liệu trực tuyến. Hỗ trợ thương mại cũng có sẵn từ các nhà cung cấp.
- MacOS Server: MacOS Server có hỗ trợ từ Apple, nhưng nó không phải là một lựa chọn phổ biến cho môi trường doanh nghiệp rộng lớn.

Tiêu chí	Windows Server	Linux	MacOS Server
Hiệu năng và ổn định	Tốt	Ổn định	Tốt
Giá cả	Cao	Thấp	Trung bình
Tích hợp ứng dụng	Tích hợp tốt với Microsoft	Tích hợp tốt với ứng dụng mã nguồn mở	Tích hợp với sản phẩm Apple
Hỗ trợ và cộng đồng	Hỗ trợ dài hạn	Cộng đồng lớn	Hỗ trợ từ Apple
Phát triển ứng dụng	Công cụ mạnh mẽ từ Microsoft	Phát triển ứng dụng đa dạng	Hạn chế cho phát triển ứng dụng
Đa nền tảng	Không	Có	Không

### 1.2. Lựa chọn NOS phù hợp với dự án:

Dựa vào các tiêu chí so sánh ở trên, Window Server là sự thích hợp, mạnh mẽ và phù hợp trong nhiều tình huống, đặc biệt là môi trường doanh nghiệp và một số lợi ích chính của việc chọn Window Server:

- **Hiệu năng và ổn định:** Windows Server thường được biết đến với hiệu năng và ổn định tốt, làm cho nó phù hợp với các môi trường doanh nghiệp đòi hỏi tính đáng tin cậy.
- **Tích hợp ứng dụng:** Windows Server tích hợp tốt với các sản phẩm và dịch vụ Microsoft phổ biến như Active Directory, Exchange, SharePoint, và nhiều ứng dụng doanh nghiệp khác. Điều này giúp bạn tối ưu hóa tích hợp và tương thích trong môi trường Microsoft.
- **Hỗ trợ và bảo mật:** Microsoft cung cấp hỗ trợ dài hạn và đảm bảo tính bảo mật cho mạng của bạn thông qua các bản vá bảo mật định kỳ. Điều này đặc biệt quan trọng trong môi trường doanh nghiệp.
- **Phát triển ứng dụng:** Windows Server cung cấp môi trường phát triển mạnh mẽ với nhiều công cụ và khung làm việc cho việc phát triển các ứng dụng doanh nghiệp.
- **Tùy chỉnh và cấu hình:** Windows Server cho phép tùy chỉnh mạnh mẽ và cấu hình linh hoạt, cho phép bạn điều chỉnh hệ thống theo nhu cầu cụ thể của dự án.

### 1.3. Các dịch vụ Mạng cần triển khai:

Dịch vụ mạng là những yếu tố quan trọng trong việc xây dựng và duy trì một hệ thống mạng hoạt động hiệu quả. Các dịch vụ mạng, bao gồm DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), và Domain Controller, đóng

vai trò quan trọng trong việc cung cấp, quản lý và bảo vệ tài nguyên mạng. Trong luận văn này, chúng ta sẽ xem xét một cách chi tiết về mỗi dịch vụ này và tại sao chúng cần được triển khai trong môi trường mạng.

#### 1.3.1. Dịch vụ DHCP (Dynamic Host Configuration Protocol):

DHCP là một dịch vụ quản lý phân phối địa chỉ IP tự động cho các thiết bị trong mạng.

Dịch vụ này giúp:

- Tối ưu hóa việc quản lý và cấu hình địa chỉ IP cho các máy tính và thiết bị mạng, ngăn tránh xung đột địa chỉ IP.
- Tiết kiệm thời gian và nguồn lực, tránh việc cấu hình thủ công địa chỉ IP trên từng thiết bị.
- Cho phép mạng mở rộng linh hoạt khi có sự gia tăng hoặc thay đổi trong cấu trúc mạng.

#### 1.3.2. Dịch vụ DNS (Domain Name System):

DNS là một hệ thống biến đổi tên miền thành địa chỉ IP và ngược lại. Dịch vụ này có ý nghĩa quan trọng vì:

- Nó giúp con người dễ dàng ghi nhớ và sử dụng tên miền thay vì phải nhớ địa chỉ IP dài và phức tạp.
- DNS làm cho việc thay đổi cấu hình mạng và di chuyển các tài nguyên mạng trở nên dễ dàng hơn, mà không cần thay đổi mãi mãi địa chỉ IP của từng thiết bị.
- Nó giúp quản lý và bảo vệ danh sách trắng và đen, đảm bảo an toàn trong mạng.

#### 1.3.3. Dịch vụ Domain Controller:

Domain Controller (DC) là máy chủ chứa thông tin xác thực và quản lý tài khoản người dùng và máy tính trong mạng. DC đóng vai trò quan trọng vì:

- Nó cung cấp xác thực cho người dùng khi họ đăng nhập vào mạng, đảm bảo tính bảo mật của hệ thống.
- DC quản lý các tài khoản, nhóm và chính sách bảo mật, giúp quản lý tài nguyên mạng dễ dàng hơn.
- Nó tạo điều kiện cho việc quản lý tập trung và tự động hóa việc triển khai và cấu hình cho các máy tính và thiết bị mạng.

#### 1.3.4. Dịch vụ Firewall:

Firewall là một thành phần quan trọng để bảo vệ mạng khỏi các mối đe dọa từ bên ngoài. Việc triển khai dịch vụ Firewall trong môi trường giáo dục quốc tế mang lại nhiều lợi ích:

- Ngăn chặn truy cập không an toàn, giúp kiểm soát và lọc lưu lượng mạng, ngăn chặn các truy cập không mong muốn và tấn công từ Internet.
- Quản lý quyền truy cập bằng cách xác định quy tắc truy cập, giúp quản lý quyền truy cập vào các tài nguyên mạng, đảm bảo tính riêng tư và an toàn.
- Bảo vệ dữ liệu quan trọng ngăn chặn sự truy cập trái phép vào các thông tin quan trọng của người dùng.

#### 1.3.5. Dịch vụ Backup and Restore:

Backup and Restore đóng vai trò quan trọng trong việc bảo vệ và phục hồi dữ liệu quan trọng.

- Bảo vệ dữ liệu, tự động sao lưu dữ liệu định kỳ, giảm thiểu rủi ro mất mát dữ liệu do sự cố hệ thống, virus hay lỗi.
- Phục hồi nhanh chóng, trong trường hợp mất dữ liệu, dịch vụ Restore giúp khôi phục lại thông tin một cách nhanh chóng, đảm bảo tiếp tục hoạt động một cách liền mạch.
- An toàn và linh hoạt, giúp duy trì ổn định và liên tục của hệ thống mạng ngay cả khi xảy ra sự cố.

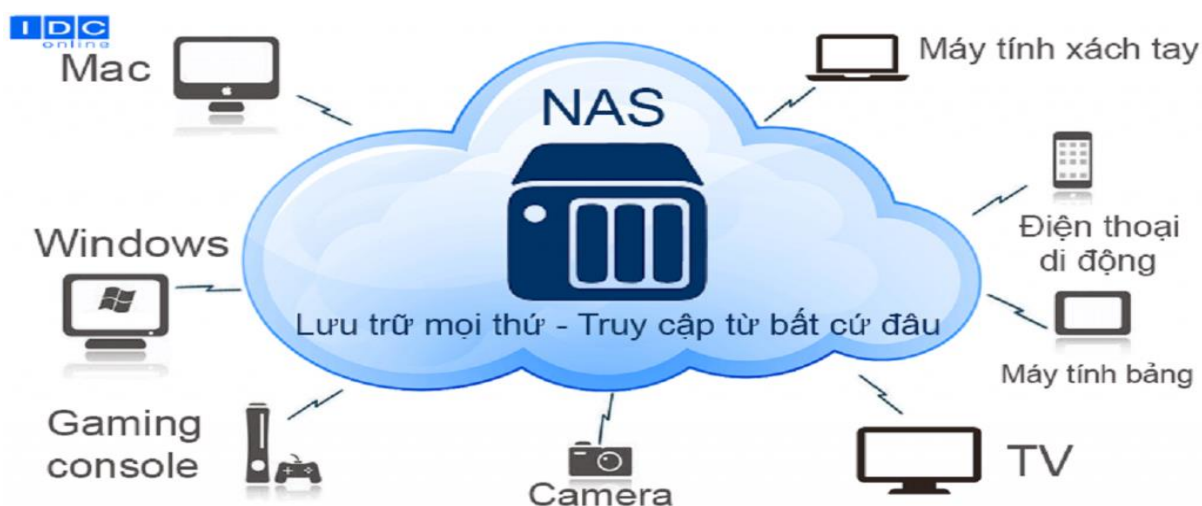
Tóm lại, trong môi trường giáo dục quốc tế, việc triển khai các dịch vụ mạng như DHCP, DNS, Domain Controller, Firewall, Backup and Restore, và IDS đóng vai trò quan trọng trong việc xây dựng một hệ thống mạng an toàn, linh hoạt và hiệu quả. Các dịch vụ này giúp tối ưu hóa quản lý mạng, bảo vệ dữ liệu, và ngăn chặn các mối đe dọa mạng. Tổng cộng, sự tích hợp này đảm bảo tính ổn định, an toàn, và liên tục của môi trường học tập và quản lý trong ngữ cảnh giáo dục đa dạng và phức tạp.

## 2. Khả năng dự phòng, phục hồi hệ thống hoạt động liên tục:

### 2.1. Các hệ thống lưu trữ tập trung:

### 2.1.1. Giải pháp lưu trữ dữ liệu theo công nghệ NAS:

Giải pháp lưu trữ dữ liệu theo công nghệ NAS là một hệ thống lưu trữ tập trung, kết nối trực tiếp với mạng LAN như một thiết bị mạng bình thường. Các thiết bị NAS cũng được gán các địa chỉ IP cố định và được người dùng truy cập thông qua sự điều khiển của máy chủ.



Hình 1

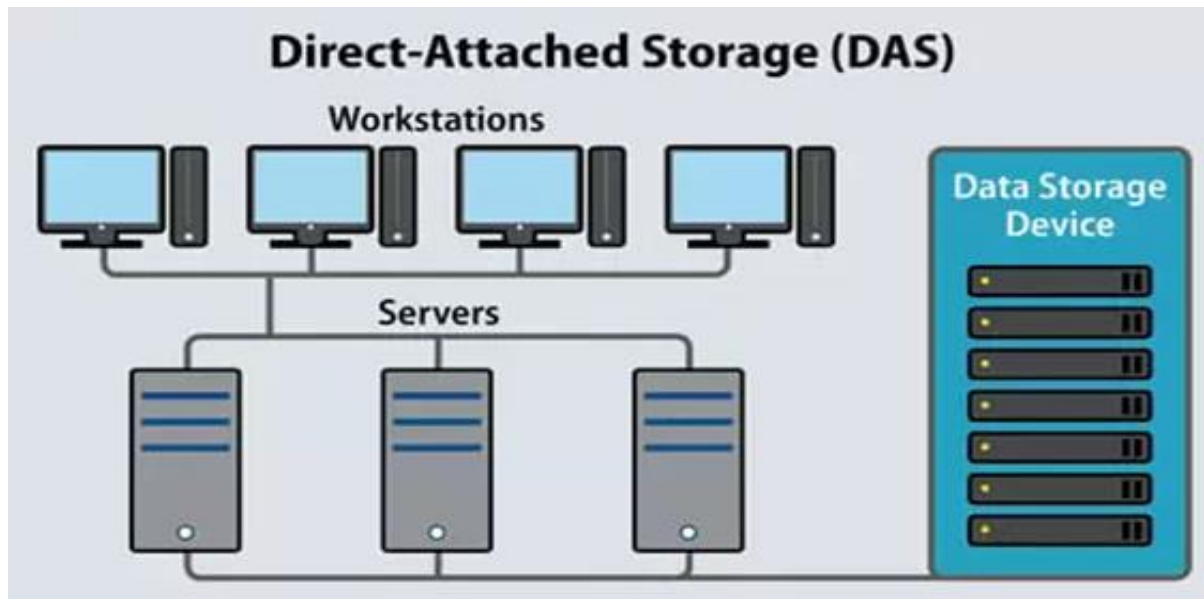
- Nas có thể cung cấp một số lợi ích cho doanh nghiệp, bao gồm:
  - Dung lượng lưu trữ lớn: NAS có thể chứa nhiều ổ đĩa cứng, cung cấp dung lượng lưu trữ lớn cho dữ liệu của doanh nghiệp.
  - Truy cập tập trung: NAS cho phép dữ liệu được truy cập trung từ bất kỳ máy tính hoặc thiết bị nào trong mạng. Điều này giúp tăng cường tính linh hoạt và năng suất.
  - Bảo mật nâng cao: NAS có thể được sử dụng để thực hiện sao lưu dữ liệu, giúp bảo vệ dữ liệu khỏi bị mất hoặc hư hỏng.
  - Chi phí hiệu quả: NAS thường có chi phí thấp hơn so với các giải pháp lưu trữ khác, chẳng hạn như SAN.
- NAS có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm:
  - Lưu trữ dữ liệu chung: NAS có thể được sử dụng để lưu trữ dữ liệu chung cho doanh nghiệp, chẳng hạn như tài liệu, hình ảnh, video và ứng dụng.
  - Sao lưu dữ liệu: NAS có thể được sử dụng để sao lưu dữ liệu từ các máy tính và thiết bị khác nhau trong mạng.
  - Chung chia dữ liệu: NAS có thể được sử dụng để chia sẻ dữ liệu giữa các nhân viên trong doanh nghiệp.
  - Máy chủ lưu trữ: NAS có thể được sử dụng để lưu trữ và chạy các ứng dụng web, ứng dụng email và các ứng dụng khác.

- Khi lựa chọn giải pháp NAS cho doanh nghiệp, cần cân nhắc các yếu tố sau:
  - Dung lượng lưu trữ: Dung lượng lưu trữ cần thiết sẽ phụ thuộc vào khối lượng dữ liệu của doanh nghiệp.
  - Tốc độ truy cập: Tốc độ truy cập cần thiết sẽ phụ thuộc vào nhu cầu sử dụng của doanh nghiệp.
  - Các tính năng: NAS có thể cung cấp một số tính năng bổ sung, chẳng hạn như sao lưu dữ liệu, máy chủ lưu trữ và chia sẻ dữ liệu.
  - Chi phí: Chi phí NAS sẽ phụ thuộc vào các tính năng và dung lượng lưu trữ.
- Dưới đây là một số thương hiệu NAS nổi tiếng trên thị trường:
  - Synology: Là một trong những thương hiệu NAS phổ biến nhất trên thế giới. Synology cung cấp nhiều dòng sản phẩm NAS đa dạng, phù hợp với nhu cầu của doanh nghiệp.
  - QNAP: Là một thương hiệu NAS nổi tiếng khác, cung cấp nhiều tính năng và giải pháp lưu trữ cho doanh nghiệp.
  - Buffalo: Là một thương hiệu NAS nổi tiếng tại Nhật Bản, cung cấp các sản phẩm NAS chất lượng cao với giá cả cạnh tranh.
  - Netgear: Là một thương hiệu NAS nổi tiếng tại Mỹ, cung cấp các sản phẩm NAS dễ sử dụng và có nhiều tính năng bổ sung.
  - Western Digital: Là một thương hiệu NAS nổi tiếng, cung cấp các sản phẩm NAS sử dụng ổ đĩa cứng của Western Digital.

NAS là một giải pháp lưu trữ dữ liệu hiệu quả và linh hoạt, có thể đáp ứng nhiều nhu cầu của doanh nghiệp.

#### 2.1.2. Giải pháp lưu trữ dữ liệu truyền thống – DAS:

DAS là viết tắt của Direct Attached Storage, là một giải pháp lưu trữ dữ liệu truyền thống, trong đó các thiết bị lưu trữ được gắn trực tiếp vào máy chủ. DAS là công nghệ lưu trữ lâu đời nhất và vẫn được sử dụng rộng rãi trong các doanh nghiệp nhỏ và doanh nghiệp vừa và nhỏ (SMB).



Hình 2

- DAS có một số ưu điểm như:
  - Dễ dàng thiết lập và quản lý: DAS rất dễ thiết lập và quản lý, ngay cả đối với người dùng không chuyên.
  - Chi phí thấp: DAS thường có chi phí thấp hơn so với các giải pháp lưu trữ khác, chẳng hạn như SAN.
  - Tốc độ truy cập cao: DAS có thể cung cấp tốc độ truy cập cao cho các ứng dụng đòi hỏi hiệu suất cao.
- Tuy nhiên, DAS cũng có một số nhược điểm như:
  - Khả năng mở rộng hạn chế: DAS có khả năng mở rộng hạn chế, vì các thiết bị lưu trữ được gắn trực tiếp vào máy chủ.
  - Hiệu quả năng lượng thấp: DAS có thể có hiệu quả năng lượng thấp, vì các thiết bị lưu trữ luôn được bật nguồn.
  - An ninh kém: DAS có thể có tính bảo mật kém, vì các thiết bị lưu trữ không được tách biệt khỏi mạng.
- DAS thường được sử dụng cho các ứng dụng sau:
  - Lưu trữ dữ liệu ứng dụng: DAS có thể được sử dụng để lưu trữ dữ liệu ứng dụng, chẳng hạn như dữ liệu cơ sở dữ liệu, dữ liệu web, và dữ liệu email.



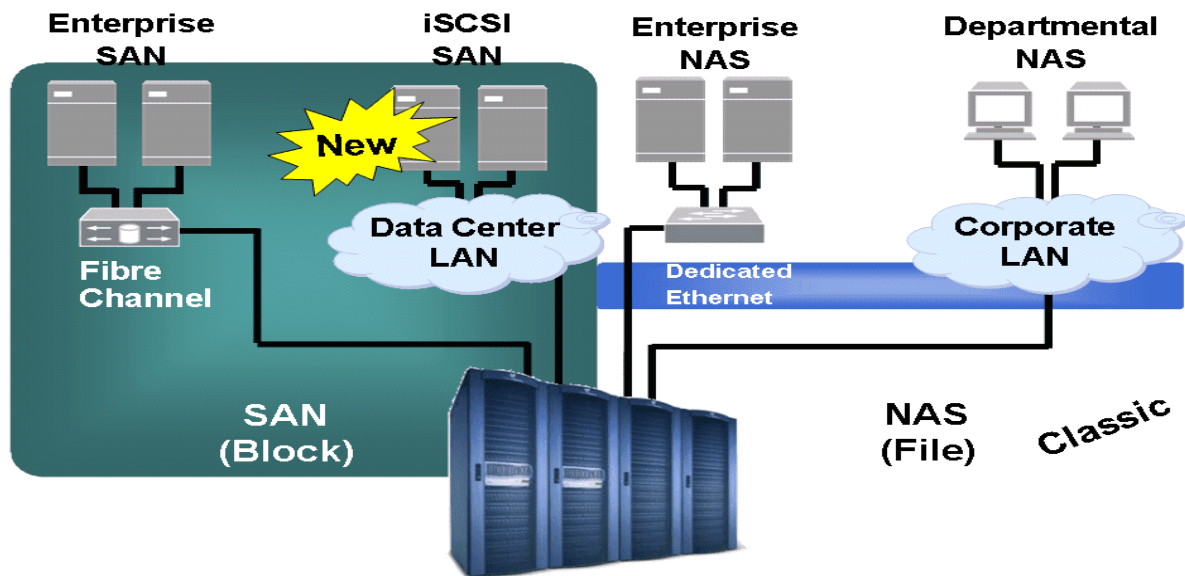
- Sao lưu dữ liệu: DAS có thể được sử dụng để sao lưu dữ liệu từ các máy tính và thiết bị khác trong mạng.
- Chung chia dữ liệu: DAS có thể được sử dụng để chia sẻ dữ liệu giữa các máy tính và thiết bị khác trong mạng.
- Khi lựa chọn giải pháp DAS cho doanh nghiệp, cần cân nhắc các yếu tố sau:
  - Dung lượng lưu trữ: Dung lượng lưu trữ cần thiết sẽ phụ thuộc vào khối lượng dữ liệu của doanh nghiệp.
  - Tốc độ truy cập: Tốc độ truy cập cần thiết sẽ phụ thuộc vào nhu cầu sử dụng của doanh nghiệp.
  - Các tính năng: DAS có thể cung cấp một số tính năng bổ sung, chẳng hạn như sao lưu dữ liệu, máy chủ lưu trữ, và chia sẻ dữ liệu.
  - Chi phí: Chi phí DAS sẽ phụ thuộc vào các tính năng và dung lượng lưu trữ.
- Dưới đây là một số thương hiệu DAS nổi tiếng trên thị trường:
  - HPE: Là một trong những nhà cung cấp giải pháp lưu trữ hàng đầu thế giới. HPE cung cấp nhiều dòng sản phẩm DAS đa dạng, phù hợp với nhu cầu của doanh nghiệp.
  - Dell EMC: Là một nhà cung cấp giải pháp lưu trữ hàng đầu thế giới khác. Dell EMC cung cấp nhiều dòng sản phẩm DAS chất lượng cao với giá cả cạnh tranh.
  - IBM: Là một nhà cung cấp giải pháp lưu trữ hàng đầu thế giới. IBM cung cấp các sản phẩm DAS hiệu quả và đáng tin cậy.
  - Western Digital: Là một nhà cung cấp ổ đĩa cứng hàng đầu thế giới. Western Digital cũng cung cấp các sản phẩm DAS sử dụng ổ đĩa cứng của Western Digital.

DAS là một giải pháp lưu trữ dữ liệu hiệu quả và đáng tin cậy, phù hợp với các doanh nghiệp có nhu cầu lưu trữ dữ liệu nhỏ và vừa.

### 2.1.3. Giải pháp lưu trữ dữ liệu tập trung SAN:

Giải pháp lưu trữ dữ liệu tập trung SAN (Storage Area Network) là một mạng riêng tốc độ cao dùng cho việc truyền dữ liệu giữa các máy chủ tham gia vào hệ thống lưu

trữ cũng như giữa các thiết bị lưu trữ với nhau. SAN cho phép thực hiện quản lý tập trung và cung cấp khả năng chia sẻ dữ liệu và tài nguyên lưu trữ.



Hình 3

- SAN có thể cung cấp một số lợi ích cho doanh nghiệp, bao gồm:
  - Tốc độ truy cập cao: SAN có thể cung cấp tốc độ truy cập cao cho các ứng dụng đòi hỏi hiệu suất cao.
  - Dung lượng lưu trữ lớn: SAN có thể chứa nhiều ổ đĩa cứng, cung cấp dung lượng lưu trữ lớn cho dữ liệu của doanh nghiệp.
  - Truy cập tập trung: SAN cho phép dữ liệu được truy cập tập trung từ bất kỳ máy tính hoặc thiết bị nào trong mạng. Điều này giúp tăng cường tính linh hoạt và năng suất.
  - Bảo mật nâng cao: SAN có thể được sử dụng để thực hiện sao lưu dữ liệu, giúp bảo vệ dữ liệu khỏi bị mất hoặc hư hỏng.
  - Khả năng mở rộng cao: SAN có khả năng mở rộng cao, có thể đáp ứng nhu cầu lưu trữ ngày càng tăng của doanh nghiệp.
- SAN thường được sử dụng cho các ứng dụng sau:
  - Lưu trữ dữ liệu ứng dụng: SAN có thể được sử dụng để lưu trữ dữ liệu ứng dụng, chẳng hạn như dữ liệu cơ sở dữ liệu, dữ liệu web, và dữ liệu email.

- Sao lưu dữ liệu: SAN có thể được sử dụng để sao lưu dữ liệu từ các máy tính và thiết bị khác trong mạng.
  - Chung chia dữ liệu: SAN có thể được sử dụng để chia sẻ dữ liệu giữa các máy tính và thiết bị khác trong mạng.
  - Máy chủ lưu trữ: SAN có thể được sử dụng để lưu trữ và chạy các ứng dụng web, ứng dụng email, và các ứng dụng khác.
- Khi lựa chọn giải pháp SAN cho doanh nghiệp, cần cân nhắc các yếu tố sau:
- Dung lượng lưu trữ: Dung lượng lưu trữ cần thiết sẽ phụ thuộc vào khối lượng dữ liệu của doanh nghiệp.
  - Tốc độ truy cập: Tốc độ truy cập cần thiết sẽ phụ thuộc vào nhu cầu sử dụng của doanh nghiệp.
  - Các tính năng: SAN có thể cung cấp một số tính năng bổ sung, chẳng hạn như sao lưu dữ liệu, máy chủ lưu trữ, và chia sẻ dữ liệu.
  - Chi phí: Chi phí SAN sẽ phụ thuộc vào các tính năng và dung lượng lưu trữ.

Dưới đây là một số thương hiệu SAN nổi tiếng trên thị trường:

- HPE: Là một trong những nhà cung cấp giải pháp lưu trữ hàng đầu thế giới. HPE cung cấp nhiều dòng sản phẩm SAN đa dạng, phù hợp với nhu cầu của doanh nghiệp.
- Dell EMC: Là một nhà cung cấp giải pháp lưu trữ hàng đầu thế giới khác. Dell EMC cung cấp nhiều dòng sản phẩm SAN chất lượng cao với giá cả cạnh tranh.
- IBM: Là một nhà cung cấp giải pháp lưu trữ hàng đầu thế giới. IBM cung cấp các sản phẩm SAN hiệu quả và đáng tin cậy.
- Lenovo: Là một nhà cung cấp giải pháp lưu trữ hàng đầu thế giới. Lenovo cung cấp các sản phẩm SAN giá cả phải chăng và dễ sử dụng.
- Western Digital: Là một nhà cung cấp ổ đĩa cứng hàng đầu thế giới. Western Digital cũng cung cấp các sản phẩm SAN sử dụng ổ đĩa cứng của Western Digital.

SAN là một giải pháp lưu trữ dữ liệu hiệu quả và linh hoạt, có thể đáp ứng nhiều nhu cầu của doanh nghiệp.

## 2.2. Các kiểu backup, Raid:

### 2.2.1. Raid là gì:

Raid (Redundant Array of Independent Disks) là một kỹ thuật lưu trữ dữ liệu trên nhiều ổ đĩa cứng để tăng cường khả năng bảo mật và hiệu suất của hệ thống lưu trữ. RAID có nhiều cấp độ khác nhau, mỗi cấp độ có những ưu điểm và nhược điểm riêng.



Hình 4

#### - Một số cấp độ Raid phổ biến:

- RAID 0: RAID 0 không có tính năng sao chép dữ liệu, thay vào đó, dữ liệu được chia thành các phân đoạn và lưu trữ trên nhiều ổ đĩa cứng. RAID 0 có tốc độ truy cập dữ liệu cao nhất, nhưng không có khả năng bảo vệ dữ liệu.
- RAID 1: RAID 1 là cấp độ RAID đơn giản nhất, dữ liệu được sao chép sang ổ đĩa cứng thứ hai. RAID 1 có khả năng bảo vệ dữ liệu cao nhất, nhưng dung lượng lưu trữ bị giảm một nửa.
- RAID 5: RAID 5 là cấp độ RAID phổ biến nhất, dữ liệu được chia thành các phân đoạn và lưu trữ trên nhiều ổ đĩa cứng. Một phân đoạn được sử dụng để lưu trữ dữ liệu parity, được sử dụng để khôi phục dữ liệu trong trường hợp một ổ đĩa cứng bị hỏng. RAID 5 có khả năng bảo vệ dữ liệu tốt và dung lượng lưu trữ không bị giảm.

- RAID 6: RAID 6 tương tự như RAID 5, nhưng sử dụng hai phân đoạn để lưu trữ dữ liệu parity, giúp tăng cường khả năng bảo vệ dữ liệu trong trường hợp hai ổ đĩa cứng bị hỏng. RAID 6 có khả năng bảo vệ dữ liệu tốt nhất, nhưng dung lượng lưu trữ bị giảm hai phần ba.
- RAID 10: RAID 10 kết hợp RAID 0 và RAID 1, dữ liệu được chia thành các phân đoạn và lưu trữ trên nhiều ổ đĩa cứng. Mỗi phân đoạn được sao chép sang một ổ đĩa cứng khác. RAID 10 có tốc độ truy cập dữ liệu cao nhất và khả năng bảo vệ dữ liệu tốt, nhưng dung lượng lưu trữ bị giảm một nửa.
- Những ưu thế của Raid:
  - Tính liên tục không bị gián đoạn trong trường hợp lỗi phần cứng: Như đã đề cập ở trên, lý do chính để sử dụng RAID là để bảo vệ dữ liệu của bạn chống lại sự cố ổ đĩa trong thời gian thực.
  - Đó là điều mà Backup không thể làm được. Nếu bạn chỉ có một ổ cứng và nó bị lỗi, bạn sẽ mất thời gian để thay thế ổ cứng đó trước khi chuyển dữ liệu đã sao lưu của mình vào đó.
  - Ngay cả khi giải pháp Backup làm giảm thời gian khôi phục xuống còn vài phút, nhưng điều mà nó không thể loại bỏ là thời gian để bạn tìm một ổ đĩa mới và cài đặt nó.
- Những bất lợi khi sử dụng Raid:
  - Chi phí: Bạn phải trả tiền cho nhiều đĩa cứng hơn. Bạn sẽ trả ít nhất gấp đôi chi phí cho RAID 1 và gấp ba chi phí cho RAID 5 - và đó là khi bạn đang sử dụng số lượng đĩa cứng tối thiểu. Và đối với RAID Cứng, bạn phải mua bộ điều khiển RAID trước khi chi tiền cho đĩa cứng đầu tiên.
  - Thảm họa từ môi trường xung quanh: RAID không bảo vệ bạn chống lại các thảm họa từ môi trường xung quanh. Nếu hỏa hoạn xảy ra trong hoặc xung quanh hệ thống máy của bạn. Xin chia buồn! Điều này cũng đúng với lũ lụt hoặc ai đó cố tình hay vô ý làm hỏng hệ thống máy tính.

- Không đề phòng lỗi do con người thao tác: thiết lập RAID chỉ có nghĩa là nó sao chép dữ liệu trên các đĩa cứng. Nói một cách đơn giản - nếu bạn vô tình ghi đè lên dữ liệu bằng một dữ liệu khác, thiết lập RAID cũng sẽ ghi đè dữ liệu đó.
- Bị nhiễm Vi-rút: Nếu bạn bị dính phần mềm độc hại hoặc vi-rút, RAID hoàn toàn không làm gì để ngăn chặn điều này.
- SPOF[4]: Nếu xảy ra hiện tượng tăng điện áp đủ lớn, nó sẽ làm cháy tất cả các đĩa trong RAID.
- Trộm cắp: Nếu ai đó vào và nhìn thấy ổ RAID của bạn, họ sẽ không ăn trộm chỉ một đĩa cứng mà họ sẽ ăn cắp toàn bộ.
- Raid thì rất khó để giải thích với mọi người: Việc giải thích cho bất kỳ ai - dù là khách hàng hay sếp của bạn về “RAID là gì?”, “Dự phòng là gì?” và “Tại sao những điều này lại quan trọng?” thường là một trận chiến khó khăn.

### 2.2.2. Backups là gì:

Backup dữ liệu là một quá trình sao chép dữ liệu từ một vị trí sang vị trí khác nhằm mục đích bảo vệ dữ liệu khỏi bị mất hoặc hư hỏng. Backup dữ liệu có thể được thực hiện theo nhiều cách khác nhau, tùy thuộc vào nhu cầu và khả năng của doanh nghiệp.



Hình 5

- Các kiểu backup dữ liệu Dưới đây là một số kiểu backup dữ liệu phổ biến:
  - Backup cục bộ: Backup dữ liệu được lưu trữ trên một thiết bị lưu trữ cục bộ, chẳng hạn như ổ cứng gắn ngoài, ổ cứng di động, hoặc thiết bị NAS. Backup

cục bộ là cách backup dữ liệu đơn giản và dễ thực hiện nhất, nhưng có khả năng bảo vệ dữ liệu thấp nhất.

- Backup đám mây: Backup dữ liệu được lưu trữ trên một máy chủ đám mây. Backup đám mây là cách backup dữ liệu an toàn nhất, nhưng có chi phí cao hơn so với backup cục bộ.
  - Backup theo thời gian thực: Backup dữ liệu được thực hiện liên tục trong thời gian thực. Backup theo thời gian thực là cách bảo vệ dữ liệu tốt nhất, nhưng có chi phí cao nhất.
  - Backup theo lịch trình: Backup dữ liệu được thực hiện theo một lịch trình xác định, chẳng hạn như hàng ngày, hàng tuần, hoặc hàng tháng. Backup theo lịch trình là cách backup dữ liệu phổ biến nhất, cân bằng được giữa chi phí và khả năng bảo vệ dữ liệu.
- Những ưu thế của Backup:
- Bảo vệ bạn khỏi những thứ RAID không thể: Miễn là bạn đã có một kế hoạch tốt, Backup sẽ bảo vệ dữ liệu của bạn chống lại toàn bộ thảm họa tự nhiên (Hỏa hoạn, lũ lụt), hỏng dữ liệu, phần mềm độc hại, vi rút, trộm cắp, phá hoại và lỗi của người dùng.
  - Khôi phục dữ liệu cũ hơn: Đây có lẽ là lợi ích quan trọng nhất của giải pháp Backup. Với Backup, bạn có thể sao lưu dữ liệu của mình vào bất kỳ ngày nào bạn tạo bản sao, cho phép bạn khôi phục dữ liệu tại các thời điểm cũ hơn. Trong khi đó, RAID chỉ cung cấp khả năng bảo vệ hạn chế cho dữ liệu hiện tại của bạn.
  - Rẻ hơn: Việc mua và thiết lập một số phần mềm sao lưu không tốn nhiều chi phí như RAID và giá trị đồng tiền của bạn cao hơn nhiều.
  - Ít phức tạp hơn: Bạn không cần phải biết nhiều khi nói đến phần mềm sao lưu - dành cho mọi trình độ thông thạo kỹ thuật, cho dù bạn là người dùng gia đình hay chủ doanh nghiệp nhỏ hay chuyên gia CNTT. Và việc giải thích cho mọi

người tại sao việc sao chép dữ liệu của bạn vào một ổ đĩa lại quan trọng dễ dàng hơn nhiều so với việc giải thích các loại RAID.

- Khả năng mở rộng: Với RAID, bạn sẽ muốn có nhiều dung lượng lưu trữ trước khi bắt đầu. Đó là bởi vì việc mở rộng quy mô sẽ là một quá trình mang rủi ro không lường trước được. Nhưng với Backup, sẽ không có rủi ro khi chuyển dữ liệu hoặc có được thiết bị lưu trữ lớn hơn.
- Nó có tính di động: Bạn không thể chỉ lấy một trong các ổ RAID của mình và đi đến chỗ của bạn bè và cắm nó vào. Với Backup thì có thể làm được như vậy.

- Những bất lợi khi sử dụng Backup:

Không có tính liên tục nếu một ổ đĩa bị lỗi: Như đã nêu ở trên, bạn sử dụng RAID để đảm bảo tính liên tục của phần cứng. Nếu phần cứng đó bị lỗi và bạn đã có bản sao lưu của nó, bạn phải tìm một ổ đĩa thay thế mới để sao chép, cài đặt và sau đó chuyển dữ liệu trở lại.

## 2.3. Các dịch vụ tương lửa:

### 2.3.1. Prophaze WAF:

Prophaze WAF là máy chủ proxy chạy trên nền tảng đám mây. Dịch vụ này tạo quy trình bằng cách sử dụng AI để hoàn thiện các quy tắc bảo mật, giảm thiểu các cảnh báo sai và cấp quyền truy cập website cho người dùng. Prophaze WAF hoạt động dựa trên các container của Kubernetes, từ đó đảm bảo an toàn và khả năng mở rộng cho hệ thống.

Tính năng chính:

- Giao diện thân thiện với người dùng (GUI).
- Hệ thống phát hiện mối đe dọa dựa trên machine learning.
- Bảo vệ website khỏi tấn công DDoS, hỗ trợ vớ ảo.
- Miễn phí không giới hạn chứng chỉ SSL.
- Tích hợp WAF chỉ trong 15 phút.





Hình 6

### 2.3.2. Bizfly Cloud WAF:

Bizfly Cloud WAF là giải pháp tường lửa ứng dụng web tiên phong tại Việt Nam được Bizfly Cloud phát triển, tối ưu dành cho người dùng trong nước nhằm bảo vệ khỏi các cuộc tấn công phổ biến. Với ưu điểm vượt trội, giải pháp WAF của Bizfly Cloud đã và đang được nhiều doanh nghiệp lớn trong nước và quốc tế tin tưởng sử dụng. Dịch vụ WAF sẽ theo dõi các thông tin trao đổi thông qua giao thức HTTP/HTTPS giữa trình duyệt của người dùng và máy chủ web. Sau đó dựa trên các quy tắc bảo mật được cài đặt từ trước để phát hiện các giao thức tiêu chuẩn, dấu hiệu bất thường và lượng truy cập bất thường để ngăn chặn kịp thời các tấn công. Ngoài ra, người dùng cũng sẽ nhận được hỗ trợ trực tiếp từ các chuyên gia an ninh hàng đầu nếu có vướng mắc về kỹ thuật.

Tính năng chính:

- Bảo vệ ứng dụng web trước các tấn công phổ biến (SQL Injection, XSS, XXE,...), ngăn chặn lưu lượng truy cập trái phép.
- Đạt hiệu năng website cao nhất khi kết hợp Bizfly Cloud WAF với Bizfly Cloud CDN, mà không cần lo lắng về vấn đề bảo mật.
- Tăng năng xem chi tiết doanh mục, danh tính và các thông số khác về lưu lượng bot theo thời gian thực, giúp xác định và ngăn chặn hiệu quả lưu lượng bot xấu.
- Chống tấn công hiệu quả ở tầng ứng dụng với tính năng bảo vệ 24/7.

- Dễ dàng triển khai phòng chống tấn công, cài đặt nhanh chóng trên hệ thống ứng dụng web.

### 2.3.3. Cloudflare WAF:

Cloudflare WAF là dịch vụ tường lửa ứng dụng web giúp bảo vệ máy chủ web khỏi các cuộc tấn công DDoS. Sở hữu cơ sở dữ liệu người dùng khổng lồ, máy chủ của Cloudflare có khả năng quản lý 2.9 triệu yêu cầu mỗi giây. Ưu điểm của dịch vụ WAF này đó là khi thiết bị của một khách hàng bị tấn công thì ngay lập tức nó sẽ bị chặn khỏi tất cả các máy chủ của Cloudflare.

Tính năng chính:

- Quản lý, lưu lại log và báo cáo để cải thiện trải nghiệm người dùng.
- Hệ thống theo dõi sự cố dựa trên phân tích số liệu.
- Kiểm soát tầng ứng dụng (Application Layer) để cung cấp mức độ bảo vệ cao hơn.



Hình 7

### 2.4. Các hệ thống phát hiện xâm nhập và phần mềm:

Hệ thống phát hiện xâm nhập - IDS (Intrusion Detection Systems) là phần mềm hoặc công cụ giúp bảo mật hệ thống và cảnh báo lỗi khi có các hành vi đáng ngờ xâm nhập vào hệ thống. Mục đích chính của IDS là ngăn ngừa và phát hiện những hành động phá hoại tính bảo mật của hệ thống hoặc những hành vi như dò tìm, quét các cổng.

Phần mềm IDS cũng có thể phân biệt được đâu là những cuộc tấn công nội bộ (từ chính nhân viên trong tổ chức) hoặc từ bên ngoài (từ hacker). Trong một số trường hợp, IDS

còn có thể phản ứng lại với các traffic độc hại bằng cách chặn IP nguồn truy cập mạng. Hiện nay có rất nhiều những phần mềm bị nhầm tưởng là IDS.

Một số những thiết bị bảo mật dưới đây không phải là IDS như:

- Hệ thống ghi nhật ký mạng đây là các hệ thống giám sát traffic trong mạng được sử dụng để phát hiện lỗi hỏng đối với những cuộc tấn công từ chối dịch vụ trên mạng đang bị tắc nghẽn.
- Các công cụ đánh giá lỗi hỏng, các bộ quét bảo mật dùng để kiểm soát lỗi và lỗi hỏng trong hệ điều hành, dịch vụ mạng.
- Các phần mềm diệt virus mặc dù có những tính năng giống hệ thống phát hiện xâm nhập nhưng xét về tổng thể thì chúng không phải là IDS.
- Tường lửa: Mặc dù có nhiều tường lửa hiện được tích hợp sẵn IDS, nhưng IDS không phải là tường lửa.

Có nhiều loại IDS khác nhau, mỗi loại có một chức năng và nhiệm vụ riêng chúng bao gồm:

- NIDS: Network Intrusion Detection Systems thường được bố trí tại những điểm dễ bị tấn công trong hệ thống. NIDS được sử dụng để giám sát traffic đến và đi từ tất cả các thiết bị trên mạng. Điểm cộng lớn nhất của NIDS là có thể quét tất cả traffic inbound và outbound, nhưng việc này có thể làm giảm tốc độ chung của mạng.
- HIDS: Host Intrusion Detection Systems, hệ thống phát hiện xâm nhập này hoạt động trên tất cả các thiết bị trong hệ thống có thể kết nối Internet. HIDS chỉ giám sát các gói dữ liệu inbound và outbound từ thiết bị hoặc những hành động đáng ngờ tại cấp truy cập nội bộ.
- Signature-Based: Đây là các IDS hoạt động dựa trên chữ ký, giám sát các gói tin trên mạng tương tự như cách phần mềm diệt virus hoạt động. Tuy nhiên Signature-Based có thể không phát hiện được những mối đe dọa mới, khi chữ ký để nhận biết nó chưa được IDS cập nhật.

- **Anomaly-Based:** IDS này được sử dụng để phát hiện mối đe dọa dựa trên sự bất thường. Anomaly-Based sẽ giám sát traffic mạng và so sánh với baseline đã được thiết lập từ trước. Baseline sẽ xác định đâu là mức bình thường của mạng và cảnh báo cho quản trị viên mạng hoặc người dùng khi phát hiện traffic truy cập bất thường hoặc khác biệt so với baseline.
- **Passive:** Đây là IDS thụ động chỉ phát hiện và cảnh báo. Khi phát hiện traffic đáng ngờ hoặc độc hại, nó sẽ tạo và gửi cảnh báo đến các nhà quản trị hoặc người dùng. Những hành động sau đó sẽ phụ thuộc vào người quản trị.
- **Reactive:** Loại IDS này ngoài nhiệm vụ như IDS Passive, nó còn thực hiện những hành động đã được thiết lập sẵn để phản ứng lại các mối đe dọa một cách nhanh chóng, ví như: chặn nguồn truy cập, khóa IP.

#### 2.4.1. OSSEC:



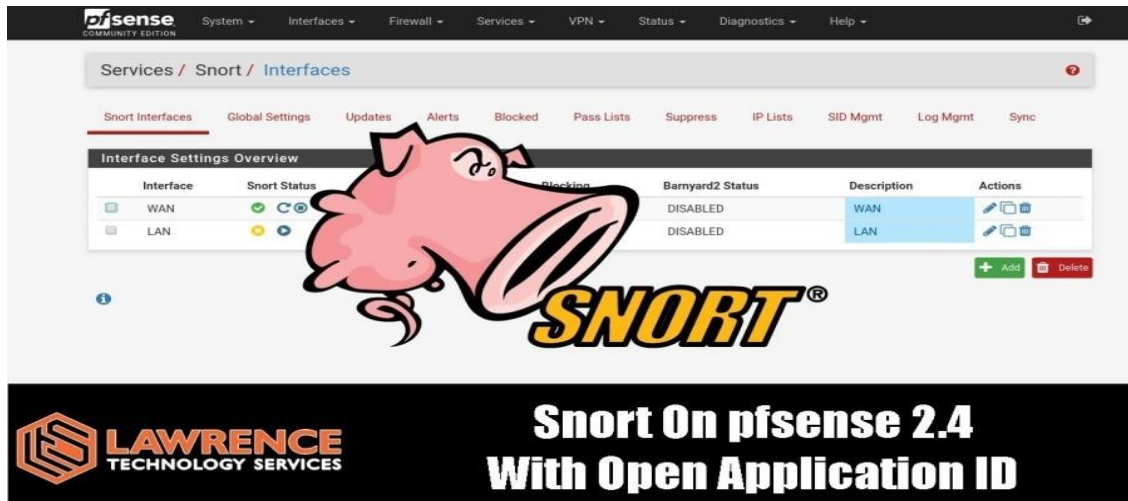
Hình 8

OSSEC là 1 HIDS (Host-based intrusion detection system-hệ thống phát hiện chống xâm nhập được cài đặt trên từng máy tính nhất định, khác với NIDS(Network intrusion detection system) được cài đặt cho toàn bộ mạng lưới. OSSEC là công cụ nguồn mở do hãng bảo mật nổi tiếng Trend Micro phát triển.

OSSEC là một sản phẩm miễn phí, được dùng để: kiểm tra tính toàn vẹn,thuộc tính,truy cập của file, ghi log, phân tích đăng nhập, giám sát chính sách (policy), phát hiện

rootkit, cảnh báo theo thời gian thực. Nó có thể chạy được trên hệ điều hành Linux, MacOS, Solaris, HP-UX, AIX và Windows.

#### 2.4.2. Snort:



Hình 9

Snort là một hệ thống phát hiện xâm nhập mạng, viết tắt là NIDS (Network intrusion detection system). Snort là một mã nguồn mở miễn phí với nhiều tính năng tuyệt vời trong việc bảo vệ hệ thống bên trong, phát hiện và ngăn chặn sự tấn công từ bên ngoài vào hệ thống.

Snort có thể phát hiện tấn công mạng trong thời gian thực, Snort cũng có thể được dùng như một chương trình bắt gói tin (sniffer packet), lưu trữ và kiểm tra logger (packet logger) hoặc xếp chúng, từ đó snort sẽ tự so sánh mỗi nguy hiểm của hiểm họa nhằm phát hiện xâm nhập.

#### 2.4.3. Bro:



Hình 10

Bro Security Network Monitor cho phép các chuyên gia bảo mật giám sát tất cả máy tính trên mạng (có thể can thiệp vào luồng dữ liệu mạng và kiểm tra các gói tin truyền trên mạng) và cho phép các nhà phân tích kiểm tra lớp ứng dụng. Ngôn ngữ kịch bản của Bro có thể dùng để tạo các chính sách giám sát cho website. Theo thông tin trên trang web của dự án, Bro được sử dụng nhiều trong môi trường khoa học như các trường đại học, viện nghiên cứu và các trung tâm điện toán.

#### 2.4.4. Suricata:



Hình 11

Suricata là giải pháp IDS/IPS mã nguồn mở hiệu quả cho các hệ thống mạng chưa được đầu tư các giải pháp IDS/IPS thương mại. Nó được xây dựng từ các thành phần khác nhau và khả năng hoạt động của nó tùy thuộc vào cách thức cấu hình, cài đặt cho hệ



thống. Ở chế độ mặc định được xem là cơ chế hoạt động tương đối tối ưu cho việc phát hiện các dạng tấn công mạng. Suricata có thể được triển khai theo 02 cơ chế: cơ chế phát hiện (IDS) và ngăn chặn(IPS).

#### 2.4.5. Security Onion:



Hình 12

Security Onion là 1 công cụ miễn phí và mã nguồn mở trên Linux để phát hiện xâm nhập, giám sát an ninh doanh nghiệp và quản lý nhật ký. Nó bao gồm Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner và nhiều công cụ bảo mật khác. Trình hướng dẫn cài đặt rất dễ sử dụng và cho phép bạn xây dựng một hệ thống quản lý bảo mật doanh nghiệp trong vài phút.

#### 2.4.6. Sagan:

Dashboard

Events

Welcome guy | Logout

Comments

Sensors

Store

< 2012

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug

Sep

Oct

Nov

Dec

2012 >

1%

TimeRange: 2012-11-13 00:00:00 until 2012-11-15 23:59:59 (+0:00)

Filtered by Object: NO

Filtered by Sensor: NO

Status: Subscribed

Tools

Event Groupings: 

on

Event Queue Only: 

on

Flag: 

off

Event Summary

Queued Events: 211

Total Events: 49542

Total Signatures: 35

Total Sources: -

Total Destinations: -

Event Count by Priority

High: 207 (36.1%)

Medium: -

Low: 4 (3.9%)

Other: -

Event Count by Classification

Admin Access: -

User Access: -

Attempted Access: -

Denial of Service: -

Policy Violation: -

Reconnaissance: -

Malware: -

No Hits

3.9%

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
4	1	1	2	23:16:57	[OPENSSH] No identification string - possible scan	5000970	6	0.008%
18	1	1	1	11:56:10	[OPENSSH] Invalid or illegal user [nacle]	5001113	6	0.037%
20	1	1	1	11:55:53	[OPENSSH] Invalid or illegal user [guest]	5001109	6	0.041%
26	1	1	1	11:54:31	[OPENSSH] Invalid or illegal user [admin]	5001107	6	0.053%
19	1	1	1	11:54:26	[OPENSSH] Invalid or illegal user [webmaster]	5001118	6	0.039%
25	1	1	1	11:54:16	[OPENSSH] Invalid or illegal user [test]	5001115	6	0.051%
17	1	1	1	11:54:15	[OPENSSH] Invalid or illegal user [postgres]	5001114	6	0.035%
15	1	1	1	11:53:36	[OPENSSH] Invalid or illegal user [info]	5001110	6	0.031%
12	1	1	1	11:52:52	[OPENSSH] Invalid or illegal user [web]	5001117	6	0.024%
19	1	1	1	11:51:43	[OPENSSH] Invalid or illegal user [user]	5001116	6	0.031%
2	1	1	1	11:06:44	[OPENSSH] Attempt to login using a denied user	5000977	6	0.004%
6	1	1	1	10:57:29	[OPENSSH] Invalid or illegal user [negate]	5001112	6	0.012%
20	1	1	1	10:20:02	[OPENSSH] Invalid or illegal user	5000922	6	0.041%
4	1	1	1	10:20:02	[OPENSSH] Invalid or illegal user [x]	5001106	6	0.008%
9	1	1	1	10:20:02	[OPENSSH] Failed password - Brute force	5001646	6	0.016%

update

Hình 13

Sagan là một host-based intrusion detection system, có thể coi Sagan như một lựa chọn thay thế cho OSSEC.

#### 2.4.7. AIDE:

```
[root@tecmint ~]# aide --check
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2017-11-29 17:38:05

Summary:
  Total number of files:      67081
  Added files:                2
  Removed files:              0
  Changed files:              0

-----
Added files:
-----
added: /etc/script.sh
added: /root/all.txt
```

Hình 14

“Advanced Intrusion Detection Environment” – Do cái tên của nó dài quá nên các nhà phát triển IDS này đã quyết định viết tắt tên thành AIDE. Đây là một HIDS tập trung vào việc phát hiện rootkit và so sánh chữ ký tập tin cho các hệ điều hành Unix và Unix-like OS , vì vậy nó cũng sẽ hoạt động trên Mac OS và Linux.

#### 2.4.8. Open WIPS-NG:

```
root@OpenWIPS:~# iwconfig
wlan0 IEEE 802.11bg ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry long limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off

lo no wireless extensions.

mon0 IEEE 802.11bg Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm
      Retry long limit:7 RTS thr:off Fragment thr:off
      Power Management:on

eth0 no wireless extensions.
```

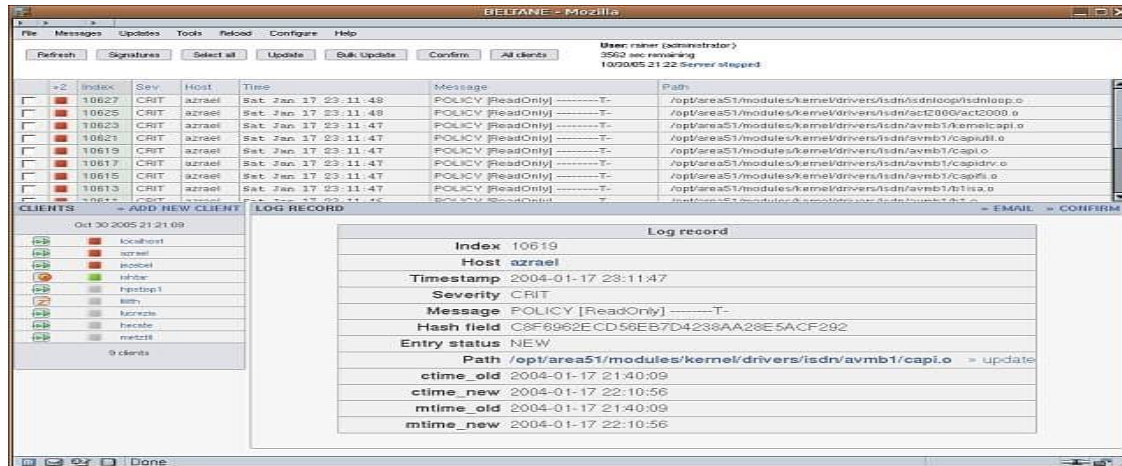
Hình 15

Nó cho phép bắt gói mạng không dây và trình bẻ khóa mật khẩu. Tuy nhiên ngược lại WIPS-NG thì được thiết kế để bảo vệ mạng không dây. Với Aircrack-NG thì người dùng có thể sử dụng ở nhiều HĐH như Linux, Windows., tuy nhiên WIPS-NG thì chỉ chạy với Linux.



WIPS là viết tắt của wireless intrusion prevention system (hệ thống phòng chống xâm nhập không dây) nên có thể hiểu WIPS-NG vừa phòng và cũng chống luôn xâm nhập cho mạng không dây.

#### 2.4.9. Samhain:



Hình 16

Samhain được sản xuất bởi Samhain Design Labs ở Đức, là một hệ thống phát hiện xâm nhập dựa trên máy chủ được sử dụng miễn phí. Nó có thể được chạy trên một máy tính duy nhất hoặc trên nhiều máy chủ, cung cấp thu thập dữ liệu tập trung trên các sự kiện được phát hiện bởi các tác nhân chạy trên mỗi máy.

#### 2.4.10.Fail2Ban:



Hình 17

Fail2Ban là một hệ thống phát hiện xâm nhập dựa trên máy chủ lưu trữ miễn phí tập trung vào việc phát hiện các sự kiện “đáng lo ngại” được ghi lại trong các tệp nhật ký, chẳng hạn như các lần đăng nhập thất bại quá mức.

Fail2Ban là một hệ thống ngăn chặn xâm nhập bởi vì nó có thể thực hiện hành động khi phát hiện hoạt động đáng ngờ và không chỉ ghi lại mà nó còn highlight các tác nhân có thể gây nguy hiểm.

## 2.5. Các hệ thống giám sát Mạng và phần mềm:

Hệ thống giám sát mạng (Network monitoring) là hệ thống giám sát các sự cố, hiệu năng, tình trạng của các thiết bị và máy tính trong hệ thống mạng. Hệ thống bao gồm một phần mềm ghi nhận thông tin và giúp người quản trị hệ thống có thể ghi nhận, theo dõi các thông tin thông qua nó.

Trong hệ thống mạng, người ta thường giám sát các thiết bị như các server, switch, router, firewall, tổng đài và điện thoại VoIP, máy in, tất cả các thiết bị có hỗ trợ giám sát.

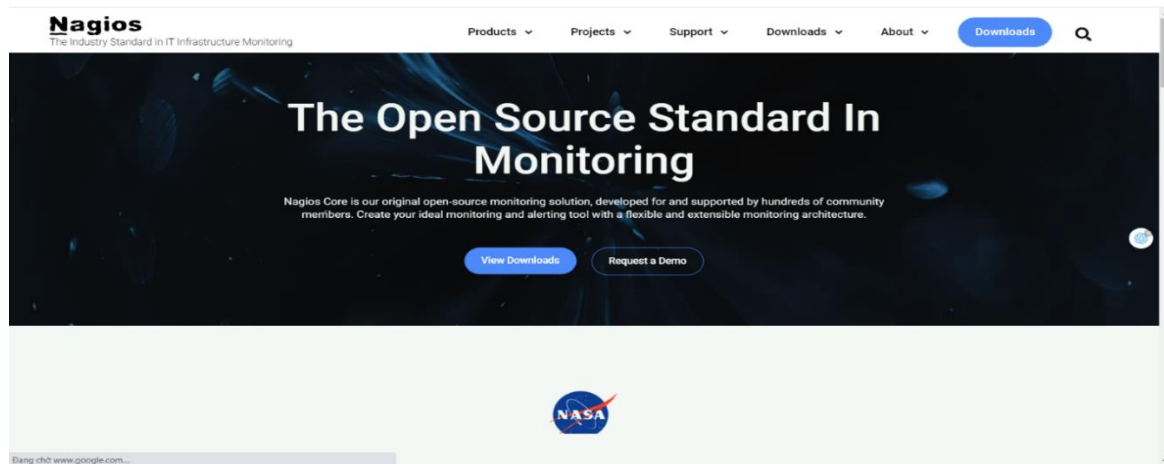
Việc giám sát sẽ thông qua các giao thức mà thiết bị hoặc hệ điều hành của nó cung cấp, một trong những giao thức quan trọng nhất và được sử dụng rộng rãi là SNMP, bên cạnh đó có rất nhiều giao thức khác như Netflow, WMI, ICMP, IPSLA...

Các phần mềm nổi tiếng để xây dựng hệ thống giám sát như PRTG Network Monitor, Zabbix, Nagios, Cacti... Ngoài ra còn có rất nhiều phần mềm miễn phí và đơn giản có thể cài vào máy tính của người quản trị, phù hợp với các môi trường nhỏ. Các thiết bị hoặc các hệ thống phần mềm, các nhà sản xuất có thể có những phần mềm giám sát riêng cùng với các giao thức riêng của nó hoặc các phần mềm phục vụ giám sát riêng lẻ cho từng dịch vụ.

### 2.5.1. Nagios:

Là một công cụ giám sát mạng mạnh mẽ. Nagios cung cấp các tính năng như cảnh báo, xử lý sự kiện và báo cáo. Nagios Core là trung tâm của các ứng dụng có chứa các công cụ giám sát cốt lõi và một giao diện web cơ bản. Chúng ta có thể thực hiện giám sát các dịch vụ, ứng dụng, và các số liệu, một lối vào lựa chọn cũng như các add-ons cho

trực quan dữ liệu, đồ thị, phân phối tải và hỗ trợ cơ sở dữ liệu MySQL, giữa những người khác.



Hình 18

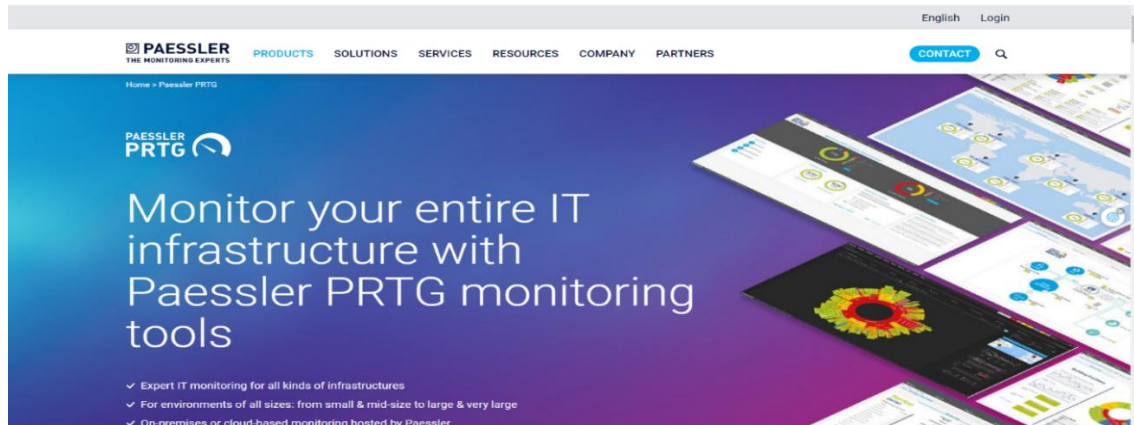
### 2.5.2. PRTG Network Monitor:

Công cụ giám sát mạng có sẵn và sử dụng một loạt các giao thức bao gồm SNMP, SSH, WMI và các luồng giao thức (Netflow, jFlow, sFlow, IPFIX).

PRTG Network Monitor là một công cụ sử dụng giao diện dựa trên web và các ứng dụng cho iOS và Android.

Tính năng chính PRTG Network Monitor bao gồm:

- Giám sát mạng toàn diện trong đó cung cấp hơn 170 loại cảm biến để theo dõi ứng dụng, theo dõi máy chủ ảo, giám sát SLA, giám sát QoS.
- Có 9 phương pháp khác nhau thông báo, cảnh báo tình trạng, cảnh báo giới hạn, cảnh báo ngưỡng, cảnh báo có điều kiện và điều độ cảnh báo.
- Có khả năng tạo ra các báo cáo trong định dạng HTML/PDF, báo cáo theo lịch trình, cũng như các báo cáo được xác định trước và báo cáo mẫu.



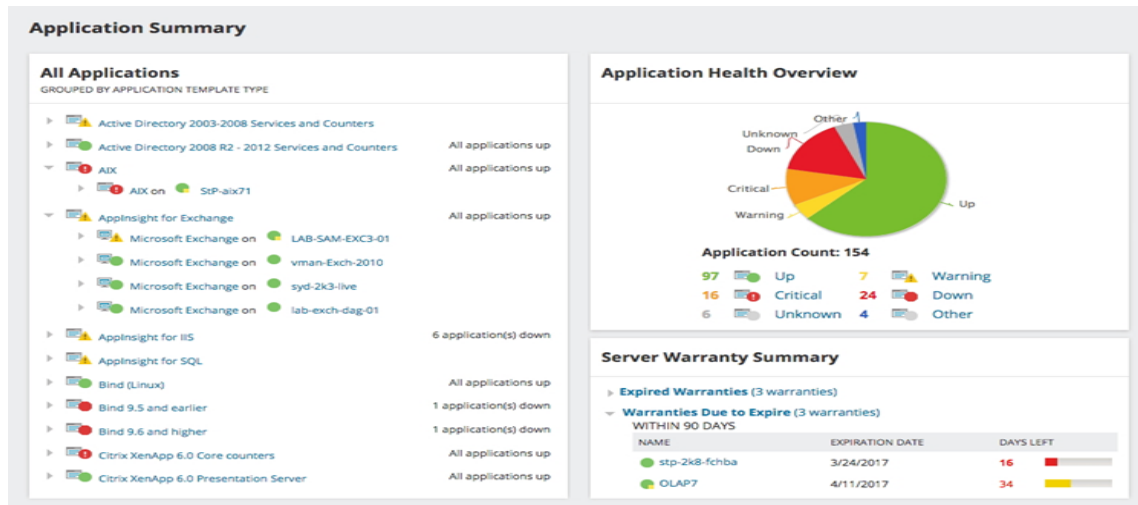
Hình 19

### 2.5.3. SolarWind Network Performance Monitor (NPM):

Là một phần của nền tảng SolarWinds Orion. Là phần mềm giám sát mạng mạnh mẽ, giá cả phải chăng giúp cho chúng ta nhanh chóng phát hiện, chẩn đoán, và giải quyết các vấn đề hiệu suất mạng, theo dõi hiệu suất của tất cả các phần tử mạng của bạn như máy chủ, thiết bị chuyên mạch và ứng dụng, cung cấp số liệu hiệu suất chi tiết để phát hiện vấn đề và giải quyết nhanh chóng. Giám sát hơn 200 ứng dụng out-of-the-box, cũng như các ứng dụng tùy chỉnh bằng cách sử dụng WMI, SNMP, CIM, JMX & VMware giao thức API.

Giống như các giải pháp giám sát mạng khác, NPM cung cấp các cảnh báo mặc định được cấu hình sẵn mà bạn có thể tùy chỉnh theo nhu cầu của mình, bao gồm các điều kiện kích hoạt cảnh báo lồng nhau để báo cáo tốt hơn. Bên cạnh tính năng lập lịch để giảm tiếng ồn cảnh báo, bạn có thể chỉ định thời gian mà các thành viên khác nhận được các thông báo khác nhau.

Với tính năng NetWork Atlas, bạn có thể tạo bản đồ tùy chỉnh thông qua kéo thả tự động tạo kết nối mạng L2 và L3 giữa các thiết bị mạng đã chọn. Công cụ trực quan hóa NetPath cho phép bạn xem các đường dẫn mà dữ liệu thực hiện trong mạng của bạn, bao gồm khả năng theo dõi từng bước nhảy.

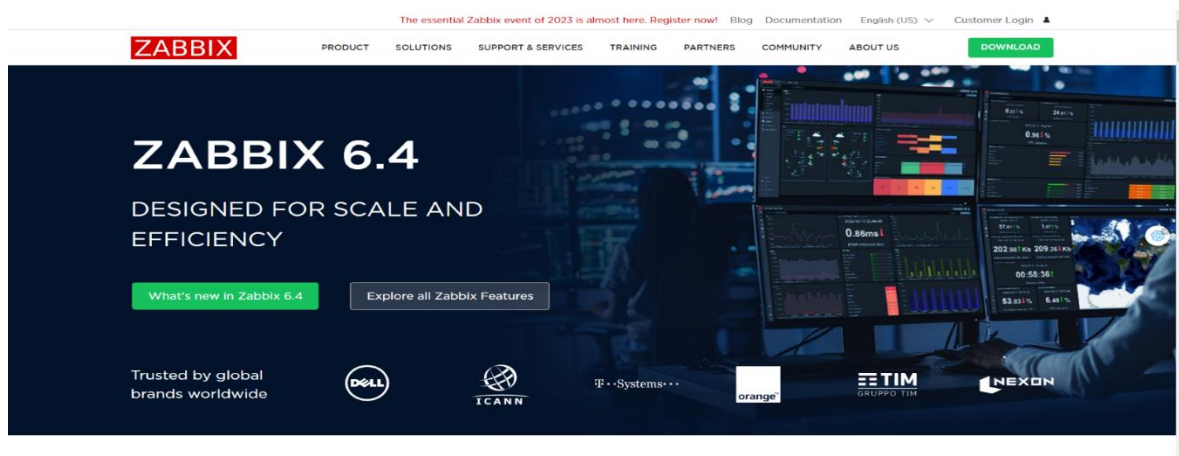


Hình 20

#### 2.5.4. Zabbix:

Công cụ này giám sát máy chủ và mạng với nhiều chức năng hữu ích. Có những Agent Zabbix cho nhiều hệ điều hành khác nhau hoặc chúng ta có thể chọn sử dụng cách kiểm tra thụ động gồm SNMP để giám sát host và các thiết bị mạng. Có chức năng thông báo và cảnh báo khi xảy ra sự cố.

Giao diện Web có thể tùy biến giúp chúng ta dễ theo dõi những thành phần mà mình quan tâm nhất. Ngoài ra, Zabbix có các chức năng đặc biệt để giám sát các ứng dụng. Zabbix cũng có thể vẽ ra các biểu đồ đa liên kết logic, liệt kê chi tiết các đối tượng được giám sát. Những biểu đồ như vậy cũng có thể tùy biến và tạo thành nhóm các thiết bị được giám sát.



Hình 21

#### 2.5.5. ISP Monitor:

Cho phép chúng ta kiểm tra tốc độ Internet. Sau khi kích hoạt ứng dụng chúng ta sẽ nhận được bảng hiển thị tốc độ đang sử dụng một cách chính xác. Đồng thời, IPS Monitor cũng cung cấp chức năng giám sát lưu lượng truy cập trong thời gian thực, việc xây dựng bảng hiển thị tốc độ mạng hiện tại thông qua 3 chế độ đồ họa khác nhau, tất cả 3 chế độ có thể được tùy chỉnh phù hợp với yêu cầu của người giám sát.

Bạn có thể chọn để cho phép ISP Monitor ngắt kết nối kết nối Internet, một khi nó đạt đến giới hạn. ISP Monitor là công cụ nhỏ gọn, giao diện đơn giản và không chứa bất kỳ phần mềm gián điệp hoặc virus, do đó chúng ta có thể hoàn toàn yên tâm sử dụng.

#### 2.5.6. Resource Monitor:

Đây là một công cụ cung cấp những thông tin chi tiết về tình trạng sử dụng tài nguyên của hệ thống. Chúng ta có thể xem toàn bộ tình trạng sử dụng của các tiến trình với CPU, ổ cứng, mạng và dung lượng bộ nhớ RAM mà hệ thống đang sử dụng. Bên cạnh việc giúp chúng ta có thể quản lý được mức độ sử dụng tài nguyên CPU và RAM của các tiến trình, Resource Monitor còn có khả năng quản lý tình trạng ổ cứng và tình trạng của mạng. Tùy vào mỗi thành phần, Resource Monitor sẽ liệt kê các tiến trình đang chạy ở bên trái.

Dựa vào đó, chúng ta sẽ biết được những tiến trình nào đang sử dụng CPU và RAM là bao nhiêu, hay là những tiến trình nào đang kết nối mạng hoặc một tiến trình nào đó đang chạy ẩn khiến ổ cứng hoạt động chậm,... Resource Monitor sẽ rất hữu ích trong việc giám sát tài nguyên hệ thống.

#### 2.5.7. System Center Operation Manager:

Là một trong những phần mềm giúp cho việc quản lý các dịch vụ đầu cuối của hãng Microsoft. SCOM hoạt động trên giao thức Simple Network Management Protocol, các phần mềm, phần cứng non-microsoft cũng có thể được quản lý bởi System Center Operations Manager.

SCOM cung cấp khả năng quản lý dịch vụ đầu cuối, dễ dàng mở rộng và tùy biến trong việc nâng cao chất lượng dịch vụ trong môi trường IT. Dưa ra hoạt động quản lý bao gồm Microsoft server, client, các nhóm ứng dụng cung cấp cho bạn kiến thức và khả

năng điều khiển giúp giám sát quản lý hệ thống hiệu quả hơn. tự động thực hiện những tác vụ và cung cấp các báo cáo kiểm tra thông minh để nâng cao hiệu quả và cho phép kiểm soát quy mô lớn hơn trong môi trường mạng.

#### 2.5.8. OpManage:

Cung cấp một số lượng lớn các màn hình hiệu suất mạng được cấu hình sẵn để triển khai và tích hợp dễ dàng hơn. Tuy nhiên, có một số tính năng không có trong Standard Edition, chẳng hạn như giám sát môi trường ảo, giám sát phân tán hoặc báo cáo. Nhiều khía cạnh khác như tường lửa hoặc giám sát lưu trữ phải được mua dưới dạng tiện ích bổ sung hoặc trình cắm thêm. Cảnh báo thời gian thực tự động thông báo cho bạn qua SMS hoặc email trong trường hợp có sự cố, các phương pháp thông báo khác nhau không khả dụng. Để trực quan hóa dữ liệu giám sát, OpManager cung cấp các trang tổng quan có cấu trúc và rõ ràng, có thể tùy chỉnh bằng cách sử dụng các tiện ích con được định cấu hình sẵn khác nhau.

## **II. Lên kế hoạch triển khai:**

### 1. Thiết kế hệ thống:

#### 1.1. Chọn các phần mềm cần triển khai và chức năng:

##### 1.1.1. Firewall:

Lựa chọn phần mềm Firewall cho doanh nghiệp:

- pfSense Firewall:
  - Chức năng chính: Bộ lọc gói, Proxy Server, VPN, IDS/ÍP, quản lý người dùng và quyền.
  - Vai trò: pfSense có thể được triển khai làm Firewall cửa ngõ, kiểm soát lưu lượng truy cập từ mạng internet và bảo vệ mạng nội bộ.
- Sophos XG Firewall:
  - Chức năng chính: Bộ lọc gói, IPS, VPN, Web Application Firewall, Sandboxing, quản lý người dùng và quyền.

- Vai trò: Sophos XG Firewall có thể được sử dụng để cải thiện bảo mật mạng nội bộ, bao gồm việc phát hiện và ngăn chặn các cuộc tấn công mạng, bảo vệ ứng dụng web và chống malware.
- Cisco Firepower:
  - Chức năng chính: Advanced Malware Protection, quản lý tập trung.
  - Vai trò: Cisco Firepower có thể được sử dụng như một hệ thống giám sát và quản lý bảo mật toàn diện, đặc biệt là để phát hiện và ngăn chặn các mối đe dọa từ malware và quản lý các thiết bị Firewall từ một nơi.

Sau một cuộc xem xét kỹ lưỡng và với sự cân nhắc, chúng tôi chọn triển khai Sophos XG Firewall cho doanh nghiệp trong đề tài yêu cầu. Dưới đây là lý do và giải thích:

### **Sophos XG Firewall**

Lý do lựa chọn: Sophos XG Firewall cung cấp một giải pháp bảo mật mạng toàn diện với nhiều tính năng bảo mật nâng cao và quản lý tập trung. Đây là một giải pháp phù hợp cho doanh nghiệp vừa và nhỏ, giúp bảo vệ mạng và dữ liệu trước các mối đe dọa hiện đại.

Chức năng chính:

- Bộ lọc gói (Packet Filtering): Cho phép tạo luật để kiểm soát lưu lượng truy cập vào và ra khỏi mạng.
- Intrusion Prevention System (IPS): Phát hiện và ngăn chặn các cuộc tấn công mạng.
- Virtual Private Network (VPN): Hỗ trợ nhiều loại VPN như SSL, VPN, Ipsec và L2TP cho phép kết nối mạng riêng ảo an toàn.
- Web Application Firewall: Bảo vệ ứng dụng web khỏi các tấn công.
- SandBoxing: Phân tích malware một cách an toàn.
- Quản lý người dùng và quyền: Cho phép quản lý tài khoản người dùng và quyền truy cập.
- Lợi ích cho doanh nghiệp 100 người dùng.



- Bảo mật mạng cao cấp: Sophos XG Firewall cung cấp nhiều tính năng bảo mật nâng cao để bảo vệ mạng khỏi các mối đe dọa hiện tại.
- Kiểm soát ứng dụng và nội dung: Doanh nghiệp có thể quản lý và kiểm soát ứng dụng và nội dung trên mạng.
- Chống malware: Giải pháp này cung cấp khả năng phát hiện và ngăn chặn malware một cách hiệu quả.
- Quản lý tập trung: Cho phép quản lý tất cả các thiết bị Firewall từ một giao diện quản lý đơn giản.

#### 1.1.2. Backup:

Chọn phần mềm triển khai:

- NAS là một giải pháp lưu trữ mạng vật lý, có thể được sử dụng để lưu trữ và sao lưu dữ liệu. Một số NAS phổ biến tại Việt Nam bao gồm Synology, QNAP, Western Digital.
- Cloud Storage là một giải pháp lưu trữ dữ liệu trên đám mây. Một số dịch vụ Cloud Storage phổ biến tại Việt Nam bao gồm Google Drive, Microsoft OneDrive, Dropbox.
- Hệ thống ảo hóa như VMware, Hyper-V, XenServer có thể được sử dụng để tạo môi trường ảo, trong đó các máy ảo chạy độc lập với nhau. Các máy ảo này có thể được sao lưu bằng các phần mềm sao lưu chuyên dụng.

Chức năng Backup:

- Backup toàn bộ là phương pháp sao lưu tất cả dữ liệu trên một máy tính hoặc hệ thống. Phương pháp này có thể được sử dụng để khôi phục dữ liệu trong trường hợp mất toàn bộ hệ thống.
- Backup theo lịch trình là phương pháp sao lưu dữ liệu theo một lịch trình định sẵn. Phương pháp này giúp đảm bảo rằng dữ liệu luôn được sao lưu thường xuyên.

- Backup theo điểm khôi phục là phương pháp sao lưu dữ liệu tại một thời điểm cụ thể. Phương pháp này giúp khôi phục dữ liệu về trạng thái trước khi xảy ra sự cố.
- Backup theo mã hóa là phương pháp mã hóa dữ liệu trước khi sao lưu. Phương pháp này giúp bảo vệ dữ liệu khỏi bị truy cập trái phép.
- Backup theo phân tán là phương pháp sao lưu dữ liệu trên nhiều vị trí lưu trữ khác nhau. Phương pháp này giúp giảm thiểu rủi ro mất dữ liệu do sự cố tại một vị trí lưu trữ.

Chọn phần mềm triển khai Backup: Sử dụng NAS Synology để lưu trữ dữ liệu và sao lưu dữ liệu. NAS Synology có nhiều mẫu mã và mức giá khác nhau, phù hợp với nhu cầu của nhiều doanh nghiệp. Phần mềm sao lưu của NAS Synology có thể sao lưu toàn bộ dữ liệu, sao lưu theo định kỳ, sao lưu theo điểm khôi phục và mã hóa dữ liệu.

#### 1.1.3. IDS:

IDS (Intrusion Detection System) là một phần mềm hoặc thiết bị phần cứng được sử dụng để giám sát và phát hiện các hoạt động không hợp lệ hoặc tấn công trong mạng máy tính. Chức năng chính của IDS là theo dõi lưu lượng mạng và các hoạt động trong mạng để phát hiện các mẫu tấn công đã biết hoặc các hoạt động bất thường có thể là dấu hiệu của tấn công.

Triển khai IDS:

- Lựa chọn phần mềm hoặc thiết bị phần cứng IDS: Có thể chọn sử dụng giải pháp IDS dựa trên phần mềm hoặc IDS dựa trên thiết bị phần cứng. Các phần mềm IDS thông thường được triển khai trên máy chủ mạng và chạy như ứng dụng độc lập. Thiết bị phần cứng IDS thường tích hợp sẵn trong một thiết bị độc lập hoặc một thành phần của firewall.
- Cấu hình IDS cho mạng cụ thể: Đặt cấu hình IDS để phát hiện các hoạt động không bình thường trong mạng cụ thể của bạn. Điều này bao gồm xác định các máy chủ, mạng con, và dịch vụ cần giám sát, cũng như thiết lập ngưỡng cảnh báo cho các sự kiện cụ thể.

- Cập nhật cơ sở dữ liệu chữ ký: IDS sử dụng cơ sở dữ liệu chữ ký để phát hiện các tấn công đã biết. Đảm bảo cơ sở dữ liệu này được cập nhật định kỳ để bảo đảm phát hiện tấn công hiệu quả. Các nhà cung cấp IDS thường cung cấp cập nhật cho cơ sở dữ liệu chữ ký này.
- Ghi lại lưu lượng mạng: IDS thường ghi lại dữ liệu lưu lượng mạng liên quan đến các sự kiện cần được kiểm tra. Điều này giúp trong việc phân tích sau khi xảy ra sự cố, xác định nguyên nhân và xác định cách cải thiện bảo mật mạng.

Chức năng của IDS:

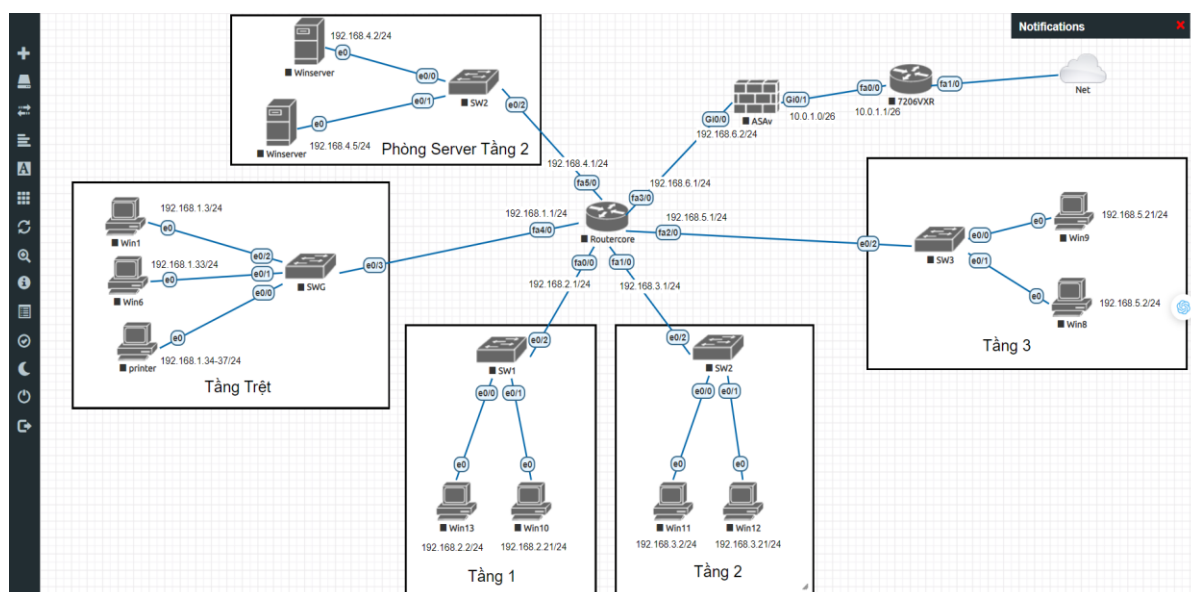
- Phát hiện tấn công đã biết: IDS sử dụng cơ sở dữ liệu chữ ký để so sánh các gói dữ liệu trong mạng với các mẫu tấn công đã biết. Nếu có sự tương quan, IDS sẽ phát hiện và báo cáo về tấn công.
- Phát hiện hoạt động bất thường: IDS theo dõi các hoạt động mạng bình thường và tạo ra mô hình hoạt động thông thường. Nếu có bất thường hoặc khác biệt lớn so với mô hình này, IDS sẽ phát hiện và báo cáo.
- Phát hiện tấn công không biết: IDS có thể phát hiện các tấn công không biết bằng cách theo dõi dấu hiệu không bình thường trong dữ liệu mạng, như lưu lượng không thường hoặc các gói tin lạ.
- Báo cáo và cảnh báo: IDS cung cấp cảnh báo cho quản trị viên hoặc hệ thống quản lý khi phát hiện tấn công hoặc hoạt động bất thường.
- Ghi lại lưu lượng mạng: IDS ghi lại dữ liệu lưu lượng mạng liên quan đến các sự kiện để có thể phân tích sau này và hỗ trợ trong việc điều tra.
- Tích hợp với IPS: IDS có thể kết hợp với IPS để tự động ngăn chặn các tấn công sau khi phát hiện chúng.
- Báo cáo và phân tích sự cố: IDS cung cấp báo cáo chi tiết về các sự cố đã xảy ra, giúp quản trị viên hiểu rõ và phản ứng nhanh chóng đối với các mối đe dọa.

## 1.2. Thiết bị cần có:

Thiết bị	Số lượng
PC	95

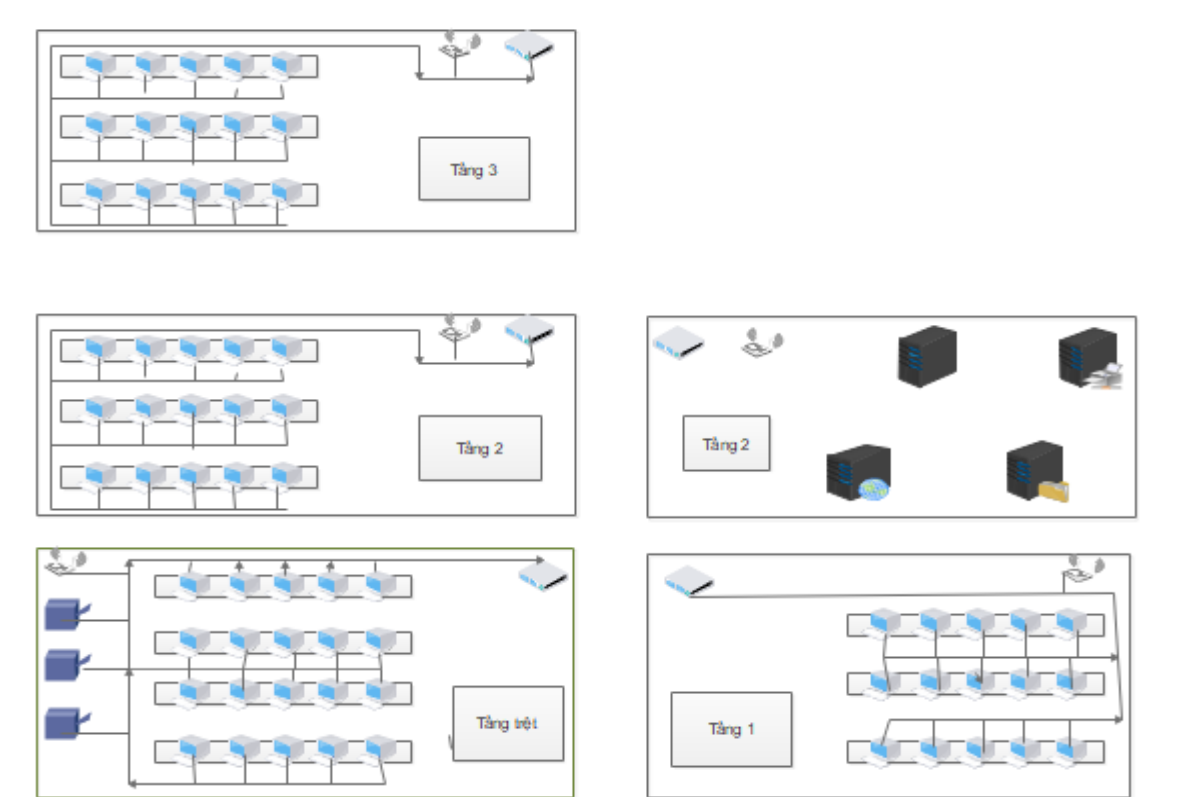
Server	4
Printer	3
FG-240D FIREWALL FORTINET FORTIGATE	1
Integrated Services Routers CISCO CISCO2921/K9	2
Switch Cisco Catalyst C1300-48P-4G-EU	4
Cat 5 Cable	
Cat 6 Cable	

### 1.3. Logic topology:



Hình 22

### 1.4. Physical topology:



Hình 23

## 1.5. IP Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	Fa0/0	10.0.1.1	-	N/A
	Fa1/0	-	-	N/A
RouterCore	Fa0/0	192.168.2.1	255.255.255.0	N/A
	Fa1/0	192.168.3.1	255.255.255.0	N/A
	Fa2/0	192.168.5.1	255.255.255.0	N/A
	Fa3/0	192.168.6.1	255.255.255.0	N/A
	Fa4/0	192.168.1.1	255.255.255.0	N/A
	Fa5/0	192.168.4.1	255.255.255.0	N/A
Firewall ASA	Gi0/0	192.168.6.2	255.255.255.0	192.168.6.1
	Gi0/1	10.0.1.0	-	-
Server	E0/0	192.168.4.2	255.255.255.0	192.168.4.1
	E0/1	192.168.4.5	255.255.255.0	192.168.4.1
Printer	Eth0	192.168.1.34-37	255.255.255.0	192.168.1.1
Host-G	Eth0	192.168.1.3-33	255.255.255.0	192.168.1.1

Host-1	Eth0	192.168.2.2-21	255.255.255.0	192.168.2.1
Host-2	Eth0	192.168.3.2-21	255.255.255.0	192.168.3.1
Host-3	Eth0	192.168.5.2-21	255.255.255.0	192.168.5.1

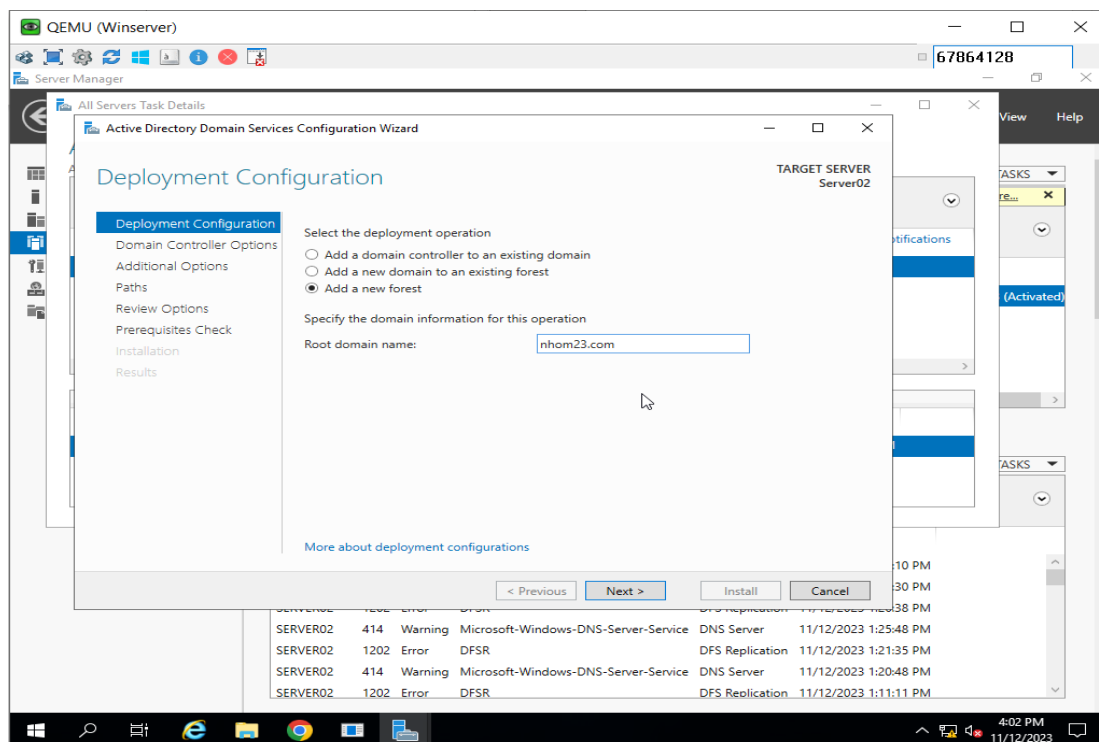
## 2. Đánh giá và kiểm chứng kế hoạch:

Mục tiêu	Kế hoạch kiểm chứng	Kết quả mong muốn
Ping Configuration	Sử dụng lệnh ping kiểm tra kết nối và thời gian đáp ứng.	Kết quả ping nhanh và ổn định là dấu hiệu mạng kết nối tốt và hiệu suất cao.
DHCP Configuration	Kết nối thiết bị mới và kiểm tra việc nhận địa chỉ IP từ DHCP.	Dịch vụ DHCP hoạt động nếu thiết bị nhận được địa chỉ IP mà không gặp xung đột.
DNS Configuration	Sử dụng lệnh nslookup kiểm tra chuyển đổi giữa tên miền và địa chỉ IP.	Dịch vụ DNS hoạt động đúng nếu chuyển đổi IP và tên miền đúng đắn.

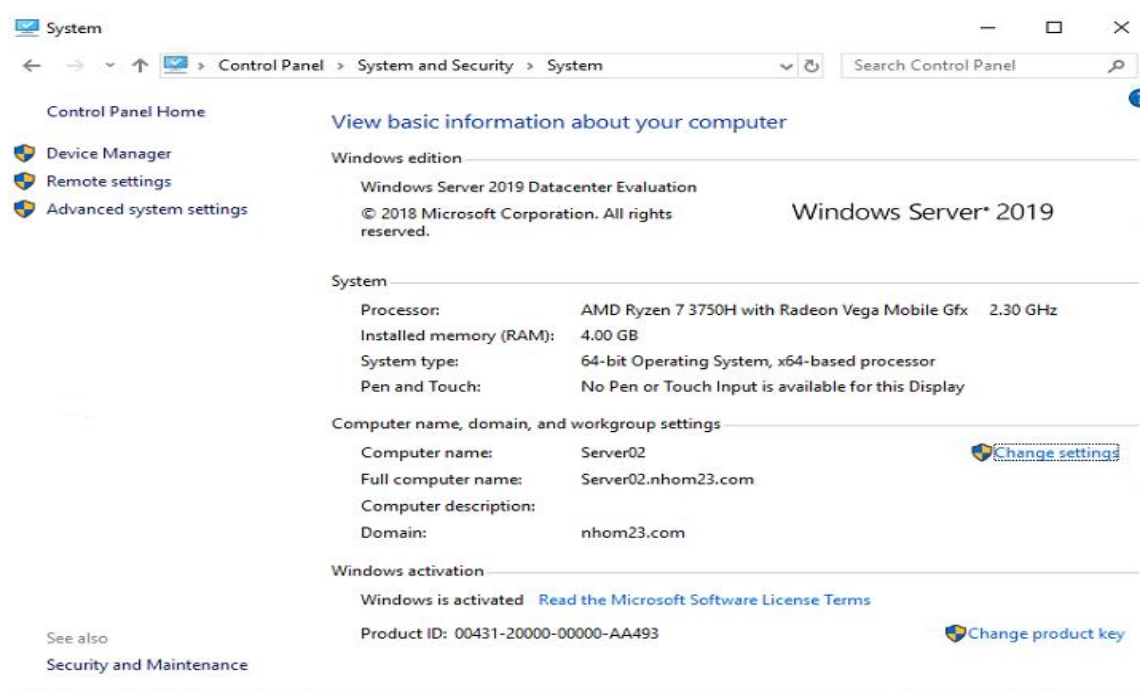
## III. Triển khai:

### 1. Triển khai setup hệ thống:

#### 1.1 Cấu hình ADDS:

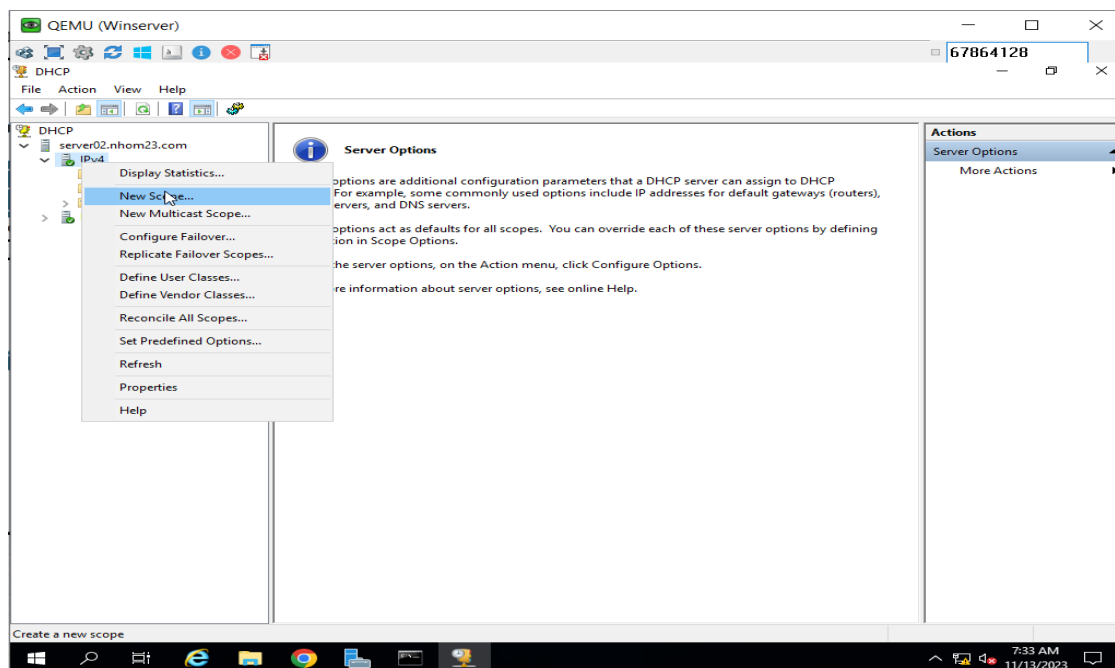


Hình 24

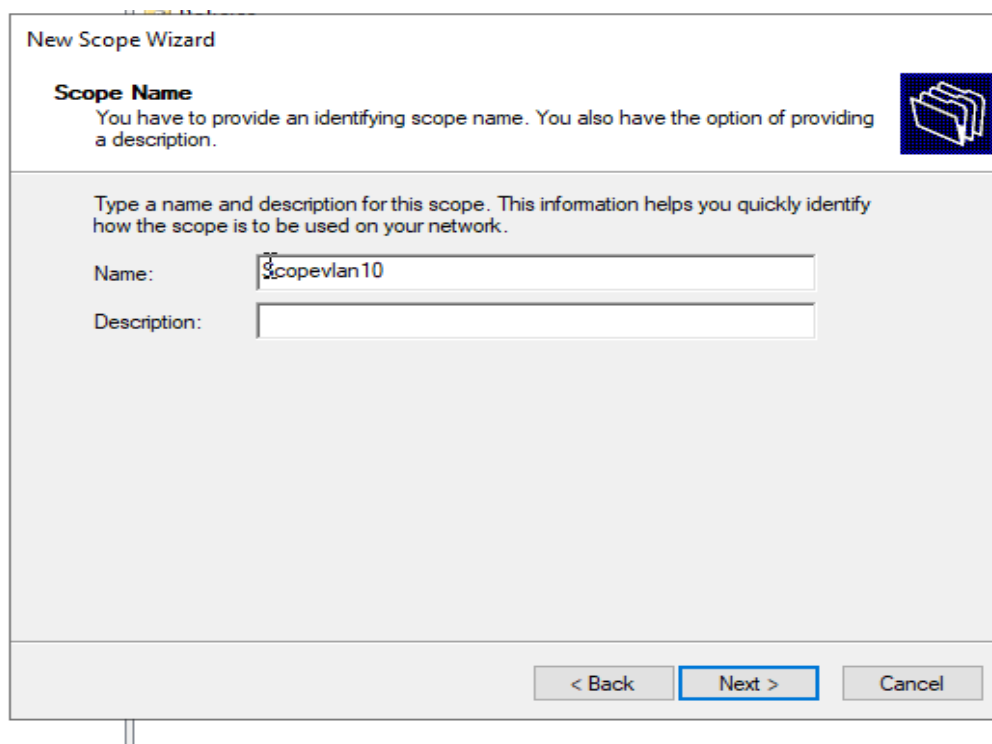


Hình 25

## 1.2 Cấu hình DHCP:

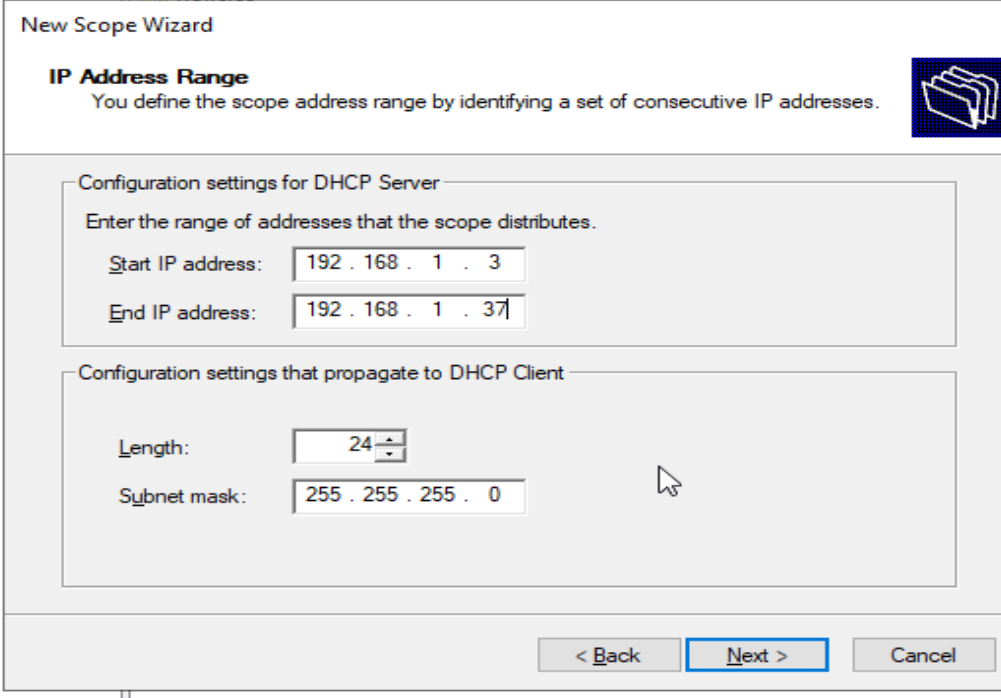


Hình 26



Hình 27





The image shows a 'New Scope Wizard' window with the title 'IP Address Range'. It contains a description: 'You define the scope address range by identifying a set of consecutive IP addresses.' Below this, there are two sections. The first section, 'Configuration settings for DHCP Server', asks to 'Enter the range of addresses that the scope distributes.' and has two input fields: 'Start IP address:' with the value '192 . 168 . 1 . 3' and 'End IP address:' with the value '192 . 168 . 1 . 37'. The second section, 'Configuration settings that propagate to DHCP Client', has two input fields: 'Length:' with a value of '24' and a dropdown arrow, and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Scope Wizard

**IP Address Range**  
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 3

End IP address: 192 . 168 . 1 . 37

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Hình 28

```
Switch(config)#ip dhcp pool vlan10
Switch(dhcp-config)#network
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0
Switch(dhcp-config)#default-router 192.168.1.1
Switch(dhcp-config)#dns-server 192.168.4.5
Switch(dhcp-config)#domain-name nhom23.com
Switch(dhcp-config)#
```

Hình 29

```

Windows IP Configuration

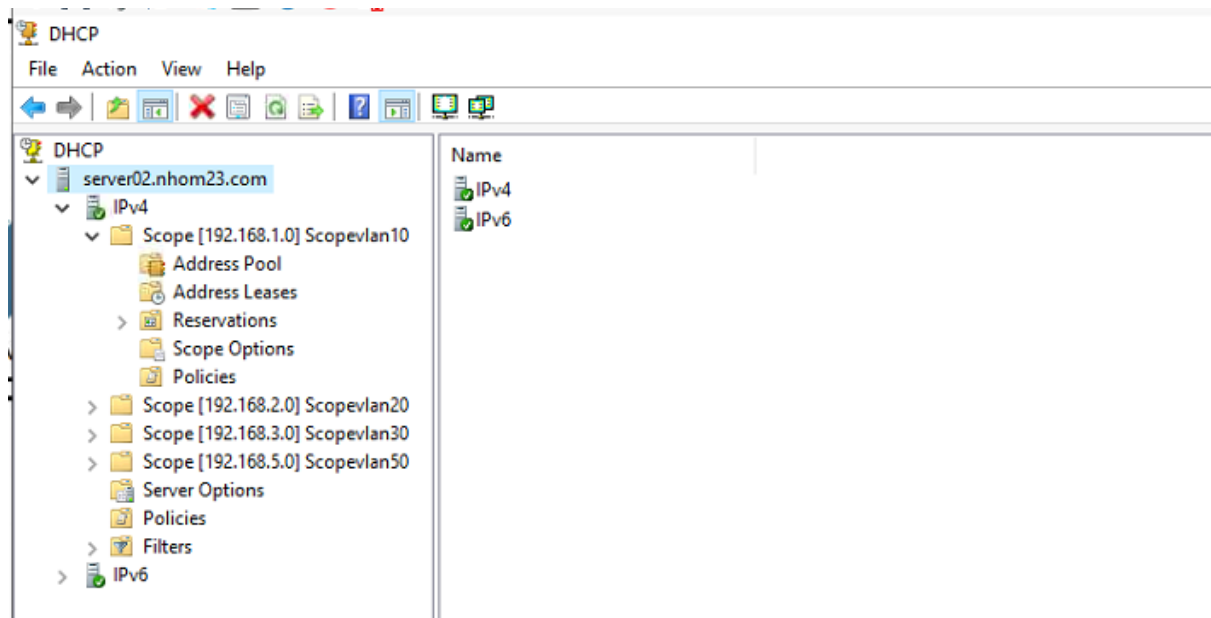
Host Name . . . . . : DESKTOP-VFNFEA4
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : nhom23.com

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : nhom23.com
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 50-00-00-06-00-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f8f2:a0d2:bcdb:3a8d%6(Preferred)
    IPv4 Address. . . . . : 192.168.1.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Tuesday, November 14, 2023 9:56:51 AM
    Lease Expires . . . . . : Wednesday, November 15, 2023 9:56:51 AM
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 122683392
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-1B-8F-FF-00-0C-29-7C-3E-02
    DNS Servers . . . . . : 192.168.4.5
    NetBIOS over Tcpip. . . . . : Enabled

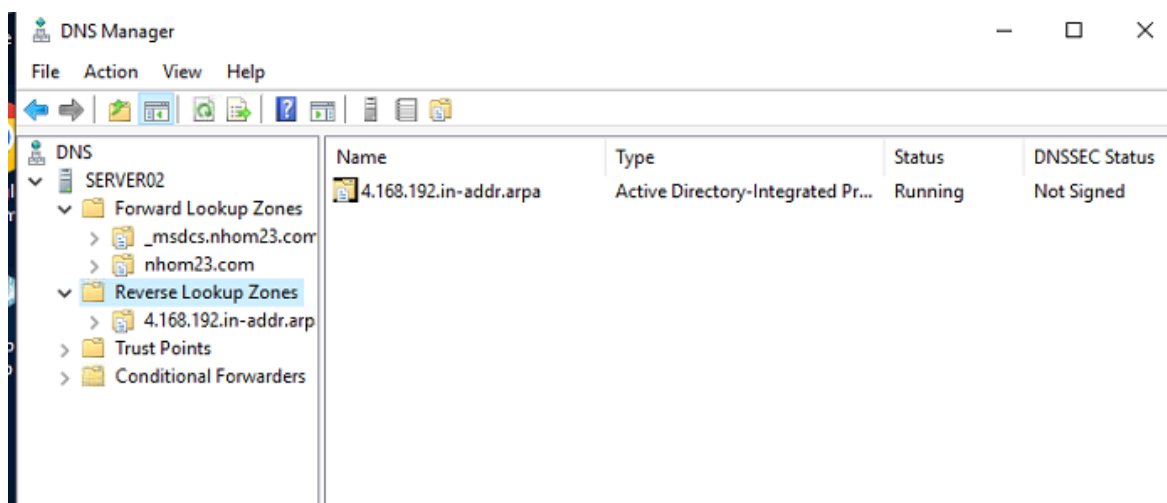
```

Hình 30



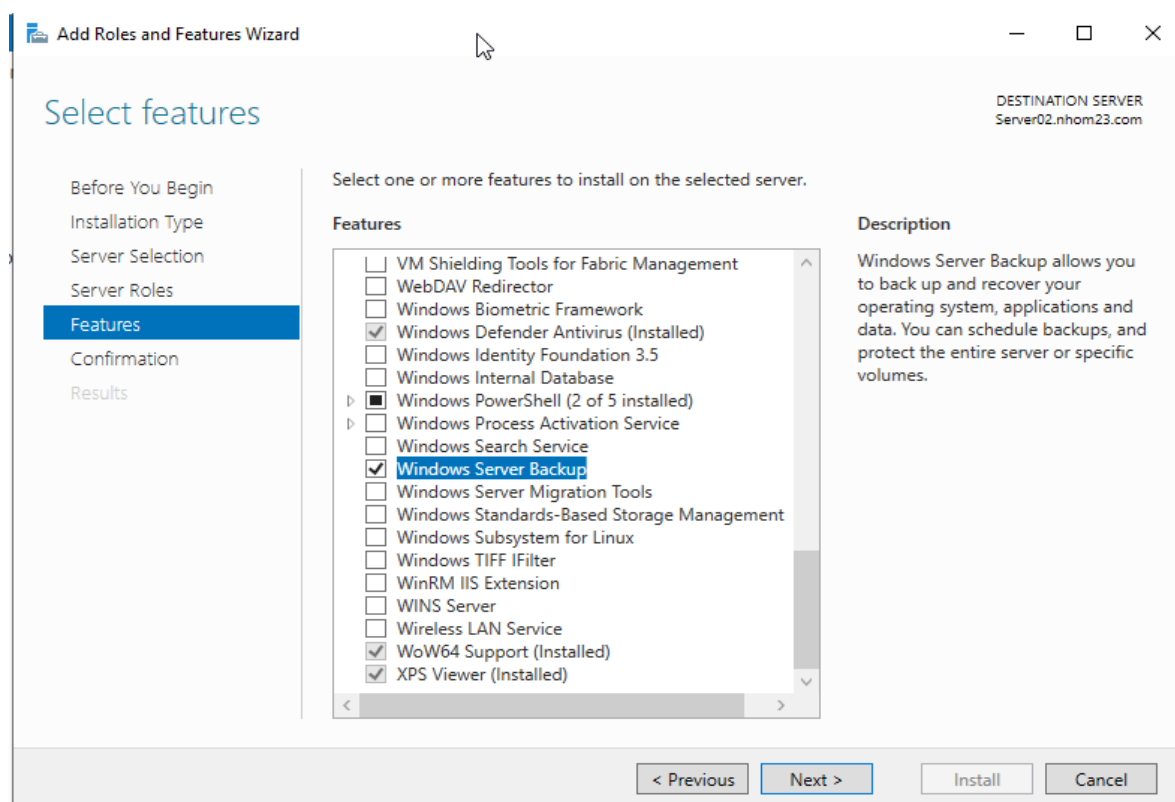
Hình 31

### 1.3 Cấu hình DNS:

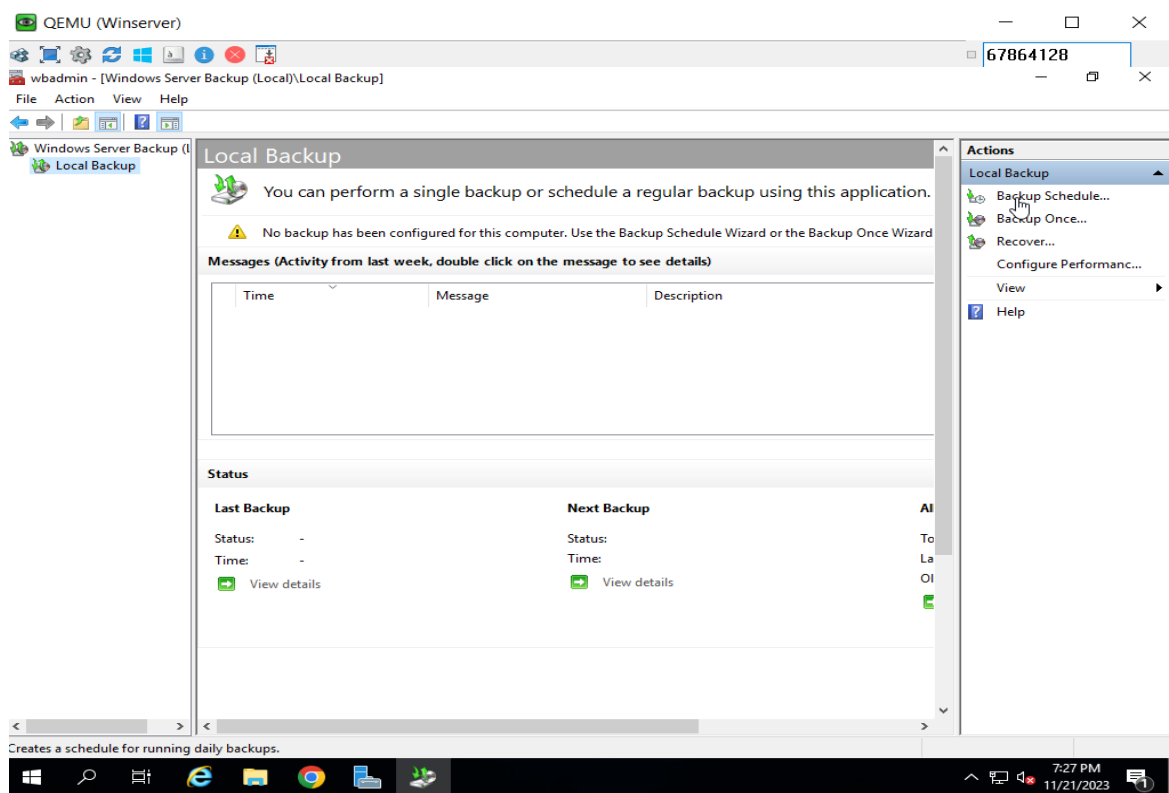


Hình 32

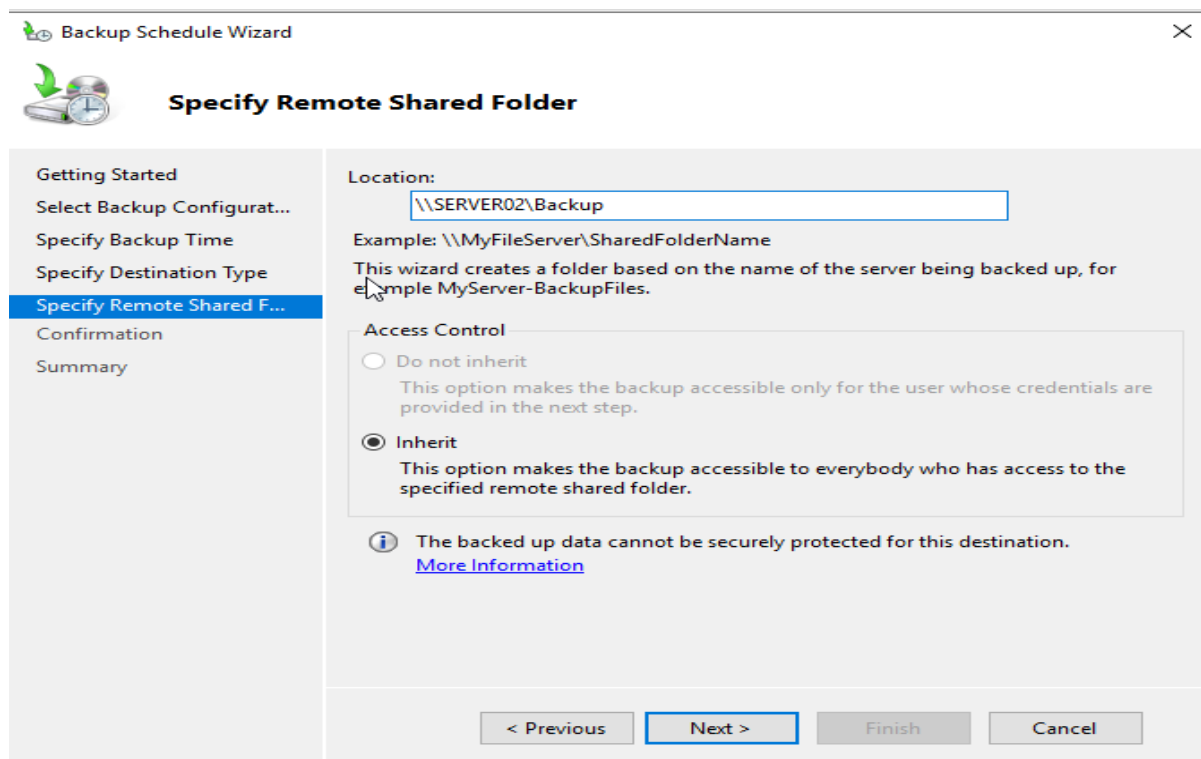
#### 1.4 Backup:



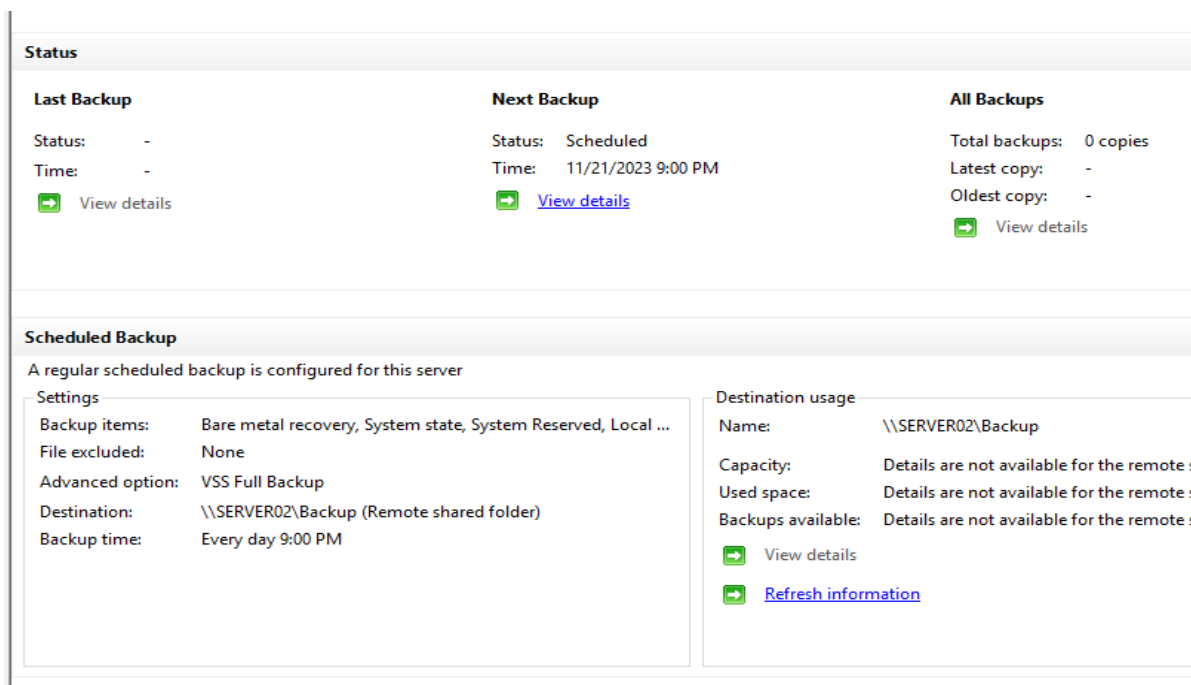
Hình 33



Hình 34

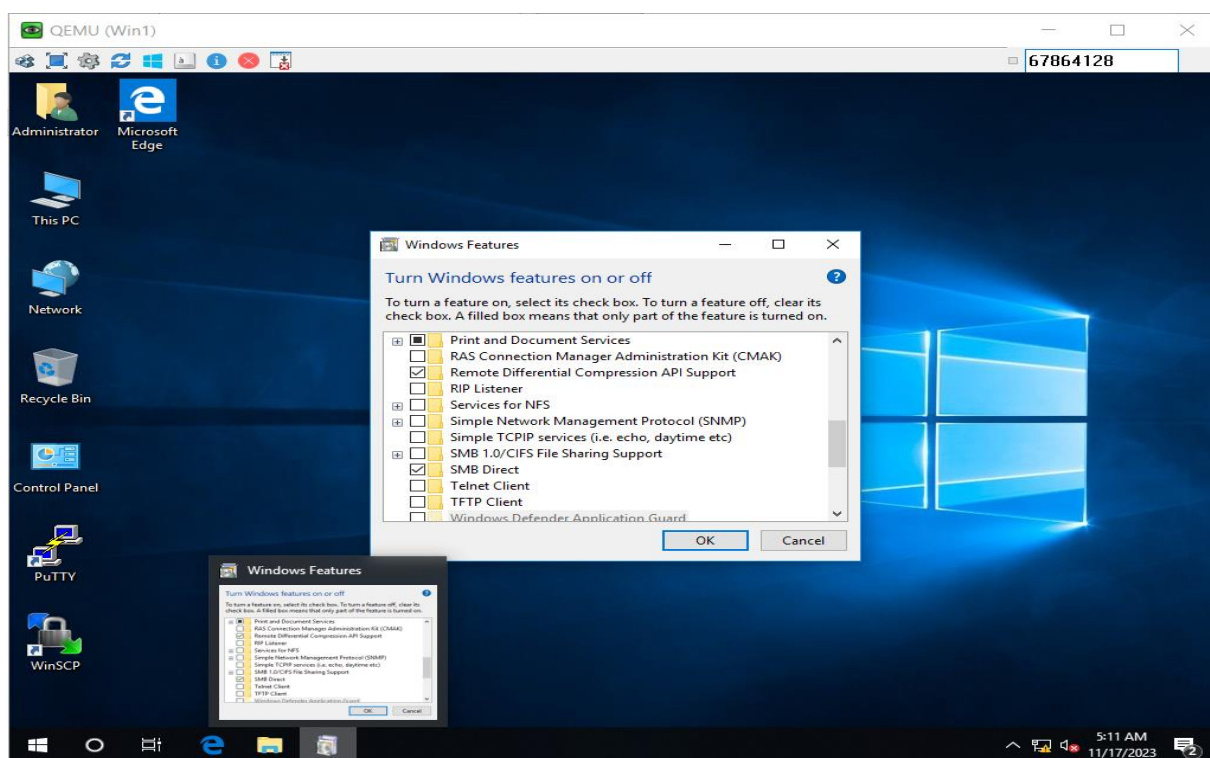


Hình 35

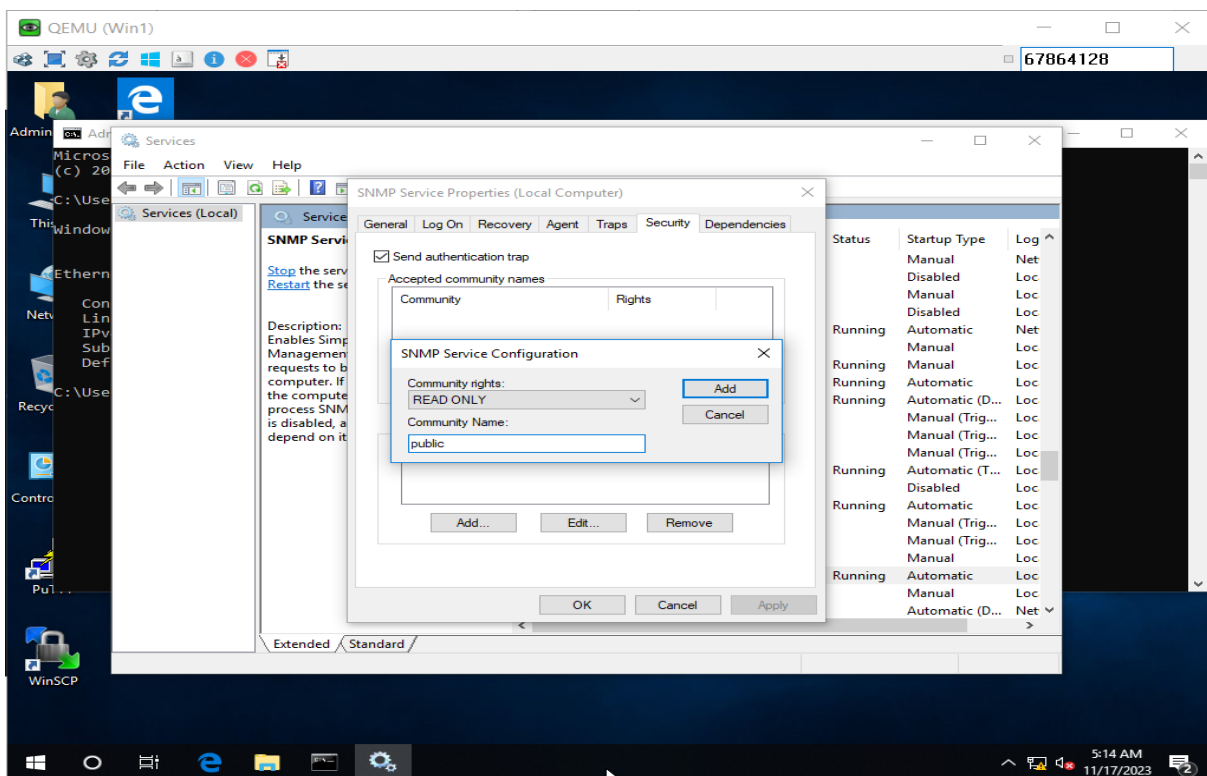


Hình 36

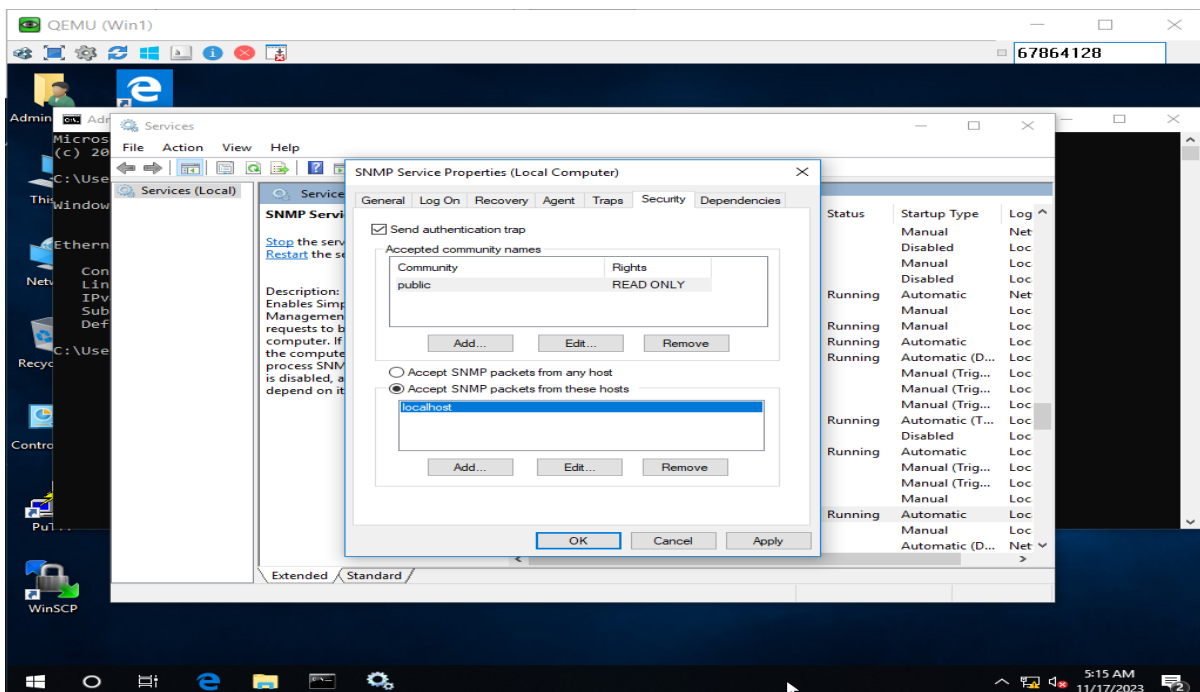
## 1.5 Giám sát mạng:



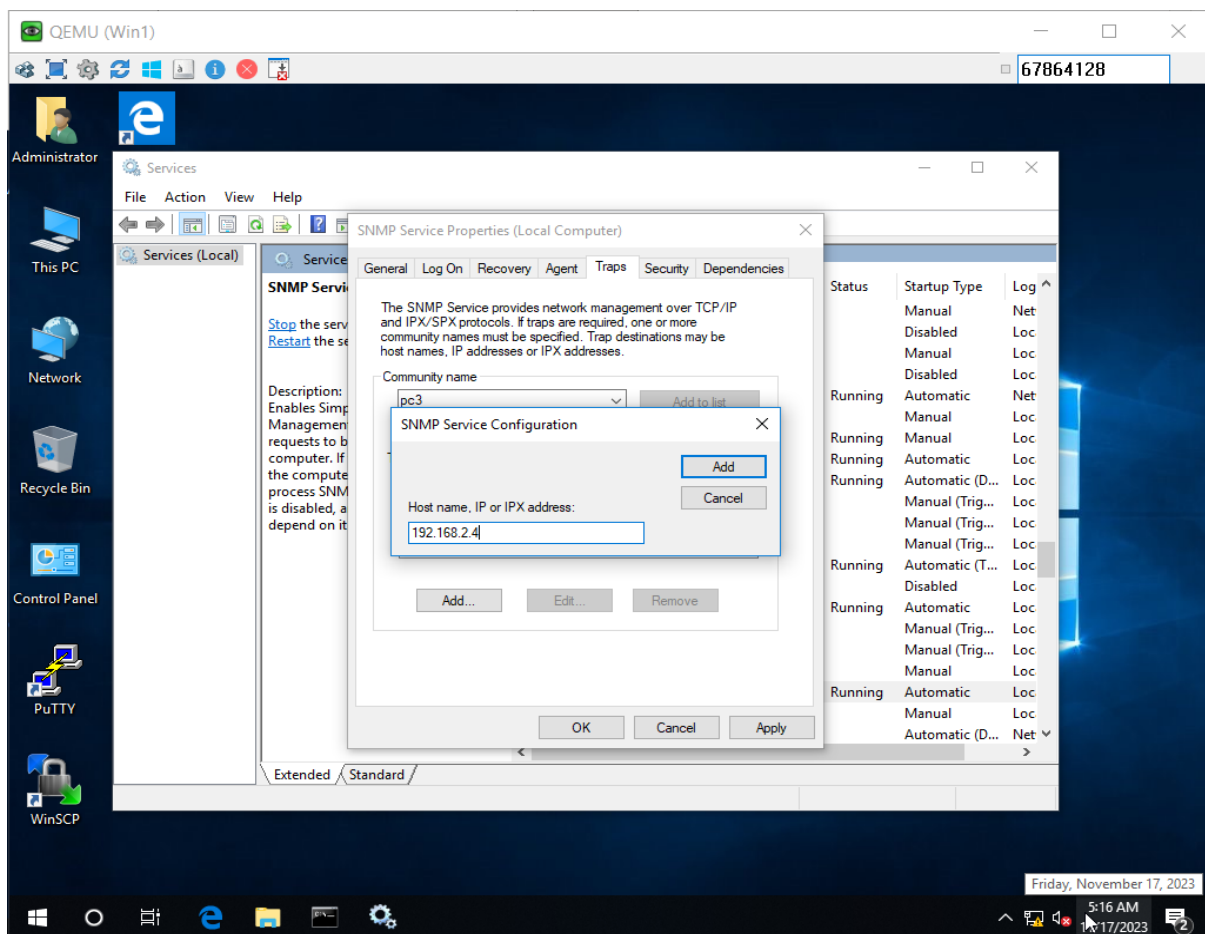
Hình 37



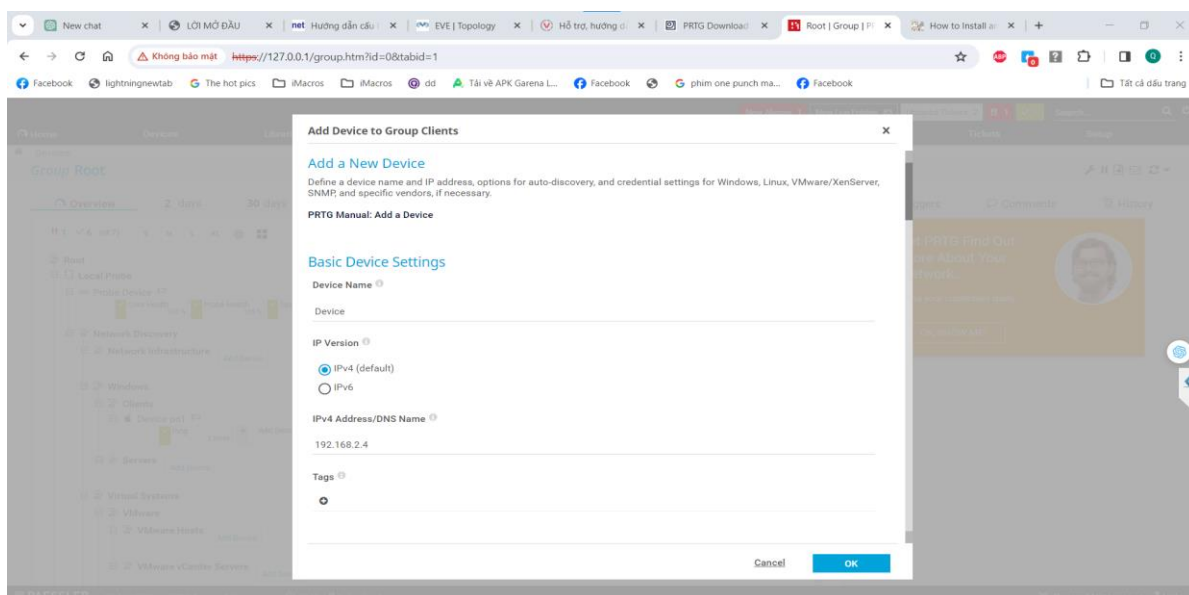
Hình 38



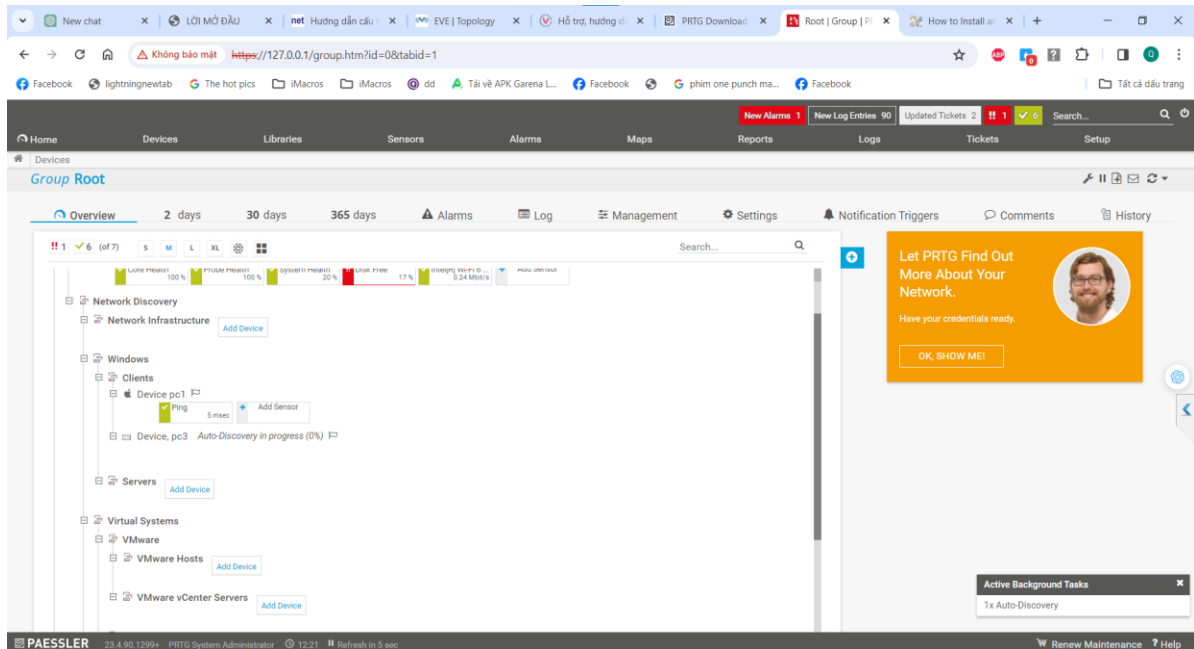
Hình 39



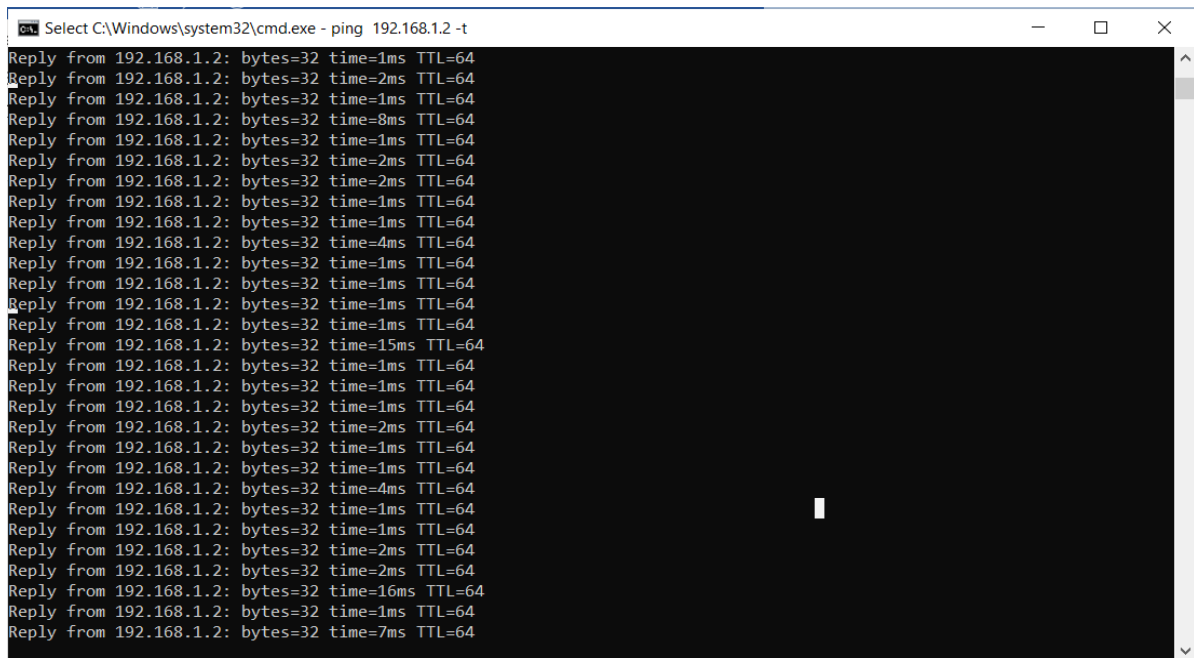
Hình 40



Hình 41

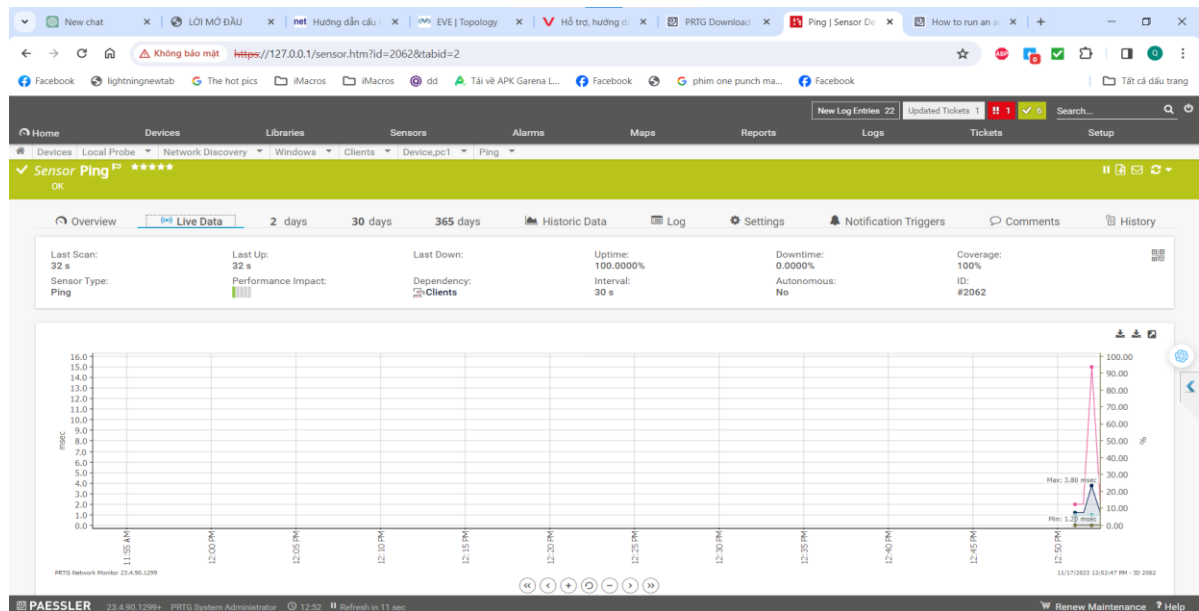


Hình 42



Hình 43





Hình 44

## 2. Đánh giá kết quả thực hiện:

Nhóm đã thiết kế được sơ đồ hệ thống mạng cho 1 doanh nghiệp nhỏ.

Đã cấu hình thành công DHCP trên Switch Core L3 để định tuyến xuống VLAN từng phòng ban.

Cấu hình hoàn chỉnh Server, triển khai DC, ADDS.

Triển khai Backup file trên Server vào Sharepoint domain.

Còn nhiều mặt hạn chế chưa hoàn thiện File Backup, IDS và Firewall.

## IV. Quản trị hệ thống:

### 1. Đánh giá và lựa chọn Network monitoring tool (SNMP, PRTG...), chọn giải pháp (giám sát được lưu lượng,...):

Trong quá trình triển khai đồ án, việc lựa chọn một công cụ giám sát mạng hiệu quả là quan trọng để đảm bảo sự ổn định và an toàn của hệ thống. Chúng tôi đã tiến hành đánh giá các công cụ phổ biến như SNMP (Simple Network Management Protocol) và PRTG để xác định công cụ nào phù hợp nhất với yêu cầu của dự án.

SNMP (Simple Network Management Protocol) đã được xem xét kỹ lưỡng vì tính đơn giản và khả năng tích hợp với nhiều thiết bị mạng. Giao thức này cho phép thu thập thông tin từ các thiết bị mạng và cung cấp cơ sở dữ liệu có thể sử dụng để theo

dõi hiệu suất hệ thống. Ưu điểm: Phổ biến: SNMP được hỗ trợ rộng rãi trên nhiều thiết bị mạng, bao gồm router, switch, và server. Dễ triển khai: Cài đặt và cấu hình SNMP là một quá trình đơn giản, giảm thời gian triển khai.

Nhược điểm: Bảo mật: SNMP có thể gặp vấn đề về bảo mật nếu không được cấu hình đúng. Hạn chế chức năng: Một số tính năng giám sát cao cấp có thể bị hạn chế so với các công cụ giám sát chuyên sâu hơn

## 2. Các báo cáo nhận được:

Tính Ổn Định và Tin Cậy:

Hệ thống PRTG Network Monitor đã hoạt động ổn định và tin cậy, không gặp sự cố lớn trong quá trình giám sát mạng và các thiết bị.

Cảm biến đa dạng:

Phản hồi cho thấy việc sử dụng nhiều loại cảm biến trong PRTG giúp theo dõi mọi khía cạnh của mạng, từ băng thông đến tình trạng kết nối và tài nguyên máy chủ.

Cảnh Báo Linh Hoạt và Thông Tin Chi Tiết:

Cảnh báo chính xác: Hệ thống cảnh báo của PRTG đã cung cấp thông báo ngay lập tức khi có sự cố xảy ra, giúp chúng tôi phản ứng kịp thời để giải quyết vấn đề.

Thông tin chi tiết: Các báo cáo cung cấp thông tin chi tiết về tình trạng mạng, giúp chúng tôi dễ dàng xác định nguyên nhân của sự cố và đưa ra giải pháp một cách nhanh chóng.

Quản Lý Dễ Dàng:

Giao diện thân thiện: Người quản trị mạng đánh giá cao giao diện người dùng của PRTG, cho phép họ dễ dàng theo dõi tình trạng mạng và tài nguyên.

Thiết lập và tùy chỉnh linh hoạt: PRTG cho phép chúng tôi tùy chỉnh các cảm biến và báo cáo theo nhu cầu cụ thể của trường, giúp quản lý mạng một cách hiệu quả.

## V. Kết luận:

Tuy nhiên, cũng cần nhấn mạnh rằng, bản báo cáo này chỉ đại diện cho một phần nhỏ của hành trình nghiên cứu và phát triển hệ thống mạng. Còn nhiều khía cạnh và phương pháp tiếp cận khác mà chúng ta có thể khám phá và áp dụng để nâng cao hiệu quả và chất lượng của hệ thống. Chúng em cam kết tiếp tục nghiên cứu và phát triển, với hy vọng đưa ra những cải tiến và đề xuất tốt hơn trong tương lai.

Được hỗ trợ bởi kinh nghiệm và kiến thức đã thu thập, chúng em tin tưởng rằng sẽ có thể ứng dụng và phát triển những kiến thức này trong các dự án sắp tới, góp phần quan trọng vào sự phát triển của lĩnh vực an ninh mạng. Chúng em cam kết duy trì sự đam mê và tìm kiếm những giải pháp đổi mới để đảm bảo rằng hệ thống của chúng tôi không chỉ đáp ứng được nhu cầu hiện tại mà còn đối mặt với thách thức của tương lai.