

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC
THÀNH PHỐ HỒ CHÍ MINH



ĐỀ TÀI MÔN

ĐỒ ÁN MẠNG


SV: Nguyễn Công Khang - 21DH110770

SV: Phạm Đức Thiên Phúc - 21DH112813

SV: Nguyễn Minh Đức – 21DH113591

GVGD: GV. Đỗ Phi Hưng


PHIẾU CHẤM ĐIỂM MÔN THI VẤN ĐÁP

 Điểm phân trình bày – Điểm hệ 10

	CBCT1	CBCT2
Họ tên CBCT Chữ ký: Chữ ký:
Điểm Bằng chữ: Bằng chữ:
Nhận xét <ul style="list-style-type: none"> Báo cáo:2d Vấn đáp:2d Chức năng và demo :5d Mở rộng và ứng dụng thực tiễn:1d 	Quyền báo cáo:(...) điểm... Vấn đáp :(...) điểm ... Chức năng :(...) điểm... Mở rộng :(...) điểm...	Quyền báo cáo:(...) điểm... Vấn đáp :(...) điểm ... Chức năng :(...) điểm... Mở rộng :(...) điểm...

 Điểm quá trình – Điểm hệ 10

Họ tên CBCT:

 Điểm tổng kết:(Bằng chữ:.....)

Lời cảm ơn

*Trong thời gian học tập dưới mái trường Đại Học Ngoại Ngữ Tin Học Thành Phố Hồ Chí Minh, được sự truyền đạt kiến thức và giúp đỡ tận tình của quý Thầy Cô Giảng viên là hành trang quý báu cho sự nhận thức và hiểu biết của em ngày hôm nay. Em xin ghi nhận nơi này lòng biết ơn chân thành nhất đối với tất cả các Thầy Cô Giảng viên và đặc biệt là thạc sĩ **ĐỖ PHI HÙNG**, giảng viên chuyên ngành Đồ án mạng, người thầy đã tận tình hướng dẫn em hoàn thành bài báo cáo tốt nghiệp này. Do kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ cũng chưa hoàn hảo nên bài báo cáo sẽ còn nhiều thiếu sót, kính mong sự góp ý và giúp đỡ từ Quý Thầy cô. Một lần nữa, em xin chân thành cảm ơn!*

Mô tả đề 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 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.

- 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.

- 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.

Nội dung	
Lời cảm ơn.....	3
Mô tả đồ án.....	4
Chương 1: CƠ SỞ LÝ THUYẾT	7
1. Network operating System (NOS).....	7
1.1 Đánh giá các loại NOS (3 điểm)	7
1.2 Khả năng dự phòng, phục hồi hệ thống	13
Chương 2: LÊN KẾ HOẠCH TRIỂN KHAI	35
2 Lên kế hoạch triển khai	35
2.1 Thiết kế hệ thống	35
2.2 Đánh giá và kiểm chứng kế hoạch	41
Chương 3: TRIỂN KHAI	42
3 Triển khai.....	42
3.1 Triển khai setup hệ thống	42
3.2 Cấu hình và test lỗi.....	55
3.3 Đánh giá kết quả thực hiện	59
Chương 4: QUẢN TRỊ HỆ THỐNG	62
4 Quản trị hệ thống.....	62
4.1 Đánh giá và lựa chọn network monitoring tool (SNMP, PRTG...).....	62
4.2 Các báo cáo nhận được	64
5 Kết luận	67
TÀI LIỆU THAM KHẢO	69

Danh mục hình ảnh

<u>Hình 1:Minh hoạ về DNS.....</u>	11
<u>Hình 2:Minh hoạ về DHCP.....</u>	12
<u>Hình 3:Minh hoạ về DHCP.....</u>	13
<u>Hình 4: Mô hình NAS.....</u>	14
<u>Hình 5: Mô Hình SAN.....</u>	15
<u>Hình 6:Minh hoạ về mô hình backup.....</u>	17
<u>Hình 7:RAID.....</u>	19
<u>Hình 8:Suricata.....</u>	22
<u>Hình 9:Mô hình Snort.....</u>	23
<u>Hình 10:Hệ thống cảm biến sensors.....</u>	24
<u>Hình 11:SIEM.....</u>	25
<u>Hình 12:Wireshark.....</u>	27
<u>Hình 13:Nagios.....</u>	29
<u>Hình 14:Zabbix.....</u>	33
<u>Hình 15:PRTG Network Monitoring.....</u>	34
<u>Hình 16:Sơ đồ logic.....</u>	38
<u>Hình 17:Sơ đồ vật lý.....</u>	39
<u>Hình 18:Đặt tên cho domain.....</u>	43
<u>Hình 20:Hoàn thành cài đặt domain.....</u>	44
<u>Hình 23:Test thử.....</u>	46
<u>Hình 25:Đặt tên và ghi chú cho scope.....</u>	48
<u>Hình 27:Hoàn thành tạo Scope.....</u>	50
<u>Hình 28:Sau khi đã tạo scope.....</u>	51
<u>Hình 29: Tạo rule cho firewall ra internet.....</u>	52
<u>Hình 31: Cấu hình port2.....</u>	53
<u>Hình 32:McAfee.....</u>	54
<u>Hình 33:Cấu hình máy Server.....</u>	55
<u>Hình 35: Ping tới Server.....</u>	57
<u>Hình 36:IDS.....</u>	58
<u>Hình 37:Cấu hình Firewall.....</u>	58

Chương 1: CƠ SỞ LÝ THUYẾT

1. Network operating System (NOS)

1.1 Đánh giá các loại NOS (3 điểm)

1.1.1 So sánh và đánh giá các loại NOS (Windows, Linux, MacOS...)

So Sánh	Windows	Linux	MacOS
Tính năng	Windows Server là một hệ điều hành chuyên biệt dành cho máy chủ, có nhiều tính năng mạnh mẽ như Active Directory, IIS (Internet Information Services), và nhiều ứng dụng doanh nghiệp.	Linux có nhiều biến thể (phân phối) khác nhau như CentOS, Ubuntu, và Debian, mỗi loại có tính năng riêng. Linux thường được sử dụng cho các máy chủ web và dự án mã nguồn mở.	MacOS không phải là một lựa chọn phổ biến cho máy chủ mạng, nhưng có khả năng thích hợp với môi trường doanh nghiệp nhỏ và dự án sáng tạo.

Hiệu suất	Thường được sử dụng trong môi trường doanh nghiệp và có hiệu suất ổn định. Windows có giao diện đồ họa dễ sử dụng.	Thường được coi là ổn định và hiệu suất cao, đặc biệt là trong các môi trường máy chủ.	Thường được thiết kế cho máy tính cá nhân, nên hiệu suất trên máy chủ có thể không cao bằng Windows hoặc Linux.
Tích hợp	Tích hợp tốt với các sản phẩm và dịch vụ Microsoft khác, nhưng có thể đắt đỏ và phụ thuộc vào giấy phép.	Có thể cần nhiều công sức hơn để tích hợp các ứng dụng doanh nghiệp, nhưng có sẵn nhiều phần mềm mã nguồn mở.	Tích hợp tốt với các sản phẩm Apple, nhưng có hạn chế trong việc tích hợp với các ứng dụng doanh nghiệp bên ngoài.
Bảo mật	Windows Server cung cấp các công cụ bảo mật mạnh mẽ như BitLocker và Windows	Linux có cộng đồng bảo mật lớn, nên các lỗ hổng thường được báo cáo và sửa đặc	MacOS có các tính năng bảo mật tốt, nhưng không phải lựa chọn hàng đầu cho môi

	Defender, nhưng thường cần phải cập nhật thường xuyên để duy trì bảo mật.	biệt nhanh. Nó cũng có các tính năng bảo mật mạnh mẽ như SELinux.	trường máy chủ mạng.
--	---	---	----------------------

1.1.2 Lựa chọn NOS phù hợp với dự án

- Windows Server là 1 lựa chọn tốt bởi những yếu tố sau:

Hỗ trợ đa dạng ứng dụng và dịch vụ: Windows Server cung cấp sự hỗ trợ tốt cho nhiều ứng dụng và dịch vụ doanh nghiệp phổ biến như Active Directory, Microsoft Exchange, SharePoint và SQL Server. Điều này làm cho nó trở thành lựa chọn hữu ích cho các môi trường doanh nghiệp đa dạng về ứng dụng.

Tích hợp với môi trường Windows sẵn có: Nếu tổ chức của bạn đã sử dụng các sản phẩm Microsoft khác như Windows 10 hoặc Office 365, việc triển khai Windows Server có thể tạo sự tương thích tốt hơn và tích hợp dễ dàng hơn giữa các thành phần của môi trường.

Hỗ trợ bảo mật và quản lý: Windows Server cung cấp các công cụ quản lý và bảo mật mạnh mẽ như Windows Defender, BitLocker,

Group Policy, và Windows Firewall. Điều này giúp duy trì tính bảo mật của hệ thống mạng và quản lý người dùng và tài nguyên dễ dàng.

Sự ổn định và hỗ trợ dài hạn: Windows Server thường có thời gian hỗ trợ dài hạn từ Microsoft, cung cấp các bản cập nhật và vá lỗi thường xuyên. Điều này đảm bảo rằng hệ thống của bạn được duy trì ổn định và an toàn trong thời gian dài.

Hệ sinh thái sản phẩm và dịch vụ thứ ba: Có nhiều nhà cung cấp phát triển ứng dụng và giải pháp bổ sung dành riêng cho Windows Server, giúp mở rộng tính năng và khả năng của hệ thống.

Dễ dàng sử dụng cho người quản trị: Giao diện quản trị của Windows Server thường được thiết kế để sử dụng và quen thuộc đối với người quản trị hệ thống Windows.

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

- **DNS (Domain Name System):**

Chức năng: DNS là dịch vụ quản lý và ánh xạ tên miền (ví dụ: www.example.com) thành địa chỉ IP (ví dụ: 192.168.1.1). Nó giúp các thiết bị trong mạng tìm kiếm và liên lạc với nhau bằng cách sử dụng tên miền thay vì địa chỉ IP.

Lý do cần triển khai: DNS giúp dễ dàng quản lý và thay đổi cấu hình mạng, cải thiện hiệu suất trong việc tìm kiếm và kết nối thiết bị, và cung cấp tính năng bảo mật như lọc DNS để ngăn chặn truy cập vào các trang web độc hại.



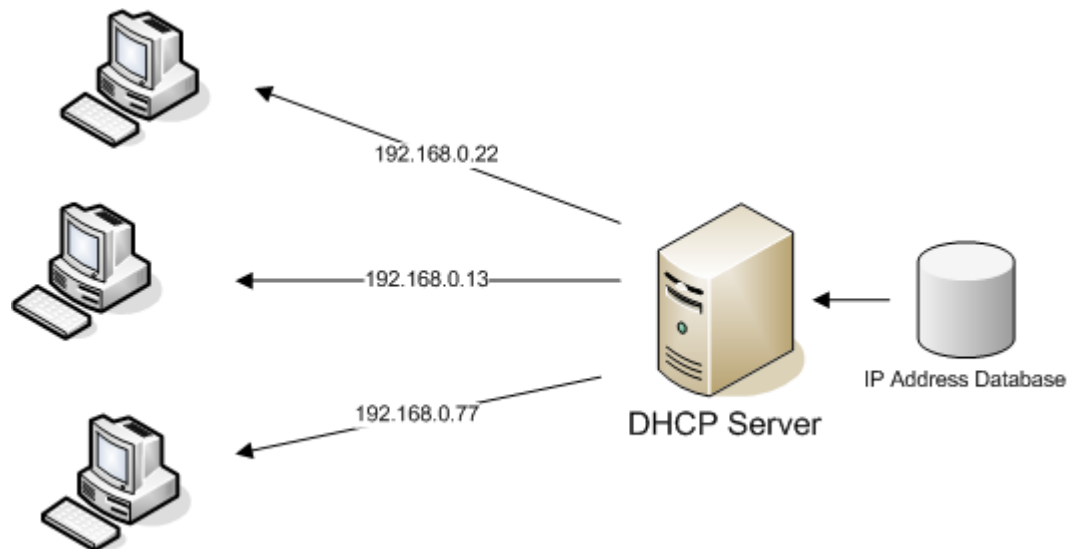
Hình 1: Minh họa về DNS

- **DHCP (Dynamic Host Configuration Protocol):**

Chức năng: DHCP là dịch vụ tự động cấp phát địa chỉ IP, cấu hình mạng, và các thông tin liên quan cho các thiết bị trong mạng. Nó giúp đơn giản hóa quản lý IP và tránh xung đột địa chỉ IP.

Lý do cần triển khai: DHCP giúp tiết kiệm thời gian và công sức cho việc cấu hình mạng. Thay vì phải thủ công cấu hình từng thiết bị,

DHCP tự động cấp phát địa chỉ IP và cấu hình, đảm bảo tính nhất quán và tránh sai sót.

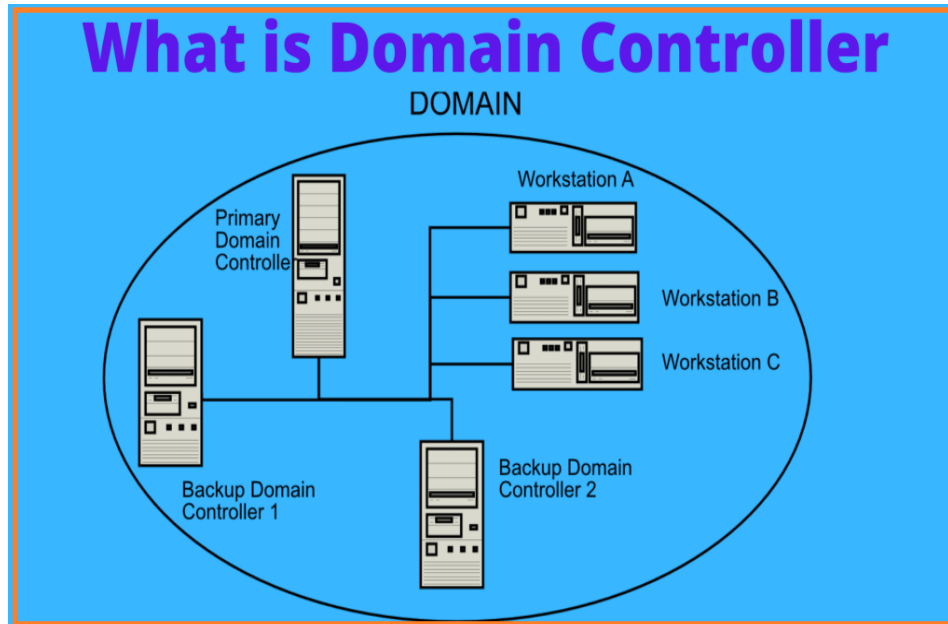


Hình 2: Minh họa về DHCP

- **Domain Controller (sử dụng Active Directory):**

Chức năng: Domain Controller là máy chủ chạy dịch vụ quản lý danh sách người dùng, máy tính và tài nguyên trong mạng. Active Directory là dịch vụ quản lý danh bạ này trên nền Windows Server.

Lý do cần triển khai: Active Directory cung cấp tính năng quản lý quyền truy cập, xác thực người dùng, và quản lý tài khoản người dùng và máy tính dễ dàng. Nó tạo ra một môi trường an toàn và quản lý tập trung cho mạng doanh nghiệp và cung cấp tính năng như Single Sign-On (SSO) và quản lý chính sách.



Hình 3: Minh họa về DHCP

1.2 Khả năng dự phòng, phục hồi hệ thống hoạt động liên tục

1.2.1 Các hệ thống lưu trữ tập trung.

Network Attached Storage (NAS):

- Ưu điểm

Đễ dàng cài đặt và quản lý: NAS thường được thiết kế để dễ dàng sử dụng và cài đặt. Hầu hết các NAS có giao diện web dựa trên trình duyệt, giúp người quản trị thiết lập và quản lý dễ dàng.

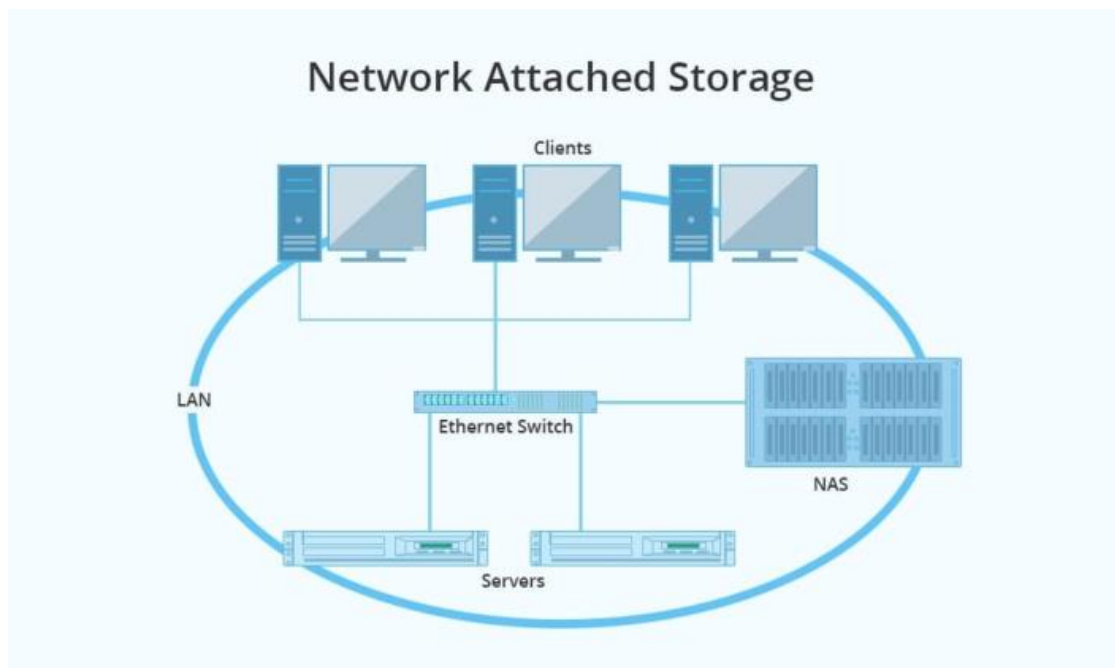
Giá thành thấp hơn: NAS thường có giá thành thấp hơn so với SAN, phù hợp với ngân sách của các tổ chức giáo dục.

Dự phòng dữ liệu: Các NAS có thể được cấu hình để sao lưu dữ liệu tự động, giúp đảm bảo tính sẵn sàng của dữ liệu.

- **Nhược điểm:**

Hiệu suất có thể hạn chế: NAS thường không có hiệu suất cao như SAN và thích hợp cho việc lưu trữ dữ liệu và chia sẻ tệp tin hơn là cho các ứng dụng yêu cầu tốc độ và thời gian thực.

Mở rộng hạn chế: Khả năng mở rộng của NAS có thể bị giới hạn, đặc biệt nếu bạn cần thêm dung lượng lưu trữ lớn hơn.



- Hình 4: Mô hình NAS

Storage Area Network (SAN):

- **Ưu điểm:**

Hiệu suất cao: SAN cung cấp hiệu suất cao hơn so với NAS, thích hợp cho các ứng dụng yêu cầu tốc độ và thời gian thực như máy chủ ảo và cơ sở dữ liệu.

Khả năng mở rộng linh hoạt: SAN cho phép mở rộng dễ dàng bằng cách thêm ổ cứng hoặc hệ thống lưu trữ mới.

Khả năng chia sẻ lưu trữ: SAN cho phép nhiều máy chủ truy cập và chia sẻ lưu trữ chung, tạo điều kiện cho mô hình ảo hóa.

- **Nhược điểm:**

Đòi hỏi kiến thức kỹ thuật: Cài đặt và quản lý SAN phức tạp hơn và đòi hỏi kiến thức kỹ thuật cao hơn.

Giá thành cao: SAN thường có chi phí cao hơn so với NAS, đặc biệt khi xây dựng một hệ thống SAN đầy đủ tính năng.



- Hình 5: Mô Hình SAN

-

Dựa trên yêu cầu của dự án, việc sử dụng NAS có thể là một lựa chọn hợp lý hơn cho Viện Giáo Dục Quốc Tế HUFLIT. NAS đủ để lưu trữ và quản lý dữ liệu của một tổ chức giáo dục với hiệu suất và tính ổn định tốt, đồng thời giữ được chi phí dưới sự kiểm soát. Tuy nhiên, nếu có yêu cầu về hiệu suất và mở rộng lớn hơn trong tương lai, SAN có thể xem xét làm lựa chọn mở rộng.

1.2.2 Các kiểu Backup, Raid

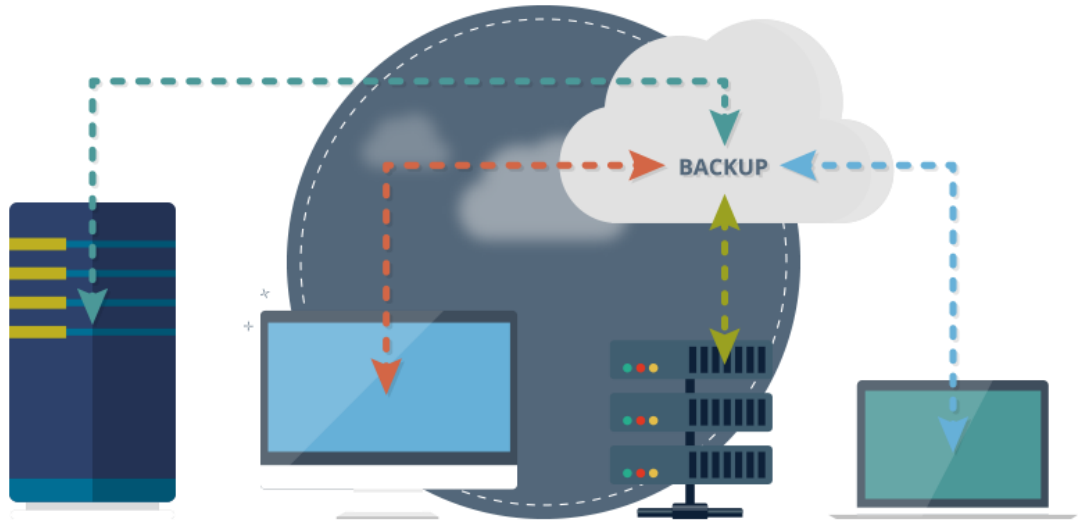
Các kiểu sao lưu (Backup):

Sao lưu toàn bộ hệ thống (Full Backup): Đây là quá trình sao lưu toàn bộ dữ liệu và hệ thống. Nó bao gồm tất cả các tập tin và thư mục trên máy chủ. Full backup thường tiêu tốn nhiều dung lượng lưu trữ và thời gian hơn, nhưng cho phép phục hồi toàn bộ hệ thống nhanh chóng.

Sao lưu ghi chú (Incremental Backup): Trong phương pháp này, chỉ các tập tin và thư mục đã thay đổi kể từ lần sao lưu trước đó mới được sao lưu. Điều này giúp tiết kiệm dung lượng lưu trữ và thời gian sao lưu, nhưng có thể tạo ra nhiều bản sao lưu nhỏ.

Sao lưu lịch sử (Historical Backup): Sao lưu lịch sử (hay còn gọi là sao lưu điểm thời gian) cho phép bạn lưu trữ nhiều phiên bản trước đó

của dữ liệu. Điều này hữu ích trong trường hợp cần phục hồi dữ liệu từ một thời điểm cụ thể trong quá khứ.



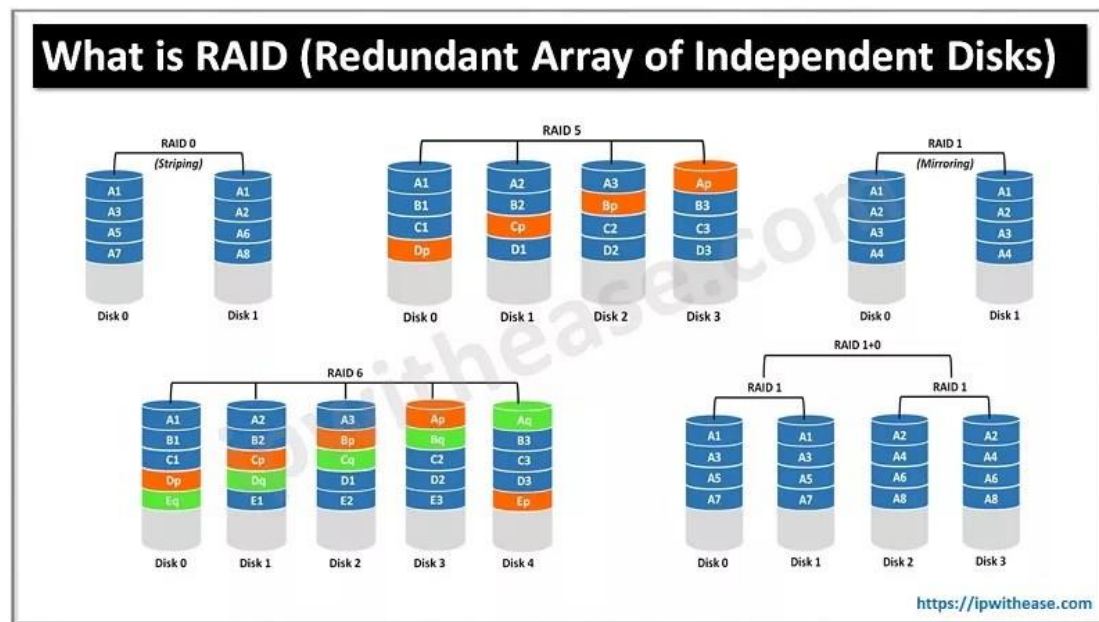
- Hình 6: Minh họa về mô hình backup

RAID (Redundant Array of Independent Disks):

RAID là một công nghệ kết hợp nhiều ổ đĩa cứng thành một hệ thống để cải thiện hiệu suất và đảm bảo tính sẵn sàng của dữ liệu. Dưới đây là một số cấu hình RAID phổ biến:

- **RAID 0 (Striping):** RAID 0 chia dữ liệu thành các phần nhỏ và lưu trữ chúng trên nhiều ổ đĩa, giúp tăng hiệu suất đọc/ghi dữ liệu. Tuy nhiên, RAID 0 không có tính năng dự phòng và nếu một ổ đĩa hỏng, dữ liệu trên toàn bộ hệ thống có thể bị mất.

- **RAID 1 (Mirroring):** RAID 1 sao lưu dữ liệu hoàn toàn lên hai ổ đĩa khác nhau. Nếu một ổ đĩa hỏng, dữ liệu vẫn được bảo toàn trên ổ đĩa còn lại. RAID 1 có tính năng dự phòng tốt nhưng hiệu suất đọc/ghi có thể thấp hơn so với RAID 0.
- **RAID 5 (Striping with Parity):** RAID 5 sử dụng kỹ thuật chia dữ liệu thành các phần nhỏ và lưu trữ thông tin dự phòng (parity) trên các ổ đĩa khác nhau. Nếu một ổ đĩa hỏng, dữ liệu vẫn có thể được khôi phục từ thông tin dự phòng. RAID 5 kết hợp tính năng dự phòng với hiệu suất tốt.
- **RAID 10 (Striping + Mirroring):** RAID 10 kết hợp cả hai phương pháp RAID 0 và RAID 1. Dữ liệu được chia thành các phần nhỏ và sau đó được sao lưu hoàn toàn lên các ổ đĩa khác nhau. RAID 10 cung cấp tính năng dự phòng và hiệu suất cao nhưng đòi hỏi nhiều ổ đĩa hơn.



- Hình 7:RAID

1.2.3 Các dịch vụ tường lửa

Firewall Fortinet là một sản phẩm chuyên về firewall và bảo mật mạng của Fortinet, một công ty hàng đầu trong lĩnh vực bảo mật mạng và giám sát mạng. Dưới đây là mô tả chi tiết về các đặc điểm và chức năng của Firewall Fortinet:

- **Đặc Điểm của Firewall Fortinet:**

Bảo Vệ Mạng: Firewall Fortinet cung cấp khả năng ngăn chặn các tấn công mạng độc hại, bao gồm tấn công từ chối dịch vụ (DDoS), tấn công

từ chối dịch vụ phân tán (DDoS), và các hình thức khác của tấn công mạng.

Tường Lửa Ứng Dụng: Fortinet Firewall kiểm tra và kiểm soát ứng dụng trên mạng, giúp ngăn chặn sử dụng các ứng dụng không an toàn hoặc không mong muốn trong môi trường mạng công ty.

VPN (Virtual Private Network): Hỗ trợ thiết lập kết nối VPN để bảo vệ thông tin và dữ liệu truyền qua mạng. Điều này cho phép người dùng từ xa hoặc các chi nhánh kết nối mạng an toàn với trung tâm dữ liệu hoặc văn phòng chính.

Quản Lý Tài Nguyên và Kiểm Soát Truy Cập: Cho phép quản trị viên thiết lập chính sách kiểm soát truy cập để quản lý quyền truy cập vào mạng, tối ưu hóa tài nguyên mạng và ngăn chặn việc sử dụng trái phép.

- Chức Năng của Firewall Fortinet:

Bảo Vệ Chống Malware: Tích hợp chức năng chống malware để ngăn chặn và phát hiện phần mềm độc hại và vi-rút trên mạng.

Bảo Mật Người Dùng Cuối: Hỗ trợ bảo vệ người dùng cuối khỏi mối đe dọa trực tuyến và giúp quản trị viên thiết lập chính sách bảo mật cho các thiết bị kết nối vào mạng.

Firewall Fortinet là một giải pháp bảo mật mạng phổ biến và mạnh mẽ được sử dụng rộng rãi trong các tổ chức để bảo vệ mạng và dữ liệu khỏi các mối đe dọa mạng.

1.2.4 Các hệ thống phát hiện xâm nhập

Hệ thống phát hiện xâm nhập (IDS) là một thành phần quan trọng trong bảo mật mạng, được triển khai để giám sát và phát hiện các hoạt động xâm nhập hoặc bất thường trong mạng. Dưới đây là một số chi tiết cụ thể về việc triển khai hệ thống IDS:

- **Lựa chọn loại IDS:**
 - **Suricata:**

Suricata là một hệ thống phát hiện xâm nhập dựa trên mã nguồn mở. Nó được phát triển bởi Open Information Security Foundation (OISF)

Là dụng cụ IDS/IPS (Intrusion Detection System / Intrusion Prevention System) phát hiện và ngăn chặn xâm nhập dựa trên luật để theo dõi lưu lượng mạng và cung ứng cảnh báo tới người quản trị hệ thống lúc có sự kiện đáng ngờ xảy ra. Nó được thiết kế để tương thích với các thành phần an ninh mạng hiện có.

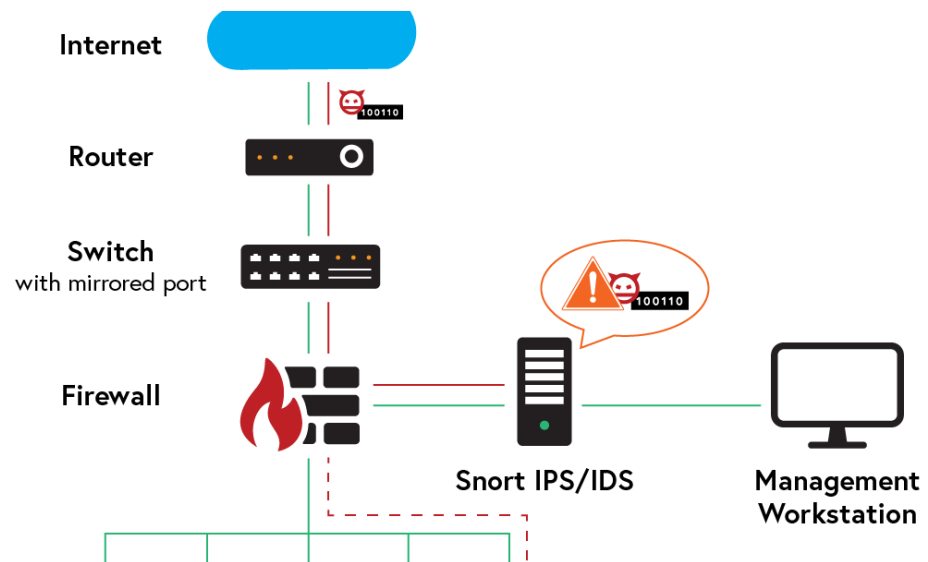


Hình 8:Suricata

Suricata là dụng cụ IDS/IPS miễn phí trong lúc nó vẫn cung ứng những lựa chọn khả năng mở rộng cho các kiến trúc an ninh mạng phức tạp nhất.

Là một dụng cụ đa luồng, Suricata cung ứng tăng vận tốc và hiệu quả trong việc phân tích lưu lượng mạng. Ngoài việc tăng hiệu quả phản ứng (với phản ứng và card mạng giới hạn), dụng cụ này được xây dựng để tận dụng khả năng xử lý cao được cung ứng bởi chip CPU đa lõi mới nhất

- **Snort:**



Hình 9: Mô hình Snort

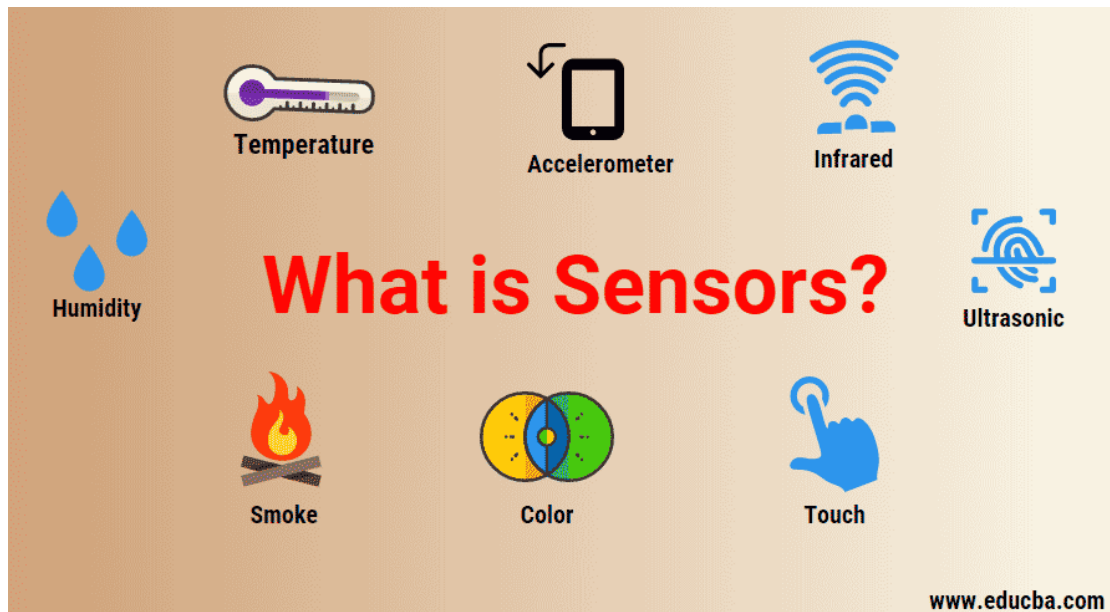
Snort là phần mềm IDS được phát triển bởi Martin Roesh dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập

Với kiến trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình

- **Triển khai các cảm biến (Sensors):**

Nếu sử dụng NIDS, cần triển khai các cảm biến ở các điểm chiến lược trong mạng như trước cửa mạng, trong mạng nội bộ và tại các biên giới mạng để thu thập dữ liệu lưu lượng mạng.

Trong trường hợp HIDS, cần cài đặt các cảm biến trực tiếp trên máy tính hoặc máy chủ cần được giám sát.



Hình 10:Hệ thống cảm biến sensors

- **Cấu hình quy tắc và chữ ký:**

Định rõ các quy tắc và chữ ký mà hệ thống IDS sẽ sử dụng để phát hiện các mẫu xâm nhập hoặc hoạt động bất thường. Các quy tắc này có thể dựa trên mẫu chuỗi, tìm kiếm byte cụ thể, hoặc thậm chí sử dụng mã hóa để phát hiện các cuộc tấn công.

- **Thiết lập cảnh báo và báo cáo:**

Cấu hình hệ thống IDS để tạo ra cảnh báo khi phát hiện các hoạt động xâm nhập hoặc bất thường. Các cảnh báo này cần được gửi đến người quản trị hoặc hệ thống quản lý bảo mật để thực hiện các biện pháp cần thiết.

Có thể thiết lập báo cáo tự động để theo dõi và phân tích các sự kiện xâm nhập trong thời gian thực và theo định kỳ.

- **Liên kết với hệ thống quản lý sự cố (SIEM):**

Liên kết hệ thống IDS với hệ thống quản lý sự cố (Security Information and Event Management - SIEM) để tự động hóa quy trình phân tích sự kiện và báo cáo.

SIEM có thể tích hợp dữ liệu từ nhiều nguồn bảo mật khác nhau và cung cấp cái nhìn toàn diện về tình trạng bảo mật của mạng.



Hình 11:SIEM

- **Cập nhật và theo dõi liên tục:**

Cập nhật các quy tắc và chữ ký IDS thường xuyên để đảm bảo khả năng phát hiện các mối đe dọa mới.

Liên tục theo dõi hoạt động của hệ thống IDS và thực hiện kiểm tra hệ thống để đảm bảo tính hiệu quả của nó.

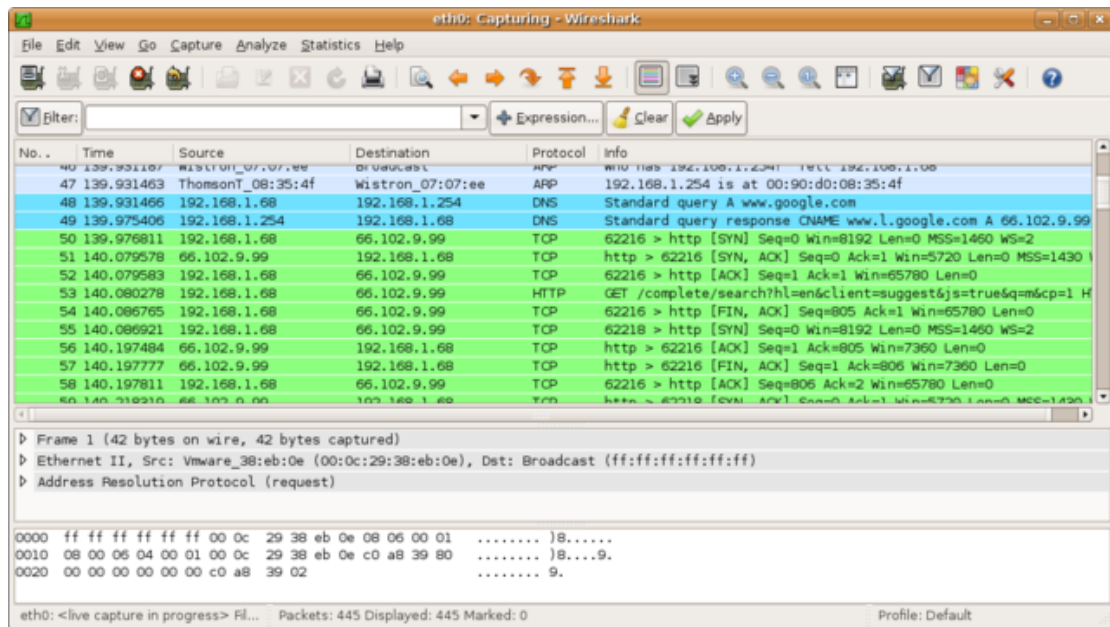
1.2.5 Các hệ thống giám sát Mạng.

Có nhiều hệ thống giám sát mạng khác nhau được sử dụng để theo dõi và quản lý mạng máy tính. Dưới đây là một số hệ thống giám sát mạng phổ biến:

-Wireshark:

Muốn biết Wireshark dùng để làm gì, cách sử dụng Wireshark như thế nào thì trước hết, điều mà chúng ta cần làm đó chính là tìm hiểu xem Wireshark là gì. Wireshark là ứng dụng phân tích mạng (network packet analyzer). Công dụng của ứng dụng này là dùng để bắt, phân tích và xác định các vấn đề có liên quan đến network bao gồm: kết nối chậm, rớt gói tin hoặc các truy cập bất thường.

Thông qua Wireshark, quản trị viên có thể hiểu hơn về các Network Packets đang chạy trên hệ thống. Như vậy, việc xác định nguyên nhân gây ra lỗi cũng sẽ dễ dàng hơn.



Hình 12:Wireshark

Phần mềm Wireshark dùng để làm gì?

Vậy Wireshark dùng để làm gì hay nói cách khác mục đích sử dụng của phần mềm là gì? Sau đây sẽ là câu trả lời dành cho bạn.

Trước hết, Wireshark được Network administrators sử dụng trong việc khắc phục sự cố về mạng.

Bên cạnh đó, Wireshark còn được các kỹ sư Network security dùng để kiểm tra các vấn đề liên quan đến bảo mật.

Trong khi đó thì Wireshark lại được các kỹ sư QA sử dụng để xác minh các network applications.

Và các developers dùng Wireshark trong việc gỡ lỗi triển khai giao thức.

Còn đối với người dùng mạng máy tính bình thường thì Wireshark giúp chúng ta học internals giao thức mạng.

Ngoài ra, Wireshark còn được sử dụng trong rất nhiều tình huống thực tế khác nữa mà chỉ những người trong giới chuyên môn mới biết câu trả lời.

- **Tính năng nổi bật của Wireshark**

Có thể thấy rằng Wireshark có rất nhiều công dụng khác nhau. Vậy còn về tính năng của chúng thì như thế nào? Sau đây hãy cùng khám phá xem những tính năng nổi bật của Wireshark là gì nhé.

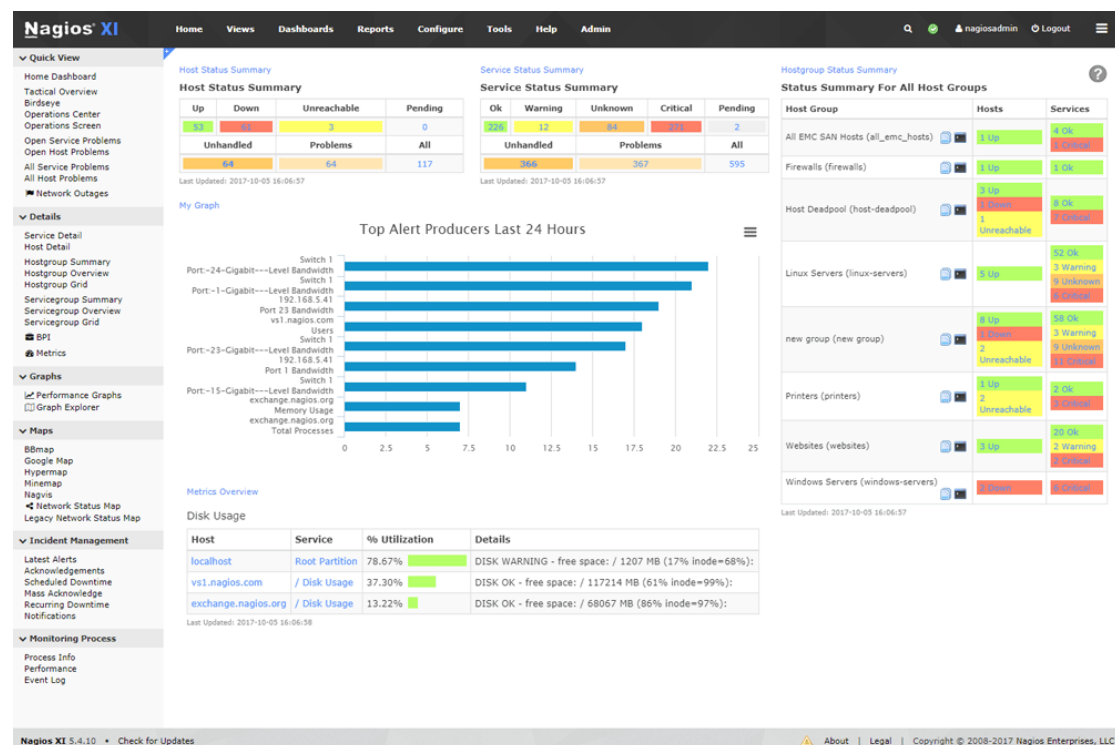
- Wireshark có sẵn cho hệ điều hành UNIX và Windows.
- Ứng dụng này giúp người dùng có thể chụp dữ liệu gói trực tiếp từ giao diện mạng.
- Thực hiện mở các tệp có chứa dữ liệu gói bằng tcpdump/ WinDump, Wireshark cũng như một số chương trình packet capture khác.
- Nhập các gói từ các tệp văn bản có chứa các hex dumps của packet data.
- Hiển thị các gói thông tin một cách vô cùng chi tiết.
- Tiến hành việc lưu trữ tất cả các dữ liệu gói đã bị bắt.
- Xuất một số hoặc tất cả các gói thông qua định dạng capture file.
- Dựa vào các tiêu chí khác nhau để lọc các gói tin.
- Dựa trên nhiều tiêu chí để tìm kiếm các gói.

-Colorize là gói hiển thị dựa trên bộ lọc.

-Wireshark còn giúp tạo các số liệu thống kê khác nhau.

Nagios:

Nagios là một phần mềm giám sát hệ thống và mạng mã nguồn mở mạnh mẽ được phát triển để giúp quản trị hệ thống và mạng kiểm tra trạng thái và hiệu suất của các tài nguyên khác nhau trong môi trường IT. Nó giúp tự động phát hiện các sự cố, cảnh báo quản trị viên và cho phép họ thực hiện các biện pháp sửa chữa kịp thời trước khi sự cố gây ra hậu quả nghiêm trọng.



Hình 13:Nagios

Dưới đây là một số đặc điểm và tính năng quan trọng của Nagios:

- Giám sát nhiều tài nguyên: Nagios có khả năng giám sát nhiều loại tài nguyên khác nhau như máy chủ, máy tính, thiết bị mạng, dịch vụ ứng dụng, và nhiều tài nguyên khác.

- Cảnh báo đa dạng: Nagios có khả năng cảnh báo qua nhiều kênh như email, SMS, thông báo trang web, và nhiều hình thức khác để quản trị viên có thể nhận thông báo sự cố kịp thời.

- Phát hiện sự cố tự động: Nagios tự động phát hiện sự cố bằng cách kiểm tra các tài nguyên theo các quy tắc đã được cấu hình, giúp ngăn chặn sự cố trước khi chúng gây ra tác động xấu đến hệ thống.

- Quản lý cơ sở dữ liệu cấu hình: Nagios sử dụng một cơ sở dữ liệu cấu hình để lưu trữ thông tin về tài nguyên cần giám sát, quy tắc kiểm tra, và cấu hình cảnh báo. Điều này giúp quản trị viên dễ dàng thay đổi cấu hình và mở rộng hệ thống giám sát.

Hiển thị trạng thái thời gian thực: Nagios cung cấp giao diện web cho phép quản trị viên xem trạng thái của các tài nguyên và dịch vụ trong thời gian thực, giúp họ nhanh chóng phát hiện và giải quyết sự cố.

- Mô-đun và tiện ích bổ sung: Nagios hỗ trợ các mô-đun và tiện ích bổ sung để mở rộng khả năng giám sát và cảnh báo. Cộng đồng người dùng và các nhà phát triển có thể tạo ra các plugin tùy chỉnh cho các nhu cầu cụ thể.

-Hỗ trợ đa nền tảng: Nagios có thể chạy trên nhiều hệ điều hành, bao gồm Linux, Unix, Windows, và nhiều hệ thống khác.

Kết luận, Nagios đã trở thành một công cụ quan trọng cho quản trị hệ thống và mạng, giúp họ duyệt qua rất nhiều thông tin về trạng thái hệ thống và cảnh báo sự cố một cách hiệu quả. Phần mềm này đã trở thành một phần không thể thiếu trong môi trường IT để đảm bảo tính ổn định và hiệu suất của hệ thống và mạng.

Zabbix:

-Zabbix là một phần mềm giám sát mạng và hệ thống mã nguồn mở mạnh mẽ và phổ biến được sử dụng để giám sát và quản lý hiệu suất của các tài nguyên trong môi trường IT. Nó cung cấp các tính năng mạnh mẽ cho việc theo dõi và cảnh báo, giúp tự động phát hiện sự cố và cung cấp thông tin hữu ích cho quản trị viên hệ thống và mạng. Dưới đây là một số điểm nổi bật về Zabbix:

-Kiểm tra đa dạng: Zabbix cho phép quản trị viên giám sát nhiều loại tài nguyên khác nhau, bao gồm máy chủ, máy tính, thiết bị mạng, ứng dụng, cơ sở dữ liệu, và nhiều hệ thống khác.

-Cảnh báo linh hoạt: Zabbix cung cấp khả năng cảnh báo dựa trên nhiều nguồn thông báo như email, SMS, Slack, và nhiều kênh khác. Quản trị viên

có thể cấu hình các ngưỡng cảnh báo tùy chỉnh dựa trên các yếu tố như giờ làm việc, ngày nghỉ, và ưu tiên.

-Phát hiện sự cố tự động: Zabbix tự động phát hiện sự cố và theo dõi hiệu suất dựa trên các quy tắc cấu hình, giúp ngăn chặn sự cố trước khi chúng gây ra tác động xấu đến hệ thống.

-Giao diện web đa chức năng: Zabbix cung cấp một giao diện web thân thiện và đa chức năng cho phép quản trị viên xem trạng thái của các tài nguyên và dịch vụ trong thời gian thực, tạo và cấu hình báo cáo, và thực hiện quản lý hệ thống.

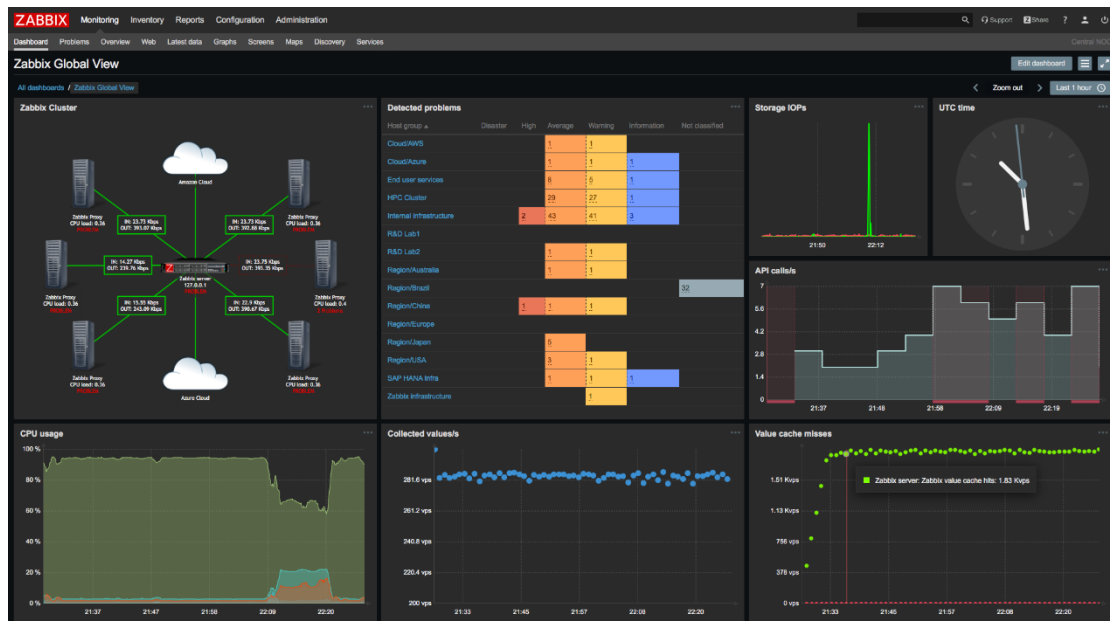
-Tích hợp linh hoạt: Zabbix hỗ trợ tích hợp với nhiều ứng dụng và dịch vụ khác nhau, cho phép bạn thu thập thông tin từ nhiều nguồn khác nhau và tùy chỉnh các tương tác với các ứng dụng và thiết bị.

-Bảo mật cao: Zabbix có các tính năng bảo mật mạnh mẽ như quyền truy cập dựa trên vai trò, mã hóa dữ liệu, và cơ chế xác thực mạnh mẽ để bảo vệ thông tin quan trọng.

-Hỗ trợ đa nền tảng: Zabbix có thể chạy trên nhiều hệ điều hành như Linux, Unix, Windows, và nhiều nền tảng khác.

-Zabbix đã trở thành một công cụ quan trọng trong việc quản lý và giám sát hệ thống và mạng trong các môi trường doanh nghiệp. Nó giúp đảm bảo

tính ổn định và hiệu suất của hệ thống, giúp quản trị viên phát hiện và giải quyết sự cố kịp thời.



Hình 14:Zabbix

PRTG Network Monitor:

-SolarWinds Network Performance Monitor (NPM): NPM của SolarWinds là một giải pháp thương mại mạnh mẽ cho việc giám sát mạng. Nó cung cấp phân tích lưu lượng mạng, cảnh báo, và quản lý hiệu suất.

-Splunk: Splunk không chỉ giám sát mạng mà còn phân tích dữ liệu từ nhiều nguồn khác nhau. Nó có khả năng xây dựng các trang tổng hợp dữ liệu mạng và tạo cảnh báo dựa trên sự kiện.

-Prometheus: Prometheus là một hệ thống giám sát mã nguồn mở chuyên dụng cho các môi trường đám mây và ứng dụng phân tán. Nó chủ yếu được sử dụng cho giám sát hệ thống và ứng dụng, nhưng cũng có thể được sử dụng để giám sát mạng.

-Những hệ thống giám sát này có những đặc điểm riêng biệt và phù hợp với các môi trường và yêu cầu sử dụng khác nhau. Lựa chọn hệ thống phù hợp phụ thuộc vào quy mô mạng của bạn, tính năng cần thiết, và nguồn kinh phí có sẵn.



Hình 15:PRTG Network Monitoring

Chương 2: LÊN KẾ HOẠCH TRIỂN KHAI

2 Lên kế hoạch triển khai

2.1 Thiết kế hệ thống

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

Phần mềm tường lửa:

- **Fortigate/Fortinet:**

- Phần mềm PfSense là giải pháp tường lửa và bộ định tuyến mã nguồn mở dựa trên hệ điều hành FreeBSD. Thích hợp cho các công ty vừa và nhỏ, PfSense cung cấp giải pháp bộ định tuyến và tường lửa chuyên dụng, chi phí thấp cho các mạng máy tính ảo và vật lý.
- Phần mềm này có thể chạy trên máy tính vật lý hoặc máy tính ảo, cung cấp nhiều tính năng mạnh mẽ, gần giống với những gì mà các thiết bị tường lửa thương mại cung cấp. Nó cũng hỗ trợ các giải pháp của bên thứ ba khác như Squid, Snort và các giải pháp khác để tăng thêm khả năng của nó

Phần mềm phát hiện xâm nhập:

- **Snort**

- Snort là Hệ thống ngăn chặn xâm nhập mã nguồn mở (IPS) hàng đầu trên thế giới. Snort IPS sử dụng một loạt các quy tắc giúp xác định hoạt động mạng độc hại và sử dụng các quy tắc đó để tìm các gói phù hợp với chúng và tạo cảnh báo cho người dùng.
- Snort cũng có thể được triển khai nội tuyến để ngăn chặn các gói này. Snort có ba cách sử dụng chính: Là một bộ dò tìm gói tin như tcpdump, như một bộ ghi gói tin — rất hữu ích cho việc gỡ lỗi lưu lượng mạng hoặc nó có thể được sử dụng như một hệ thống ngăn chặn xâm nhập mạng toàn diện. Snort có thể được tải xuống và định cấu hình để sử dụng cho mục đích cá nhân và doanh nghiệp.

Phần mềm giám sát quá trình thực hiện:

- **Glances**

- Glances là một công cụ giám sát đa nền tảng nhằm mục đích trình bày tối đa thông tin trong một không gian tối thiểu thông qua giao diện dựa trên web hoặc lời nguyên. Nó có thể tự động điều chỉnh thông tin được hiển thị tùy thuộc vào kích thước thiết bị đầu cuối.

- Nó cũng có thể hoạt động ở chế độ máy khách/máy chủ. Giám sát từ xa có thể được thực hiện thông qua thiết bị đầu cuối, giao diện Web hoặc API (XMLRPC và RESTful). Glances được viết bằng Python và sử dụng thư viện psutil để lấy thông tin từ hệ thống của bạn.

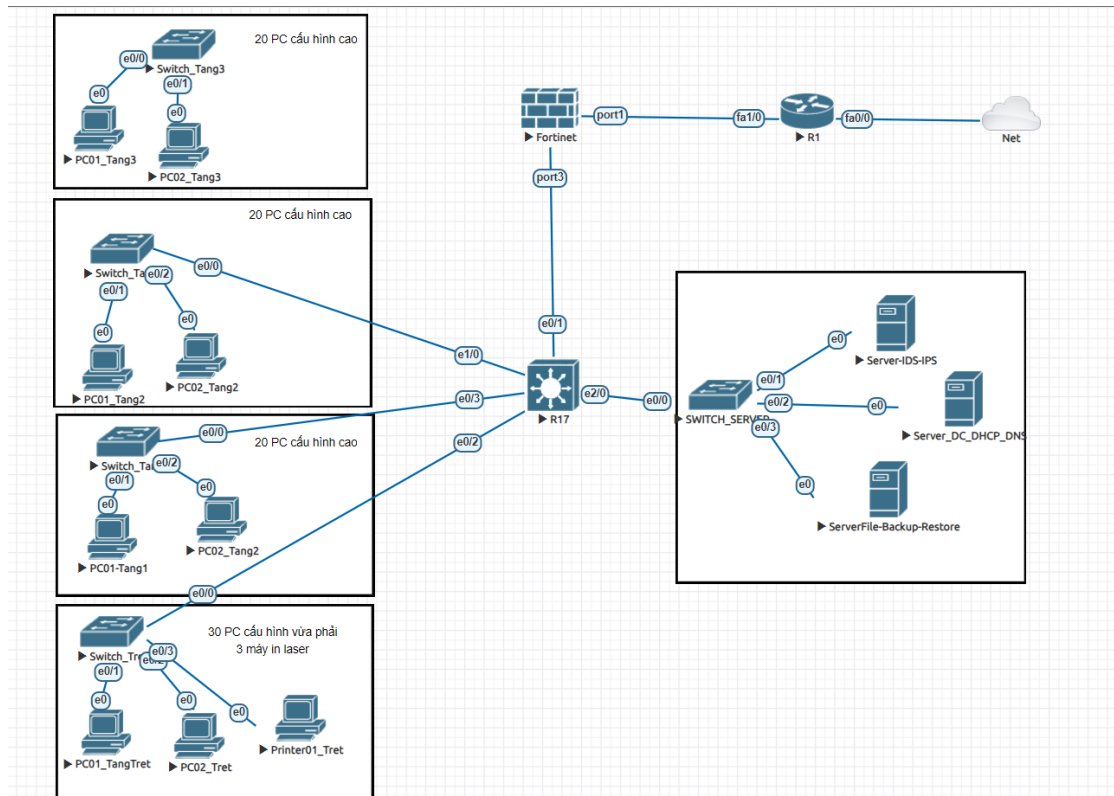
2.1.2 Thiết bị cần có

Để có thể triển khai được một hệ thống dành cho Viện Giáo Dục Quốc Tế HUFLIT thì cần có:

- Tầng trệt gồm:
 - 35 máy tính cơ bản
 - 3 máy in
- Tầng 1 gồm:
 - Phòng LAB: 20 máy tính
- Tầng 2 gồm:
 - Phòng LAB: 20 máy tính
- Tầng 3 gồm:
 - Phòng LAB: 20 máy tính

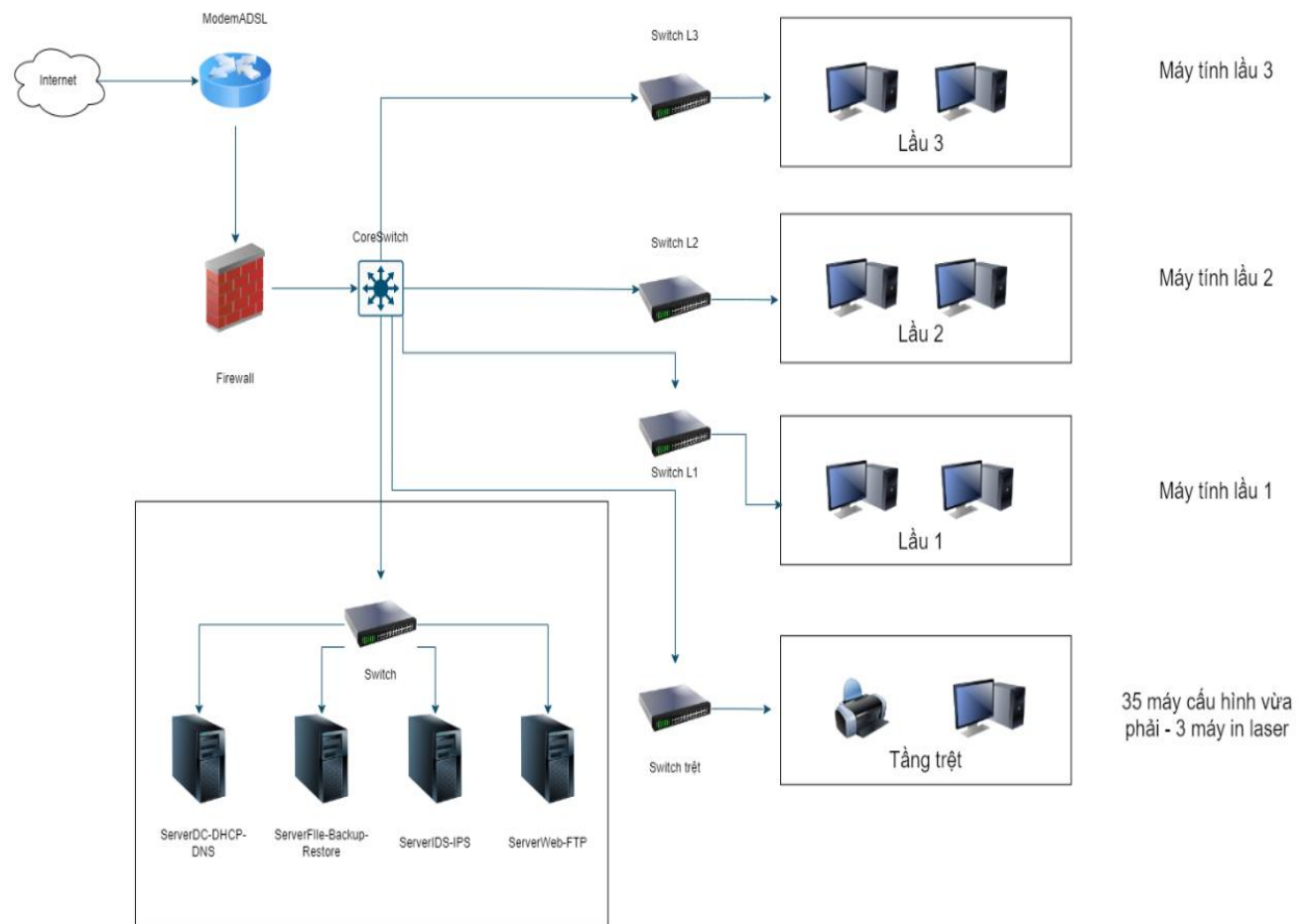
2.1.3 Logical topology và Physical topology, IP Table.

Logical topology



Hình 16:Sơ đồ logic

Physical topology



Hình 17:Sơ đồ vật lý

IP Table.

Lầu	Thiết bị	IP	Subnet Mask	Default Gateway
Trệt	6 server phòng máy	192.168.1.11- 75	255.255.255.224	192.168.0.70
Trệt	1 server DHCP, Firewall, ANTIVIRUS	192.168.1.1-10	255.255.255.224	192.168.0.1
Trệt	35 máy nhân viên	192.168.1.100- 155	255.255.255.224	192.168.0.150
Trệt	3 máy in	192.168.1.156- 165	255.255.255.224	192.168.0.160
1	20 máy tính phòng lab	192.168.1.200- 230	255.255.255.224	192.168.0.220
2	20 máy phòng lab	192.168.1.240- 270	255.255.255.224	192.168.0.260
3	20 máy phòng lab	192.168.1.280-310	255.255.255.224	192.168.0.300

2.2 Đánh giá và kiểm chứng kế hoạch

- Mục Tiêu Kế Hoạch:

Mô tả mục tiêu của kế hoạch: Triển khai và xây dựng hệ thống mạng cho Viện Giáo Dục Quốc Tế Huflit, cũng như thiết lập, bảo trì, bảo vệ hệ thống cho kế hoạch tránh những mối nguy hiểm ảnh hưởng đến dự án, và cũng như Viện Giáo Dục.

- Quá Trình Thực Hiện:

Các hoạt động đã thực hiện: do thời gian có hạn nên chúng em tạm thời vừa hoàn thành xong phần cấu hình DHCP, DNS, Firewall và Ping thành công giữa các máy phòng ban khác nhau.

Thời gian thực hiện: Thời gian đã được chúng em tải lên Planner, kế hoạch và thời gian rõ ràng.

Tài nguyên sử dụng: Hệ thống giải lập EVE-NG.

- Đánh giá kết quả:

Các kết quả chính: Còn những chức năng còn lại chúng em đang tiến hành thực hiện và sớm hoàn thành.

Chương 3: TRIỂN KHAI

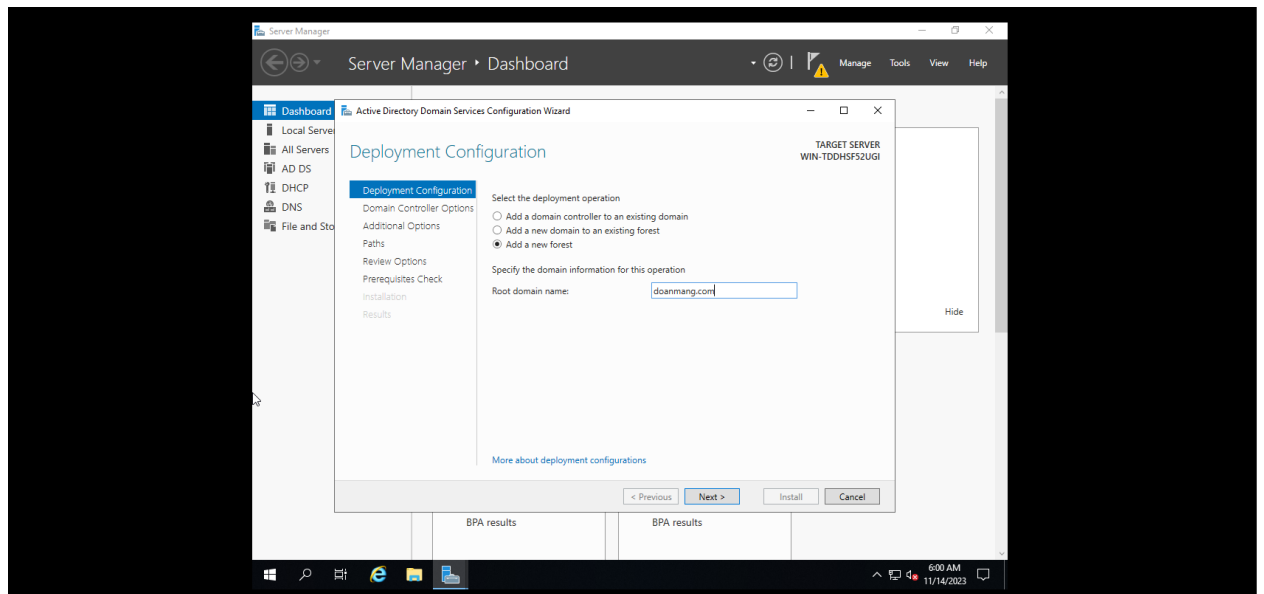
3 Triển khai

3.1 Triển khai setup hệ thống

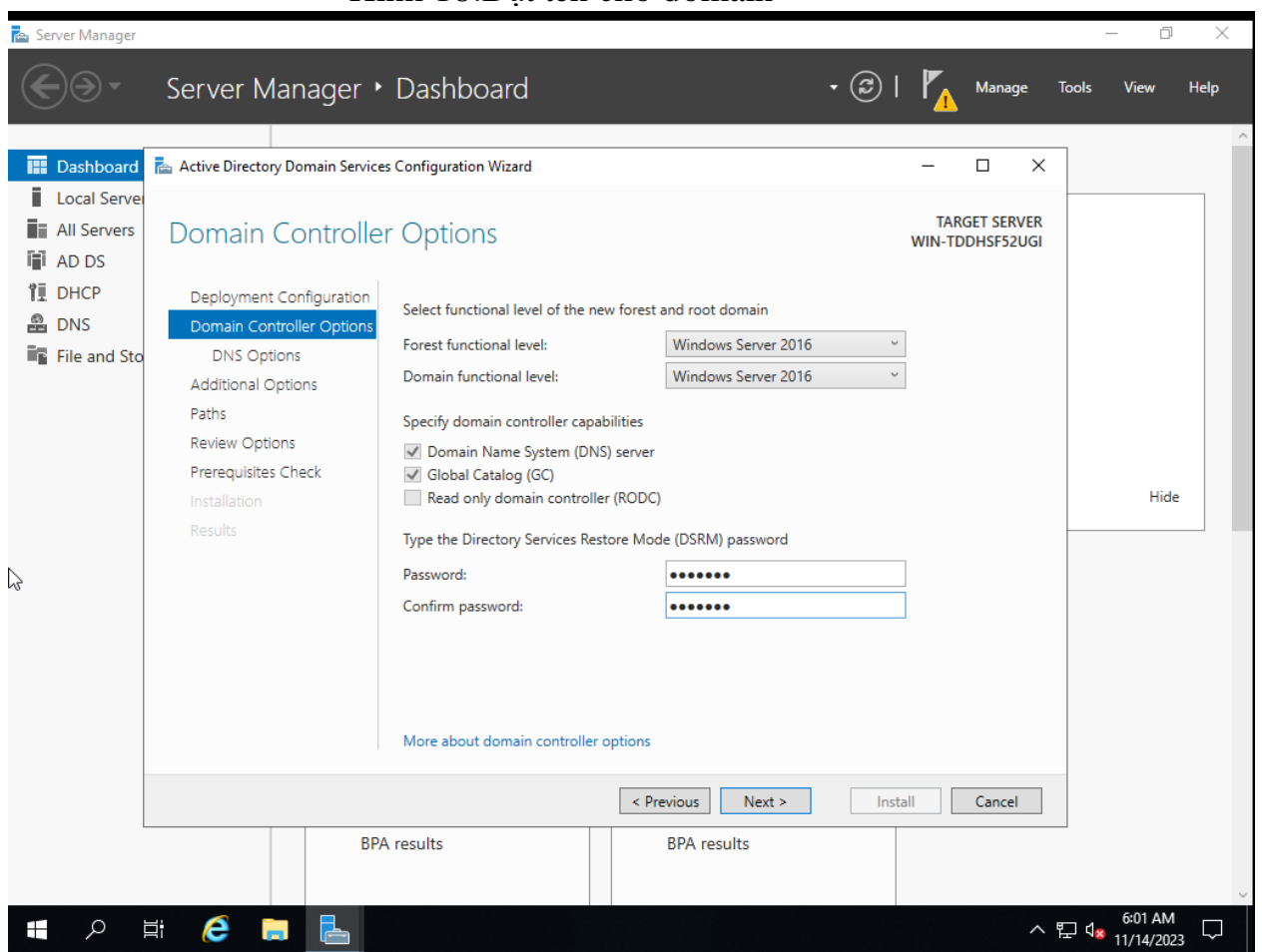
a. Triển khai Domain Controller

Domain Controller là một thành phần quan trọng trong hệ thống Active Directory (AD) của Microsoft. Domain Controller là máy chủ chạy hệ điều hành Windows Server và được cấu hình để chứa và quản lý thông tin xác thực, quản lý tài khoản người dùng, nhóm, và các đối tượng khác trong một mạng doanh nghiệp dựa trên Active Directory.

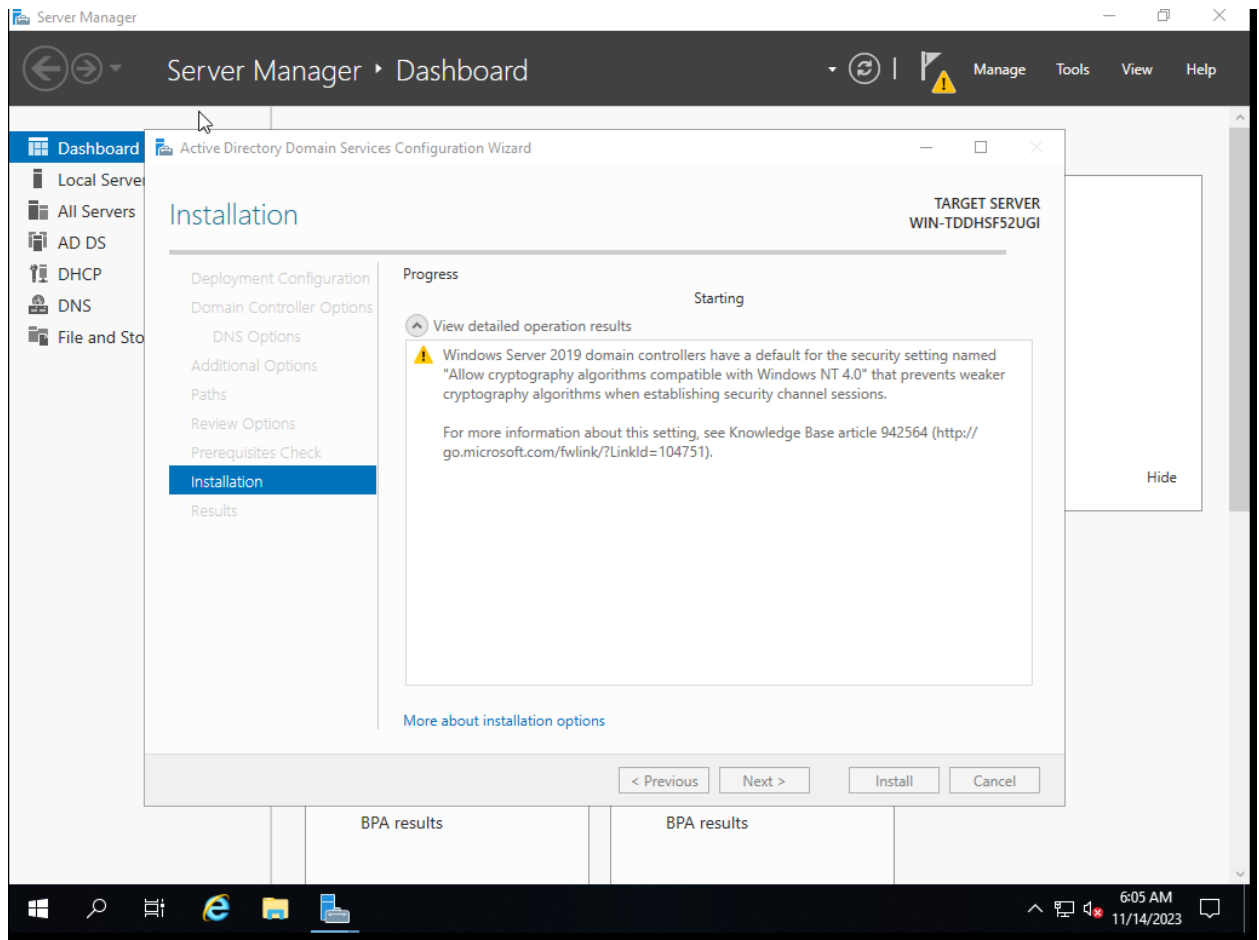
Tóm lại, Domain Controller là một phần quan trọng trong hệ thống Active Directory của Microsoft, đóng vai trò trong việc quản lý tài khoản, quyền truy cập, xác thực và tích hợp dữ liệu trong mạng doanh nghiệp, giúp tổ chức quản lý dễ dàng và bảo vệ thông tin người dùng. Dưới đây, chúng em sẽ tóm tắt lại những bước để tạo ra một Domain Controller.



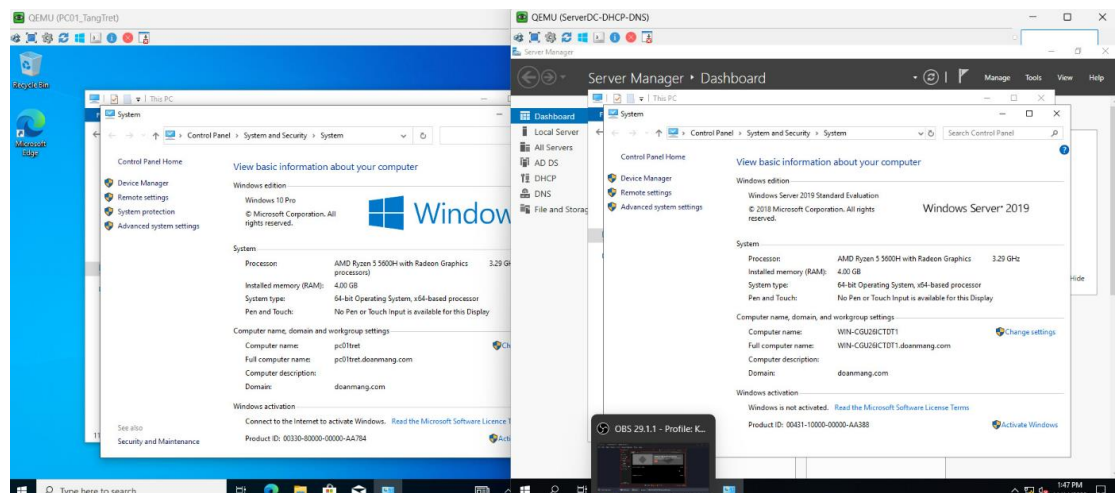
Hình 18:Đặt tên cho domain



Hình 19:Nhập mật khẩu cho Domain



Hình 20: Hoàn thành cài đặt domain

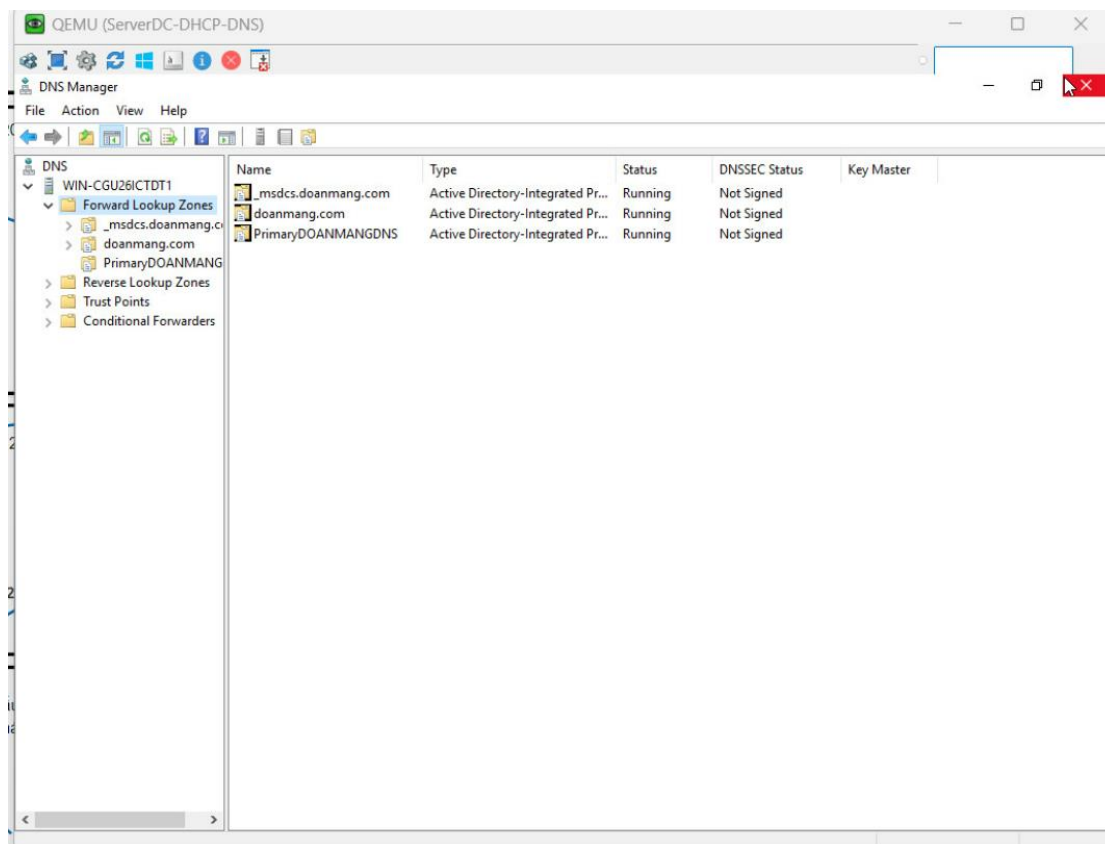


Hình 21: Sau khi đã cài đặt và join domain

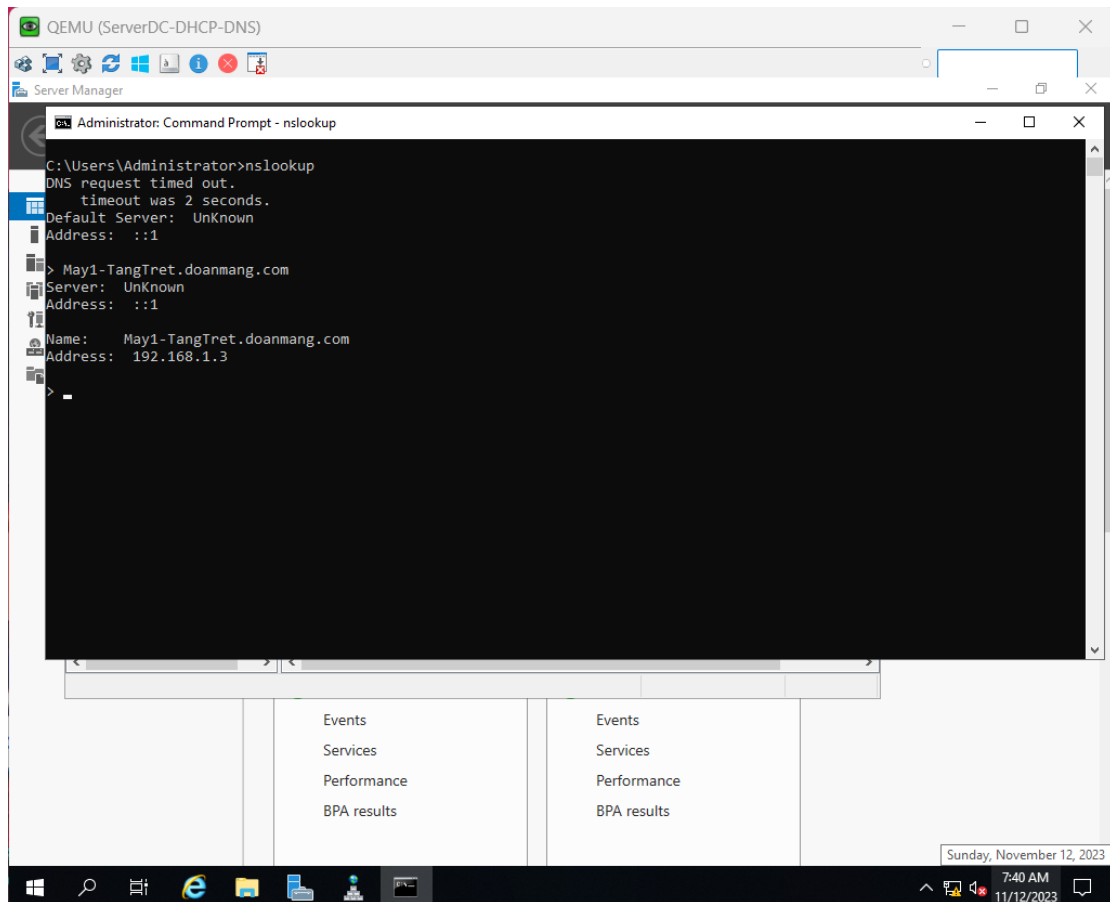
b. DNS Server

DNS là viết tắt của "Domain Name System", DNS là một hệ thống phân giải tên miền thành địa chỉ IP và ngược lại. Nó là một dịch vụ quan trọng trong cơ sở hạ tầng internet và giúp các máy tính trên mạng liên kết với nhau thông qua tên miền thay vì địa chỉ IP.

Tóm lại, DNS là hệ thống quan trọng trong internet cho phép người dùng sử dụng tên miền để nhớ thay vì địa chỉ IP, và nó có nhiều công dụng quan trọng như phân giải tên miền, tạo cấu trúc hệ thống, cân bằng tải, bảo mật và quản lý tên miền.



Hình 22:Cấu hình DNS



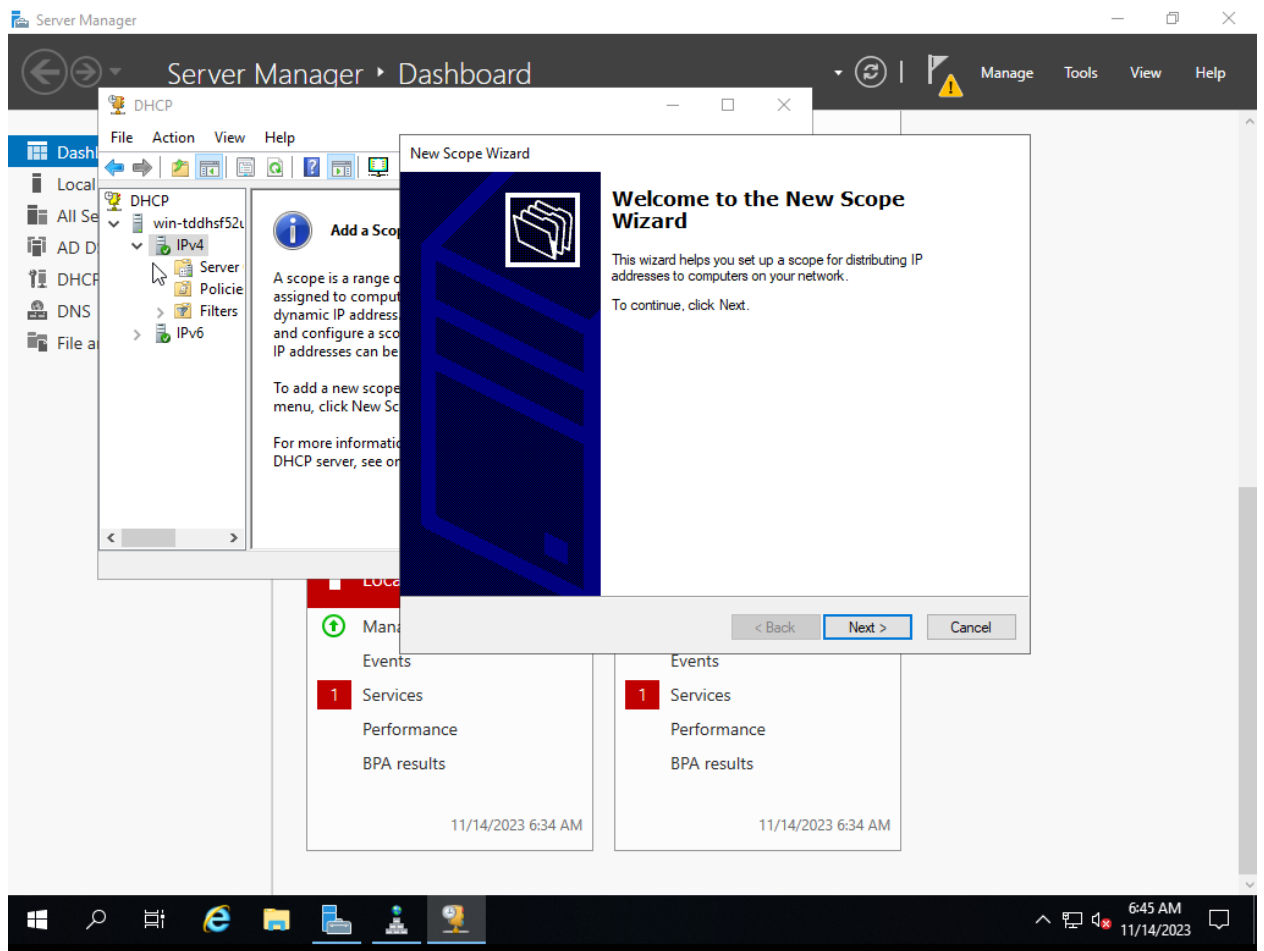
Hình 23: Test thử

c. Cấu hình DHCP

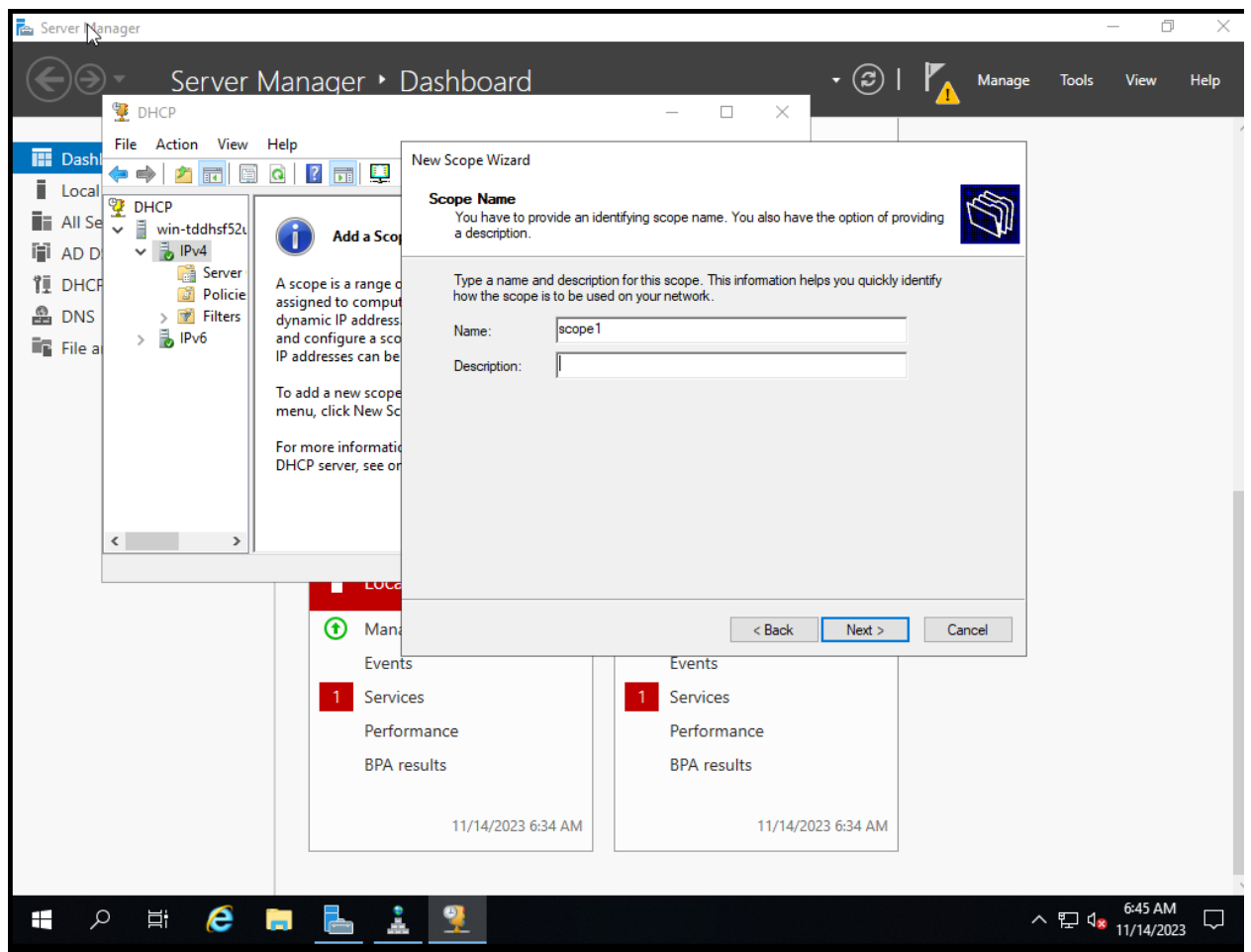
DHCP (Dynamic Host Configuration Protocol) là một giao thức trong mạng máy tính dùng để tự động cấu hình các thông số mạng cho các thiết bị kết nối vào mạng. DHCP là một giao thức mạng dùng để cấp phát địa chỉ IP, cổng mặc định và các thông số liên quan khác cho các thiết bị trong mạng một cách tự động và động.

Tóm lại, DHCP là một giao thức quan trọng trong mạng máy tính cho phép tự động cấu hình các thông số mạng cho các thiết bị, giúp quản lý mạng dễ

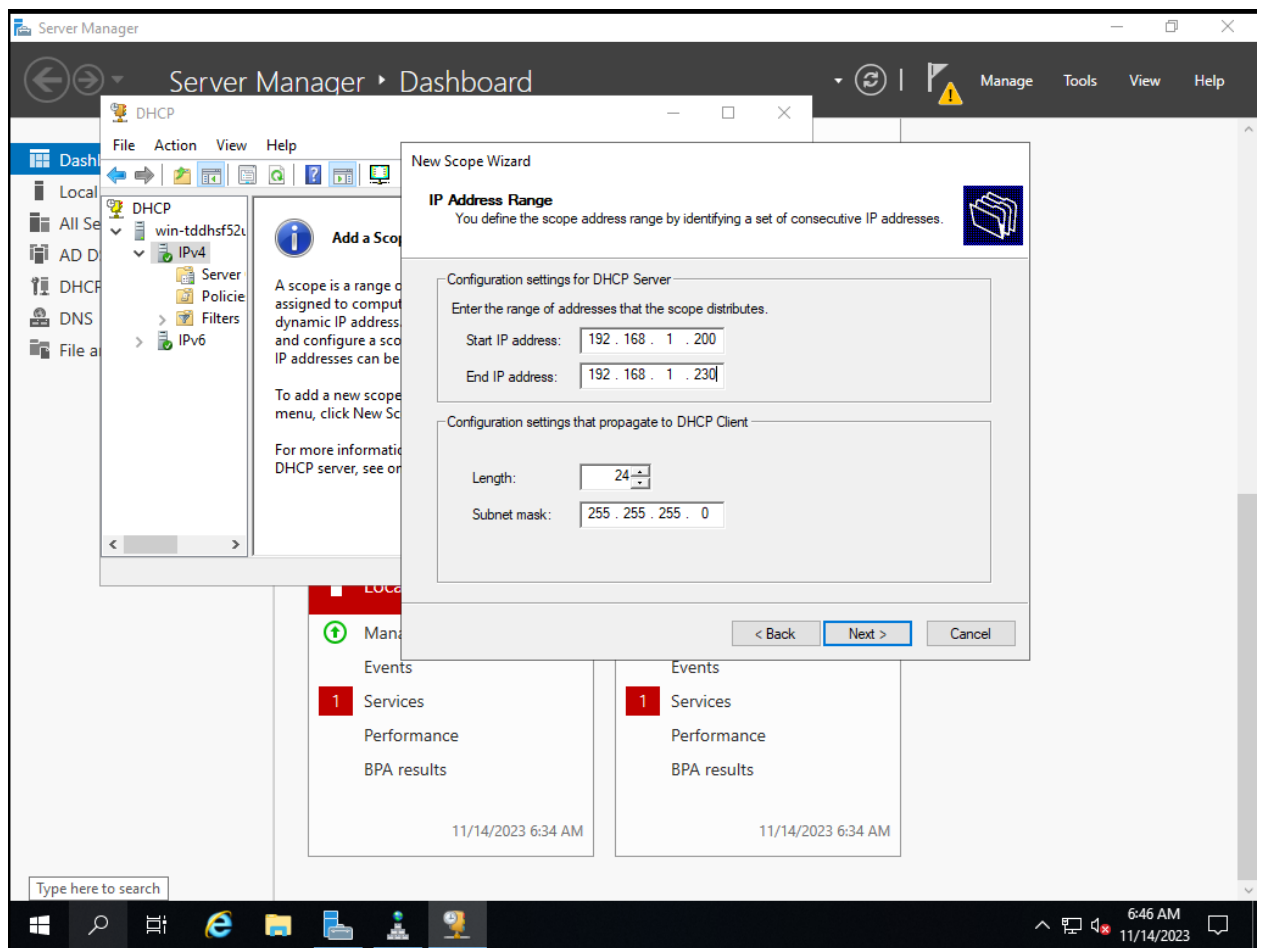
dàng hơn và tối ưu hóa việc sử dụng địa chỉ IP trong mạng.viên theo dõi
và báo cáo về tình trạng bảo mật mạng



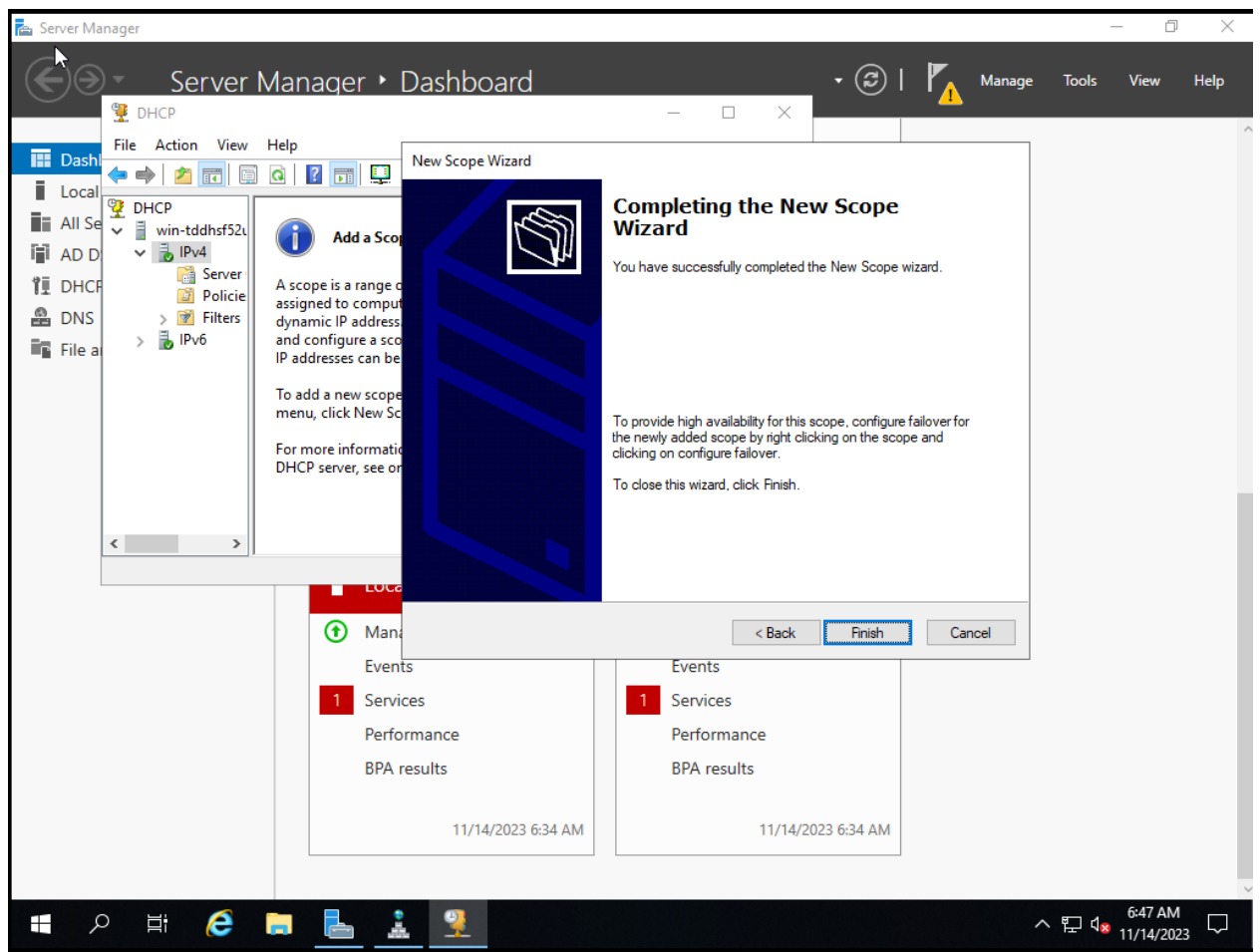
Hình 24:Tiến hành tạo 1 scope mới



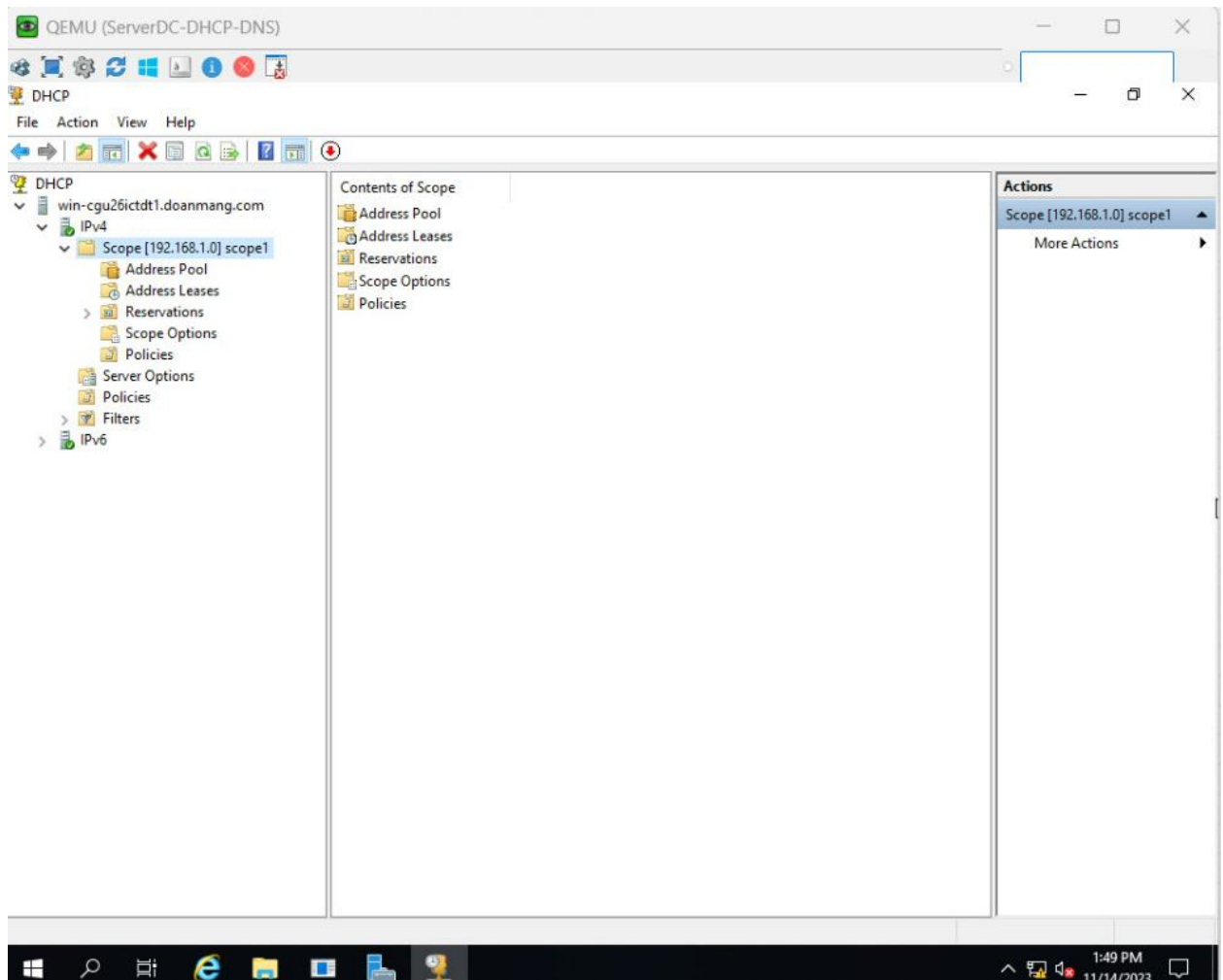
Hình 25:Đặt tên và ghi chú cho scope



Hình 26:Nhập khoảng địa chỉ IP cung cấp



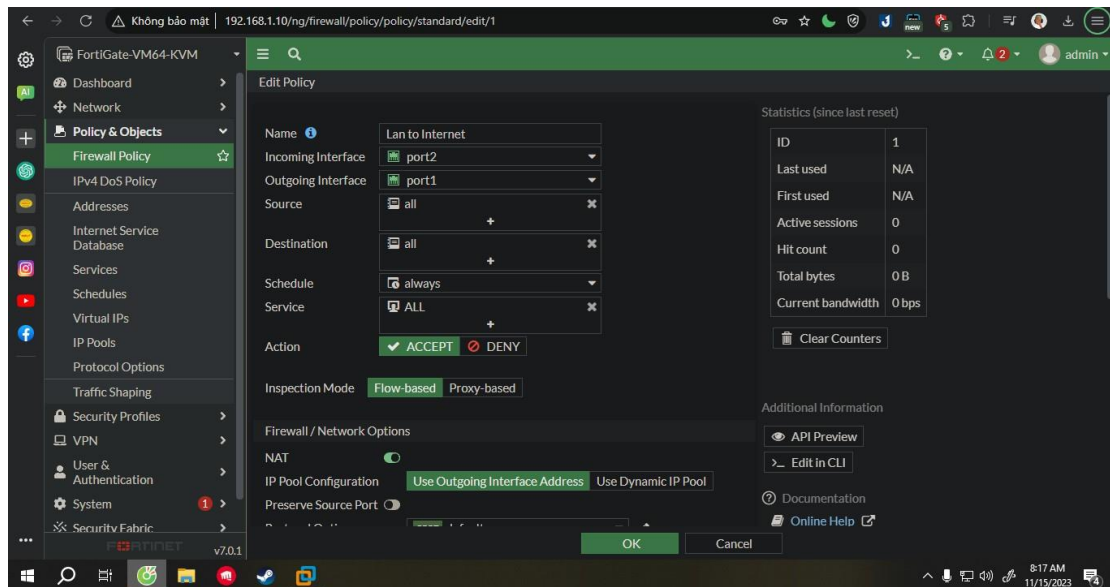
Hình 27: Hoàn thành tạo Scope



Hình 28: Sau khi đã tạo scope

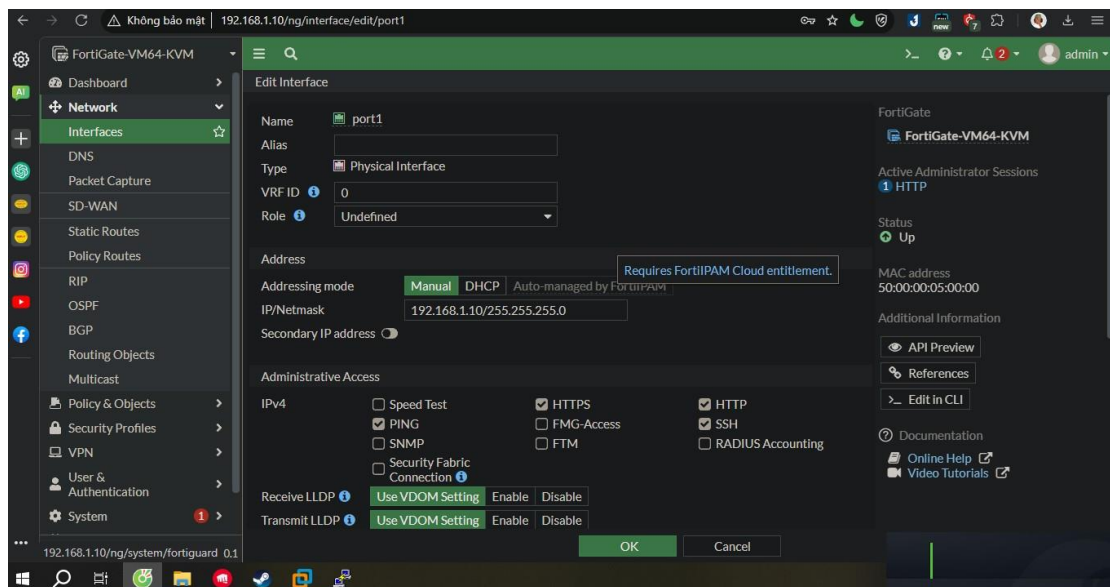
d. Firewall (Fortinet)

Firewall Fortinet là một giải pháp bảo mật mạng. Firewall Fortinet là một loại firewall (tường lửa) chuyên nghiệp và mạnh mẽ được phát triển bởi Fortinet. Nó cung cấp các giải pháp bảo mật mạng để bảo vệ các tổ chức khỏi các mối đe dọa trực tuyến và tấn công mạng.

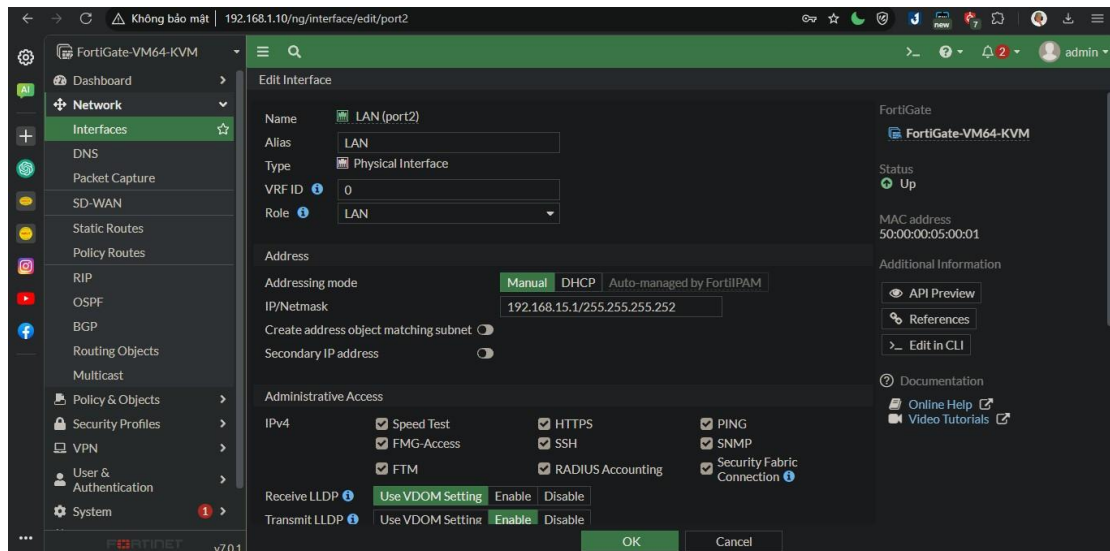


Hình 29: Tạo rule cho firewall ra internet

Tóm lại, Firewall Fortinet là một giải pháp bảo mật mạng mạnh mẽ được thiết kế để bảo vệ mạng và dữ liệu của tổ chức khỏi các mối đe dọa trực tuyến và tấn công mạng, kiểm soát quyền truy cập, và giúp quản trị



Hình 30: Cấu hình port1



Hình 31: Cấu hình port2

e. Backup và Restore

Backup và restore trên Windows Server là quá trình tạo bản sao lưu (backup) của dữ liệu và hệ thống và khôi phục (restore) chúng khi cần thiết. Backup giúp đảm bảo an toàn dữ liệu, trong khi restore cho phép khôi phục dữ liệu sau khi mất mát hoặc khi có sự cố. Quá trình này giữ cho hệ thống ổn định và giảm thiểu rủi ro mất dữ liệu quan trọng trên máy chủ chạy hệ điều hành Windows Server.

f. IDS(McAfee)

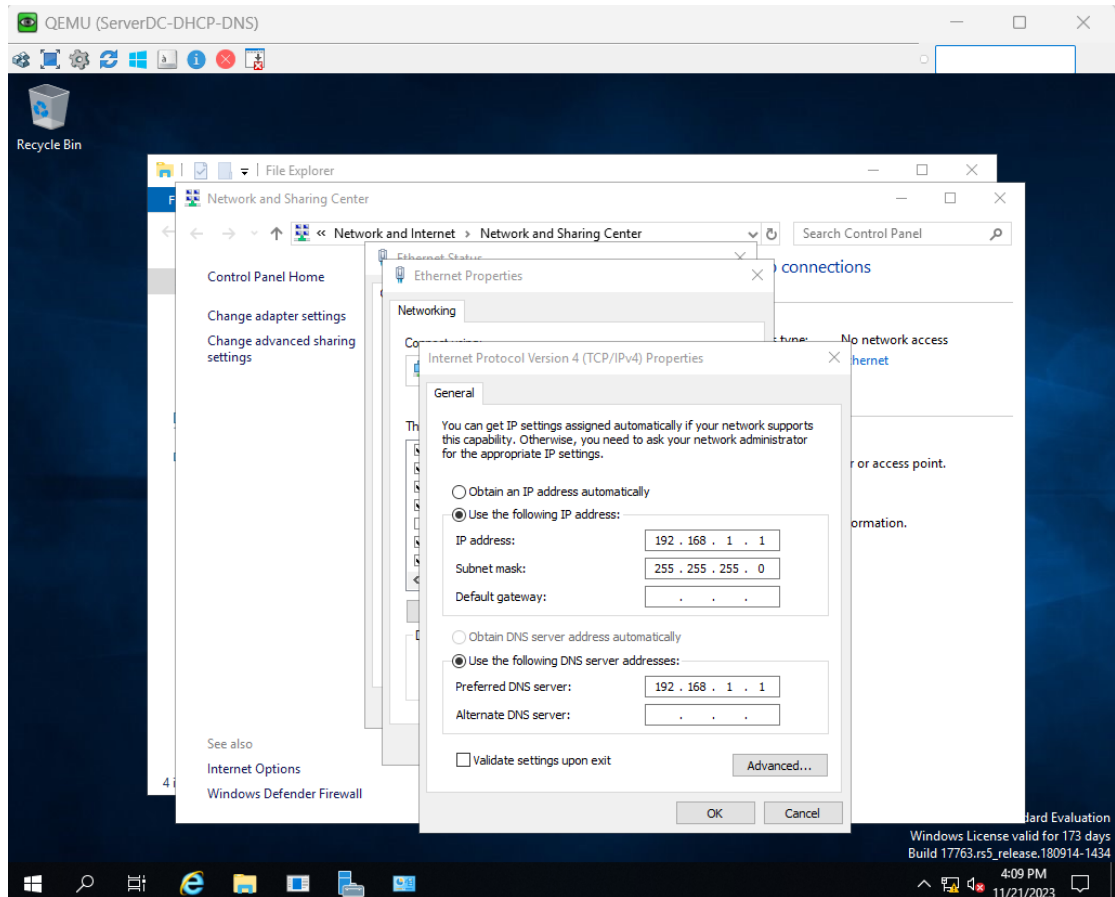
IDS (Intrusion Detection System) là một hệ thống giám sát và phát hiện xâm nhập vào mạng. Một số công ty an ninh mạng, bao gồm McAfee, cung cấp giải pháp IDS để bảo vệ hệ thống và dữ liệu khỏi các mối đe dọa bảo mật. IDS theo dõi lưu lượng mạng và hành vi của hệ thống để phát hiện các hoạt động đáng ngờ, có thể là dấu hiệu của một tấn công mạng.



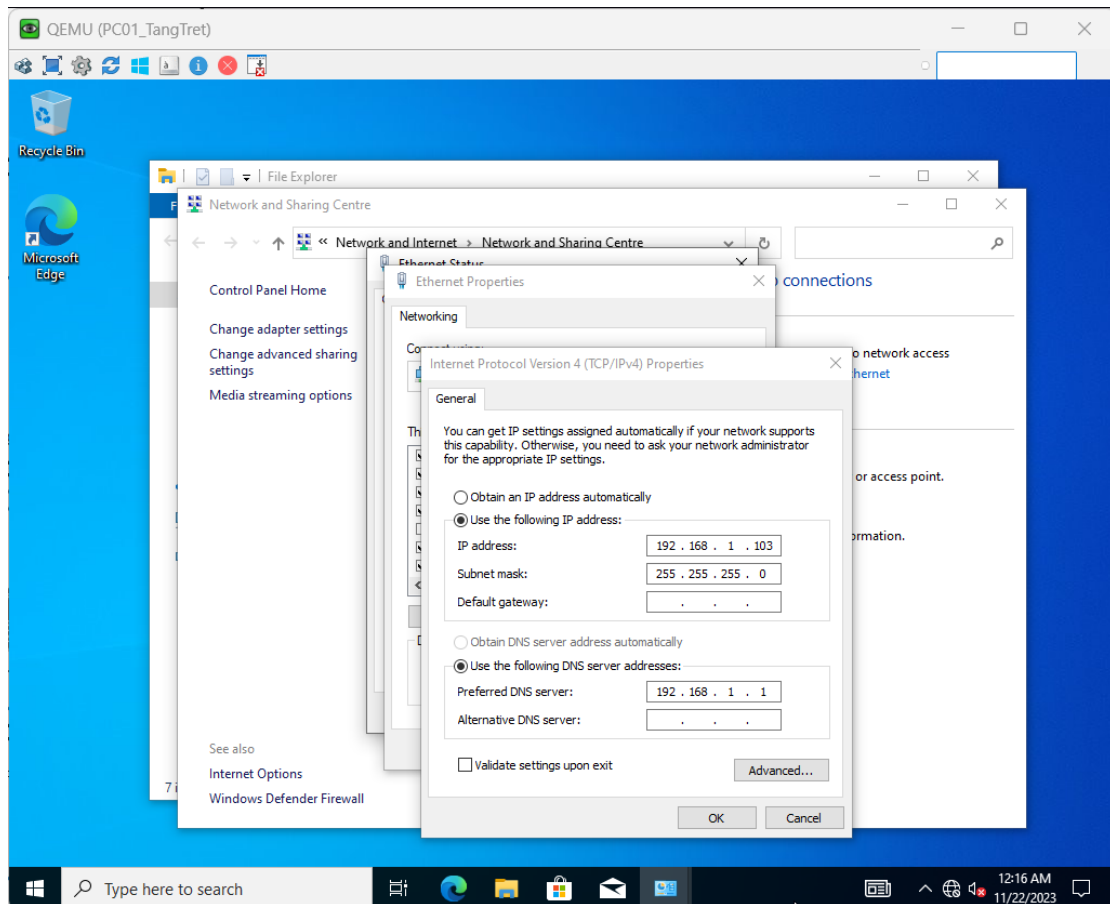
Hình 32:McAfee

McAfee IDS là một phần của các giải pháp bảo mật của McAfee, nhằm giúp ngăn chặn, phát hiện và đối phó với các mối đe dọa mạng. Các sản phẩm McAfee IDS có thể cung cấp cảnh báo và bản ghi chi tiết về các sự kiện xâm nhập có thể xảy ra trong môi trường mạng, giúp quản trị viên hệ thống nắm bắt thông tin quan trọng và đưa ra các biện pháp phòng ngừa.

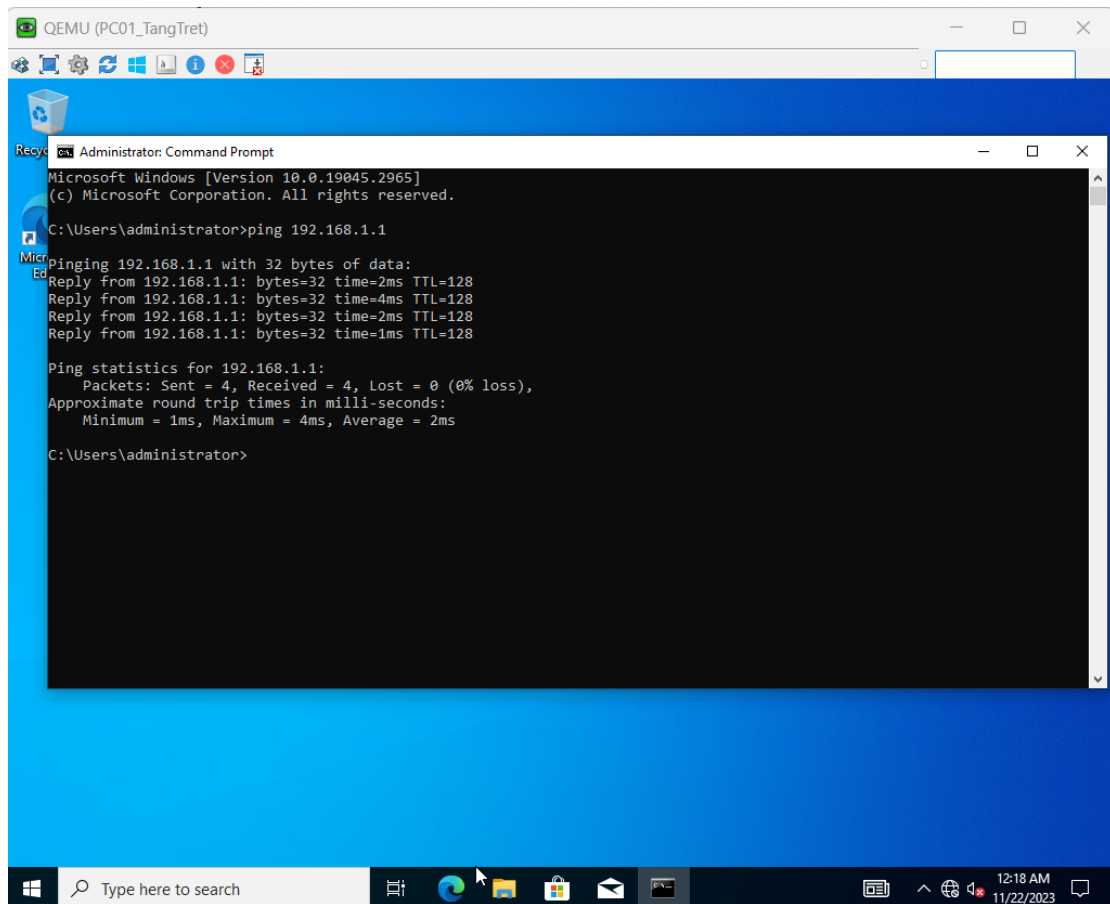
3.2 Cấu hình và test lỗi



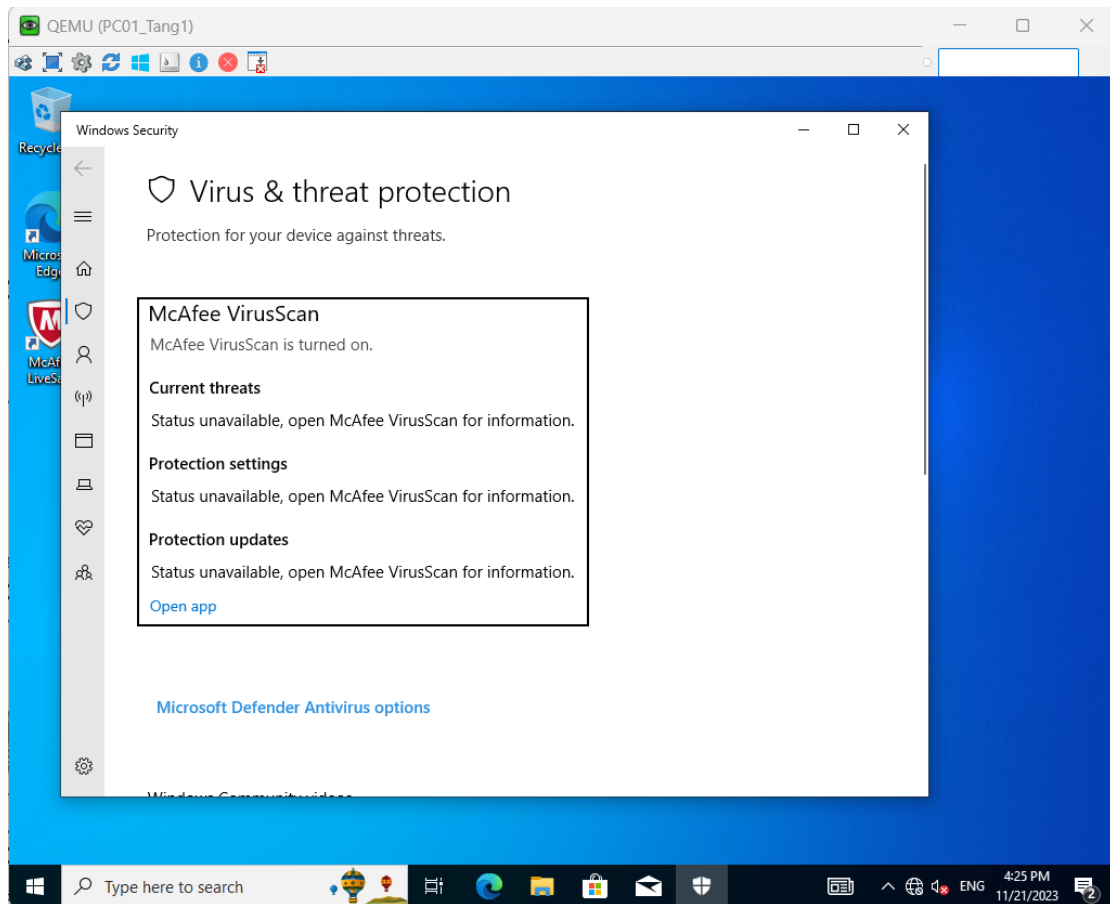
Hình 33:Cấu hình máy Server



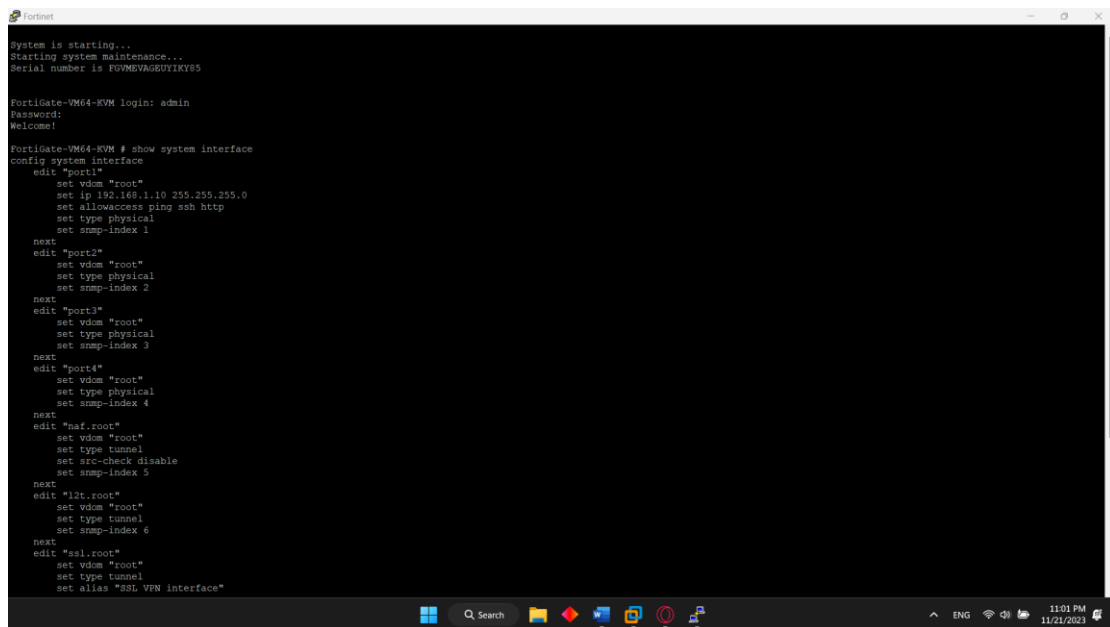
Hình 34:Cấu hình máy Client



Hình 35: Ping tới Server



Hình 36:IDS



Hình 37:Cấu hình Firewall

3.3 Đánh giá kết quả thực hiện

Đánh giá xây dựng dự án " XÂY DỰNG HỆ THỐNG MẠNG CHO VIỆN
GIÁO DỤC QUỐC TẾ HUFLIT "

- Ngày: 15/11/2023

- Sinh viên:

- Phạm Đức Thiên Phúc
- Nguyễn Công Khang
- Nguyễn Minh Đức

Dưới đây là bản đánh giá về việc thực hiện dự án này.

Mục tiêu dự án:

Dự án đã đề ra mục tiêu cụ thể, bao gồm:

- 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.

Thực hiện mục tiêu

- Tiến độ thực hiện: Dự án đã hoàn thành đúng tiến độ đã lên kế hoạch.

Mọi công việc đã được thực hiện theo lịch trình và không có sự trễ hẹn nào.

- Chất lượng dự án: Hệ thống được xây dựng với chất lượng cao, đảm bảo an toàn cho các phòng lab và những phòng khác. Kiểm tra chất lượng đã được thực hiện thường xuyên, và không có sự cố nghiêm trọng nào xảy ra, cũng như không thể xâm nhập hoặc đánh mất thông tin.

- Ngân sách: Dự án đã được thực hiện trong ngân sách đã đề ra ban đầu. Không có vấn đề về quản lý tài chính hoặc vượt quá kinh phí.

- Tuân thủ quy định: Dự án đã tuân thủ các quy định về an toàn thông tin và bảo mật hệ thống cho Viện Giáo Dục. Không có vi phạm nào về mặt pháp lý hoặc quy định.

Đánh giá tổng quan:

- Dự án "Xây dựng hệ thống mạng cho viện giáo dục quốc tế HUFLIT" đã thực hiện một cách xuất sắc và đáp ứng được mục tiêu đã đề ra. Nó đã tạo ra một hệ thống mới, an toàn và chất lượng cho cộng đồng, và đã quản lý tài chính một cách hiệu quả. Dự án này đã hoàn thành đúng tiến độ và đạt chất lượng cao, đáng để ghi nhận và khen ngợi.

Đề xuất cải tiến (nếu cần):

- Vì thời gian có hạn nên chúng em sẽ sớm hoàn thành và hoàn tất những bước tiếp theo, cũng như nộp dự án đúng theo yêu cầu và thời gian

- Dựa trên kết quả thực hiện dự án, không có đề xuất cải tiến cụ thể nào.

Tuy nhiên, việc duyệt xem chất lượng và bảo trì công trình là cần thiết để đảm bảo rằng nó vẫn đáp ứng được yêu cầu trong tương lai.

Chương 4: QUẢN TRỊ HỆ THỐNG

4 Quản trị hệ thống

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

PRTG Network Monitor là một công cụ phổ biến được sử dụng để giám sát mạng và cung cấp thông tin chi tiết về hiệu suất và sự hoạt động của các thiết bị mạng.

PRTG Network Monitor cung cấp các tính năng sau:

-Giám sát thiết bị mạng: Công cụ này cho phép bạn giám sát các thiết bị mạng như máy chủ, switch, router, tường lửa và điểm truy cập không dây. Bạn có thể theo dõi trạng thái hoạt động, khả năng phản hồi, tài nguyên sử dụng (CPU, bộ nhớ) và thông lượng mạng của các thiết bị này.

-Giám sát mạng LAN và WAN: PRTG Network Monitor cho phép bạn theo dõi các thông số mạng như băng thông, độ trễ, gói tin mất và gói tin hủy. Bạn có thể xác định các vấn đề về hiệu suất mạng, đánh giá sự ổn định và tìm hiểu nguyên nhân gây ra sự cố mạng.

-Giám sát ứng dụng: Công cụ này cung cấp khả năng giám sát ứng dụng và dịch vụ mạng chạy trên hệ thống. Bạn có thể theo dõi các thông số như tài nguyên sử dụng, thời gian phản hồi và khả năng phục hồi của ứng

dụng. Điều này giúp bạn xác định các vấn đề hoạt động của ứng dụng và đảm bảo rằng chúng hoạt động một cách hiệu quả.

-Báo cáo và cảnh báo: PRTG Network Monitor cho phép tạo báo cáo tự động về hiệu suất mạng và các sự cố liên quan. Bạn có thể tùy chỉnh các báo cáo này để phù hợp với yêu cầu của bạn. Ngoài ra, công cụ này có khả năng cảnh báo thông qua email, tin nhắn hoặc thông báo trực tiếp khi phát hiện sự cố hoặc vượt ngưỡng được xác định.

-Giao diện đồ họa và dễ sử dụng: PRTG Network Monitor có giao diện đồ họa thân thiện và dễ sử dụng. Bạn có thể tùy chỉnh giao diện để xem thông tin mạng theo cách bạn muốn và theo dõi từ xa thông qua giao diện web hoặc ứng dụng di động.

*** Đánh giá:**

PRTG Network Monitor là một công cụ giám sát mạng rất phổ biến và có nhiều ưu điểm đáng kể. Dưới đây là một số đánh giá về PRTG Network Monitor:

-Dễ cài đặt và cấu hình: PRTG Network Monitor được đánh giá cao về tính dễ cài đặt và cấu hình. Giao diện người dùng thân thiện và trực quan giúp người dùng nhanh chóng thiết lập các thiết bị mạng và cấu hình các thông số giám sát một cách dễ dàng.

-Đa dạng tính năng giám sát: PRTG Network Monitor cung cấp một loạt các tính năng giám sát mạnh mẽ. Bạn có thể giám sát các thiết bị mạng, mạng LAN và WAN, ứng dụng và dịch vụ mạng. Công cụ cung cấp thông tin chi tiết về hiệu suất, tài nguyên sử dụng và sự hoạt động của các thành phần mạng, giúp người dùng nắm bắt tình trạng mạng và xử lý sự cố một cách hiệu quả.

-Báo cáo và cảnh báo linh hoạt: PRTG Network Monitor cho phép tạo báo cáo tự động về hiệu suất mạng và các sự cố liên quan. Bạn có thể tùy chỉnh các báo cáo này để phù hợp với yêu cầu của bạn. Ngoài ra, công cụ cung cấp cảnh báo linh hoạt thông qua email, tin nhắn hoặc thông báo trực tiếp khi phát hiện sự cố hoặc vượt ngưỡng được xác định.

-Hỗ trợ đa nền tảng: PRTG Network Monitor hỗ trợ nhiều hệ điều hành và nền tảng, bao gồm Windows, Linux và macOS. Điều này giúp công cụ phù hợp với nhiều môi trường mạng và cho phép người dùng giám sát từ xa thông qua giao diện web hoặc ứng dụng di động.

-Hỗ trợ khách hàng tốt: PRTG Network Monitor có một cộng đồng người dùng lớn và hỗ trợ khách hàng chuyên nghiệp. Bạn có thể tìm thấy tài liệu hướng dẫn chi tiết, diễn đàn thảo luận và tư vấn từ nhóm hỗ trợ để giúp giải quyết các vấn đề và tận dụng tối đa các tính năng của công cụ.

4.2 Các báo cáo nhận được

PRTG Network Monitor cung cấp các báo cáo tự động về hiệu suất mạng và các sự cố liên quan. Dưới đây là một số báo cáo mà bạn có thể nhận được từ PRTG Network Monitor:

-Báo cáo hiệu suất mạng: Báo cáo này cung cấp thông tin chi tiết về tình trạng hiệu suất mạng. Nó bao gồm thông số như băng thông sử dụng, độ trễ, gói tin mất và gói tin hủy. Báo cáo này giúp bạn đánh giá tình trạng mạng và xác định các vấn đề về hiệu suất.

-Báo cáo tài nguyên mạng: Báo cáo này cung cấp thông tin về tài nguyên sử dụng của các thiết bị mạng như CPU, bộ nhớ, ổ đĩa và giao diện mạng. Bạn có thể theo dõi việc sử dụng tài nguyên của các thiết bị và xác định các vấn đề liên quan đến tài nguyên. Báo cáo sự cố mạng: Báo cáo này liệt kê các sự cố mạng đã xảy ra trong một khoảng thời gian cụ thể. Nó bao gồm thông tin chi tiết về thời gian xảy ra sự cố, thiết bị liên quan và mô tả về sự cố. Báo cáo này giúp bạn nhanh chóng nhận biết và giải quyết các sự cố mạng.

-Báo cáo khả năng phục hồi: Báo cáo này cung cấp thông tin về thời gian phục hồi của các thiết bị mạng sau khi xảy ra sự cố. Nó giúp bạn đánh giá hiệu suất và thời gian phục hồi của các thành phần mạng và xác định các vấn đề về khả năng phục hồi.

-Báo cáo sử dụng ứng dụng: Báo cáo này cung cấp thông tin về hiệu suất và sử dụng của các ứng dụng và dịch vụ mạng. Nó bao gồm thông

tin về tài nguyên sử dụng, thời gian phản hồi và khả năng phục hồi của các ứng dụng. Báo cáo này giúp bạn đánh giá và tối ưu hóa hiệu suất của các ứng dụng và dịch vụ mạng.

5 Kết luận

Trong quá trình thực hiện báo cáo này với đề tài " Xây dựng hệ thống mạng cho viện giáo dục quốc tế HUFLIT " trong môn học " Đồ án mạng", chúng em đã nhận được sự hỗ trợ và đồng hành không thể thiếu từ thầy Đỗ Phi Hưng. Thầy đã tận tâm và kiên nhẫn hướng dẫn chúng em từ giai đoạn lựa chọn đề tài cho đến việc thực hiện và trình bày báo cáo. Sự am hiểu và kiến thức chuyên môn của thầy đã đóng góp quan trọng vào thành công của dự án.

Tuy nhiên, cũng cần nhấn mạnh rằng báo cáo này chỉ là một bước đầu trong quá trình nghiên cứu và phát triển hệ thống mạng. Vẫn còn nhiều khía cạnh và phương pháp tiếp cận khác có thể được khám phá và áp dụng để nâng cao hiệu quả và chất lượng của hệ thống. Chúng em sẽ tiếp tục nghiên cứu và phát triển để đưa ra các cải tiến và đề xuất tốt hơn trong tương lai.

Cuối cùng, chúng em xin bày tỏ lòng biết ơn chân thành và sâu sắc đến giáo viên hướng dẫn và các tác giả của tài liệu tham khảo đã cung cấp cho chúng em kiến thức quý giá và hỗ trợ trong quá trình thực hiện báo cáo này. Sự đóng góp và sự tận tâm của họ đã góp phần quan trọng vào sự thành công của dự án. Chúng em cũng xin chân thành cảm ơn đến các thành

viên trong nhóm nghiên cứu đã cống hiến và hỗ trợ nhau trong suốt quá trình thực hiện.

Với những kinh nghiệm và kiến thức đã thu thập được, chúng em tin rằng chúng em sẽ có thể áp dụng và phát triển những kiến thức này trong các dự án tương lai và đóng góp vào sự phát triển của chuyên ngành an ninh mạng.

TÀI LIỆU THAM KHẢO

Trong quá trình thực hiện báo cáo này, chúng em đã tham khảo các tài liệu sau đây để tìm hiểu và nghiên cứu về Xây dựng hệ thống mạng cho viện giáo dục quốc tế HUFLIT:

- Tác giả David B. Makofske, năm 2004, tên sách TCP/IP Sockets in C#
- Tác giả EC-Council, năm 2017 Ethical Hacking and Countermeasures
- Tác giả Cisco Press, năm 2011, tên sách Priscilla Oppenheimer, Top-Down
- Christian Nagel, năm 2014, tên sách Professional C# 5.0 and .NET 4.5.1 Wrox
- Các tài liệu trên đã cung cấp cho chúng em nền tảng kiến thức vững chắc để áp dụng các phương pháp và kỹ thuật vào dự án của chúng em. Chúng em xin chân thành cảm ơn tất cả các tác giả, nhà xuất bản và nguồn tài liệu đã cung cấp kiến thức quý báu cho quá trình nghiên cứu.