BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO MÔN HỌC

QUẢN TRỊ HỆ THỐNG BẢO MẬT

Giảng viên hướng dẫn: ThS Đinh Xuân Lâm
Sinh viên thực hiện: Phạm Đức Thiên Phúc (21DH112813)
Nguyễn Công Khang (21DH110770)
Nguyễn Minh Đức (21DH113591)
Lê Viết Nam (21DH112687)
Khóa: 2021

TP.HCM, ngày 04 tháng 11 năm 2024

Mở đầu

Trong thời đại công nghệ số phát triển mạnh mẽ, hệ thống thông tin đóng vai trò quan trọng trong mọi lĩnh vực, từ quản lý doanh nghiệp, tài chính, y tế đến giáo dục và dịch vụ công. Tuy nhiên, cùng với sự phát triển của công nghệ, các mối đe dọa an ninh mạng ngày càng gia tăng cả về số lượng lẫn mức độ tinh vi. Các cuộc tấn công mạng như xâm nhập trái phép, đánh cắp dữ liệu, phát tán mã độc, tấn công từ chối dịch vụ (DDoS) hay lừa đảo trực tuyến không chỉ gây thiệt hại về tài chính mà còn ảnh hưởng nghiêm trọng đến uy tín và hoạt động của tổ chức, doanh nghiệp. Vì vậy, việc xây dựng, quản trị và duy trì một hệ thống bảo mật vững chắc là yêu cầu cấp thiết để đảm bảo an toàn thông tin và bảo vệ hệ thống trước những rủi ro tiềm ẩn.

Quản trị hệ thống bảo mật không chỉ đơn thuần là việc triển khai các giải pháp công nghệ mà còn bao gồm các chính sách, quy trình và chiến lược nhằm phát hiện, ngăn chặn và xử lý các mối đe dọa an ninh mạng. Một hệ thống bảo mật hiệu quả phải đảm bảo tính bảo mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn sàng (availability) của dữ liệu và hệ thống thông tin. Điều này đòi hỏi sự kết hợp giữa công nghệ tiên tiến như tường lửa, hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), mã hóa dữ liệu, xác thực đa yếu tố với các biện pháp quản lý như phân quyền truy cập, đào tạo nhận thức bảo mật cho nhân viên, và thực hiện các quy trình kiểm tra, đánh giá định kỳ.

Báo cáo này sẽ đi sâu vào các nguyên tắc quản trị hệ thống bảo mật, phân tích các mô hình bảo mật phổ biến, đánh giá những thách thức trong việc triển khai và duy trì hệ thống bảo mật tại các tổ chức. Ngoài ra, báo cáo cũng sẽ đề xuất một số giải pháp nhằm nâng cao khả năng bảo vệ hệ thống trước những nguy cơ tấn công ngày càng phức tạp. Thông qua nghiên cứu này, chúng tôi hy vọng cung cấp một cái nhìn tổng quan và thực tiễn về quản trị hệ thống bảo mật, giúp nâng cao nhận thức và khả năng ứng phó với các mối đe dọa an ninh mạng trong môi trường công nghệ hiện đại.

Mục lục

Chương I: Giới thiệu doanh nghiệp

I. Lĩnh vực kinh doanh

NET.VN là một doanh nghiệp chuyên kinh doanh và sửa chữa các sản phẩm điện tử. Chúng tôi cung cấp đa dạng các sản phẩm như laptop, điện thoại, linh kiện máy tính và các thiết bị điện tử khác. Bên cạnh đó, NET.VN còn cung cấp dịch vụ sửa chữa máy tính, điện thoại với chi phí hợp lý, hỗ trợ tư vấn và lắp đặt thiết bị theo yêu cầu. Với tinh thần phục vụ tận tâm, NET.VN mong muốn trở thành một địa chỉ đáng tin cậy cho mọi nhu cầu về thiết bị điện tử.

II. Tổ chức và quy mô

NET.VN hiện tại chỉ có 1 chi nhánh duy nhất tại Thành phố Hồ Chí Minh với 2 phòng ban cơ bản là phòng Sale dành cho bộ phần bán hàng và phòng IT dành cho bộ phận kỹ thuật

III. Hoạt động kinh doanh

Cung cấp và phân phối các thiết bị điện tử chất lượng, đảm bảo nguồn gốc rõ ràng.
Nhận sửa chữa, bảo hành điện thoại, máy tính, laptop với linh kiện chính hãng.
Hỗ trợ tư vấn các sản phẩm phù hợp với người tiêu dùng.

Chương II. Lý thuyết tổng quan

I. Mạng Domain là gì?

Mạng Domain là một loại mạng máy tính trong đó các máy tính và tài nguyên (như máy in, thư mục chia sẻ, v.v.) được quản lý và điều khiển bởi một máy chủ trung tâm, thường được gọi là Domain Controller. Các Domain giúp tổ chức và bảo mật các tài nguyên trong mạng.

Một Domain có thể bao gồm hàng nghìn máy tính và người dùng, và tất cả các máy tính trong Domain đều có thể truy cập tài nguyên chung. Quản trị viên có thể thiết lập quyền truy cập cho người dùng và máy tính thông qua các chính sách bảo mật, giúp dễ dàng quản lý và bảo mật dữ liệu.

Trong môi trường Windows, khi một công ty sử dụng Active Directory để quản lý các máy tính và người dùng trong hệ thống của họ. Khi một máy tính gia nhập Domain, người dùng có thể đăng nhập vào bất kỳ máy tính nào trong Domain và vẫn sử dụng các tài nguyên mạng chung.

II. VPN là gì?

1. Định nghĩa

VPN (Virtual Private Network) đóng vai trò rất quan trọng trong việc bảo mật và kết nối mạng từ xa giữa các nhân viên và tài nguyên của công ty. Khi sử dụng VPN trong doanh nghiệp, nhân viên có thể truy cập vào hệ thống nội bộ (như các file, ứng dụng, hoặc cơ sở dữ liệu) từ bất kỳ đâu mà không cần phải có mặt trực tiếp tại văn phòng, đồng thời đảm bảo tính bảo mật cao.

2. Lợi ích của VPN trong doanh nghiệp

Bảo mật kết nối từ xa: VPN mã hóa kết nối của người dùng, giúp bảo vệ dữ liệu truyền tải giữa các thiết bị của nhân viên và mạng công ty khỏi việc bị nghe lén, tấn công hay đánh cắp khi sử dụng mạng công cộng (như Wi-Fi công cộng).

Truy cập tài nguyên nội bộ: Nhân viên có thể kết nối với các tài nguyên mạng nội bộ của công ty (như máy chủ, file server, ứng dụng doanh nghiệp) từ xa mà không gặp phải các rào cản mạng hoặc các vấn đề về bảo mật.

Giảm chi phí cơ sở hạ tầng: VPN cho phép công ty tạo ra một mạng riêng ảo mà không cần phải đầu tư quá nhiều vào cơ sở hạ tầng đắt đỏ như các kết nối WAN (Wide Area Network) truyền thống, từ đó tiết kiệm chi phí.

Quản lý và kiểm soát dễ dàng: Các quản trị viên có thể kiểm soát việc truy cập mạng của nhân viên từ xa bằng cách thiết lập chính sách truy cập, bao gồm việc phân quyền cho từng nhân viên, nhóm, hoặc bộ phận cụ thể.

Hỗ trợ làm việc từ xa: VPN là công cụ quan trọng đối với các doanh nghiệp có nhân viên làm việc từ xa, trong các tình huống làm việc từ nhà hoặc khi di chuyển giữa các văn phòng chi nhánh.
Giảm rủi ro bảo mật: Việc sử dụng VPN giúp ngăn chặn các mối đe dọa như tấn công man-in-the-middle (MITM) hoặc tấn công vào các kết nối không bảo mật, giảm nguy cơ bị lộ thông tin doanh nghiệp quan trọng.

3. Các loại VPN trong doanh nghiệp

Site-to-Site VPN: Đây là loại VPN giữa hai hoặc nhiều văn phòng hoặc chi nhánh của doanh nghiệp. Nó cho phép các mạng LAN của các văn phòng khác nhau kết nối với nhau qua Internet và trao đổi dữ liệu một cách bảo mật.
Remote Access VPN: Loại VPN này cho phép các nhân viên làm việc từ xa kết nối với mạng công ty, như thể họ đang làm việc trực tiếp tại văn phòng. Nhân viên có thể sử dụng các thiết bị cá nhân hoặc máy tính công ty để kết nối với hệ thống mạng nội bộ của công ty.
Client-to-Site VPN: Nhân viên cài đặt một phần mềm VPN client trên thiết bị của mình để kết nối với một VPN gateway tại công ty. Loại này phổ biến cho các doanh nghiệp có nhân viên làm việc từ xa.
SSL VPN: SSL VPN sử dụng giao thức SSL (Secure Sockets Layer) để mã hóa kết nối. Loại này thường được sử dụng khi người dùng không muốn cài đặt phần mềm VPN client mà chỉ cần truy cập qua trình duyệt web.

III. Proxy là gì?

1. Định nghĩa

Proxy là một máy chủ hoặc dịch vụ trung gian giữa người dùng và internet, đóng vai trò như một "cầu nối" giúp chuyển tiếp các yêu cầu từ người dùng đến các máy chủ khác. Khi bạn sử dụng proxy, thay vì kết nối trực tiếp với một trang web hoặc dịch vụ trực tuyến, yêu cầu của bạn sẽ được gửi đến proxy, và sau đó proxy sẽ gửi yêu cầu đó đến máy chủ đích.

2. Các chức năng chính của Proxy

Ẩn danh và bảo mật: Proxy có thể giúp ẩn địa chỉ IP của người dùng, khiến cho các trang web hoặc dịch vụ không thể biết được vị trí thực tế của người dùng. Điều này giúp bảo vệ sự riêng tư và bảo mật khi duyệt web.
Truy cập vào nội dung bị chặn: Nếu một trang web hoặc dịch vụ bị chặn ở một quốc gia hoặc khu vực, proxy có thể cho phép người dùng truy cập vào các trang web đó bằng cách thay đổi địa chỉ IP của họ, giả mạo vị trí ở một nơi khác.

Lọc nội dung: Proxy có thể được sử dụng để lọc hoặc kiểm soát nội dung truy cập, ví dụ như ngăn chặn truy cập vào các trang web không phù hợp trong môi trường doanh nghiệp hoặc trường học.
Tăng tốc độ truy cập: Proxy có thể lưu trữ (cache) các dữ liệu từ các trang web, giúp giảm thời gian tải trang khi người dùng truy cập lại vào các trang web đó. Điều này có thể cải thiện tốc độ truy cập, đặc biệt trong môi trường doanh nghiệp.
Quản lý và giám sát: Trong các doanh nghiệp, proxy có thể được sử dụng để giám sát và ghi lại hoạt động của người dùng trên internet, từ đó giúp quản lý việc sử dụng mạng và đảm bảo tuân thủ các chính sách công ty.

3. Các loại proxy phổ biến

Forward Proxy: Đây là loại proxy truyền thống, nơi người dùng gửi yêu cầu đến proxy, và proxy sẽ gửi yêu cầu đó đến máy chủ đích thay mặt người dùng.
Reverse Proxy: Khác với forward proxy, reverse proxy đứng giữa máy chủ web và người dùng. Nó nhận yêu cầu từ người dùng và chuyển tiếp yêu cầu đó đến một máy chủ web phía sau. Reverse proxy giúp bảo vệ máy chủ web khỏi các tấn công và có thể phân tải giữa các máy chủ.
Transparent Proxy: Proxy này không thay đổi yêu cầu của người dùng hoặc phản hồi từ máy chủ, nhưng có thể vẫn giám sát và ghi lại dữ liệu. Nó thường được sử dụng trong môi trường doanh nghiệp để giám sát lưu lượng mạng.
Anonymous Proxy: Loại proxy này giúp ẩn danh người dùng khi duyệt web, ngăn chặn các trang web biết được địa chỉ IP thực của người dùng.
High Anonymity Proxy (Elite Proxy): Đây là loại proxy mạnh mẽ nhất trong việc ẩn danh, vì nó không chỉ ẩn địa chỉ IP của người dùng mà còn không tiết lộ rằng người dùng đang sử dụng proxy.

4. Ưu điểm và nhược điểm của Proxy:

- **Ưu điểm**:

Tăng cường bảo mật và quyền riêng tư.
Giúp truy cập nội dung bị hạn chế hoặc chặn.
Giảm tải và tăng tốc độ cho mạng nội bộ.
Dễ dàng quản lý và giám sát người dùng trong môi trường doanh nghiệp.

- **Nhược điểm**:

Proxy có thể làm giảm hiệu suất mạng nếu không được cấu hình tốt.
Không phải tất cả các ứng dụng đều hỗ trợ proxy.
Một số trang web và dịch vụ có thể phát hiện và chặn proxy.

IV. Firewall là gì?

1. Định nghĩa

Firewall (tường lửa) là một hệ thống bảo mật mạng được thiết kế để giám sát và kiểm soát lưu lượng mạng vào và ra khỏi một hệ thống hoặc mạng. Tường lửa hoạt động như một "rào chắn" giữa mạng nội bộ và mạng ngoài (ví dụ: Internet), giúp bảo vệ các tài nguyên trong mạng khỏi các mối đe dọa và tấn công từ bên ngoài, đồng thời cho phép hoặc chặn các kết nối mạng dựa trên các quy tắc bảo mật đã được cấu hình.

2. Các chức năng chính của Firewall

Kiểm soát truy cập: Firewall giám sát các kết nối mạng và chỉ cho phép các kết nối hợp lệ dựa trên các quy tắc đã thiết lập. Nó có thể cho phép hoặc từ chối lưu lượng mạng dựa trên địa chỉ IP, giao thức, cổng, hoặc các yếu tố khác.
Ngăn chặn tấn công: Tường lửa giúp ngăn chặn các tấn công mạng như DoS (Denial of Service), DDoS (Distributed Denial of Service), SQL injection, và các mối đe dọa khác bằng cách chặn các lưu lượng không hợp lệ hoặc đáng ngờ.
Giám sát và ghi lại lưu lượng mạng: Tường lửa có thể ghi lại và phân tích lưu lượng mạng để phát hiện các hành vi bất thường hoặc các cuộc tấn công, đồng thời cung cấp các báo cáo để quản trị viên có thể theo dõi tình hình bảo mật.
Tạo mạng riêng ảo (VPN): Một số loại tường lửa có tính năng hỗ trợ VPN, cho phép tạo kết nối bảo mật từ xa giữa các chi nhánh hoặc người dùng từ xa và mạng nội bộ của doanh nghiệp.
Lọc nội dung: Firewall có thể được cấu hình để lọc nội dung web, chặn các trang web không mong muốn hoặc các loại nội dung gây hại, giúp ngăn chặn các truy cập không hợp lệ trong môi trường doanh nghiệp.

3. Các loại Firewall

Packet Filtering Firewall (Tường lửa lọc gói tin): Đây là loại tường lửa cơ bản nhất, hoạt động bằng cách kiểm tra các gói tin mạng và quyết định xem liệu chúng có được phép đi qua hay không dựa trên các quy tắc như địa chỉ IP nguồn, địa chỉ IP đích, cổng, và giao thức.
Stateful Inspection Firewall (Tường lửa kiểm tra trạng thái): Loại firewall này không chỉ kiểm tra các gói tin, mà còn theo dõi trạng thái của kết nối (connection state). Nó cho phép chỉ các gói tin hợp lệ thuộc về một kết nối đã được xác nhận đi qua, giúp ngăn chặn các gói tin không hợp lệ.
Proxy Firewall (Tường lửa proxy): Tường lửa này hoạt động như một proxy giữa người dùng và internet. Nó sẽ thay mặt người dùng gửi yêu cầu và nhận phản hồi

từ máy chủ đích, kiểm tra nội dung và bảo vệ hệ thống khỏi các mối đe dọa trực tiếp.
Next-Generation Firewall (NGFW) (Tường lửa thế hệ tiếp theo): Tường lửa thế hệ tiếp theo kết hợp nhiều tính năng bảo mật, bao gồm tường lửa lọc gói tin, kiểm tra trạng thái, ngăn chặn xâm nhập (IPS), lọc ứng dụng, và hỗ trợ VPN. NGFW có thể phân tích lưu lượng ứng dụng, nhận diện và ngăn chặn các mối đe dọa tinh vi hơn.
Application Firewall (Tường lửa ứng dụng): Loại firewall này hoạt động ở tầng ứng dụng của mô hình OSI, giúp bảo vệ các ứng dụng web khỏi các tấn công như SQL injection, cross-site scripting (XSS), và các mối đe dọa khác mà không thể được bảo vệ bởi các tường lửa thông thường.

4. Ưu điểm và nhược điểm của Firewall

- **Ưu điểm:**

Bảo vệ hệ thống khỏi các tấn công từ bên ngoài: Tường lửa giúp ngăn chặn các tấn công mạng và bảo vệ tài nguyên trong mạng khỏi việc bị xâm nhập.
Kiểm soát lưu lượng mạng: Tường lửa cho phép các quản trị viên mạng kiểm soát và hạn chế các kết nối không mong muốn.
Phân quyền truy cập: Firewall có thể giới hạn quyền truy cập vào các dịch vụ mạng chỉ cho các địa chỉ IP hoặc người dùng đã được ủy quyền.
Tăng cường bảo mật tổng thể: Ngoài việc ngăn chặn các tấn công từ bên ngoài, firewall cũng giúp giám sát và bảo vệ các ứng dụng và dịch vụ trong mạng nội bộ.

- **Nhược điểm của Firewall:**

Có thể làm giảm hiệu suất: Một số loại firewall, đặc biệt là khi cấu hình phức tạp hoặc bảo mật cao, có thể làm giảm tốc độ của mạng hoặc hệ thống.
Phải cấu hình và duy trì thường xuyên: Tường lửa cần được cấu hình đúng đắn và cập nhật các quy tắc bảo mật thường xuyên để ngăn chặn các mối đe dọa mới.
Không thể ngăn chặn tất cả các mối đe dọa: Mặc dù tường lửa rất quan trọng trong việc bảo mật mạng, nhưng nó không thể ngăn chặn tất cả các loại tấn công, đặc biệt là các mối đe dọa tinh vi hoặc tấn công đã vượt qua các lớp bảo mật khác.

V. IDS là gì?

1. Định nghĩa

IDS (Intrusion Detection System) là một hệ thống bảo mật được thiết kế để giám sát lưu lượng mạng hoặc hoạt động hệ thống nhằm phát hiện các hành vi đáng ngờ hoặc các cuộc tấn công mạng. IDS không chặn lưu lượng mạng mà chỉ cảnh báo quản trị viên về các sự kiện bất thường để có hành động xử lý kịp thời.

2. Chức năng của IDS:

Phát hiện tấn công mạng: IDS có thể phát hiện các cuộc tấn công như DDoS, brute force attack, SQL injection, cross-site scripting (XSS), buffer overflow, v.v.
Giám sát lưu lượng mạng: Theo dõi và phân tích tất cả các gói dữ liệu đi qua hệ thống để tìm ra các dấu hiệu của hành vi đáng ngờ.
Cảnh báo bảo mật: Khi phát hiện một mối đe dọa, IDS sẽ gửi cảnh báo cho quản trị viên dưới dạng email, nhật ký (log), hoặc giao diện quản lý bảo mật.
Hỗ trợ phân tích sự cố: IDS giúp thu thập dữ liệu về các cuộc tấn công để quản trị viên có thể phân tích và cải thiện chiến lược bảo mật.

3. Các loại IDS chính

IDS có thể được phân loại thành HIDS (Host-based IDS) và NIDS (Network-based IDS)

a) HIDS (Host-based Intrusion Detection System) – IDS trên máy chủ

Cài đặt trực tiếp trên máy chủ hoặc thiết bị đầu cuối (endpoint).
Giám sát nhật ký hệ thống, tệp tin, tiến trình đang chạy, registry để phát hiện các hoạt động đáng ngờ.
Phát hiện các cuộc tấn công như malware, rootkits, unauthorized file changes, privilege escalation.
Ví dụ: OSSEC, Tripwire, AIDE.

b) NIDS (Network-based Intrusion Detection System) – IDS trên mạng

Giám sát toàn bộ lưu lượng mạng trong thời gian thực.
Phát hiện các dấu hiệu tấn công như port scanning, ARP spoofing, DoS, worms, exploits bằng cách kiểm tra các gói tin.
Ví dụ: Snort, Suricata, Zeek (Bro).

4. Phương pháp phát hiện của IDS

IDS sử dụng hai phương pháp chính để phát hiện mối đe dọa:

a) Signature-Based Detection (Dựa trên chữ ký)

IDS kiểm tra lưu lượng mạng hoặc hệ thống dựa trên các mẫu tấn công đã biết (signatures).
Giống như phần mềm diệt virus, IDS có một cơ sở dữ liệu chứa các mẫu tấn công và sẽ cảnh báo nếu phát hiện mẫu đó trong lưu lượng mạng.
Ưu điểm: Chính xác khi phát hiện các mối đe dọa đã biết.

Nhược điểm: Không phát hiện được các cuộc tấn công mới hoặc biến thể chưa có trong cơ sở dữ liệu.

b) Anomaly-Based Detection (Dựa trên hành vi bất thường)

DS sử dụng machine learning hoặc AI để phân tích hành vi bình thường của hệ thống và phát hiện các bất thường so với tiêu chuẩn.
Phát hiện các mối đe dọa mới hoặc các cuộc tấn công zero-day.
Ưu điểm: Có thể phát hiện các kiểu tấn công mới chưa được biết trước.
Nhược điểm: Dễ xảy ra cảnh báo sai (false positives).

VI. IPS là gì?

1. Giới thiệu

IPS (Intrusion Prevention System) là một hệ thống bảo mật chủ động có nhiệm vụ phát hiện và ngăn chặn các cuộc tấn công mạng theo thời gian thực. Không giống như IDS (Intrusion Detection System) chỉ phát hiện và cảnh báo, IPS có thể chặn hoặc giảm thiểu tác động của các cuộc tấn công bằng cách tự động thực hiện các hành động phòng thủ.

2. Chức năng của IPS

Giám sát lưu lượng mạng: IPS phân tích toàn bộ lưu lượng mạng để phát hiện các hành vi đáng ngờ hoặc nguy hiểm.
Ngăn chặn các cuộc tấn công: Khi phát hiện một mối đe dọa, IPS có thể tự động chặn gói tin, ngắt kết nối hoặc vô hiệu hóa nguồn tấn công.
Bảo vệ hệ thống và ứng dụng: IPS giúp ngăn chặn DDoS, malware, SQL injection, brute-force attack, buffer overflow và nhiều loại tấn công khác.
Giảm rủi ro bảo mật: Hạn chế nguy cơ bị tấn công trước khi các mối đe dọa kịp gây ra thiệt hại.

3. Các loại IPS

IPS có thể được triển khai dưới nhiều hình thức khác nhau:

a) NIPS (Network-based IPS) – IPS trên mạng

Giám sát và bảo vệ toàn bộ mạng.
Được triển khai tại điểm vào (gateway) của hệ thống để chặn các cuộc tấn công trước khi chúng xâm nhập vào mạng nội bộ.
Ví dụ: Suricata, Snort (chế độ IPS), Cisco Firepower.

b) HIPS (Host-based IPS) – IPS trên máy chủ

Cài đặt trên từng máy chủ hoặc thiết bị đầu cuối (endpoint).
Phát hiện và ngăn chặn các cuộc tấn công nhắm vào hệ điều hành, phần mềm và tệp tin quan trọng.
Ví dụ: OSSEC, Symantec Endpoint Protection.

4. Phương pháp phát hiện của IPS

IPS sử dụng hai phương pháp chính để phát hiện và ngăn chặn các cuộc tấn công:

a) Signature-Based Detection (Dựa trên chữ ký)

IPS kiểm tra lưu lượng mạng dựa trên **các mẫu tấn công đã biết** trong cơ sở dữ liệu.
Nếu phát hiện một gói tin hoặc kết nối khớp với chữ ký tấn công, IPS sẽ ngay lập tức chặn nó.
Ưu điểm: Hiệu quả với các cuộc tấn công đã được nhận diện trước đó.
Nhược điểm: Không thể phát hiện các cuộc tấn công mới hoặc biến thể chưa có trong cơ sở dữ liệu.

b) Anomaly-Based Detection (Dựa trên hành vi bất thường)

IPS sử dụng AI hoặc Machine Learning để phân tích lưu lượng mạng và phát hiện các hoạt động bất thường.
Khi một hành vi không khớp với mô hình "bình thường" của hệ thống, IPS sẽ cảnh báo và có thể chặn kết nối đó.
Ưu điểm: Có thể phát hiện các cuộc tấn công mới chưa có chữ ký.
Nhược điểm: Dễ xảy ra lỗi false positive (cảnh báo sai), có thể chặn nhầm lưu lượng hợp lệ.

4. So sánh IDS và IPS

Đặc điểm	IDS	IPS
Chức năng	Phát hiện và cảnh báo về các cuộc tấn công	Phát hiện và ngăn chặn các cuộc tấn công
Hành động	Chỉ giám sát và ghi lại sự kiện	Có thể chặn gói tin, ngắt kết nối, hoặc vô hiệu hóa nguồn tấn công
Ảnh hưởng đến hiệu suất	Không ảnh hưởng trực tiếp đến lưu lượng mạng	Có thể gây chậm mạng nếu không được tối ưu hóa
Vị trí triển khai	Passive (thụ động) – giám sát lưu lượng mà không can thiệp	Active (chủ động) – nằm giữa mạng và thực thi các quy tắc bảo mật

Chương III: Triển khai giải pháp bảo mật

I. Yêu cầu của doanh nghiệp

Triển khai giải pháp bảo mật cho doanh nghiệp cần tuân thủ các yêu cầu quan trọng sau để đảm bảo an toàn dữ liệu, hệ thống và thông tin khách hàng:

1. Đánh giá rủi ro & Xác định yêu cầu bảo mật

Xác định tài sản quan trọng (dữ liệu khách hàng, hệ thống mạng, ứng dụng quan trọng).
Đánh giá các rủi ro tiềm ẩn như tấn công mạng, rò rỉ dữ liệu, lỗi hệ thống.
Tuân thủ các tiêu chuẩn bảo mật liên quan như ISO 27001, NIST, GDPR (nếu có).

2. Bảo mật mạng & hệ thống

Tường lửa (Firewall): Dùng pfSense, FortiGate hoặc các thiết bị firewall chuyên dụng.
Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Sử dụng Suricata hoặc Snort.
VPN & Mạng riêng ảo: Cấu hình OpenVPN, WireGuard để bảo mật truy cập từ xa.
Phân đoạn mạng (Network Segmentation): Tách biệt các hệ thống quan trọng khỏi mạng chung.
Giám sát hệ thống (SIEM): Dùng Wazuh, Splunk để theo dõi nhật ký và phát hiện sự kiện bất thường.

3. Bảo vệ dữ liệu & thiết bị đầu cuối

Mã hóa dữ liệu: Sử dụng BitLocker, VeraCrypt để bảo vệ dữ liệu quan trọng.
Sao lưu dữ liệu định kỳ: Sử dụng NAS, cloud storage (AWS S3, Google Drive) để đảm bảo phục hồi khi cần.
Chính sách quản lý thiết bị di động (MDM): Đảm bảo các thiết bị di động truy cập hệ thống được kiểm soát.

4. Kiểm soát truy cập & xác thực

Xác thực hai yếu tố (2FA/MFA): Kích hoạt trên email, VPN, hệ thống quan trọng.
Quản lý tài khoản & phân quyền: Dùng nguyên tắc Least Privilege (cấp quyền tối thiểu cần thiết).

Quản lý mật khẩu: Yêu cầu sử dụng mật khẩu mạnh, thay đổi định kỳ, và lưu trữ bằng trình quản lý mật khẩu.

5. Giám sát & phản ứng sự cố

Hệ thống cảnh báo & logging: Theo dõi sự kiện bảo mật, cảnh báo kịp thời khi có dấu hiệu tấn công.
Kế hoạch phản ứng sự cố (Incident Response Plan): Xây dựng quy trình xử lý khi có sự cố.
Diễn tập an ninh mạng: Kiểm tra khả năng phản ứng với tấn công giả lập.

6. Nâng cao nhận thức bảo mật

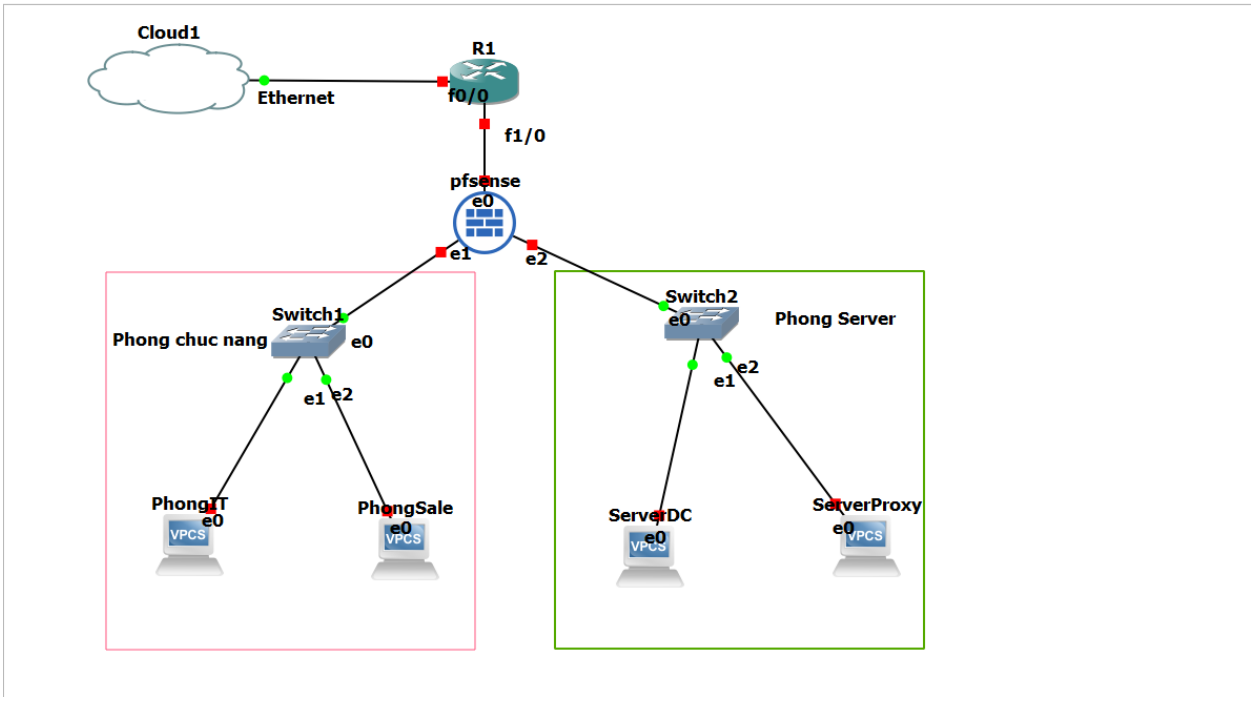
Đào tạo nhân viên: Hướng dẫn nhận diện email lừa đảo, mã độc, cách bảo vệ thông tin cá nhân.
Chính sách bảo mật nội bộ: Xây dựng quy định rõ ràng về việc sử dụng hệ thống và dữ liệu.

II. Xây dựng giải pháp

1. Sơ đồ vật lý

NET.VN sẽ triển khai mô hình mạng doanh nghiệp bao gồm:

- 1 router Cisco 7200
- 1 firewall Netgate 6100
- 2 switch Cisco Catalyst 2960G
- 2 máy server
- 3 máy tính cho phòng IT
- 3 máy tính cho phòng Sale



2. Chính sách bảo mật vật lý, hệ điều hành, mạng

a. Chính sách bảo mật vật lý

Bảo vệ phần cứng và truy cập vật lý vào hệ thống.
Kiểm soát truy cập: Hạn chế người không phận sự vào phòng server, dùng khóa từ, vân tay.
Giám sát an ninh: Lắp đặt camera 24/7, nhật ký ra vào.
Bảo vệ thiết bị: Khóa màn hình khi rời máy, bố trí server trong khu vực an toàn.
Phòng chống sự cố: Dùng UPS, hệ thống chữa cháy tự động, kế hoạch khôi phục dữ liệu.
Kiểm tra định kỳ: Rà soát an ninh vật lý và thiết bị lưu trữ.

b. Chính sách bảo mật hệ điều hành

Bảo vệ hệ thống máy chủ, máy trạm tránh lỗ hổng bảo mật.
Cập nhật & vá lỗi: Luôn cập nhật hệ điều hành Windows, Linux, macOS.
Quản lý tài khoản: Áp dụng nguyên tắc **Least Privilege**, bật UAC, hạn chế quyền admin.
Xác thực & kiểm soát truy cập: Sử dụng **MFA/2FA**, đặt mật khẩu mạnh, khóa tài khoản sau nhiều lần nhập sai.
Bảo vệ dữ liệu: Mã hóa ổ cứng bằng BitLocker, FileVault, LUKS, hạn chế sao chép dữ liệu.
Giám sát & kiểm tra bảo mật: Theo dõi nhật ký hệ thống, chạy phần mềm bảo mật endpoint (Windows Defender, CrowdStrike).

c. Chính sách bảo mật mạng

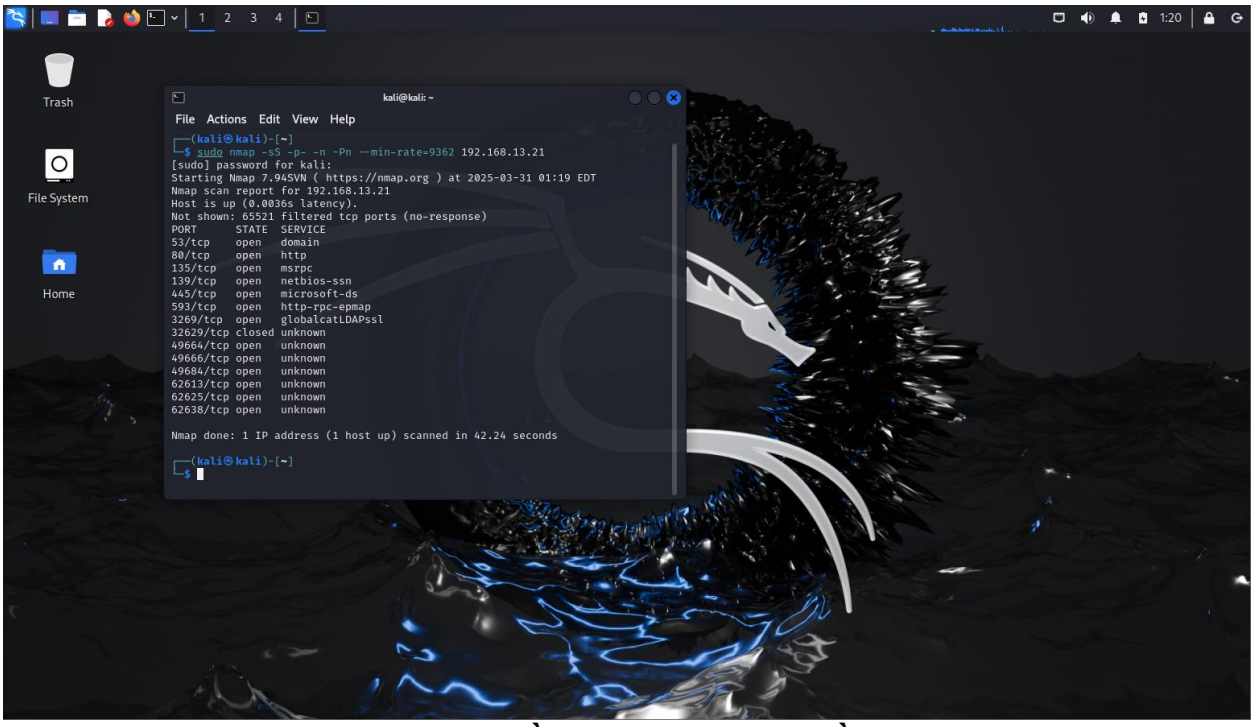
Bảo vệ hệ thống mạng trước các cuộc tấn công và truy cập trái phép.
Tường lửa (Firewall): Sử dụng pfSense, FortiGate hoặc các firewall chuyên dụng.
IDS/IPS: Dùng Suricata, Snort để phát hiện và ngăn chặn tấn công.
Phân đoạn mạng (Network Segmentation): Tách biệt mạng nội bộ, server và thiết bị IoT.
VPN & Mã hóa: Dùng OpenVPN, WireGuard để bảo mật truy cập từ xa.
Quản lý truy cập: Giới hạn quyền truy cập theo VLAN, chỉ cho phép IP đáng tin cậy.
Giám sát & kiểm tra: Theo dõi log mạng, phát hiện xâm nhập bất thường, kiểm tra lỗ hổng bảo mật định kỳ.

3. Bảng ước tính chi phí

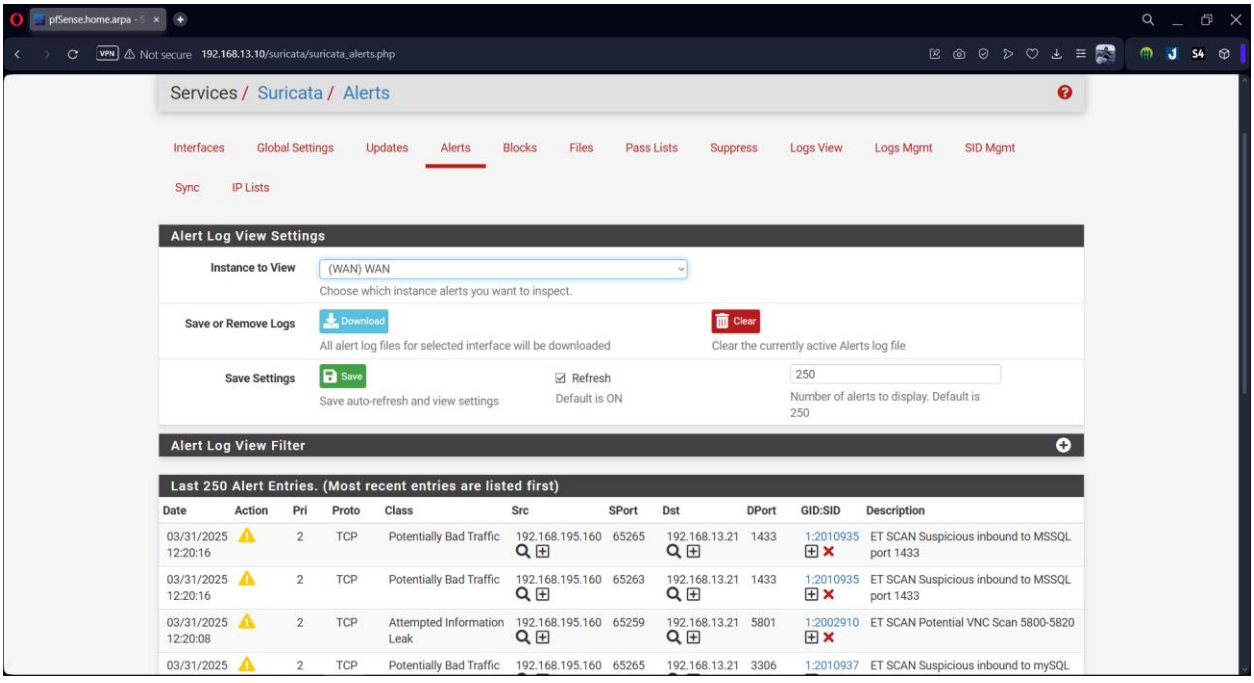
Thiết bị	Số lượng	Đơn giá
Router Cisco 7200	1	50.000.000
Firewall Netgate 6100	1	22.000.000
Switch Cisco Catalyst 2960G	2	7.000.000
Máy chủ	2	40.000.000
Máy trạm	6	15.000.000
Cáp mạng và phụ kiện	~	10.000.000
Tổng	12	266.000.000

III. Triển khai

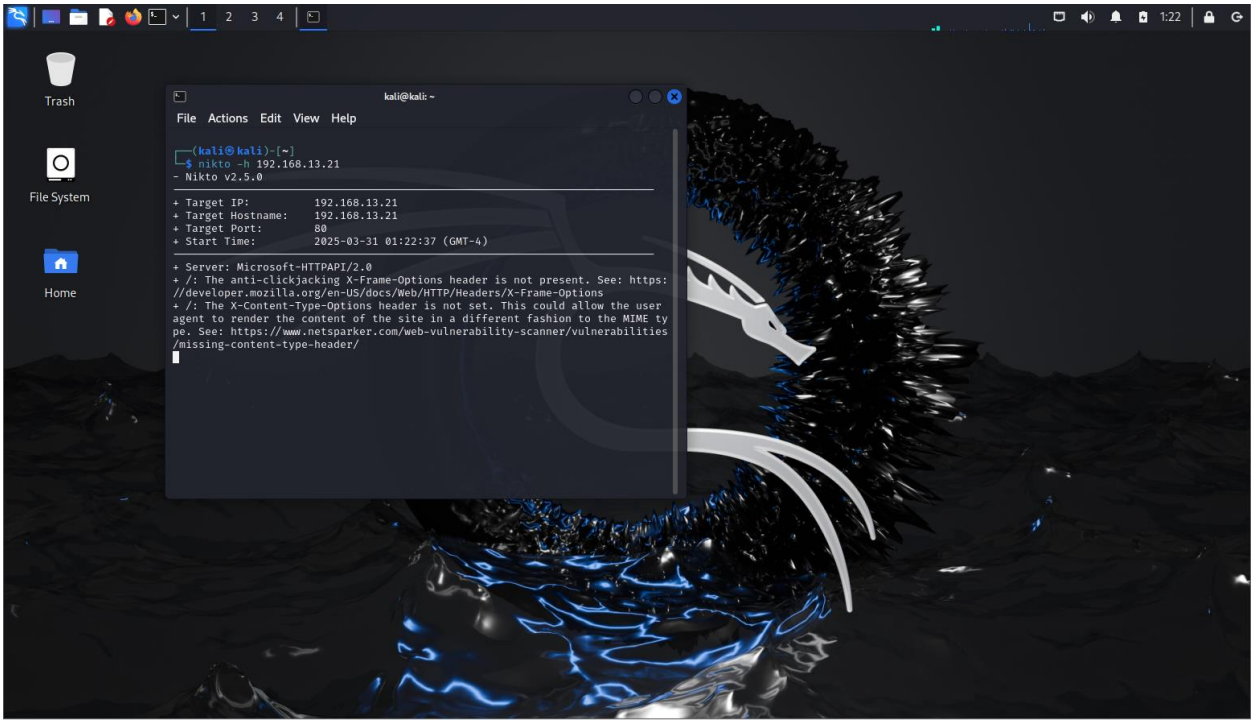
1. Firewall pfSense sử dụng IDS Suricata



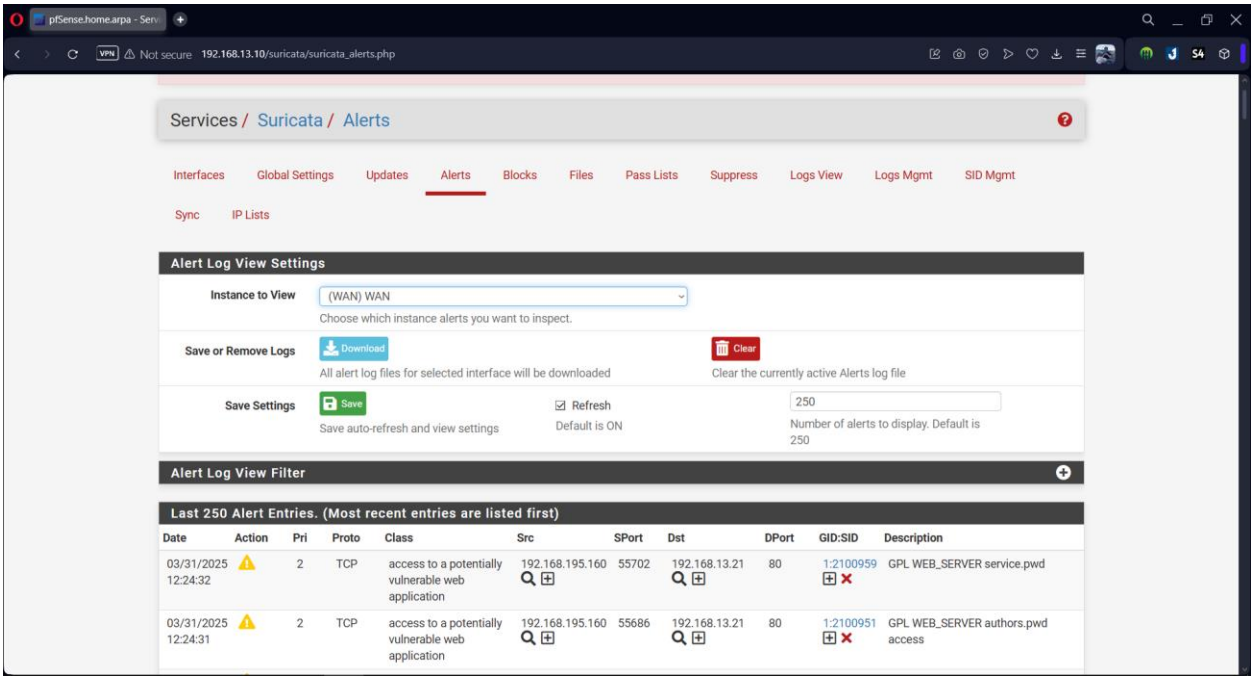
Hình 1: nmap máy chủ bằng máy chạy hệ điều hành kali linux



Hình 2: Suricata gửi cảnh báo

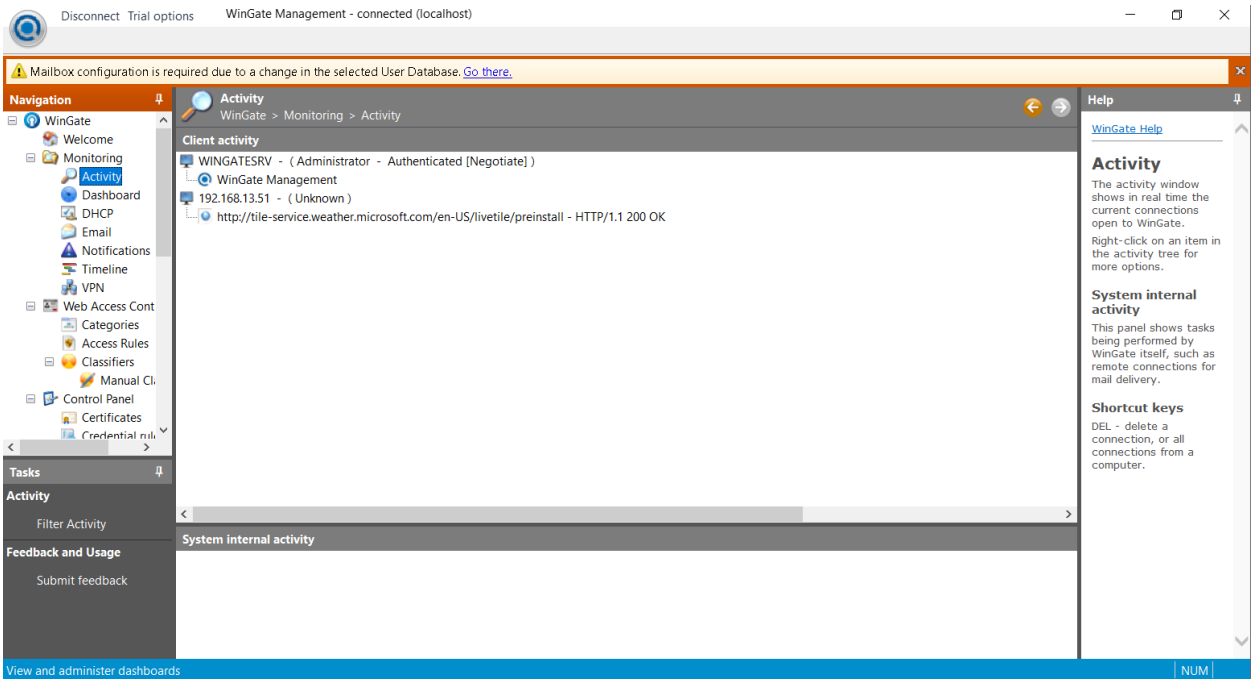


Hình 3: Nikto tới webserver

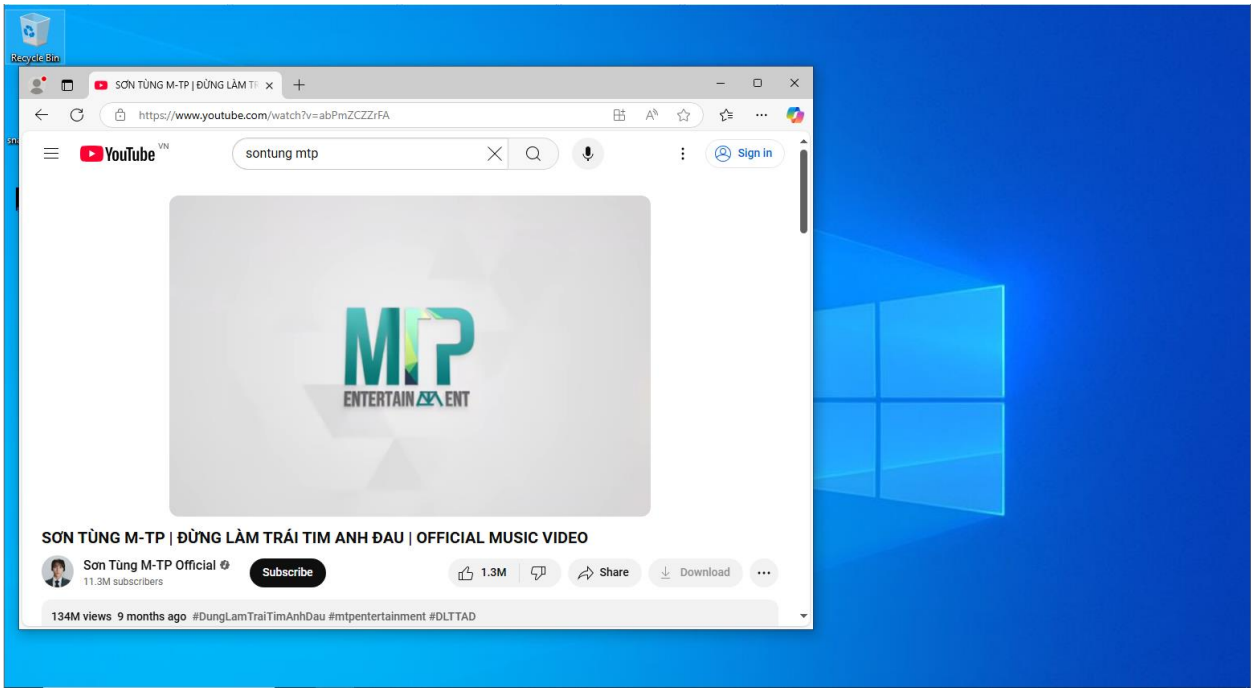


Hình 4: Suricata gửi cảnh báo

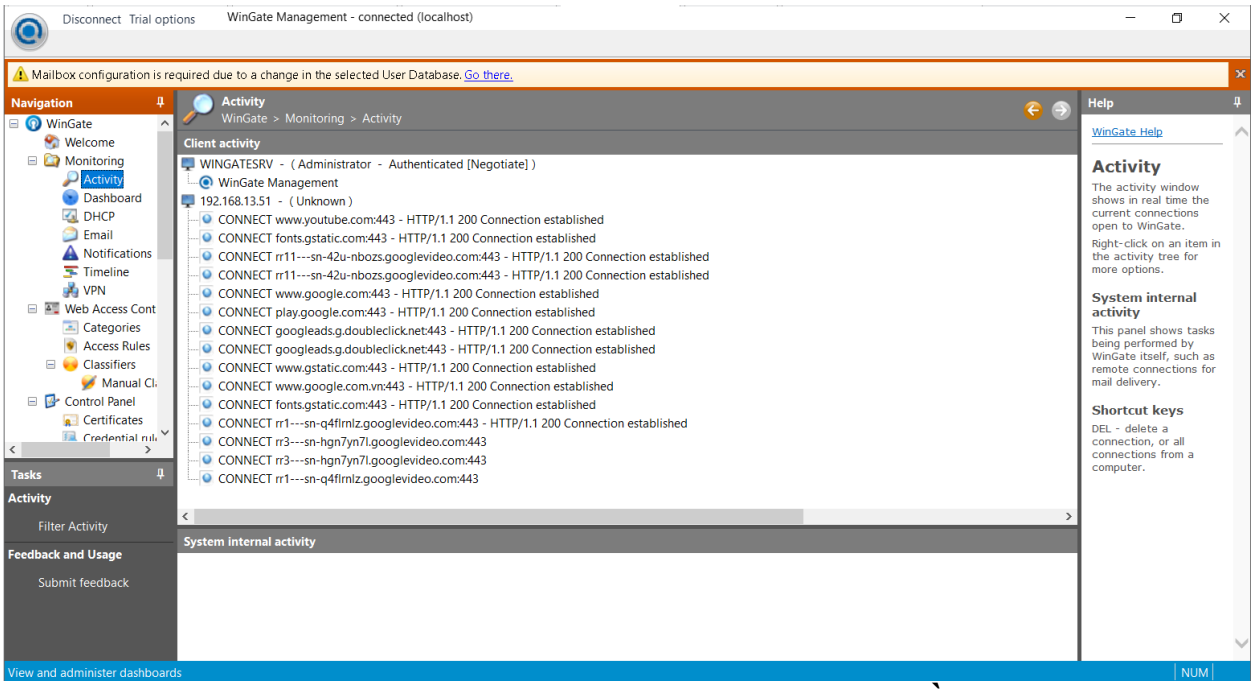
2. Proxy theo dõi truy cập mạng và chặn truy cập trang web nhất định



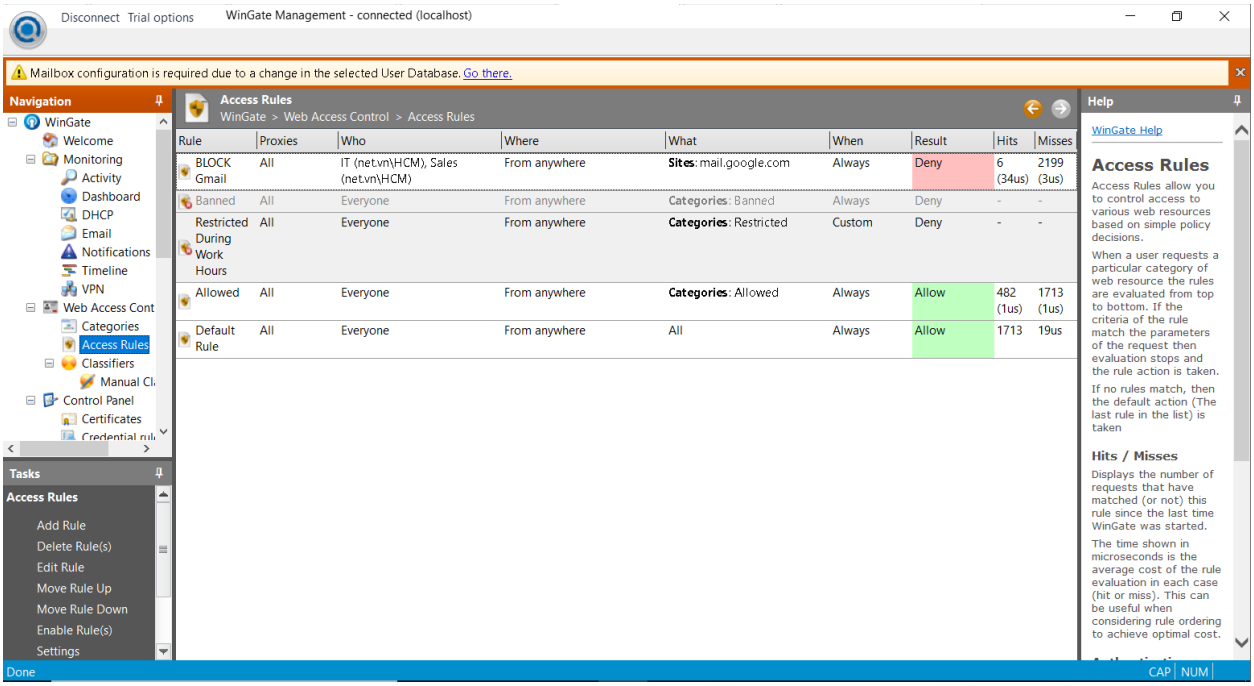
Hình 5: Proxy theo dõi truy cập mạng



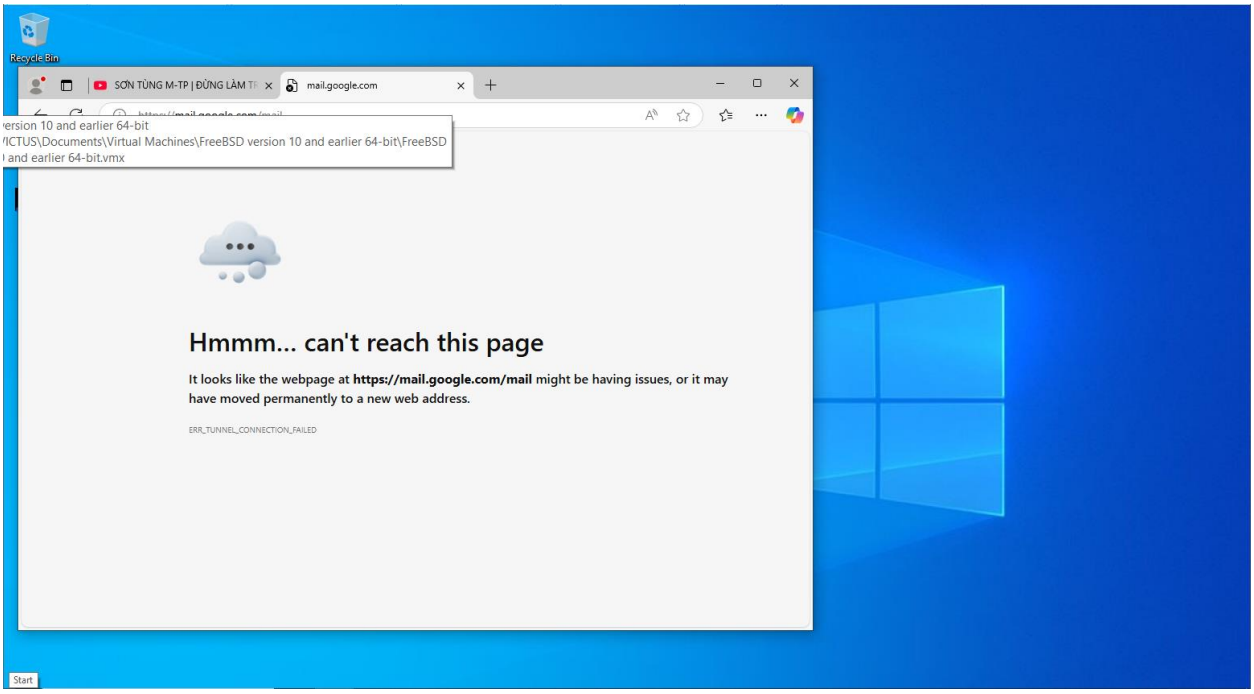
Hình 6: Khi người dùng truy cập mạng



Hình 7: Thông báo truy cập mạng được gửi về proxy

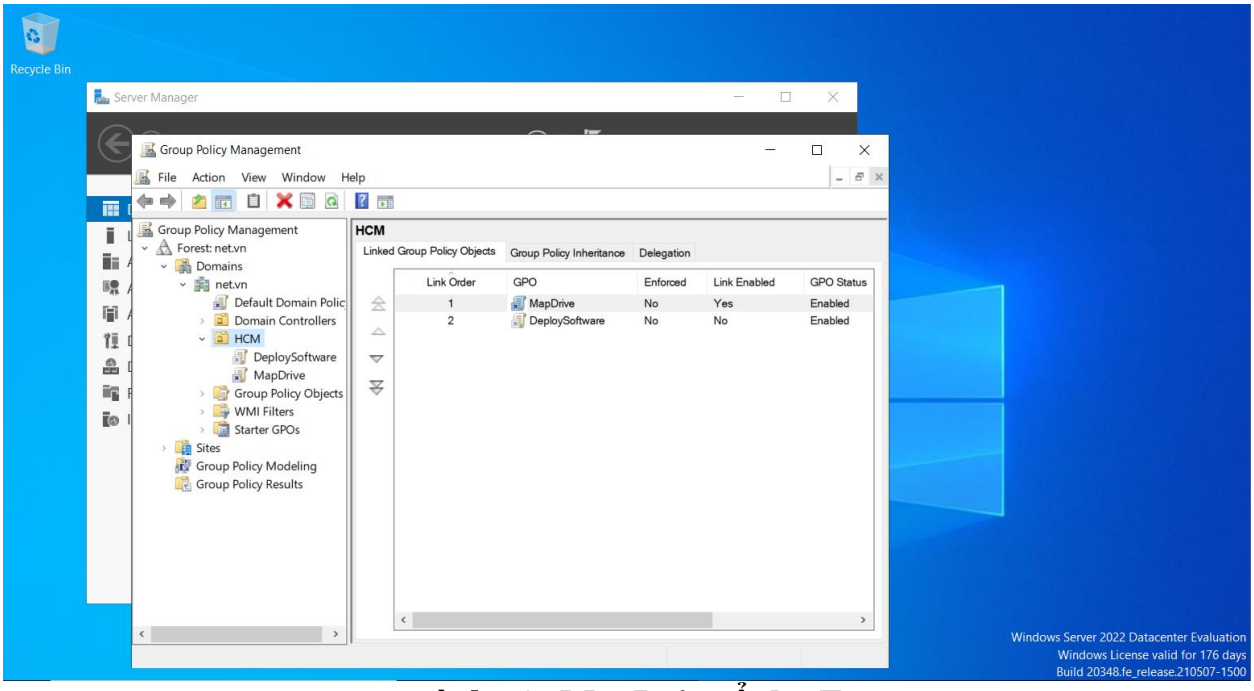


Hình 8: Rule chặn truy cập Gmail

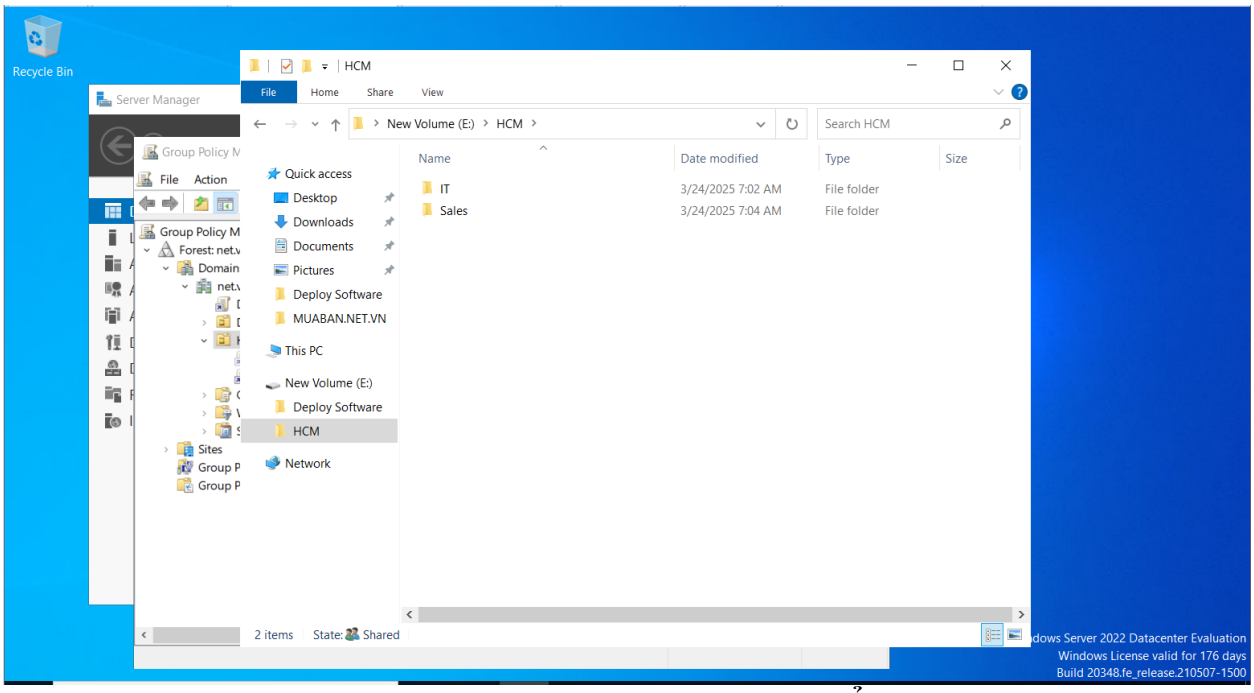


Hình 9: Màn hình của máy user khi truy cập Gmail

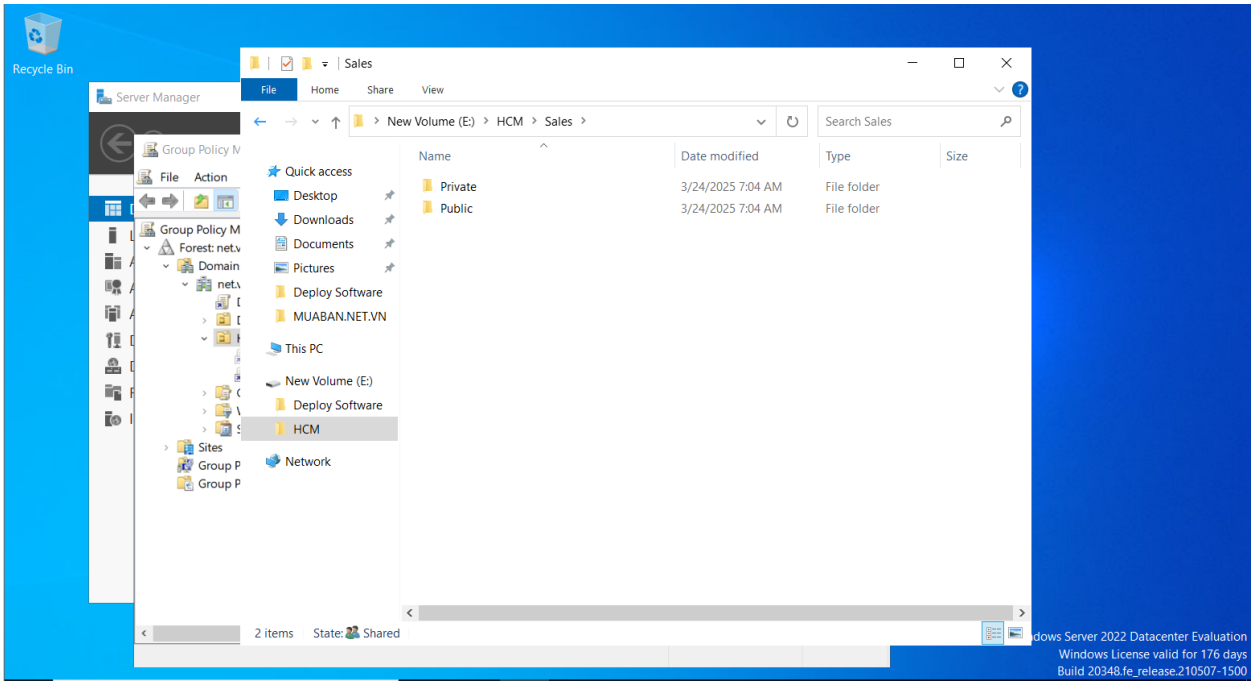
3. GPO MapDrive



Hình 10: MapDrive ổ đĩa E

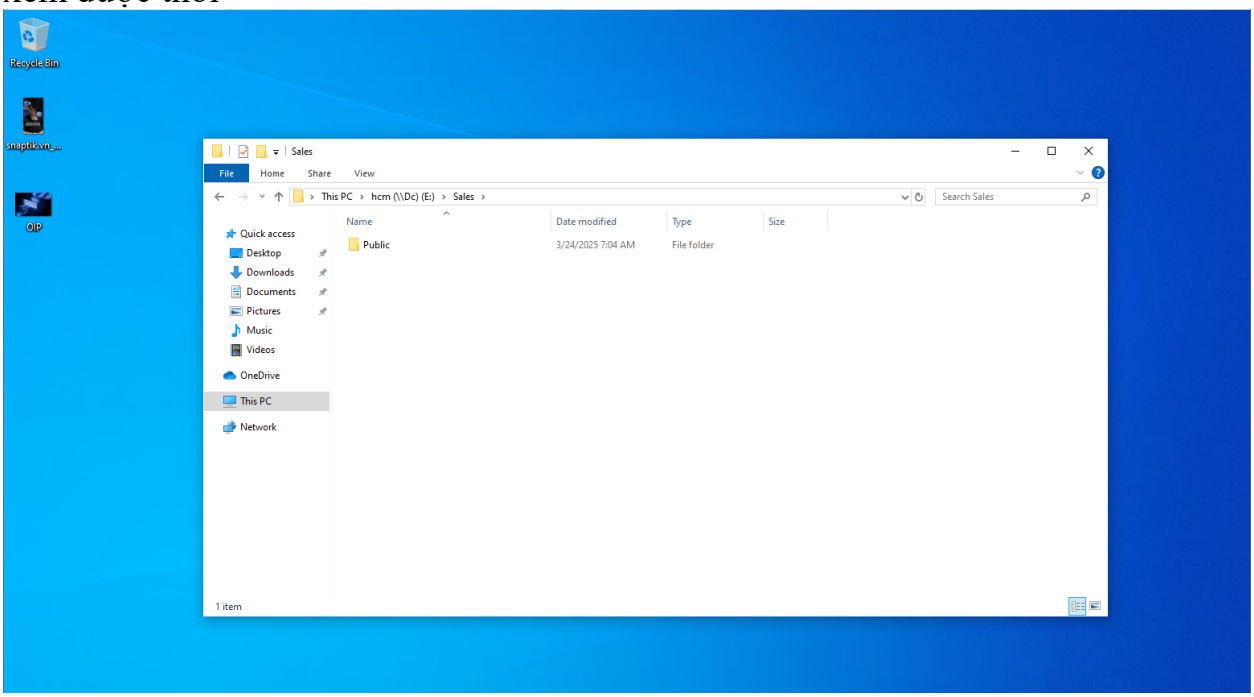


Hình 11: Tạo 2 thư mục cha trong ổ đĩa E

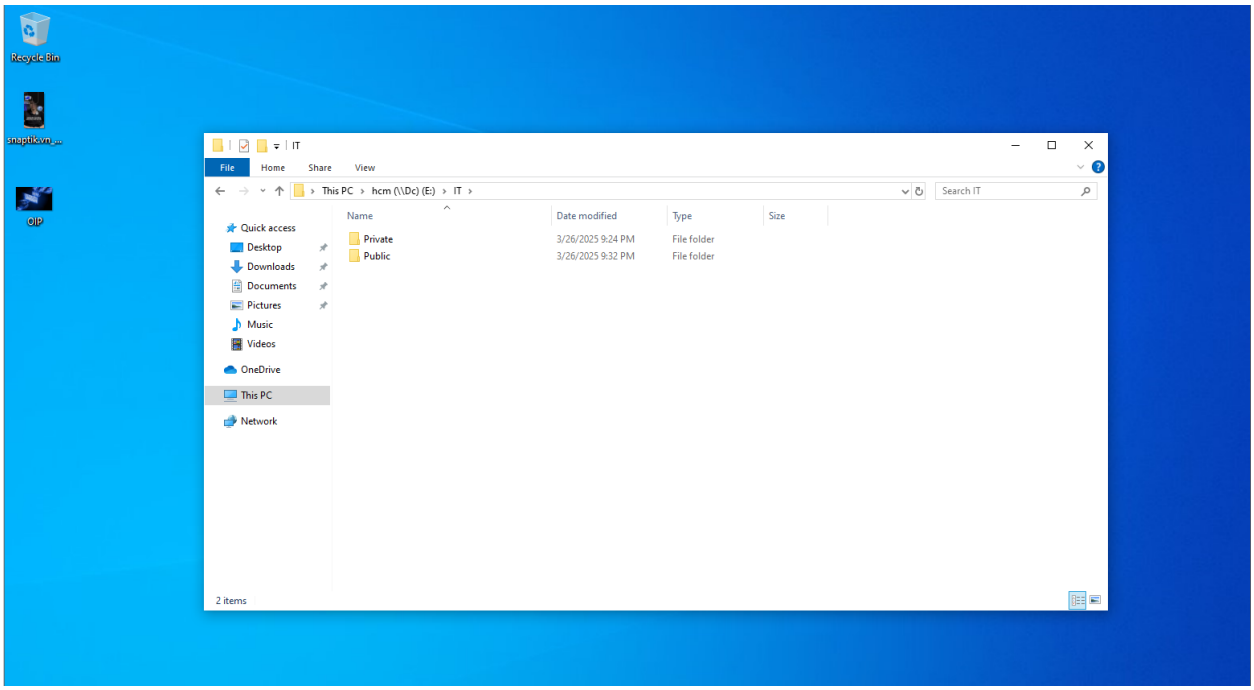


Hình 12: Tạo thêm 2 thư mục con là Private và Public trong 2 thư mục trên

Với Public thì ai cũng có thể vào xem được nhưng với Private thì chỉ phòng ban đó xem được thôi

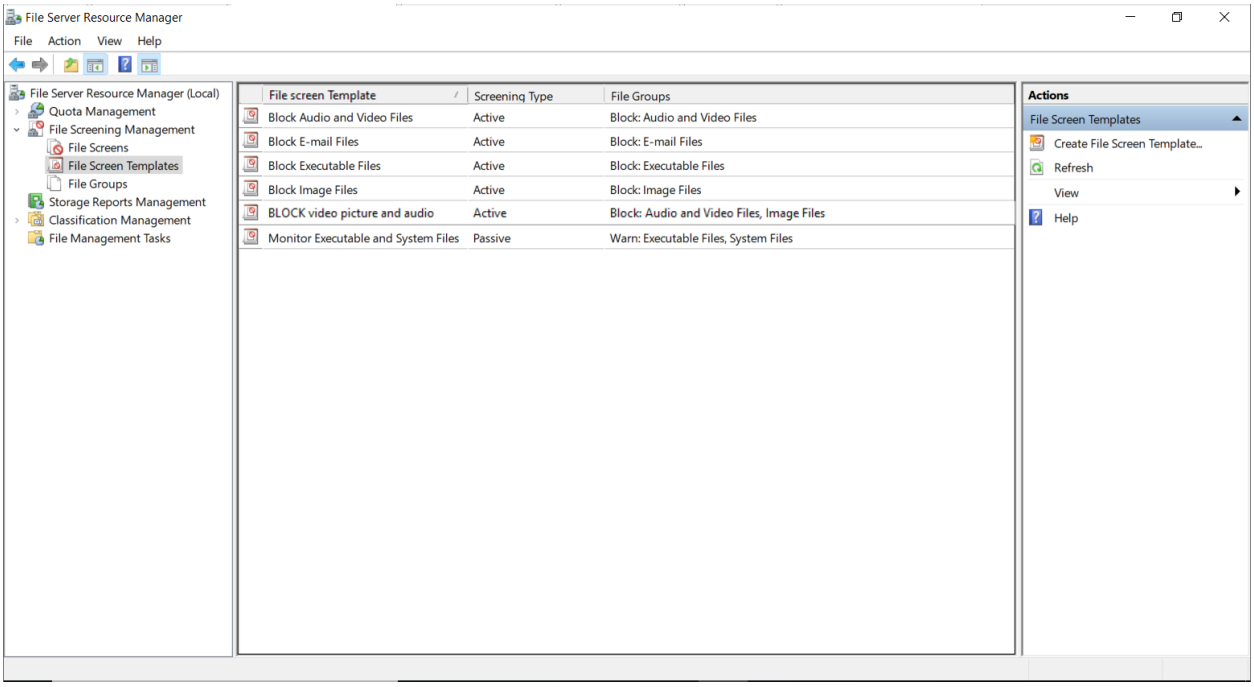


Hình 13: Đây là góc nhìn của user phòng IT trong thư mục Sale

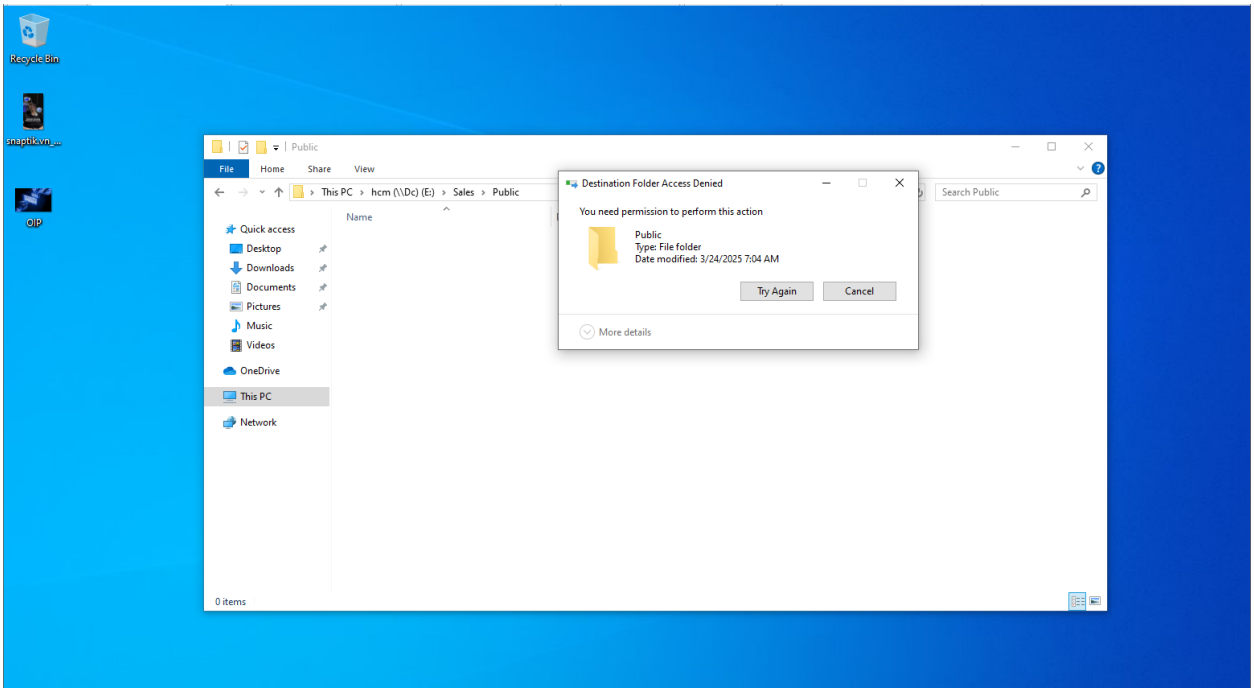


Hình 14: Đây là góc nhìn của user phòng IT trong thư mục IT

4. File Screening

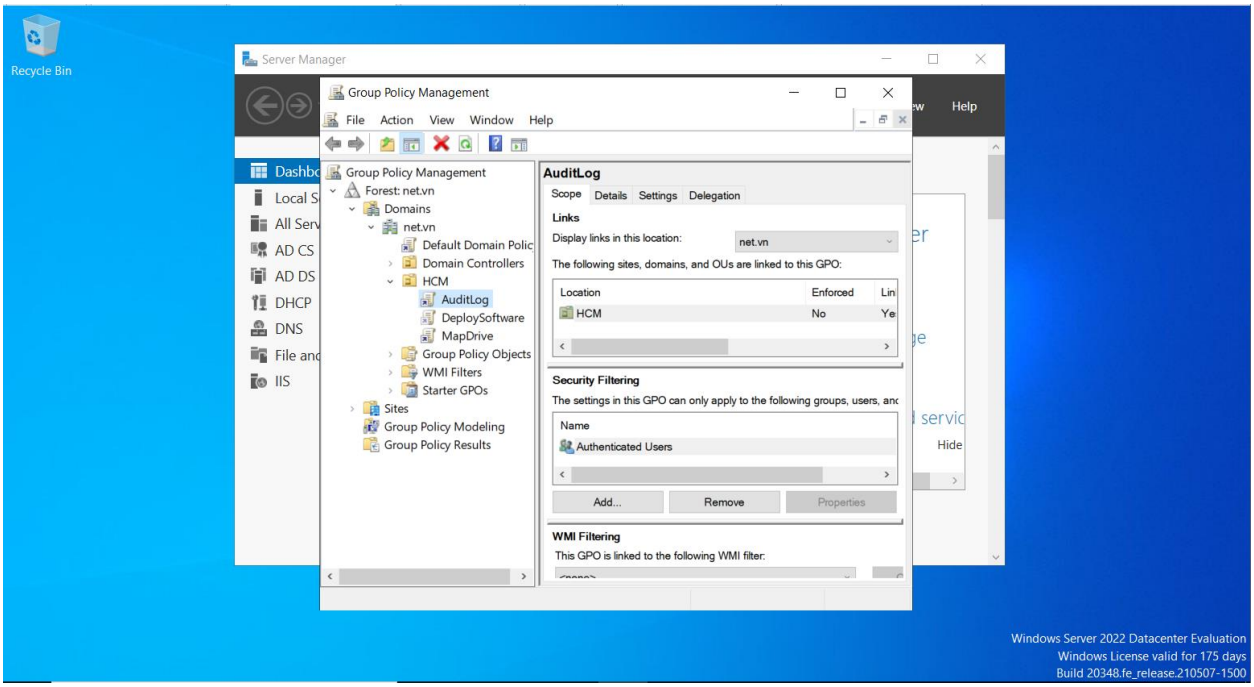


Hình 15: Chặn User gửi file dưới định dạng video, picture và audio

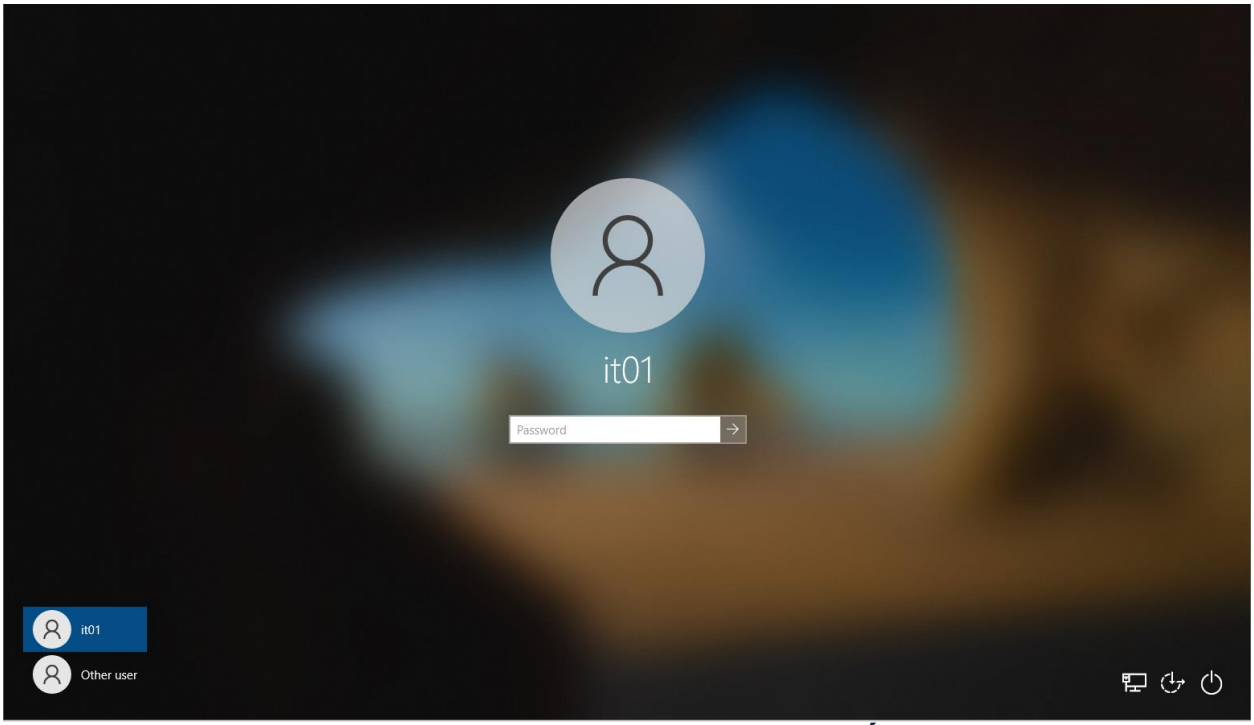


Hình 16: Khi user gửi file video, picture hoặc audio sẽ bị chặn

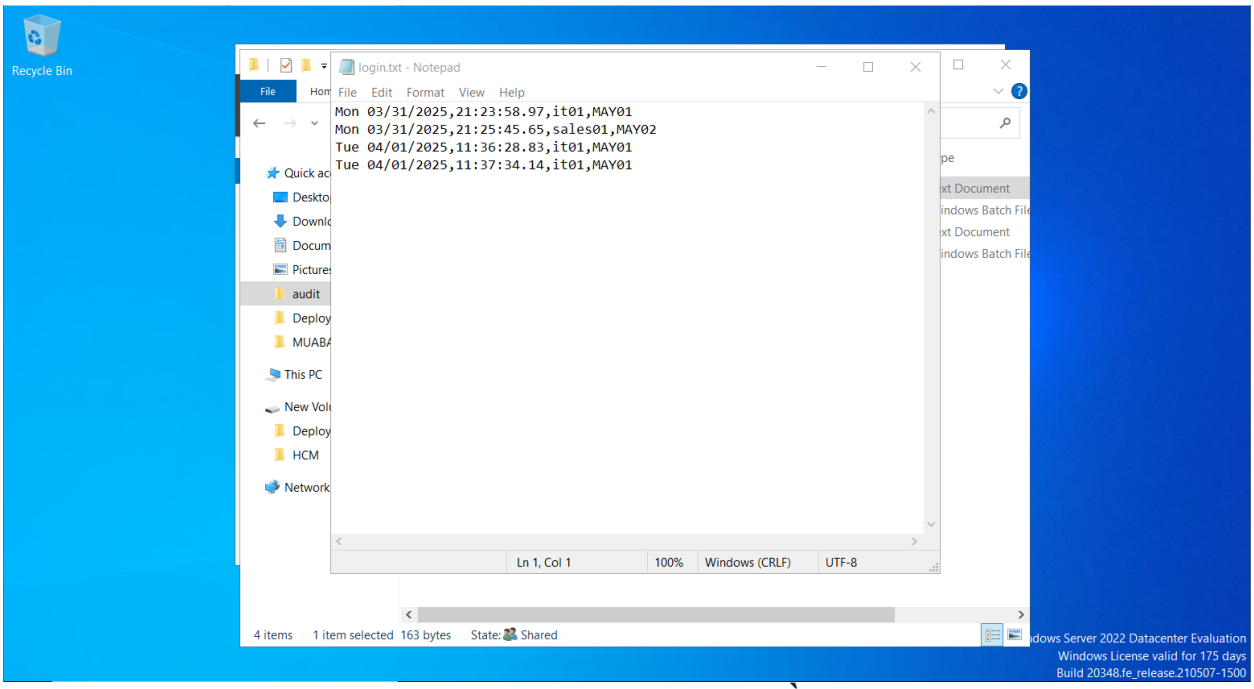
5. GPO auditlog



Hình 17: Theo dõi tình trang đăng nhập của máy User

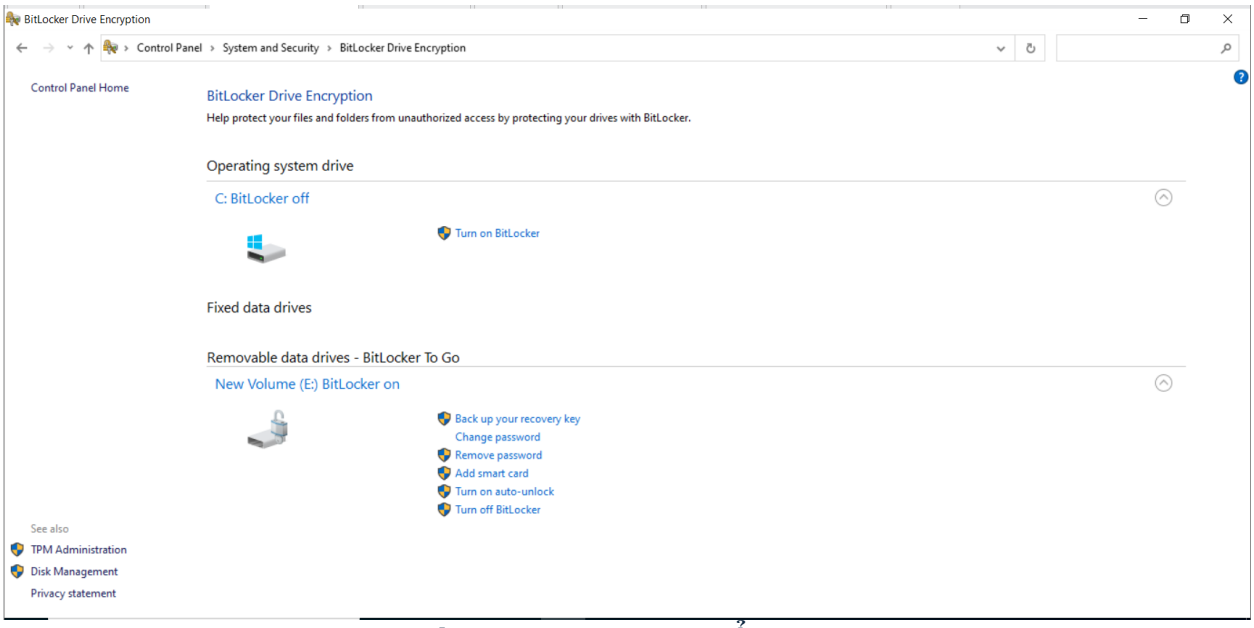


Hình 18: Khi User đăng nhập hoặc tắt máy

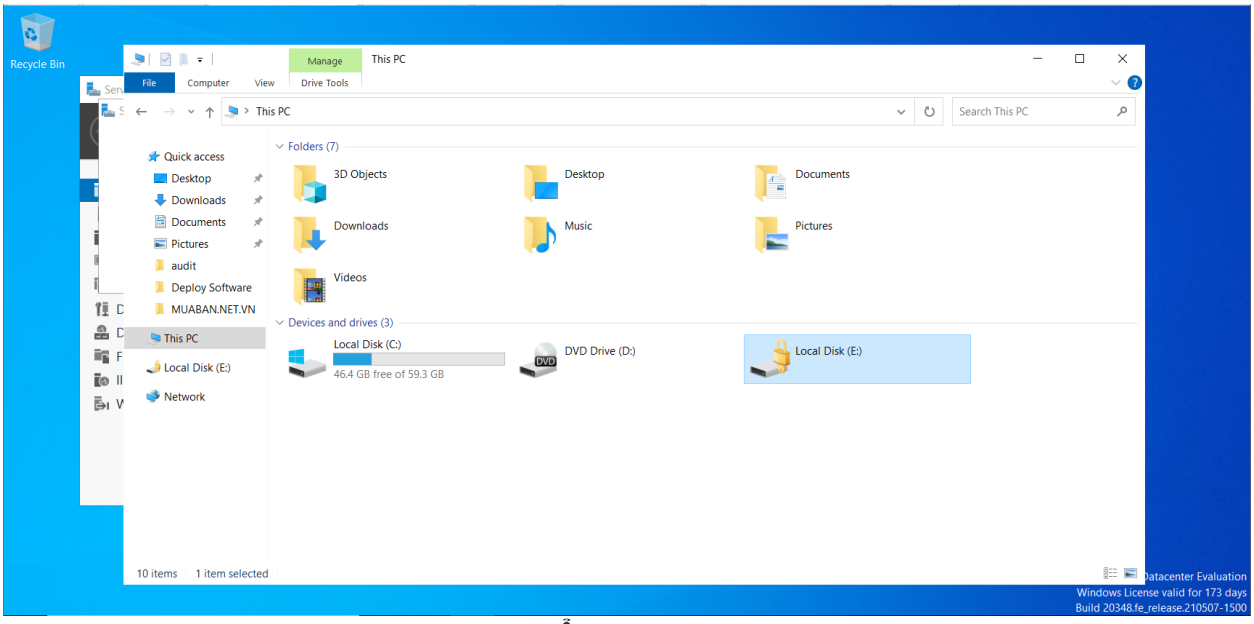


Hình 19: Thông báo sẽ gửi về Server

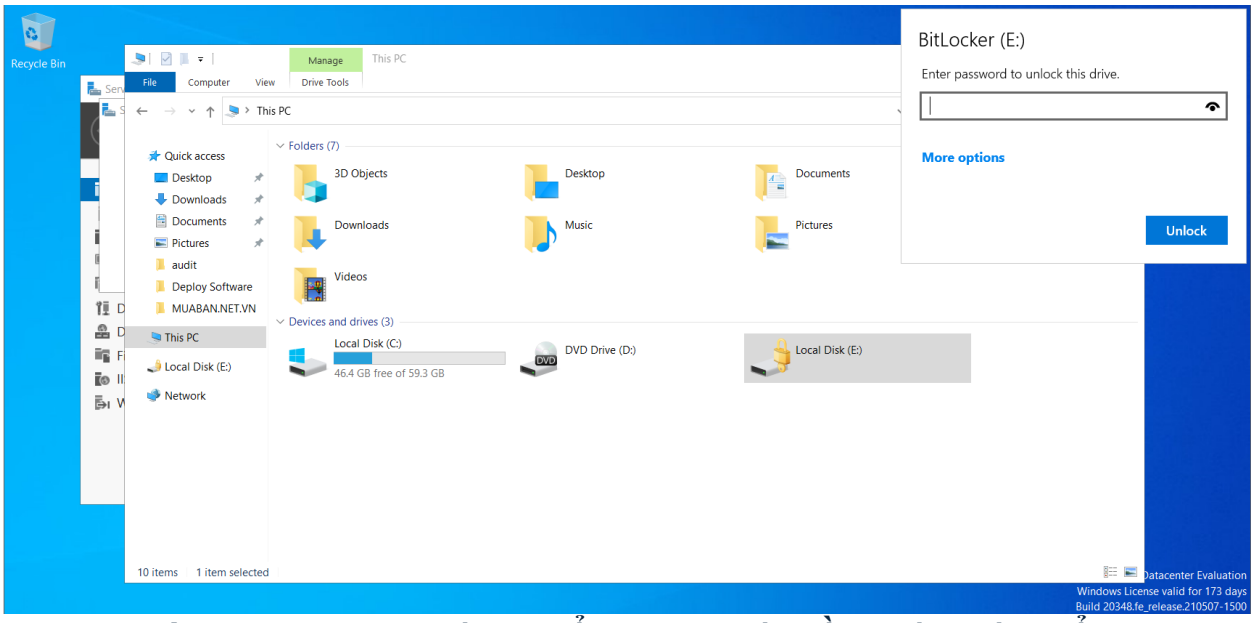
6. BitLocker



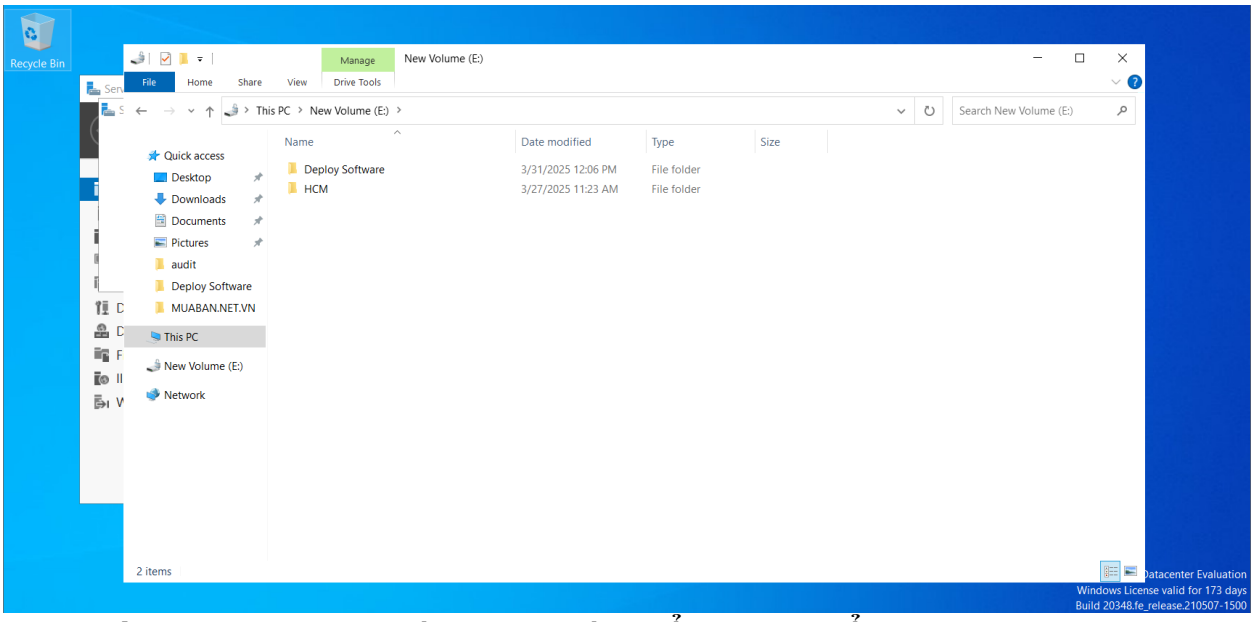
Hình 20: BitLocker ổ đĩa E



Hình 21: Ổ đĩa E đã bị khóa



Hình 22: Khi truy cập vào ổ đĩa sẽ bị yêu cầu nhập mật khẩu



Hình 23: Sau khi nhập đúng mật khẩu thì có thể vào được thư mục

Kết luận

I. Đã làm được

Đồ án Quản trị hệ thống bảo mật này của nhóm đã hoàn thành được 6 thứ: IDS Suricata trên pfSense, Proxy theo dõi truy cập mạng, GPO MapDrive, GPO auditlog, File Sceening, BitLocker

II. Chưa làm được

Vẫn chưa hoàn thành chuyên sâu các rule Suricata trong pfSense

III. Hướng phát triển

Hoàn thiện hơn các rule Suricata trong pfSense

IV. Bảng phân công công việc

Tên thành viên	Công việc
Phạm Đức Thiên Phúc	Làm VMware
Nguyễn Công Khang	Tìm tài liệu, làm Word, hỗ trợ
Nguyễn Minh Đức	Tìm tài liệu, làm Word, hỗ trợ
Lê Viết Nam	Tìm tài liệu, làm Word, hỗ trợ