

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: QUẢN TRỊ HỆ THỐNG BẢO MẬT**

**ĐỀ TÀI: XÂY DỰNG CHIẾN LƯỢC BẢO MẬT CHO HỆ THỐNG  
THÔNG TIN DOANH NGHIỆP**

**Giáo Viên Hướng Dẫn:** ThS. Đinh Xuân Lâm

**Thành Viên:**

1. Nguyễn Thị Kim Doanh – MSSV:  
22DH110511
2. Nguyễn Thúy Vy – MSSV:  
22DH114363
3. Lê Tường Vi – MSSV: 22DH114421

*Tp. Hồ Chí Minh, Ngày Tháng 03 Năm 2025*

## LỜI CẢM ƠN

Chúng em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến tất cả thầy cô Trường Đại Học Ngoại Ngữ - Tin Học TP. Hồ Chí Minh nói chung cùng thầy cô trong Khoa Công Nghệ Thông Tin nói riêng đã tận tình giảng dạy, truyền đạt những kiến thức và kinh nghiệm quý báu cho chúng em trong suốt quá trình học tập tại trường.

Trong suốt thời gian nhóm làm bài báo cáo đề tài môn Quản trị Hệ thống Bảo mật, chúng em xin gửi lời cảm ơn chân thành và sâu sắc đến Thầy Đinh Xuân Lâm, người đã hết lòng giúp đỡ và theo sát nhóm chúng em trong suốt quá trình thực hiện đề tài đồ án môn học này, chỉ ra cho nhóm hướng đi để nhóm có thể hoàn thành tốt nhất bài báo cáo đề tài đồ án này đúng thời hạn quy định.

Trong quá trình thực hiện đề tài môn Quản trị Hệ thống Bảo mật dù nhóm đã cố gắng hoàn thiện đề tài một cách tối ưu nhất nhưng do thời gian và kiến thức còn hạn chế nên sẽ không tránh khỏi những thiếu sót và sai sót nhất định, rất mong nhận được sự cảm thông từ những đóng góp ý chân thành từ quý thầy cô khoa Công Nghệ Thông Tin.

Sau cùng chúng em xin gửi lời cảm ơn đến tất cả các bạn đã tham gia đóng góp ý kiến và giúp đỡ em trong suốt quá trình thực hiện đề tài môn Quản trị Hệ thống Bảo mật

Chúng em xin chân thành cảm ơn!

---

## MỤC LỤC

Thành Viên: .....	1
LỜI CẢM ƠN.....	2
MỤC LỤC .....	1
DANH MỤC HÌNH ẢNH.....	3
CHƯƠNG I: GIỚI THIỆU VỀ DOANH NGHIỆP .....	1
1. Lĩnh vực kinh doanh.....	1
2. Tổ chức, qui mô (chi nhánh, số lượng) .....	1
3. Hoạt động kinh doanh.....	1
CHƯƠNG II: LÝ THUYẾT TỔNG QUAN.....	3
1. Lý do chọn đề tài .....	3
2. Mục tiêu đề tài.....	3
3. Đối tượng và phạm vi nghiên cứu .....	3
4. Các dịch vụ triển khai .....	4
5. Các dịch vụ bảo vệ mạng.....	6
6. Các mối đe dọa an toàn hệ thống mạng .....	14
CHƯƠNG III. XÂY DỰNG VÀ TRIỂN KHAI GIẢI PHÁP BẢO MẬT .....	17
1. Yêu cầu doanh nghiệp .....	17
1.1 Yêu cầu kỹ thuật .....	17
1.2 Yêu cầu nghiệp vụ kinh doanh .....	17
2. Xây dựng giải pháp.....	18
2.1. Sơ đồ vật lý:.....	18
2.2. Sơ đồ logic:.....	19
3. Chính sách bảo mật vật lý: .....	19
4. Chính sách bảo mật Hệ điều hành: .....	20
5. Chính sách bảo mật mạng: .....	22
6. Bảng ước tính chi phí.....	23
7. Các thảm họa và Kế hoạch phục hồi sau thảm họa.....	23

7.1 Hư hệ điều hành và Kế hoạch phục hồi .....	23
Cách khắc phục: .....	24
7.2 Hư phần cứng và Kế hoạch phục hồi .....	24
Cách khắc phục .....	25
7.3 Bị virus mã độc và Kế hoạch phục hồi .....	25
Cách khắc phục: .....	25
7.4 Server bị hack và Kế hoạch phục hồi.....	26
Cách khắc phục: .....	26
8. Triển khai .....	28
9. Triển khai các bảo mật.....	36
9.1 Server.....	37
9.2 LAN:.....	44
9.3 Wifi: .....	54
9.4 Group Policy: .....	59
CHƯƠNG IV. KẾT LUẬN.....	61
Kết quả đạt được .....	61
TÀI LIỆU THAM KHẢO .....	62

## DANH MỤC HÌNH ẢNH

Hình 1. Giả lập cửa hàng DVV .....	2
Hình 2. VPN .....	8
Hình 3. Tấn công mạng .....	16
Hình 4. Sơ đồ vật lý .....	18
Hình 5. Sơ đồ logic .....	19
Hình 6. Tầng trệt .....	28
Hình 7. Cửa ở sảnh .....	28
Hình 8. Phòng kinh doanh .....	29
Hình 9. Phòng Marketing .....	29
Hình 10. Phòng làm việc Tầng 1 .....	30
Hình 11. Sảnh .....	30
Hình 12. Phòng hành chính nhân sự .....	31
Hình 13. Phòng kế toán .....	31
Hình 14. Phòng làm việc tầng 2 .....	32
Hình 15. Sảnh .....	32
Hình 16. Phòng bảo hành kỹ thuật .....	33
Hình 17. Phòng IT và Server .....	33
Hình 18. Tầng 3 .....	34
Hình 19. Phòng Giám Đốc .....	34
Hình 20. Cửa phòng Giám Đốc .....	35
Hình 21. Vị trí khác trong Phòng Giám Đốc .....	35
Hình 22. Các dự định bảo mật sẽ triển khai .....	36
Hình 23. Trang web HTTP .....	37
Hình 24. Trang web HTTPS .....	38
Hình 25. Các users không thể gửi file quá 5MB .....	39
Hình 26. Bitlocker Pass: abc@123456789 .....	40
Hình 27. Mã hóa ổ E chứa dữ liệu .....	41
Hình 28. Backup thành công .....	42
Hình 29. Dữ liệu đã Backup .....	43
Hình 30. Rule của máy LAN: .....	44
Hình 31. Truy xuất dữ liệu phòng ban .....	45
Hình 32. Không thể truy xuất thanhvien.vn .....	46
Hình 33. Không thể truy cập tuoitre.vn .....	47
Hình 34. Không thể ping tới thanhvien.vn và facebook.com .....	48
Hình 35. Truy suất web .....	48
Hình 36. Truy xuất Youtube.com .....	49
Hình 37. truy xuất Facebook.com .....	50
Hình 38. Truy xuất Google.com .....	51
Hình 39. Join vào domain .....	52
Hình 40. Rule Wifi .....	54
Hình 41. Truy xuất Facebook.com .....	55
Hình 42. Truy suất Youtube.com .....	56
Hình 43. Truy xuất web .....	56

Hình 44. Cắm ping .....	57
Hình 45. Không thể Join Domain .....	58
Hình 46. Cắm USB ghi dữ liệu.....	59
Hình 47. Yêu cầu mật khẩu.....	60

## **CHƯƠNG I: GIỚI THIỆU VỀ DOANH NGHIỆP**

### **1. Lĩnh vực kinh doanh**

Công ty DVV là doanh nghiệp chuyên kinh doanh các linh kiện thiết bị điện tử tại Việt Nam. Bao gồm: điện thoại thông minh, máy tính xách tay, PC, máy tính bảng, thiết bị âm thanh, thiết bị gia dụng thông minh, phụ kiện điện tử và các thiết bị điện tử tiêu dùng khác. Được thành lập vào đầu năm 2025. Dù mới thành lập nhưng công ty chúng tôi đã nhanh chóng phát triển và khẳng định được trên thị trường kinh doanh nhờ các sản phẩm chất lượng, mức giá hợp lý phù hợp với người tiêu dùng và các khuyến mãi để tạo điều kiện dành cho học sinh sinh viên, chế độ bảo hành và dịch vụ chuyên nghiệp.

### **2. Tổ chức, qui mô (chi nhánh, số lượng)**

Công ty có trụ sở văn phòng và cửa hàng tại Thành phố Hồ Chí Minh

Tổng số nhân viên: 85 người, trong đó:

- Ban giám đốc: 3 người
- Phòng kinh doanh: 20 người
- Phòng kỹ thuật và bảo hành: 20 người
- Phòng marketing: 15 người
- Phòng hành chính nhân sự: 10 người
- Phòng tài chính kế toán: 15 người
- Phòng IT: 2 người

### **3. Hoạt động kinh doanh**

Công ty triển khai các hoạt động kinh doanh sau:

- Phân phối và bán lẻ các sản phẩm điện tử từ nhiều thương hiệu uy tín như Apple, Samsung, Xiaomi, MiniGo,...
- Cung cấp dịch vụ bảo hành, sửa chữa và hỗ trợ kỹ thuật
- Tư vấn và thiết kế giải pháp công nghệ cho doanh nghiệp và cá nhân
- Kinh doanh trực tuyến thông qua website và các sàn thương mại điện tử như Shopee, Tiki, Lazada trong nước và Taobao, Amazone, Alibaba ngoài nước
- Nhập khẩu và phân phối độc quyền một số dòng sản phẩm điện tử
- Tổ chức các sự kiện, hội thảo giới thiệu sản phẩm công nghệ mới
- Triển khai chương trình khách hàng thân thiết và các chương trình khuyến mãi định kỳ
- Cung cấp các gói bảo hành và dịch vụ sau khi mua sản phẩm

Công ty DVV không trực tiếp sản xuất linh kiện mà hoạt động theo mô hình nhập khẩu và phân phối từ các nhà cung cấp uy tín hàng đầu thế giới. Công ty cũng đang phát triển các dịch vụ mới như cho thuê thiết bị điện tử, triển khai giải pháp smarthome và cung cấp dịch vụ tư vấn chuyển đổi số cho doanh nghiệp vừa và nhỏ.



Hình 1. Giả lập cửa hàng DVV



## CHƯƠNG II: LÝ THUYẾT TỔNG QUAN

### 1. Lý do chọn đề tài

Đề tài là sự dựa trên tính cấp thiết ngày càng gia tăng trong môi trường kinh doanh số hiện nay. Với làn sóng chuyển đổi số diễn ra mạnh mẽ, các doanh nghiệp đang phụ thuộc nhiều hơn vào hệ thống thông tin, đồng thời đối mặt với các mối đe dọa an ninh mạng ngày càng tinh vi và phức tạp.

Các vụ tấn công mạng đã tăng đáng kể về số lượng và mức độ nghiêm trọng, gây thiệt hại lớn về tài chính và uy tín doanh nghiệp. Theo thống kê gần đây, chi phí trung bình của một vụ vi phạm dữ liệu có thể lên đến hàng triệu đô la, bao gồm cả thiệt hại trực tiếp và gián tiếp như gián đoạn hoạt động, mất dữ liệu và suy giảm niềm tin khách hàng.

Bên cạnh đó, các quy định pháp lý về bảo vệ dữ liệu đang được tăng cường trên toàn cầu, đòi hỏi doanh nghiệp phải có biện pháp bảo vệ thông tin hiệu quả. Một chiến lược bảo mật toàn diện không chỉ giúp phòng ngừa rủi ro mà còn tạo lợi thế cạnh tranh, đảm bảo sự phát triển bền vững trong kỷ nguyên số.

### 2. Mục tiêu đề tài

Mục tiêu đề tài được đưa ra nhằm đảm bảo các tài sản thông tin và đảm bảo hoạt động kinh doanh liên tục. Nhằm giúp nhận diện và đánh giá các rủi ro bảo mật đối với tài sản thông tin quan trọng, xây dựng khung chính sách và quy trình bảo mật phù hợp với đặc thù doanh nghiệp, thiết kế giải pháp kỹ thuật bảo vệ hạ tầng mạng, hệ thống và ứng dụng, phát triển năng lực ứng phó sự cố và phục hồi sau thảm họa, nâng cao nhận thức bảo mật cho nhân viên và đảm bảo tuân thủ quy định pháp lý.

### 3. Đối tượng và phạm vi nghiên cứu

Đề tài tập trung nghiên cứu về chiến lược bảo mật cho hệ thống thông tin doanh nghiệp, với đối tượng nghiên cứu chính là toàn bộ hệ thống các doanh nghiệp bao gồm hạ tầng mạng, máy chủ, ứng dụng và dữ liệu. Bên cạnh đó, đề tài cũng xem xét các mối đe dọa bảo mật đang tồn tại như các hình thức tấn công mạng, lỗ hổng bảo mật và rủi ro từ yếu tố con người.

Về phạm vi, nghiên cứu hướng đến các doanh nghiệp vừa và lớn có hệ thống phức tạp, tập trung vào bốn lĩnh vực chính: bảo mật hạ tầng mạng, bảo mật hệ thống và ứng dụng, bảo mật dữ liệu, và quản lý danh tính và truy cập. Đề tài bao quát các khía cạnh quản lý từ đánh giá rủi ro, xây dựng chính sách đến giám sát và ứng phó sự cố, đồng thời đảm bảo tuân thủ các quy định pháp lý và tiêu chuẩn quốc tế về bảo mật thông tin.

Nghiên cứu sẽ không đi sâu vào chi tiết kỹ thuật của các công cụ bảo mật cụ thể, không bao gồm giải pháp bảo mật vật lý cho trung tâm dữ liệu, và không tập trung vào các vấn đề bảo mật của hệ thống IoT. Trọng tâm chính là xây dựng một khung chiến lược bảo mật toàn diện và có thể áp dụng được cho nhiều loại hình doanh nghiệp khác nhau.

## 4. Các dịch vụ triển khai

### 4.1 Active Directory Domain Services

ADDS (Active Directory Domain Services) là một dịch vụ của Windows Server cung cấp cho phép quản lý tập trung các tài nguyên, người dùng, máy tính, nhóm, chính sách bảo mật và các dịch vụ khác trong một mạng lưới. ADDS sử dụng một cơ sở dữ liệu phân cấp và phân tán để lưu trữ các đối tượng và thuộc tính của chúng. ADDS cũng cung cấp các dịch vụ như xác thực, ủy quyền, cấu hình, đồng bộ hóa và tìm kiếm. ADDS có thể được triển khai trên nhiều máy chủ để tăng độ tin cậy và hiệu suất. Nhóm sử dụng Windows Server 2016 để triển khai ADDS với mục đích tạo một miền cho hệ thống, quản lý các tài khoản người dùng và máy tính.

### 4.2 Dynamic Host Configuration Protocol

DHCP (Dynamic Host Configuration Protocol) là một giao thức cung cấp cho phép cấp phát địa chỉ IP và các thông số cấu hình mạng khác cho các máy tính và thiết bị kết nối vào mạng một cách tự động và linh hoạt. DHCP giúp giảm thiểu công việc cấu hình thủ công cho mỗi máy tính, tránh xung đột địa chỉ IP và quản lý hiệu quả dải địa chỉ IP. DHCP hoạt động theo mô hình client-Server, trong đó một máy chủ DHCP sẽ cấp phát địa chỉ IP cho các máy khách DHCP theo yêu cầu.

### 4.3 DNS (Domain Name System)

DNS (Domain Name System - Hệ thống tên miền) là một hệ thống phân cấp phân tán được sử dụng để dịch tên miền (ví dụ: [google.com](https://www.google.com)) thành địa chỉ IP (ví dụ: 172.217.160.142) và ngược lại. DNS đóng vai trò quan trọng trong việc giúp người dùng truy cập các trang web và dịch vụ trực tuyến một cách dễ dàng hơn.

**Tấn công DNS:** DNS có thể bị tấn công bởi các tin tặc, dẫn đến việc chuyển hướng người dùng đến các trang web giả mạo.

**DNSSEC (Domain Name System Security Extensions):** Là một bộ mở rộng bảo mật cho DNS, giúp bảo vệ chống lại các cuộc tấn công DNS.

### 4.4 File Server (Máy chủ tập tin)

Là một máy tính hoặc hệ thống lưu trữ chuyên dụng được kết nối với mạng, có nhiệm vụ chính là lưu trữ và quản lý các tệp tin dữ liệu để các máy tính khác trong mạng có thể truy cập và chia sẻ.

#### Các giao thức thường dùng:

- **SMB/CIFS (Server Message Block/Common Internet File System):**
  - Giao thức phổ biến trong môi trường Windows, cho phép chia sẻ tệp tin và máy in.

- **NFS (Network File System):**
  - Giao thức phổ biến trong môi trường Unix/Linux, cho phép chia sẻ tệp tin qua mạng.
- **FTP (File Transfer Protocol):**
  - Giao thức dùng để truyền tải tệp tin qua mạng Internet.
- **HTTP/HTTPS (Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure):**
  - Giao thức dùng để truyền tải tệp tin qua web.

#### 4.5 IIS (Internet Information Services)

Là một máy chủ web được phát triển bởi Microsoft, chạy trên hệ điều hành Windows. Nó được sử dụng để lưu trữ, cung cấp và quản lý các trang web, ứng dụng web và các dịch vụ trực tuyến khác.

##### Các thành phần chính:

- **HTTP.sys:**
  - Là trình điều khiển chế độ kernel xử lý các yêu cầu HTTP.
- **Worker Processes:**
  - Là các tiến trình thực thi mã ứng dụng web.
- **Application Pools:**
  - Là các nhóm worker processes chia sẻ cùng một cấu hình.
- **Modules:**
  - Là các thành phần phần mềm mở rộng chức năng của IIS.
- **Handlers:**
  - Là các thành phần phần mềm xử lý các yêu cầu cho các loại tệp tin cụ thể.

#### 4.6 DHCP Failover

DHCP Failover là tính năng cho phép 2 Server chạy dịch vụ DHCP có thể liên kết và đồng bộ dữ liệu với nhau, 2 Server sẽ thay nhau cấp ip cho các máy client trong hệ thống, với mục đích tăng độ sẵn sàng và tính liên tục cho hệ thống.

DHCP Failover có 2 cơ chế:

- **Load Balancing:** đây là chế độ cho phép 2 DHCP Server có thể hoạt động song song với nhau, cùng nhau cấp ip cho các máy client trong hệ thống, 2 máy này hoạt động theo tỷ lệ phân chia được thiết lập từ trước, có thể hoạt động song song nhau với tỷ lệ 50-50 hoặc một máy chính 1 máy phụ với tỷ lệ 70-30.
- **Hot Standby:** chế độ hoạt động cho phép 1 Server DHCP làm dịch vụ cung cấp ip tất cả các máy client trong hệ thống, máy còn lại sẽ ở trong trạng thái standby, Server trong trạng thái này chỉ để dự phòng và không hoạt động,

khi Server DHCP chính bị lỗi Server dự phòng sẽ lập tức thay thế và tiếp tục cung cấp ip thay cho Server DHCP chính.

Nhóm sử dụng cơ chế Hot Standby của DHCP Failover cho Backup Server để làm dự phòng cho Server DHCP để khi có những sự cố với Server DHCP thì Backup Server sẽ lập tức đứng ra thay thế cấp DHCP cho các máy client đảm bảo tính liên tục cho hệ thống.

#### 4.7 Windows Server Backup

Windows Server Backup là công cụ được tích hợp vào Windows Server từ phiên bản Windows Server 2008, đây là công cụ cung cấp tính năng sao lưu và phục hồi toàn bộ hệ thống Server, file, thư mục. Windows Server Backup có khả năng thực hiện Full Backup (Backup toàn bộ hệ thống) và Incremental Backup (sau khi sử dụng Backup toàn bộ hệ thống thì những lần Backup up sau chỉ lưu lại những thay đổi mới)

### 5. Các dịch vụ bảo vệ mạng

#### 5.1 VPN (Virtual Private Network - Mạng riêng ảo)

VPN (Virtual Private Network - Mạng riêng ảo) là một công nghệ mạng cho phép tạo ra một kết nối mạng an toàn và riêng tư qua một mạng công cộng như Internet.

#### 1. Khái niệm và nguyên lý hoạt động VPN

- **Đường hầm (Tunneling):**
  - VPN tạo ra một "đường hầm" ảo, mã hóa dữ liệu truyền tải giữa thiết bị của người dùng và máy chủ VPN.
  - Đường hầm này đảm bảo rằng dữ liệu được truyền đi một cách an toàn, không bị các bên thứ ba can thiệp hoặc đánh cắp.
- **Mã hóa (Encryption):**
  - Dữ liệu được mã hóa trước khi truyền đi qua đường hầm, biến nó thành một chuỗi ký tự không thể đọc được.
  - Chỉ máy chủ VPN và thiết bị của người dùng mới có thể giải mã dữ liệu này.
- **Ẩn địa chỉ IP (IP Masking):**
  - VPN ẩn địa chỉ IP thực của người dùng, thay thế bằng địa chỉ IP của máy chủ VPN.
  - Điều này giúp bảo vệ danh tính và vị trí của người dùng, đồng thời vượt qua các hạn chế địa lý.

#### 2. Các loại VPN:

- **Remote Access VPN:**

- Cho phép người dùng cá nhân hoặc nhân viên từ xa kết nối an toàn vào mạng nội bộ của công ty hoặc mạng riêng.
- Thường được sử dụng để truy cập các tài nguyên mạng nội bộ từ xa.
- **Site-to-Site VPN:**
  - Kết nối hai hoặc nhiều mạng LAN (Local Area Network) với nhau qua Internet.
  - Cho phép các chi nhánh của một công ty kết nối với nhau một cách an toàn.
- **Personal VPN (Consumer VPN):**
  - Dành cho người dùng cá nhân, giúp bảo vệ quyền riêng tư và bảo mật khi truy cập Internet.
  - Thường được sử dụng để ẩn danh trực tuyến, vượt qua kiểm duyệt và truy cập nội dung bị chặn.

### 3. Lợi ích của VPN:

- **Bảo mật:**
  - Mã hóa dữ liệu, bảo vệ thông tin cá nhân và dữ liệu nhạy cảm khỏi các cuộc tấn công mạng.
- **Quyền riêng tư:**
  - Ẩn địa chỉ IP, bảo vệ danh tính và vị trí của người dùng.
  - Ngăn chặn việc theo dõi hoạt động trực tuyến của người dùng.
- **Truy cập nội dung bị chặn:**
  - Vượt qua các hạn chế địa lý, truy cập các trang web và dịch vụ bị chặn ở một số quốc gia.
- **An toàn trên Wi-Fi công cộng:**
  - Bảo vệ dữ liệu khi sử dụng Wi-Fi công cộng, giảm nguy cơ bị tấn công mạng.

### 4. Các giao thức VPN phổ biến:

- **PPTP (Point-to-Point Tunneling Protocol):**
  - Giao thức cũ, không còn được coi là an toàn.
- **L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security):**
  - Giao thức an toàn hơn PPTP, thường được sử dụng kết hợp với IPsec để mã hóa dữ liệu.
- **OpenVPN:**
  - Giao thức mã nguồn mở, rất linh hoạt và an toàn.
- **WireGuard:**
  - Giao thức mới, nhanh chóng và an toàn, đang ngày càng phổ biến.
- **IKEv2 (Internet Key Exchange version 2):**
  - Nhanh và ổn định thường được sử dụng trên các thiết bị di động.

### 5. Lưu ý khi sử dụng VPN:

- **Chọn nhà cung cấp VPN uy tín:**
  - Đảm bảo nhà cung cấp VPN có chính sách bảo mật rõ ràng và không ghi nhật ký hoạt động của người dùng.

- **Hiểu rõ các giao thức VPN:**
  - Chọn giao thức VPN phù hợp với nhu cầu và mức độ bảo mật mong muốn.
- **Cập nhật phần mềm VPN thường xuyên:**
  - Đảm bảo phần mềm VPN được cập nhật để vá các lỗ hổng bảo mật.
- **Không sử dụng VPN miễn phí:**
  - Các VPN miễn phí thường có nhiều rủi ro về bảo mật và quyền riêng tư.

VPN là một công cụ hữu ích để bảo vệ quyền riêng tư và bảo mật trực tuyến. Tuy nhiên, việc sử dụng VPN cũng cần được thực hiện một cách cẩn thận và có trách nhiệm.



Hình 2. VPN



## 5.2 Proxy

Proxy là một máy chủ trung gian hoạt động giữa người dùng và Internet. Khi bạn sử dụng proxy, yêu cầu truy cập Internet của bạn sẽ được gửi đến máy chủ proxy trước, sau đó máy chủ proxy sẽ gửi yêu cầu đó đến máy chủ web đích. Máy chủ web đích sẽ trả về phản hồi cho máy chủ proxy, và máy chủ proxy sẽ chuyển tiếp phản hồi đó cho bạn.

### Các loại proxy:

- **Proxy chuyển tiếp (Forward Proxy):**
  - Đây là loại proxy phổ biến nhất.
  - Nó hoạt động như một trung gian giữa người dùng và Internet.
  - Nó thường được sử dụng để:
    - Ẩn địa chỉ IP của người dùng.
    - Vượt qua các hạn chế địa lý.
    - Kiểm soát quyền truy cập Internet.
    - Tăng tốc độ truy cập Internet bằng cách lưu trữ các trang web được truy cập thường xuyên.
- **Proxy đảo ngược (Reverse Proxy):**
  - Loại proxy này hoạt động như một trung gian giữa máy chủ web và Internet.
  - Nó thường được sử dụng để:
    - Cân bằng tải giữa nhiều máy chủ web.
    - Tăng cường bảo mật cho máy chủ web.
    - Lưu trữ các trang web để tăng tốc độ truy cập.
- **Proxy trong suốt (Transparent Proxy):**
  - Loại proxy này không ẩn địa chỉ IP của người dùng.
  - Nó thường được sử dụng bởi các tổ chức để kiểm soát quyền truy cập Internet của người dùng.
- **Proxy ẩn danh (Anonymous Proxy):**
  - Loại proxy này ẩn địa chỉ IP của người dùng.
  - Nó thường được sử dụng để bảo vệ quyền riêng tư của người dùng.
- **Proxy biến dạng (Distorting Proxy):**
  - Loại proxy này thay đổi địa chỉ IP của người dùng thành một địa chỉ IP khác.
  - Nó thường được sử dụng để vượt qua các hạn chế địa lý.

### Lợi ích của việc sử dụng proxy:

- **Bảo mật:** Proxy có thể giúp bảo vệ quyền riêng tư của bạn bằng cách ẩn địa chỉ IP của bạn.
- **Quyền riêng tư:** Proxy có thể giúp bạn truy cập các trang web bị chặn ở quốc gia của bạn.

- **Hiệu suất:** Proxy có thể giúp tăng tốc độ truy cập Internet của bạn bằng cách lưu trữ các trang web được truy cập thường xuyên.
- **Kiểm soát:** Proxy có thể được sử dụng để kiểm soát quyền truy cập Internet của người dùng trong một tổ chức.

#### **Rủi ro của việc sử dụng proxy:**

- **Bảo mật:** Một số proxy không an toàn và có thể được sử dụng để đánh cắp thông tin cá nhân của bạn.
- **Hiệu suất:** Một số proxy có thể làm chậm tốc độ truy cập Internet của bạn.
- **Tin cậy:** Không phải tất cả các proxy đều đáng tin cậy. Một số proxy có thể ghi lại hoạt động trực tuyến của bạn.

Khi chọn một proxy, điều quan trọng là phải chọn một proxy đáng tin cậy và an toàn. Bạn cũng nên cân nhắc các nhu cầu cụ thể của mình để chọn loại proxy phù hợp.

### **5.3 Tường lửa (Firewall)**

Là một hệ thống bảo mật mạng, đóng vai trò như một "người gác cổng" để giám sát và kiểm soát lưu lượng mạng ra vào. Nó thiết lập một rào cản giữa mạng nội bộ (mạng riêng của bạn) và mạng bên ngoài (thường là Internet), giúp bảo vệ mạng khỏi các truy cập trái phép và các mối đe dọa từ bên ngoài.

#### **1. Chức năng chính:**

- **Kiểm soát truy cập:**
  - Tường lửa kiểm tra các gói dữ liệu ra vào mạng dựa trên các quy tắc bảo mật được thiết lập.
  - Nó cho phép hoặc chặn các gói dữ liệu dựa trên địa chỉ IP nguồn và đích, cổng, giao thức và nội dung.
- **Ngăn chặn truy cập trái phép:**
  - Tường lửa giúp ngăn chặn tin tặc và các phần mềm độc hại xâm nhập vào mạng.
  - Nó cũng giúp ngăn chặn các truy cập trái phép từ bên trong mạng.
- **Ghi nhật ký hoạt động:**
  - Tường lửa ghi lại các hoạt động mạng, giúp quản trị viên theo dõi và phân tích lưu lượng mạng.
  - Điều này giúp phát hiện và ứng phó với các sự cố bảo mật.
- **NAT (Network Address Translation):**
  - Một số tường lửa có tính năng NAT, giúp che giấu địa chỉ IP nội bộ của các thiết bị trong mạng.
  - Điều này giúp tăng cường bảo mật và tiết kiệm địa chỉ IP công cộng.

#### **2. Các loại tường lửa:**

- **Tường lửa phần cứng:**
  - Là các thiết bị chuyên dụng được thiết kế để thực hiện chức năng tường lửa.
  - Thường được sử dụng trong các mạng doanh nghiệp lớn.
- **Tường lửa phần mềm:**
  - Là các phần mềm được cài đặt trên máy tính hoặc máy chủ.



- Thường được sử dụng trong các mạng gia đình và doanh nghiệp nhỏ.
- **Tường lửa thế hệ mới (NGFW):**
  - Là các tường lửa tiên tiến, tích hợp nhiều tính năng bảo mật như IPS (Intrusion Prevention System), lọc URL, kiểm soát ứng dụng.

### 3. Cơ chế hoạt động:

- **Lọc gói tin (Packet filtering):**
  - Kiểm tra các gói dữ liệu dựa trên địa chỉ IP, cổng và giao thức.
- **Kiểm tra trạng thái (Stateful inspection):**
  - Theo dõi trạng thái của các kết nối mạng và chỉ cho phép các gói dữ liệu hợp lệ đi qua.
- **Kiểm tra ứng dụng (Application inspection):**
  - Kiểm tra nội dung của các gói dữ liệu để phát hiện các ứng dụng độc hại.
- **Proxy firewall:**
  - hoạt động như một trung gian giữa các máy tính và máy chủ.
- **Tường lửa Web (WAF):**
  - Tường lửa Web(Web Application Firewall) là một hình thức bảo vệ giao thức HTTP(Hypertext Transfer Protocol) . Nó áp dụng một tập hợp các quy tắc cho các cuộc hội thoại HTTP để bảo vệ khỏi các cuộc tấn công.

### 4. Tầm quan trọng của tường lửa:

- Tường lửa là một thành phần thiết yếu của hệ thống bảo mật mạng.
- Nó giúp bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa từ bên ngoài.
- Việc sử dụng tường lửa giúp đảm bảo an toàn cho thông tin cá nhân và dữ liệu quan trọng.

#### 5.4 IDS (Intrusion Detection System - Hệ thống phát hiện xâm nhập)

IDS (Intrusion Detection System - Hệ thống phát hiện xâm nhập) là một hệ thống giám sát mạng hoặc hệ thống máy tính để phát hiện các hoạt động độc hại hoặc các vi phạm chính sách bảo mật. IDS không ngăn chặn các cuộc tấn công, mà chỉ cảnh báo cho quản trị viên về các hoạt động đáng ngờ.

#### 1. Chức năng chính:

- **Giám sát lưu lượng mạng:**
  - IDS theo dõi lưu lượng mạng để phát hiện các mẫu hoạt động bất thường hoặc đáng ngờ.
- **Phân tích dữ liệu:**
  - IDS phân tích dữ liệu mạng để tìm kiếm các dấu hiệu của các cuộc tấn công hoặc các vi phạm bảo mật.
- **Cảnh báo:**
  - Khi phát hiện hoạt động đáng ngờ, IDS sẽ gửi cảnh báo cho quản trị viên.
- **Ghi nhật ký:**
  - IDS ghi lại các hoạt động mạng để phục vụ cho việc phân tích và điều tra sau này.

## 2. Các loại IDS:

- **NIDS (Network Intrusion Detection System - Hệ thống phát hiện xâm nhập mạng):**
  - Giám sát lưu lượng mạng trên toàn bộ mạng.
- **HIDS (Host Intrusion Detection System - Hệ thống phát hiện xâm nhập máy chủ):**
  - Giám sát hoạt động trên một máy chủ cụ thể.

## 3. Phương pháp phát hiện:

- **Phát hiện dựa trên chữ ký (Signature-based detection):**
  - So sánh lưu lượng mạng với các mẫu tấn công đã biết.
- **Phát hiện dựa trên hành vi bất thường (Anomaly-based detection):**
  - Phát hiện các hoạt động bất thường so với hành vi bình thường của mạng.

## 4. Tầm quan trọng của IDS:

- **Phát hiện sớm các cuộc tấn công:**
  - IDS giúp phát hiện sớm các cuộc tấn công, cho phép quản trị viên phản ứng kịp thời.
- **Cải thiện khả năng bảo mật:**
  - IDS giúp cải thiện khả năng bảo mật của mạng bằng cách phát hiện các lỗ hổng và các hoạt động đáng ngờ.
- **Tuân thủ các quy định:**
  - IDS giúp các tổ chức tuân thủ các quy định về bảo mật dữ liệu.

## 5. So sánh IDS và IPS:

- **IDS (Intrusion Detection System):**
  - Phát hiện các cuộc tấn công.
  - Cảnh báo quản trị viên.
  - Không ngăn chặn các cuộc tấn công.
- **IPS (Intrusion Prevention System):**
  - Phát hiện các cuộc tấn công.
  - Ngăn chặn các cuộc tấn công.

IDS là một công cụ quan trọng trong hệ thống bảo mật mạng, giúp phát hiện sớm các cuộc tấn công và cải thiện khả năng bảo mật của mạng.

### 5.5 IPS (Intrusion Prevention System - Hệ thống ngăn chặn xâm nhập)

IPS (Intrusion Prevention System - Hệ thống ngăn chặn xâm nhập) là một công cụ bảo mật mạng hoạt động bằng cách giám sát lưu lượng mạng để phát hiện và ngăn chặn các cuộc tấn công độc hại. IPS không chỉ phát hiện các mối đe dọa như IDS (Intrusion Detection System - Hệ thống phát hiện xâm nhập), mà còn chủ động ngăn chặn chúng.

## 1. Chức năng chính:

- **Phát hiện và ngăn chặn xâm nhập:**
  - IPS phân tích lưu lượng mạng để tìm kiếm các dấu hiệu của các cuộc tấn công, chẳng hạn như phần mềm độc hại, khai thác lỗ hổng và tấn công từ chối dịch vụ (DoS).
  - Khi phát hiện một cuộc tấn công, IPS sẽ thực hiện các hành động để ngăn chặn nó, chẳng hạn như chặn lưu lượng độc hại, chấm dứt kết nối hoặc gửi cảnh báo cho quản trị viên.
- **Kiểm soát truy cập:**
  - IPS có thể được sử dụng để kiểm soát truy cập vào mạng dựa trên các quy tắc bảo mật.
- **Bảo vệ khỏi các cuộc tấn công zero-day:**
  - IPS có thể sử dụng các kỹ thuật phân tích hành vi để phát hiện các cuộc tấn công zero-day, là các cuộc tấn công khai thác các lỗ hổng chưa được biết đến.

## 2. Các loại IPS:

- **NIPS (Network Intrusion Prevention System - Hệ thống ngăn chặn xâm nhập mạng):**
  - Giám sát lưu lượng mạng trên toàn bộ mạng.
- **HIPS (Host Intrusion Prevention System - Hệ thống ngăn chặn xâm nhập máy chủ):**
  - Giám sát hoạt động trên một máy chủ cụ thể.

## 3. Phương pháp hoạt động:

- **Phát hiện dựa trên chữ ký (Signature-based detection):**
  - So sánh lưu lượng mạng với các mẫu tấn công đã biết.
- **Phát hiện dựa trên hành vi bất thường (Anomaly-based detection):**
  - Phát hiện các hoạt động bất thường so với hành vi bình thường của mạng.
- **Phân tích trạng thái (Stateful analysis):**
  - Phân tích các kết nối mạng để xác định xem chúng có hợp lệ hay không.

## 4. Tầm quan trọng của IPS:

- **Bảo vệ khỏi các cuộc tấn công mạng:**
  - IPS giúp bảo vệ mạng khỏi các cuộc tấn công độc hại, giúp bảo vệ dữ liệu và hệ thống khỏi bị tổn hại.
- **Giảm thiểu rủi ro:**
  - IPS giúp giảm thiểu rủi ro bị tấn công mạng, giúp các tổ chức tuân thủ các quy định về bảo mật dữ liệu.
- **Tự động hóa phản ứng:**
  - IPS tự động hóa phản ứng đối với các cuộc tấn công, giúp giảm thiểu thời gian và công sức cần thiết để xử lý các sự cố bảo mật.

## 5. So sánh IPS và Firewall:

- **Firewall:**
  - Kiểm soát truy cập vào mạng dựa trên các quy tắc.
  - Chặn lưu lượng dựa trên địa chỉ IP, cổng và giao thức.
  - Không phân tích nội dung của lưu lượng mạng.
- **IPS:**
  - Phân tích nội dung của lưu lượng mạng.
  - Phát hiện và ngăn chặn các cuộc tấn công độc hại.
  - Có thể ngăn chặn các cuộc tấn công mà tường lửa không thể.

## 6. Các mối đe dọa an toàn hệ thống mạng

### 6.1 Mã độc (Malware)

Gồm mã độc bên trong và mã độc bên ngoài

#### Malware từ bên ngoài:

- Đây là nguồn gốc phổ biến nhất. Malware có thể xâm nhập vào hệ thống thông qua:
  - Internet: Tải xuống tệp tin độc hại, truy cập các trang web bị nhiễm độc, hoặc nhấp vào các liên kết độc hại.
  - Email: Mở các tệp đính kèm hoặc nhấp vào các liên kết trong email lừa đảo.
  - Thiết bị lưu trữ di động: Sử dụng ổ USB, ổ cứng di động, hoặc thẻ nhớ bị nhiễm độc.
  - Mạng không dây: Kết nối vào các mạng Wi-Fi công cộng không an toàn.
- Các cuộc tấn công này thường được thực hiện bởi tin tặc, tội phạm mạng, hoặc các nhóm tấn công có tổ chức.

#### Malware từ bên trong:

- Mặc dù ít phổ biến hơn, nhưng malware cũng có thể được đưa vào hệ thống từ bên trong tổ chức. Điều này có thể xảy ra do:
  - Nhân viên vô tình: Nhân viên có thể vô tình tải xuống hoặc cài đặt malware mà không biết.
  - Nhân viên cố ý: Nhân viên có thể cố ý đưa malware vào hệ thống để gây hại, đánh cắp dữ liệu, hoặc phá hoại hệ thống.
  - Nhân viên bị lừa đảo: Nhân viên có thể bị lừa đảo để cài đặt malware hoặc cung cấp thông tin đăng nhập cho kẻ tấn công.
- Các cuộc tấn công nội bộ thường khó phát hiện hơn vì kẻ tấn công có thể có quyền truy cập hợp pháp vào hệ thống.

"Malware" là một thuật ngữ chung chỉ các phần mềm độc hại được thiết kế để gây hại cho hệ thống máy tính, mạng hoặc thiết bị. Mục tiêu của malware rất đa dạng, bao gồm:

- **Phá hoại:** Xóa, sửa đổi hoặc làm hỏng dữ liệu, chương trình hoặc hệ điều hành.

- **Đánh cắp:** Thu thập thông tin nhạy cảm như mật khẩu, số thẻ tín dụng hoặc dữ liệu cá nhân.
- **Kiểm soát:** Chiếm quyền kiểm soát máy tính hoặc thiết bị để sử dụng cho các mục đích xấu như tấn công mạng hoặc gửi thư rác.
- **Tống tiền:** Mã hóa dữ liệu và yêu cầu tiền chuộc để khôi phục.
- **Gián điệp:** Theo dõi hoạt động của người dùng mà họ không hề hay biết.

Một số loại malware phổ biến:

- **Virus:** Lây lan bằng cách gắn vào các tệp hoặc chương trình khác.
- **Worm (Sâu máy tính):** Tự sao chép và lây lan qua mạng.
- **Trojan:** Giả mạo phần mềm hợp pháp để lừa người dùng cài đặt.
- **Ransomware:** Mã hóa dữ liệu và yêu cầu tiền chuộc.
- **Spyware:** Theo dõi hoạt động của người dùng và thu thập thông tin.
- **Adware:** Hiện thị quảng cáo không mong muốn.

## 6.2 Tấn công mạng (Cyber Attacks)

- Các mối đe dọa phổ biến nhất, bao gồm các hình thức như:
  - **Mã độc tống tiền (Ransomware):** Mã hóa dữ liệu và yêu cầu tiền chuộc.
  - **Tấn công từ chối dịch vụ (DoS/DDoS):** Làm tê liệt hệ thống bằng cách quá tải lưu lượng truy cập.
  - **Tấn công SQL Injection:** Lợi dụng lỗ hổng trong ứng dụng web để truy cập trái phép cơ sở dữ liệu.
  - **Lừa đảo (Phishing):** Giả mạo email, trang web,... để đánh cắp thông tin đăng nhập.
  - **Tấn công APT (Advanced Persistent Threat):** Tấn công có chủ đích, tinh vi, kéo dài để xâm nhập và đánh cắp dữ liệu quan trọng.

## 6.3 Truy cập trái phép (Unauthorized Access):

Kẻ tấn công tìm cách xâm nhập vào hệ thống mà không được phép, có thể thông qua lỗ hổng bảo mật hoặc đánh cắp thông tin đăng nhập.

## 6.4 Tấn công nội bộ (Insider Threats):

- Nhân viên, cựu nhân viên hoặc đối tác có quyền truy cập hệ thống có thể gây hại do:
  - Vô tình: Do thiếu hiểu biết hoặc bất cẩn.
  - Cố ý: Vì động cơ cá nhân hoặc lợi ích riêng.

## 6.5 Lỗ hổng phần mềm (Software Vulnerabilities):

Các lỗ hổng trong phần mềm, hệ điều hành,... có thể bị khai thác để tấn công.

## 6.6 Mất dữ liệu (Data Loss):

Do lỗi phần cứng, phần mềm, thiên tai hoặc hành động của con người.

## 6.7 Cấu hình sai:

Các sai sót trong quá trình cấu hình hệ thống bảo mật có thể dẫn đến việc tạo ra các điểm yếu, tạo điều kiện cho các cuộc tấn công mạng.

## 6.8 Tấn công chuỗi cung ứng:

- Khi các nhà cung cấp bên thứ ba bị tấn công, hệ thống của doanh nghiệp cũng có thể bị ảnh hưởng.

## 6.9 Các cuộc tấn công dựa trên AI:

- Hacker sử dụng các công cụ AI để tăng cường độ tinh vi và hiệu quả của các cuộc tấn công.



Hình 3. Tấn công mạng

## CHƯƠNG III. XÂY DỰNG VÀ TRIỂN KHAI GIẢI PHÁP BẢO MẬT

### 1. Yêu cầu doanh nghiệp

#### 1.1 Yêu cầu kỹ thuật

Đây là một kỹ thuật quan trọng mà các doanh nghiệp rất cần thiết. Vì thế, công ty DVV cần một hệ thống bảo mật có thể đáp ứng được các yêu cầu sau:

- ☐ **Đảm bảo chất lượng:** Yêu cầu kỹ thuật giúp doanh nghiệp kiểm soát và duy trì chất lượng sản phẩm, dịch vụ, từ đó nâng cao sự hài lòng của khách hàng.
- ☐ **Tăng hiệu suất:** Các tiêu chuẩn kỹ thuật giúp tối ưu hóa quy trình làm việc, giảm thiểu sai sót và tăng năng suất.
- ☐ **Đảm bảo an toàn:** Đặc biệt trong các ngành công nghiệp có rủi ro cao, yêu cầu kỹ thuật đảm bảo an toàn cho nhân viên, khách hàng và môi trường.
- ☐ **Tuân thủ pháp luật:** Yêu cầu kỹ thuật giúp doanh nghiệp tuân thủ các quy định và tiêu chuẩn của pháp luật, tránh các rủi ro pháp lý.
- ☐ **Nâng cao tính cạnh tranh:** Các doanh nghiệp có tiêu chuẩn kỹ thuật cao thường có lợi thế cạnh tranh trên thị trường.

Ngoài ra phải đáp ứng được các nghiệp vụ như:

- Kiểm tra được các truy cập mạng
- Giám sát phát hiện sự cố để giải quyết kịp thời
- Bảo mật web
- Quản lý danh tính, thông tin cá nhân và truy cập
- Sao lưu và khôi phục

#### 1.2 Yêu cầu nghiệp vụ kinh doanh

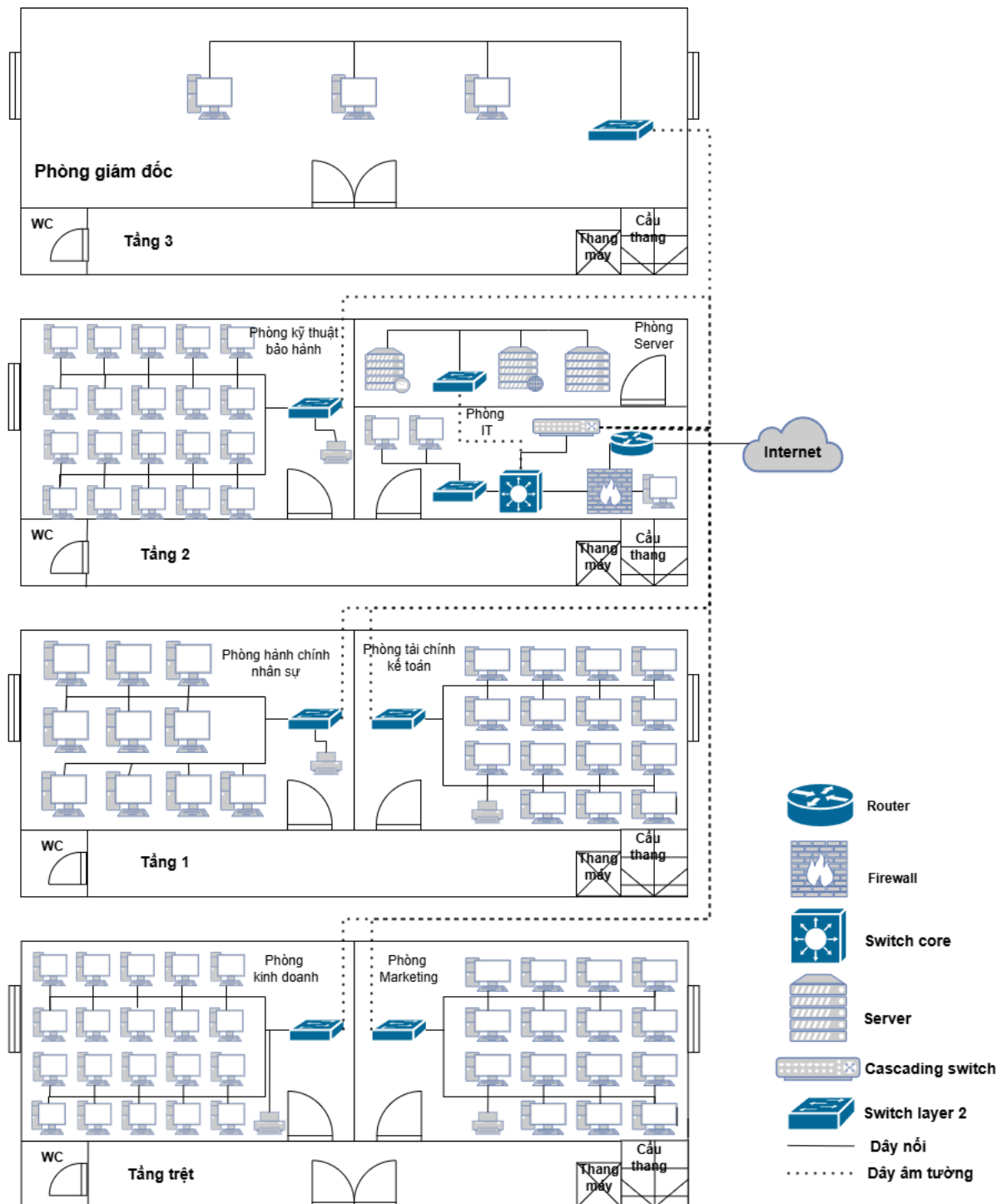
Để đáp ứng các yêu cầu cần có những đặc điểm sau:

- Đảm bảo thời gian hoạt động được liên tục
- Tránh rò rỉ thông tin khách hàng và các dữ liệu như thông tin mã đơn, các giao dịch thanh toán
- Có khả năng truy cập từ xa có thể làm việc tại nhà tạo điều kiện cho nhân viên làm việc
- Tuân thủ các quy định về an toàn thông tin theo các quy định pháp luật



## 2. Xây dựng giải pháp

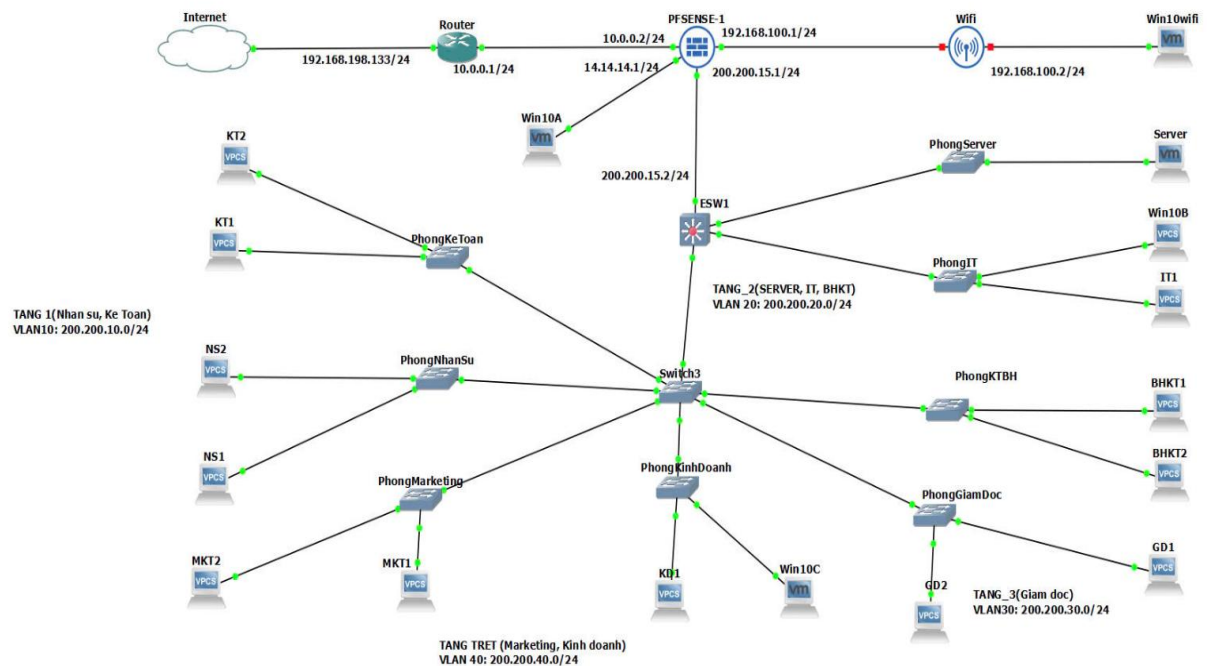
### 2.1. Sơ đồ vật lý:



Hình 4. Sơ đồ vật lý



## 2.2. Sơ đồ logic:



### Hình 5. Sơ đồ logic

### 3. Chính sách bảo mật vật lý:

Chính sách bảo mật vật lý của doanh nghiệp là một tập hợp các biện pháp và quy trình được thiết kế để bảo vệ tài sản vật lý của doanh nghiệp, bao gồm phần cứng, thiết bị, dữ liệu và cơ sở hạ tầng, khỏi các mối đe dọa vật lý.

### Tầm quan trọng của chính sách bảo mật vật lý:

- **Bảo vệ tài sản quan trọng:** Đảm bảo an toàn cho máy chủ, trung tâm dữ liệu, thiết bị mạng và các tài sản vật lý khác.
- **Ngăn chặn truy cập trái phép:** Hạn chế quyền truy cập vật lý vào các khu vực nhạy cảm, giảm thiểu nguy cơ bị đánh cắp hoặc phá hoại.
- **Bảo vệ dữ liệu:** Ngăn chặn việc truy cập trái phép vào dữ liệu lưu trữ trên các thiết bị vật lý.
- **Đảm bảo tính liên tục của hoạt động:** Giảm thiểu nguy cơ gián đoạn hoạt động do các sự cố vật lý như mất điện, hỏa hoạn hoặc thiên tai.
- **Tuân thủ pháp luật:** Đáp ứng các yêu cầu về bảo mật vật lý theo quy định của pháp luật.

### Các thành phần chính của chính sách bảo mật vật lý:

- **Kiểm soát truy cập vật lý:**
  - Hệ thống khóa cửa, thẻ từ, sinh trắc học.
  - Giám sát bằng camera quan sát (CCTV).
  - Bảo vệ khu vực trung tâm dữ liệu và phòng máy chủ.
  - Quy trình đăng ký và kiểm soát khách ra vào.
- **Bảo vệ môi trường:**

- Hệ thống báo cháy và chữa cháy.
- Hệ thống kiểm soát nhiệt độ và độ ẩm.
- Hệ thống chống sét.
- Hệ thống nguồn điện dự phòng (UPS).
- **Bảo vệ thiết bị:**
  - Khóa vật lý cho thiết bị.
  - Bảo vệ cáp và dây nối.
  - Định vị và theo dõi thiết bị di động.
- **Quản lý dữ liệu vật lý:**
  - Bảo vệ dữ liệu lưu trữ trên các thiết bị vật lý.
  - Quy trình tiêu hủy dữ liệu an toàn.
  - Sao lưu và phục hồi dữ liệu.
- **Đào tạo và nhận thức:**
  - Đào tạo nhân viên về các biện pháp bảo mật vật lý.
  - Nâng cao nhận thức về các mối đe dọa vật lý.
  - Quy trình báo cáo sự cố.

### Các bước triển khai chính sách bảo mật vật lý:

- **Đánh giá rủi ro:** Xác định các mối đe dọa vật lý tiềm ẩn và mức độ rủi ro.
- **Xây dựng chính sách:** Phát triển các chính sách và quy trình bảo mật vật lý phù hợp với nhu cầu của doanh nghiệp.
- **Triển khai biện pháp:** Áp dụng các biện pháp bảo mật vật lý cần thiết.
- **Giám sát và đánh giá:** Thường xuyên giám sát và đánh giá hiệu quả của các biện pháp bảo mật vật lý.
- **Cập nhật và cải tiến:** Cập nhật và cải tiến chính sách bảo mật vật lý theo thời gian để đáp ứng các thay đổi của môi trường và công nghệ.

Chính sách bảo mật vật lý là một phần không thể thiếu trong chiến lược bảo mật tổng thể của doanh nghiệp. Việc triển khai các biện pháp bảo mật vật lý hiệu quả sẽ giúp doanh nghiệp bảo vệ tài sản quan trọng và đảm bảo tính liên tục của hoạt động.

### 4. Chính sách bảo mật Hệ điều hành:

Chính sách bảo mật hệ điều hành là một tập hợp các quy tắc, biện pháp và công nghệ được thiết kế để bảo vệ hệ điều hành và dữ liệu của người dùng khỏi các mối đe dọa bảo mật. Chính sách này bao gồm nhiều khía cạnh khác nhau, từ việc quản lý quyền truy cập đến việc cập nhật phần mềm và vá lỗi bảo mật.

#### Tầm quan trọng của chính sách bảo mật hệ điều hành:

- **Bảo vệ dữ liệu:** Ngăn chặn truy cập trái phép vào dữ liệu nhạy cảm, bao gồm thông tin cá nhân, tài chính và doanh nghiệp.
- **Đảm bảo tính toàn vẹn của hệ thống:** Ngăn chặn phần mềm độc hại, virus và các mối đe dọa khác làm hỏng hoặc phá hủy hệ điều hành.
- **Duy trì tính khả dụng của hệ thống:** Đảm bảo rằng hệ điều hành luôn hoạt động ổn định và có thể truy cập được khi cần thiết.
- **Tuân thủ các quy định:** Đáp ứng các yêu cầu về bảo mật dữ liệu của các cơ quan quản lý và tiêu chuẩn ngành.

- **Nâng cao lòng tin của người dùng:** Chứng minh rằng doanh nghiệp coi trọng bảo mật dữ liệu và bảo vệ thông tin của người dùng.

#### **Các thành phần chính của chính sách bảo mật hệ điều hành:**

- **Quản lý quyền truy cập:**
  - Kiểm soát quyền truy cập của người dùng và ứng dụng vào hệ thống.
  - Sử dụng mật khẩu mạnh và xác thực đa yếu tố.
  - Phân quyền người dùng theo nguyên tắc đặc quyền tối thiểu.
- **Cập nhật phần mềm và vá lỗi:**
  - Cài đặt các bản cập nhật và vá lỗi bảo mật kịp thời.
  - Tự động cập nhật phần mềm khi có sẵn.
  - Theo dõi các cảnh báo bảo mật và lỗ hổng.
- **Phần mềm chống virus và phần mềm độc hại:**
  - Cài đặt và cập nhật phần mềm chống virus và phần mềm độc hại.
  - Quét hệ thống thường xuyên để phát hiện và loại bỏ các mối đe dọa.
  - Sử dụng tường lửa để ngăn chặn truy cập trái phép.
- **Mã hóa dữ liệu:**
  - Mã hóa dữ liệu nhạy cảm để bảo vệ khỏi truy cập trái phép.
  - Sử dụng mã hóa ổ đĩa để bảo vệ dữ liệu khi thiết bị bị mất hoặc bị đánh cắp.
  - Mã hóa dữ liệu truyền qua mạng.
- **Giám sát và ghi nhật ký:**
  - Giám sát hoạt động của hệ thống để phát hiện các hành vi bất thường.
  - Ghi nhật ký các sự kiện bảo mật để điều tra các sự cố.
  - Sử dụng phần mềm phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS).
- **Sao lưu và phục hồi:**
  - Sao lưu dữ liệu thường xuyên để phục hồi khi cần thiết.
  - Kiểm tra định kỳ các bản sao lưu để đảm bảo tính toàn vẹn.
  - Lập kế hoạch phục hồi sau thảm họa.

#### **Các bước triển khai chính sách bảo mật hệ điều hành:**

- **Đánh giá rủi ro:** Xác định các mối đe dọa bảo mật tiềm ẩn và mức độ rủi ro.
- **Xây dựng chính sách:** Phát triển các chính sách và quy trình bảo mật phù hợp với nhu cầu của doanh nghiệp.
- **Triển khai biện pháp:** Áp dụng các biện pháp bảo mật cần thiết.
- **Giám sát và đánh giá:** Thường xuyên giám sát và đánh giá hiệu quả của các biện pháp bảo mật.
- **Cập nhật và cải tiến:** Cập nhật và cải tiến chính sách bảo mật theo thời gian để đáp ứng các thay đổi của môi trường và công nghệ.

Chính sách bảo mật hệ điều hành là một phần quan trọng của chiến lược bảo mật tổng thể của doanh nghiệp. Việc triển khai các biện pháp bảo mật hiệu quả sẽ giúp doanh nghiệp bảo vệ dữ liệu quan trọng và đảm bảo tính liên tục của hoạt động.

## 5. Chính sách bảo mật mạng:

Chính sách bảo mật mạng là một tập hợp các quy tắc, hướng dẫn và công nghệ được thiết kế để bảo vệ mạng máy tính của một tổ chức và dữ liệu được truyền tải qua mạng đó. Chính sách này nhằm mục đích ngăn chặn truy cập trái phép, sử dụng sai mục đích, sửa đổi, phá hủy hoặc tiết lộ thông tin nhạy cảm.

### Tầm quan trọng của chính sách bảo mật mạng:

- **Bảo vệ dữ liệu:** Ngăn chặn việc đánh cắp hoặc rò rỉ dữ liệu nhạy cảm, bao gồm thông tin khách hàng, tài chính và bí mật kinh doanh.
- **Đảm bảo tính liên tục của hoạt động:** Giảm thiểu nguy cơ gián đoạn hoạt động do các cuộc tấn công mạng.
- **Tuân thủ các quy định:** Đáp ứng các yêu cầu về bảo mật dữ liệu của các cơ quan quản lý và tiêu chuẩn ngành.
- **Xây dựng lòng tin:** Chứng minh rằng tổ chức coi trọng bảo mật dữ liệu và bảo vệ thông tin của khách hàng và đối tác.
- **Giảm thiểu rủi ro tài chính và pháp lý:** Tránh các khoản phạt, chi phí pháp lý và thiệt hại danh tiếng do vi phạm bảo mật.

### Các thành phần chính của chính sách bảo mật mạng:

- **Kiểm soát truy cập:**
  - Xác thực người dùng và thiết bị trước khi cấp quyền truy cập vào mạng.
  - Phân quyền truy cập theo nguyên tắc đặc quyền tối thiểu.
  - Sử dụng mật khẩu mạnh và xác thực đa yếu tố.
- **Tường lửa và hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS):**
  - Tường lửa kiểm soát lưu lượng mạng ra vào dựa trên các quy tắc được xác định trước.
  - IDS/IPS giám sát lưu lượng mạng để phát hiện và ngăn chặn các hành vi xâm nhập.
- **Mã hóa dữ liệu:**
  - Mã hóa dữ liệu truyền tải qua mạng để bảo vệ khỏi việc bị nghe lén.
  - Sử dụng các giao thức mã hóa như HTTPS và VPN.
- **Quản lý lỗ hổng:**
  - Thường xuyên quét và vá các lỗ hổng bảo mật trong phần mềm và hệ thống.
  - Cập nhật phần mềm và hệ điều hành thường xuyên.
- **Giám sát và ghi nhật ký:**
  - Giám sát hoạt động mạng để phát hiện các hành vi bất thường.
  - Ghi nhật ký các sự kiện bảo mật để điều tra các sự cố.
- **Sao lưu và phục hồi:**

- Sao lưu dữ liệu thường xuyên để phục hồi khi cần thiết.
- Lập kế hoạch phục hồi sau thảm họa.
- **Đào tạo và nhận thức:**
  - Đào tạo nhân viên về các biện pháp bảo mật mạng.
  - Nâng cao nhận thức về các mối đe dọa mạng và các hành vi an toàn.

#### Các bước triển khai chính sách bảo mật mạng:

- **Đánh giá rủi ro:** Xác định các mối đe dọa mạng tiềm ẩn và mức độ rủi ro.
- **Xây dựng chính sách:** Phát triển các chính sách và quy trình bảo mật phù hợp với nhu cầu của tổ chức.
- **Triển khai biện pháp:** Áp dụng các biện pháp bảo mật cần thiết.
- **Giám sát và đánh giá:** Thường xuyên giám sát và đánh giá hiệu quả của các biện pháp bảo mật.
- **Cập nhật và cải tiến:** Cập nhật và cải tiến chính sách bảo mật theo thời gian để đáp ứng các thay đổi của môi trường và công nghệ.

Chính sách bảo mật mạng là một yếu tố quan trọng trong việc bảo vệ tài sản và thông tin của tổ chức. Việc triển khai một chính sách bảo mật mạng toàn diện và hiệu quả sẽ giúp tổ chức giảm thiểu rủi ro và đảm bảo tính liên tục của hoạt động.

## 6. Bảng ước tính chi phí

STT	Thiết bị	Đơn giá	Số lượng	Chi phí
1	Máy tính để bàn	15.000.000đ	85	1.275.000.000đ
2	Router Wifi	10.000.000đ	2	20.000.000đ
3	Firewall	30.000.000đ	1	30.000.000đ
4	Router	1.000.000đ	1	1.000.000đ
5	Máy in, photo, scan 3 trong 1	3.000.000đ	6	18.000.000đ
6	Switch lớp 2	2.900.000đ	8	23.200.000đ
7	Switch lớp 3	18.000.000đ	1	18.000.000đ
Tổng chi phí ( chưa tính chi phí các khoản phát sinh khác)				1.385.200.000đ

## 7. Các thảm họa và Kế hoạch phục hồi sau thảm họa

### 7.1 Hư hệ điều hành và Kế hoạch phục hồi

Hệ điều hành (OS) là nền tảng giúp máy tính hoạt động. Nếu nó hỏng, có thể gây ra:

- Máy tính không thể khởi động, dữ liệu bị mắc kẹt.
- Các ứng dụng quan trọng không hoạt động, gián đoạn công việc.
- Có thể mất dữ liệu nếu phải cài lại hệ điều hành mà không có backup.
- Mất thời gian và chi phí để khắc phục hoặc cài lại từ đầu.

**Ví dụ:** Windows bị lỗi màn hình xanh (BSOD), macOS bị lỗi kernel panic, Linux không boot được do lỗi GRUB.

### Cách Khắc phục

**Triệu chứng:** Máy tính không khởi động được, bị lỗi màn hình xanh (BSOD), kernel panic, hoặc ứng dụng không hoạt động.

Cách khắc phục:

#### Khởi động vào chế độ an toàn (Safe Mode):

- Windows: Nhấn **F8** hoặc **Shift + F8** khi bật máy → Chọn "Safe Mode".
- macOS: Nhấn giữ **Shift** khi khởi động.

#### Sử dụng công cụ sửa lỗi hệ điều hành:

- Windows: Chạy **Startup Repair** từ USB boot hoặc **SFC /scannow** trong Command Prompt.
- macOS: Mở **Disk Utility** (Command + R) và chạy **First Aid**.

#### Khôi phục từ điểm sao lưu (System Restore):

- Nếu có bản sao lưu, sử dụng **System Restore** (Windows) hoặc **Time Machine** (macOS).

#### Cài đặt lại hệ điều hành:

- Nếu không thể sửa lỗi, cài lại Windows/macOS bằng USB boot.
- **Lưu ý:** Nếu chưa sao lưu, dùng USB boot Linux để cứu dữ liệu trước khi cài lại.

## 7.2 Hư phần cứng và Kế hoạch phục hồi

Hỏng phần cứng có thể gây thiệt hại lớn hơn vì nó ảnh hưởng đến cả dữ liệu và khả năng vận hành của thiết bị:

- Hỏng ổ cứng: Mất dữ liệu hoàn toàn nếu không có backup.
- Hỏng RAM, CPU, bo mạch chủ: Máy không thể khởi động, phải thay linh kiện.
- Hỏng nguồn: Máy tính mất điện đột ngột, có thể gây hư hại thêm linh kiện khác.

**Ví dụ:** Ổ cứng HDD bị bad sector làm mất dữ liệu quan trọng, quạt tản nhiệt hỏng khiến CPU quá nhiệt và chết.

**Triệu chứng:** Máy không bật được, hay bị treo, xuất hiện lỗi lạ.

## Cách khắc phục

### Kiểm tra nguồn điện:

- Đổi ổ cắm điện, thử bộ nguồn khác.

### Thay thế phần cứng bị lỗi:

- **Hư ổ cứng:** Nếu HDD/SSD hỏng, thay mới và dùng phần mềm khôi phục dữ liệu (Recuva, EaseUS).
- **Hư RAM:** Thử tháo RAM ra và gắn lại, nếu vẫn lỗi thì thay RAM mới.
- **Hư bo mạch chủ:** Đưa đến kỹ thuật viên để kiểm tra chi tiết.

### Làm mát thiết bị:

- Kiểm tra quạt, bôi keo tản nhiệt CPU nếu máy quá nóng.

### Dùng thiết bị cứu dữ liệu:

- Nếu ổ cứng lỗi nhưng chưa chết hẳn, dùng **USB cứu hộ** (Hiren's Boot, MiniTool) để sao chép dữ liệu trước khi thay ổ mới.

## 7.3 Bị virus mã độc và Kế hoạch phục hồi

Virus và phần mềm độc hại (malware) có thể gây ra:

- Mất dữ liệu hoặc bị mã hóa (ransomware).
- Rò rỉ thông tin cá nhân, tài khoản ngân hàng, thông tin doanh nghiệp.
- Máy chạy chậm, bị lợi dụng để đào tiền ảo hoặc tấn công mạng.
- Tốn thời gian và tiền bạc để khôi phục hệ thống.

**Ví dụ:** WannaCry mã hóa dữ liệu, yêu cầu tiền chuộc để giải mã; trojan đánh cắp thông tin đăng nhập ngân hàng

**Triệu chứng:** Máy chậm, xuất hiện pop-up lạ, dữ liệu bị mã hóa.

## Cách khắc phục:

### Quét virus bằng phần mềm chuyên dụng:

- Dùng Windows Defender, Malwarebytes, Kaspersky, hoặc Bitdefender để quét toàn bộ hệ thống.

### Khởi động vào Safe Mode để diệt virus:

- Vào **Safe Mode** (F8 hoặc Shift + F8), chạy trình diệt virus để xóa malware.



### Gỡ bỏ phần mềm lạ:

- Kiểm tra **Task Manager** (Windows) hoặc **Activity Monitor** (macOS) để tắt tiến trình đáng ngờ.
- Xóa các ứng dụng không rõ nguồn gốc trong **Control Panel** hoặc **Finder**.

### Khôi phục dữ liệu bị mã hóa bởi ransomware:

- Nếu dữ liệu bị mã hóa, thử công cụ **No More Ransom** ([nomoreransom.org](https://nomoreransom.org)).
- Nếu không có giải pháp giải mã, cần **khôi phục từ bản sao lưu** hoặc chấp nhận mất dữ liệu.

### Cài lại hệ điều hành nếu cần thiết:

- Nếu virus lây lan quá rộng, cài lại OS để đảm bảo sạch 100%.

## 7.4 Server bị hack và Kế hoạch phục hồi

Khi một server bị tấn công, hậu quả có thể nghiêm trọng:

- Rò rỉ dữ liệu khách hàng, gây mất uy tín.
- Website bị tấn công DDoS, làm gián đoạn dịch vụ.
- Hacker chiếm quyền điều khiển, sử dụng server để phát tán mã độc.
- Doanh nghiệp có thể bị phạt nếu vi phạm quy định về bảo mật dữ liệu (GDPR, PCI DSS).

**Ví dụ:** Vụ hack Yahoo năm 2013 khiến 3 tỷ tài khoản bị lộ; website doanh nghiệp bị deface (thay đổi giao diện bởi hacker).

**Triệu chứng:** Website bị deface, mất dữ liệu, server bị khóa, thông tin bị rò rỉ.

Cách khắc phục:

### Ngắt kết nối ngay lập tức:

- Tắt server, ngắt mạng để tránh hacker truy cập tiếp.

### Kiểm tra log để xác định lỗ hổng:

- Dùng lệnh cat /var/log/auth.log (Linux) hoặc xem **Event Viewer** (Windows) để tìm dấu hiệu tấn công.

### Khôi phục từ bản sao lưu:

- Nếu có backup, khôi phục hệ thống từ bản sao lưu sạch trước khi bị hack.

### Đổi mật khẩu & khóa lỗ hổng:



- Thay toàn bộ mật khẩu admin, database, SSH key.
- Kiểm tra và cập nhật phần mềm, cài firewall, kích hoạt xác thực 2 lớp (2FA).

**Quét malware trên server:**

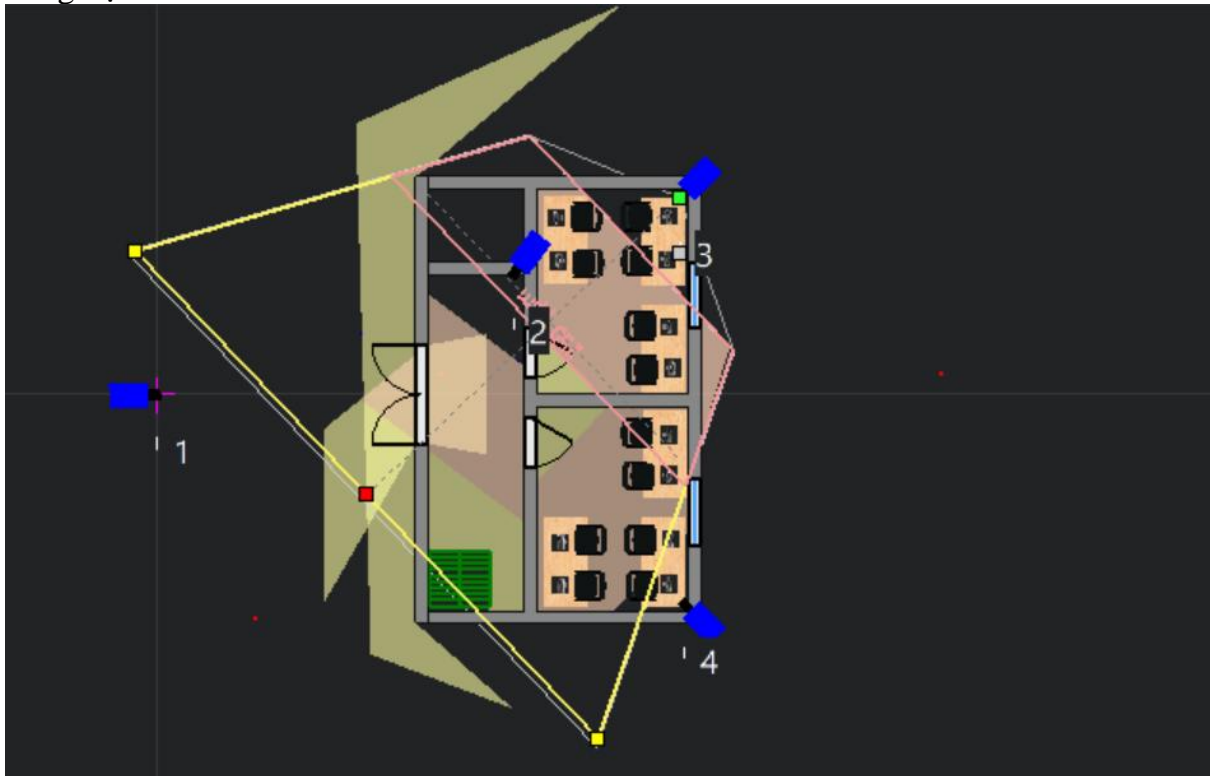
- Dùng ClamAV, Maldet (Linux) hoặc Windows Defender để kiểm tra mã độc.

**Báo cáo & tăng cường bảo mật:**

- Nếu dữ liệu người dùng bị lộ, cần thông báo và tuân theo quy định bảo mật dữ liệu.
- Cài đặt hệ thống giám sát (IDS/IPS) để phát hiện xâm nhập trong tương lai.

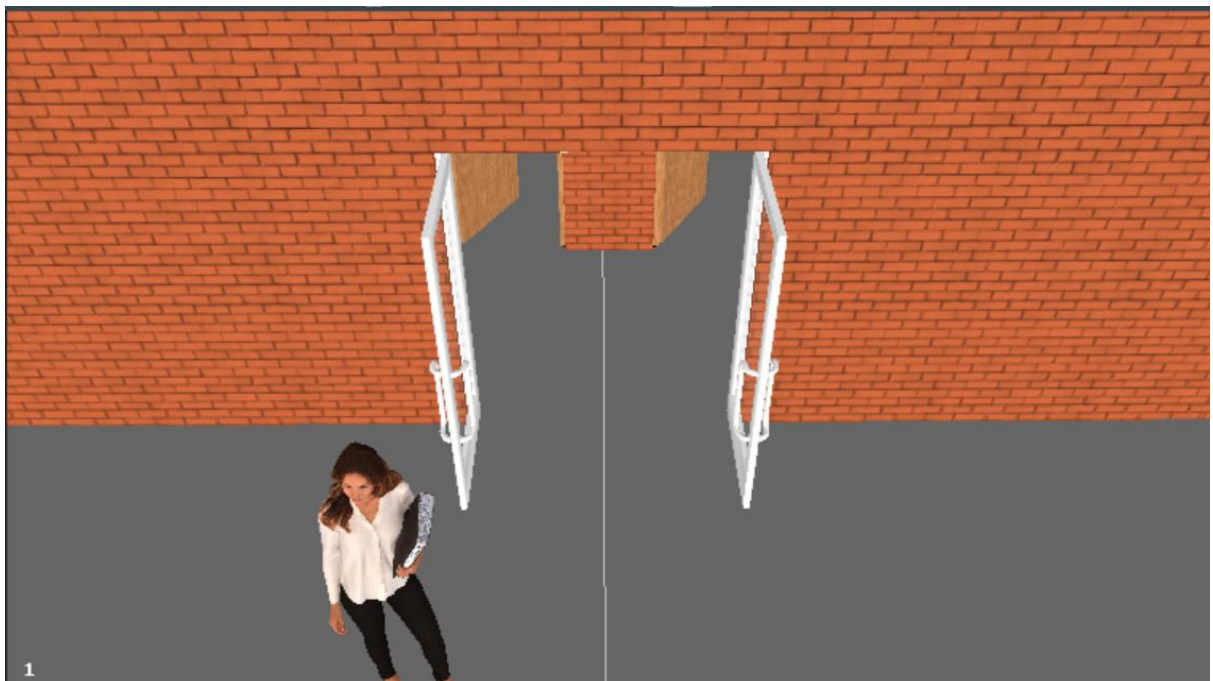
## 8. Triển khai

### Tầng trệt



Hình 6. Tầng trệt

### - Sảnh



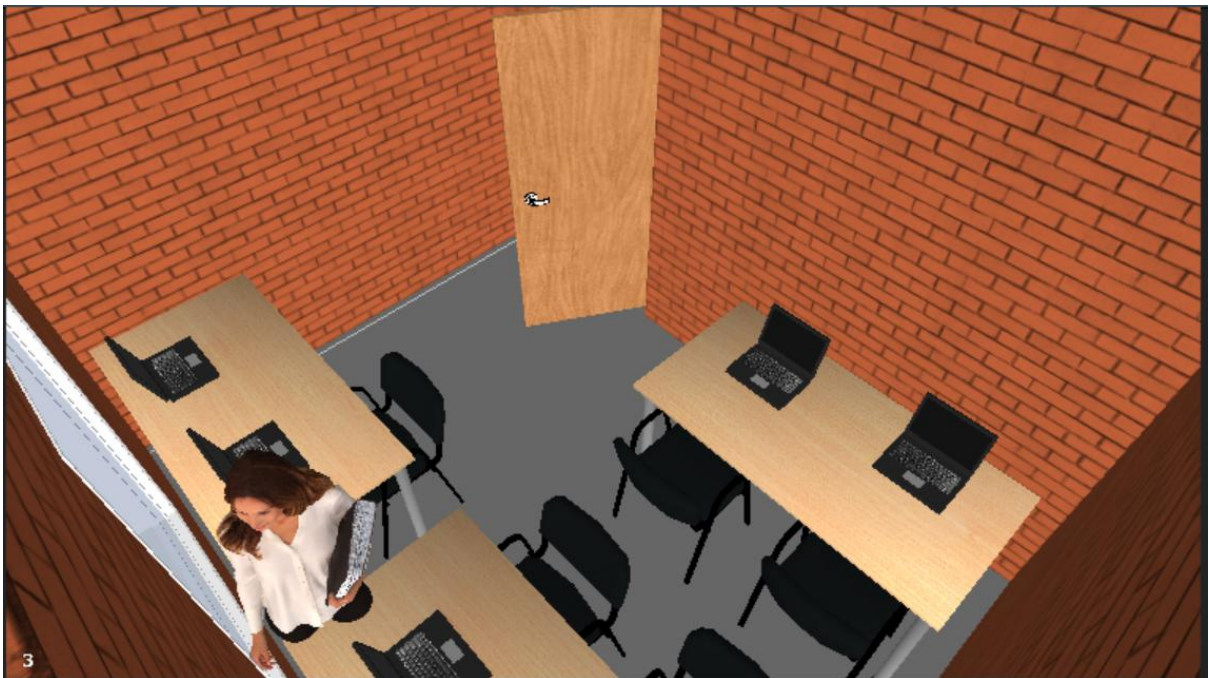
Hình 7. Cửa ở sảnh

- Phòng kinh doanh



Hình 8. Phòng kinh doanh

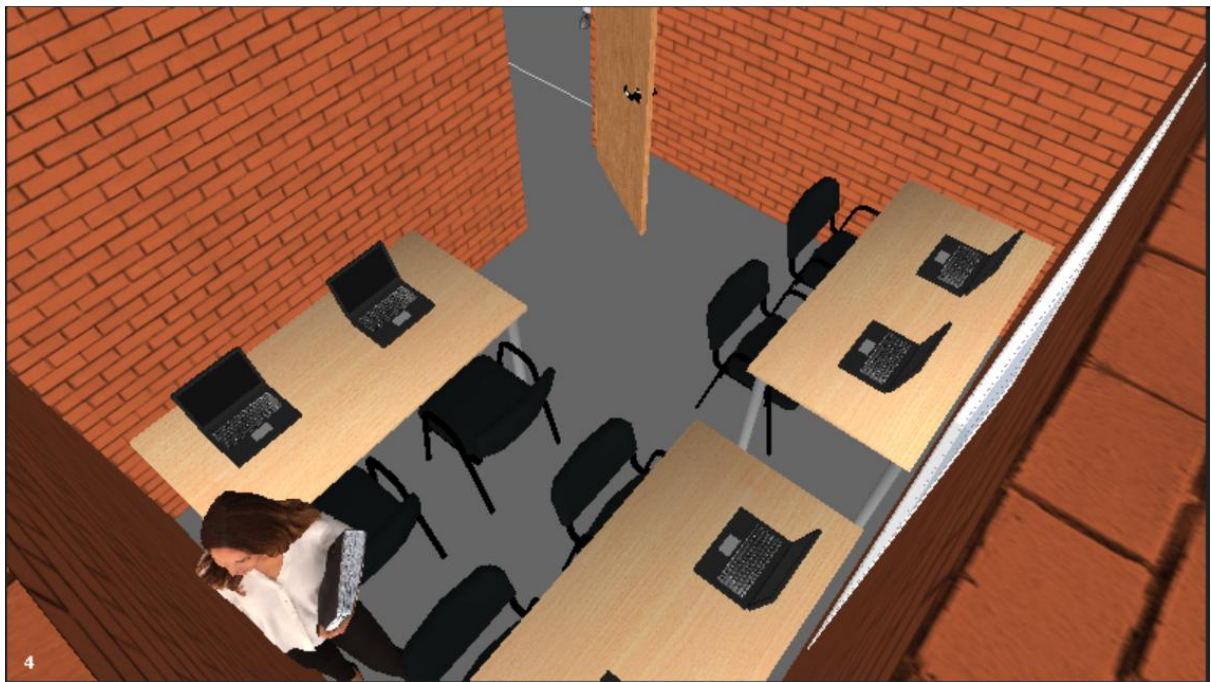
- Phòng Marketing



Hình 9. Phòng Marketing

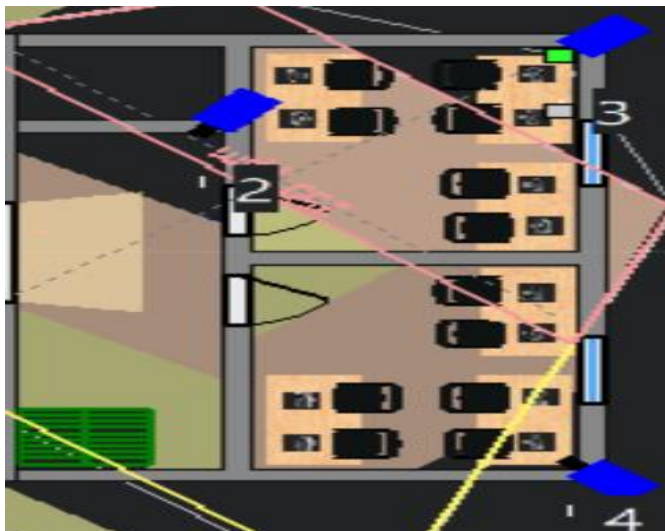


Tầng 1



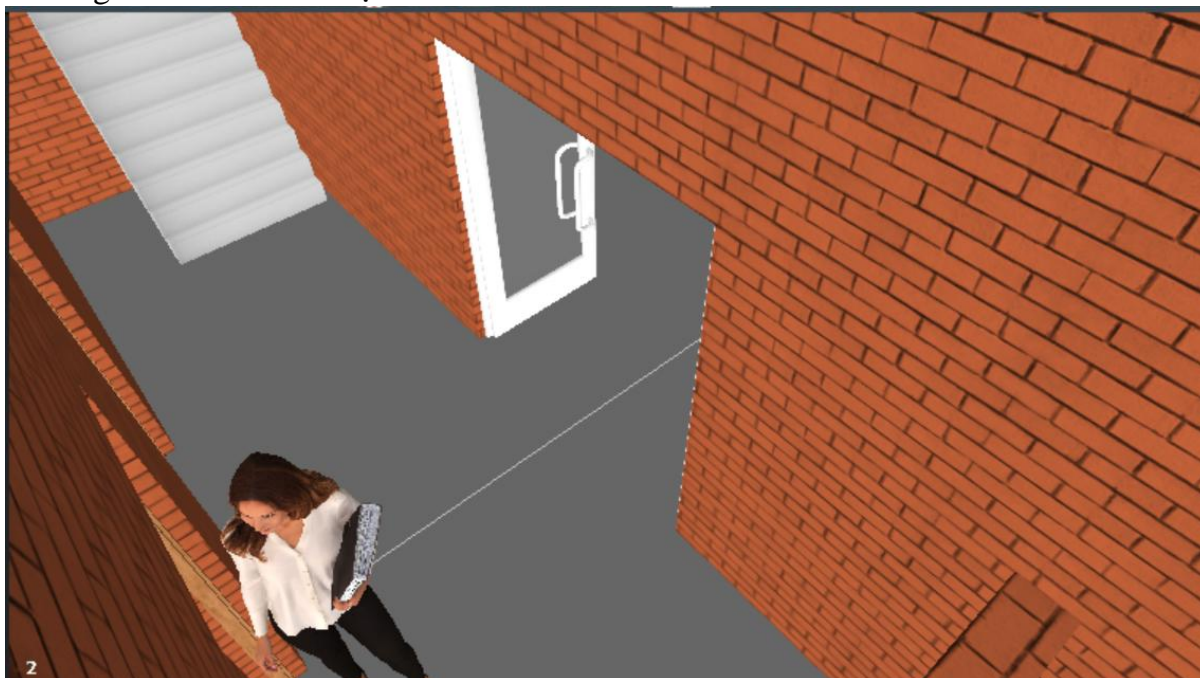
Hình 10. Phòng làm việc Tầng 1

- Sân



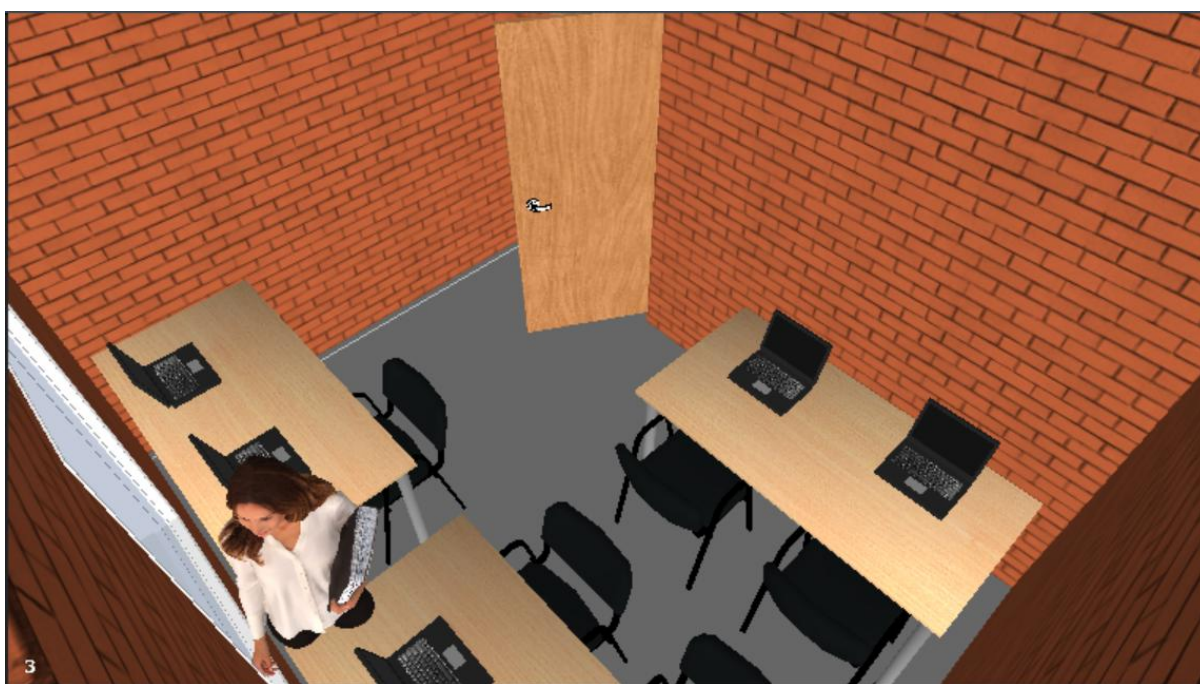
Hình 11. Sân

- Phòng hành chính nhân sự



Hình 12. Phòng hành chính nhân sự

- Phòng kế toán



Hình 13. Phòng kế toán



Tầng 2

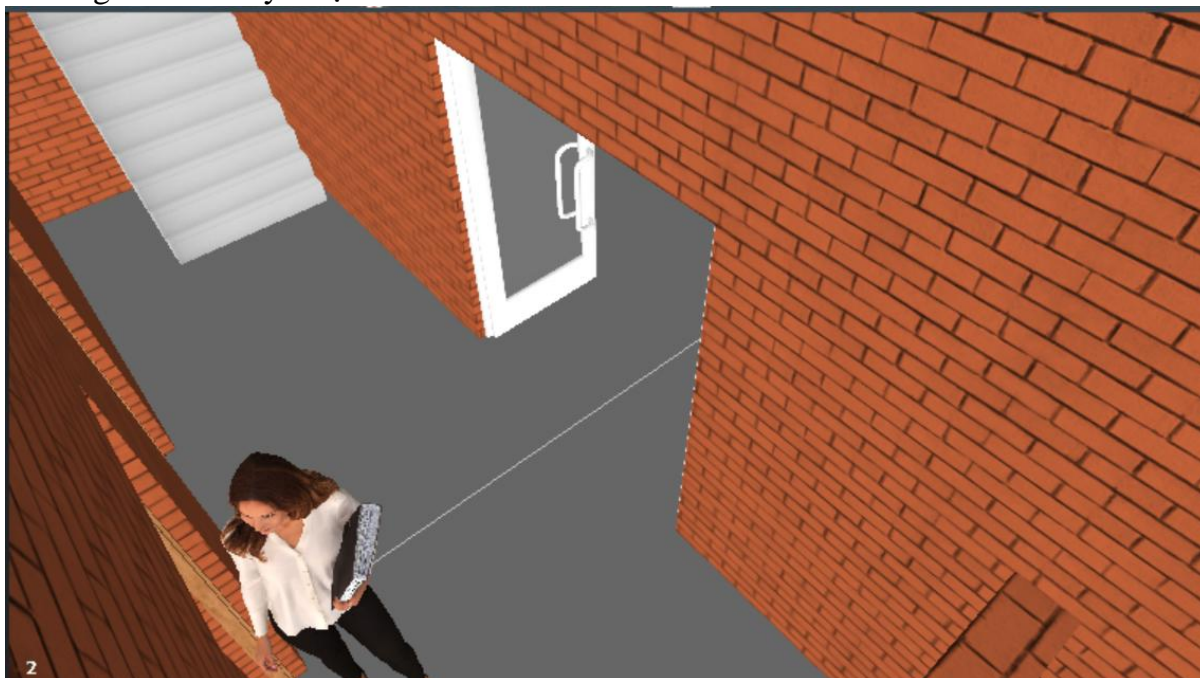


Hình 14. Phòng làm việc tầng 2



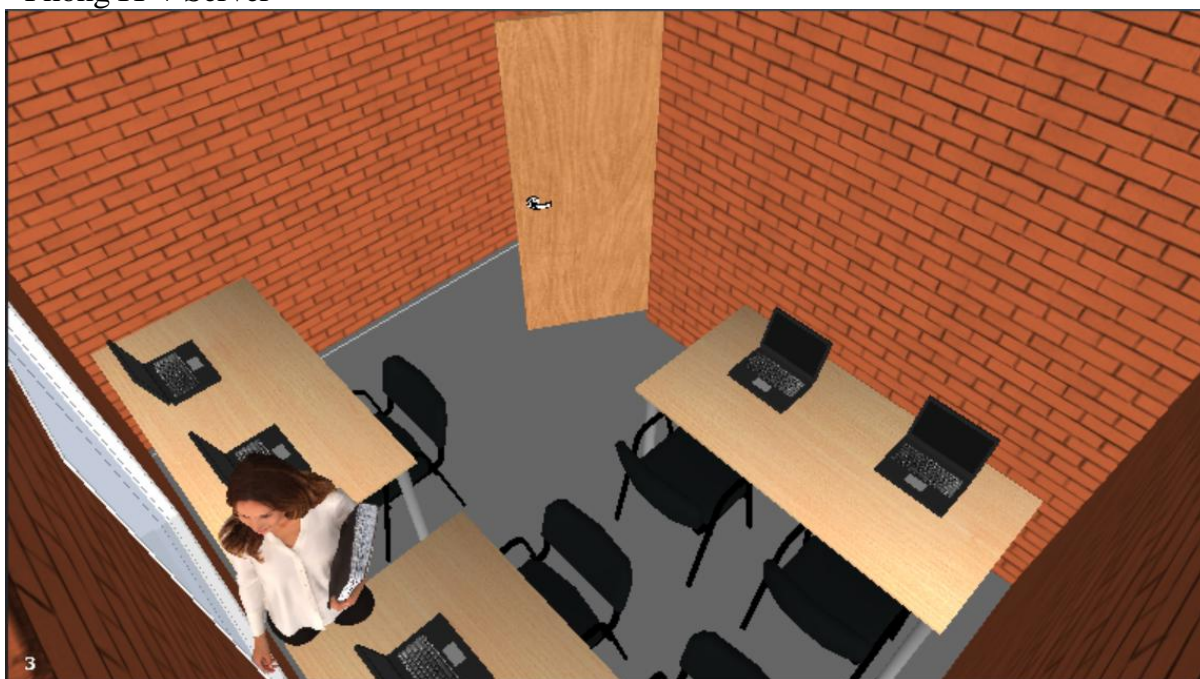
Hình 15. Sảnh

- Phòng bảo hành kỹ thuật



Hình 16. Phòng bảo hành kỹ thuật

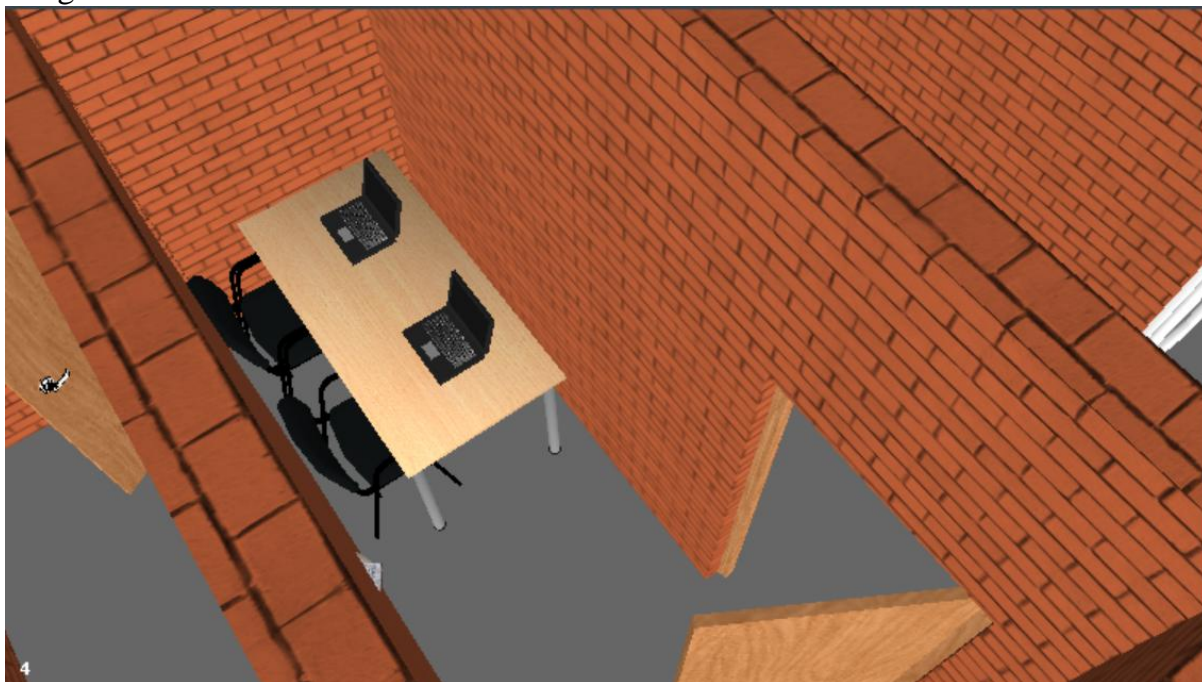
- Phòng IT + Server



Hình 17. Phòng IT và Server



Tầng 3



Hình 18. Tầng 3

- Phòng Giám Đốc

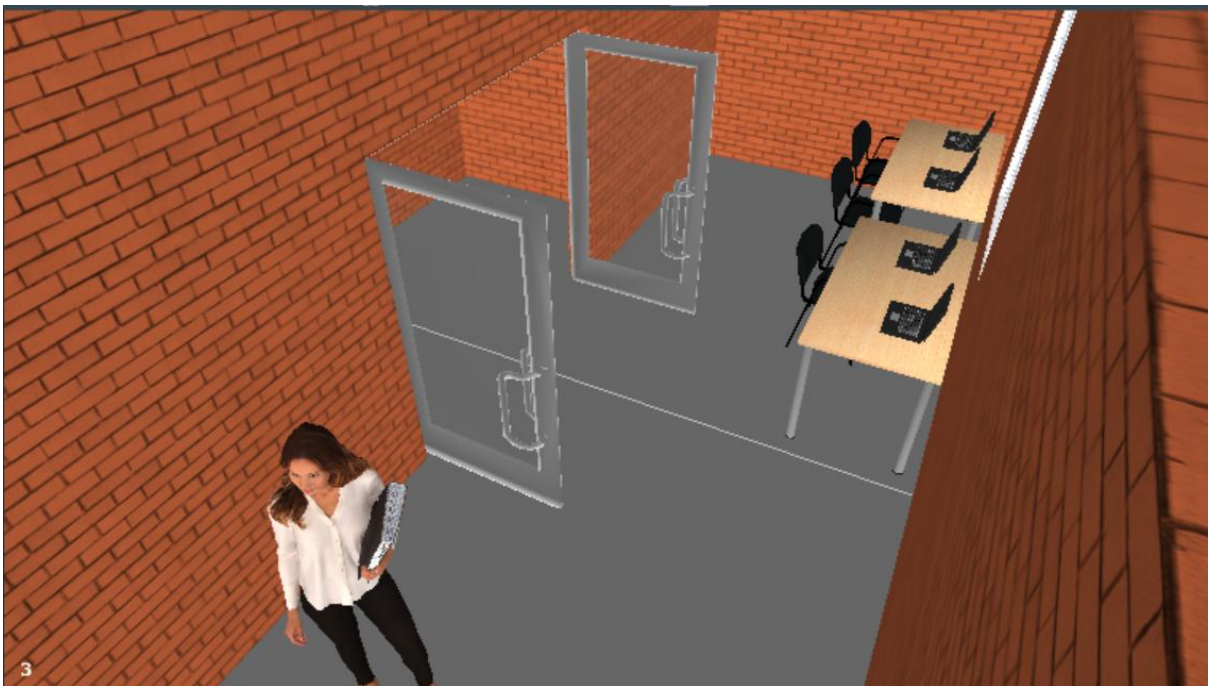


Hình 19. Phòng Giám Đốc





Hình 20. Cửa phòng Giám Đốc



Hình 21. Vị trí khác trong Phòng Giám Đốc

## 9. Triển khai các bảo mật

Các dự định sẽ cấu hình bảo mật

```
Group policy:
1. Cấm usb.
2. Đổi mật khẩu 3 tháng 1 lần.
3. Mật khẩu có kí tự đặc biệt (mk mạnh).

LAN:
1. Mỗi phòng ban có thể truy xuất dữ liệu của mình, nhưng k thể truy xuất phòng khác.
2. Không thể truy xuất web, ping tất cả.
3. Cho login vào domain.
4. Cho truy xuất web server.
5. Cho nslookup tất cả trang web.
6. Cho truy xuất youtube, google, facebook.
7. Cho ping nội bộ.

Wifi:
1. Truy xuất tất cả các web.
2. Cấm ping vào lan, server.
3. Không thể join domain.

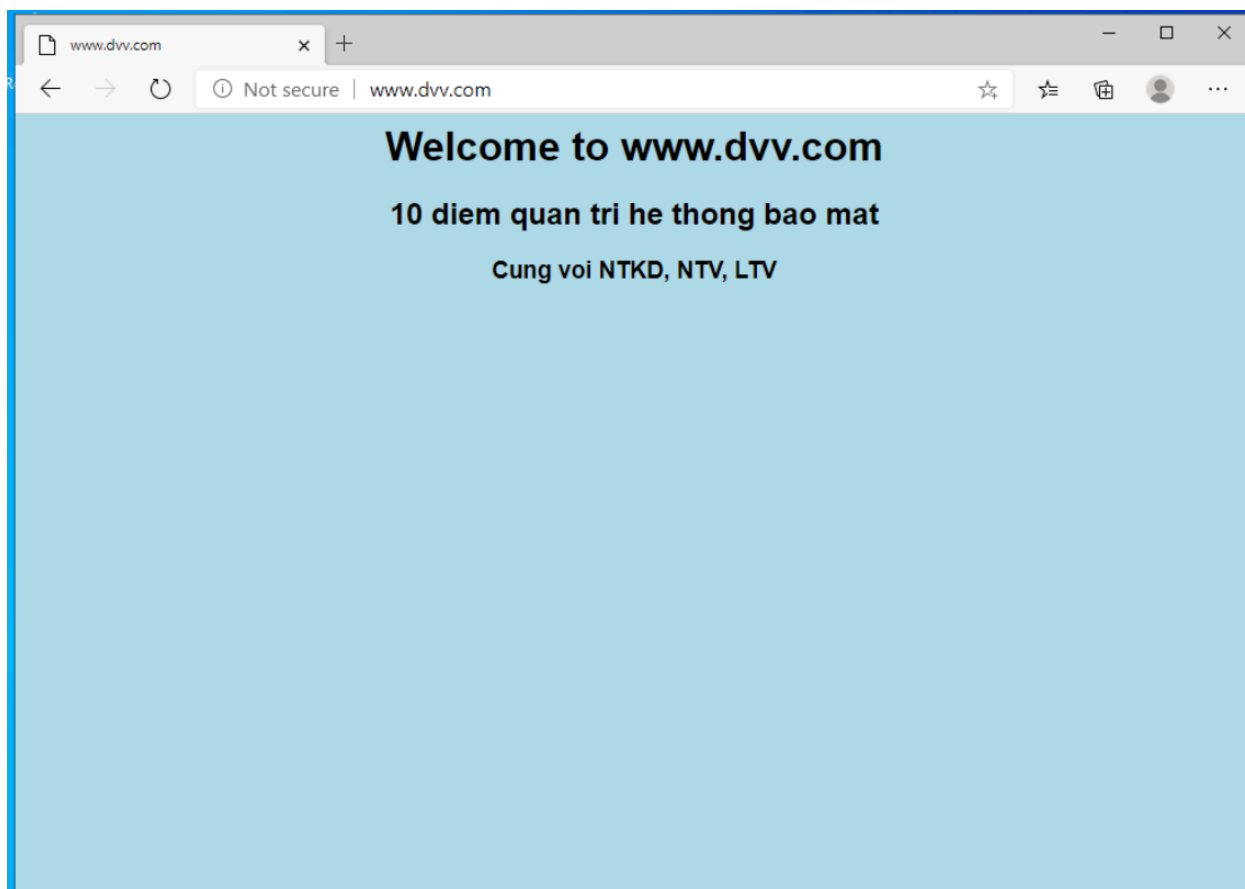
Server:
1. Backup dữ liệu.
2. Web server.
3. File server.
4. Bitlocker.
5. HTTPS.
6. Proxy.
```

Hình 22. Các dự định bảo mật sẽ triển khai

## 9.1 Server

### 1. Web server:

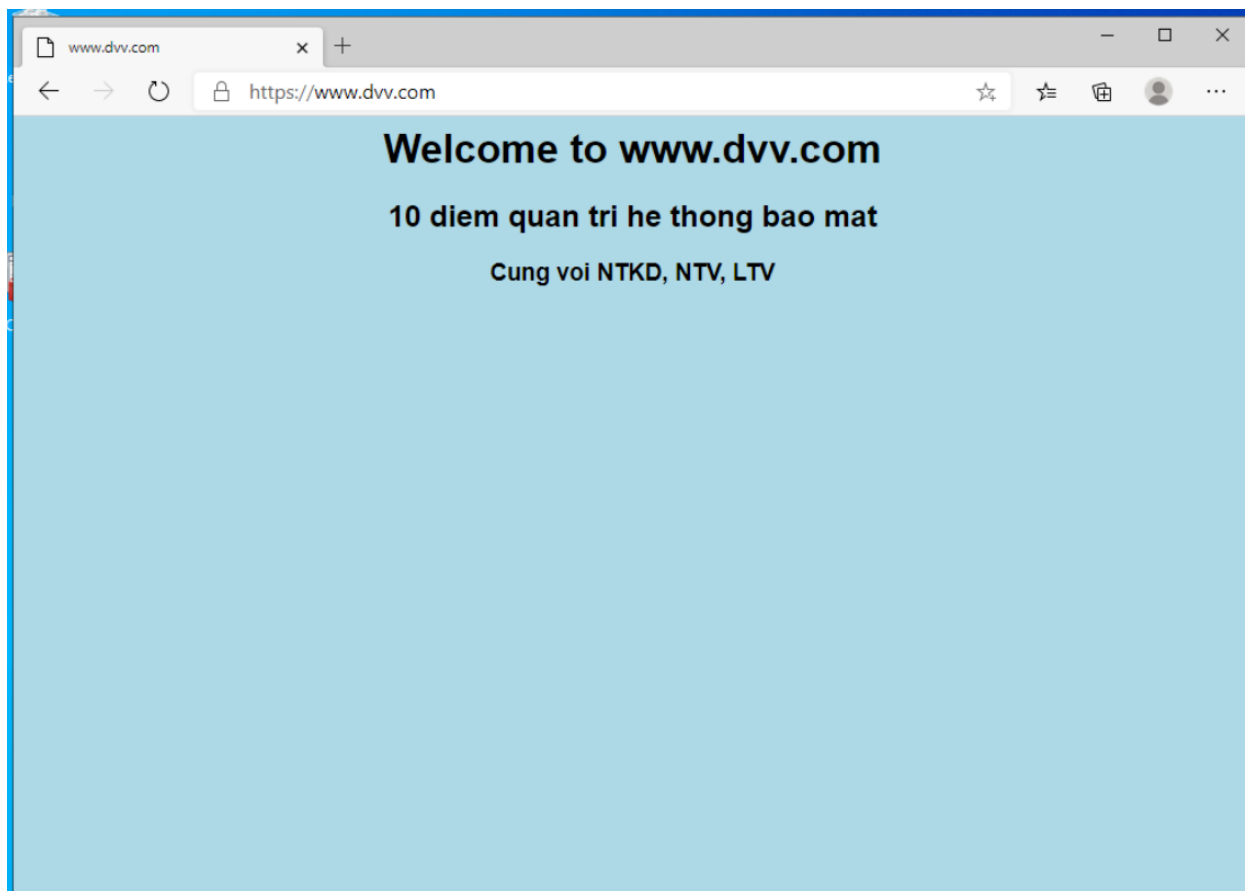
- Trang web http.



Hình 23. Trang web HTTP

## 2. HTTPS:

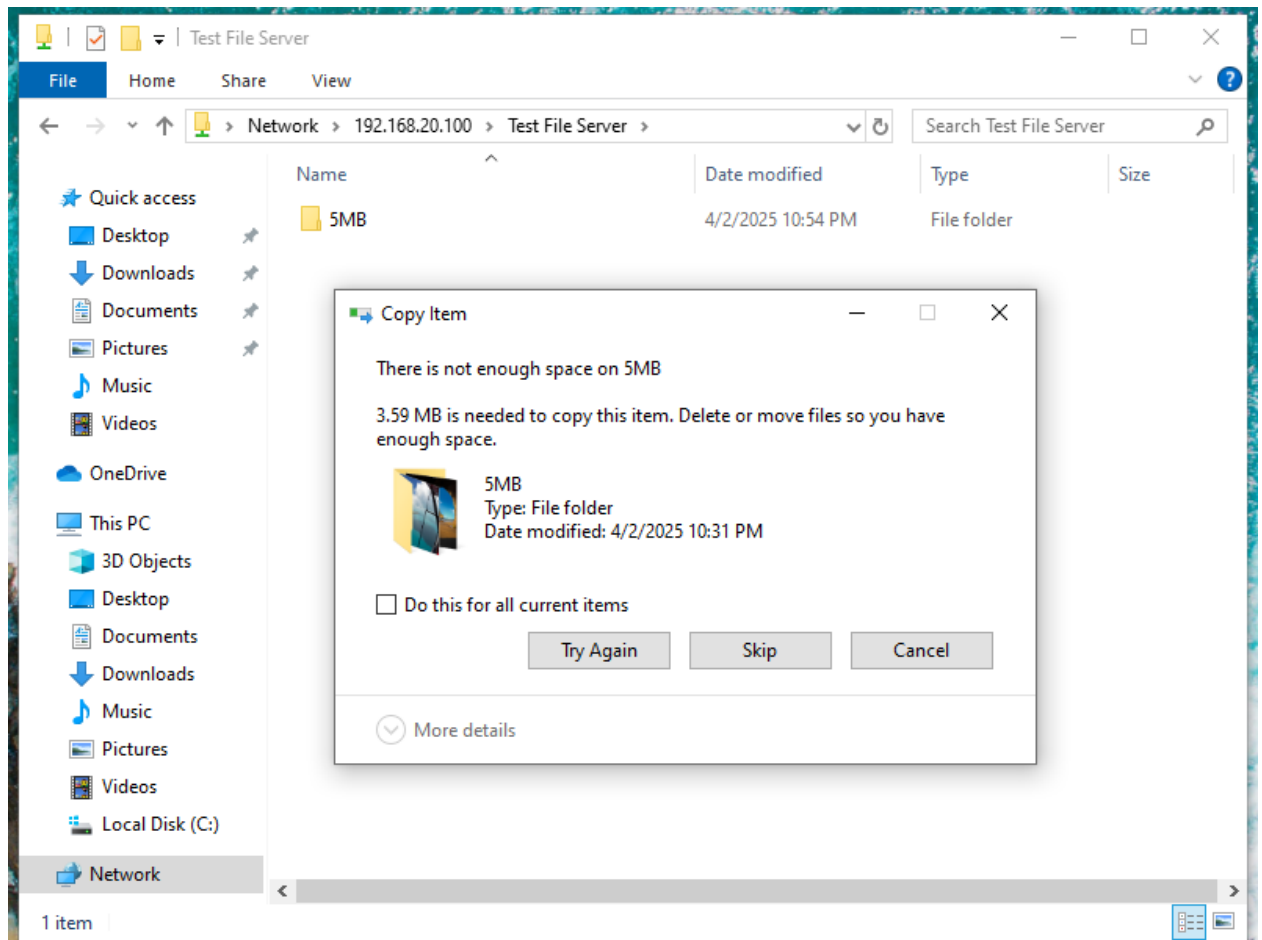
- Trang web https.



Hình 24. Trang web HTTPS

### 3. File server:

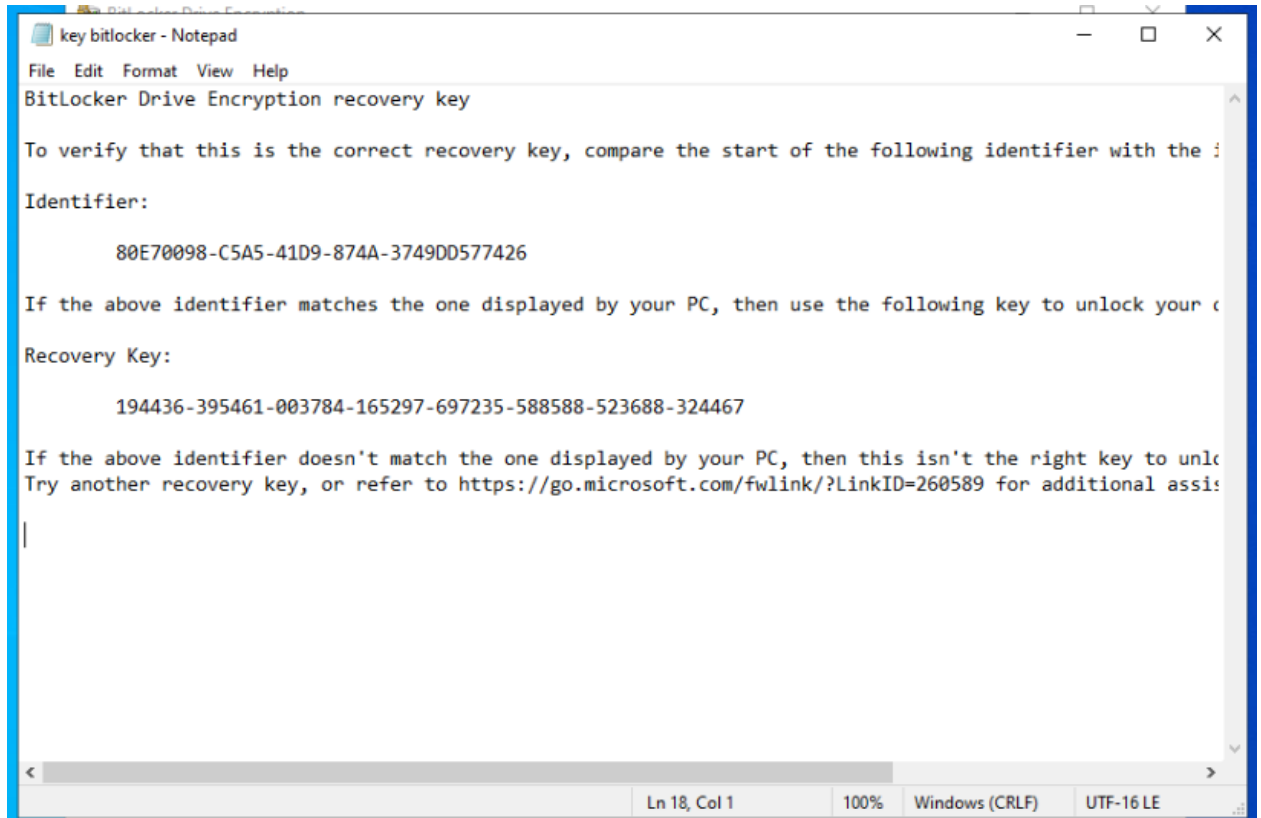
- Các users không thể gửi file quá 5MB.



Hình 25. Các users không thể gửi file quá 5MB.

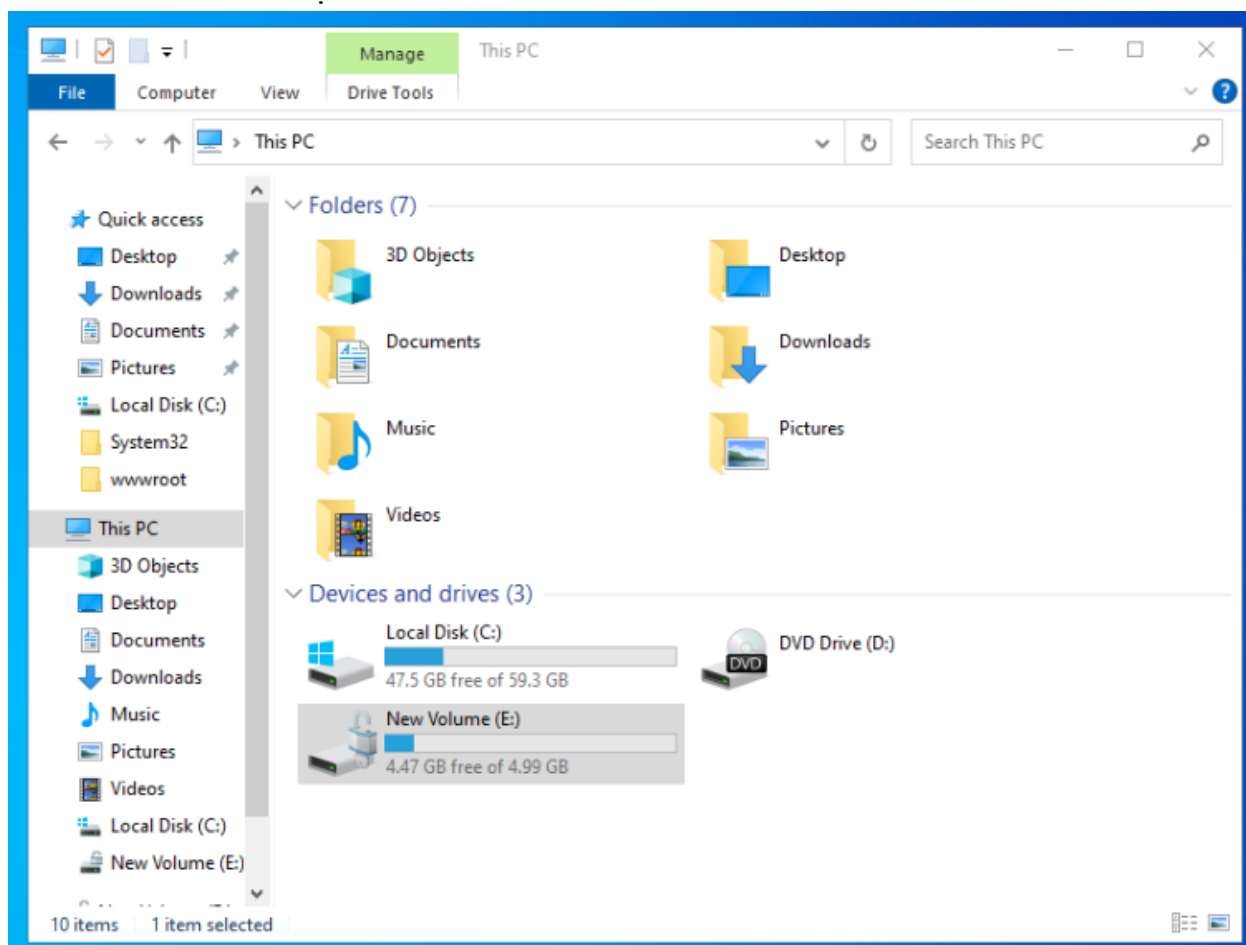
#### 4. Bitlocker:

- Pass: abc@123456789



Hình 26. Bitlocker Pass: abc@123456789

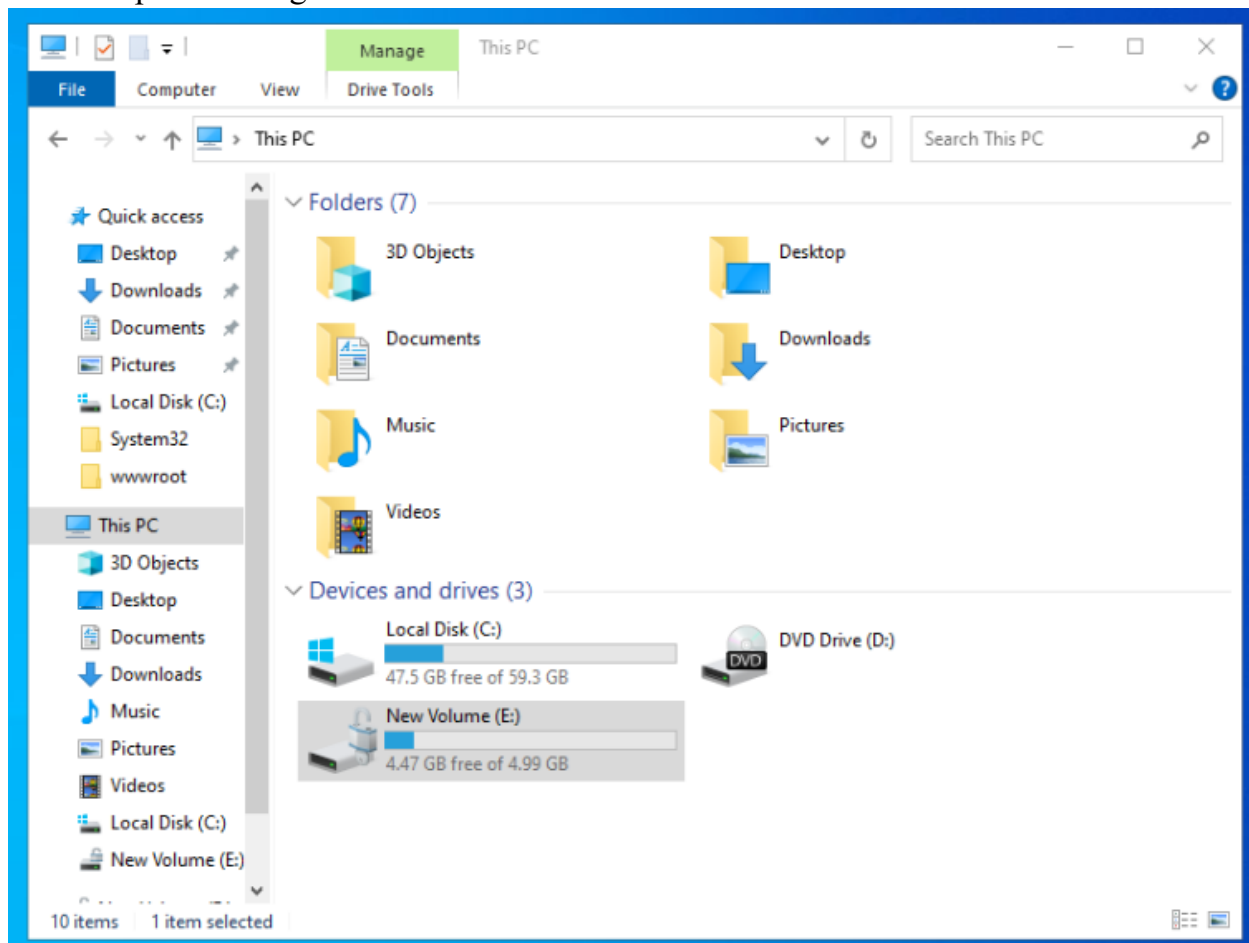
Mã hóa ổ E: chứa dữ liệu.



Hình 27. Mã hóa ổ E chứa dữ liệu

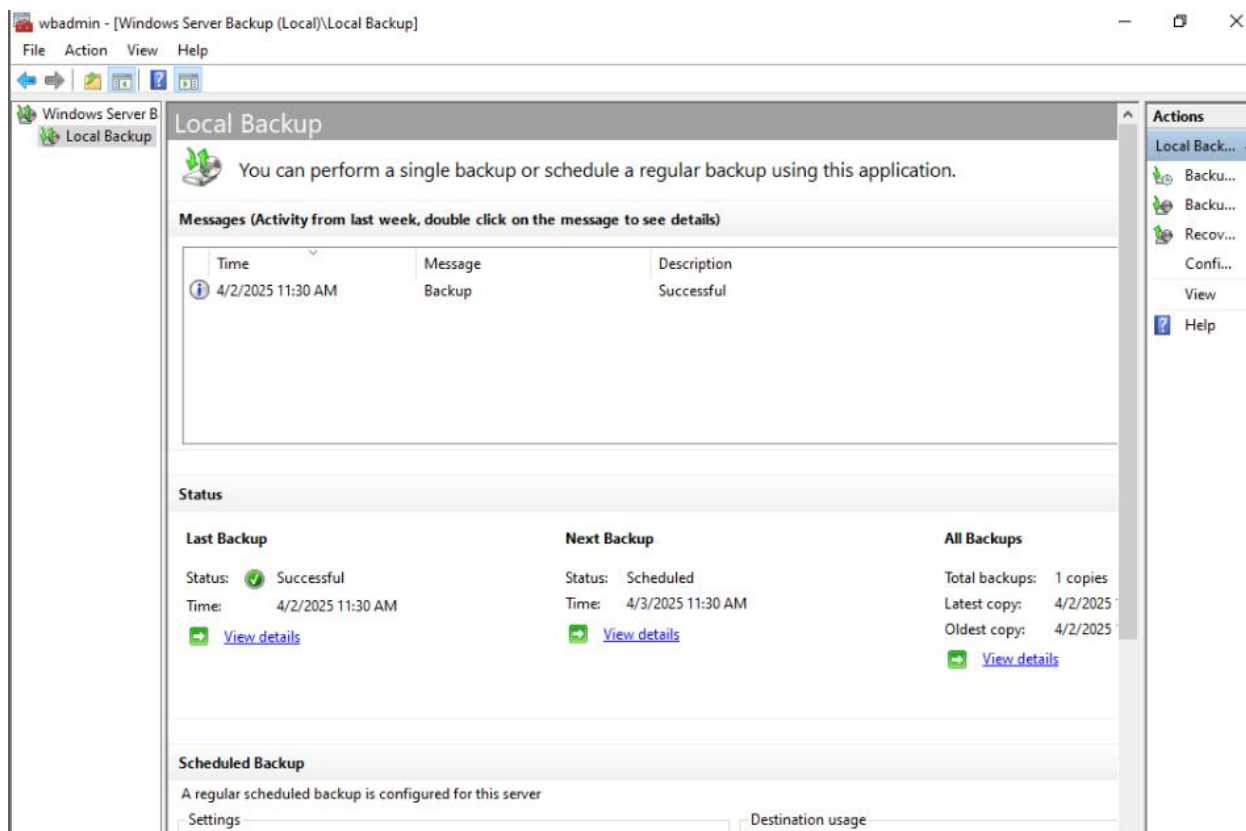
## 5. Backup server.

- Đã backup thành công.

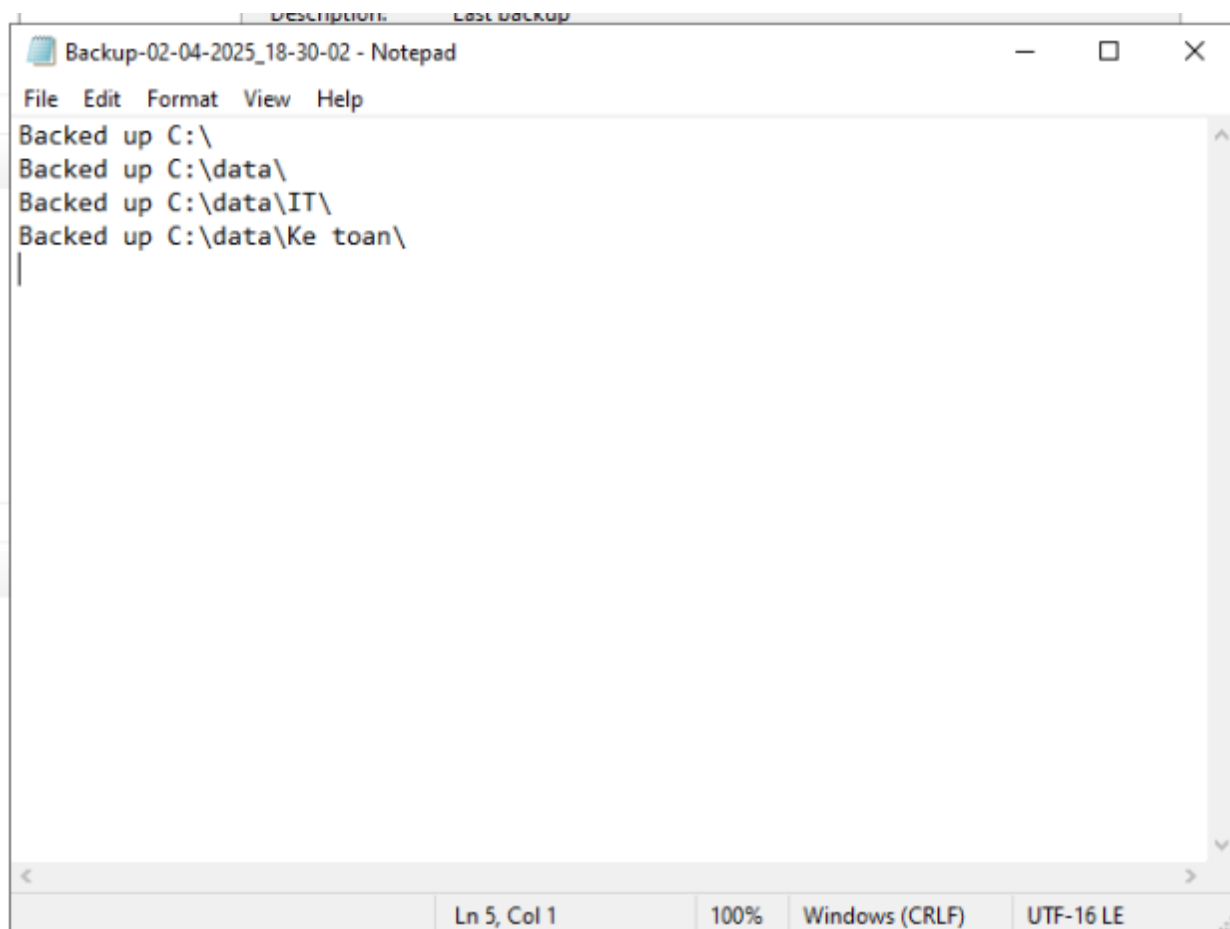


Hình 28. Backup thành công





- Những gì đã backup.



Hình 29. Dữ liệu đã Backup

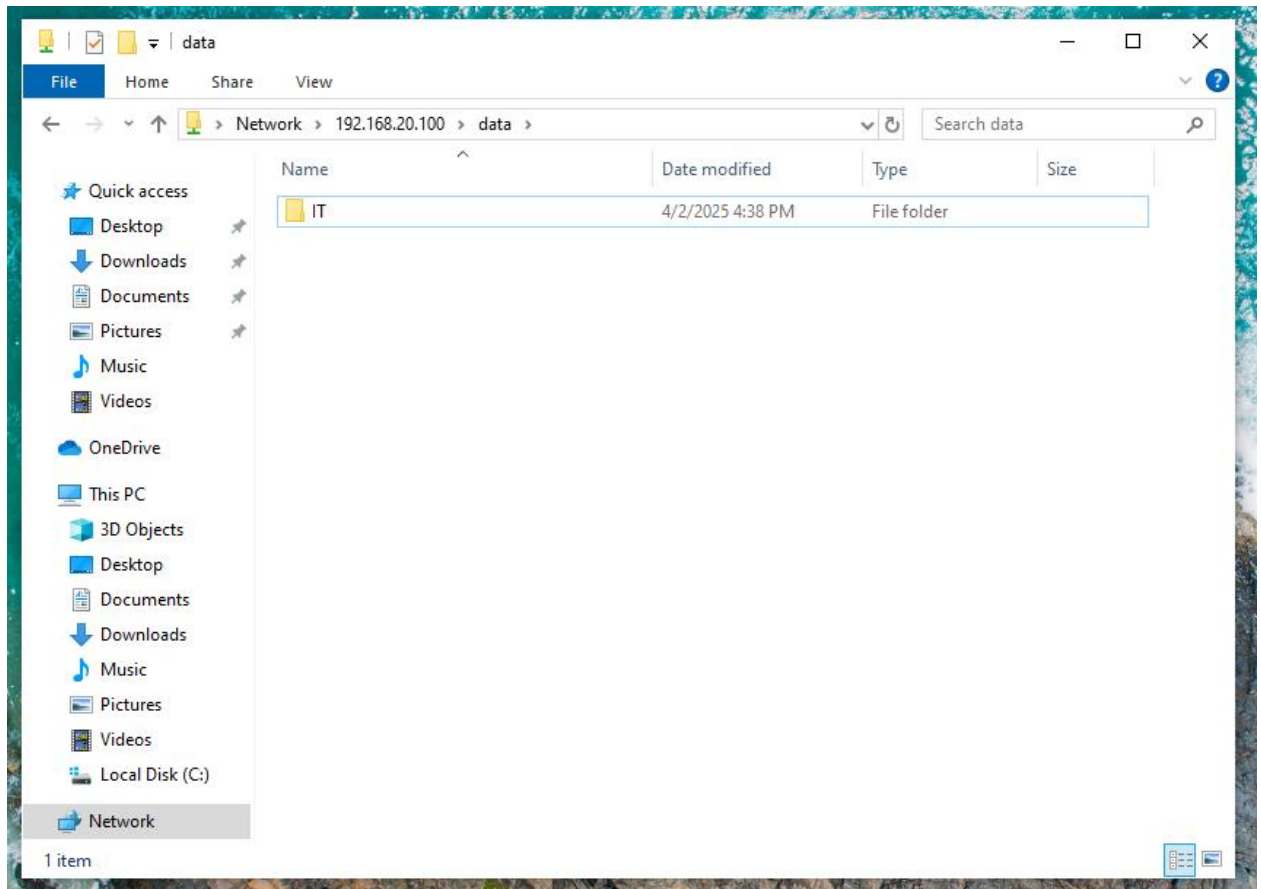
## 9.2 LAN:

- Rule của máy LAN:

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/1.45 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	3/253 KiB	IPv4 TCP	LAN subnets	*	57.144.144.1	443 (HTTPS)	*	none		truy xuất facebook	
<input type="checkbox"/>	0/170 KiB	IPv4 TCP	LAN subnets	*	142.250.199.78	443 (HTTPS)	*	none		truy xuất google	
<input type="checkbox"/>	0/2.96 MiB	IPv4 TCP	LAN subnets	*	142.250.197.238	443 (HTTPS)	*	none		truy xuất youtube	
<input type="checkbox"/>	61/150 KiB	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	0/960 B	IPv4 ICMP any	LAN subnets	*	192.168.20.100	*	*	none		ping server	
<input type="checkbox"/>	0/8 KiB	IPv4 TCP	LAN subnets	*	OPT2 subnets	80 (HTTP)	*	none		cho truy xuất web	
<input type="checkbox"/>	0/81 KiB	IPv4 TCP	LAN subnets	*	OPT2 subnets	443 (HTTPS)	*	none		truy xuất web noi bo	
<input type="checkbox"/>	1/7.74 MiB	IPv4 *	LAN subnets	*	OPT2 subnets	*	*	none		cho login	
<input type="checkbox"/>	70/25.38 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

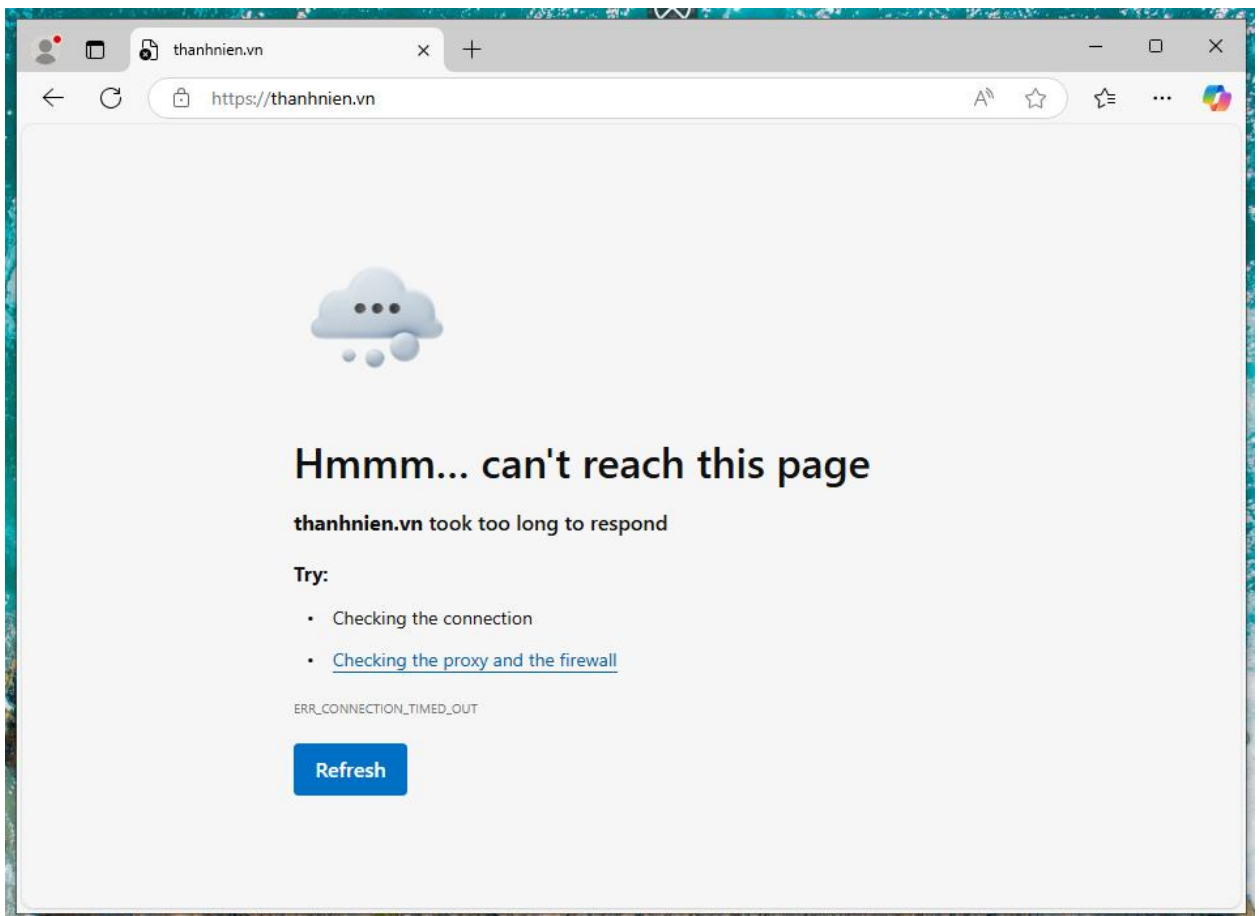
Hình 30. Rule của máy LAN:

1. Truy xuất dữ liệu của phòng ban nhưng không thể truy xuất phòng ban khác:
  - Đang đăng nhập user IT1 thì chỉ có thể truy cập file của phòng IT, không thấy được các phòng khác.



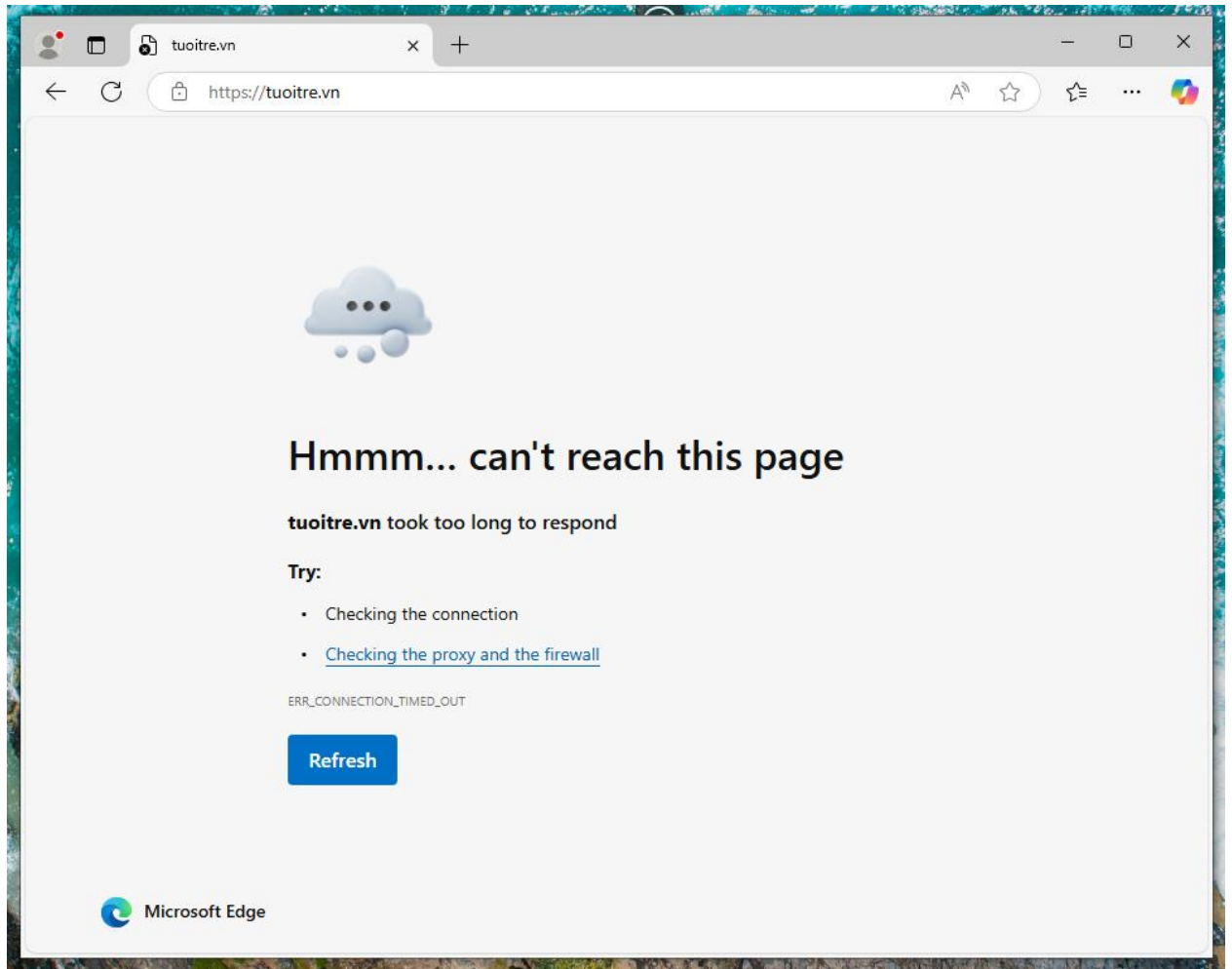
Hình 31. Truy xuất dữ liệu phòng ban

2. Không thể truy xuất web bên ngoài:
- Không thể truy xuất thanhnien.vn.



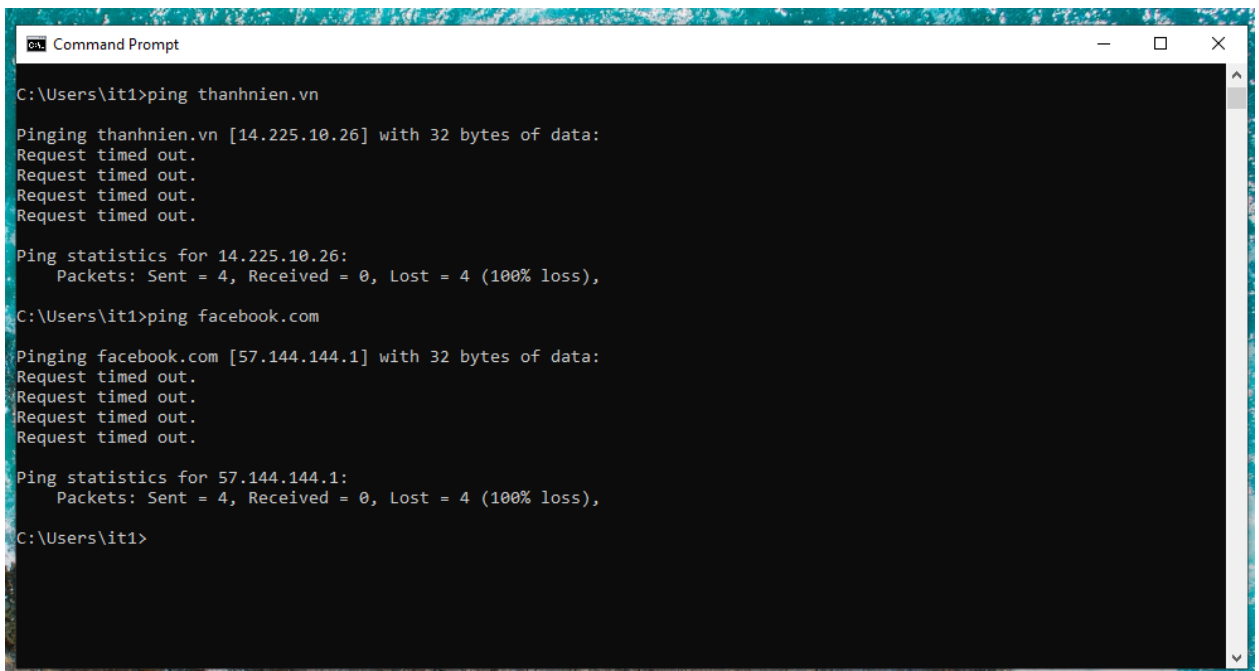
Hình 32. Không thể truy xuất thanhnien.vn.

- Không thể truy cập tuoitre.vn



Hình 33. Không thể truy cập tuoitre.vn

3. Không thể ping ra bên ngoài:
- Không thể ping tới thanhnien.vn và facebook.com:



```
C:\Users\it1>ping thanhkien.vn

Pinging thanhkien.vn [14.225.10.26] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 14.225.10.26:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\it1>ping facebook.com

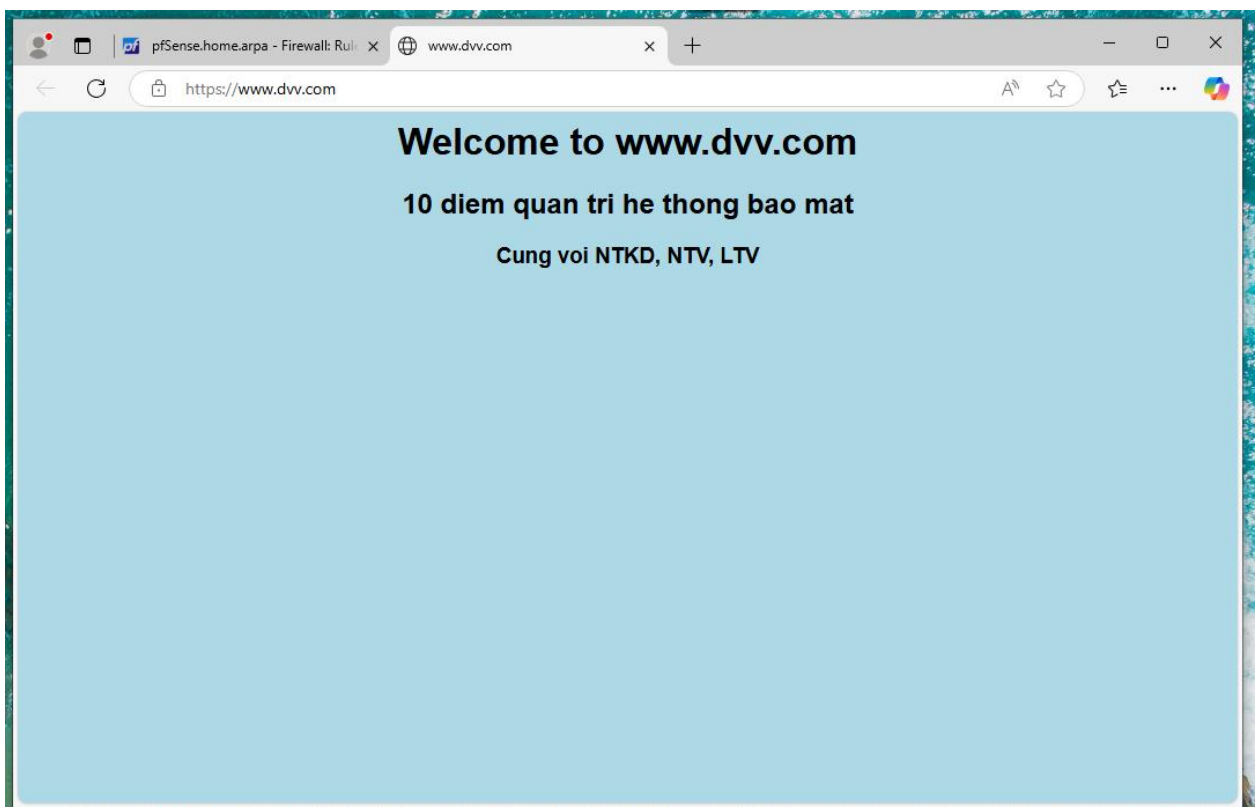
Pinging facebook.com [57.144.144.1] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 57.144.144.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\it1>
```

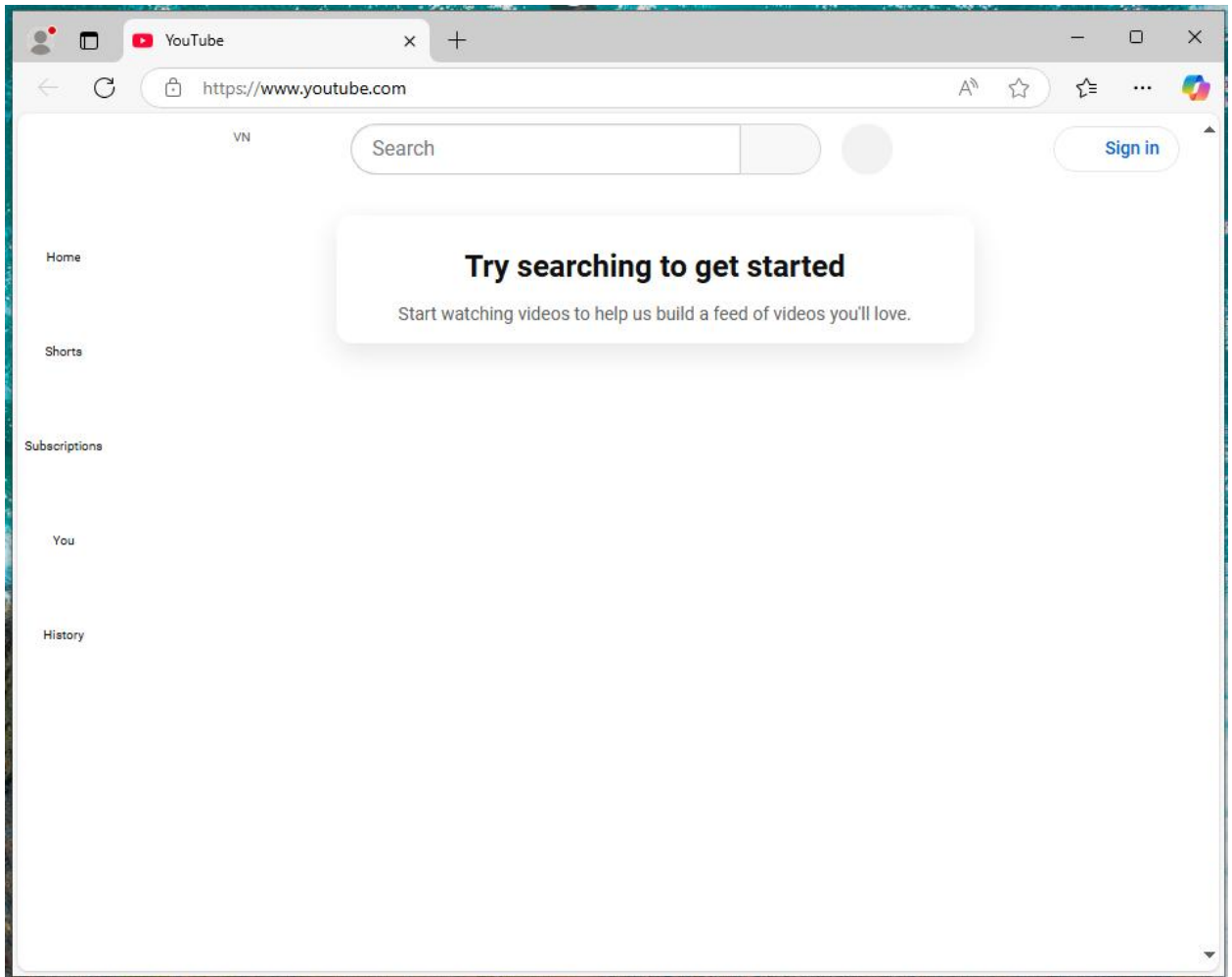
Hình 34. Không thể ping tới thanhnien.vn và facebook.com

4. Truy xuất web nội bộ:



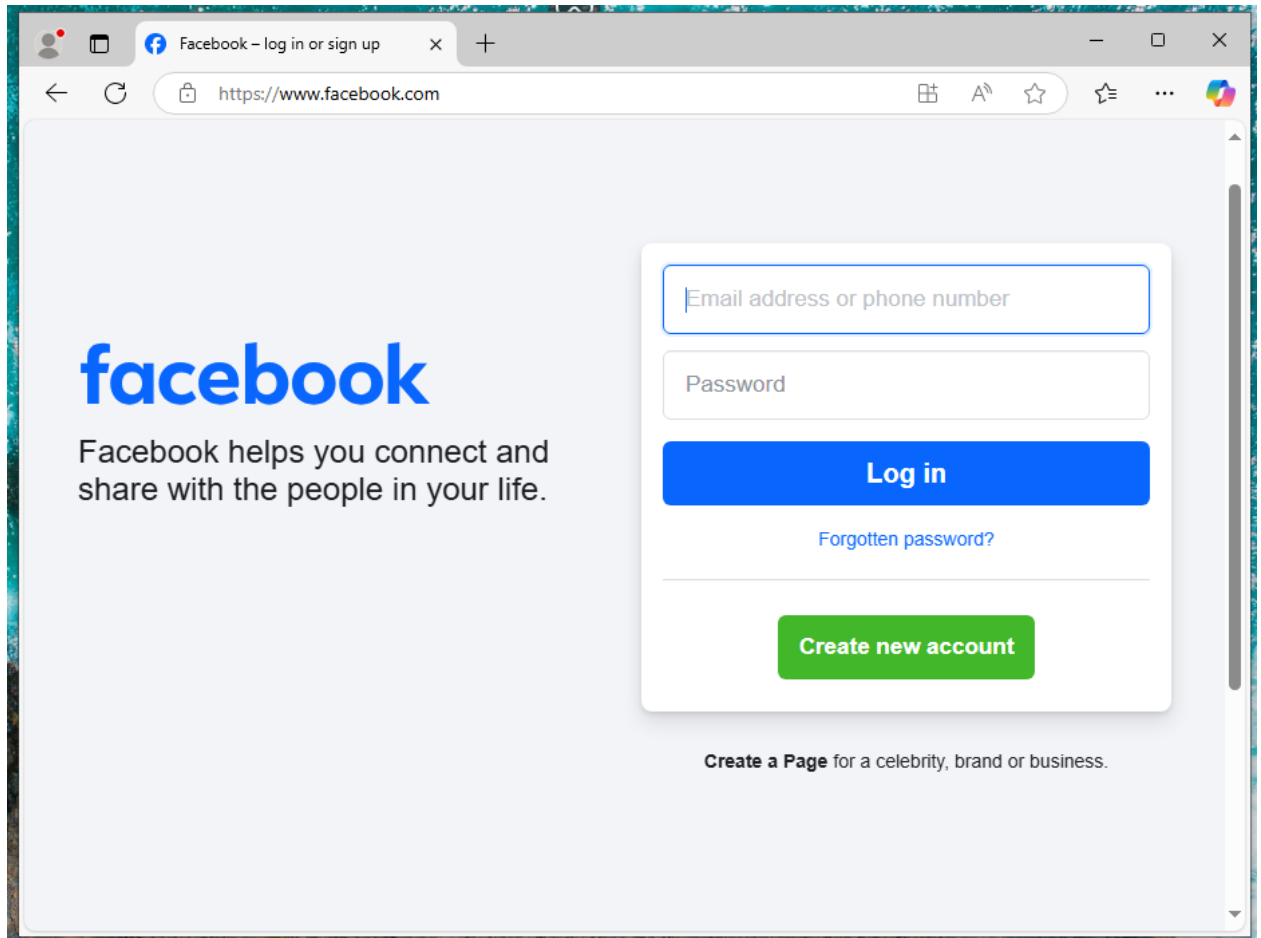
Hình 35. Truy suất web

5. Truy xuất youtube.com, google.com, facebook.com:
- Youtube.com:



Hình 36. Truy xuất Youtube.com

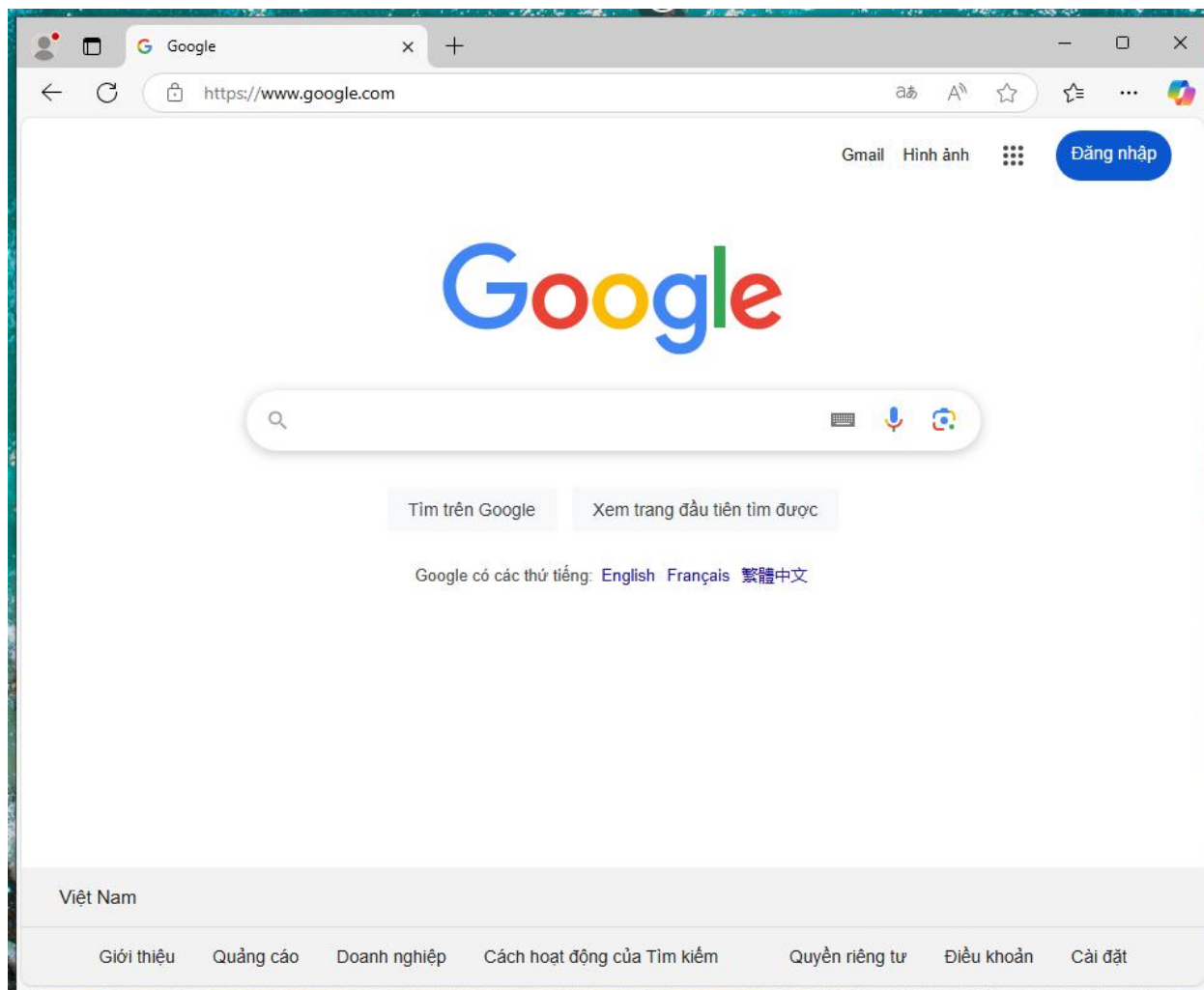
- Facebook.com:



Hình 37. truy xuất Facebook.com

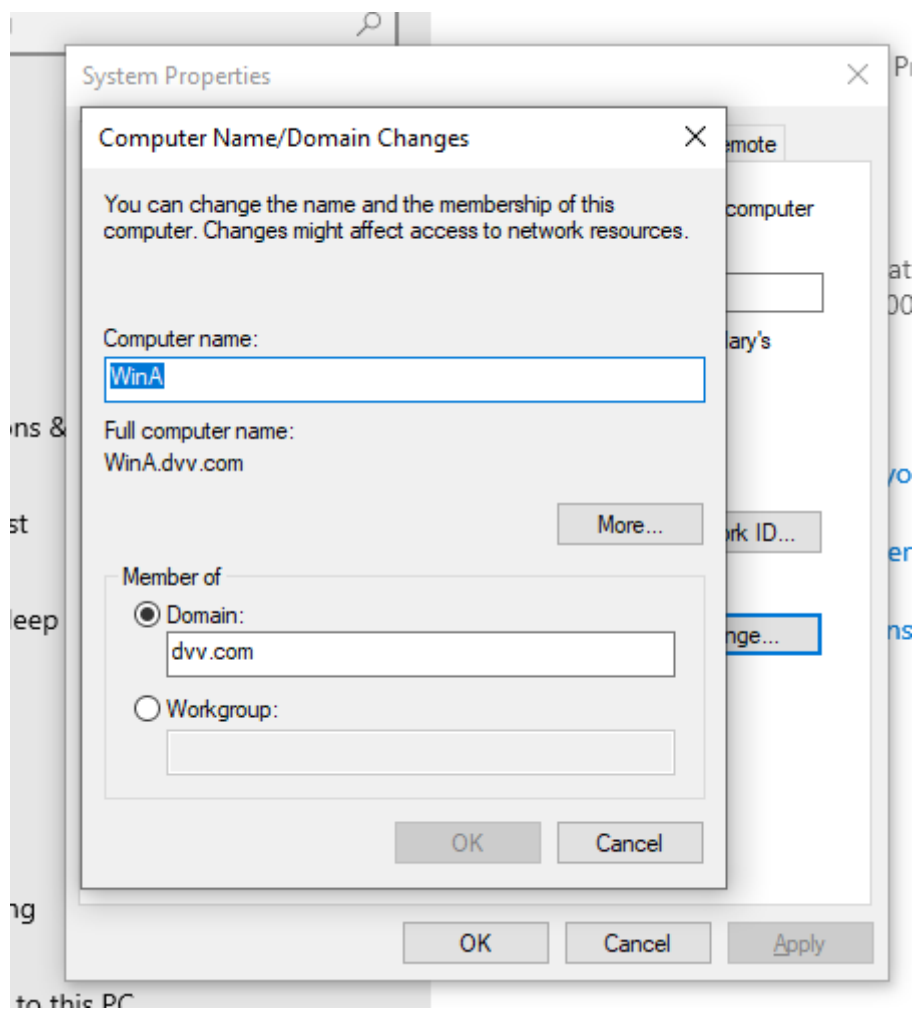


- Google.com:



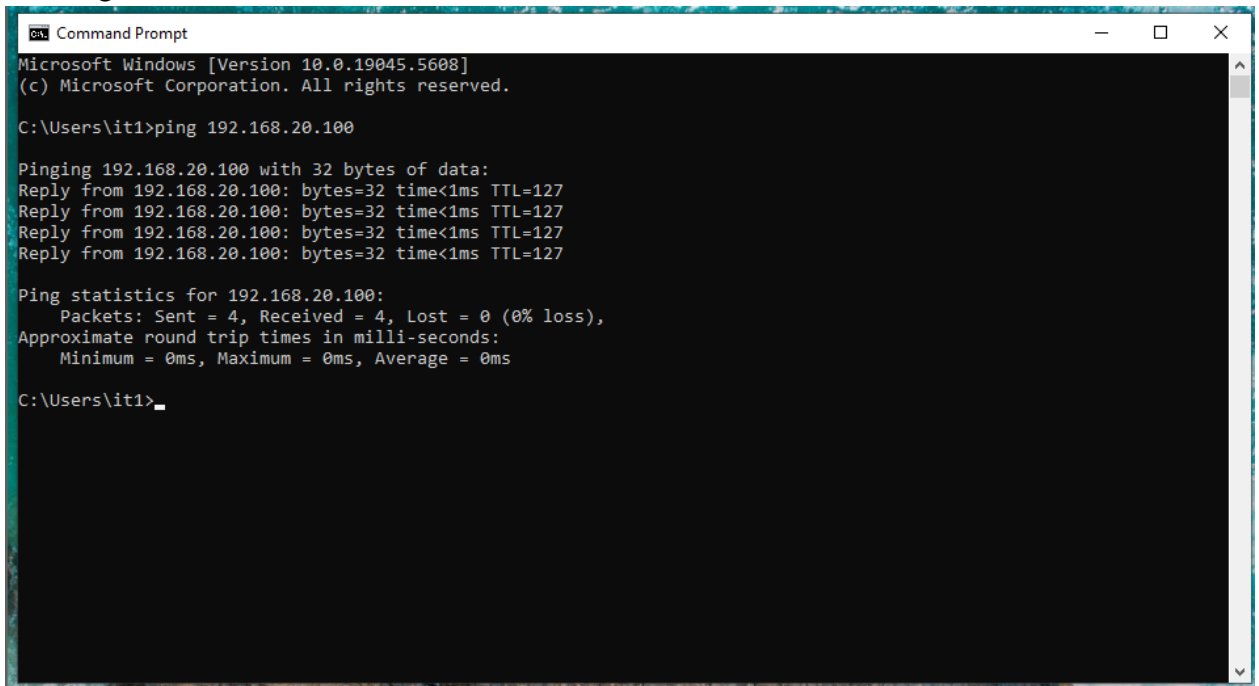
Hình 38. Truy xuất Google.com

6. Cho login vào domain:



Hình 39. Join vào domain

Ping nội bộ, server:



```
Command Prompt
Microsoft Windows [Version 10.0.19045.5608]
(c) Microsoft Corporation. All rights reserved.

C:\Users\it1>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:
Reply from 192.168.20.100: bytes=32 time<1ms TTL=127
Reply from 192.168.20.100: bytes=32 time<1ms TTL=127
Reply from 192.168.20.100: bytes=32 time<1ms TTL=127
Reply from 192.168.20.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms






C:\Users\it1>
```

9.3 Wifi:

- Rule của wifi:

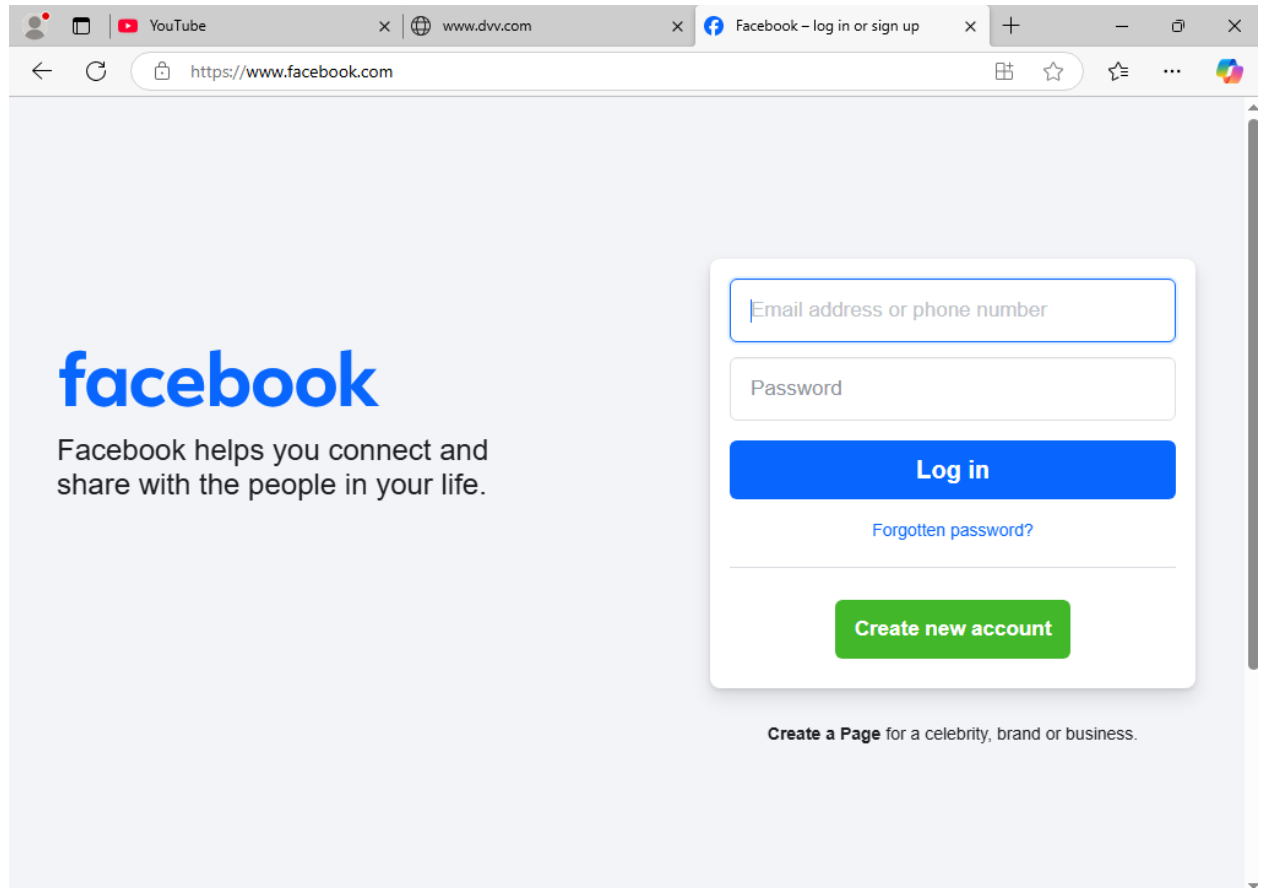
Floating   WAN   LAN   **OPT1**   OPT2

Rules (Drag to Change Order)

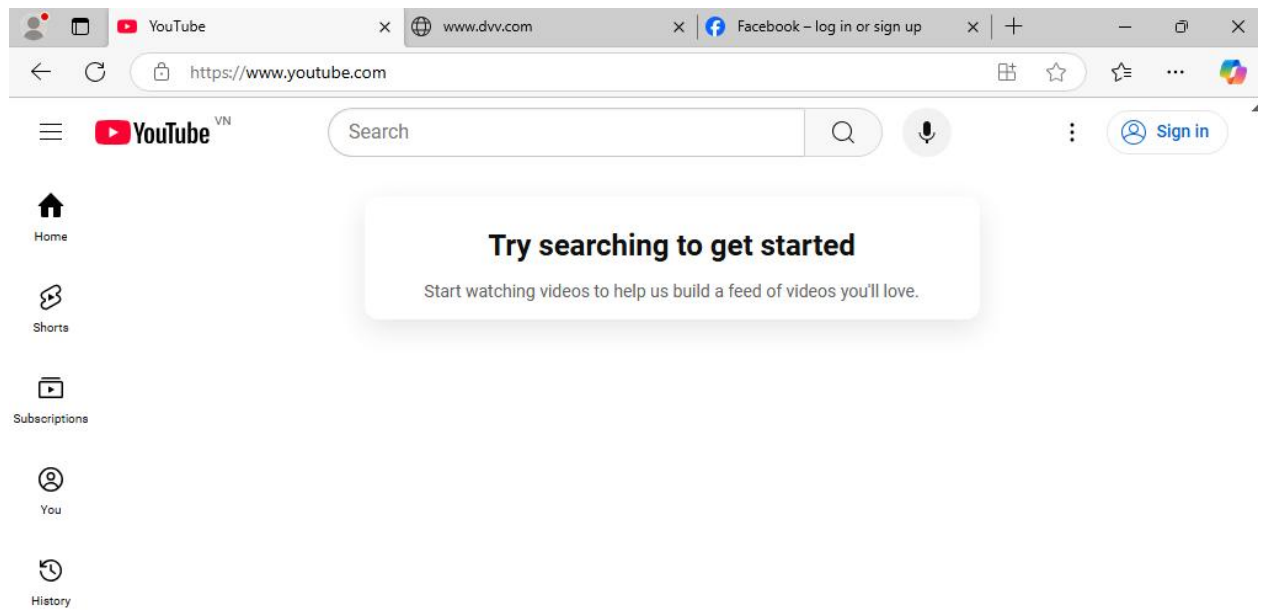
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/9 KiB	IPv4 TCP	OPT1 subnets	*	OPT2 subnets	80 (HTTP)	*	none		cho truy xuất web noi bo	
<input type="checkbox"/>	✓ 0/33 KiB	IPv4 TCP	OPT1 subnets	*	OPT2 subnets	443 (HTTPS)	*	none		truy xuất web noi bo	
<input type="checkbox"/>	✗ 0/240 B	IPv4 *	OPT1 subnets	*	192.168.100.100	*	*	none		cam lan	
<input type="checkbox"/>	✗ 0/971 B	IPv4 *	OPT1 subnets	*	192.168.20.100	*	*	none		cam server	
<input type="checkbox"/>	✓ 10/107.72 MiB	IPv4 *	OPT1 subnets	*	*	*	*	none		truy xuất tat ca	

Hình 40. Rule Wifi

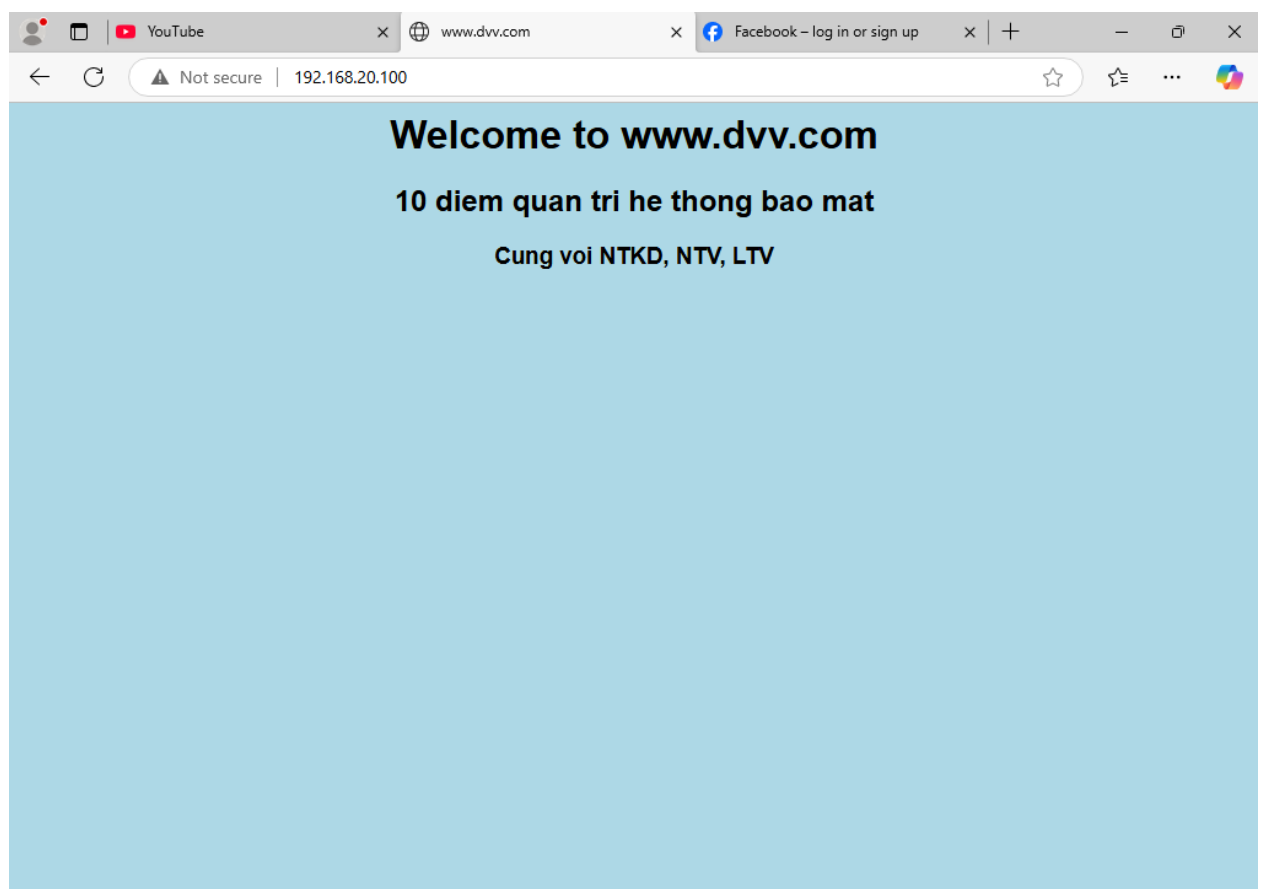
## 1. Truy xuất tất cả web:



Hình 41. Truy xuất Facebook.com

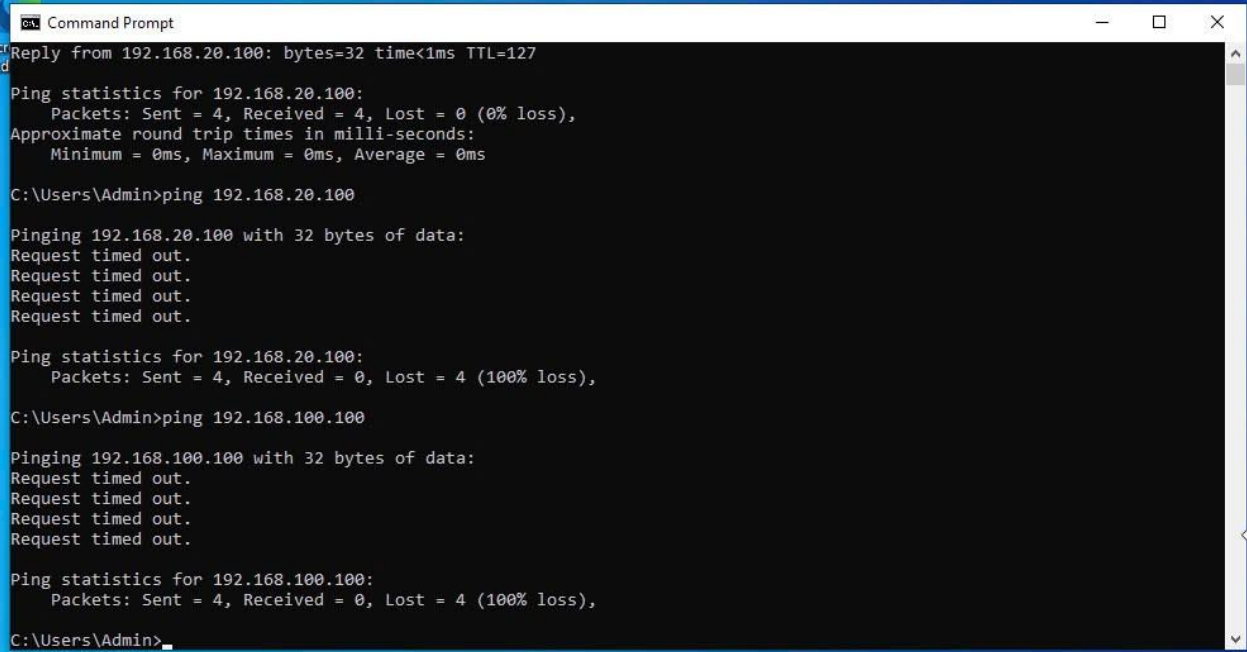


Hình 42. Truy suất Youtube.com



Hình 43. Truy xuất web

## 2. Cắm Ping vào LAN, Server:



```
Command Prompt
Reply from 192.168.20.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Admin>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

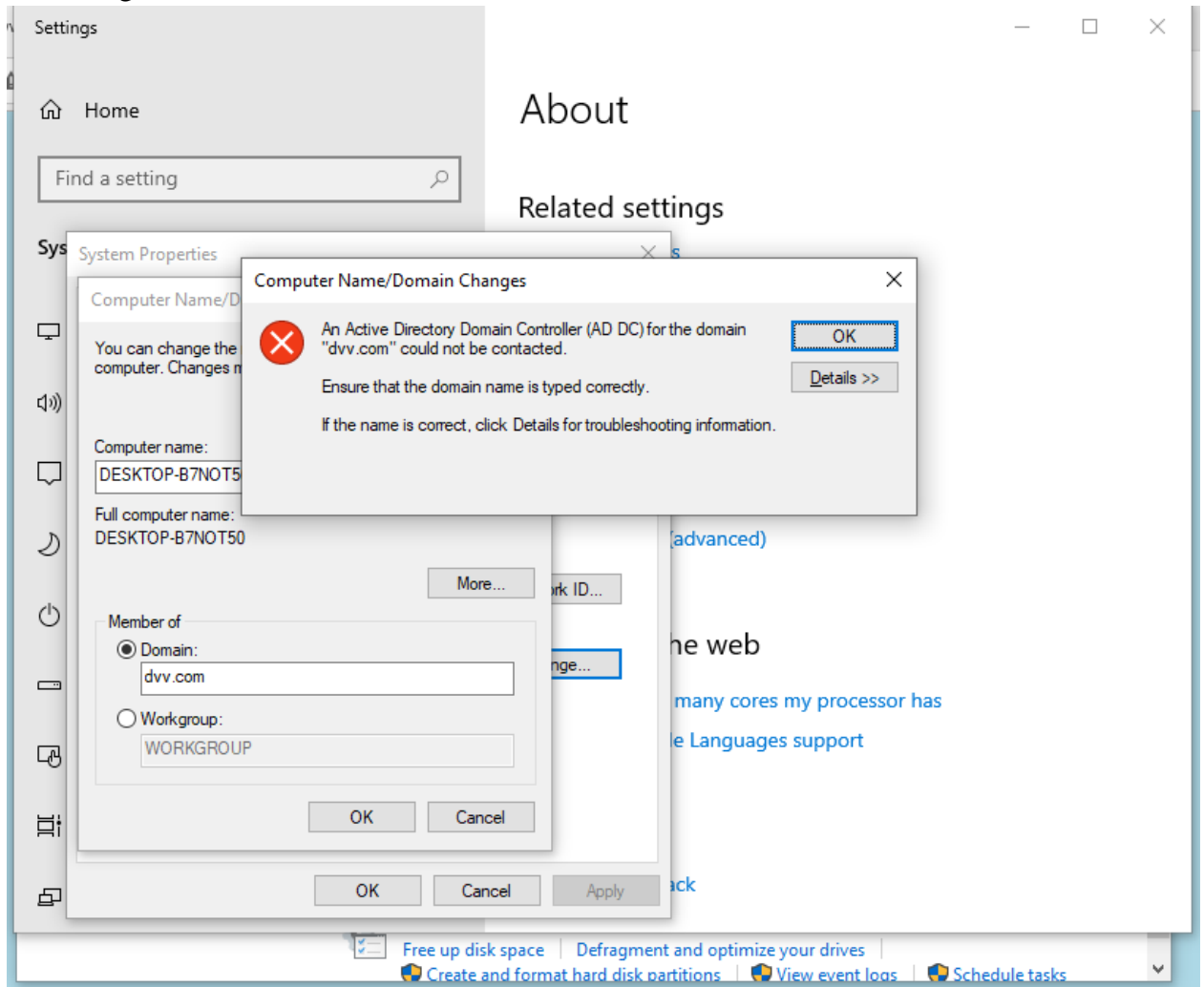
Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>
```

Hình 44. Cắm ping



## 2. Không thể Join Domain:

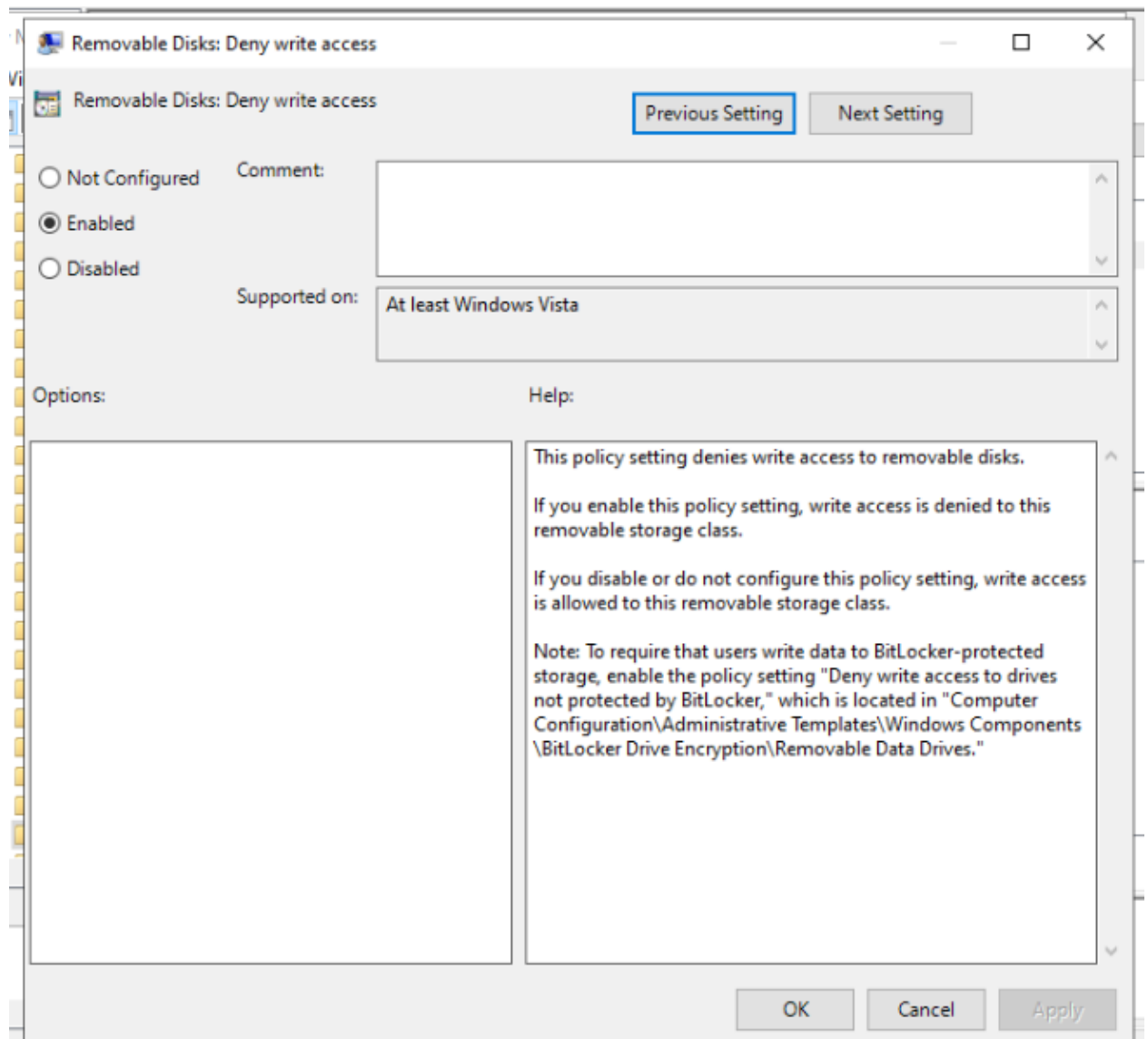


Hình 45. Không thể Join Domain



#### 9.4 Group Policy:

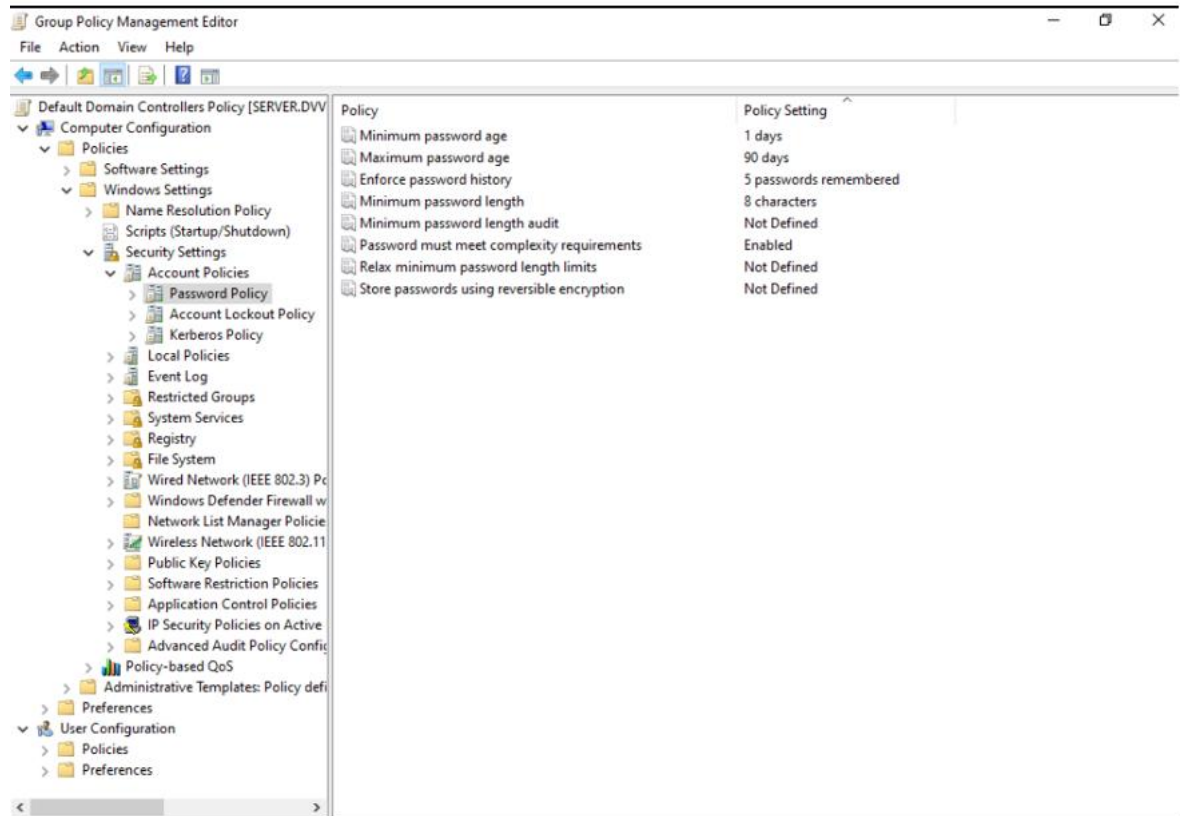
##### 1. Cấm USB ghi dữ liệu:



Hình 46. Cấm USB ghi dữ liệu

## 2. Yêu cầu mật khẩu:

- Mật khẩu có thể dùng tối đa 3 tháng.
- 1 ngày chỉ được đổi 1 lần.
- Không dùng lại mật khẩu cũ trong 5 lần gần nhất.
- Mật khẩu ít nhất 8 ký tự bao gồm chữ hoa, chữ thường, ký tự đặc biệt.



Hình 47. Yêu cầu mật khẩu

## CHƯƠNG IV. KẾT LUẬN

### Kết quả đạt được

Đã thiết lập, cấu hình

#### Server

- Web
- HTTP
- HTTPS
- File Server
- Bitlocker

#### LAN

- Rule máy LAN
- Không thể truy xuất dữ liệu
- Không thể truy xuất web bên ngoài

#### Wifi

- Rule wifi
- Truy xuất tất cả web
- Cấm ping
- Không thể join domain

#### Group policy

- Cấm USB
- Yêu cầu mật khẩu

## TÀI LIỆU THAM KHẢO

- [1] <https://viblo.asia/p/active-directory-domain-services-in-computer-network-active-directory-domain-services-trong-mang-may-tinh-phan-1-aNj4vDnxL6r>
- [2] <https://nhanhoa.com/tin-tuc/dhcp-la-gi.html>
- [3] <https://fptshop.com.vn/tin-tuc/danh-gia/dns-la-gi-168829>
- [4] <https://interdata.vn/blog/file-server-la-gi/>
- [5] <https://aws.amazon.com/vi/what-is/vpn/>
- [6] <https://quantrimang.com/cong-nghe/ly-thuyet-proxy-la-gi-117220>
- [7] <https://quantrimang.com/cong-nghe/ips-he-thong-ngan-ngua-xam-nhap-tuong-lua-the-he-ke-tiep-6377>
- [8] <https://tnten.vn/tin-tuc/ids-la-gi/>
- [9] <https://quantrimang.com/cong-nghe/tong-quan-ve-firewall-84474>