

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ – TIN HỌC THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN MÔN HỌC: Quản Trị Hệ Thống Bảo Mật
ĐỀ TÀI : XÂY DỰNG CHIẾN LƯỢC BẢO MẬT CHO HỆ THỐNG THÔNG TIN
DOANH NGHIỆP BÁN NHẠC CỤ

GIÁO VIÊN HƯỚNG DẪN : Th.S Đinh Xuân Lâm

Nhóm: 1

Thành Viên :

- | | |
|--------------------|------------------|
| 1. Trần Quang Khải | MSSV: 22DH114583 |
| 2. Ngô Thế Đức | MSSV: 22DH114504 |
| 3. Đào Đức Lương | MSSV: 22DH114621 |

Tp. Hồ chí minh, Ngày 3 tháng 4 năm 2024

LỜI CẢM ƠN

Tôi xin gửi lời cảm ơn chân thành và sâu sắc đến ThS. Đinh Xuân Lâm, người đã tận tình hướng dẫn, hỗ trợ và truyền đạt những kiến thức quý báu trong suốt quá trình tôi thực hiện đồ án này. Nhờ có sự chỉ dạy tận tâm của thầy, tôi không chỉ hiểu rõ hơn về các nguyên tắc lý thuyết mà còn có cơ hội vận dụng chúng vào thực tiễn, rèn luyện tư duy logic, kỹ năng phân tích và giải quyết vấn đề một cách khoa học. Những góp ý và định hướng từ thầy đã giúp tôi hoàn thiện đồ án với chất lượng tốt nhất và tích lũy thêm nhiều kinh nghiệm quý giá trong quá trình nghiên cứu và phát triển.

Tôi cũng xin gửi lời cảm ơn đến quý thầy cô trong khoa, những người đã giảng dạy và trang bị cho tôi nền tảng kiến thức vững chắc trong suốt thời gian học tập. Những bài giảng, những chia sẻ và định hướng của thầy cô không chỉ giúp tôi mở rộng hiểu biết về lĩnh vực mình theo đuổi mà còn tạo động lực để tôi tiếp tục học hỏi và nâng cao năng lực của bản thân.

Việc thực hiện đồ án một mình là một trải nghiệm đầy thử thách nhưng cũng rất ý nghĩa, giúp tôi nâng cao khả năng tự học, tự nghiên cứu và giải quyết vấn đề một cách độc lập. Quá trình này không chỉ giúp tôi củng cố kiến thức chuyên môn mà còn rèn luyện tinh thần trách nhiệm, sự kiên trì trước những khó khăn. Những kinh nghiệm quý báu có được từ quá trình thực hiện đồ án chắc chắn sẽ là hành trang hữu ích, hỗ trợ tôi trong công việc sau này, giúp tôi có thể thích nghi và phát triển tốt hơn trong môi trường làm việc thực tế.

Tôi xin chân thành cảm ơn!

NHẬN XÉT GIẢNG VIÊN

MỤC LỤC

CHƯƠNG I:	9
GIỚI THIỆU TỔNG QUAN VỀ DOANH NGHIỆP	9
1.1. Lĩnh vực kinh doanh	9
1.2. Quy mô tổ chức của doanh nghiệp	9
1.3. Mục đích triển khai hệ thống	12
1.3.1. Các yêu cầu cơ bản về kĩ thuật.....	12
1.3.2. Sơ đồ vật lí cụ thể.....	13
CHƯƠNG II:	15
LÝ THUYẾT TỔNG QUAN	15
2.1. Giới thiệu về Domain	15
2.1.1. Khái niệm	15
2.1.2. Tính năng và lợi ích.....	15
2.2. Giới thiệu về Proxy	18
2.2.1. Khái niệm	18
2.2.2. Tính năng và lợi ích.....	19
2.3. Giới thiệu về Firewall	20
2.3.1. Khái niệm	20
2.3.2. Chức năng và lợi ích.....	21
2.4. Giới thiệu về IDS/IPS	22
2.4.1. Khái niệm	22
2.4.2. Chức năng và lợi ích.....	23
2.5. Giới thiệu về Honeypot.....	24
2.5.1. Khái niệm	24
2.5.2. Chức năng và lợi ích.....	24
2.6. Giới thiệu về DNS	25
2.6.1. Khái niệm	25
2.6.2. Chức năng và lợi ích.....	26
CHƯƠNG III:	28
XÂY DỰNG CHIẾN LUỢC BẢO MẬT	28
3.1. Các thiết bị và phần mềm	28

3.1.1.	Phần cứng	28
3.1.2.	Phần mềm	30
3.2.	Các rủi ro	30
3.3.	Chính sách bảo mật.....	31
3.3.1.	Chính sách bảo mật vật lý	31
3.3.2.	Chính sách bảo mật hệ điều hành	32
3.3.3.	Chính sách bảo mật mạng	32
3.3.4.	Chính sách bảo mật con người	32
3.3.5.	Kế hoạch ứng phó sự cố (Incident Response Plan - IRP)	33
3.3.6.	Kế hoạch khôi phục sau thảm họa (Disaster Recovery Plan-DRP)	33
CHƯƠNG IV:	35
TRIỂN KHAI GIẢI PHÁP	35
4.1.	Triển khai hệ thống bảo mật vật lí	35
4.1.1.	Khóa	35
4.1.2.	Camera.....	35
4.2.	Xây dựng hệ thống mạng.....	44
4.2.1.	Bảng phân hoạch địa chỉ IPv4.....	44
4.2.2.	Sơ đồ logic mạng.....	44
4.3.	Triển khai Group Policy(Chính sách bảo mật).....	45
4.4.	Kiểm soát truy cập	49
4.4.1.	Phân quyền truy cập file	49
4.5.	Triển khai các công nghệ bảo mật	52
4.5.1.	Triển khai Firewall (pfSense).....	52
4.5.2.	Triển khai IDS (Snort).....	54
4.5.3.	Triển khai Honey Pots	55
4.6.	Triển khai Proxy (Squid)	58
4.7.	Sao lưu và phục hồi	61
4.7.1.	Backup bằng bộ nhớ	61
CHƯƠNG V:	64
KẾT LUẬN	64
5.1.	Kết quả triển khai và hướng phát triển	64
5.1.1.	Kết quả đã đạt được	64
5.1.2.	Hướng phát triển trong tương lai.....	65

5.1.3.	Kết luận	66
5.2.	Bảng phân công	66
5.3.	Tài liệu tham khảo	66

DANH MỤC HÌNH VÀ BẢNG

Hình 1. Sơ đồ vật lí.....	13
Hình 2. Mô hình mạng Domain.....	16
Hình 3. Domain Controller và Active Directory	17
Hình 4. Proxy.....	18
Hình 5. Chức năng Proxy	19
Hình 6. Firewall.....	20
Hình 7. IDS và IPS	23
Hình 8. HoneyPot	24
Hình 9. DNS	26
Hình 10. Hệ thống Camera hành lang	36
Hình 11. Camera 1 của hành lang	36
Hình 12. Camera 2 của hành lang	37
Hình 13. Camera 3 của hành lang	37
Hình 14. Camera 4 của hành lang	38
Hình 15. Camera các phòng phía trên	38
Hình 16. Camera phòng Kinh doanh/Bán hàng.....	39
Hình 17. Camera phòng Marketing	39
Hình 18. Camera phòng Nhân sự	40
Hình 19. Camera phòng IT	40
Hình 20. Camera phòng Họp.....	41
Hình 21. Camera các phòng phía dưới	41
Hình 22. Camera phòng Quản lý	42
Hình 23. Camera phòng Kế toán - Tài chính.....	42
Hình 24. Camera phòng Kho vận/Logistics	43
Hình 25. Camera phòng Nhập hàng/Cung ứng	43
Hình 26. Sơ đồ Logic mạng.....	44
Hình 27. Quy định về Password	45
Hình 28. Tắt máy sau 5 phút	45
Hình 29. Tự update	46
Hình 30. Toàn quyền tài nguyên	46
Hình 31. Bảo mật cao	47
Hình 32. Cấm truy cập web	47
Hình 33. Chặn các thiết bị lưu trữ ngoài	48
Hình 34. Cấp quyền cho Admin	48
Hình 35. Tạo Organization Unit.....	49
Hình 36. Tạo User	49
Hình 37. Thêm Group và User	50
Hình 38. Phân quyền xem, xóa và sửa file	50
Hình 39. Thành công share file	51
Hình 40. Map network drive	51
Hình 41. Thông tin của các cổng mạng	52

Hình 42. Gateways trên pfSense	52
Hình 43. Cấu hình rules trên pfSense	53
Hình 44. Danh sách Aliases.....	53
Hình 45. Rule dẫn đến Honeypot	53
Hình 46. Thiết lập chặn kết nối đến Server	54
Hình 47. Rule cho Server kết nối	54
Hình 48. Chặn DMZ kết nối	54
Hình 49. Thông tin của Snort	55
Hình 50. Nmap từ Kali đến Snort.....	55
Hình 51. Snort Bắt gói tin của Kali	55
Hình 52. Thông tin của Honey Pot.....	56
Hình 53. Chạy Honey Pot.....	56
Hình 54. Mở ip đến Honey Pot.....	57
Hình 55. Cấu hình NAT, public ip Honey Pot	57
Hình 56. Cấu hình rules ip honeypot.....	58
Hình 57. Ping tới địa chỉ public Honeypot.....	58
Hình 58. Ping tới ip private của Honeypot	58
Hình 59. Cấu hình Client.....	60
Hình 60. Thủ duyệt web	61
Hình 61. Snort bắt gói tin	61
Hình 62. Chọn vị trí để backup	62
Hình 63. Thiết lập thời gian backup	62
Hình 64. Chọn loại ổ để backup	63
Hình 65. Thiết lập update thành công	63

CHƯƠNG I:

GIỚI THIỆU TỔNG QUAN VỀ DOANH NGHIỆP

1.1. Lĩnh vực kinh doanh

Infinity Sould là doanh nghiệp chuyên kinh doanh nhạc cụ, với sứ mệnh mang đến những sản phẩm chất lượng cao cho cộng đồng yêu âm nhạc. Cung cấp đa dạng các loại nhạc cụ, từ guitar, piano, violin đến các thiết bị âm thanh chuyên nghiệp, phục vụ cho mọi đối tượng từ người mới bắt đầu đến nghệ sĩ chuyên nghiệp.

Với đội ngũ giàu kinh nghiệm và am hiểu về âm nhạc, Infinity Sould không chỉ là nơi mua sắm mà còn là không gian để khách hàng trải nghiệm và khám phá thế giới âm thanh theo cách riêng của mình. Chúng tôi cam kết mang đến dịch vụ tận tâm, chế độ bảo hành uy tín và không ngừng cập nhật những sản phẩm mới nhất để đáp ứng nhu cầu ngày càng cao của thị trường.

1.2. Quy mô tổ chức của doanh nghiệp

Hiện tại, Infinity Sould chỉ có chi nhánh tại Hồ Chí Minh, đang nỗ lực phát triển và mở rộng thêm trong tương lai. Dù là một công ty với quy mô nhỏ, Infinity Sould vẫn có một mô hình tổ chức phòng ban chặt chẽ và đội ngũ nhân viên chuyên nghiệp

Tổ chức phòng ban và nhân viên của Infinity Sould:

- **Phòng Kinh doanh/Bán hàng**
 - Chức năng:
 - Thực hiện nhiệm vụ bán hàng trực tiếp và online
 - Tiếp đón khách hàng, đàm phán bán hàng (bán hàng trực tiếp)
 - Chăm sóc khách hàng (bán hàng trực tiếp và online)
 - Nghiên cứu thị trường, giám sát thị trường
 - Số lượng nhân viên: 4 nhân viên
 - 2 nhân viên bán hàng trực tiếp (gánh thêm một phần công việc bán hàng online).
 - 2 nhân viên bán hàng trực tuyến (kiêm quản lý website & sàn TMĐT).
- **Phòng Marketing**

- Chức năng:
 - Xây dựng chiến lược tiếp thị, quảng bá thương hiệu.
 - Quản lý truyền thông (social media, PR, quảng cáo).
 - Phân tích đối thủ cạnh tranh và nhu cầu khách hàng.
 - Tổ chức sự kiện, chương trình khuyến mãi.
- Số lượng nhân viên: 3 nhân viên
 - 1 nhân viên Marketing tổng hợp (làm chiến lược, nội dung, quảng cáo).
 - 1 nhân viên Digital Marketing (chạy quảng cáo, SEO, tối ưu hóa chiến dịch).
 - 1 nhân viên Thiết kế (hỗ trợ nội dung, làm hình ảnh).
- **Phòng Nhập hàng/Cung ứng**
- Chức năng:
 - Tìm kiếm nhà cung cấp, nguồn cung ứng
 - Đảm bảo số lượng, chất lượng hàng nhập, giá cả
- Số lượng nhân viên: 2 nhân viên
 - 1 nhân viên mua hàng (kiêm luôn điều phối logistics).
 - 1 nhân viên logistics (phụ trách vận chuyển, kho vận).
- **Phòng Kho vận/Logistics**
- Chức năng
 - Quản lý kho hàng (nhập/xuất, kiểm kê).
 - Vận chuyển, phân phối sản phẩm đến khách hàng.
 - Tối ưu hóa quy trình vận hành để giảm chi phí.
- Số lượng nhân viên: 2 nhân viên
 - 1 quản lý kho (kiêm luôn kiểm kê, theo dõi hàng hóa).
 - 1 nhân viên kho (đóng gói, hỗ trợ xuất nhập hàng).
- **Phòng Kế toán - Tài chính**
- Chức năng:
 - Quản lý dòng tiền, báo cáo tài chính, thuế.
 - Kiểm soát chi phí, lập ngân sách.
 - Tính lương, thanh toán với đối tác/nhà cung cấp.
- Số lượng nhân viên: 2 nhân viên

- 1 kế toán tổng hợp (kiêm luôn công nợ, báo cáo tài chính).
 - 1 kế toán viên (quản lý giao dịch, hóa đơn).
- **Phòng Nhân sự**
 - Chức năng:
 - Tuyển dụng, đào tạo và phát triển nhân viên.
 - Xây dựng chính sách lương thưởng, phúc lợi.
 - Giải quyết các vấn đề nội bộ, văn hóa doanh nghiệp.
 - Số lượng nhân viên: 2 nhân viên
 - 1 trưởng phòng nhân sự (kiêm luôn tuyển dụng, đào tạo).
 - 1 nhân viên phúc lợi (quản lý lương, chế độ đãi ngộ).
- **Phòng IT**
 - Chức năng:
 - Điều hành hệ thống mạng, hệ thống Server
 - Bảo trì hệ thống máy tính, phần mềm, mạng.
 - Hỗ trợ kỹ thuật, phát triển website của công ty.
 - Đảm bảo an ninh dữ liệu, chống rủi ro bảo mật.
 - Số lượng nhân viên: 2 nhân viên
 - 1 nhân viên quản trị hệ thống & bảo mật (quản lý server, phần mềm).
 - 1 nhân viên hỗ trợ kỹ thuật & phát triển website (xử lý lỗi kỹ thuật, tối ưu website).
- **Ban lãnh đạo/Quản trị**
 - Chức năng:
 - Hoạch định chiến lược dài hạn của công ty.
 - Ra quyết định quan trọng (đầu tư, mở rộng).
 - Giám sát hoạt động các phòng ban, đánh giá hiệu quả.
 - Số lượng nhân viên: 2 người
 - 1 Giám đốc điều hành (quản lý tổng thể).
 - 1 Quản lý kinh doanh & vận hành (gánh cả hoạt động bán hàng & nội bộ).

Với thời đại công nghệ hóa, mọi công việc đều có sự giúp đỡ của công nghệ nên tất cả phòng ban trên đều sử dụng các thiết bị của hệ thống mạng máy tính, để thực hiện các công việc như: kiểm kê hàng hóa, quản lý nhân sự, giao dịch bán hàng, ...

1.3. Mục đích triển khai hệ thống

Trong quá trình công ty vận hành, công ty sẽ thu thập khá nhiều thông tin từ thông tin khách hàng, thông tin nhân viên, thông tin đối tác,... và sẽ có nhiều thông tin được sinh ra như thông tin hóa đơn, thông tin thuế, thông tin về nhân sự,...

Việc triển khai hệ thống bảo mật cho Infinity Sould nhằm bảo vệ dữ liệu kinh doanh, thông tin nhạy cảm và đảm bảo an toàn cho hệ thống thanh toán trực tuyến. Trong bối cảnh các mối đe dọa an ninh mạng ngày càng tinh vi, một hệ thống bảo mật vững chắc giúp công ty ngăn chặn rủi ro, duy trì uy tín và đảm bảo hoạt động kinh doanh diễn ra an toàn, liên tục.

1.3.1. Các yêu cầu cơ bản về kỹ thuật

Bảo mật hệ thống mạng

- Firewall & IDS/IPS: Cấu hình tường lửa (Firewall) và hệ thống phát hiện/xử lý xâm nhập (IDS/IPS) để giám sát và ngăn chặn truy cập trái phép.
- Phân tách mạng nội bộ: Sử dụng VLAN để tách biệt mạng khách hàng, nhân viên và hệ thống thanh toán.
- Mã hóa dữ liệu truyền tải: Cấu hình HTTPS, TLS 1.2+ cho website và các dịch vụ mạng.

Bảo mật dữ liệu và hệ thống lưu trữ

- Sao lưu dữ liệu định kỳ: Thiết lập backup tự động trên máy chủ an toàn, có khả năng phục hồi nhanh chóng.
- Mã hóa dữ liệu quan trọng: Dữ liệu khách hàng, đơn hàng phải được mã hóa bằng AES-256 hoặc tương đương.
- Quản lý quyền truy cập: Nguyên tắc Least Privilege (chỉ cấp quyền tối thiểu cần thiết).

Bảo mật ứng dụng và website

- Chống tấn công OWASP Top 10: Kiểm tra và phòng chống SQL Injection, XSS, CSRF, SSRF...
- Xác thực mạnh (MFA): Bật xác thực hai yếu tố (2FA) cho tài khoản quản trị.
- Cập nhật và vá lỗi: Luôn cập nhật các bản vá bảo mật mới nhất cho phần mềm và hệ điều hành.

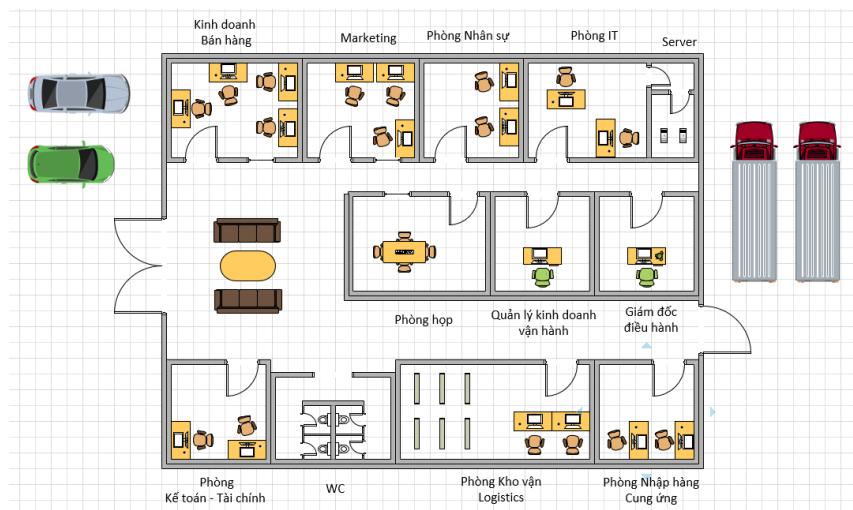
Giám sát và phản ứng sự cố

- Hệ thống giám sát: Cấu hình SIEM (Security Information and Event Management) để theo dõi log hệ thống.
- Kế hoạch phản ứng sự cố: Xây dựng quy trình xử lý khi phát hiện sự cố an ninh mạng.
- Diễn tập an ninh: Tổ chức kiểm tra, diễn tập ứng phó tấn công mạng định kỳ.

Nâng cao nhận thức bảo mật

- Đào tạo nhân viên: Hướng dẫn về phishing, lừa đảo trực tuyến và các rủi ro an ninh.
- Chính sách bảo mật: Thiết lập chính sách sử dụng mật khẩu mạnh, không chia sẻ tài khoản...
- Hệ thống bảo mật này sẽ giúp Infinity Sould đảm bảo an toàn thông tin và hoạt động ổn định trước các mối đe dọa mạng.

1.3.2. Sơ đồ vật lý cụ thể



Hình 1. Sơ đồ vật lý

Sơ đồ vật lý của công ty được xây dựng với cấu trúc chặt chẽ, đầy tính logic và mỹ quan, cho thấy sự chuyên nghiệp trong bố trí phòng ban:

- Lối vào chính dẫn vào sẽ một sảnh có chỗ tiếp khách và ngay phòng Kinh doanh/ Bán hàng, Marketing, Kế toán
 - Khách hàng dễ được tiếp đón và trao đổi tức thì
 - Thao tác mua bán hàng được thực hiện dễ dàng
- Phía trên sơ đồ là các phòng ban chính:
 - Nhân sự, IT, Quản lý và Giám đốc được đặt nơi khuất, riêng tư
 - Server được đặt trong một phòng riêng biệt, đảm bảo bảo mật.
- Phía dưới sơ đồ là các phòng làm nhiệm vụ nhập xuất hàng hóa
 - Kho vận/Logistics và Nhập hàng/Cung ứng được đặt ngay cửa lớn thuận tiện việc di chuyển hàng hóa
 - Phía ngoài là khu bãi xe của công ty

Bố trí này giúp phân chia không gian làm việc hợp lý, tối ưu luồng di chuyển và quản lý nhân sự.

CHƯƠNG II:

LÝ THUYẾT TỔNG QUAN

2.1. Giới thiệu về Domain

2.1.1. Khái niệm

Mạng Domain là một hệ thống quản lý tập trung các tài nguyên mạng trong doanh nghiệp, bao gồm tài khoản người dùng, máy tính, và các thiết bị khác, thông qua các máy chủ Domain Controller (thường dựa trên Active Directory của Microsoft).

Hệ thống này giúp quản trị viên dễ dàng áp dụng chính sách bảo mật, kiểm soát truy cập, và quản lý cấu hình cho toàn bộ các thiết bị trong mạng công ty, từ đó nâng cao tính bảo mật và hiệu quả quản trị hệ thống.

Mạng Domain là một môi trường quản trị tập trung, trong đó các tài nguyên mạng như tài khoản người dùng, máy tính, ứng dụng và dữ liệu được quản lý qua một hoặc nhiều máy chủ Domain Controller (thường sử dụng Active Directory của Microsoft).

2.1.2. Tính năng và lợi ích

Các tính năng và lợi ích của mạng Domain:

- Quản trị tập trung: Cho phép quản lý và kiểm soát người dùng, nhóm, máy chủ liên quan và chính sách bảo mật tại một điểm duy nhất giúp giảm thời gian và công sức để quản trị.
- Chính sách nhóm (Group Policy): Áp dụng các chính sách bảo mật và cấu hình máy tính cho toàn bộ hệ thống một cách nhanh chóng nhưng vẫn đảm bảo tính nhất quán và dễ kiểm soát trong hệ thống mạng.
- Xác thực và phân quyền: Cung cấp hệ thống *Single Sign-On (SSO)* giúp người dùng chỉ cần đăng nhập một lần để truy cập tất cả tài nguyên được cấp quyền trên hệ thống và đồng thời kiểm soát truy cập một cách chặt chẽ.
- Mở rộng và tin cậy: Hỗ trợ quản lý quy mô lớn và có thể thiết lập các mối quan hệ tin cậy (*Trust Relationships*) giữa các domain giúp tạo điều kiện cho giao tiếp an toàn giữa các bộ phận và chi nhánh.

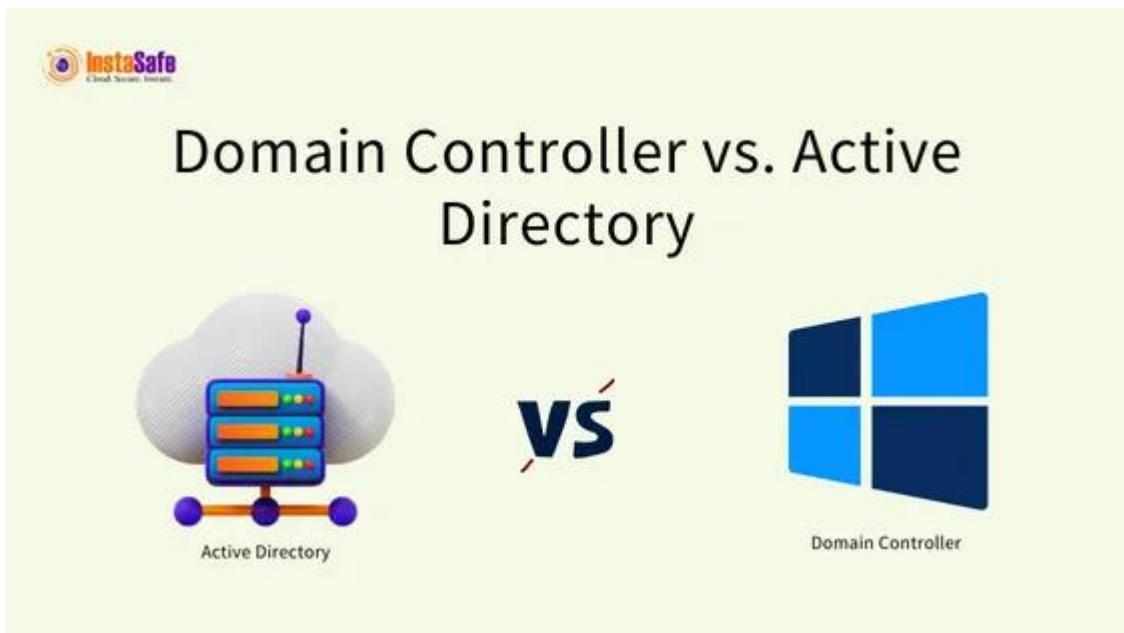
- Giám sát và báo cáo: Cho phép ghi nhận và theo dõi các hoạt động đăng nhập, thay đổi cấu hình và truy cập tài nguyên lẫn các công cụ hỗ trợ công tác giám sát và phản ứng sự cố.



Hình 2. Mô hình mạng Domain

Dịch vụ Active Directory (AD):

- Active Directory là một dịch vụ của Microsoft dùng để quản lý thông tin người dùng và tài nguyên trên cùng một mạng, cho phép quản trị viên quản lý tài khoản người dùng, nhóm và các chính sách bảo mật một cách tập trung trong cùng 1 hệ thống.
- Active Directory Domain Services (AD DS) là thành phần chính của AD, cung cấp chức năng quản lý và xác thực các tài nguyên của mạng như người dùng, máy tính và các dịch vụ khác.



Hình 3. Domain Controller và Active Directory

➤ **Các khái niệm chính thường dùng trong AD:**

- *Forest (rừng):* Là tập hợp của một hoặc nhiều domain có cùng cấu trúc AD, với một cấu trúc bảo mật và schema duy nhất.
- *Tree (cấu trúc cây):* Là tập hợp các domain liên quan với nhau theo một phân cấp, với các tên miền con được mở rộng từ domain gốc.
- *OU (Organizational Unit):* Là đơn vị tổ chức, giúp chia nhỏ các đối tượng trong AD thành các nhóm nhỏ hơn để dễ quản lý.

Lợi ích của AD và Domain:

- *Quản lý tập trung:* Cho phép quản lý người dùng, nhóm và thiết bị một cách tập trung, giúp dễ dàng thực thi các chính sách bảo mật, chia sẻ tài nguyên và thiết lập các quyền truy cập trong domain.
- *Bảo mật:* AD cung cấp khả năng xác thực và ủy quyền người dùng, đảm bảo rằng chỉ những người dùng được phép mới có thể truy cập vào các tài nguyên trong domain.
- *Scalability (mở rộng):* AD có thể mở rộng để phù hợp với mọi quy mô của doanh nghiệp, từ các tổ chức nhỏ cho đến các tập đoàn lớn với nhiều chi nhánh khác nhau.

Không những thế trong thực tế, AD và mô hình miền(Domain) đóng vai trò rất quan trọng trong việc duy trì và quản lý mạng doanh nghiệp, từ việc đảm bảo bảo mật cho tới việc tạo điều kiện thuận lợi cho quản trị hệ thống cho doanh nghiệp dễ dàng quản lý và phân chia tài nguyên.

2.2. Giới thiệu về Proxy



Hình 4. Proxy

2.2.1. Khái niệm

Trong mạng máy tính, máy chủ proxy là một ứng dụng máy chủ đóng vai trò trung gian giữa máy khách yêu cầu tài nguyên và máy chủ cung cấp tài nguyên đó.

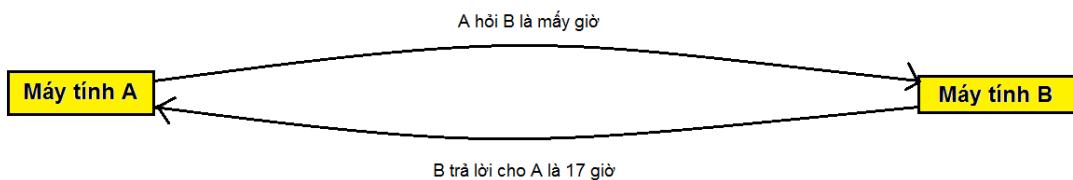
Thay vì kết nối trực tiếp với máy chủ có thể đáp ứng yêu cầu tài nguyên, chẳng hạn như tệp hoặc trang web, máy khách chuyển yêu cầu đến máy chủ proxy, máy chủ sẽ đánh giá yêu cầu và thực hiện các yêu cầu. Đây là một phương pháp để đơn giản hóa hoặc kiểm soát mức độ phức tạp của yêu cầu hoặc cung cấp các lợi ích bổ sung như quyền riêng tư hoặc bảo mật. Các proxy được tạo ra để thêm cấu trúc và đóng gói vào các hệ thống phân tán. Do đó, máy chủ proxy hoạt động thay mặt cho máy khách khi yêu cầu dịch vụ, có khả năng che dấu nguồn gốc thực sự của yêu cầu đối với máy chủ tài nguyên.

2.2.2. Tính năng và lợi ích

Kết nối qua Proxy



Kết nối trực tiếp



Hình 5. Chức năng Proxy

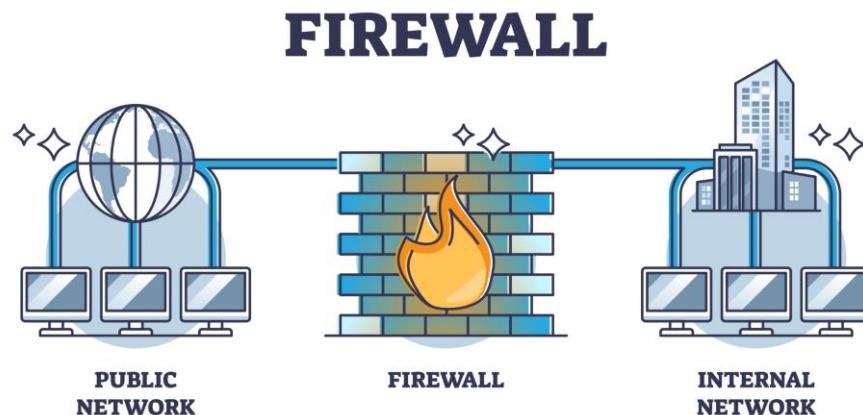
Tính năng của Proxy

- Ân địa chỉ IP: Proxy giúp che giấu địa chỉ IP thật của người dùng, bảo vệ danh tính khi truy cập internet.
- Tường lửa và lọc nội dung: Proxy có thể kiểm soát truy cập web, chặn các trang web độc hại hoặc không phù hợp.
- Tăng tốc độ duyệt web (Caching): Proxy lưu trữ dữ liệu web được truy cập thường xuyên, giúp giảm tải băng thông và tăng tốc độ tải trang.
- Chia sẻ kết nối Internet: Trong mạng doanh nghiệp, proxy giúp nhiều máy tính dùng chung một kết nối internet hiệu quả hơn.
- Hỗ trợ kiểm soát và giám sát: Quản trị viên có thể theo dõi lưu lượng mạng, lọc nội dung và áp dụng chính sách bảo mật.
- Bypass chặn nội dung (VPN & Proxy Anonymizer): Proxy có thể giúp truy cập các trang web bị chặn theo khu vực địa lý (Geo-blocking).
- Bảo mật dữ liệu: Một số proxy mã hóa dữ liệu để ngăn chặn nghe lén và tấn công mạng.

Lợi ích của Proxy

- Bảo vệ quyền riêng tư:Ẩn danh tính khi truy cập internet, giảm nguy cơ theo dõi và đánh cắp thông tin.
- Tăng hiệu suất mạng: Caching giúp giảm tải băng thông, cải thiện tốc độ truy cập trang web.
- Kiểm soát truy cập trong doanh nghiệp: Giúp quản lý nhân viên sử dụng internet hiệu quả hơn, ngăn chặn truy cập vào nội dung không mong muốn.
- Tăng cường bảo mật: Chặn các trang web độc hại, ngăn chặn tấn công mạng như phishing, malware.
- Hỗ trợ vượt tường lửa: Giúp truy cập nội dung bị giới hạn tại một số quốc gia hoặc tổ chức.
- Cân bằng tải và tối ưu hóa hệ thống: Proxy có thể phân phối yêu cầu truy cập giữa nhiều máy chủ, cải thiện hiệu suất và giảm tải cho hệ thống.

2.3. Giới thiệu về Firewall



Hình 6. Firewall

2.3.1. Khái niệm

Trong điện toán, tường lửa hay Firewall là một hệ thống bảo mật mạng giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật được xác định trước. Một tường lửa thường thiết lập một rào cản giữa một mạng nội bộ đáng tin cậy và mạng bên ngoài không tin cậy, chẳng hạn như Internet.

Tường lửa (Firewall) thường được phân loại thành: Tường lửa mạng” hay “tường lửa dựa” trên máy chủ. Tường lửa mạng lọc lưu lượng giữa hai hoặc nhiều mạng và chạy trên phần cứng mạng. Tường lửa dựa trên máy chủ chạy trên máy tính chủ và kiểm soát lưu lượng mạng vào và ra khỏi các máy đó. Chúng cũng được phân loại thành tường lửa bảo vệ để bảo vệ an ninh cho máy tính cá nhân hay mạng cục bộ, tránh sự xâm nhập, tấn công từ bên ngoài và tường lửa ngăn chặn thường do các nhà cung cấp dịch vụ Internet thiết lập và có nhiệm vụ ngăn chặn không cho máy tính truy cập một số trang web hay máy chủ nhất định, thường dùng với mục đích kiểm duyệt Internet.

2.3.2. Chức năng và lợi ích

Chức năng của Tường lửa

- Kiểm soát lưu lượng mạng: Lọc và phân loại lưu lượng mạng dựa trên quy tắc do quản trị viên thiết lập, chỉ cho phép các kết nối hợp lệ và chặn những truy cập trái phép.
- Bảo vệ trước các cuộc tấn công mạng: Ngăn chặn các cuộc tấn công DDoS, brute force, scanning port, và các cuộc tấn công xâm nhập khác.
- Chặn truy cập trái phép: Ngăn chặn hacker, phần mềm độc hại hoặc người dùng không có quyền truy cập vào hệ thống.
- Lọc nội dung và kiểm soát truy cập: Chặn các trang web độc hại, nội dung không phù hợp hoặc hạn chế quyền truy cập internet của nhân viên.
- Phát hiện và ngăn chặn xâm nhập (IDS/IPS): Một số tường lửa hiện đại tích hợp hệ thống phát hiện (IDS) và ngăn chặn xâm nhập (IPS) để phản ứng với các mối đe dọa theo thời gian thực.
- Ghi nhật ký và giám sát lưu lượng mạng: Theo dõi hoạt động mạng, cung cấp dữ liệu phục vụ phân tích và điều tra sự cố bảo mật.
- Hỗ trợ VPN và bảo mật từ xa: Một số tường lửa hỗ trợ kết nối VPN, giúp bảo mật dữ liệu khi truy cập từ xa.

Lợi ích của Tường lửa

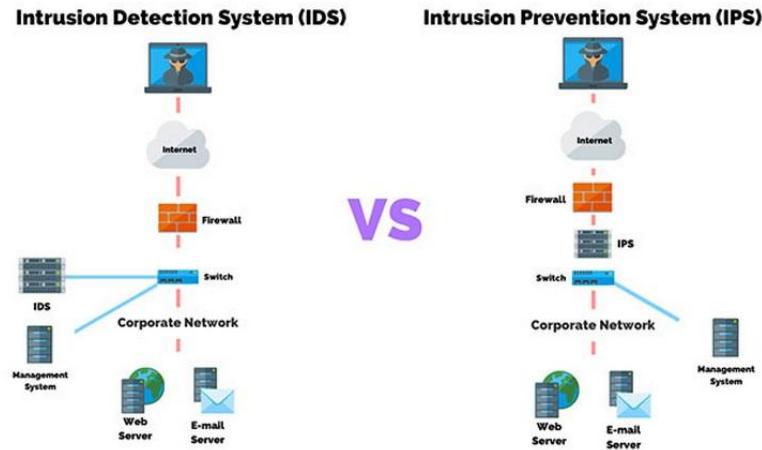
- Tăng cường bảo mật hệ thống: Ngăn chặn các mối đe dọa từ internet, bảo vệ dữ liệu quan trọng khỏi hacker và malware.
- Bảo vệ dữ liệu doanh nghiệp: Đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào tài nguyên quan trọng.
- Ngăn chặn truy cập trái phép: Chặn các kết nối không mong muốn từ bên ngoài vào hệ thống nội bộ.
- Cải thiện hiệu suất mạng: Giảm tải cho hệ thống bằng cách lọc bớt lưu lượng không cần thiết và chặn các cuộc tấn công DDoS.
- Hỗ trợ tuân thủ các tiêu chuẩn bảo mật: Các tổ chức cần firewall để đáp ứng các yêu cầu bảo mật như ISO 27001, PCI DSS, HIPAA, v.v.
- Quản lý và giám sát tốt hơn: Cung cấp nhật ký hoạt động để phân tích và tối ưu hóa chính sách bảo mật.

2.4. Giới thiệu về IDS/IPS

2.4.1. Khái niệm

IDS: là hệ thống phát hiện xâm nhập, có chức năng giám sát và phát hiện các hoạt động xâm nhập hoặc bất thường trong hệ thống mạng. IDS chỉ cung cấp cảnh báo và thông báo về các hoạt động xâm nhập, không có khả năng ngăn chặn hoặc phản ứng lại các cuộc tấn công. IDS có thể triển khai dưới dạng Network IDS (NIDS) hoặc Host IDS (HIDS).

IPS: IPS là hệ thống phòng ngừa xâm nhập, có chức năng giám sát và ngăn chặn các hoạt động xâm nhập hoặc bất thường trong hệ thống mạng. IPS không chỉ cung cấp cảnh báo mà còn có khả năng ngăn chặn và phản ứng lại các cuộc tấn công bằng cách ngăn chặn luồng dữ liệu xâm nhập. IPS có thể triển khai dưới dạng Network IPS (NIPS) hoặc Host IPS (HIPS).



Hình 7. IDS và IPS

Kết hợp cả hai ta sẽ được một hệ thống phát hiện và ngăn chặn xâm nhập, giúp bảo vệ mạng khỏi các mối đe dọa tiềm ẩn

2.4.2. Chức năng và lợi ích

Chức năng của IDS/IPS

- IDS (Intrusion Detection System) – Hệ thống phát hiện xâm nhập
 - IDS có nhiệm vụ giám sát mạng và hệ thống, phát hiện các hành vi bất thường hoặc tấn công, nhưng không can thiệp trực tiếp.
 - Phân tích lưu lượng mạng để phát hiện dấu hiệu xâm nhập.
 - Cảnh báo quản trị viên khi có hoạt động đáng ngờ.
 - Ghi lại log sự kiện để điều tra sau này.
- IPS (Intrusion Prevention System) – Hệ thống ngăn chặn xâm nhập
 - IPS không chỉ phát hiện mà còn chủ động ngăn chặn các mối đe dọa ngay lập tức.
 - Chặn lưu lượng độc hại theo thời gian thực.
 - Tự động phản hồi các tấn công như DDoS, brute force, malware.
 - Áp dụng chính sách bảo mật để giảm thiểu rủi ro.

Lợi ích của IDS/IPS

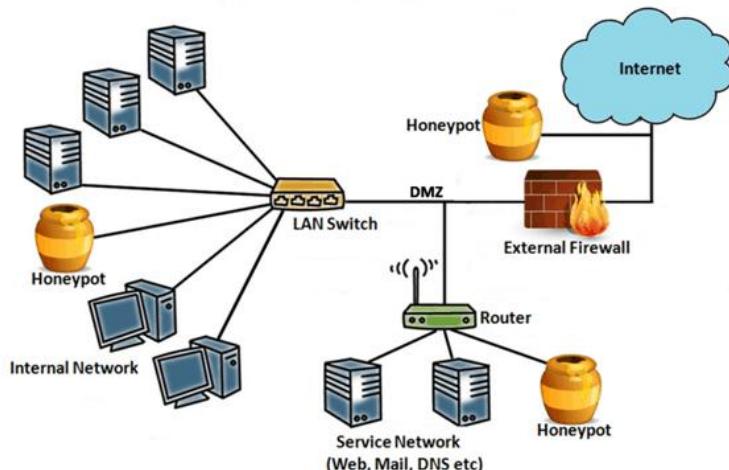
- Bảo vệ hệ thống khỏi tấn công mạng: Giúp phát hiện và ngăn chặn các cuộc tấn công trước khi gây hậu quả.

- Giám sát an ninh liên tục: Theo dõi mạng 24/7, giúp phát hiện nhanh các hành vi bất thường.
- Giảm thiểu rủi ro bảo mật: IPS có thể tự động phản ứng ngay lập tức, giảm nguy cơ bị tấn công.
- Cung cấp dữ liệu điều tra: IDS ghi lại log chi tiết về các sự kiện an ninh, hỗ trợ phân tích và điều tra sự cố.
- Tăng cường tuân thủ bảo mật: Giúp doanh nghiệp đáp ứng các tiêu chuẩn bảo mật như PCI-DSS, ISO 27001.

2.5. Giới thiệu về Honeypot

2.5.1. Khái niệm

Honeypot là một phần mềm hoặc thiết lập điều khiển có mục tiêu để thu hút các hành vi không mong muốn như tấn công mạng, thâm nhập trái phép hoặc lừa đảo. Honeypot thường được sử dụng để giám sát và thu thập thông tin về các kỹ thuật tấn công, nhận diện các mối đe dọa tiềm ẩn và bảo vệ các hệ thống mạng khỏi các mối đe dọa này.



Hình 8. HoneyPot

2.5.2. Chức năng và lợi ích

Chức năng của Honeypot

- Phát hiện và ghi nhận cuộc tấn công: Honeypot được thiết kế để trông giống như một máy chủ thật hoặc một hệ thống mạng dễ bị tấn công, khi tin tặc có gắng khai thác, hệ thống sẽ ghi lại toàn bộ hoạt động của chúng.
- Phân tích kỹ thuật tấn công: Giúp các chuyên gia bảo mật hiểu rõ phương thức, công cụ mà hacker sử dụng, cung cấp dữ liệu để cải thiện hệ thống phòng thủ thực sự.
- Ngăn chặn và đánh lạc hướng kẻ tấn công: Tin tặc tốn thời gian tấn công vào Honeypot thay vì hệ thống chính, cho phép quản trị viên có thêm thời gian để phản ứng và xử lý sự cố.
- Hỗ trợ phát triển và thử nghiệm giải pháp bảo mật: Có thể dùng để kiểm tra mức độ hiệu quả của IDS/IPS hoặc các hệ thống bảo mật khác, hỗ trợ nghiên cứu các loại phần mềm độc hại (malware) mới.

Lợi ích của Honeypot

- Cải thiện khả năng phát hiện mối đe dọa: Không gây nhiều cảnh báo giả (false positives) như IDS/IPS, phát hiện ngay khi có truy cập trái phép.
- Giảm thiểu rủi ro bảo mật thực tế: Tin tặc bị thu hút vào Honeypot, giúp hệ thống chính ít bị nhắm đến hơn, có thể làm chậm tiến trình tấn công và giúp quản trị viên phản ứng kịp thời.
- Cung cấp dữ liệu có giá trị về hacker: Ghi lại kỹ thuật tấn công để phát triển các biện pháp phòng thủ hiệu quả hơn, phát hiện các loại phần mềm độc hại mới trước khi chúng lan rộng.
- Chi phí thấp nhưng hiệu quả cao: Không cần tài nguyên lớn như hệ thống bảo mật phức tạp, dễ triển khai trên máy chủ ảo hoặc container.

2.6. Giới thiệu về DNS

2.6.1. Khái niệm

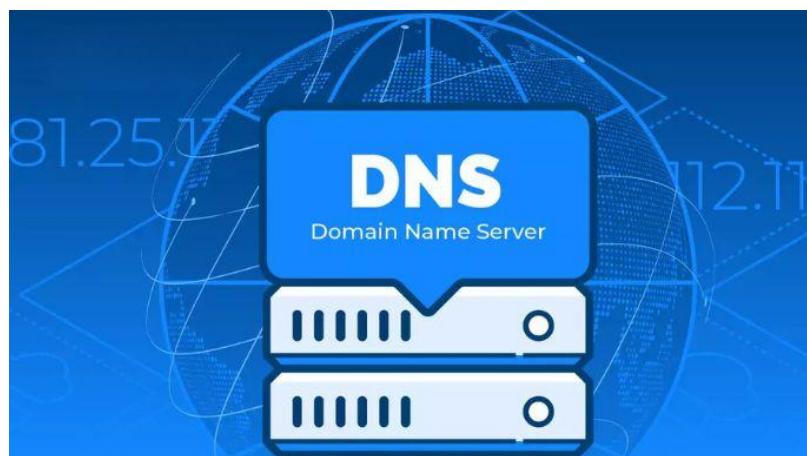
DNS (Domain Name System) là hệ thống phân giải tên miền cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Khi người dùng nhập địa chỉ trang web trên trình duyệt, DNS sẽ tìm địa chỉ IP của máy chủ chứa trang web và trả về kết quả hiển thị tương ứng của trang web cần tìm.

Do đó, thay vì phải ghi nhớ địa chỉ IP phức tạp, người dùng có thể dễ dàng truy cập các trang web thông qua tên miền. Ngoài ra, DNS cũng giúp tăng tính linh hoạt và quản lý hiệu quả hơn cho hệ thống mạng, cung cấp tính bảo mật và tăng tốc độ truy cập internet.

2.6.2. Chức năng và lợi ích

Chức năng của DNS

- Chuyển đổi tên miền thành địa chỉ IP: Giúp người dùng nhập tên miền dễ nhớ thay vì các chuỗi số IP phức tạp.
- Hỗ trợ phân tán và tối ưu hóa hệ thống mạng
 - DNS Caching: Lưu trữ tạm thời các bản ghi DNS để tăng tốc độ truy cập.
 - Load Balancing: Phân phối lưu lượng truy cập giữa nhiều máy chủ khác nhau.
- Tăng cường bảo mật và chống tấn công mạng: DNSSEC (DNS Security Extensions) giúp bảo vệ chống giả mạo DNS, chặn truy cập vào các trang web độc hại bằng DNS filtering.
- Quản lý và phân giải nhiều loại bản ghi khác nhau
 - A Record: Chuyển tên miền → Địa chỉ IPv4.
 - AAAA Record: Chuyển tên miền → Địa chỉ IPv6.
 - CNAME Record: Chuyển hướng tên miền sang tên miền khác.
 - MX Record: Xác định máy chủ email.



Hình 9. DNS

Lợi ích của DNS

- Giúp truy cập internet dễ dàng hơn: Người dùng chỉ cần nhớ tên miền thay vì IP phức tạp.
- Tăng tốc độ truy cập website: Hệ thống DNS Cache giảm thời gian phân giải tên miền, giúp tải trang nhanh hơn.
- Hỗ trợ khả năng mở rộng của website: Load balancing giúp phân phối tải giữa nhiều máy chủ, tránh tình trạng quá tải.
- Tăng cường bảo mật
 - DNS Filtering có thể chặn các trang web độc hại hoặc nội dung không mong muốn.
 - DNSSEC giúp ngăn chặn các cuộc tấn công giả mạo DNS.
- Hỗ trợ dịch vụ email và nhiều ứng dụng khác
 - MX Record giúp định tuyến email đúng cách.
 - SRV Record hỗ trợ VoIP, Microsoft Teams, v.v.

CHƯƠNG III:

XÂY DỰNG CHIẾN LƯỢC BẢO MẬT

3.1. Các thiết bị và phần mềm

3.1.1. Phần cứng

- **Router: Cisco ISR 1100 Series (ISR 1111-4P)**
 - Mô tả: Cisco ISR 1100 Series là dòng router hiệu quả cho các doanh nghiệp nhỏ và vừa. Nó hỗ trợ nhiều tính năng như định tuyến, tường lửa, VPN, QoS và phù hợp cho các doanh nghiệp cần triển khai dịch vụ mail.
 - Lợi ích: Dòng ISR này cung cấp khả năng mở rộng tốt và dễ dàng cấu hình để tích hợp vào hệ thống mạng doanh nghiệp.
- **Switch lớp 2: Cisco Catalyst 2960L-24TS-LL**
 - Mô tả: Đây là dòng switch lớp 2 đáng tin cậy, phù hợp cho việc kết nối các thiết bị đầu cuối như máy tính và điện thoại IP.
 - Lợi ích: Catalyst 2960L hỗ trợ các tính năng cơ bản của switch lớp 2, như VLAN và quản lý băng thông, phù hợp cho việc triển khai hệ thống trong mạng doanh nghiệp.
- **Switch lớp 3: Cisco Catalyst 3560CX-12PC-S**
 - Mô tả: Dòng switch này hỗ trợ định tuyến tĩnh và các tính năng lớp 3, thích hợp cho việc quản lý lưu lượng mạng nội bộ và giữa các VLAN.
 - Lợi ích: Hỗ trợ các tính năng định tuyến lớp 3, cho phép doanh nghiệp định tuyến các VLAN và tối ưu hóa hiệu suất mạng.
- **Router WiFi: Cisco Business 145AC Access Point**
 - Mô tả: Đây là bộ phát WiFi dễ triển khai, hỗ trợ chuẩn 802.11ac Wave 2, phù hợp với yêu cầu kết nối WiFi cho văn phòng doanh nghiệp.
 - Lợi ích: Cung cấp khả năng kết nối WiFi ổn định, dễ quản lý và phù hợp cho khu vực văn phòng, đảm bảo người dùng có thể truy cập dịch vụ email và tài nguyên mạng qua WiFi.

- **Máy client: HP ProDesk 400 G7**
- Máy client sẽ được sử dụng cho nhân viên của các phòng ban như Kinh doanh, Kỹ thuật, Hỗ trợ Kỹ thuật, Nhân sự, và Hành chính. Máy tính cho client cần đảm bảo hiệu suất đủ mạnh để sử dụng các ứng dụng văn phòng, bảo mật và duyệt web một cách hiệu quả.
 - CPU: Intel Core i5 hoặc i7 thế hệ mới (từ thế hệ thứ 10 trở lên).
 - RAM: 16GB .
 - Ổ cứng: SSD 1TB (để tăng tốc độ khởi động và xử lý công việc).
 - Hệ điều hành: Windows 11 Home .
 - Màn hình: 21 inch trở lên, độ phân giải Full HD.

Phần cứng cho các máy Server

Vì là một công ty nhỏ nên chỉ cần 2 server để đảm bảo đáp ứng nhu cầu của hệ thống, mỗi server sẽ đảm nhiệm các vai trò khác nhau, bao gồm Domain Controller kiêm DNS Server, Mail Server, và Web Server.

- **Domain Controller kiêm DNS Server: HP ProLiant DL360 Gen10**
 - CPU: Intel Xeon Silver (2 CPUs, tối thiểu 6 lõi mỗi CPU).
 - RAM: 128GB (đảm bảo hiệu suất tốt cho dịch vụ AD và DNS).
 - Ổ cứng: SSD 480GB + HDD 1TB (SSD để chạy hệ điều hành và ứng dụng, HDD để lưu trữ dữ liệu).
 - RAID: RAID 1 (để đảm bảo an toàn dữ liệu).
 - Hệ điều hành: Windows Server 2019/2022.
- **Mail Server kiêm Web Server: HP ProLiant DL380 Gen10**
 - CPU: Intel Xeon Silver (2 CPUs, tối thiểu 8 lõi mỗi CPU).
 - RAM: 64GB (để đáp ứng yêu cầu của dịch vụ mail, hỗ trợ lượng người dùng lớn).
 - Ổ cứng: SSD 480GB + HDD 2TB (SSD để hệ điều hành và ứng dụng, HDD để lưu trữ dữ liệu mail).
 - RAID: RAID 1 hoặc RAID 5 (để cân bằng giữa bảo mật và dung lượng lưu trữ).

- Hệ điều hành: Windows Server 2019/2022.
- **Máy in (Printer)**
 - Máy in đa chức năng (MFP): HP LaserJet Pro MFP M428fdw
 - Chức năng: In, sao chép, quét và fax (nếu cần).
 - Loại in: In laser màu để đảm bảo chất lượng in tốt và chi phí cho mỗi trang in thấp.
 - Kết nối: USB, Ethernet và Wi-Fi.
- **Access Point (AP)**
 - Model: Cisco Aironet 2800 Series
 - Chức năng: Cung cấp kết nối Wi-Fi cho nhân viên trong văn phòng, đảm bảo mạng không dây ổn định và an toàn.

3.1.2. Phần mềm

- **Microsoft Office 365 Business**
 - Hãng: Microsoft
 - Tính năng nổi bật: Làm việc linh hoạt, Cộng tác hiệu quả, Bảo mật mạnh mẽ, Tiết kiệm chi phí, Tích hợp công cụ, Hỗ trợ 24/7

3.2. Các rủi ro

- Tấn công mạng & Ransomware
- Nguy cơ: Hacker tấn công hệ thống, mã hóa dữ liệu (đơn hàng, thông tin KH) và đòi tiền chuộc.
- Lừa đảo qua Email (Phishing)
 - Nguy cơ: Nhân viên nhấp vào link giả mạo, tiết lộ thông tin đăng nhập hoặc chuyển tiền sai.
- Rò rỉ thông tin khách hàng
 - Nguy cơ: Lộ thông tin cá nhân (tên, SDT, địa chỉ) do hệ thống bị hack hoặc nhân viên thiếu ý thức.
- Gian lận thanh toán
 - Nguy cơ: Khách hàng dùng thẻ tín dụng giả, hoặc hacker chiếm quyền giao dịch.

- Lỗi từ nhân viên (Vô ý hoặc cố ý)
- Nguy cơ: Xóa nhầm dữ liệu, chia sẻ mật khẩu, hoặc nhân viên cũ phá hoại.
- Tân công vào Website bán hàng
- Nguy cơ: Website bị SQL Injection, DDoS làm chậm/đánh cắp dữ liệu.

3.3. Chính sách bảo mật

Chính sách bảo mật được xây dựng dựa trên 5 nguyên tắc của NIST CSF và yêu cầu của Nghị định 53/2023/NĐ-CP:

Bảng 1. Bảng nguyên tắc

Nguyên tắc	Yêu cầu từ NĐ-CP 53/2023	Áp dụng từ NIST
Nhận diện (Identify)	Xác định hệ thống thông tin quan trọng, bảo vệ dữ liệu người dùng tại Việt Nam.	Xây dựng danh sách tài sản quan trọng, đánh giá rủi ro an ninh.
Bảo vệ (Protect)	Kiểm soát truy cập dữ liệu, yêu cầu xác thực mạnh (2FA).	Mã hóa dữ liệu (AES-256, TLS), bảo mật thiết bị đầu cuối.
Phát hiện (Detect)	Hệ thống giám sát an ninh mạng, báo cáo sự cố lên Bộ Công an.	IDS/IPS, SIEM để phát hiện tấn công trong thời gian thực.
Phản ứng (Respond)	Quy trình xử lý sự cố, hợp tác với cơ quan chức năng khi cần.	Kế hoạch ứng phó sự cố, diễn tập an ninh mạng định kỳ.
Khôi phục (Recover)	Sao lưu dữ liệu tại Việt Nam, đảm bảo khôi phục nhanh sau sự cố.	Kế hoạch khôi phục sau thảm họa (BCP/DRP), kiểm tra định kỳ.

3.3.1. Chính sách bảo mật vật lý

Theo NĐ-CP 53/2023:

- Kiểm soát truy cập vào phòng máy chủ, chỉ nhân viên được ủy quyền mới có quyền vào.
- Camera giám sát và hệ thống báo động tại các khu vực quan trọng.

Theo NIST:

- Sử dụng hệ thống kiểm soát truy cập RFID, vân tay cho các phòng quan trọng.
- Kết hợp UPS/máy phát điện để bảo vệ thiết bị khỏi gián đoạn do mất điện.

3.3.2. Chính sách bảo mật hệ điều hành

Theo NĐ-CP 53/2023:

- Cập nhật hệ điều hành, phần mềm bảo mật thường xuyên để tránh lỗ hổng bảo mật.
- Hạn chế cài đặt phần mềm không rõ nguồn gốc.

Theo NIST:

- Áp dụng nguyên tắc Least Privilege Access (Chỉ cấp quyền tối thiểu cần thiết).
- Sử dụng phần mềm diệt virus có tính năng EDR (Endpoint Detection & Response).

3.3.3. Chính sách bảo mật mạng

Theo NĐ-CP 53/2023:

- Xây dựng hệ thống bảo vệ dữ liệu tường lửa, VPN, IDS/IPS.
- Mạng nội bộ doanh nghiệp phải có biện pháp phòng chống tấn công mạng.

Theo NIST:

- Triển khai Zero Trust Architecture (Mô hình Không tin tưởng mặc định).
- Sử dụng mã hóa dữ liệu đầu cuối khi truyền qua Internet (TLS 1.2+).
- Phân tách VLAN: mạng nhân viên, mạng khách hàng, mạng thanh toán.

3.3.4. Chính sách bảo mật con người

Theo NĐ-CP 53/2023:

- Đào tạo nhân viên về quy định bảo mật dữ liệu.

- Nhân viên phải ký cam kết bảo mật khi làm việc.

Theo NIST:

- Huấn luyện nhân viên nhận biết các cuộc tấn công phishing, social engineering.
- Xác thực 2 yếu tố (2FA) cho tất cả tài khoản quan trọng.
- Chính sách offboarding: Thu hồi quyền truy cập khi nhân viên nghỉ việc.

3.3.5. Kế hoạch ứng phó sự cố (Incident Response Plan - IRP)

Theo NĐ-CP 53/2023:

- Khi xảy ra sự cố an ninh mạng, doanh nghiệp phải báo cáo Bộ Công an trong vòng 24 giờ.
- Cố lập hệ thống bị tấn công để giảm thiểu thiệt hại.

Theo NIST:

- Xây dựng kịch bản ứng phó sự cố theo 4 giai đoạn: Phát hiện → Phản ứng → Đối phó → Hồi phục.
- Diễn tập phản ứng với tấn công mạng ít nhất 6 tháng/lần.
- Triển khai SIEM (Security Information and Event Management) để giám sát sự cố theo thời gian thực.

3.3.6. Kế hoạch khôi phục sau thảm họa (Disaster Recovery Plan-DRP)

Theo NĐ-CP 53/2023:

- Doanh nghiệp phải có kế hoạch khôi phục dữ liệu khi xảy ra mất mát thông tin hoặc tấn công mạng.
- Sao lưu dữ liệu định kỳ và lưu trữ bản sao tại máy chủ đặt tại Việt Nam.

Theo NIST:

- Áp dụng quy tắc sao lưu 3-2-1:
 - 3 bản sao dữ liệu.
 - 2 loại thiết bị lưu trữ khác nhau.
 - 1 bản lưu trữ ở vị trí tách biệt.

- Thử nghiệm phục hồi dữ liệu hàng tháng để đảm bảo khả năng khôi phục nhanh chóng.
- Có phương án Cloud Backup để duy trì hoạt động khi hệ thống chính gặp sự cố.
 - Sự kết hợp giữa Nghị định 53/2023/NĐ-CP của Việt Nam và khung NIST giúp doanh nghiệp xây dựng hệ thống bảo mật toàn diện, vừa đáp ứng yêu cầu pháp lý trong nước vừa tuân thủ thông lệ quốc tế tốt nhất trong bảo vệ hệ thống mạng và dữ liệu

CHƯƠNG IV:

TRIỂN KHAI GIẢI PHÁP

4.1. Triển khai hệ thống bảo mật vật lí

Dựa trên sơ đồ vật lí có thể thấy, về vị trí địa lí các phòng cơ bản đặt đủ tiêu chuẩn an toàn, nhưng cần nâng cấp thêm các biện pháp bảo vệ:

4.1.1. Khóa

Các phòng ban quan trọng như: Quản lí, Giám đốc, IT, Server,... Cần sử dụng các khóa có mức an toàn cao:

- Khóa sử dụng: **Khóa Cửa Vân Tay Thông Minh HiLock HL01A** của HiLock.vn
 - Kiểu mở khóa 5 chức năng: Vân tay, thẻ từ, mã số, chìa cơ và App Ttlock
 - An toàn cao với hợp kim và kính cường lực

4.1.2. Camera

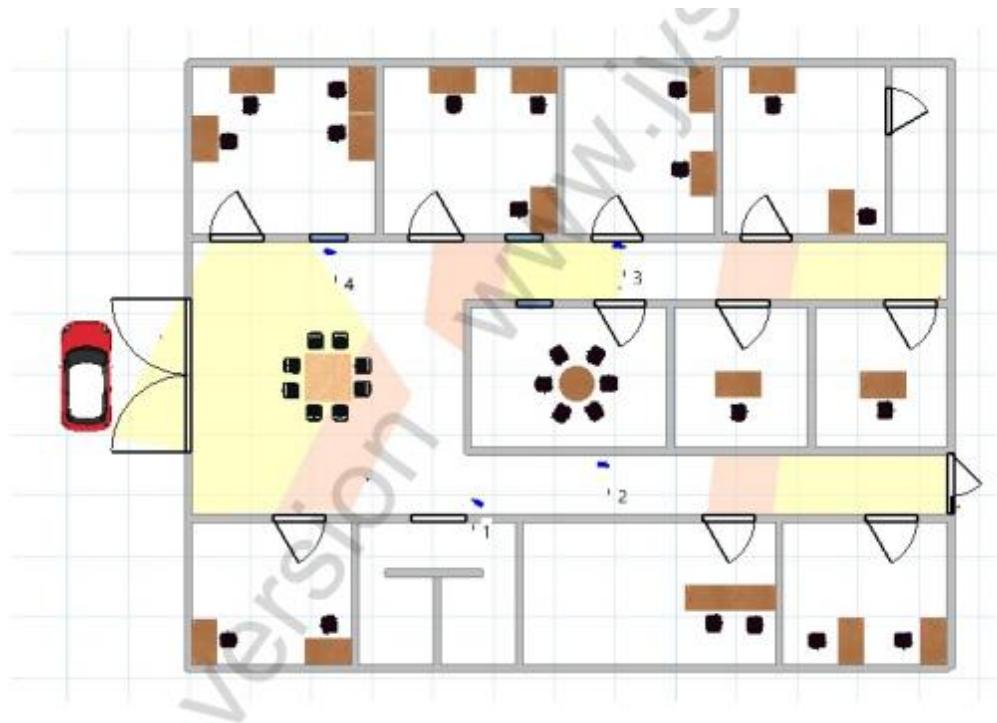
Công ty có trang bị hệ thống camera bao phủ toàn bộ mọi nơi, mục đích bảo vệ kiên cố toàn nhà không để xảy ra trường hợp bị tấn công vật lí

Toàn bộ Camera trong công ty đều sử dụng một loại:

- **Camera AHD VICOM A-130CNS20D**
 - Camera thân ống hồng ngoại sử dụng ngày và đêm
 - Cảm biến hình ảnh 1/3" SONY Super CMOS
 - Độ phân giải hình ảnh 1.3 Megapixel.
 - Chuẩn hình ảnh HD 1280 x 720 và 1280 x 960 Low Illumination
 - Chức năng chống ngược sáng WDR, 3D NR, Sense-up

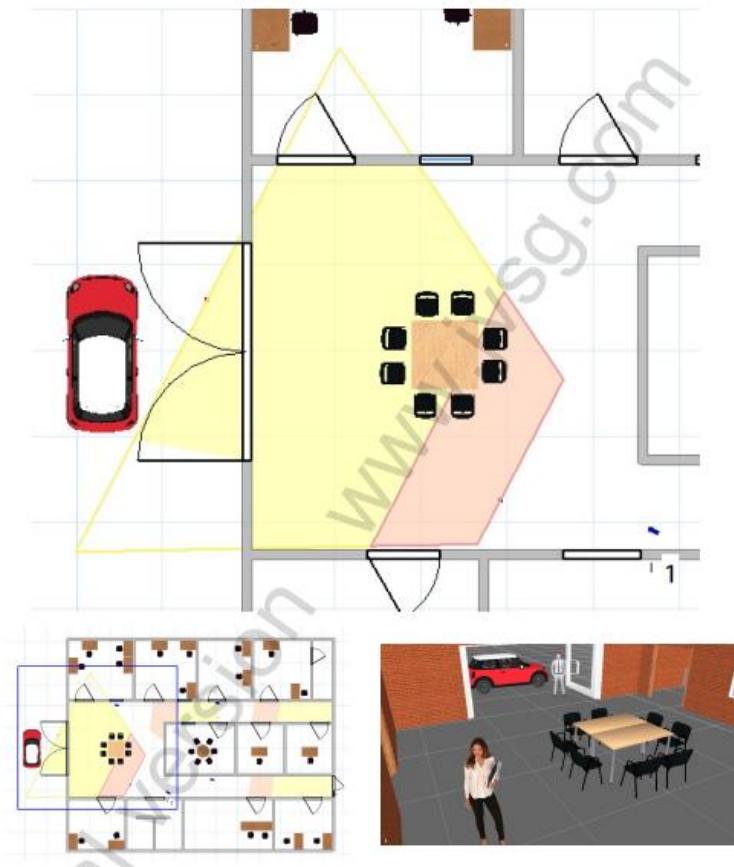
Sau đây là chi tiết lắp đặt Camera tại công ty

- **Hệ thống Camera hành lang**



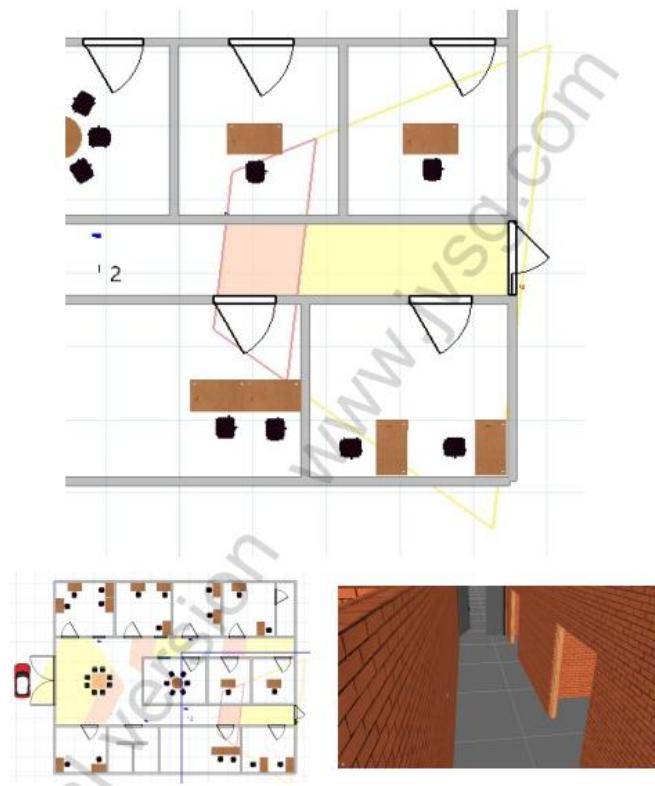
Hình 10. Hệ thống Camera hành lang

- Camera 1: Giám sát khu vực sảnh



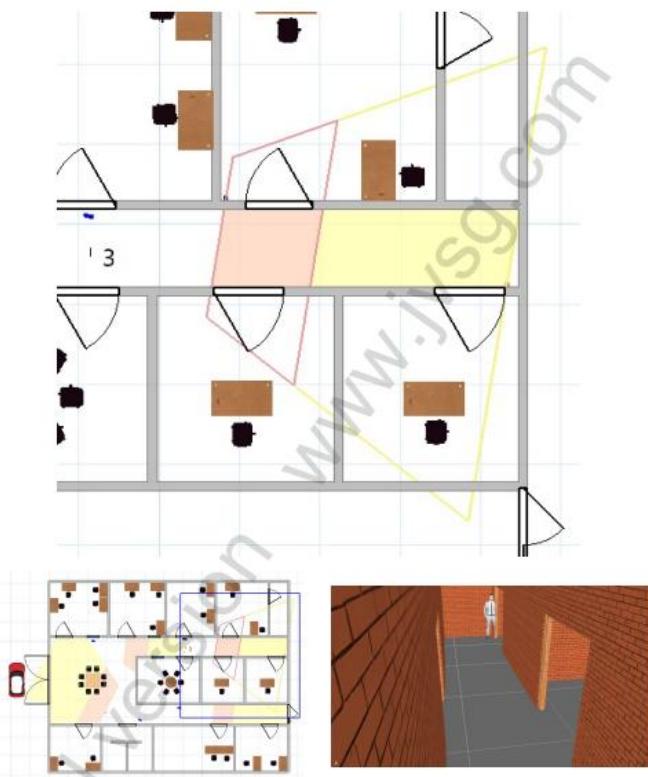
Hình 11. Camera 1 của hành lang

- Camera 2: Giám sát khu vực hành lang và cửa ra vận chuyển hàng hóa



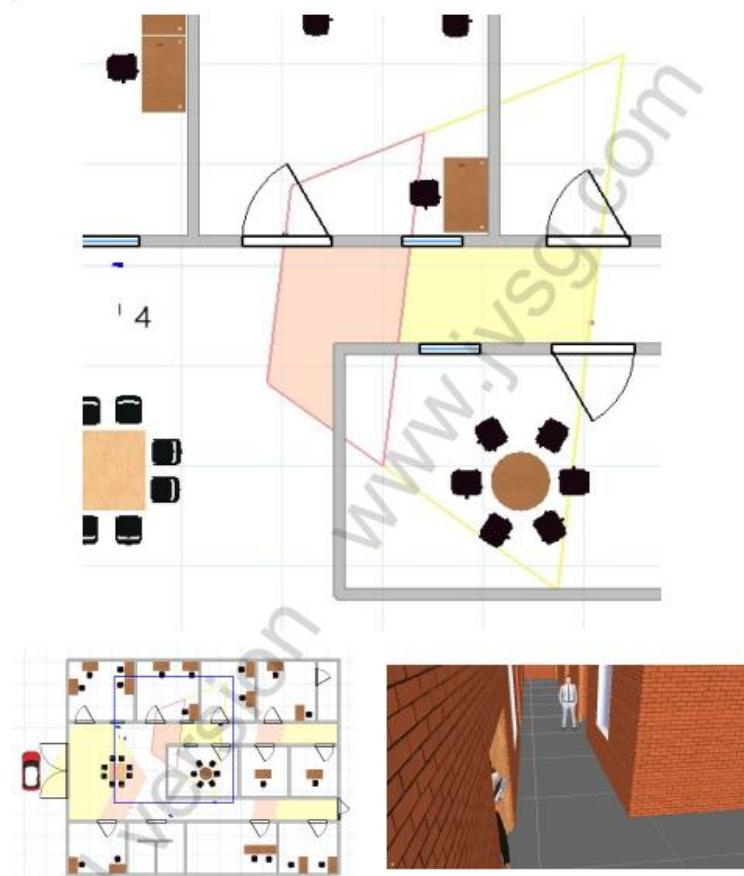
Hình 12. Camera 2 của hành lang

- Camera 3: Giám sát hành lang trước cửa phòng IT, Quản lí và phòng Giám đốc



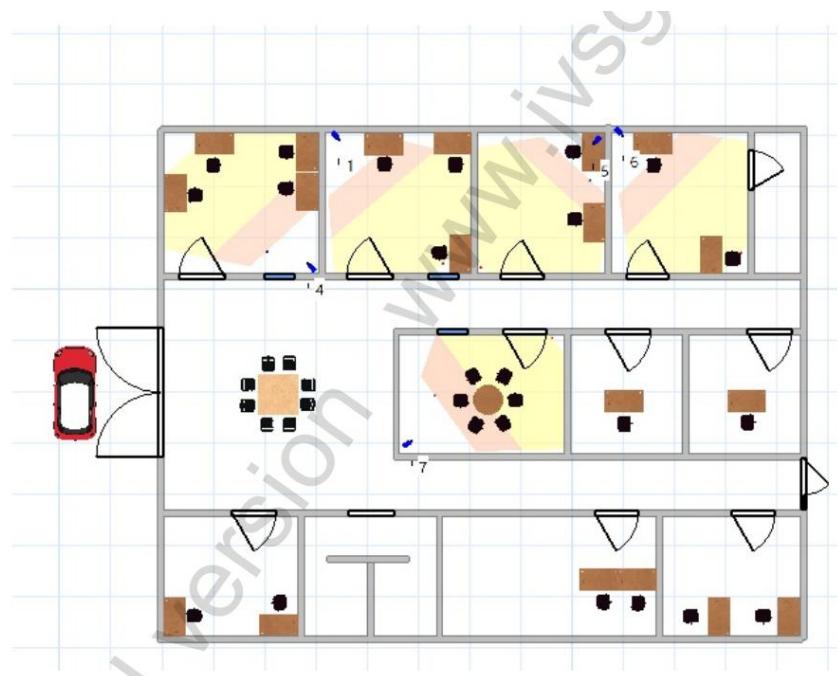
Hình 13. Camera 3 của hành lang

- Camera 4: Giám sát hành lang trước cửa phòng Họp, Marketing và Nhân sự



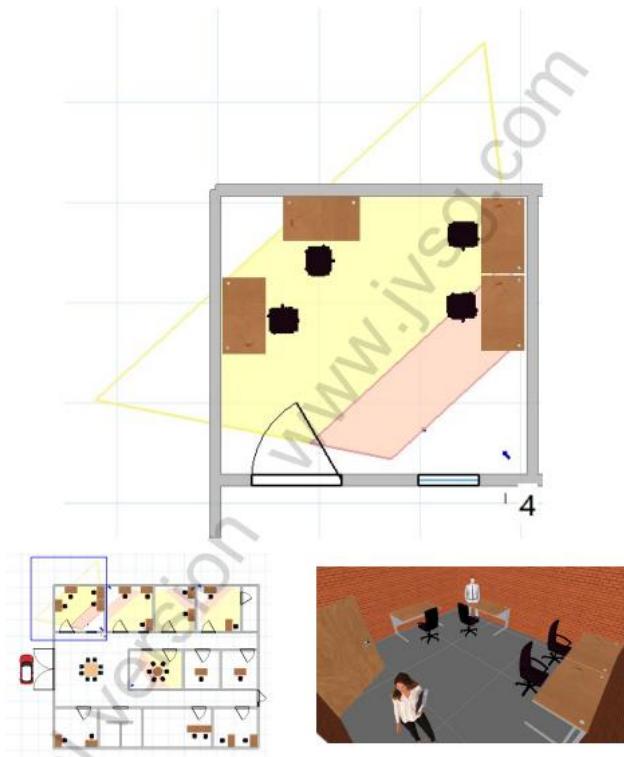
Hình 14. Camera 4 của hành lang

- Camera các phòng ở phía trên sơ đồ vật lí



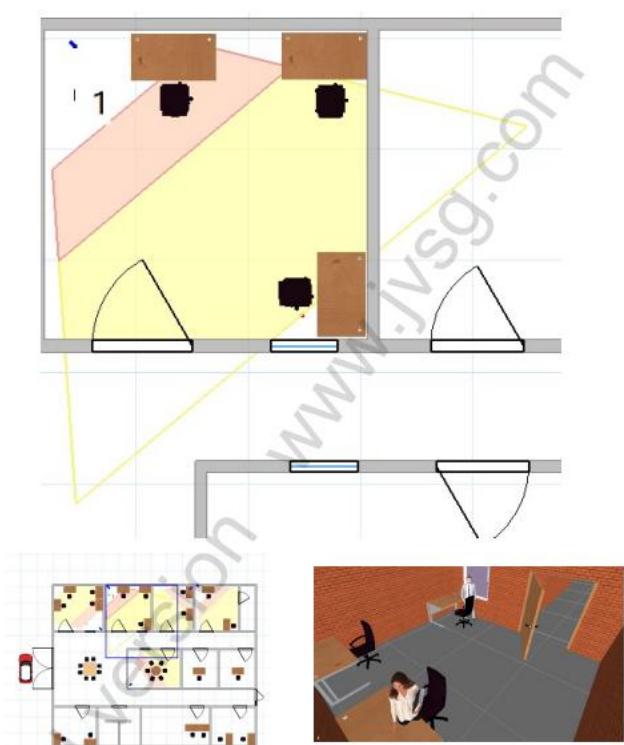
Hình 15. Camera các phòng phía trên

- Camera 1: Giám sát phòng Kinh doanh/Bán hàng



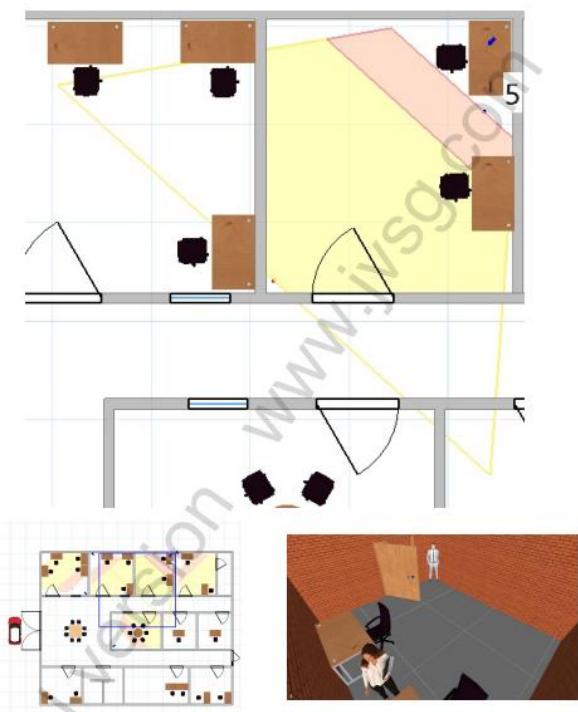
Hình 16. Camera phòng Kinh doanh/Bán hàng

- Camera 2: Giám sát phòng Marketing



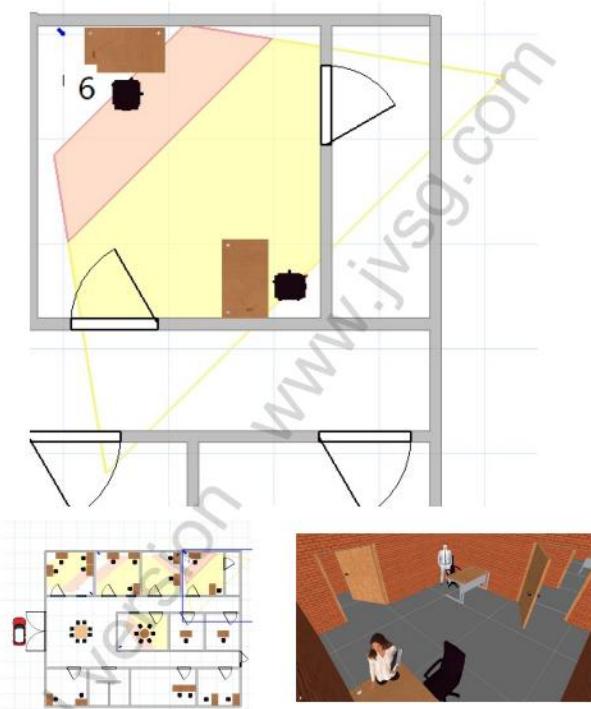
Hình 17. Camera phòng Marketing

- Camera 3: Giám sát phòng Nhân Sự



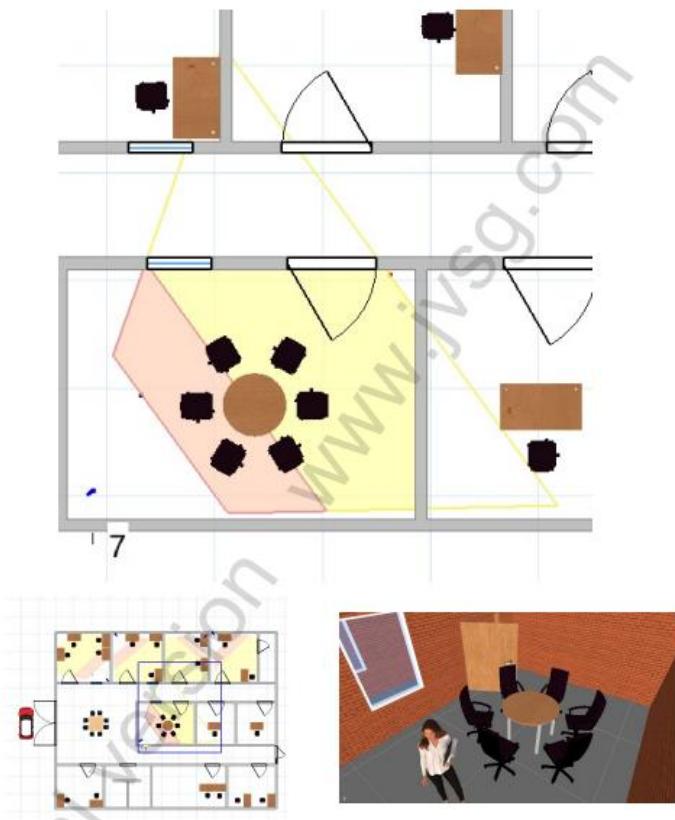
Hình 18. Camera phòng Nhân sự

- Camera 4: Giám sát phòng IT



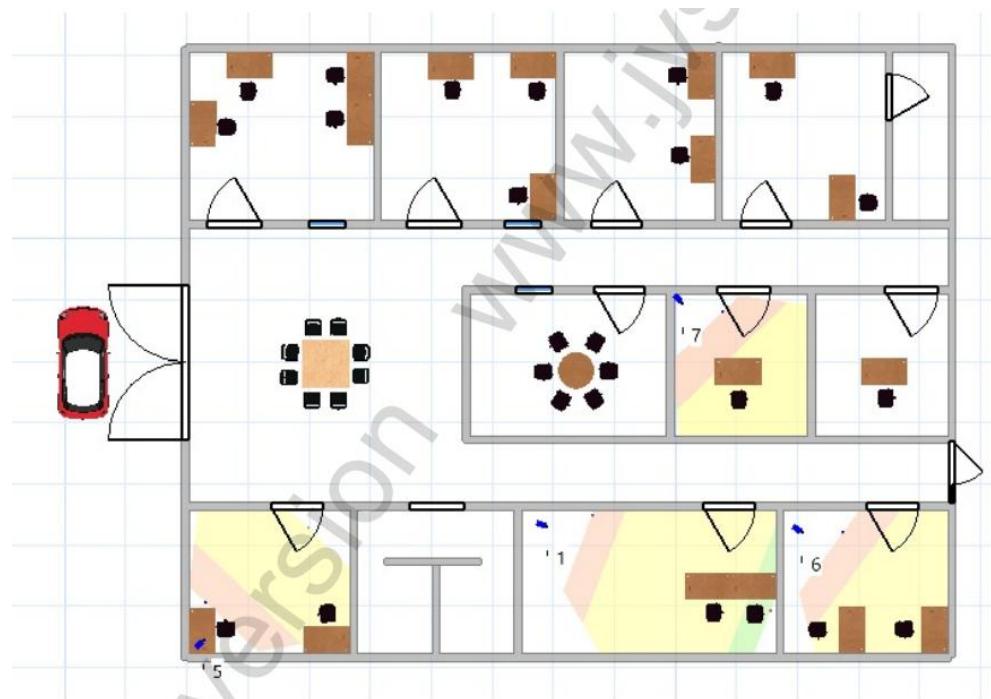
Hình 19. Camera phòng IT

- Camera 5: Giám sát phòng Họp



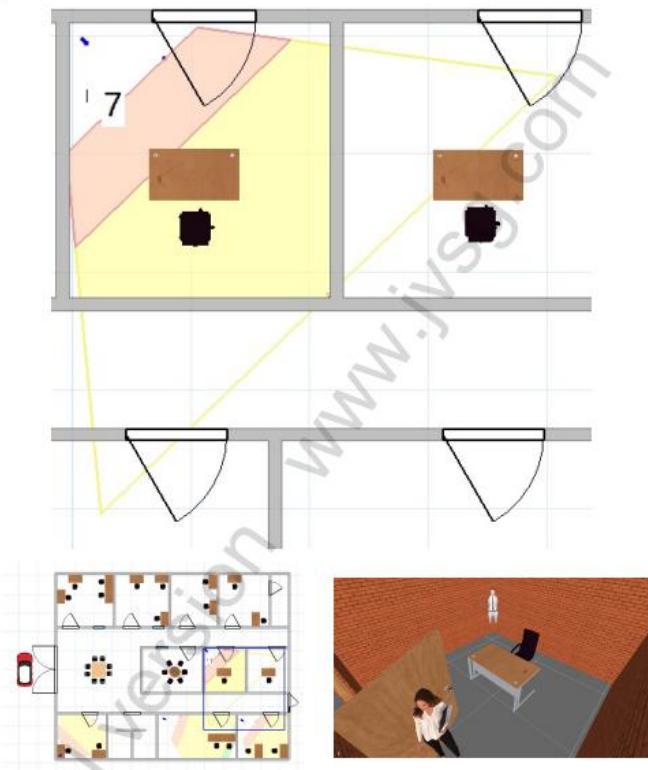
Hình 20. Camera phòng Họp

- Camera các phòng ở phía dưới sơ đồ vật lí



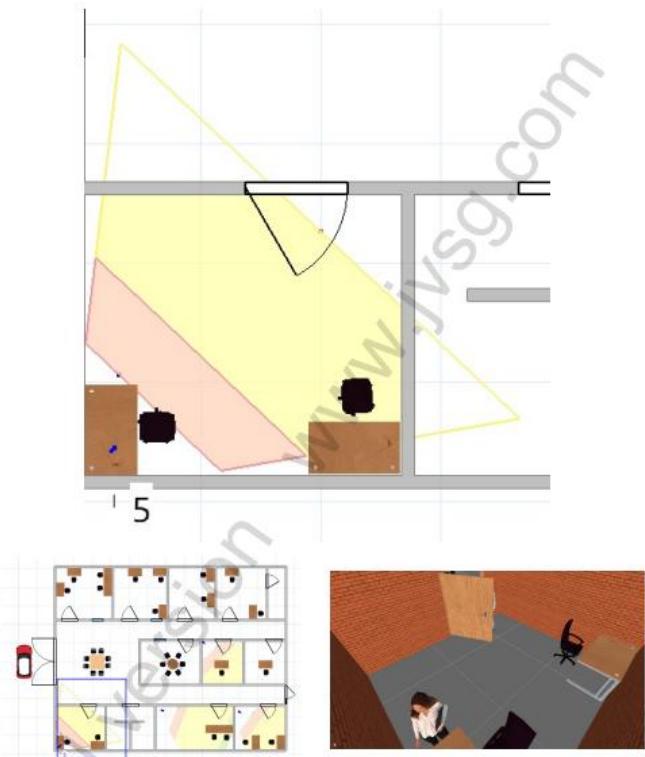
Hình 21. Camera các phòng phía dưới

- Camera 1: Giám sát phòng Quản lý



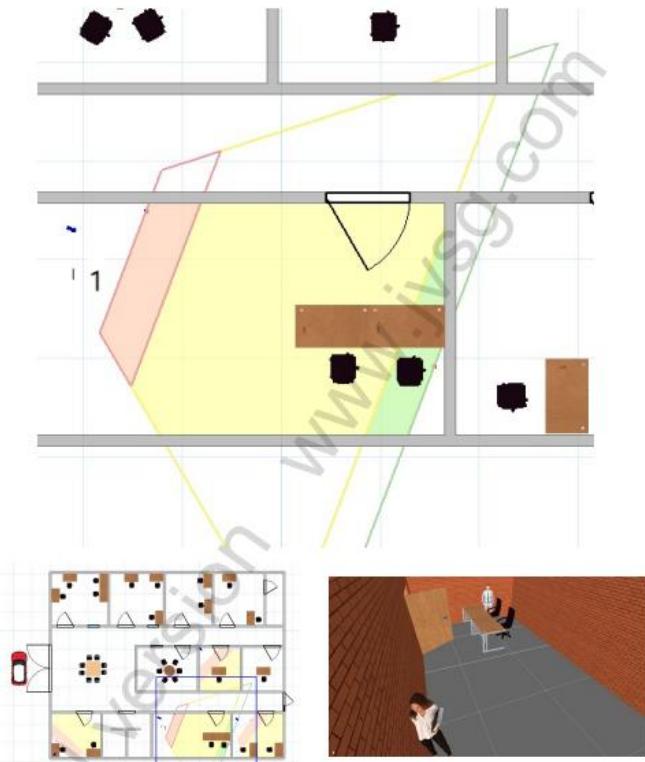
Hình 22. Camera phòng Quản lý

- Camera 2: Giám sát phòng Kế toán



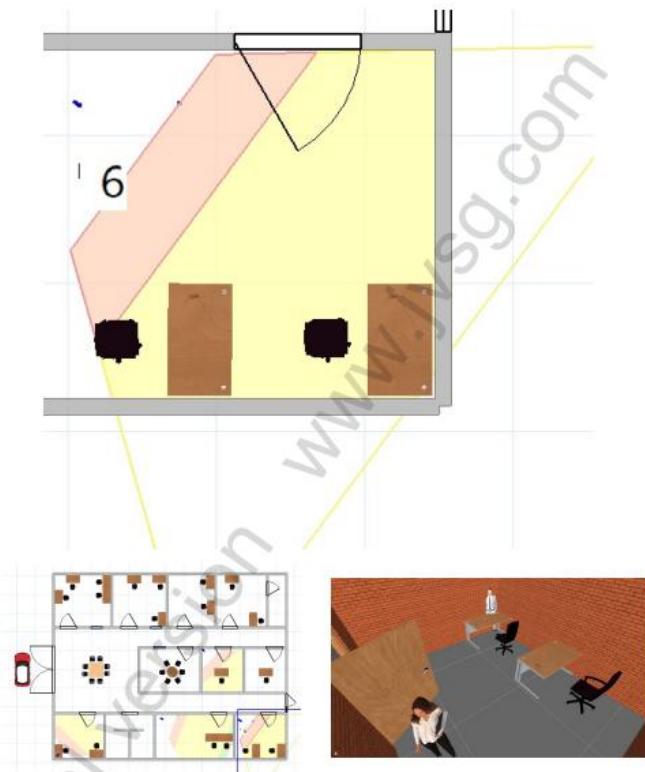
Hình 23. Camera phòng Kế toán - Tài chính

- Camera 3: Giám sát phòng Kho vận/Logistics



Hình 24. Camera phòng Kho vận/Logistics

- Camera 4: Giám sát phòng Nhập hàng/Cung ứng



Hình 25. Camera phòng Nhập hàng/Cung ứng

4.2. Xây dựng hệ thống mạng

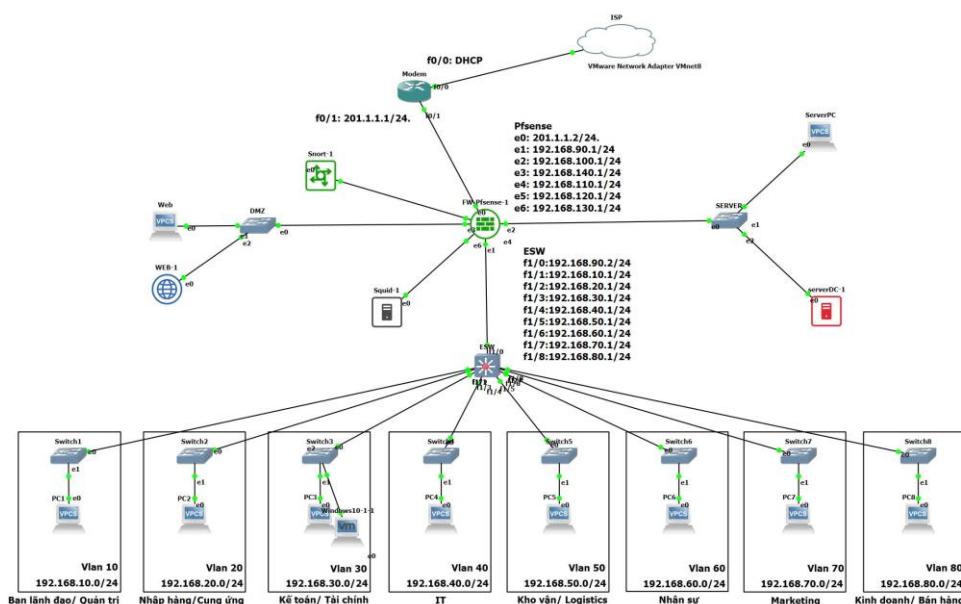
4.2.1. Bảng phân hoạch địa chỉ IPv4

Bảng 2. Bảng phân hoạch địa chỉ IPv4

Phòng Ban	Dải mạng	Subnet Mask	Khoảng IP khả dụng	VLAN ID
Ban lãnh đạo/Quản trị	192.168.10.0/24	255.255.255.0	192.168.10.1 - 192.168.10.254	10
Phòng Nhập hàng/Cung ứng	192.168.20.0/24	255.255.255.0	192.168.20.1 - 192.168.20.254	20
Phòng Kế toán - Tài chính	192.168.30.0/24	255.255.255.0	192.168.30.1 - 192.168.30.254	30
Phòng IT	192.168.40.0/24	255.255.255.0	192.168.40.1 - 192.168.40.254	40
Phòng Kho vận/Logistics	192.168.50.0/24	255.255.255.0	192.168.50.1 - 192.168.50.254	50
Phòng Nhân sự	192.168.60.0/24	255.255.255.0	192.168.60.1 - 192.168.60.254	60
Phòng Nhân sự	192.168.70.0/24	255.255.255.0	192.168.70.1 - 192.168.70.254	70
Phòng Kinh doanh/Bán hàng	192.168.80.0/24	255.255.255.0	192.168.80.1 - 192.168.80.254	80
Servers	192.168.100.0/24	255.255.255.0	192.168.100.1 - 192.168.100.254	100

4.2.2. Sơ đồ logic mạng

Do giới hạn về phần cứng, phần mềm nên đây là những phần sẽ được triển khai chính và nếu triển khai thành công thì sẽ được cấu hình trong môi trường mạng thực tế

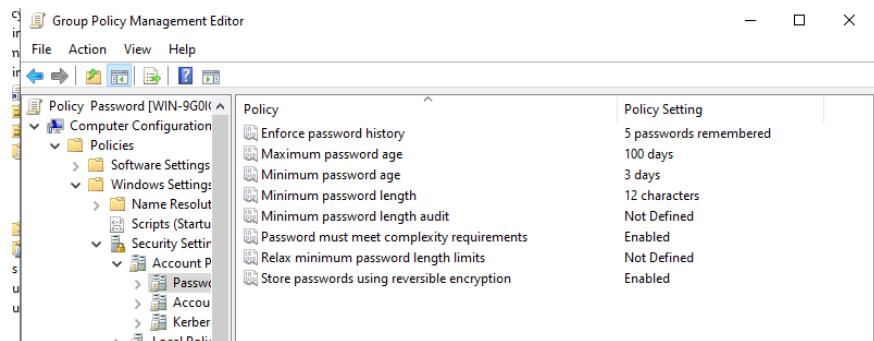


Hình 26. Sơ đồ Logic mạng

4.3. Triển khai Group Policy(Chính sách bảo mật)

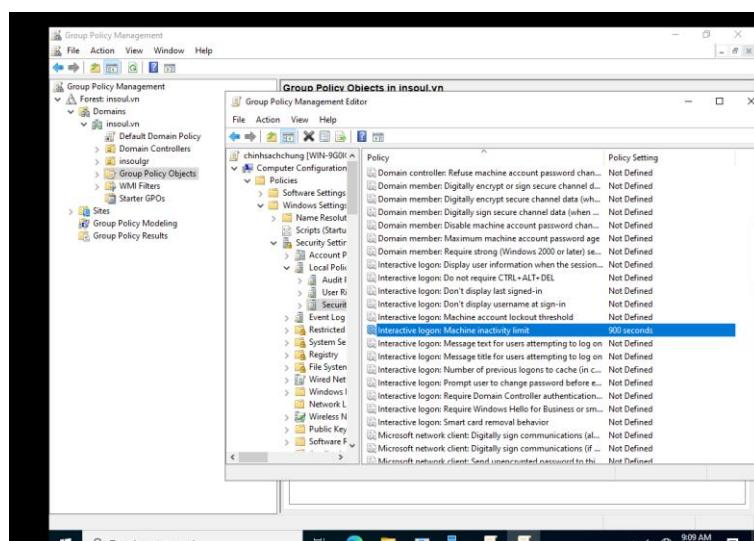
Áp dụng chính sách bảo mật đã đề ra và xây dựng Group Policy ở trong hệ thống mạng:

- Password policy
 - không được đặt mk trùng với 5 mật cũ gần nhất
 - bắt buộc đổi mk sau 100 ngày
 - ít nhất sau 3 ngày mới được đặt mk mới
 - mk dài hơn 12 ký tự
 - mk phải có đủ phức tạp
 - lưu mk được mã hóa



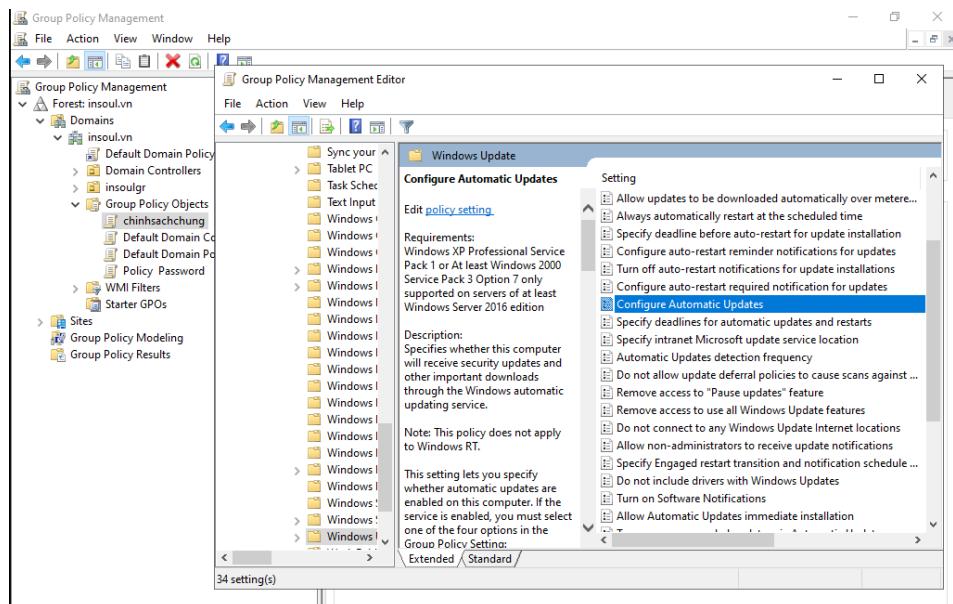
Hình 27. Quy định về Password

- Chính sách chung
- máy tự động khóa sau 15p



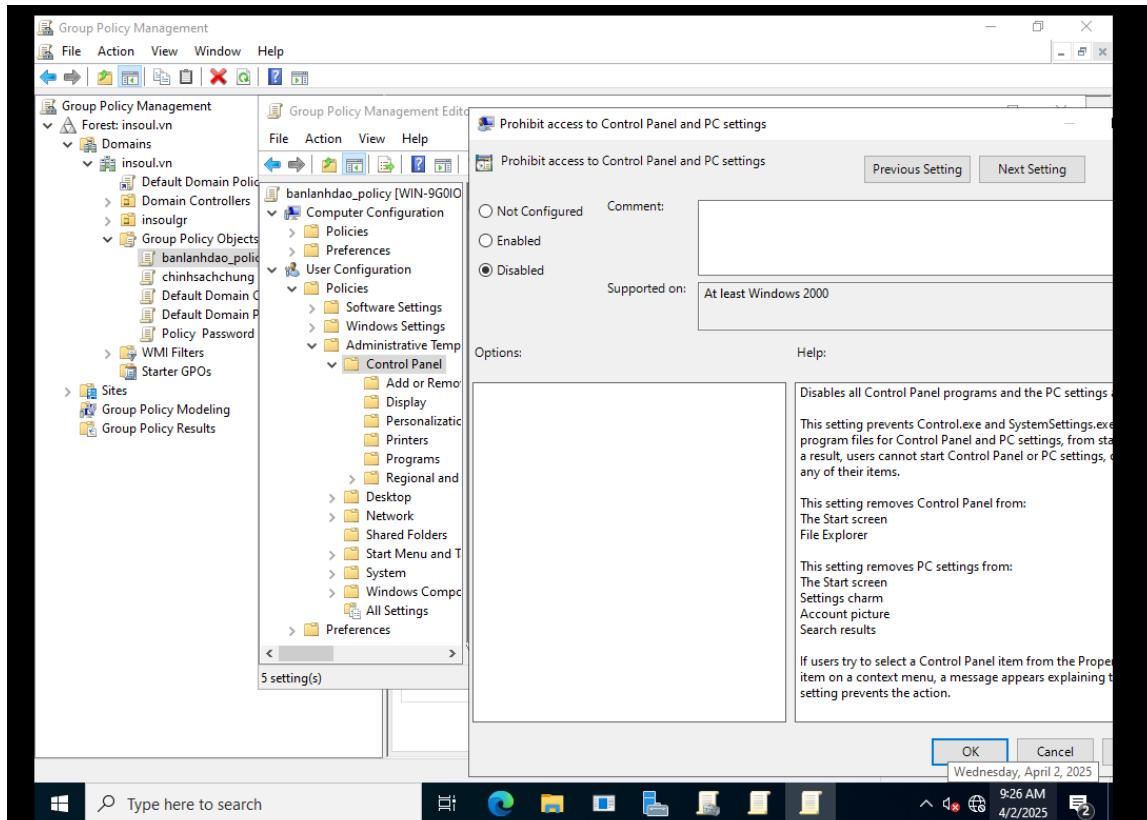
Hình 28. Tắt máy sau 5 phút

- tự động update khi có thông báo



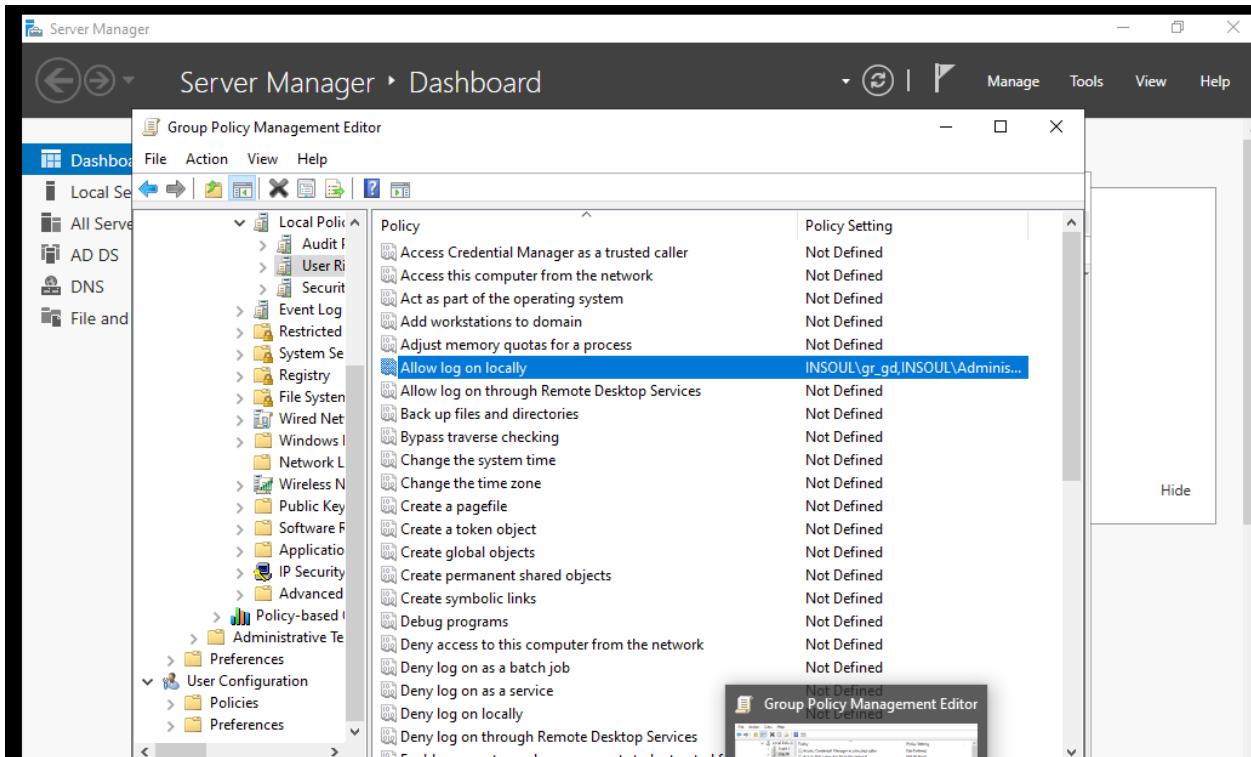
Hình 29. Tự update

- “banlanhdao” Policy
- Truy cập đầy đủ vào tài nguyên mạng



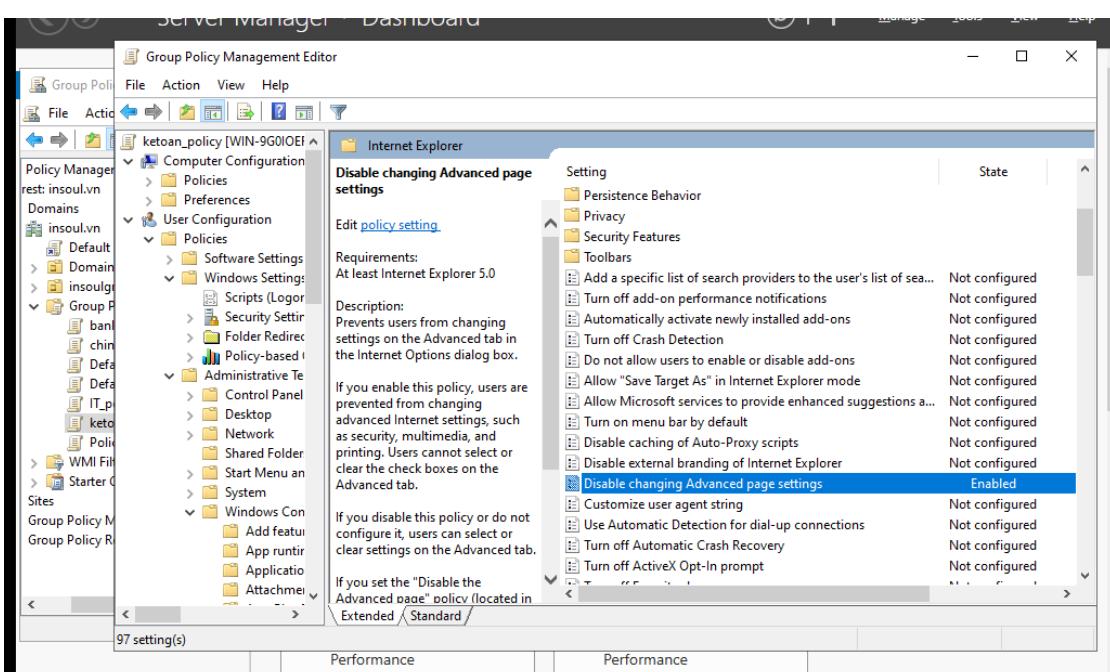
Hình 30. Toàn quyền tài nguyên

- Bảo mật cao hơn (2FA)



Hình 31. Bảo mật cao

- “ketoan” Policy
- Hạn chế truy cập website không liên quan



Hình 32. Cấm truy cập web

- Chặn USB và thiết bị lưu trữ ngoài

The screenshot shows the Group Policy Management Editor interface. On the left, there's a navigation pane with various policy categories like Driver Inst, Early Laun, Enhanced, File Classif, etc. The main pane displays a policy named "Removable Storage Access" under "All Removable Storage classes: Deny all access". It includes sections for Requirements (At least Windows Vista), Description (Configure access to all removable storage classes), and a note about precedence. A table lists settings for different storage types, with one row highlighted: "All Removable Storage classes: Deny all access" with the state "Enabled".

Setting	State
Set time (in seconds) to force reboot	Not configured
CD and DVD: Deny execute access	Not configured
CD and DVD: Deny read access	Not configured
CD and DVD: Deny write access	Not configured
Custom Classes: Deny read access	Not configured
Custom Classes: Deny write access	Not configured
Floppy Drives: Deny execute access	Not configured
Floppy Drives: Deny read access	Not configured
Floppy Drives: Deny write access	Not configured
All Removable Storage: Allow direct access in remote sessions	Not configured
Tape Drives: Deny execute access	Not configured
Tape Drives: Deny read access	Not configured
Tape Drives: Deny write access	Not configured
WPD Devices: Deny read access	Not configured
WPD Devices: Deny write access	Not configured
All Removable Storage classes: Deny all access	Enabled

Hình 33. Chặn các thiết bị lưu trữ ngoài

- “IT” Policy
- Quyền admin trên máy tính cục bộ

The screenshot shows the Group Policy Management Editor with a policy named "IT_policy [WIN-960I0ER4CA]". The left pane shows the policy structure under "Computer Configuration / Policies / Security Settings / Local Policies / Audit Policy". The right pane displays a table of audit policies. One specific policy, "Allow log on locally", is selected and its value is set to "INSOUL\itgr\Administrators,ad".

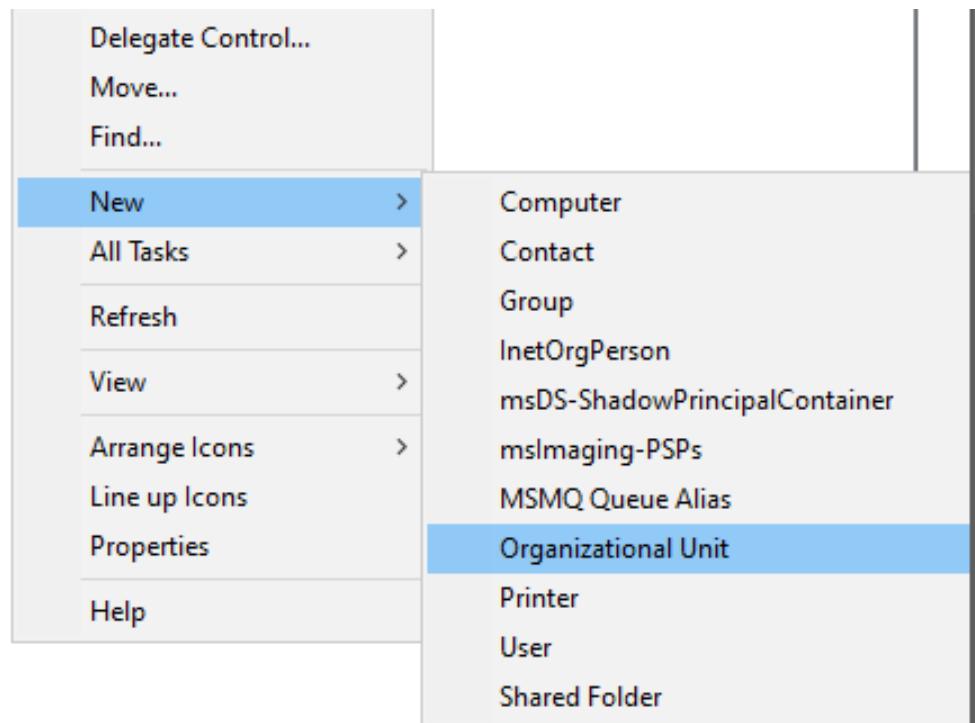
Policy Setting	State
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	INSOUL\itgr\Administrators,ad
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined

Hình 34. Cấp quyền cho Admin

4.4. Kiểm soát truy cập

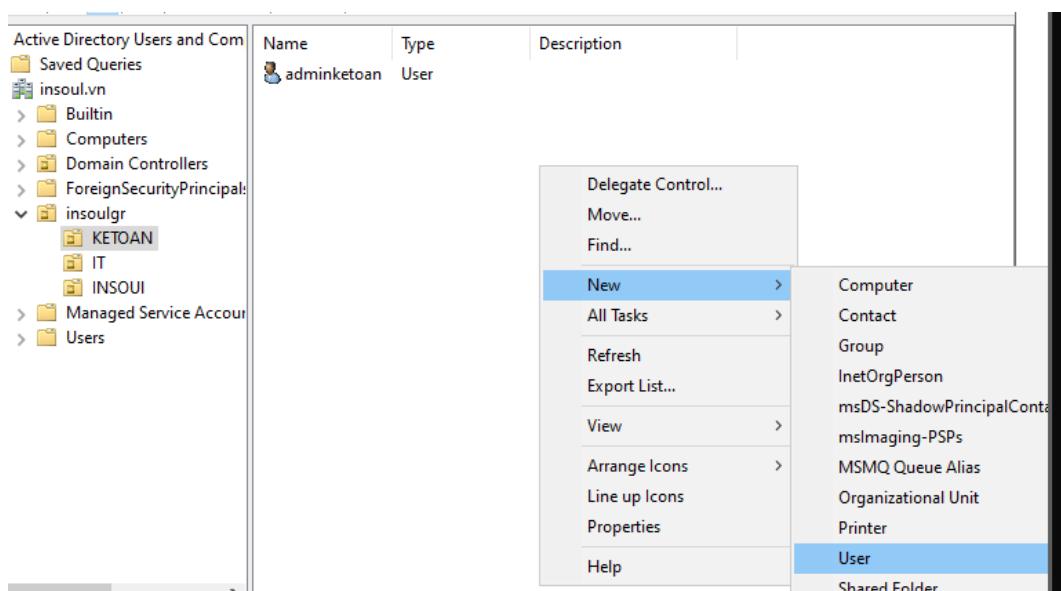
4.4.1. Phân quyền truy cập file

Bước 1: Truy cập vào AD Users and Computer và Tạo các organizational Unit



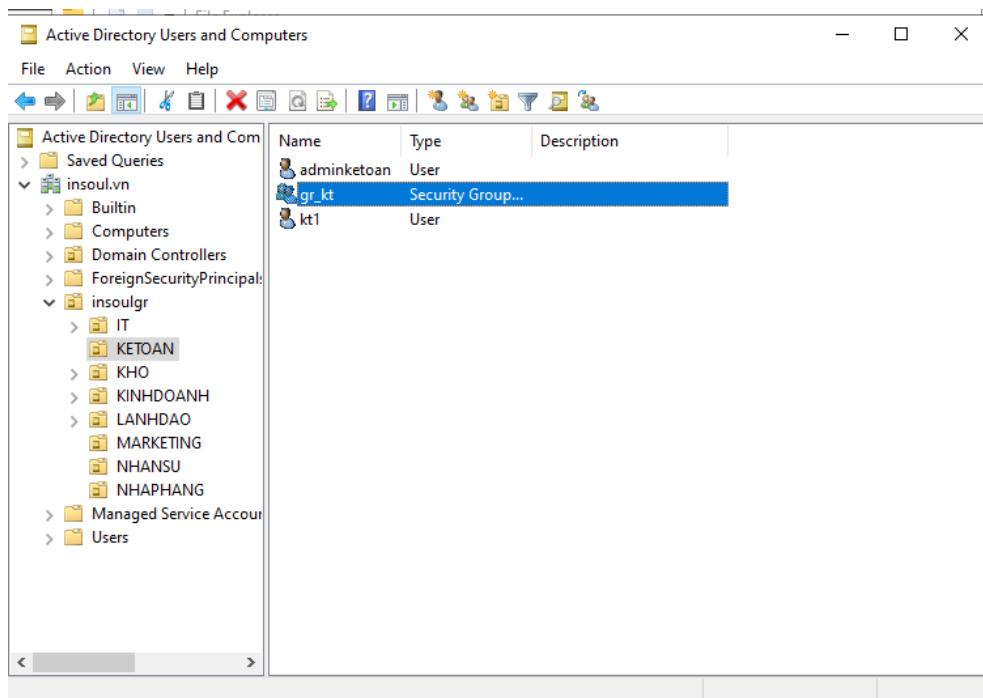
Hình 35. Tạo Organization Unit

Bước 2: Tạo user cho các phòng



Hình 36. Tạo User

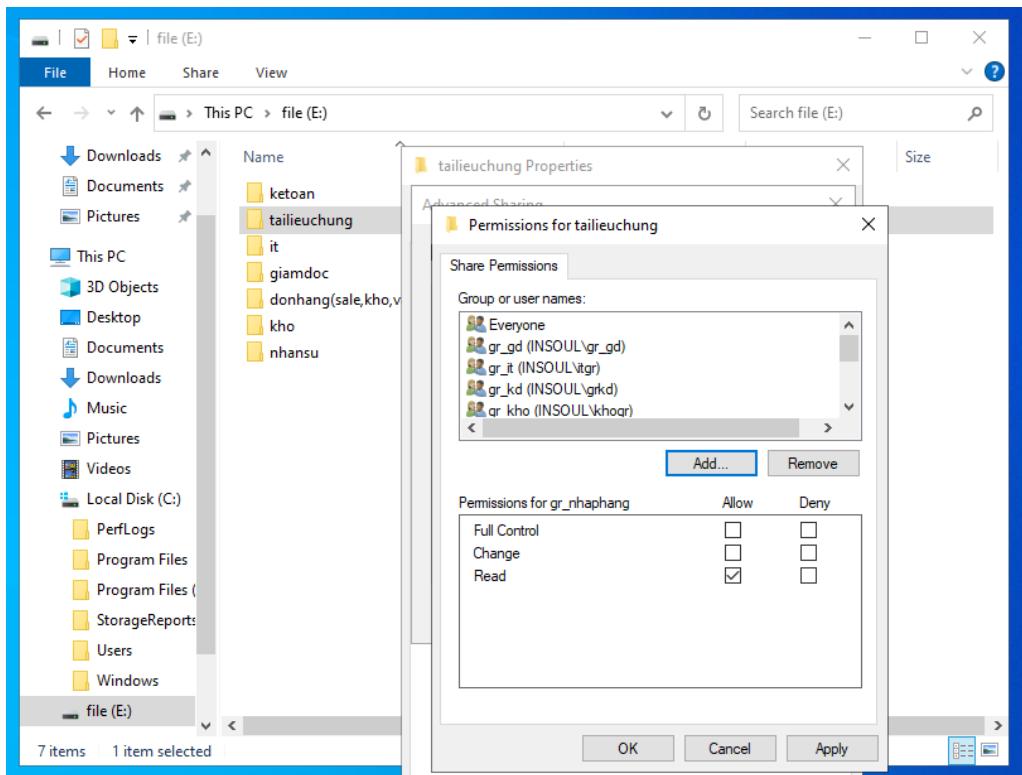
Bước 3: Tạo các group và thêm user vào



Hình 37. Thêm Group và User

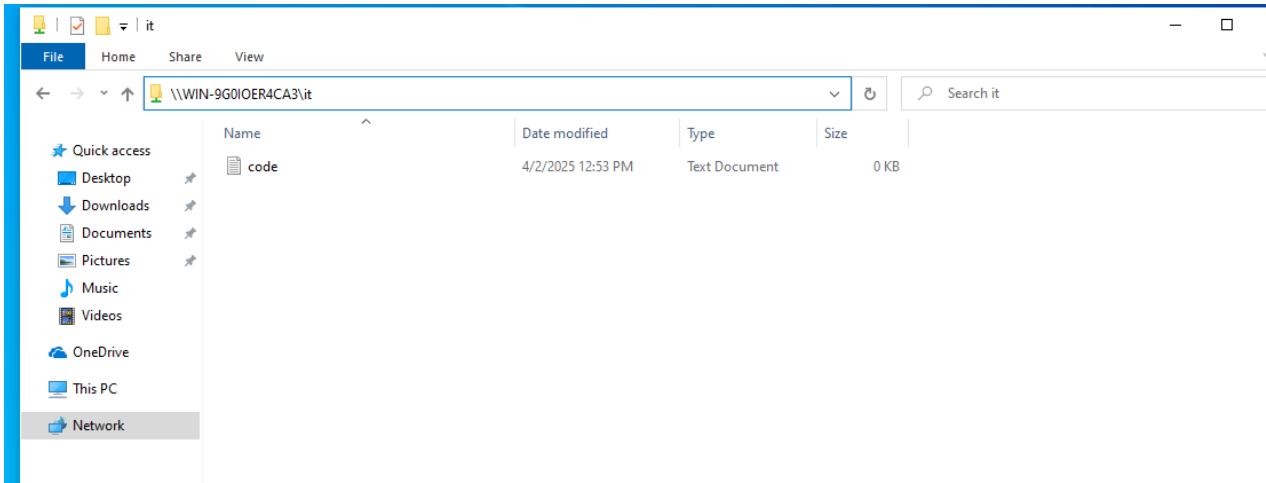
Bước 4: Thiết lập phân quyền

- Share tài liệu chung cho tất cả các group với quyền read còn it, giamdoc có thêm quyền change



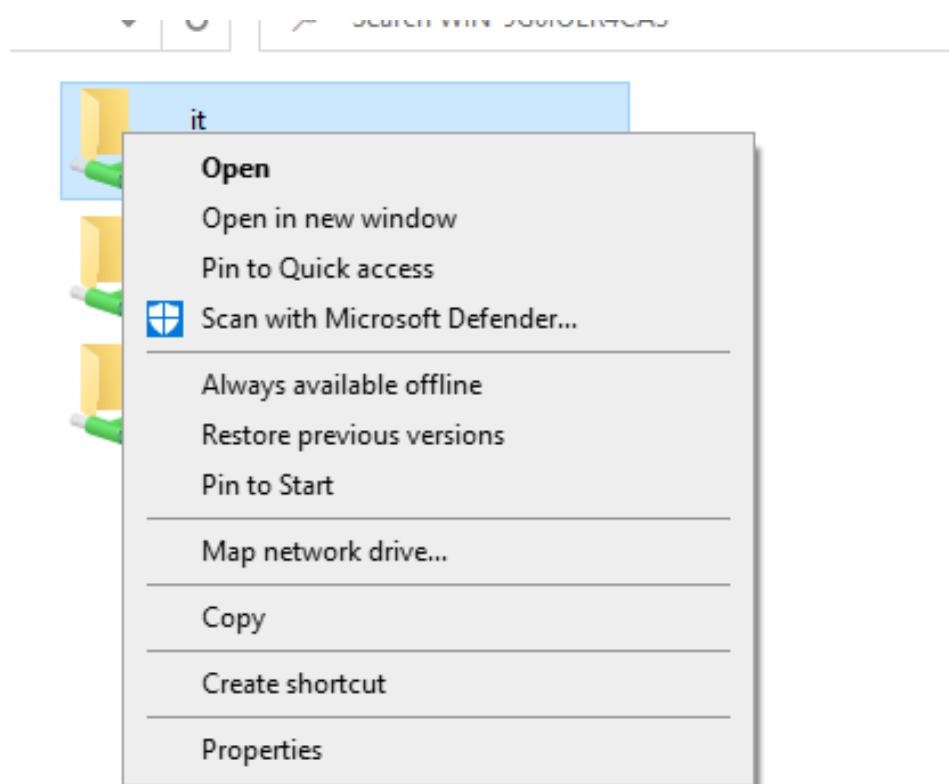
Hình 38. Phân quyền xem, xóa và sửa file

- Share thành công khi thử đăng nhập bằng IT1



Hình 39. Thành công share file

Bước 5: Chọn map network drive để tiện cho việc truy xuất sau này

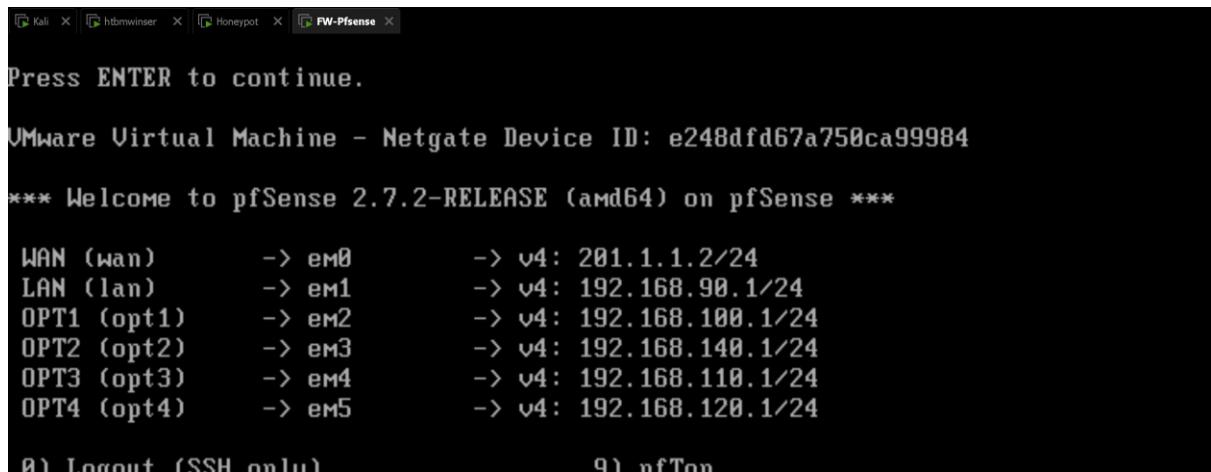


Hình 40. Map network drive

4.5. Triển khai các công nghệ bảo mật

4.5.1. Triển khai Firewall (pfSense)

Cấu hình pfSense:



```
Kali      X | htbwinser X | Honeypot X | FW-PfSense X
Press ENTER to continue.

VMware Virtual Machine - Netgate Device ID: e248dfd67a750ca99984

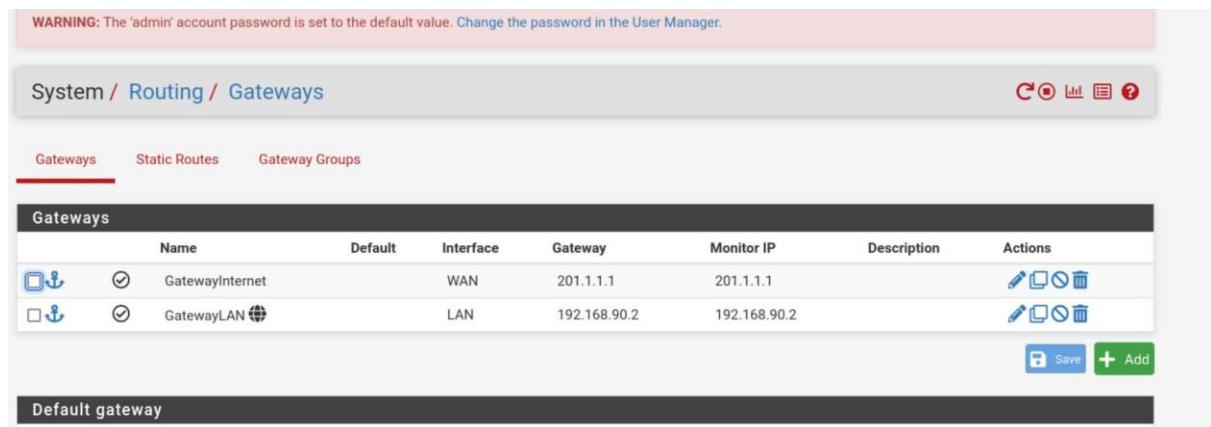
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 201.1.1.2/24
LAN (lan)      -> em1      -> v4: 192.168.90.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.100.1/24
OPT2 (opt2)    -> em3      -> v4: 192.168.140.1/24
OPT3 (opt3)    -> em4      -> v4: 192.168.110.1/24
OPT4 (opt4)    -> em5      -> v4: 192.168.120.1/24

a) Logout (SSH only)   q) nfTop
```

Hình 41. Thông tin của các cổng mạng

- Cấu hình Gateways



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Routing / Gateways

Gateways Static Routes Gateway Groups

Name	Default	Interface	Gateway	Monitor IP	Description	Actions
GatewayInternet	✓	WAN	201.1.1.1	201.1.1.1		
GatewayLAN	✓	LAN	192.168.90.2	192.168.90.2		

Default gateway

Save Add

Hình 42. Gateways trên pfSense

- Cấu hình các rules trên pfSense

The screenshot shows the 'Static Routes' section of the pfSense configuration. It lists eight static routes, each mapping a specific network range (e.g., 192.168.10.0/24) through an interface (Vlan10 to Vlan80) to a common gateway (GatewayLAN - 192.168.90.2). The 'Actions' column includes edit, copy, and delete icons.

Network	Gateway	Interface	Description	Actions
192.168.10.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan10	
192.168.20.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan20	
192.168.30.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan30	
192.168.40.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan40	
192.168.50.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan50	
192.168.60.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan60	
192.168.70.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan70	
192.168.80.0/24	GatewayLAN - 192.168.90.2	LAN	Vlan80	

Hình 43. Cấu hình rules trên pfSense

- Tạo danh sách ip VLAN để để cấu hình rules

The screenshot shows the 'Firewall Aliases IP' section. It contains one entry named 'VLAN' which maps multiple IP ranges (192.168.10.0/24, 192.168.20.0/24, etc.) to an action that allows traffic from any VLAN to anywhere. The 'Actions' column includes edit, copy, and delete icons.

Name	Type	Values	Description	Actions
VLAN	Network(s)	192.168.10.0/24, 192.168.20.0/24, 192.168.30.0/24, 192.168.40.0/24, 192.168.50.0/24, 192.168.60.0/24, 192.168.70.0/24, 192.168.80.0/24	Allow all Vlan to any where	

Hình 44. Danh sách Aliases

Thiết lập Rules:

- Chỉ cho kết nối đến máy mồi honeypot, chỉ cho kết nối đến web trong DMZ:

The screenshot shows the 'WAN' tab of the firewall rules configuration. A new rule has been added to allow traffic from WAN subnets to port 80 (HTTP) on the OPT2 subnets. The 'Actions' column includes edit, copy, and delete icons.

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
0/1 KiB	IPv4 TCP/UDP	WAN subnets	*	OPT2 subnets	80 - 443	*	none				
0/1000 B	IPv4 *	WAN subnets	*	192.168.120.10	*	*	none				

Hình 45. Rule dẫn đến Honeypot

- Thiết lập cho phép kết nối đến mọi nơi nhưng chặn kết nối đến Server

Firewall / Rules / LAN

Floating WAN LAN OPT1 OPT2 OPT3 OPT4

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/1.12 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗ 0/15 KiB	IPv4 *	VLAN	*	192.168.100.0/24	*	*	none			
✗ 0/260 KiB	IPv4 *	VLAN	*	*	*	*	none			

Add Up Add Down Delete Toggle Copy Save Separator

Hình 46. Thiết lập chặn kết nối đến Server

- Cho phép Server kết nối mọi nơi

Firewall / Rules / OPT1

Floating WAN LAN OPT1 OPT2 OPT3 OPT4

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/4 KiB	IPv4 *	OPT1 subnets	*	VLAN	*	*	none		Truy cập LAN	
✓ 0/29.67 MiB	IPv4 *	OPT1 subnets	*	*	*	*	none		DMZ 100	

Add Up Add Down Delete Toggle Copy Save Separator

Hình 47. Rule cho Server kết nối

- Không cho DMZ kết nối với LAN và Server

Firewall / Rules / OPT2

Floating WAN LAN OPT1 OPT2 OPT3 OPT4

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/1 KiB	IPv4 *	OPT2 subnets	*	VLAN	*	*	none			
✗ 0/420 B	IPv4 *	OPT2 subnets	*	192.168.100.0/24	*	*	none			
✓ 0/6 KiB	IPv4 *	OPT2 subnets	*	*	*	*	none			

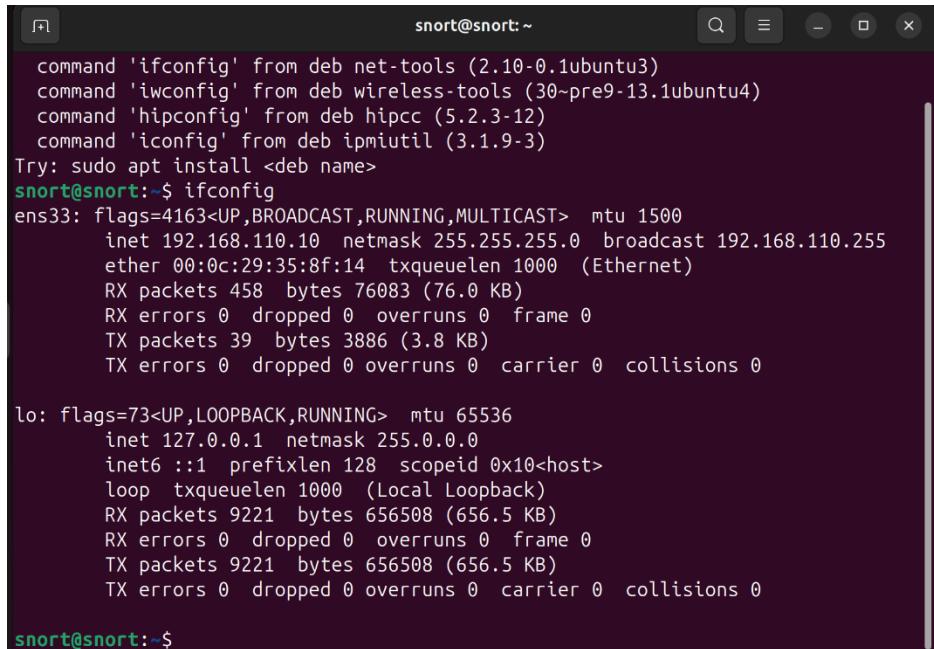
Add Up Add Down Delete Toggle Copy Save Separator

Hình 48. Chặn DMZ kết nối

4.5.2. Triển khai IDS (Snort)

Triển khai chạy Snort

- Chạy snort trên Ubuntu:
 - o snort -c /usr/local/etc/snort/snort.lua -i ens33 -A alert_fast



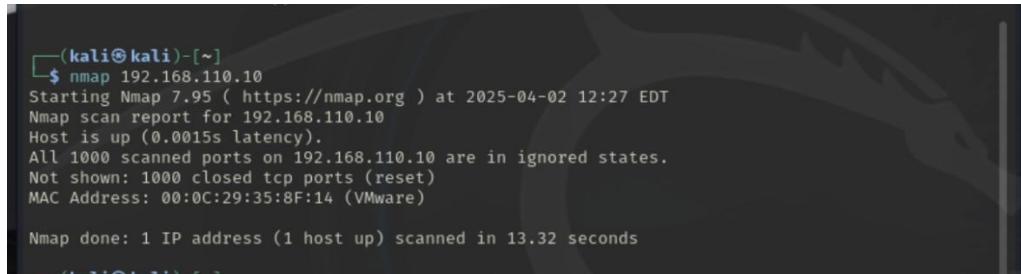
```
snort@snort:~$ ifconfig
command 'ifconfig' from deb net-tools (2.10-0.1ubuntu3)
command 'iwconfig' from deb wireless-tools (30~pre9-13.1ubuntu4)
command 'hipconfig' from deb hipcc (5.2.3-12)
command 'iconfig' from deb ipmiutil (3.1.9-3)
Try: sudo apt install <deb name>
snort@snort:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.110.10 netmask 255.255.255.0 broadcast 192.168.110.255
        ether 00:0c:29:35:8f:14 txqueuelen 1000 (Ethernet)
          RX packets 458 bytes 76083 (76.0 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 39 bytes 3886 (3.8 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 9221 bytes 656508 (656.5 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 9221 bytes 656508 (656.5 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

snort@snort:~$
```

Hình 49. Thông tin của Snort

- Giả lập tấn công, sử dụng một máy Kali, thực hiện nmap đến máy Snort

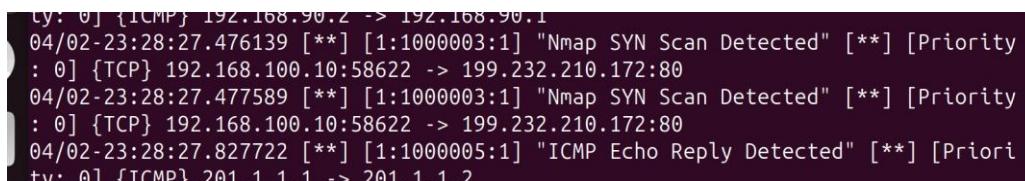


```
(kali㉿kali)-[~]
└─$ nmap 192.168.110.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 12:27 EDT
Nmap scan report for 192.168.110.10
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.110.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:35:8F:14 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

Hình 50. Nmap từ Kali đến Snort

- Ta có thể thấy rằng Snort bắt được gói tin của Kali gửi tới



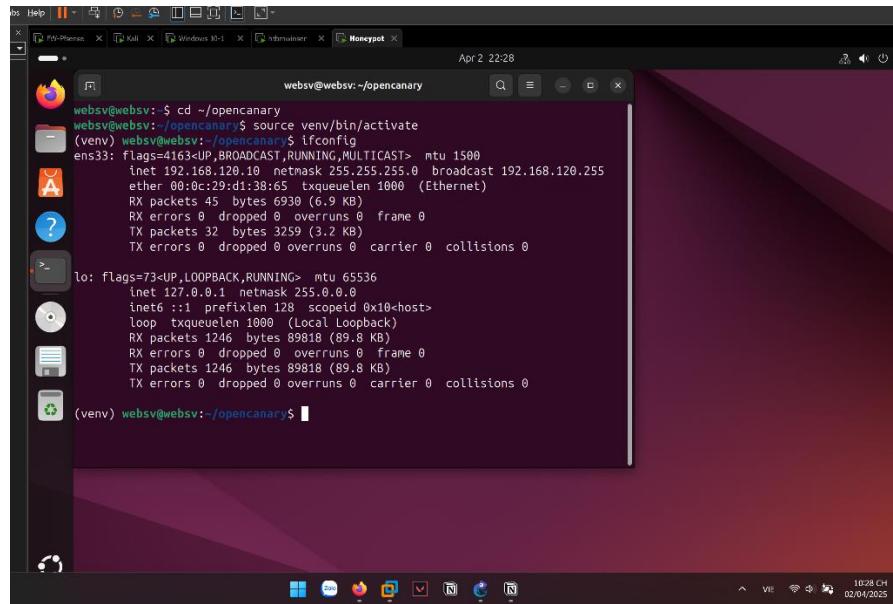
```
0y: 0] {ICMP} 192.168.90.2 -> 192.168.90.1
04/02-23:28:27.476139 [**] [1:1000003:1] "Nmap SYN Scan Detected" [**] [Priority
: 0] {TCP} 192.168.100.10:58622 -> 199.232.210.172:80
04/02-23:28:27.477589 [**] [1:1000003:1] "Nmap SYN Scan Detected" [**] [Priority
: 0] {TCP} 192.168.100.10:58622 -> 199.232.210.172:80
04/02-23:28:27.827722 [**] [1:1000005:1] "ICMP Echo Reply Detected" [**] [Priori
ty: 0] {ICMP} 201.1.1.1 -> 201.1.1.2
```

Hình 51. Snort Bắt gói tin của Kali

4.5.3. Triển khai Honey Pots

Việc triển khai honeypot giúp công ty phát hiện sớm các mối đe dọa, nâng cao bảo mật và giảm thiểu rủi ro bị xâm nhập

- Triển khai Honey Pot



Hình 52. Thông tin của Honey Pot

- Chạy Honey Pots

```
(venv) websv@websv:~/opencanary$ systemctl status opencanary
Unit opencanary.service could not be found.
(venv) websv@websv:~/opencanary$ sudo tail -f /var/tmp/opencanary.log
[sudo] password for websv:
{"dst_host": "", "dst_port": -1, "local_time": "2025-04-02 05:28:52.362475", "local_time_adjusted": "2025-04-02 12:28:52.362502", "logdata": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.modules.ftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-04-02 05:28:52.362498"} {"dst_host": "", "dst_port": -1, "local_time": "2025-04-02 05:28:52.362767", "local_time_adjusted": "2025-04-02 12:28:52.362780", "logdata": {"msg": {"logdata": "Canary running!!!!"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-04-02 05:28:52.362777"} ^C
(venv) websv@websv:~/opencanary$
```

Hình 53. Chạy Honey Pot

- o Log hiển thị "**Canary running!!!!**", có nghĩa là OpenCanary đã khởi động thành công và đang chạy
- Mở ip đến honeypot

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source
Source: Invert match | Any | Source Address | / |

Destination
Destination: Invert match | Network | 192.168.120.10 | / | 24 |

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description: Allow traffic to Honeypot
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options:

Rule Information

Tracking ID: 1743585168
Created: 4/2/25 09:12:48 by admin@192.168.90.10 (Local Database)
Updated: 4/2/25 09:12:48 by admin@192.168.90.10 (Local Database)

Hình 54. Mở ip đến Honey Pot

- Cấu hình NAT 1:1 public ip 201.1.1.10 cho honeypot

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / 1:1 / Edit

Edit NAT 1:1 Entry

Disabled: Disable this rule
When disabled, the rule will not have any effect.

No BINAT (NOT): Do not perform binat for the specified address
Excludes the address from a later, more general, rule.

Interface: WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

External subnet IP: Address: 201.1.1.10
Enter the external (usually on a WAN) subnet's starting address or interface for the 1:1 mapping.

Internal IP: Not | Network: 192.168.120.10 | Type: / 24 | Address/mask
Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the internal subnet will be applied to the external subnet.

Destination: Not | Any | Type: / | Address/mask
The 1:1 mapping will only be used for connections to or from the specified destination. Hint: this is usually "Any".

Description: 1:1 NAT for Honeypot
A description may be entered here for administrative reference (not parsed).

NAT reflection: Use system default

Hình 55. Cấu hình NAT, public ip Honey Pot

- Cấu hình rules cho Honey Pot

Firewall / Rules / WAN												
Floating	WAN	LAN	OPT1	OPT2	OPT3	OPT4						
Rules (Drag to Change Order)												
<input type="checkbox"/>	<input checked="" type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

Hình 56. Cấu hình rules ip honeypot

- Tiến hành ping thử từ một ip ở ngoài mạng vào ip public của Honeypot

```

Sending 5, 100-byte ICMP Echos to 201.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/16 ms
R2#ping 201.1.1.10
K
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.1.1.10, timeout is 2 seconds:
!...
naSuccess rate is 40 percent (2/5), round-trip min/avg/max = 1004/1468/1932 ms
R2#ping 201.1.1.10

```

Hình 57. Ping tới địa chỉ public Honeypot

- Dùng ip ngoài mạng ping vào địa chỉ ip private của Honeypot

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.120.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#

```

Hình 58. Ping tới ip private của Honeypot

4.6. Triển khai Proxy (Squid)

Cài đặt Squid:

```
sudo apt update sudo apt install squid -y
```

Cấu hình Squid:

```
sudo nano /etc/squid/squid.conf
```

Xóa nội dung và thêm cấu hình sau:

- Cổng lắng nghe của Squid: http_port 3128
- Tên máy chủ: visible_hostname proxy-server

ACL cho tất cả các VLAN:

```
acl vlan10_network src 192.168.10.0/24 # Ban lãnh đạo/Quản trị acl vlan20_network
src 192.168.20.0/24 # Nhập hàng/Cung ứng
```

```
acl vlan30_network src 192.168.30.0/24 # Kế toán/Tài chính acl vlan40_network src
192.168.40.0/24 # IT acl vlan50_network src 192.168.50.0/24 # Kho vận/Logistics acl
```

```
vlan60_network src 192.168.60.0/24 # Nhân sự acl vlan70_network src  
192.168.70.0/24 # Marketing acl vlan80_network src 192.168.80.0/24 # Kinh  
doanh/Bán hàng acl proxy_network src 192.168.130.0/24 # Mạng proxy
```

ACL cho các cổng phô biến

```
acl SSL_ports port 443 acl Safe_ports port 80 # http acl Safe_ports port 21 # ftp acl  
Safe_ports port 443 # https acl Safe_ports port 70 # gopher acl Safe_ports port 210 #  
wais acl Safe_ports port 1025-65535 # unregistered ports acl Safe_ports port 280 #  
http-mgmt acl Safe_ports port 488 # gss-http acl Safe_ports port 591 # filemaker acl  
Safe_ports port 777 # multiling http
```

Tù chối yêu cầu đến các cổng không an toàn

```
http_access deny !Safe_ports http_access deny CONNECT !SSL_ports
```

Cho phép truy cập từ localhost và mạng proxy

```
http_access allow localhost http_access allow proxy_network
```

Cho phép truy cập từ các VLAN

```
http_access allow wlan10_network http_access allow wlan20_network http_access  
allow wlan30_network http_access allow wlan40_network http_access allow  
wlan50_network http_access allow wlan60_network http_access allow wlan70_network  
http_access allow wlan80_network
```

Tù chối tất cả truy cập còn lại

```
http_access deny all
```

Cấu hình bộ nhớ cache

```
cache_dir ufs /var/spool/squid 2000 16 256 cache_mem 512 MB
```

Kích thước đối tượng tối đa được cache

```
maximum_object_size 50 MB
```

Thời gian cache

```
refresh_pattern ^ftp: 1440 20% 10080 refresh_pattern ^gopher: 1440 0% 1440  
refresh_pattern -i (/cgi-bin/|\\?) 0 0% 0 refresh_pattern . 0 20% 4320
```

Log

```
access_log /var/log/squid/access.log
```

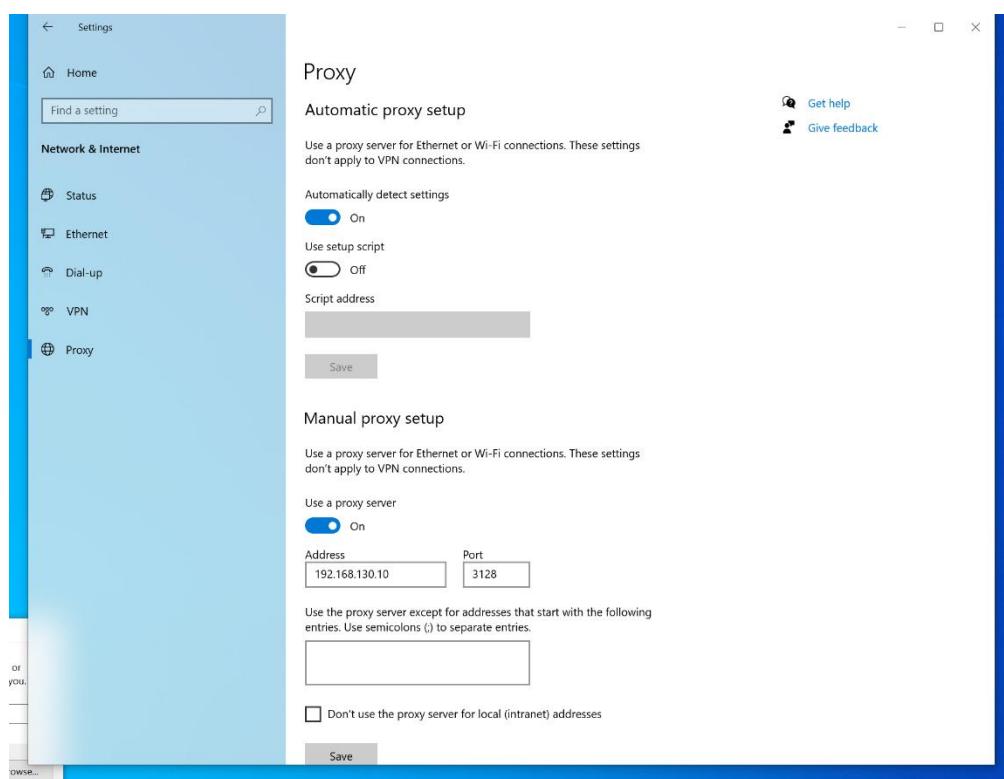
Khởi động Squid:

```
sudo systemctl restart squid sudo systemctl enable squid
```

Cấu hình client trong các VLAN

Trên mỗi máy client trong các VLAN (10-80), cấu hình proxy như sau:

- Proxy server: 192.168.130.10
- Port: 3128

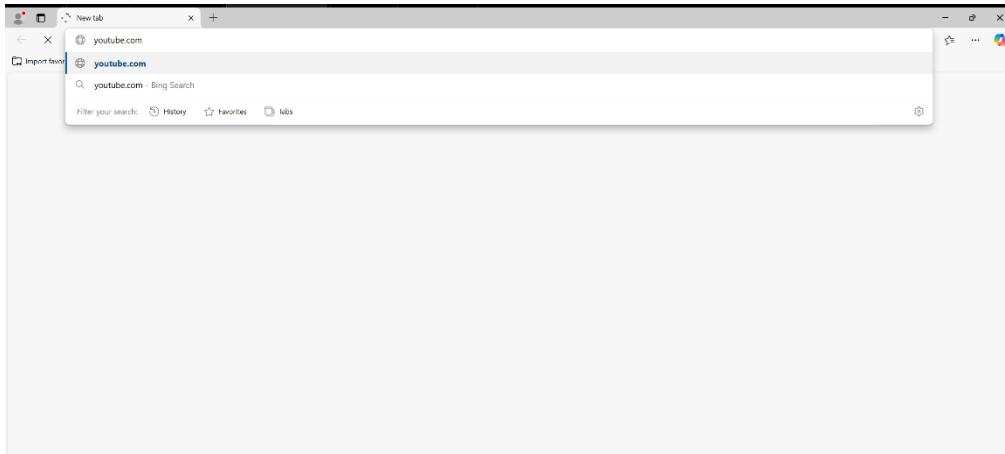


Hình 59. Cấu hình Client

Kiểm tra kết nối

```
sudo tail -f /var/log/squid/access.log
```

Duyệt web trên win10



Hình 60. Thủ duyệt web

Snort bắt được thông tin máy duyệt web

```
1743662140.720 34327 192.168.30.10 TCP_TUNNEL/503 0 CONNECT www.bing.com:443 - HIER_NONE/- -
1743662140.726 34328 192.168.30.10 TCP_TUNNEL/503 0 CONNECT www.bing.com:443 - HIER_NONE/- -
1743662140.726 34419 192.168.30.10 TCP_TUNNEL/503 0 CONNECT www.bing.com:443 - HIER_NONE/- -
1743662140.726 34482 192.168.30.10 TCP_TUNNEL/503 0 CONNECT www.bing.com:443 - HIER_NONE/- -
1743662140.729 35186 192.168.30.10 TCP_MISS_ABORTED/503 4736 GET http://edge.microsoft.com/browsernetworktime/time/1/
current? - HIER_NONE/- text/html
1743662144.890      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT edge.microsoft.com:443 - HIER_NONE/- -
1743662145.074      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT edge.microsoft.com:443 - HIER_NONE/- -
1743662145.721     39994 192.168.30.10 TCP_TUNNEL/503 0 CONNECT copilot.microsoft.com:443 - HIER_NONE/- -
1743662145.721     39600 192.168.30.10 TCP_TUNNEL/503 0 CONNECT config.edge.skype.com:443 - HIER_NONE/- -
1743662145.721     6687 192.168.30.10 TCP_TUNNEL/503 0 CONNECT config.edge.skype.com:443 - HIER_NONE/- -
1743662145.721     39282 192.168.30.10 TCP_TUNNEL/503 0 CONNECT config.edge.skype.com:443 - HIER_NONE/- -
1743662145.820      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT clients2.google.com:443 - HIER_NONE/- -
1743662146.246      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT clients2.google.com:443 - HIER_NONE/- -
1743662149.021      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT config.edge.skype.com:443 - HIER_NONE/- -
1743662149.300      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT edge.microsoft.com:443 - HIER_NONE/- -
1743662149.541      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT edge.microsoft.com:443 - HIER_NONE/- -
1743662150.166      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT config.edge.skype.com:443 - HIER_NONE/- -
1743662150.959      0 192.168.30.10 TCP_TUNNEL/503 0 CONNECT g.live.com:443 - HIER_NONE/- -

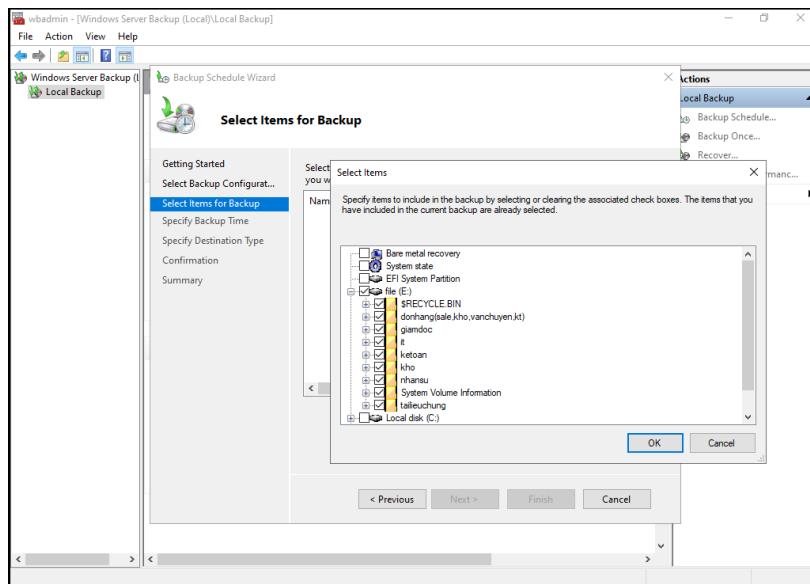
```

Hình 61. Snort bắt gói tin

4.7. Sao lưu và phục hồi

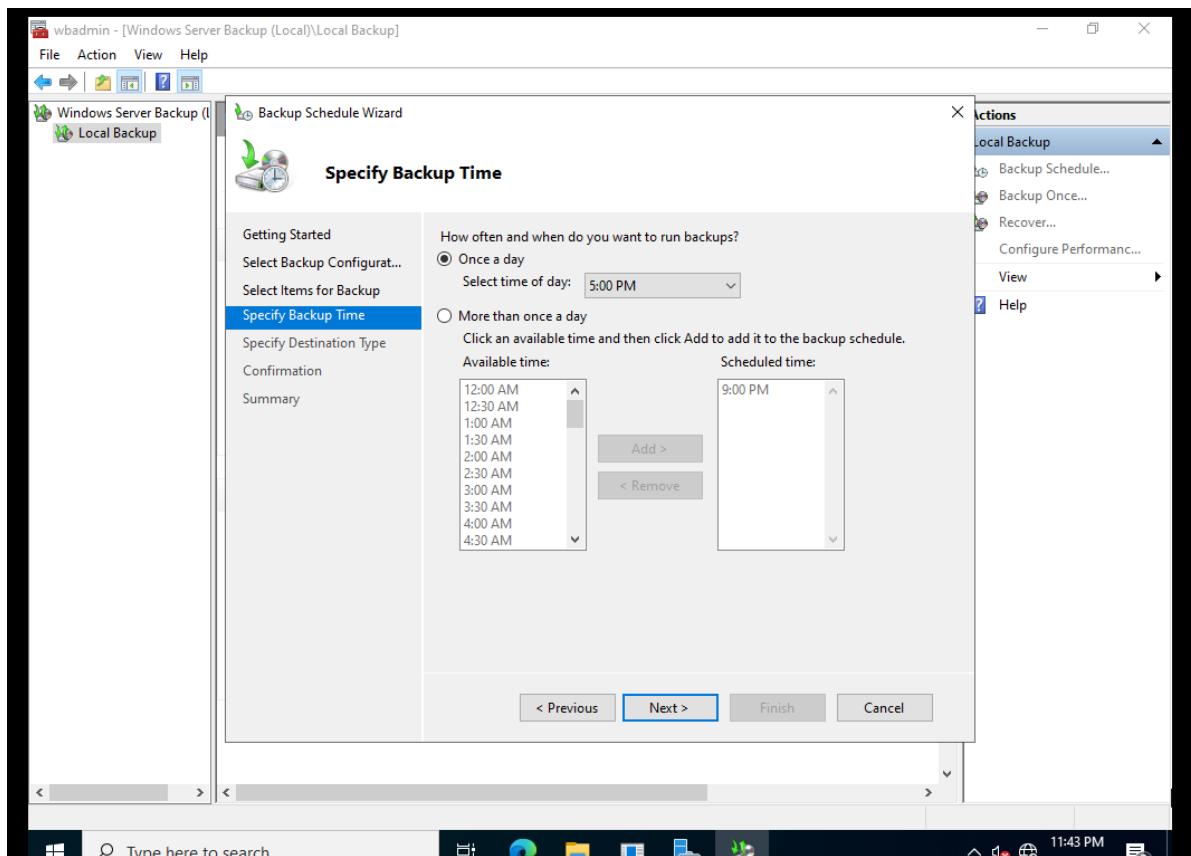
4.7.1. Backup bằng bộ nhớ

- Cài backup window, sau đó chọn ô đĩa chứa file cần backup



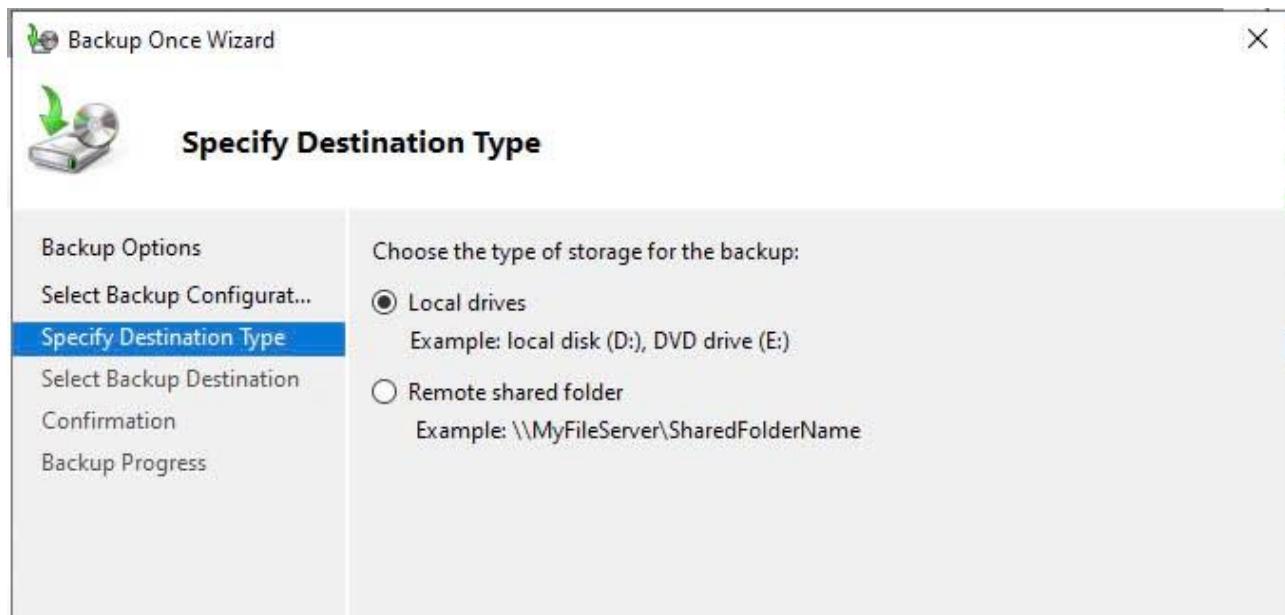
Hình 62. Chọn vị trí để backup

- Chọn thời gian backup mỗi ngày



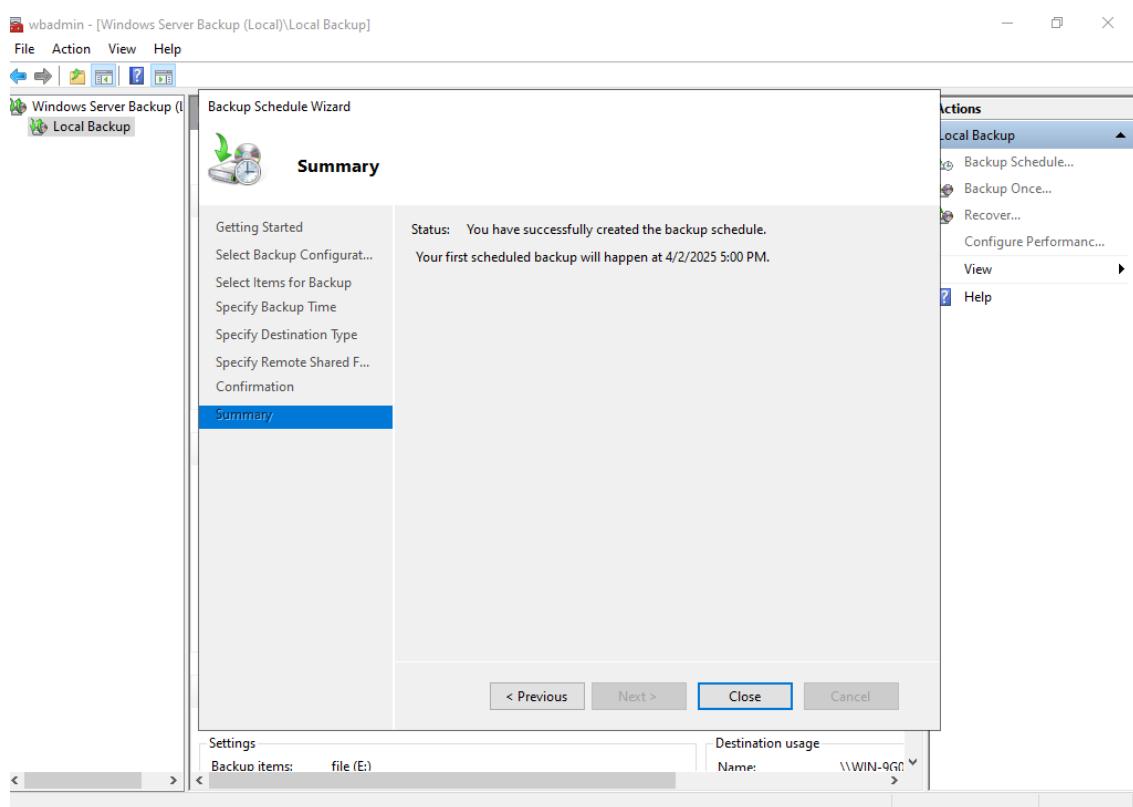
Hình 63. Thiết lập thời gian backup

- Có 2 kiểu lưu file backup, nhưng để đề phòng hư hỏng Server thì lưu vào một file và share file đó để Admin có thể truy cập được



Hình 64. Chọn loại ổ để backup

- Tùy chọn thành công và backup



Hình 65. Thiết lập update thành công

CHƯƠNG V: KẾT LUẬN

5.1. Kết quả triển khai và hướng phát triển

5.1.1. Kết quả đã đạt được

Đề tài đã triển khai thành công các giải pháp bảo mật cơ bản và nâng cao, giúp hệ thống thông tin của doanh nghiệp bán nhạc cụ được bảo vệ toàn diện hơn trước các mối đe dọa mạng. Cụ thể:

- Xây dựng chính sách bảo mật rõ ràng:
 - Đề ra các quy định về quản lý mật khẩu, phân quyền truy cập, xử lý dữ liệu nhạy cảm.
 - Đào tạo nhân viên về nhận thức an ninh mạng (phishing, social engineering).
- Triển khai hệ thống bảo mật vật lý:
 - Lắp đặt camera giám sát, hệ thống kiểm soát ra vào (nếu có trụ sở vật lý).
 - Bảo vệ server/phòng IT bằng khóa RFID hoặc sinh trắc học.
- Triển khai tường lửa (pfSense):
 - Ngăn chặn truy cập trái phép từ bên ngoài.
 - Cấu hình rules để kiểm soát lưu lượng mạng (chặn cổng không cần thiết, giới hạn IP truy cập).
- Hệ thống phát hiện xâm nhập (IDS - Snort):
 - Giám sát lưu lượng mạng, phát hiện tấn công như DDoS, brute force, malware.
 - Cảnh báo real-time khi có hoạt động đáng ngờ.
- Honeypot (bẫy mạng):
 - Đánh lừa hacker, thu thập thông tin về phương thức tấn công.
 - Phân tích xu hướng tấn công để cải thiện hệ thống phòng thủ.

Tuy nhiên vẫn còn nhiều hạn chế, và nhiều chức năng nhóm chưa thể hoàn thành được:

- Chưa cài đặt cũng như cấu hình Proxy, chưa có VPN
- Hệ thống Honey Pots và IDS(Snort) cần đội ngũ chuyên môn cao
- Hiện tại, hệ thống chưa triển khai các giải pháp giám sát hiệu năng mạng (Network Performance Monitoring)
- Mặc dù hệ thống mạng nội bộ đã được xây dựng mạnh mẽ, việc tích hợp các dịch vụ cloud (như Azure, AWS, Google Cloud) để tăng tính linh hoạt và khả năng lưu trữ dữ liệu cũng như bảo mật còn hạn chế.
- Hiện chưa có phân tích đầy đủ về tối ưu chi phí cho hệ thống, khiến việc đưa vào thực tế có thể bị tiêu tốn tài chính
- Đã triển khai nhiều biện pháp bảo mật nhưng chưa có biện pháp DDoS protection, và công nghệ zero-trust chưa được triển khai triệt để. Điều này có thể gây rủi ro nếu gặp phải các mối đe dọa mạng phức tạp trong tương lai.

5.1.2. Hướng phát triển trong tương lai

Để nâng cao hơn nữa khả năng bảo mật, doanh nghiệp cần:

- Nâng cấp lên hệ thống IPS (Ngăn chặn xâm nhập): Không chỉ phát hiện mà còn tự động chặn tấn công.
- Áp dụng AI/ML trong giám sát an ninh:
- Dùng trí tuệ nhân tạo để phân tích hành vi bất thường (VD: đăng nhập từ nhiều địa điểm khác nhau trong thời gian ngắn).
- Tích hợp với SIEM (Security Information and Event Management) để tổng hợp và phân tích log tập trung.

Mở rộng bảo mật ứng dụng web:

- Kiểm thử pentest định kỳ để phát hiện lỗ hổng trên website bán hàng.
- Triển khai WAF (Web Application Firewall) nếu chưa có.

Tuân thủ tiêu chuẩn quốc tế:

- Áp dụng ISO 27001 hoặc PCI DSS (nếu xử lý thanh toán thẻ tín dụng).

5.1.3. Kết luận

Đề tài đã thiết lập được nền tảng bảo mật cơ bản, giúp doanh nghiệp giảm thiểu rủi ro về rò rỉ dữ liệu và tấn công mạng. Trong tương lai, việc kết hợp công nghệ tiên tiến (AI, IPS) và đào tạo nhân sự sẽ giúp hệ thống trở nên vững chắc hơn, đáp ứng các mối đe dọa ngày càng tinh vi.

5.2. Bảng phân công

Họ và tên	MSSV	Công việc	% hoàn thành
Trần Quang Khải	22DH114583	Cấu hình, triển khai hệ thống	100%
Đào Đức Lương	22DH114621	Cấu hình, triển khai hệ thống	100%
Ngô thê Đức	22DH114504	Thiết kế hệ thống, viết báo cáo	100%

5.3. Tài liệu tham khảo

Các tài liệu dưới đây có thể là không đầy đủ vì có những tài liệu đã bị gỡ:

<https://nplaw.vn/bao-mat-thong-tin-trong-doanh-nghiep.html>

<https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-53-2022-ND-CP-huong-dan-Luat-An-ninh-mang-398695.aspx>

<https://chatgpt.com/>

<https://chat.deepseek.com/>

<https://www.youtube.com/@warencenter2049>

<https://www.bitdefender.vn/post/security-for-small-business/>