

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
THÔNG THÔNG TIN DOANH NGHIỆP KINH DOANH
LINH KIỆN MÁY TÍNH

Giảng Viên Hướng Dẫn : ThS. Đinh Xuân Lâm

Thành Viên :

1. Lê Thành Đạt – MSSV: 22DH110717
2. Huỳnh Minh Nhựt – MSSV: 22DH112633
3. Phạm Hoàng Gia Bảo – MSSV: 22DH110298
4. Dương Lê Huy Hoàng – MSSV: 22DH114536

TP. Hồ chí minh, Ngày 18 tháng 03 năm 2025

DANH MỤC

Mục Lục

LỜI CẢM ƠN.....	9
LỜI NÓI ĐẦU.....	10
CHƯƠNG 1: GIỚI THIỆU DOANH NGHIỆP	11
1. Lĩnh vực.....	11
2. Tổ chức và quy mô	11
3. Hoạt động sản xuất.....	12
4. Mục tiêu.....	12
CHƯƠNG 2: LÝ THUYẾT TỔNG QUAN.....	13
1. Các dịch vụ triển khai	13
a. ADDS (Active Directory Domain Services).....	13
b. DNS (Domain Name System).....	13
c. DHCP (Dynamic Host Configuration Protocol)	14
d. File Server.....	14
e. IIS (Internet Information Services)	14
2. Các dịch vụ bảo mật mạng	15
a. VPN (Virtual Private Network).....	15
b. Proxy	15
c. Firewall	16
d. IDS (Intrusion Detection System)	16
e. IPS (Intrusion Prevention System)	16

3. Các mối đe doạ	17
a. Mã độc (Malware)	17
b. Tấn công mạng	17
c. Lỗ hổng bảo mật	18
d. Tấn công kỹ thuật xã hội	18
e. Rò rỉ dữ liệu	19

CHƯƠNG 3: XÂY DỰNG VÀ TRIỂN KHAI BIỆN PHÁP BẢO MẬT 19

1. Yêu cầu kĩ thuật của doanh nghiệp	19
a. Yêu cầu nghiệp vụ kinh doanh	19
b. Yêu cầu kĩ thuật	20
2. Xây dựng giải pháp	20
a. Sơ đồ vật lý	20
b. Sơ đồ logic	22
3. Chính sách bảo mật	23
a. Chính sách bảo mật vật lý	23
b. Chính sách bảo mật hệ điều hành	25
c. Chính sách bảo mật mạng	26
d. Chính sách phục hồi sau thảm họa	27
4. Sơ đồ logic triển khai demo	27
5. Triển khai	28
a. Bảo mật vật lý	28
b. Bảo mật hệ điều hành	32
c. Bảo mật mạng	40

6.	Kết quả triển khai.....	50
a.	Bảo mật vật lý.....	50
b.	Bảo mật hệ điều hành	81
c.	Bảo mật mạng	93
7.	Kết luận	99
BẢNG PHÂN CÔNG VIỆC.....		100
TÀI LIỆU THAM KHẢO		101

DANH MỤC HÌNH ẢNH

Hình 1. Tầng 1	21
Hình 2. Tầng 2	21
Hình 3. Tầng 3	22
Hình 4. Tầng 4	22
Hình 5. Sơ đồ logic thực tế	23
Hình 6. Sơ đồ Logic Demo	28
Hình 7. Phòng trưng bày	28
Hình 8. Phòng kho	29
Hình 9. Camera thu ngân và tổng quát	29
Hình 10. Quan sát cửa ra vào	30
Hình 11. Camera giám góc chéo	30
Hình 12. Quan sát khu trưng bày	30
Hình 13. Tầng 2	31
Hình 14. Tầng 3	31
Hình 15. Tầng 4	32
Hình 16. Triển khai group policy hiện thị ổ làm việc theo phòng ban	32
Hình 17. GPO cho tài khoản nhân viên	33
Hình 18. Ân firewall	34
Hình 19. Ân control pannel	35
Hình 20. Vô hiệu hoá taskmanager	36
Hình 21. Cấm cắm usb vào	37

Hình 22. Backup cho dữ liệu	38
Hình 23. Cảm các file thực thi	39
Hình 24. Phân ngạch ổ đĩa	40
Hình 25. Firewall cho mạng Wan.....	41
Hình 26. Firewall mạng Lan	42
Hình 27. Firewall cho mạng domain	43
Hình 28. Firewall cho web.....	44
Hình 29. Firewall cho wifi	45
Hình 30. Aliases.....	46
Hình 31. Suricata và Squid	47
Hình 32. Rule test thử suricata.....	48
Hình 33. Cài đặt các trang chặn bằng squid	49
Hình 34. Thêm proxy vào máy client	50
Hình 35. Camera 4 trưng bày.....	51
Hình 36. Cam 1 trưng bày	52
Hình 37. Cam 7 trưng bày	53
Hình 38. Cam 8 trưng bày	54
Hình 39. Cam 2 kho	55
Hình 40. Cam 3 kho	56
Hình 41. Cam 4 kho	57
Hình 42. Cam 5 kho	58
Hình 43. Cam 1 Thu ngân.....	59
Hình 44. Cam 2 Thu ngân.....	60

Hình 45. Cam 3 thu ngân	61
Hình 46. Cam 1 cửa	62
Hình 47. Cam 2 cửa	63
Hình 48. Cam 3 cửa	64
Hình 49. Cam 1 giảm góc chét	65
Hình 50. Cam 3 giảm góc chét	66
Hình 51. Cam 4 giảm góc chét	67
Hình 52. Cam 5 giảm góc chét	68
Hình 53. Cam 4 trưng bày	69
Hình 54. Cam 3 trưng bày	70
Hình 55. Camera marketing- kinh doanh	71
Hình 56. Cam hành lang tầng 2	72
Hình 57. Cam phòng họp	73
Hình 58. Cam chăm sóc khách hàng	74
Hình 59. Cam tài chính kế toán	75
Hình 60. Cam phòng IT	76
Hình 61. Cam hành lang tầng 3	77
Hình 62. Cam hành lang tầng 4	78
Hình 63. Cam phòng nhân sự	79
Hình 64. Cam phòng nghỉ nữ	80
Hình 65. Cam phòng nghỉ nam	81
Hình 66. Kết quả triển khai map ô đĩa	82
Hình 67. Thư mục share của kế toán	82

Hình 68. Mật khẩu đổi lại phải đúng định dạng	83
Hình 69. Tắt TaskManager	84
Hình 70. Không thể truy cập control panel.....	85
Hình 71. Back up theo ngày.....	86
Hình 72. Khi dữ liệu chung bị mất	87
Hình 73. Khôi phục thành công	88
Hình 74. Không thể chép file thực thi vào thư mục của công ty	89
Hình 75. Giới hạn ngạch của từng phòng	90
Hình 76. Tài khoản không của phòng ban nào không thể truy cập tới thư mục của ban khác.....	91
Hình 77. Giám đốc có thể xem toàn bộ dữ liệu nhân viên	92
Hình 78. Truy cập bằng địa chỉ ip vẫn thấy được bằng tài khoản giám đốc	93
Hình 79. Mạng Lan có thể vô trang web của công ty	94
Hình 80. Mạng Lan vô được trang Facebook	94
Hình 81. Mạng Lan có thể vô được trang gmail	95
Hình 82. Máy wifi không thể truy cập tới file server	95
Hình 83. Máy wifi có thể truy cập tất cả web bình thường	96
Hình 84. Máy wifi có thể vô trang web của công ty.....	96
Hình 85. Máy wifi không thể ping tới domain và phân giải tên miền domain.....	97
Hình 86. Suricata chạy ở cổng wifi	97
Hình 87. Cảnh báo của suricata	98
Hình 88. Chặn bằng squid.....	99

LỜI CẢM ƠN

Nhóm em xin được bày tỏ lòng tôn trọng và biết ơn sâu sắc đến giảng viên Đinh Xuân Lâm – giảng viên tại trường Đại học Ngoại ngữ - Tin học Tp.HCM vì đã luôn nhiệt tình hỗ trợ và chỉ dạy những kiến thức vô cùng bổ ích cho việc học tập và thực hiện đồ án của chúng em. Nhờ có sự nhắc nhở và góp ý từ thầy mà đồ án này có thể từ từ được hoàn thiện và phát triển. Sự tận tâm cùng trái tim đầy nhiệt huyết trong việc dẫn dắt và cung cấp những kinh nghiệm, những bài học quan trọng mà chúng em có thêm động lực và kiến thức để làm nên đồ án này.

Mặc dù đã nỗ lực cố gắng nhưng do thời gian và kiến thức có hạn nên trong quá trình thực hiện đồ án khó tránh khỏi sai sót nên nhóm em rất mong có được thêm nhiều những góp ý chân thành đến từ thầy để đồ án có thể tiếp tục được phát triển và hoàn thiện hơn trong tương lai.

Nhóm em xin chân thành cảm ơn thầy ạ!

LỜI NÓI ĐẦU

Trong kỷ nguyên chuyển đổi số, hệ thống thông tin đã trở thành nền tảng cốt lõi trong mọi hoạt động doanh nghiệp. Điều này đặc biệt đúng đối với các doanh nghiệp kinh doanh trong lĩnh vực công nghệ như công ty kinh doanh linh kiện PC. Tuy nhiên, sự gia tăng không ngừng của các mối đe dọa an ninh mạng đặt ra yêu cầu cấp thiết về việc xây dựng một chiến lược bảo mật chặt chẽ và toàn diện.

Theo nghiên cứu của IBM, thiệt hại trung bình do các cuộc tấn công mạng toàn cầu năm 2023 đã đạt 4,35 triệu USD trên mỗi doanh nghiệp - một con số đáng báo động, cho thấy rõ tầm quan trọng của việc bảo vệ hệ thống thông tin doanh nghiệp. Đối với doanh nghiệp kinh doanh linh kiện PC, việc bảo mật không chỉ giúp bảo vệ dữ liệu nội bộ mà còn bảo vệ thông tin khách hàng, đảm bảo hoạt động kinh doanh liên tục và duy trì uy tín trên thị trường.

Quy trình bảo mật hệ thống thông tin là chuỗi các bước được thiết kế thực hiện một cách có hệ thống nhằm bảo vệ tài sản số của doanh nghiệp khỏi các mối đe dọa an ninh mạng. Quy trình này không chỉ bao gồm việc phát hiện, ngăn chặn mà còn đảm bảo khả năng ứng phó hiệu quả, phục hồi nhanh chóng sau sự cố, từ đó duy trì tính toàn vẹn, tính bảo mật và khả năng sẵn sàng của hệ thống thông tin.

Đồ án này trình bày chiến lược bảo mật toàn diện cho doanh nghiệp kinh doanh linh kiện PC, bao gồm các biện pháp bảo mật vật lý, bảo mật hệ điều hành và bảo mật mạng. Mục tiêu là tạo ra một hệ thống phòng thủ nhiều lớp, có khả năng phát hiện, ngăn chặn và ứng phó hiệu quả với các mối đe dọa an ninh mạng, đồng thời đảm bảo tính liên tục của hoạt động kinh doanh.

CHƯƠNG 1: GIỚI THIỆU DOANH NGHIỆP

1. Lĩnh vực

Công ty HufTech là doanh nghiệp chuyên kinh doanh linh kiện PC tại Việt Nam. Được thành lập vào năm 2024, công ty đã nhanh chóng phát triển và khẳng định vị thế trên thị trường với các sản phẩm chất lượng cao và dịch vụ chuyên nghiệp.

Các sản phẩm chính của công ty bao gồm:

- CPU (Intel, AMD)
- Mainboard (Asus, Gigabyte, MSI)
- RAM (Corsair, Kingston, G.Skill)
- Card đồ họa (Nvidia, AMD)
- Ổ cứng SSD và HDD (Samsung, Western Digital, Seagate)
- Nguồn máy tính (Corsair, EVGA, Seasonic)
- Vỏ case và các thiết bị làm mát
- Màn hình và các thiết bị ngoại vi

Ngoài việc kinh doanh linh kiện, công ty còn cung cấp các dịch vụ:

- Lắp ráp và cấu hình hệ thống máy tính theo yêu cầu
- Bảo hành và sửa chữa
- Tư vấn giải pháp công nghệ cho doanh nghiệp và cá nhân
- Dịch vụ bảo trì và nâng cấp hệ thống

2. Tổ chức và quy mô

Công ty HufTech có trụ sở chính tại thành phố Hồ Chí Minh. Tổng số nhân viên hiện tại là 98 người, phân bổ tại các phòng ban như sau:

- Ban Giám đốc: 1 người (Giám đốc điều hành)
- Phòng Kinh doanh – Marketing: 10 người
- Phòng Chăm sóc khách hàng: 20 người
- Phòng IT: 25 người (phụ trách hệ thống CNTT nội bộ và website)
- Phòng Kế toán - Tài chính: 10 người
- Phòng Nhân sự: 7 người

- Thu ngân: 5 người
- Kho và Logistic: 20 người

Mỗi chi nhánh có một trưởng chi nhánh và các nhân viên thuộc các bộ phận kinh doanh, kỹ thuật và hành chính. Sơ đồ tổ chức của công ty theo mô hình phân cấp quản lý, với các phòng ban báo cáo trực tiếp cho Ban Giám đốc.

3. Hoạt động sản xuất

Công ty HufTech không trực tiếp sản xuất linh kiện mà hoạt động theo mô hình nhập khẩu và phân phối. Quy trình kinh doanh chính của công ty bao gồm:

- Nhập khẩu linh kiện từ các nhà sản xuất uy tín trên thế giới
- Kiểm tra chất lượng và lưu kho
- Phân phối đến các chi nhánh và đại lý
- Bán hàng trực tiếp tại showroom và qua kênh online
- Cung cấp dịch vụ sau bán hàng

Công ty vận hành hệ thống website thương mại điện tử riêng và có mặt trên các sàn TMĐT lớn như Shopee, Lazada, Tiki. Doanh thu trực tuyến chiếm khoảng 40% tổng doanh thu của công ty và đang có xu hướng tăng.

Hoạt động kinh doanh của công ty phụ thuộc rất nhiều vào hệ thống công nghệ thông tin, bao gồm:

- Hệ thống quản lý kho (WMS)
- Hệ thống quản lý quan hệ khách hàng (CRM)
- Hệ thống kế toán và quản lý tài chính (ERP)
- Website thương mại điện tử và hệ thống xử lý đơn hàng
- Mạng nội bộ kết nối các phòng ban và chi nhánh

Vì vậy, bảo mật hệ thống thông tin là yếu tố then chốt đảm bảo hoạt động kinh doanh liên tục và bảo vệ dữ liệu quan trọng của công ty.

4. Mục tiêu

- Bảo vệ các linh kiện của công ty
- Chống việc truy cập bất hợp pháp vào những kho linh kiện hoặc phòng dữ liệu

- Chống việc các thông tin nội bộ công ty bị đưa ra ngoài
- Chống việc mất tài sản của khách hàng khi đến công ty
- Chống việc có virus ảnh hưởng tới dữ liệu của công ty
- Chống việc mất dữ liệu khách hàng và các linh kiện của công ty
- Chống việc truy cập bất hợp pháp vào domain của công ty
- Backup lại cơ sở dữ liệu của công ty

CHƯƠNG 2: LÝ THUYẾT TỔNG QUAN

1. Các dịch vụ triển khai

a. ADDS (Active Directory Domain Services)

- **Giới thiệu:** ADDS là một thành phần chính của Active Directory, cho phép người dùng xác thực và truy cập tài nguyên trên mạng. Nó tổ chức các đối tượng thành một cấu trúc phân cấp, giúp quản lý và lưu trữ thông tin về người dùng, thiết bị, và dịch vụ trên mạng.
- **Chức năng:** ADDS cung cấp dịch vụ xác thực, kiểm soát truy cập, và quản lý các tài nguyên mạng. Nó cho phép tạo ra một cấu trúc tổ chức linh hoạt và cung cấp một điểm truy cập duy nhất vào các tài nguyên mạng.
- **Lợi ích:** Cung cấp cấu trúc phân cấp, linh hoạt trong việc tổ chức dữ liệu, tạo điểm truy cập duy nhất, và có tính dự phòng cao.

b. DNS (Domain Name System)

- **Giới thiệu:** DNS là một cơ sở dữ liệu tên miền giúp chuyển đổi tên miền thành địa chỉ IP mà máy tính có thể hiểu được. Nó cho phép người dùng truy cập vào các trang web và tài nguyên mạng bằng tên miền thay vì địa chỉ IP.
- **Chức năng:** DNS thực hiện việc phân giải tên miền thành địa chỉ IP thông qua một quá trình gọi là "DNS resolution". Quá trình này bao gồm việc gửi yêu cầu đến các máy chủ DNS để tìm địa chỉ IP tương ứng với tên miền được nhập vào trình duyệt.

- **Lợi ích:** Giúp người dùng truy cập dễ dàng vào các trang web và tài nguyên mạng mà không cần nhớ địa chỉ IP phức tạp.

c. DHCP (Dynamic Host Configuration Protocol)

- **Giới thiệu:** DHCP là một giao thức máy khách/máy chủ tự động cung cấp địa chỉ IP và thông tin cấu hình liên quan cho các thiết bị trên mạng. Nó giúp giảm thiểu sai sót cấu hình thủ công và xung đột địa chỉ IP.
- **Chức năng:** DHCP cung cấp các địa chỉ IP và thông tin cấu hình TCP/IP cho các thiết bị trên mạng. Nó cho phép quản lý tập trung và tự động hóa việc cấp phát địa chỉ IP.
- **Lợi ích:** Cung cấp cấu hình IP đáng tin cậy, giảm thiểu quản lý mạng, và hỗ trợ việc di chuyển thiết bị giữa các mạng khác nhau.

d. File Server

- **Giới thiệu:** File Server là một máy chủ trung tâm trong mạng máy tính, cho phép các thiết bị kết nối truy cập vào khả năng lưu trữ của nó. Nó cung cấp một không gian lưu trữ tập trung cho các tệp và thư mục.
- **Chức năng:** File Server cho phép người dùng lưu trữ, chia sẻ, và quản lý tệp trên mạng. Nó cũng có thể được sử dụng để lưu trữ các chương trình và làm máy chủ sao lưu.
- **Lợi ích:** Cung cấp không gian lưu trữ tập trung, cho phép truy cập từ xa, và giúp quản lý quyền truy cập vào các tệp và thư mục.

e. IIS (Internet Information Services)

- **Giới thiệu:** IIS là một máy chủ web của Microsoft, chạy trên hệ điều hành Windows, được sử dụng để trao đổi nội dung web tĩnh và động với người dùng internet. Nó hỗ trợ các công nghệ như ASP.NET và PHP.
- **Chức năng:** IIS được sử dụng để lưu trữ, triển khai, và quản lý các ứng dụng web. Nó hỗ trợ các giao thức như HTTP, SMTP, và FTP.
- **Lợi ích:** Cung cấp bảo mật mạnh mẽ, hỗ trợ đa dạng các ứng dụng web, và có khả năng mở rộng quy mô và độ tin cậy cao.

2. Các dịch vụ bảo mật mạng

a. VPN (Virtual Private Network)

VPN là công nghệ tạo kết nối mạng riêng ảo an toàn qua một mạng công cộng như Internet. VPN hoạt động bằng cách mã hóa lưu lượng truy cập và ẩn địa chỉ IP thực của người dùng.

Lợi ích của VPN trong doanh nghiệp kinh doanh linh kiện PC:

- Bảo mật kết nối từ xa cho nhân viên tại các chi nhánh hoặc đang di chuyển
- Kết nối an toàn giữa trụ sở chính và các chi nhánh
- Bảo vệ dữ liệu nhạy cảm như thông tin khách hàng và chiến lược kinh doanh khi truyền qua mạng không an toàn
- Truy cập an toàn vào các hệ thống nội bộ như WMS, CRM và ERP từ bên ngoài

Các loại VPN phổ biến bao gồm Site-to-Site VPN, Remote Access VPN, và SSL VPN, mỗi loại có ứng dụng phù hợp với các nhu cầu khác nhau của doanh nghiệp.

b. Proxy

Proxy là một máy chủ trung gian giữa người dùng và Internet. Khi người dùng gửi yêu cầu truy cập, proxy sẽ chuyển tiếp yêu cầu đó đến máy chủ đích, nhận phản hồi và gửi lại cho người dùng.

Vai trò của proxy trong bảo mật hệ thống doanh nghiệp:

- Ẩn địa chỉ IP của mạng nội bộ
- Lọc nội dung và kiểm soát truy cập Internet của nhân viên
- Tăng tốc truy cập web thông qua bộ nhớ cache
- Ghi nhật ký hoạt động truy cập để phát hiện hành vi đáng ngờ
- Ngăn chặn truy cập vào các trang web độc hại có thể chứa mã độc

Các loại proxy phổ biến bao gồm Forward Proxy, Reverse Proxy, Transparent Proxy và SOCKS Proxy, mỗi loại phục vụ các mục đích khác nhau trong chiến lược bảo mật.

c. Firewall

Firewall là hệ thống bảo mật mạng hoạt động như một rào chắn giữa mạng nội bộ đáng tin cậy và mạng bên ngoài không đáng tin cậy như Internet. Theo kết quả tìm kiếm, firewall là một trong những giải pháp bảo mật quan trọng nhất cho doanh nghiệp³.

Chức năng chính của firewall:

- Kiểm soát lưu lượng truy cập dựa trên quy tắc đã được thiết lập
- Ngăn chặn truy cập trái phép vào mạng nội bộ
- Phát hiện và chặn các cuộc tấn công mạng
- Giám sát và ghi nhật ký hoạt động mạng

Các loại firewall bao gồm Packet Filtering Firewall, Stateful Inspection Firewall, Application Layer Firewall và Next-Generation Firewall (NGFW). Đối với doanh nghiệp kinh doanh linh kiện PC, NGFW là lựa chọn phù hợp vì tích hợp nhiều tính năng bảo mật tiên tiến.

d. IDS (Intrusion Detection System)

IDS là hệ thống phát hiện xâm nhập, có khả năng giám sát lưu lượng mạng và hoạt động hệ thống để phát hiện các hoạt động đáng ngờ hoặc vi phạm chính sách bảo mật.

Đặc điểm của IDS:

- Chủ yếu là giám sát và cảnh báo, không chủ động ngăn chặn
- Phát hiện các mẫu tấn công đã biết và hành vi bất thường
- Lưu trữ nhật ký chi tiết về các sự kiện bảo mật

Các loại IDS bao gồm Network-based IDS (NIDS), Host-based IDS (HIDS), Signature-based IDS và Anomaly-based IDS, mỗi loại có ưu điểm riêng trong việc phát hiện các loại tấn công khác nhau.

e. IPS (Intrusion Prevention System)

IPS là hệ thống phòng chống xâm nhập, tiến thêm một bước so với IDS bằng cách không chỉ phát hiện mà còn chủ động ngăn chặn các cuộc tấn công.

Đặc điểm của IPS:

- Chủ động ngăn chặn các cuộc tấn công đã phát hiện
 - Có thể chặn lưu lượng độc hại trong thời gian thực
 - Thường được tích hợp với firewall trong các giải pháp bảo mật hiện đại
- Các loại IPS bao gồm Network-based IPS, Host-based IPS, Wireless IPS và Behavior-based IPS. Đối với doanh nghiệp kinh doanh linh kiện PC, việc kết hợp các loại IPS khác nhau sẽ tạo ra một hệ thống phòng thủ toàn diện.

3. Các mối đe dọa

a. Mã độc (Malware)

Mã độc là phần mềm được thiết kế với mục đích gây hại cho hệ thống, bao gồm:

- Virus: lây nhiễm vào các tệp và chương trình khác
- Worm: tự nhân bản và lây lan qua mạng
- Trojan: giả dạng phần mềm hợp pháp nhưng thực hiện các hoạt động độc hại
- Ransomware: mã hóa dữ liệu và đòi tiền chuộc
- Spyware: theo dõi hoạt động của người dùng
- Adware: hiển thị quảng cáo không mong muốn
- Rootkit: giúp kẻ tấn công duy trì quyền truy cập vào hệ thống

Đối với doanh nghiệp kinh doanh linh kiện PC, mã độc có thể xâm nhập thông qua nhiều con đường như email, thiết bị USB, trang web độc hại, hoặc phần mềm bị nhiễm. Việc bảo vệ chống lại mã độc đòi hỏi một cách tiếp cận nhiều lớp, kết hợp giữa phần mềm bảo vệ và nhận thức của người dùng.

b. Tấn công mạng

Các hình thức tấn công mạng phổ biến đe dọa doanh nghiệp kinh doanh linh kiện PC:

- Tấn công từ chối dịch vụ (DDoS): làm quá tải hệ thống, đặc biệt nguy hiểm đối với website bán hàng
- Tấn công man-in-the-middle: chặn và sửa đổi thông tin truyền giữa khách hàng và hệ thống thanh toán

- Tấn công brute force: thử nhiều mật khẩu để đoán ra mật khẩu của tài khoản quản trị
- Tấn công SQL injection: chèn mã độc vào các truy vấn SQL, nhảm vào website và hệ thống cơ sở dữ liệu
- Cross-site scripting (XSS): chèn mã độc vào các trang web, có thể đánh cắp phiên làm việc của khách hàng
- Cross-site request forgery (CSRF): lợi dụng quyền của người dùng đã đăng nhập để thực hiện các hành động trái phép
- DNS spoofing: chuyển hướng lưu lượng đến các trang web giả mạo để đánh cắp thông tin đăng nhập

c. Lỗ hổng bảo mật

Lỗ hổng bảo mật là điểm yếu trong hệ thống có thể bị khai thác để thực hiện các cuộc tấn công:

- Lỗi trong phần mềm chưa được cập nhật kịp thời
- Lỗi cấu hình sai trong hệ thống mạng và máy chủ
- Mật khẩu yếu hoặc mặc định chưa được thay đổi
- Quyền truy cập được cấp quá mức cần thiết
- Thiếu mã hóa dữ liệu nhạy cảm như thông tin khách hàng và giao dịch
- API không được bảo vệ đúng cách
- Giao diện quản trị không an toàn và dễ bị tấn công

d. Tấn công kỹ thuật xã hội

Tấn công kỹ thuật xã hội là các phương pháp lừa đảo nhắm vào con người thay vì khai thác lỗ hổng kỹ thuật:

- Phishing: giả mạo email hoặc trang web để đánh cắp thông tin đăng nhập
- Spear phishing: phishing nhắm vào đối tượng cụ thể như quản lý cấp cao
- Pretexting: tạo ra tình huống giả để lấy thông tin nhạy cảm
- Baiting: dụ người dùng bằng những thứ hấp dẫn như phần mềm "miễn phí"
- Tailgating: theo sau người khác để truy cập vào khu vực hạn chế

Đối với doanh nghiệp kinh doanh linh kiện PC, nhân viên là tuyến phòng thủ quan trọng trước các cuộc tấn công kỹ thuật xã hội. Đào tạo nhận thức bảo mật thường xuyên là biện pháp then chốt để giảm thiểu rủi ro này.

e. Rò rỉ dữ liệu

Rò rỉ dữ liệu xảy ra khi thông tin nhạy cảm của doanh nghiệp và khách hàng bị tiết lộ:

- Mất hoặc đánh cắp thiết bị lưu trữ như laptop hay ổ cứng di động
- Chia sẻ dữ liệu không đúng cách qua email hoặc dịch vụ lưu trữ đám mây không an toàn
- Người trong tổ chức cố ý rò rỉ thông tin nhạy cảm
- Lỗi cấu hình dẫn đến dữ liệu được công khai không chủ ý

CHƯƠNG 3: XÂY DỰNG VÀ TRIỂN KHAI BIỆN PHÁP BẢO MẬT

1. Yêu cầu kỹ thuật của doanh nghiệp

a. Yêu cầu nghiệp vụ kinh doanh

Công ty HufTech cần một hệ thống bảo mật đáp ứng các yêu cầu nghiệp vụ sau:

- Đảm bảo hoạt động kinh doanh liên tục 24/7, đặc biệt là hệ thống thương mại điện tử và xử lý đơn hàng
- Bảo vệ thông tin khách hàng và dữ liệu thanh toán theo các quy định pháp luật về bảo vệ dữ liệu cá nhân
- Đảm bảo tính toàn vẹn của dữ liệu kho hàng và đơn hàng để tránh sai sót trong kinh doanh
- Bảo vệ bí mật kinh doanh, chiến lược phát triển và dữ liệu marketing
- Tuân thủ các quy định về bảo vệ dữ liệu cá nhân và an toàn thông tin

Việc đảm bảo các yêu cầu này sẽ giúp công ty duy trì uy tín với khách hàng, tăng cường niềm tin của đối tác, và đảm bảo sự phát triển bền vững trong môi trường kinh doanh cạnh tranh.

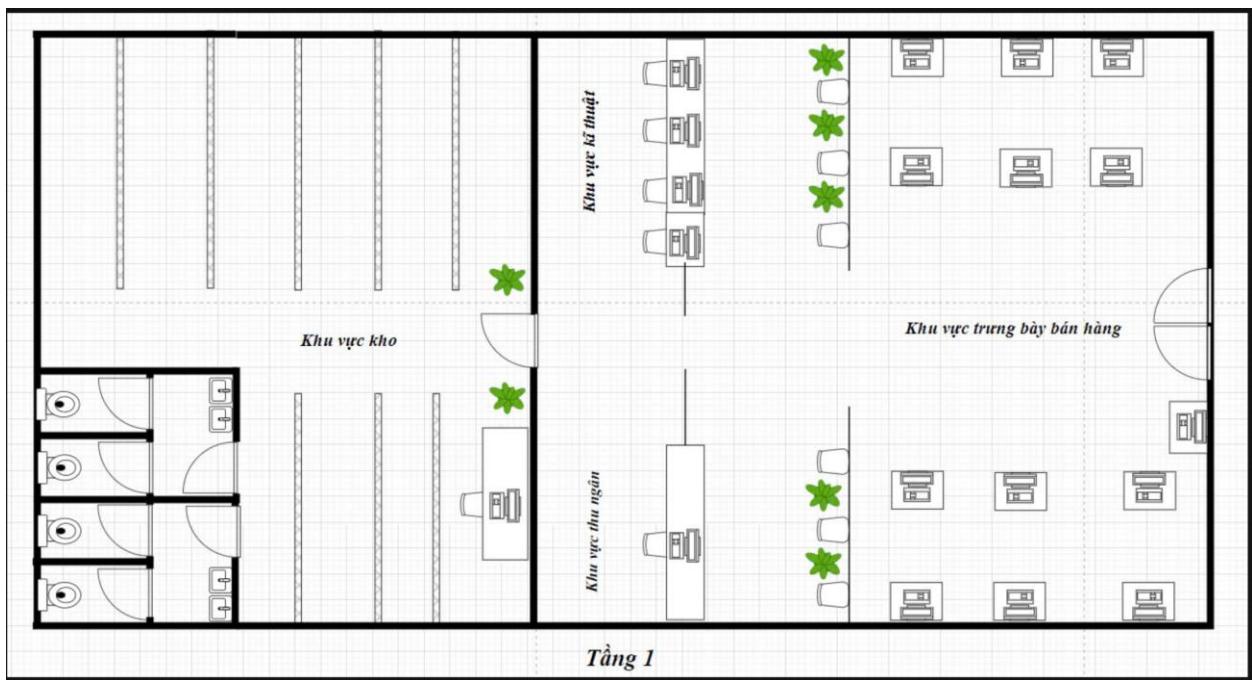
b. Yêu cầu kỹ thuật

Để đáp ứng các yêu cầu nghiệp vụ trên, hệ thống bảo mật của TechComponents cần có các đặc điểm kỹ thuật sau:

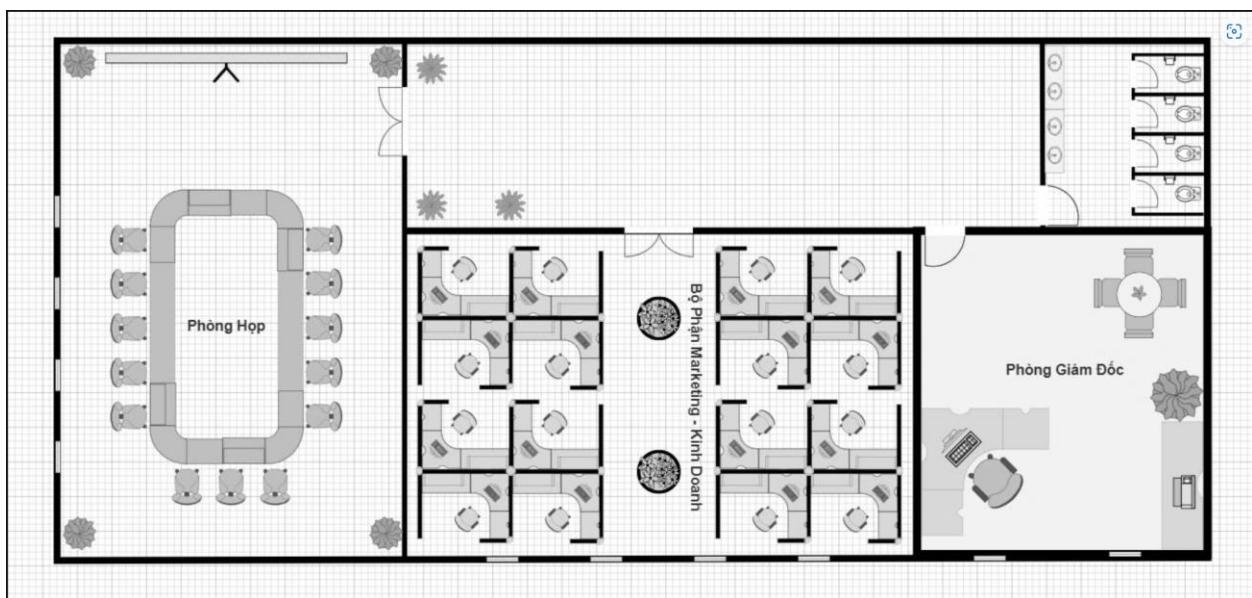
- Kiểm soát truy cập mạng: Phân vùng mạng thành các segment riêng biệt (sales, marketing, kỹ thuật, quản trị), kiểm soát lưu lượng giữa các vùng
- Bảo mật điểm cuối: Bảo vệ máy trạm, máy chủ và thiết bị di động của nhân viên khỏi malware và các mối đe dọa khác
- Bảo mật ứng dụng: Đảm bảo an toàn cho các ứng dụng kinh doanh như ERP, CRM, WMS và hệ thống xử lý đơn hàng
- Bảo mật web: Bảo vệ website thương mại điện tử khỏi các cuộc tấn công như SQL injection, XSS, CSRF
- Giám sát và phát hiện sự cố: Theo dõi hoạt động bất thường và phản ứng kịp thời trước các mối đe dọa
- Sao lưu và khôi phục: Đảm bảo khả năng phục hồi dữ liệu sau sự cố với thời gian ngừng hoạt động tối thiểu
- Quản lý danh tính và truy cập: Kiểm soát quyền truy cập của người dùng với nguyên tắc đặc quyền tối thiểu
- Mã hóa dữ liệu: Bảo vệ dữ liệu nhạy cảm khi lưu trữ và truyền tải qua mạng

2. Xây dựng giải pháp

a. Sơ đồ vật lý



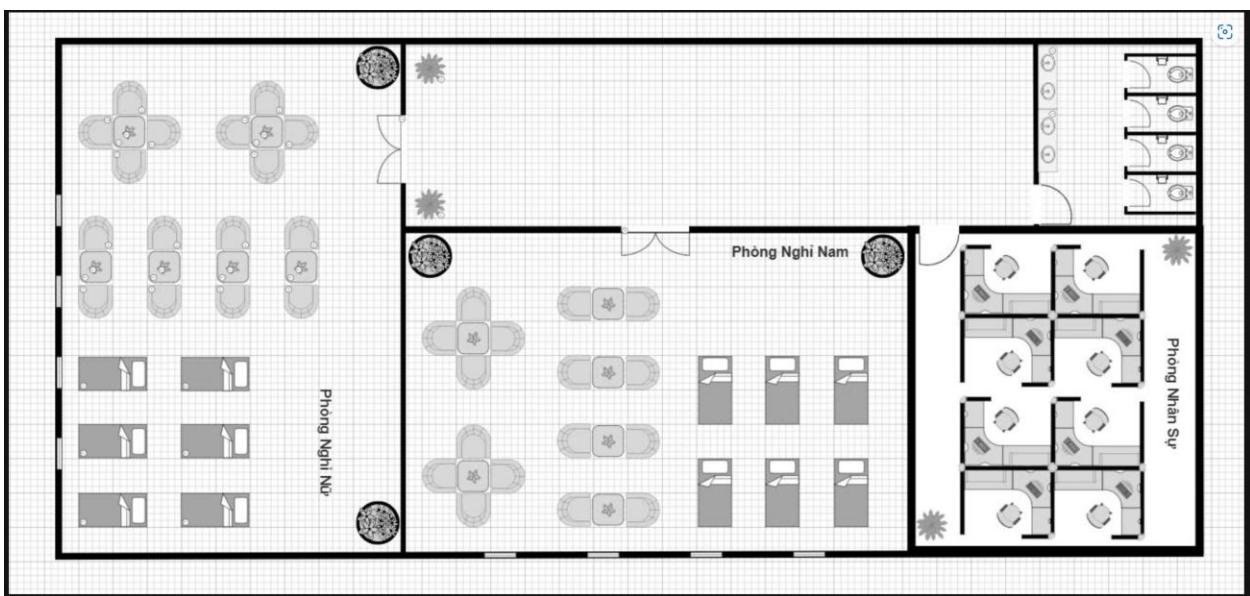
Hình 1. Tầng 1



Hình 2. Tầng 2

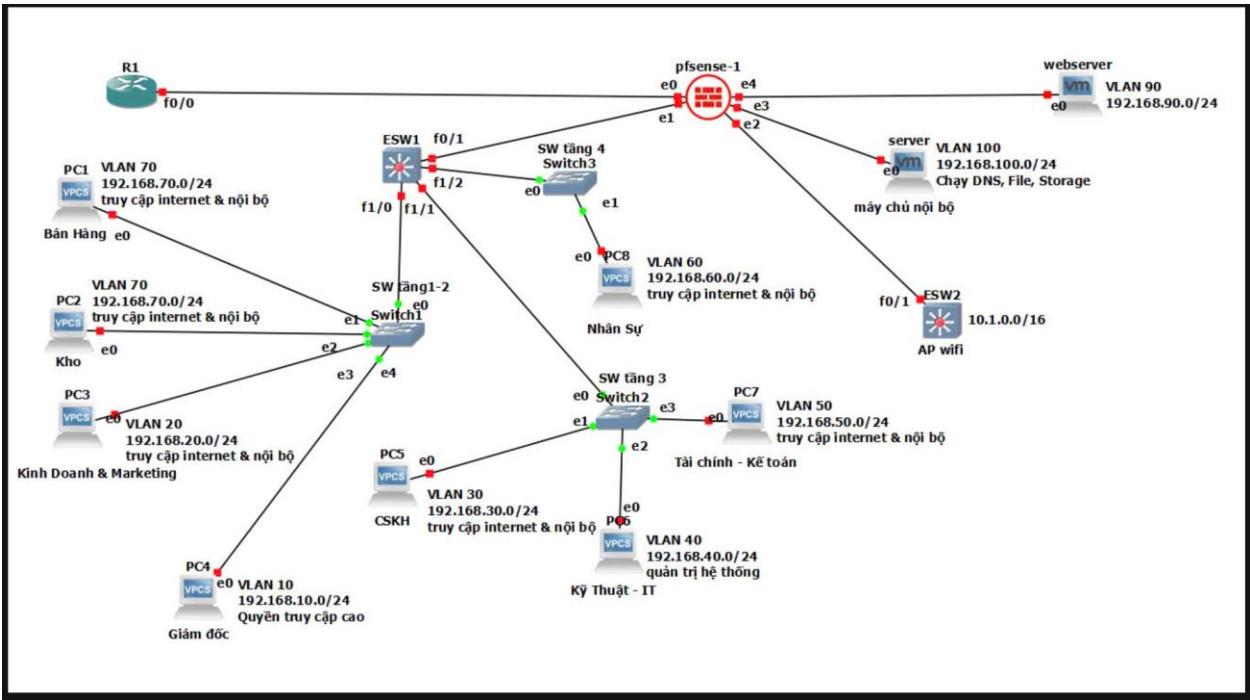


Hình 3. Tầng 3



Hình 4. Tầng 4

b. Sơ đồ logic



Hình 5. Sơ đồ logic thực tế

3. Chính sách bảo mật

a. Chính sách bảo mật vật lý

Kiểm soát truy cập:

- Khu vực như kho hàng, phòng máy chủ, phòng giám đốc không được phép vào nếu không có chức vụ ở đó
- Sử dụng thẻ vạch và xác thực vân tay ở những địa điểm quan trọng này
- Các khu vực như: phòng kinh doanh – marketing, phòng tài chính – kế toán, phòng nhân sự phải có thẻ vạch thì mới có thể vào
- Những khu vực như phòng IT, phòng chăm sóc khách hàng có thể cho bất kì ai cũng có thể vô trong giờ làm việc
- Sau giờ làm việc không cho phép bất cứ nhân viên nào ở lại công ty

Bảo vệ các thiết bị:

- Lắp camera có thể giám sát tất cả mọi người đi ra đi vào công ty

- Lắp camera có thể giám sát được phương tiện di chuyển của các nhân viên công ty và những khách hàng ra vào công ty
- Lắp camera để có thể giám sát được các nhân viên nào đi ra đi vào phòng server
- Lắp camera để có thể giám sát được các hoạt động ở các phòng ban trong công ty
- Lắp camera để có thể giám sát mọi người ra vào phòng giám đốc và toilet, không được gắn trực tiếp vào những phòng đó
- Sử dụng hệ thống ghi lại lịch sử ra vào của các nhân viên ở kho và ở phòng server
- Có UPS và máy phát điện dự phòng để các thiết bị vẫn có thể hoạt động khi cúp điện

Quản lý các thiết bị:

- Đánh dấu lại mã số cho các linh kiện thiết bị trong công ty
- Các thiết bị như máy tính làm việc của công ty phải được để trong một tủ và khoá lại
- Các thiết bị nhỏ gọn thì phải nên được trưng bày và khoá trong tủ kính
- Thiết bị laptop trưng bày phải có khoá Kensington
- Nhân viên không được phép di chuyển vị trí của các thiết bị trong cửa hàng nếu như chưa có sự cho phép của quản lý

An toàn phòng cháy chữa cháy:

- Lắp đặt hệ thống báo cháy và chữa cháy tự động để bảo vệ thiết bị và cơ sở hạ tầng
- Tổ chức các buổi huấn luyện để nhân viên biết cách phản ứng khi xảy ra hoả hoạn

Quản lý khách hàng:

- Đảm bảo khách hàng nào cũng được hướng dẫn và giám sát trong cơ sở
- Khách hàng chỉ được phép đến các khu vực: khu trưng bày, thu ngân, phòng ban IT, phòng chăm sóc khách hàng, toilet
- Khách hàng không được phép đi theo nhân viên vào kho
- Khách hàng không được phép hút thuốc, hoặc sử dụng bật lửa bên trong công ty
- Khách hàng không được phép mang đồ ăn thức uống từ ngoài và để tránh trường hợp không may đổ vào thiết bị
- Khách hàng chỉ được cầm sản phẩm ra khỏi công ty khi đã được bảo vệ kiểm tra lại hoá đơn

Kiểm tra định kỳ:

- Kiểm kê lại hàng hoá trong kho và nơi trưng bày sau mỗi cuối ngày
- Sáu tháng kiểm tra lại hệ thống phòng cháy chữa cháy và các hệ thống camera
- Tổ chức kiểm tra định kỳ kiến thức của nhân viên về các chính sách bảo mật, một năm tổ chức một lần
- Video xuất từ camera phải được lưu trữ ít nhất 15 ngày

b. Chính sách bảo mật hệ điều hành

- Chính sách người dùng:
 - Mật khẩu phải ít nhất từ 8 ký tự trở lên, có đầy đủ số, ký tự đặc biệt và chữ
 - Nhận mail có đính kèm: không được tự ý mở mail từ một nguồn mình không biết, có đuôi file khác với các đuôi file của office
 - Không được phép tắt windows security, và windows firewall
 - Không được phép tự ý gỡ cài đặt hoặc là cài đặt một ứng dụng nào đó
 - Không được phép mang máy tính cá nhân và kết nối tới mạng bằng dây
 - Nhân viên phải được huấn luyện về các chính sách bảo mật khi mới vào công ty
- Chính sách hệ thống:

- Tất cả các thư mục cá nhân như downloads, desktop, document phải chuyển tới lưu tại nơi lưu trữ tập trung
- Các dữ liệu của công việc phải lưu vào ổ đĩa của phòng ban chính mình
- Các dữ liệu chung của công gởi vào ổ đĩa chung của công ty
- Mỗi phòng ban được phân cho hạn ngạch riêng để lưu trữ
- Ổ đĩa chung của công ty không được phép chép các file thực thi vào
- Cập nhập các bản vá lỗi thường xuyên của hệ điều hành
- Sao lưu dữ liệu lại trong khoảng thời gian trong ngày: 4h sáng, 12h trưa, 17h chiều
- Sao lưu hệ điều hành định kì 1 tuần 1 lần
- Các dữ liệu được sao lưu sẽ được chuyển sang ổ rời, thiết bị lưu trữ rời hoặc lưu trữ đám mây 1 tuần 1 lần và lưu trữ trong vòng 6 tháng
- Vô hiệu hoá control panel trên các máy client
- Vô hiệu hoá gắn usb trên các máy client
- Vô hiệu task manager trên các máy client
- Người dùng không thể truy cập trái phép vào tài liệu không phải của mình
- Mã hoá ổ đĩa lưu trữ bằng bitlocker

c. Chính sách bảo mật mạng

- **Bảo mật LAN:**

- Ghi lại nhật ký các truy cập vào server domain và các máy trong mạng Lan
- Chặn không cho nhân viên truy cập vào các web ngoại trừ web đã được cho phép như:
tuoitre.vn, vnexpress.net, vietnamnet.vn, chinhphu.vn, baochinhphu.vn, thanhtra.gov.vn, customs.gov.vn, thuedientu.gdt.gov.vn, facebook.com, linkedin.com, twitter.com, google.com, microsoft.com, salesforce.com, wikipedia.org, coursera.org, edx.org, youtube.com, bbc.com, nytimes.com,

vnexpress.net,amazon.com, shopee.vn, lazada.vn,visa.com, mastercard.com, paypal.com,github.com, stackoverflow.com, techcrunch.com,...

- Tách riêng server để chạy web riêng và server chạy domain và file server riêng
- Triển khai IDS và IPS để giám sát
- Cách ly các thiết bị nghi ngờ bị nhiễm mã độc

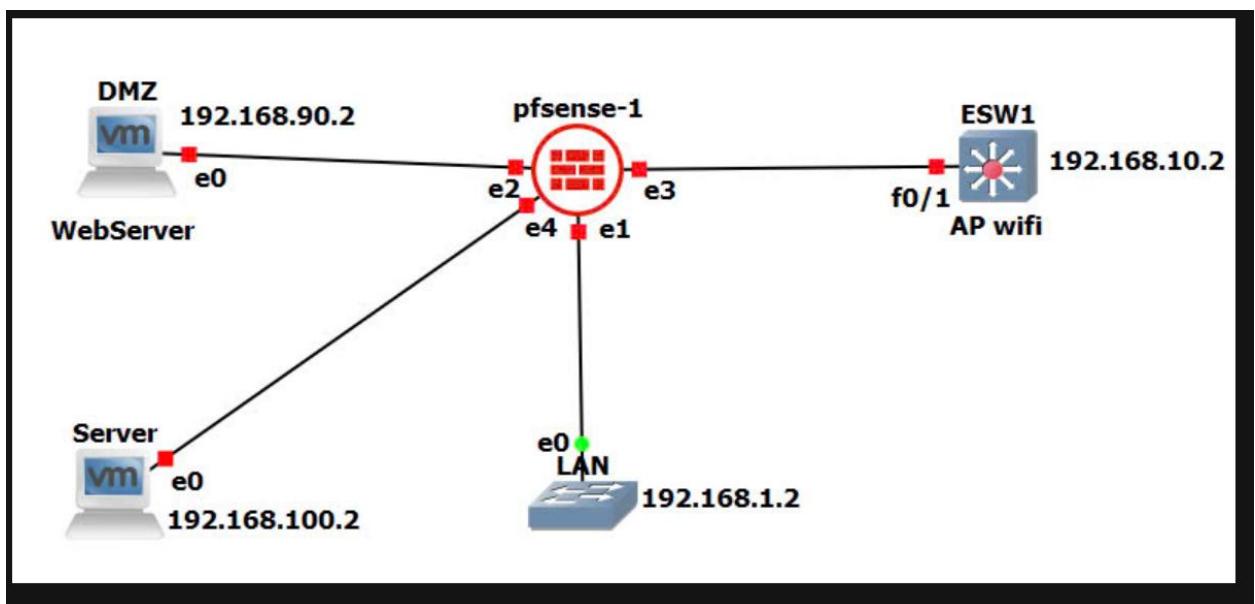
- **Bảo mật WIFI:**

- Các thiết bị khác mạng Lan không thể truy cập vào domain
- Áp dụng chuẩn WPA3-Personal/WPA3-Enterprise cho thiết bị hỗ trợ, hoặc WPA2-PSK (AES) thay thế
- Phân chia mạng wifi thành các Vlan cho các đối tượng dùng khác nhau: khách hàng, nhân viên
- Theo dõi giám sát các hoạt động wifi
- Chặn không cho thiết bị vào các trang web đen

- d. **Chính sách phục hồi sau thảm họa**

- Khôi phục dữ liệu khách hàng, dữ liệu của sản phẩm từ dịch vụ lưu trữ đám mây trở về khi bị thiên tai lũ lụt
- Khi server bị dính virus, cách ly máy bị dính virus, kiểm tra xem virus đã đi qua được máy nào và cách ly nó. Sau đó sử dụng các dữ liệu đã backup của server để khôi phục lại
- Đăng ký bảo hiểm cho tài sản để giảm thiểu rủi ro cho doanh nghiệp

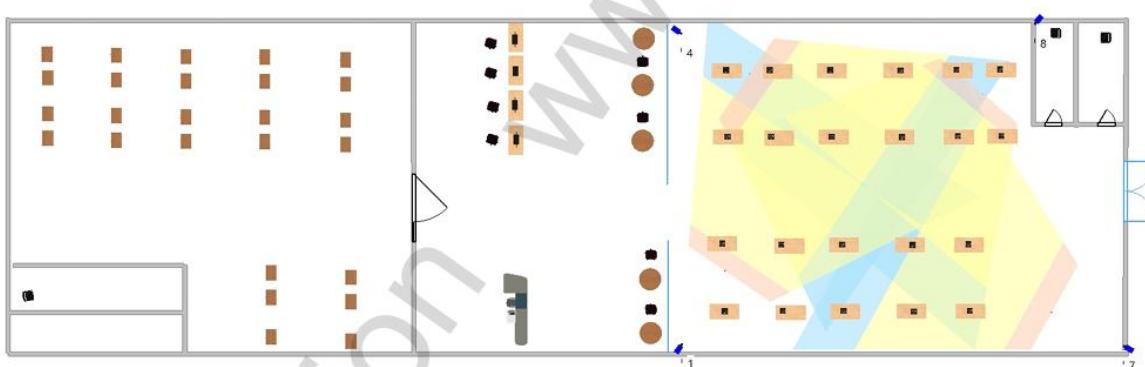
4. Sơ đồ logic triển khai demo



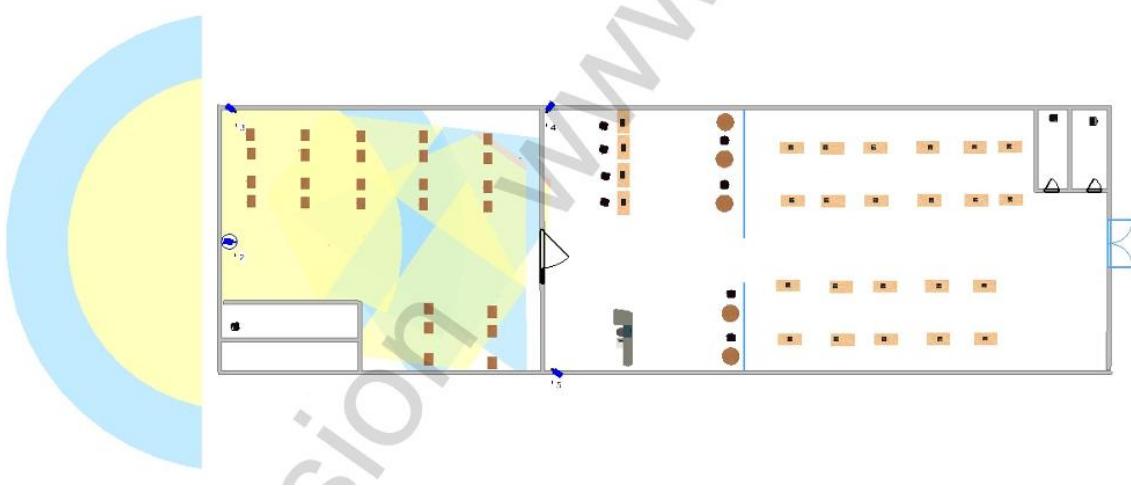
Hình 6. Sơ đồ Logic Demo

5. Triển khai

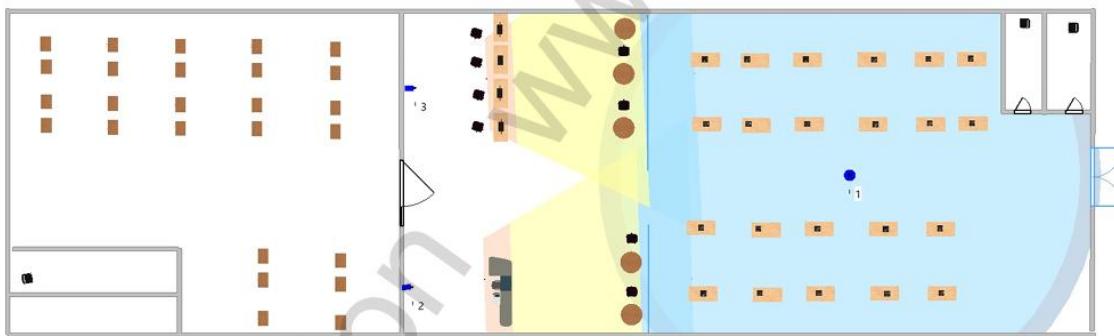
a. Bảo mật vật lý



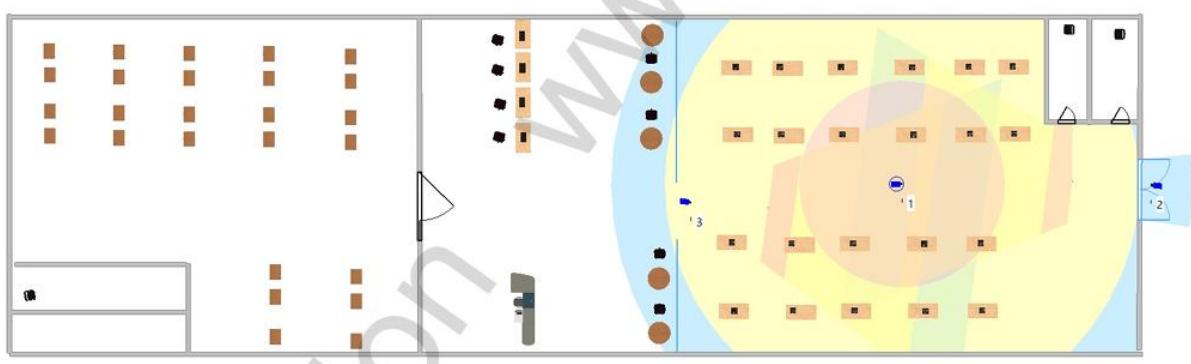
Hình 7. Phòng trưng bày



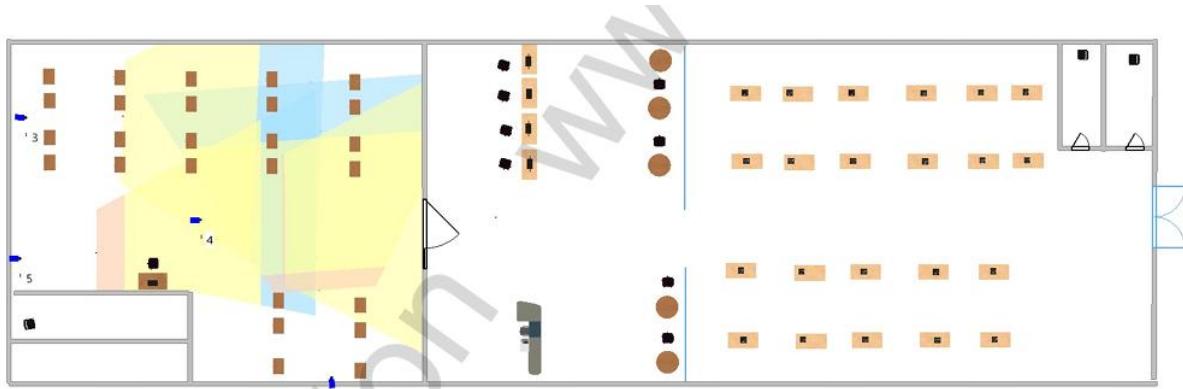
Hình 8. Phòng kho



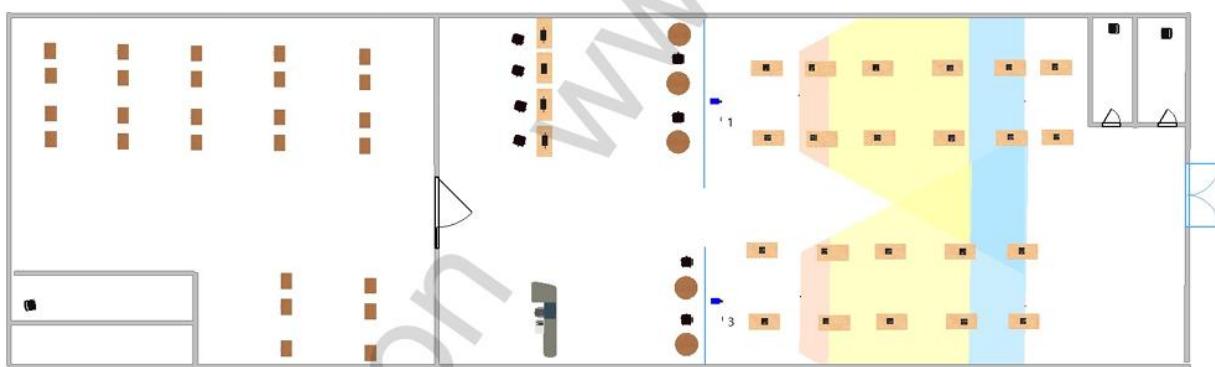
Hình 9. Camera thu ngân và tổng quát



Hình 10. Quan sát cửa ra vào



Hình 11. Camera giám sát góc chết



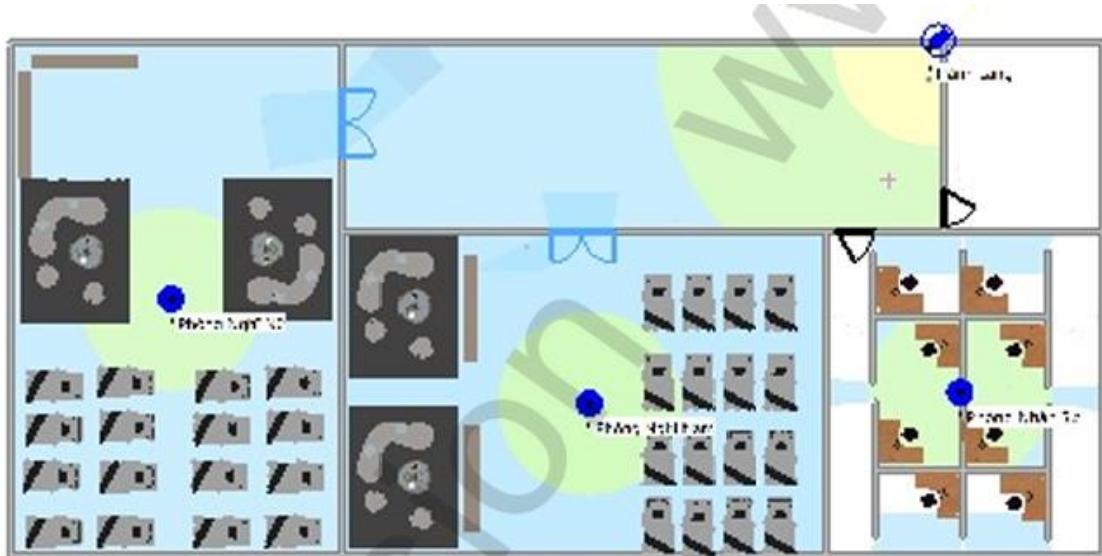
Hình 12. Quan sát khu trưng bày



Hình 13. Tầng 2

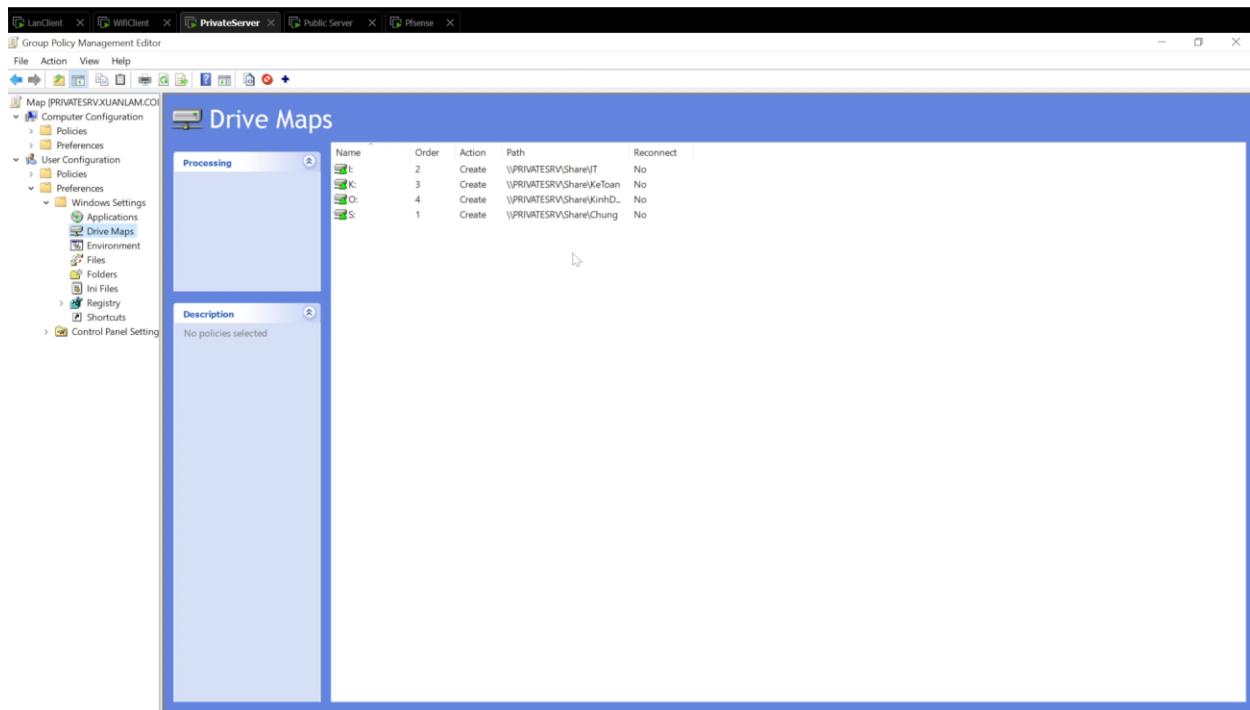


Hình 14. Tầng 3

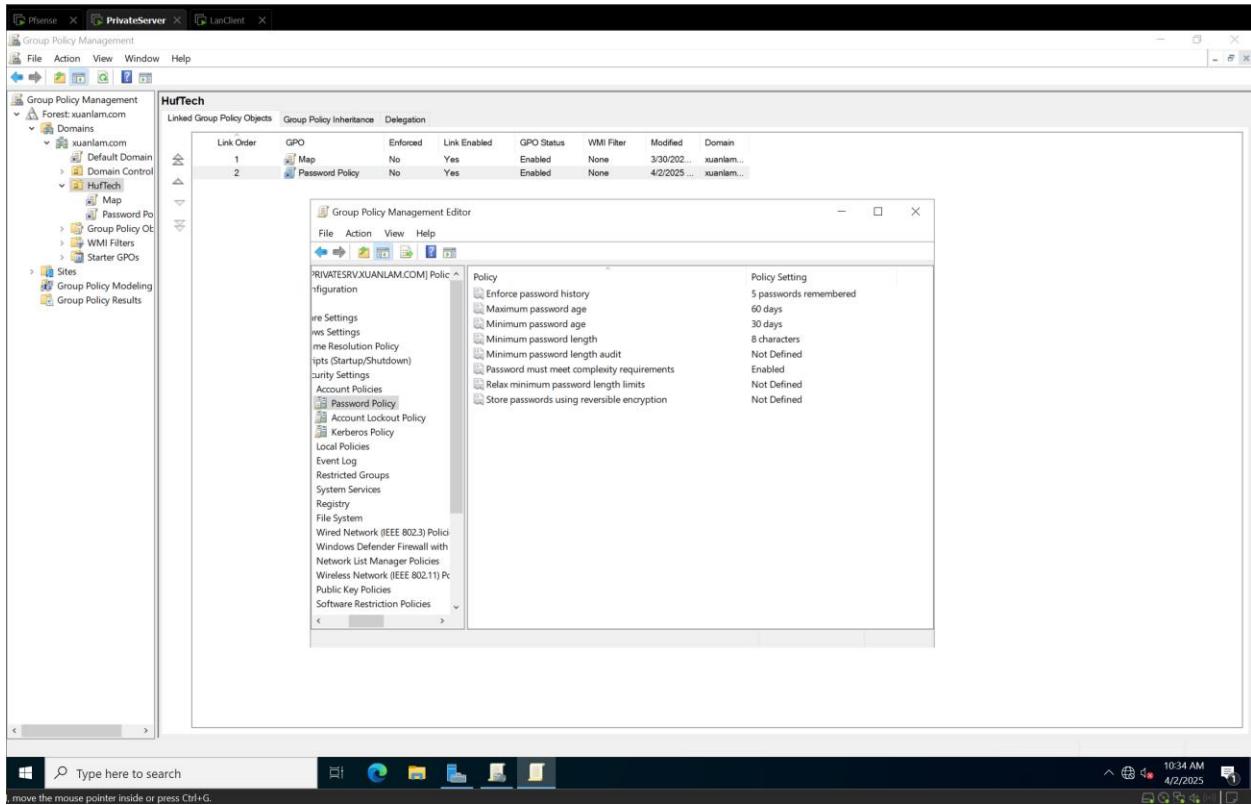


Hình 15. Tầng 4

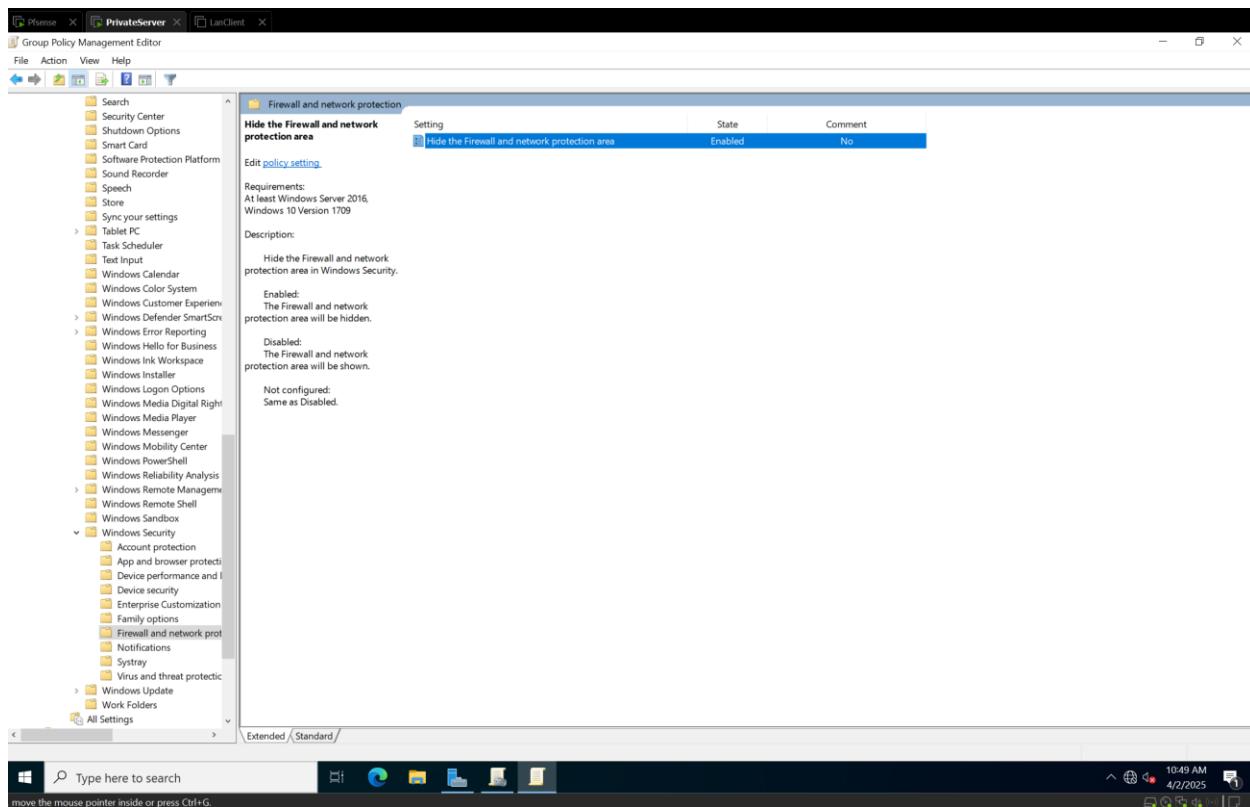
b. Bảo mật hệ điều hành



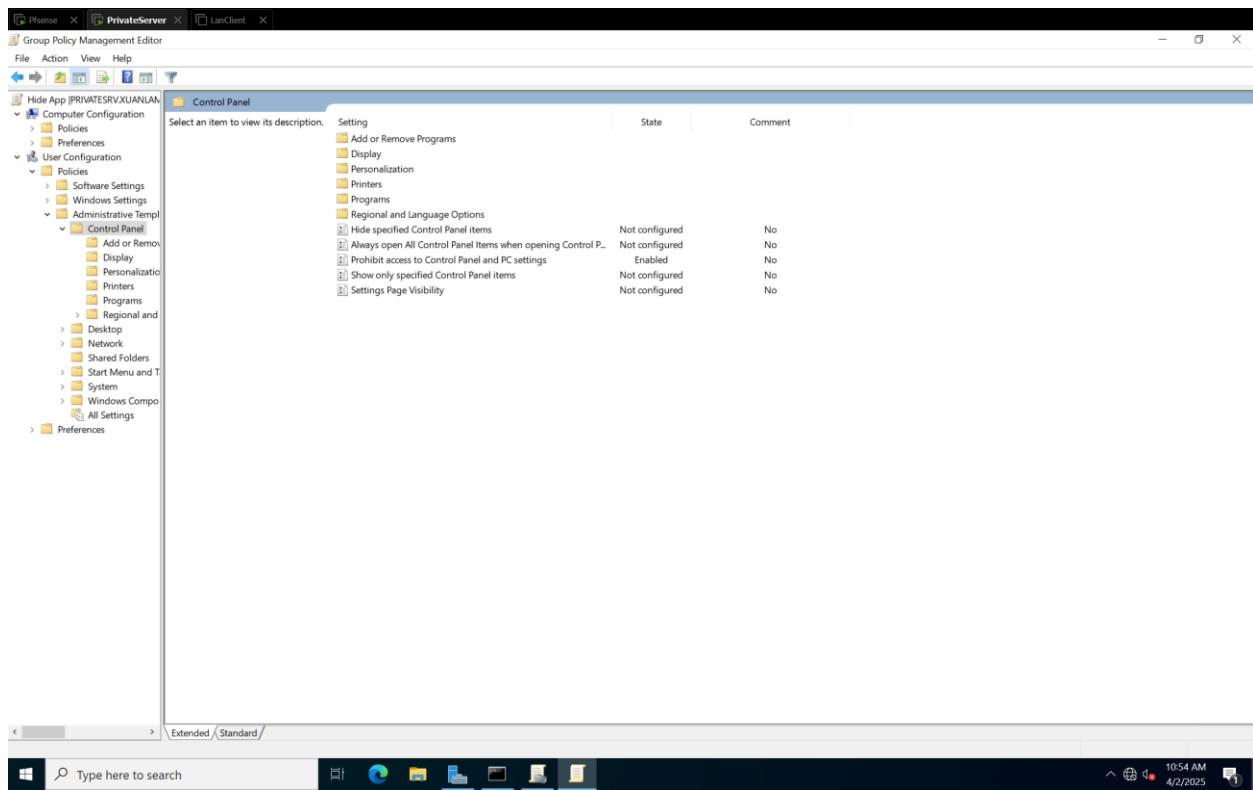
Hình 16. Triển khai group policy hiện thị ô làm việc theo phòng ban



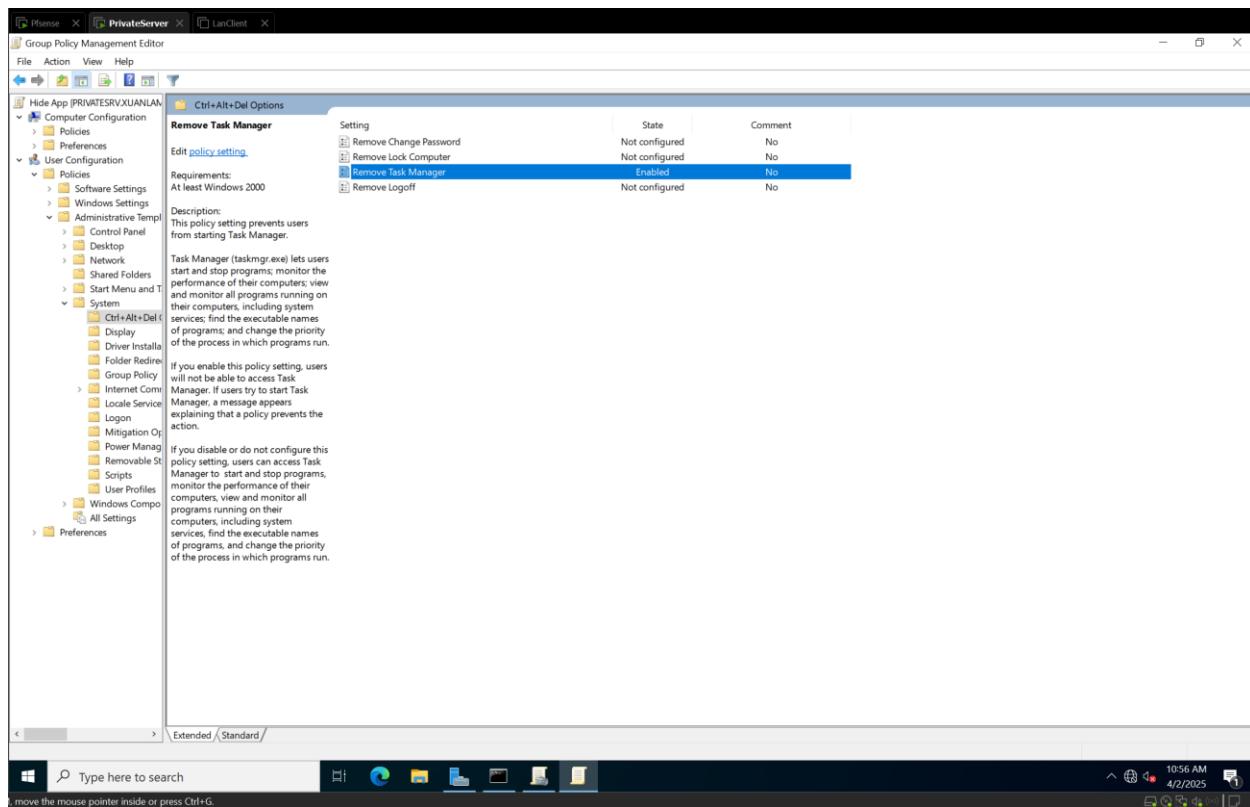
Hình 17. GPO cho tài khoản nhân viên



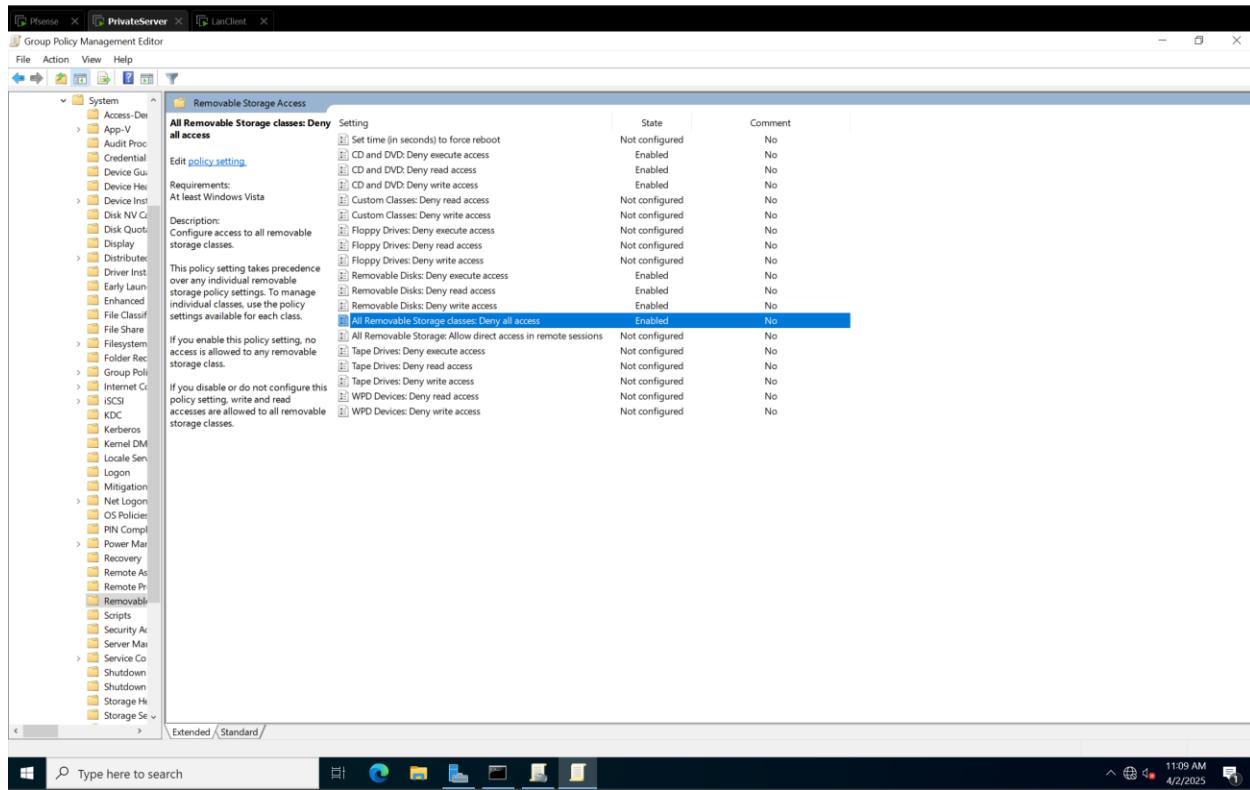
Hình 18. *Ẩn firewall*



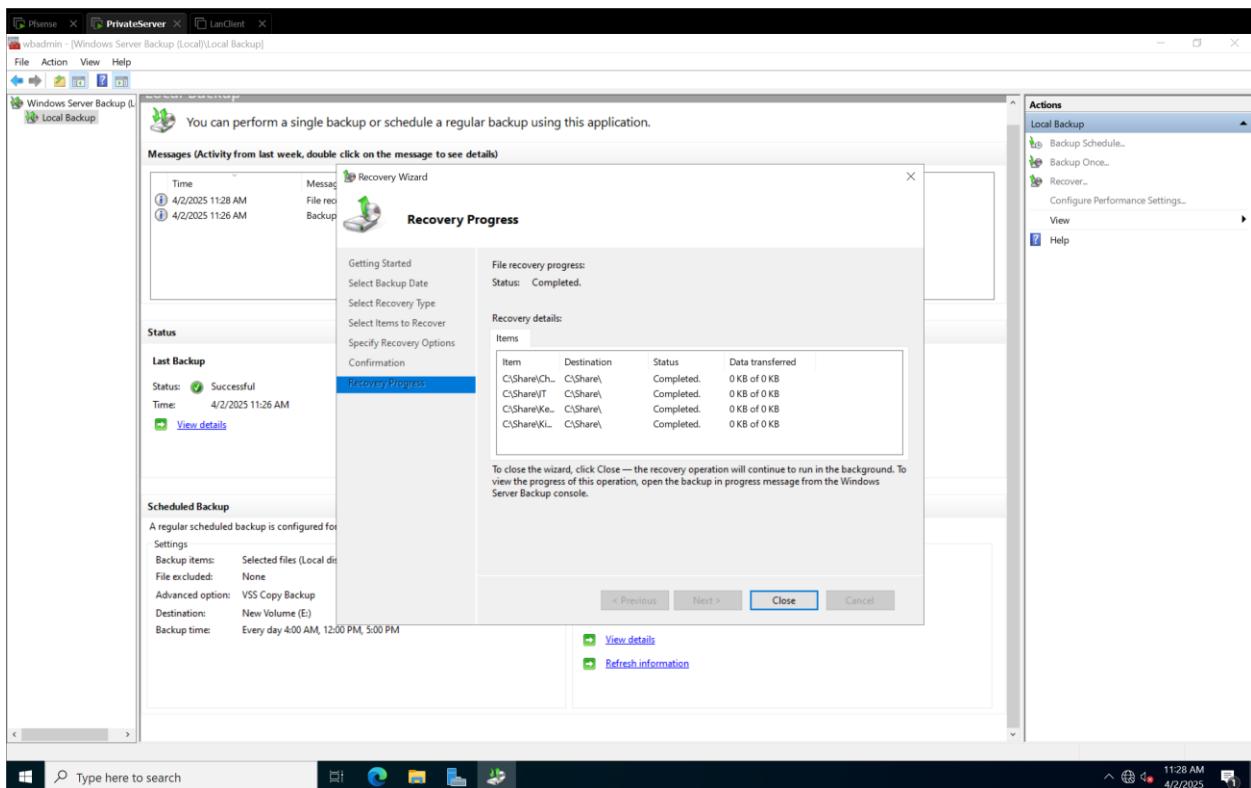
Hình 19. Ẩn control pannel



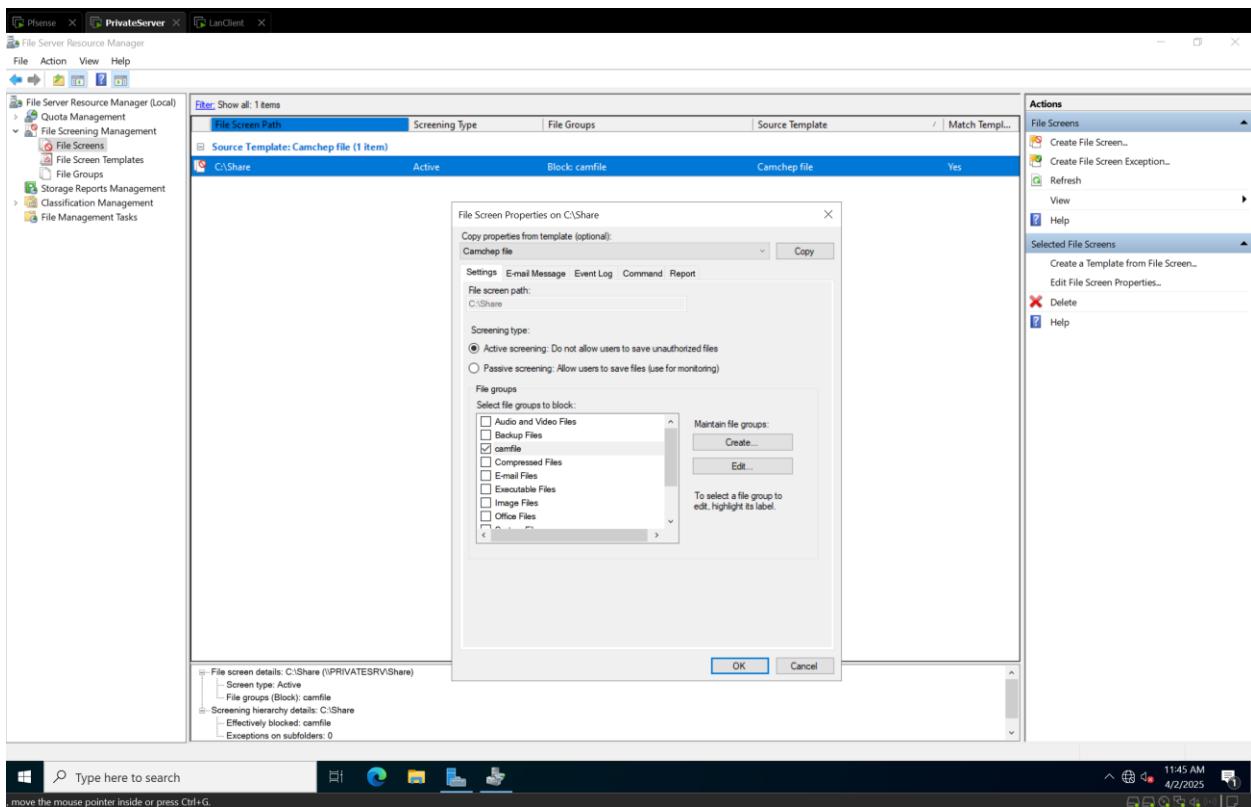
Hình 20. Vô hiệu hóa taskmanager



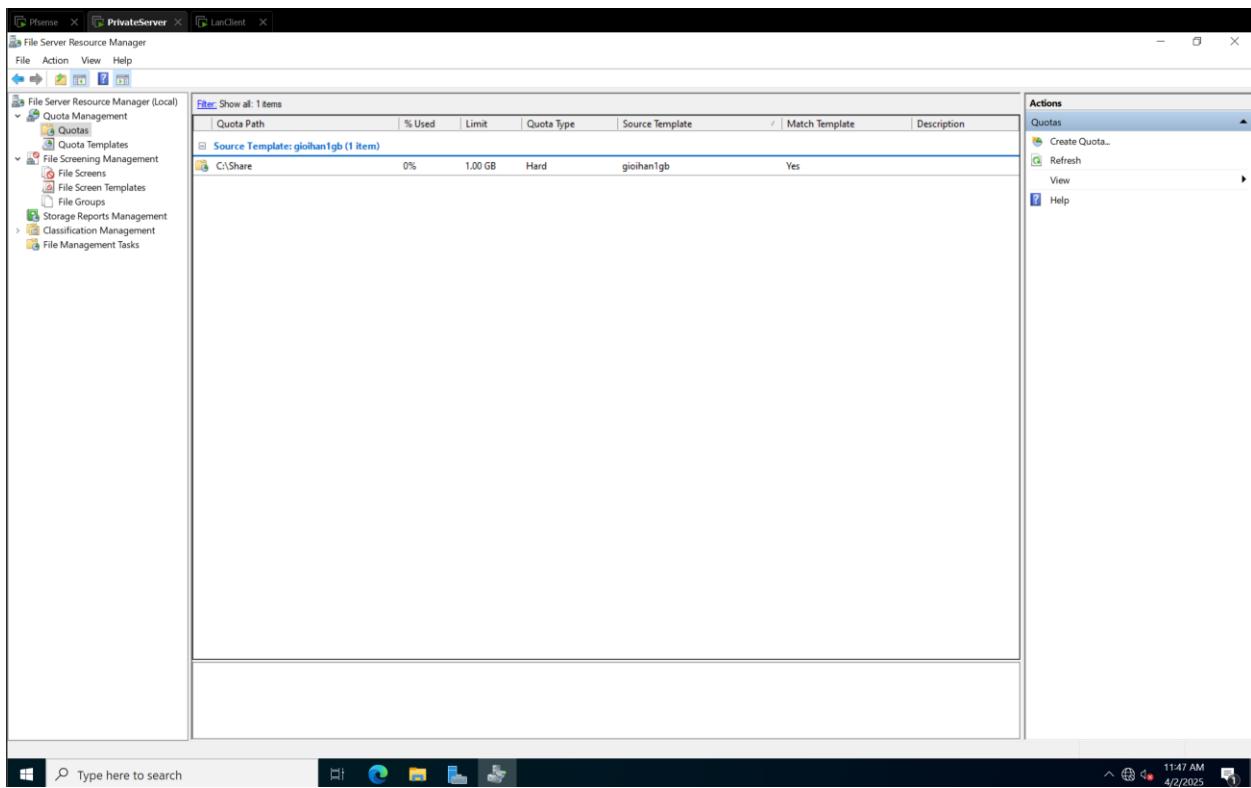
Hình 21. Cấm cắm usb vào



Hình 22. Backup cho dữ liệu



Hình 23. Cấm các file thực thi



Hình 24. Phân ngạch ô đĩa

c. Bảo mật mạng

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title bar reads "Firewall / Rules / WAN". The tabs at the top of the main content area are "Floating", "WAN" (which is selected), "LAN", "OPT1", "OPT2", and "OPT3".

The main content area displays a table titled "Rules (Drag to Change Order)". The columns are: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are two entries in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0/0 B	*	Reserved	*	*	*	*	*		Block bogon networks	

A yellow banner below the table states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom of the table are several action buttons: Add (up arrow), Add (down arrow), Delete, Toggle, Copy, Save, and Separator.

The taskbar at the bottom of the window includes icons for Start, Search, Task View, Edge, File Explorer, Mail, and File Explorer. It also shows system information: 7:42 AM, 4/2/2025, and battery status.

Hình 25. Firewall cho mạng Wan

The screenshot shows the pfSense Firewall Rules LAN configuration page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title bar says "Firewall / Rules / LAN". The tabs at the top are Floating, WAN, LAN (which is selected), OPT1, OPT2, and OPT3. The main area is titled "Rules (Drag to Change Order)" and contains a table of rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	14/949 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	Facebook	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	Gmail	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	Thanhnien	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	192.168.90.2	*	*	none			
<input checked="" type="checkbox"/>	11/552 KIB	IPv4 *	LAN subnets	*	192.168.100.2	*	*	none			
<input checked="" type="checkbox"/>	8/12 KIB	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none			
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	LAN subnets	*	*	*	*	none			
<input type="checkbox"/>	0/0 B	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	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

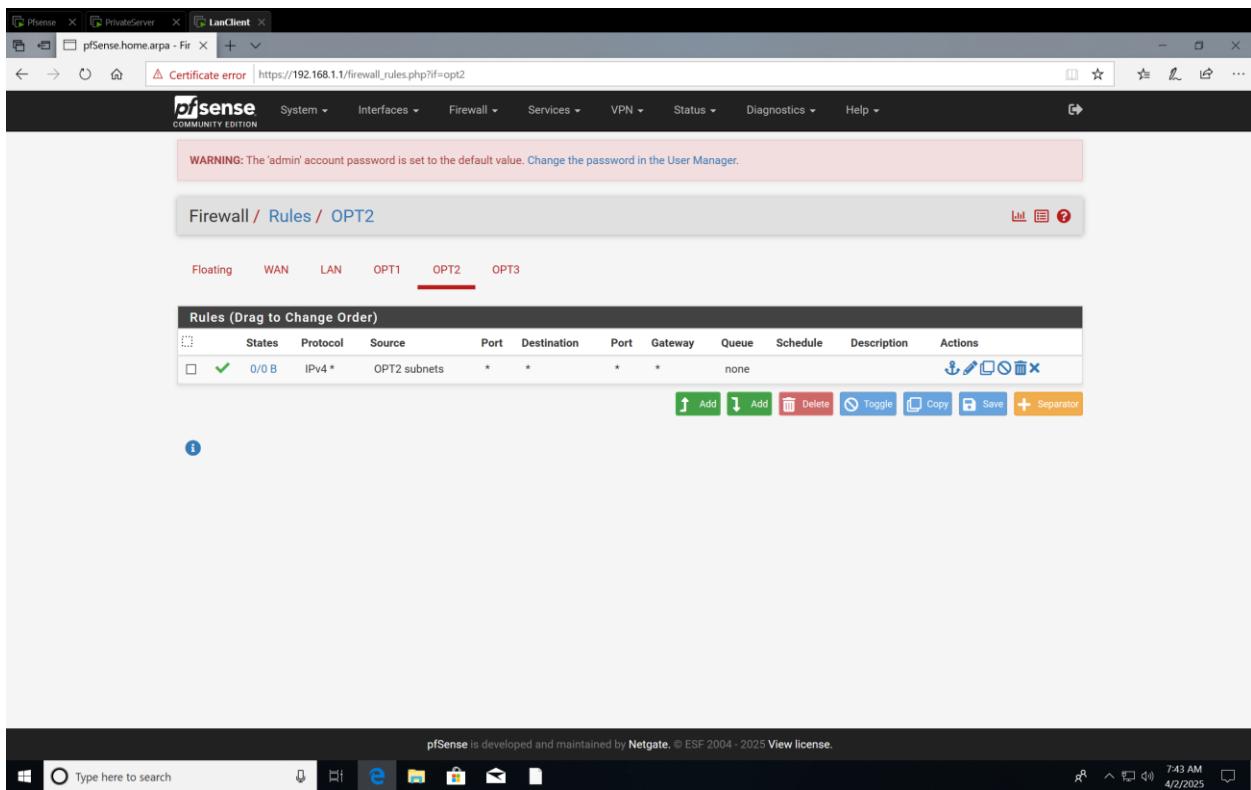
Hình 26. Firewall mạng Lan

The screenshot shows the pfSense Firewall Rules configuration page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "Firewall / Rules / OPT1". The tab "OPT1" is selected, indicated by a red underline. The main area displays a table titled "Rules (Drag to Change Order)". The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A single rule is listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 57/181.31 MiB	IPv4 *	OPT1 subnets	*	*	*	*	none			🔗 📝 ✖

Below the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator. The pfSense footer at the bottom states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#)".

Hình 27. Firewall cho mạng domain



Hình 28. Firewall cho web

The screenshot shows the pfSense Firewall Rules OPT3 configuration page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "Firewall / Rules / OPT3". The tab "OPT3" is selected. The main area displays a table titled "Rules (Drag to Change Order)". The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are two entries:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	OPT3 subnets	*	192.168.100.2	*	*	none			
0/0 B	IPv4 *	OPT3 subnets	*	*	*	*	none			

Below the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator. The pfSense footer at the bottom includes the text "pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license." and the date "4/2/2025".

Hình 29. Firewall cho wifi

The screenshot shows the pfSense Firewall Aliases IP configuration page. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "Firewall / Aliases / IP". The "IP" tab is selected. The main table displays three entries:

Name	Type	Values	Description	Actions
Facebook	Host(s)	57.144.144.1, 57.144.160.1		Edit Delete Import
Gmail	Host(s)	142.250.197.133, 172.253.118.83, 172.253.118.18, 172.253.118.19, 172.253.118.17, 172.253.118.84, 74.125.24.83, 74.125.24.19, 74.125.24.17, 74.125.24.18...		Edit Delete Import
Thanhnien	Host(s)	123.30.151.89, 14.225.10.26		Edit Delete Import

At the bottom right of the table, there are "Add" and "Import" buttons. The pfSense footer at the bottom of the screen indicates it is developed and maintained by Netgate.

Hinh 30. Aliases

The screenshot shows the pfSense Package Manager interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title bar reads "System / Package Manager / Installed Packages". There are two tabs: "Installed Packages" (which is selected) and "Available Packages".

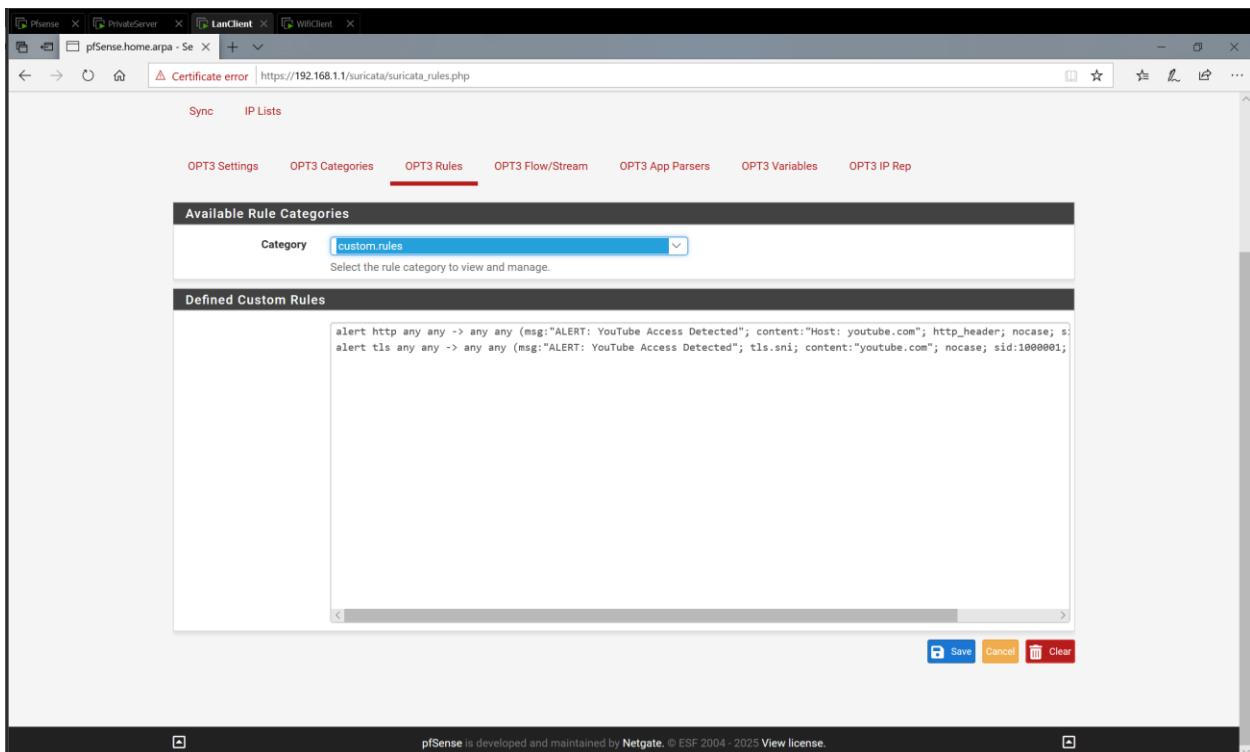
Name	Category	Version	Description	Actions
squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	
			Package Dependencies:	
			squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c_icap_modules-0.5.5_1	
squidGuard	www	1.16.19	High performance web proxy URL filter.	
			Package Dependencies:	
			squidguard-1.4.15 pfSense_pkg_squid-0.4.46	
suricata	security	7.0.8_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF.	
			Package Dependencies:	
			suricata-7.0.8	

At the bottom of the package list, there are several status indicators and links:

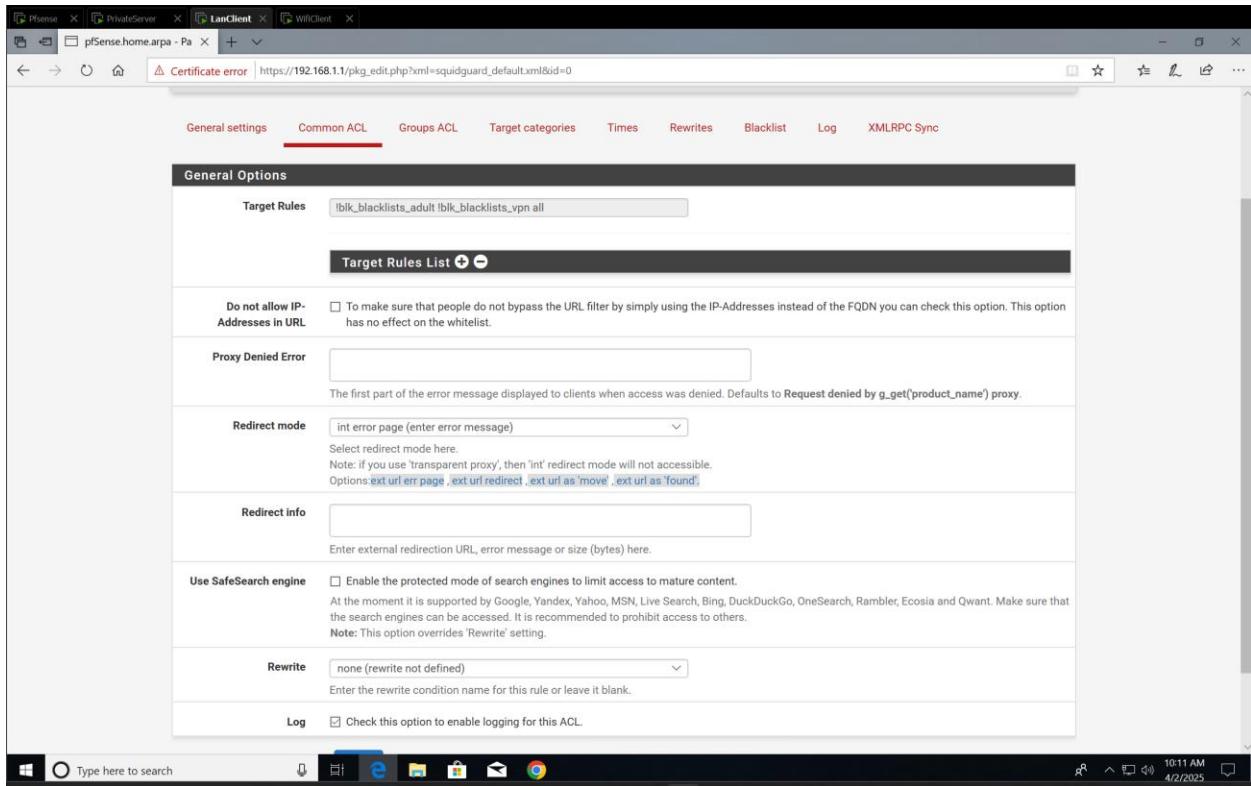
- = Update = Current
- = Remove = Information = Reinstall
- Newer version available
- Package is configured but not (fully) installed or deprecated

The taskbar at the bottom of the window shows the Windows Start button, a search bar, and various pinned icons. The system tray indicates the date and time as 4/2/2025 at 8:23 AM.

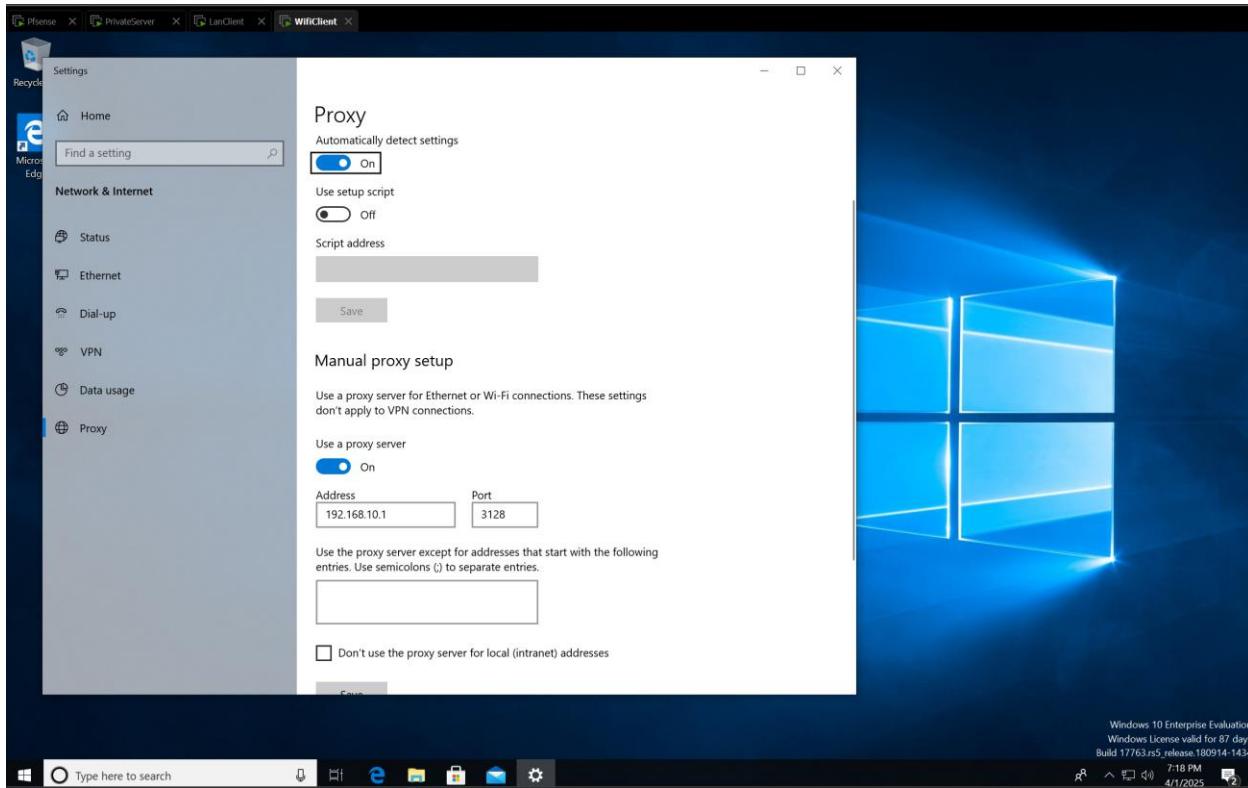
Hình 31. Suricata và Squid



Hình 32. Rule test thử suricata



Hình 33. Cài đặt các trang chặn bằng squid



Hình 34. Thêm proxy vào máy client

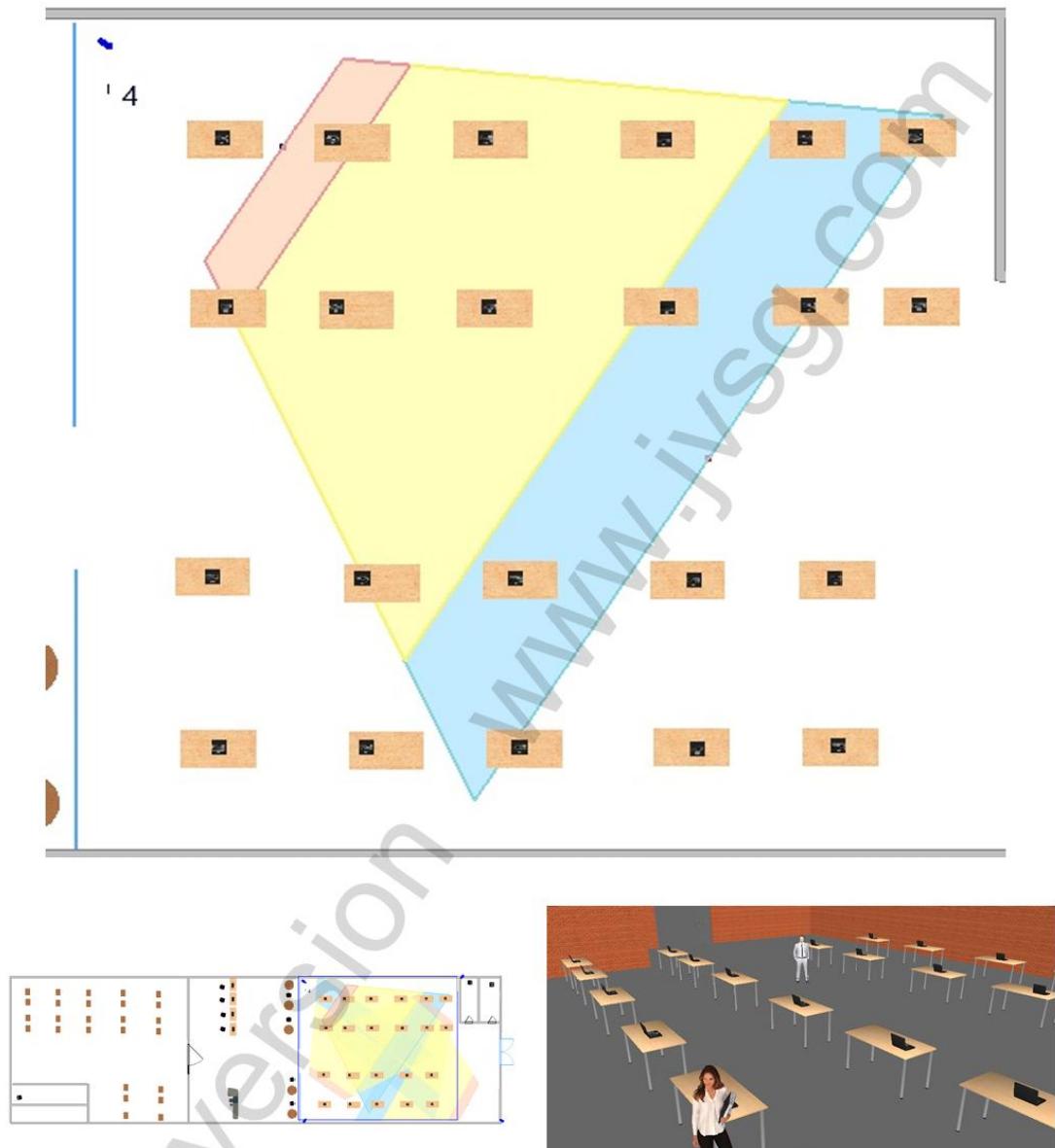
6. Kết quả triển khai

a. Bảo mật vật lý

- Phòng Trung bày



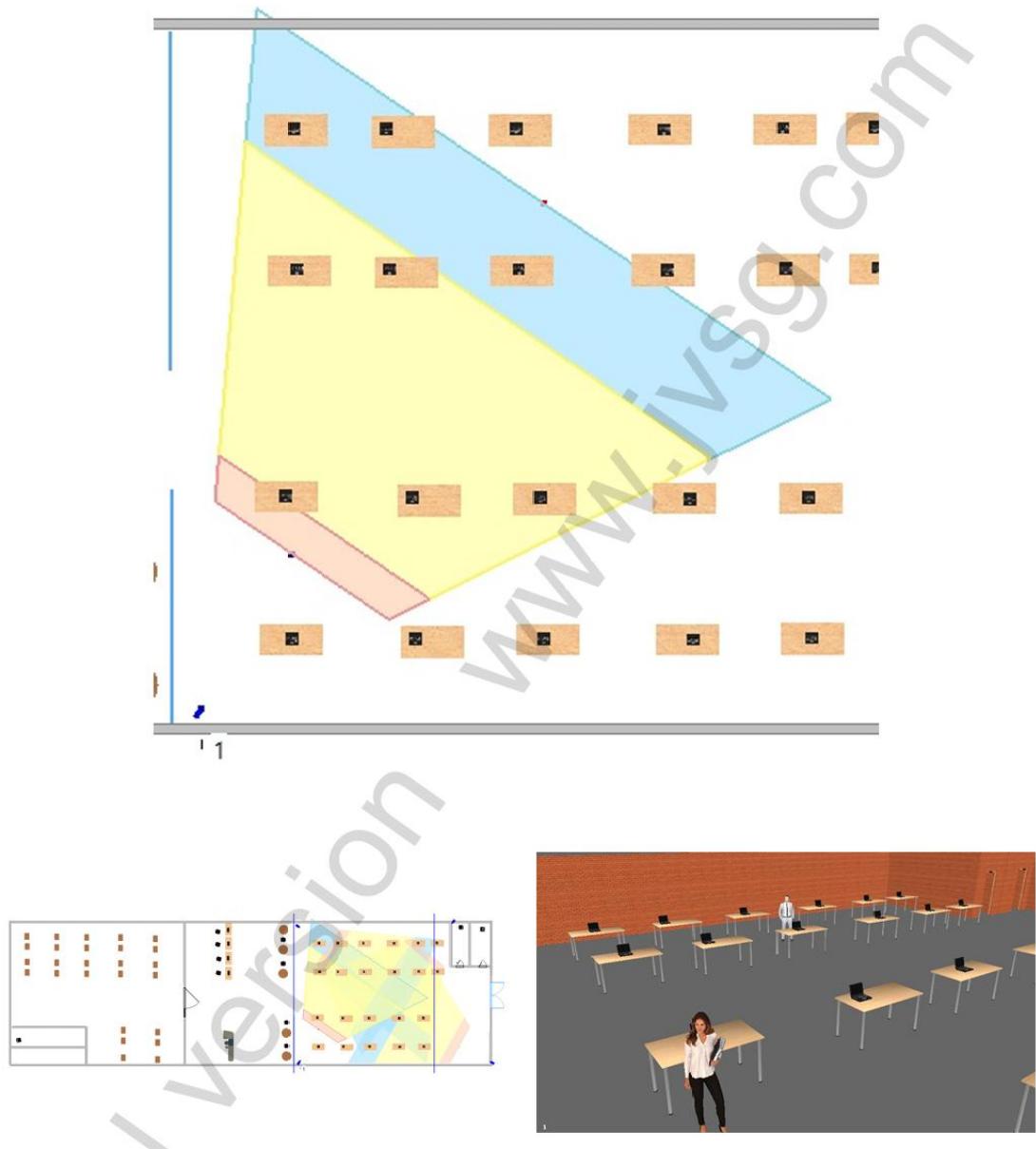
Camera 4 Bullet



Hình 35. Camera 4 trưng bày



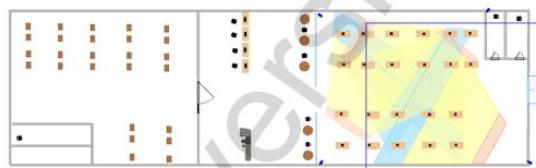
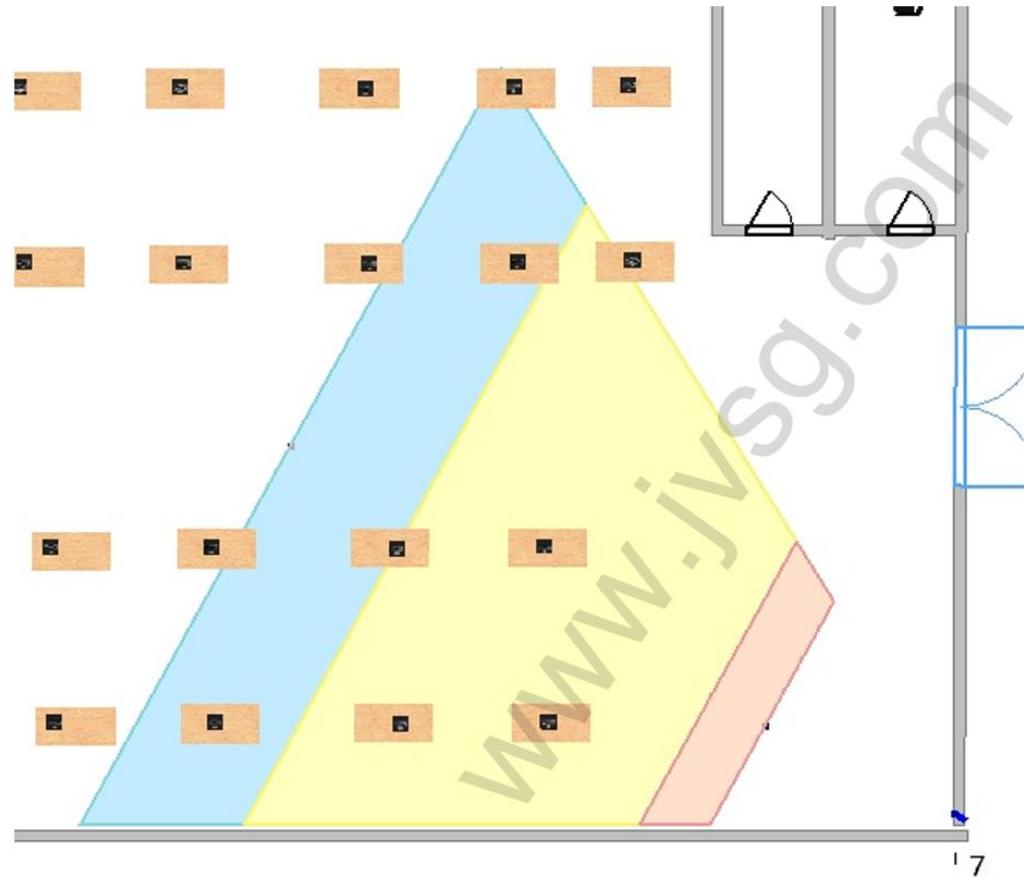
Camera 1 Bullet



Hình 36. Cam 1 trung bày



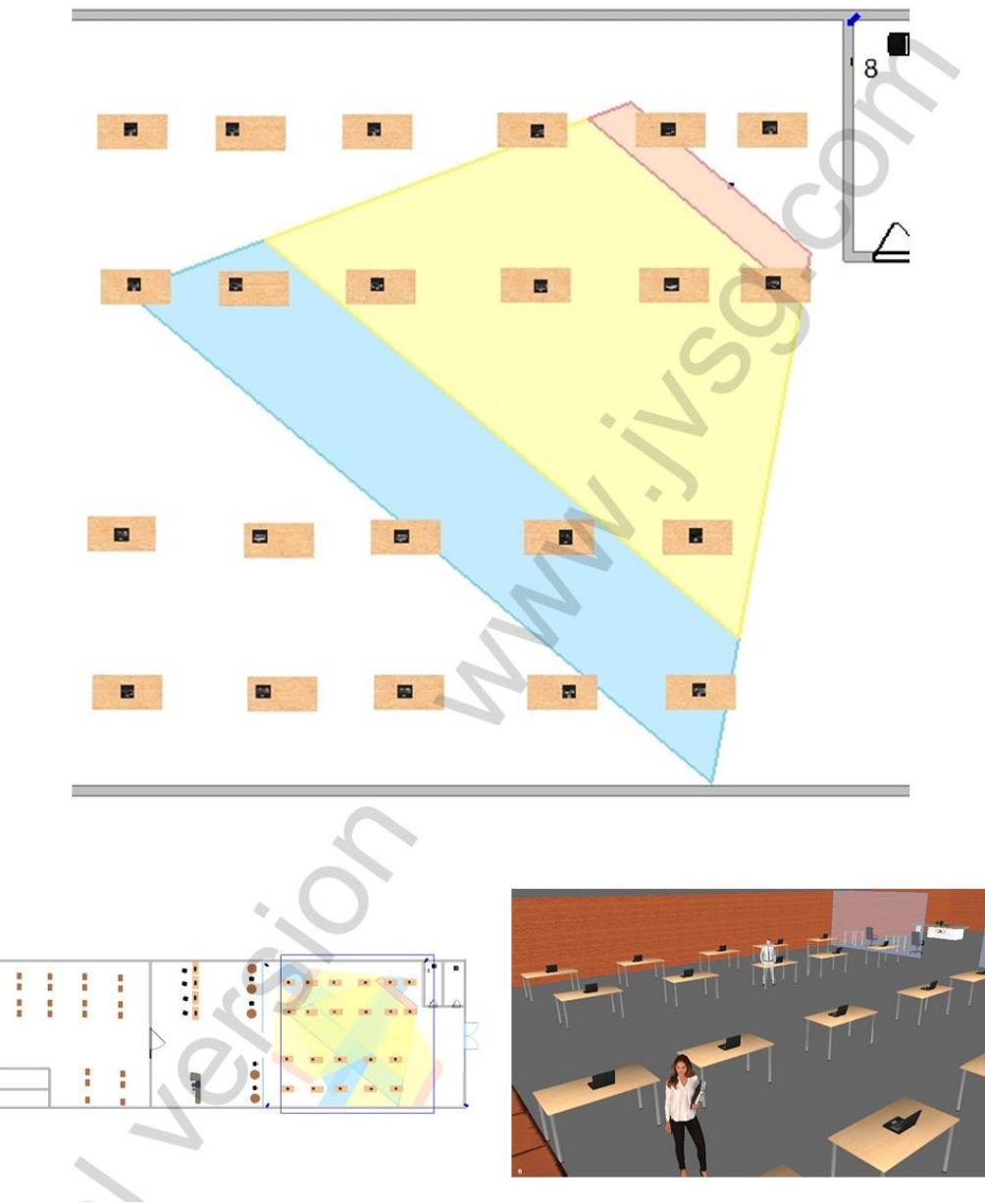
Camera 7 Bullet



Hình 37. Cam 7 trung bày



Camera 8 Bullet

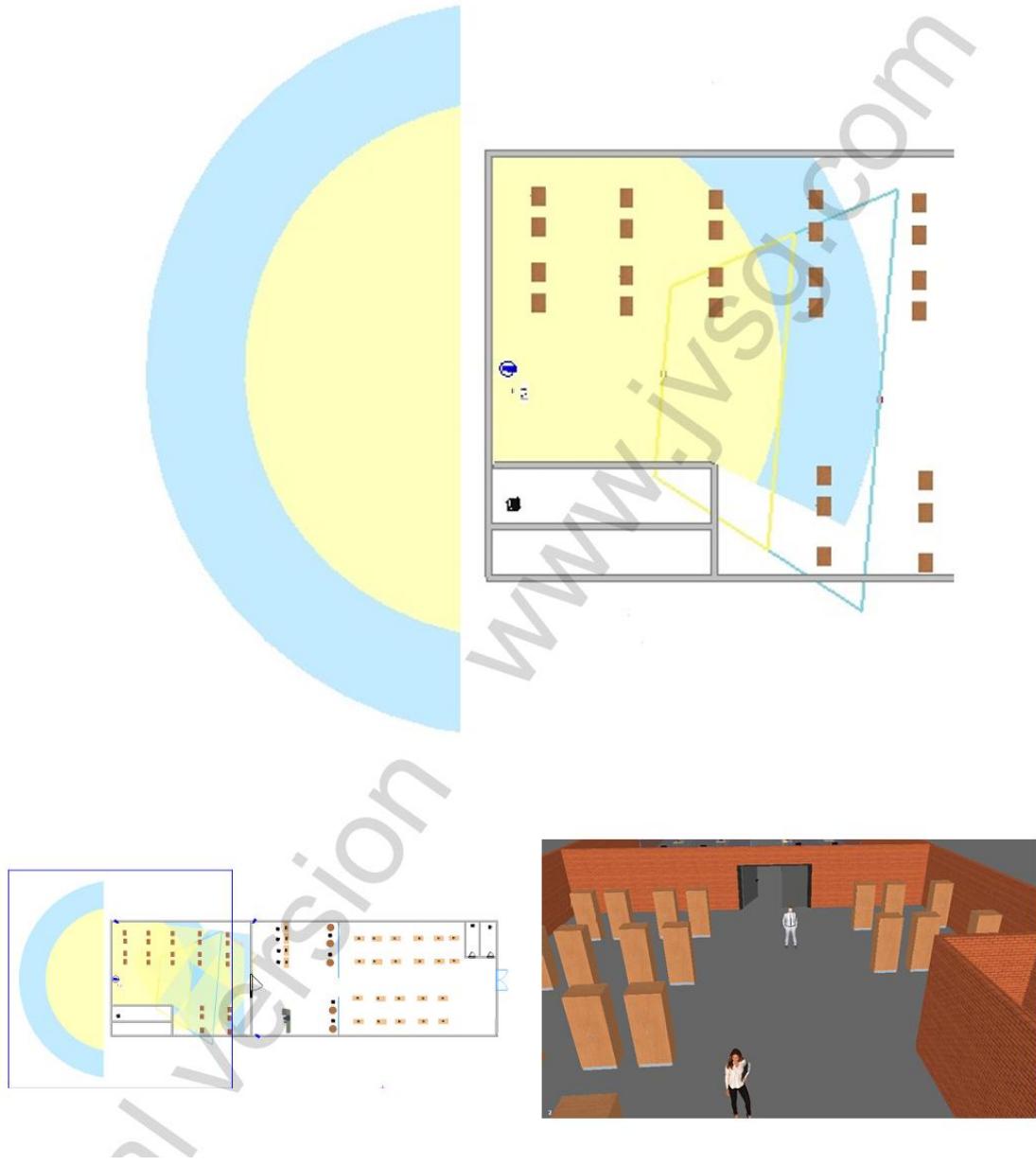


Hình 38. Cam 8 trung bày

- Phòng Kho



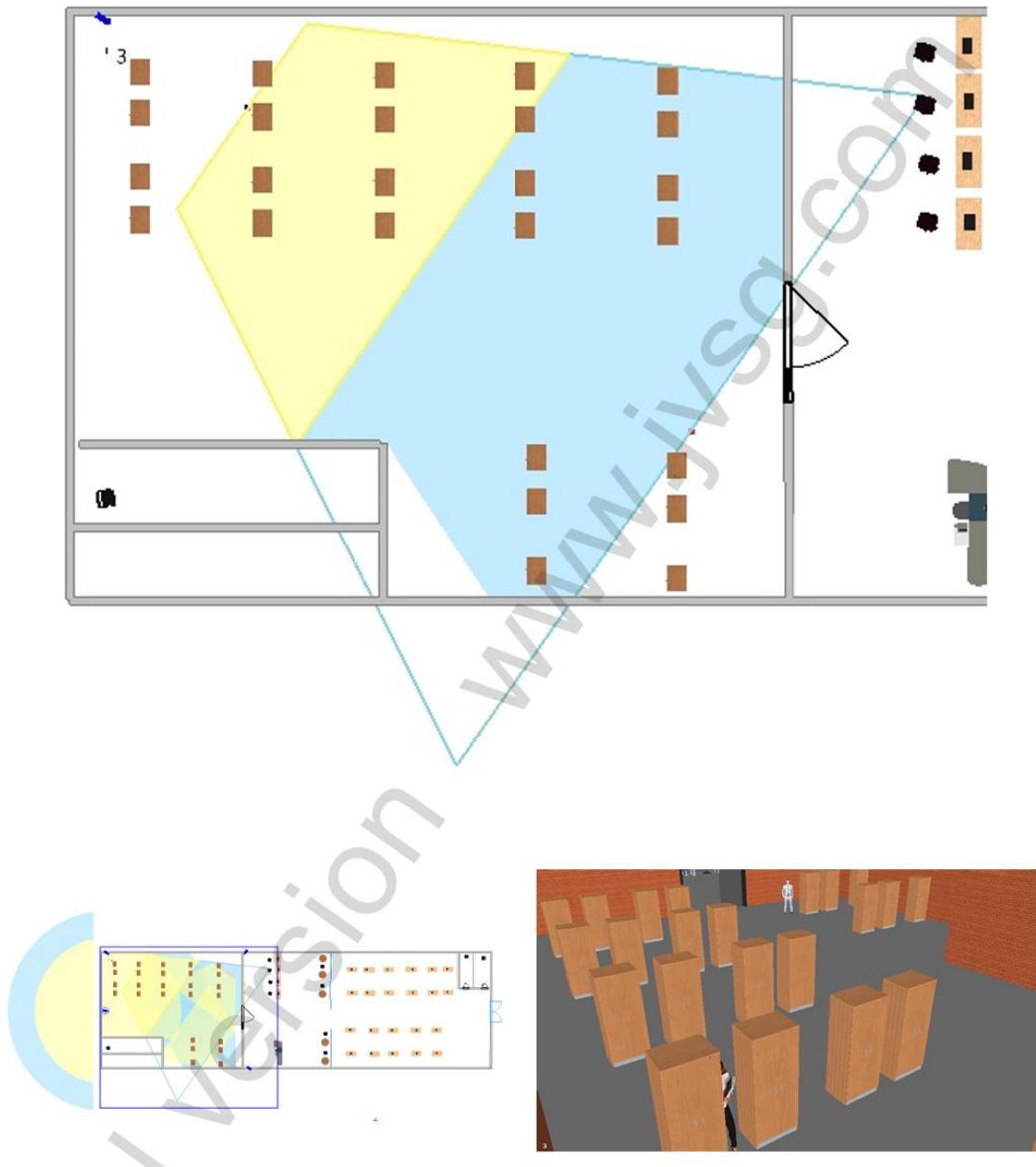
Camera 2 PTZ



Hình 39. Cam 2 kho



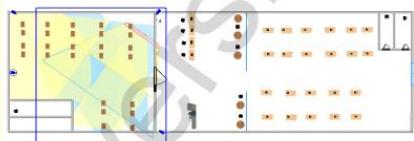
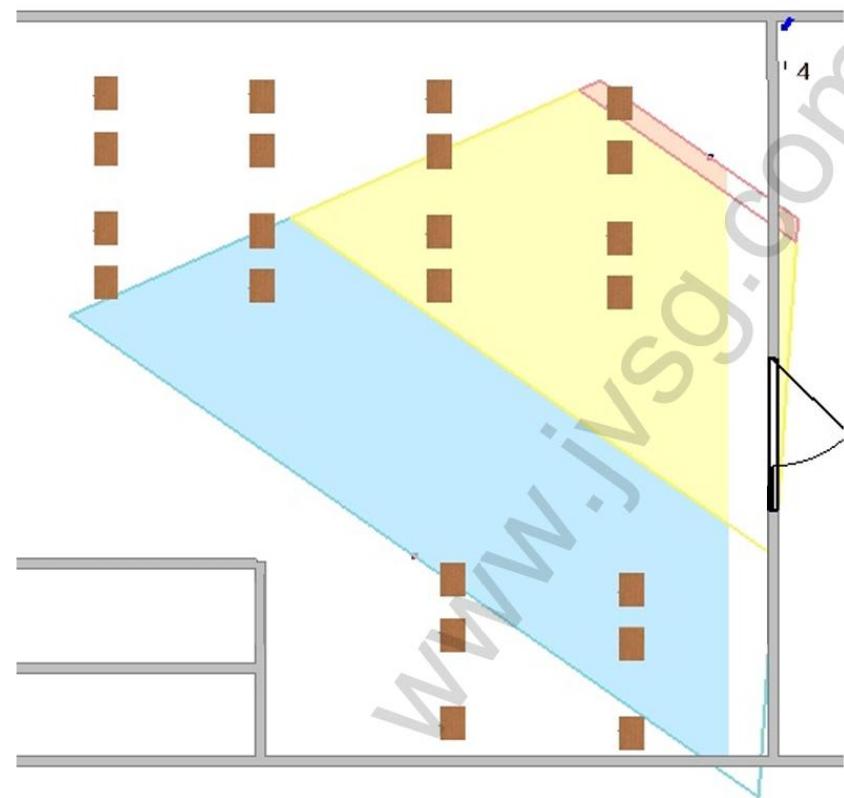
Camera 3 Bullet



Hình 40. Cam 3 kho



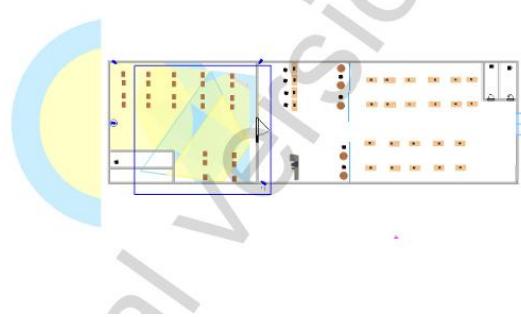
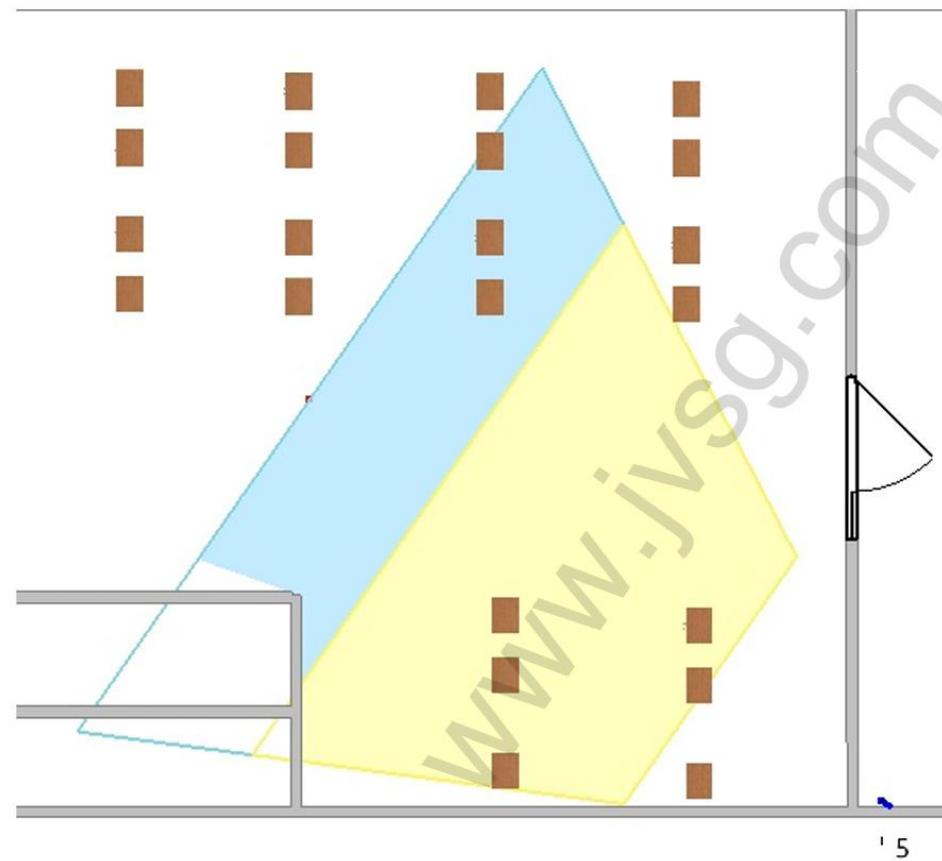
Camera 4 Bullet



Hình 41. Cam 4 kho



Camera 5 Bullet

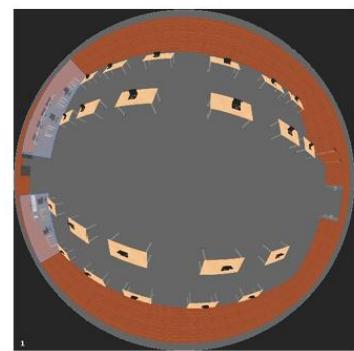
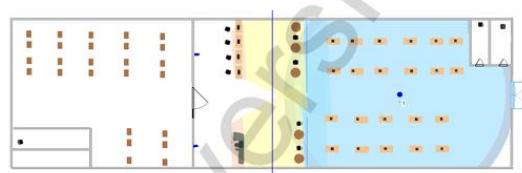
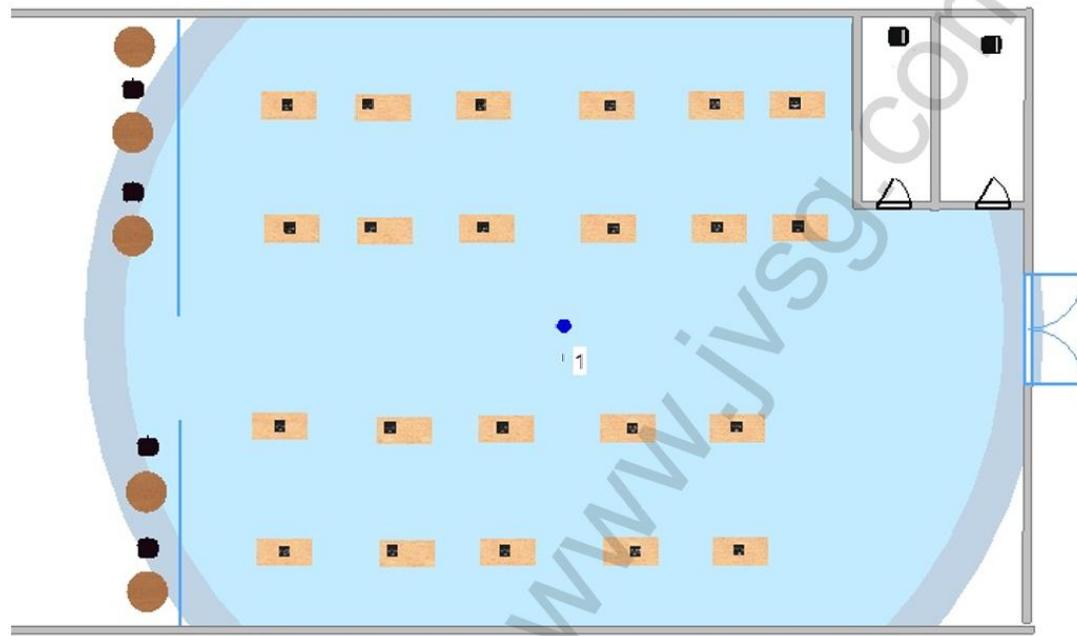


Hình 42. Cam 5 kho

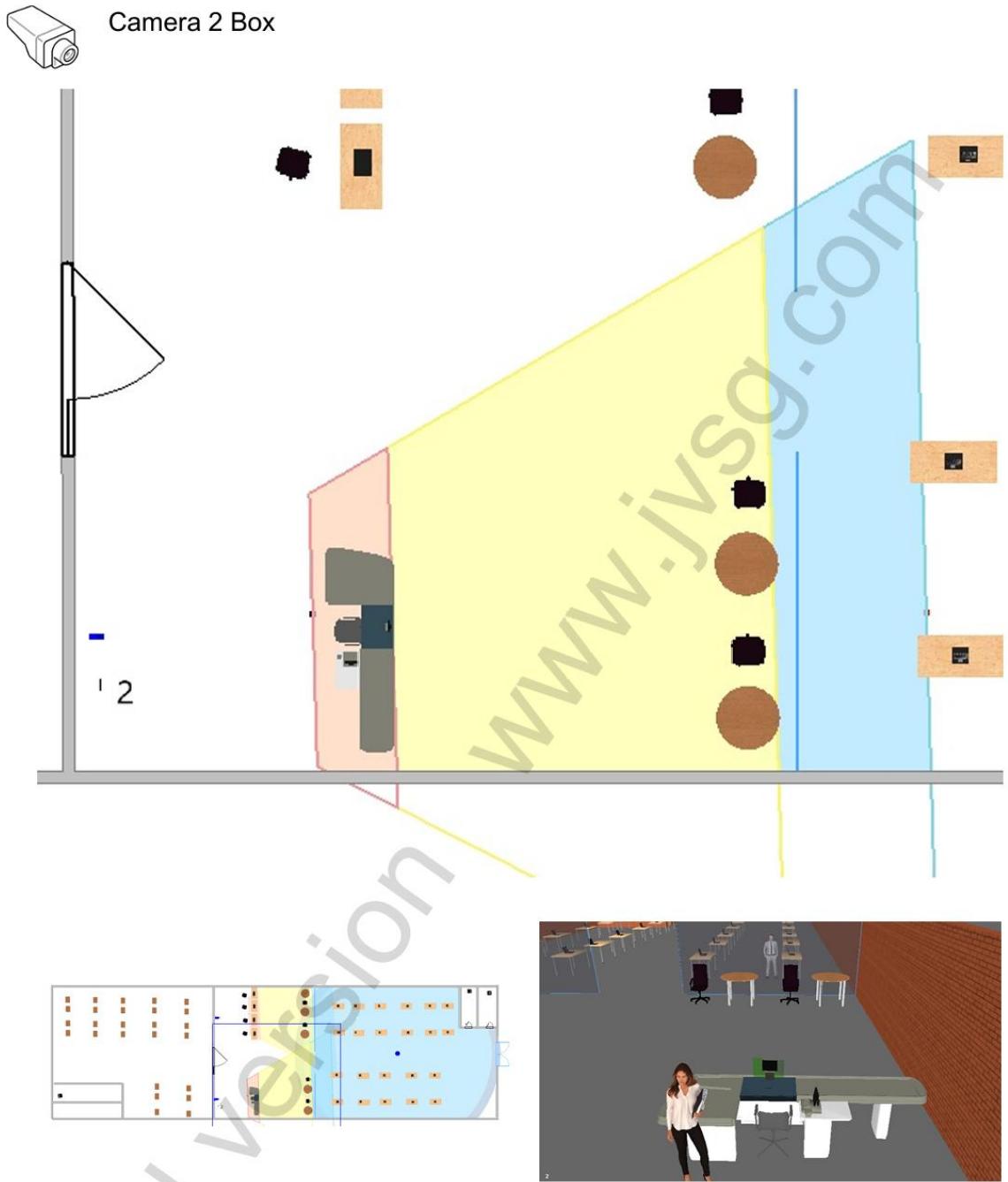
- Camera thu ngân và tổng quát



Camera 1 Fisheye



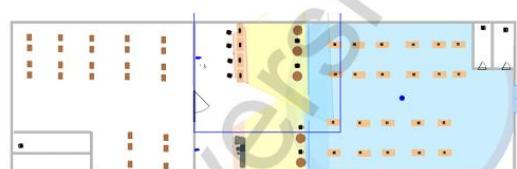
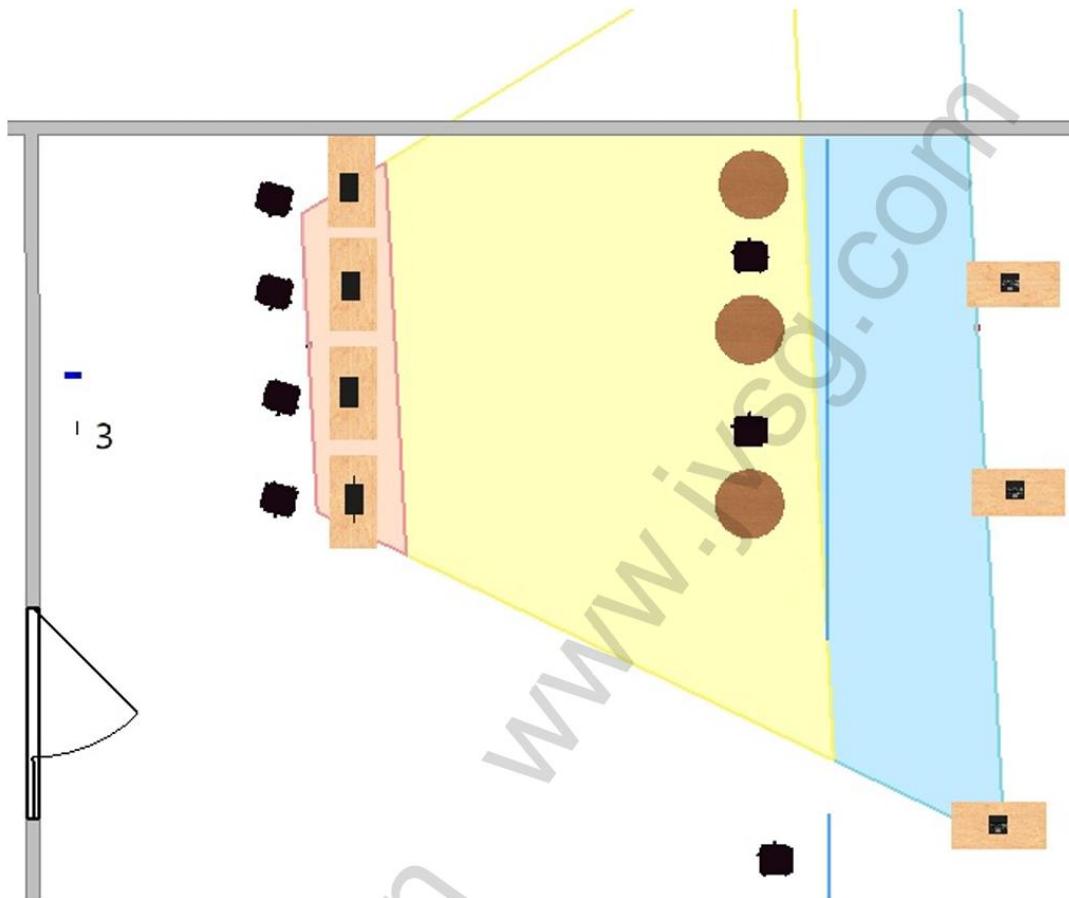
Hình 43. Cam 1 Thu ngân



Hình 44. Cam 2 Thu ngân



Camera 3 Box

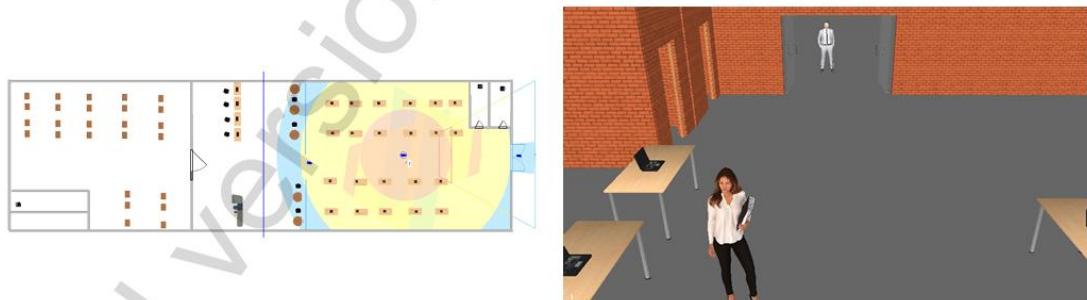
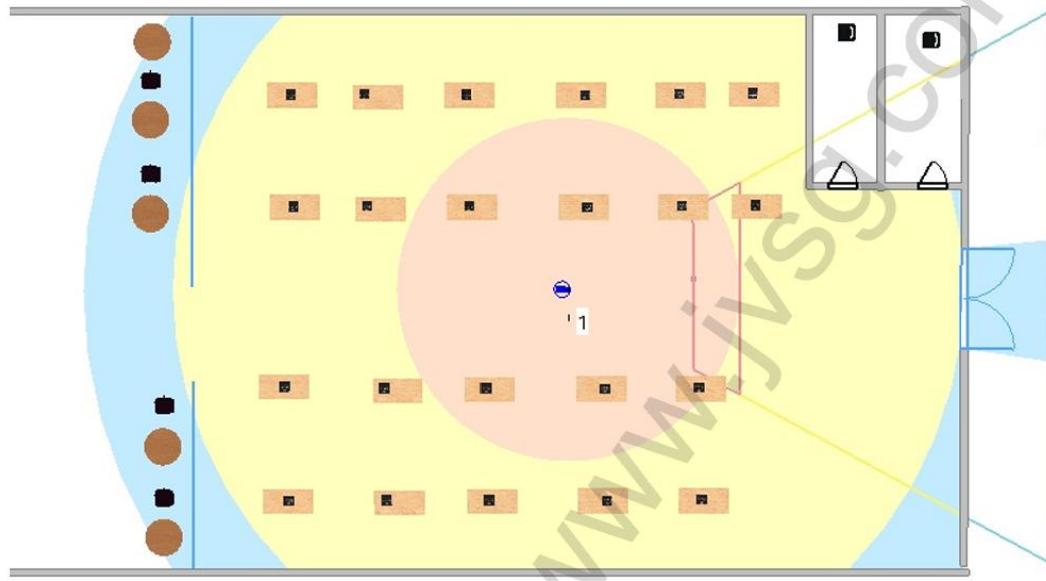


Hình 45. Cam 3 thu ngân

- Quan sát cửa ra vào



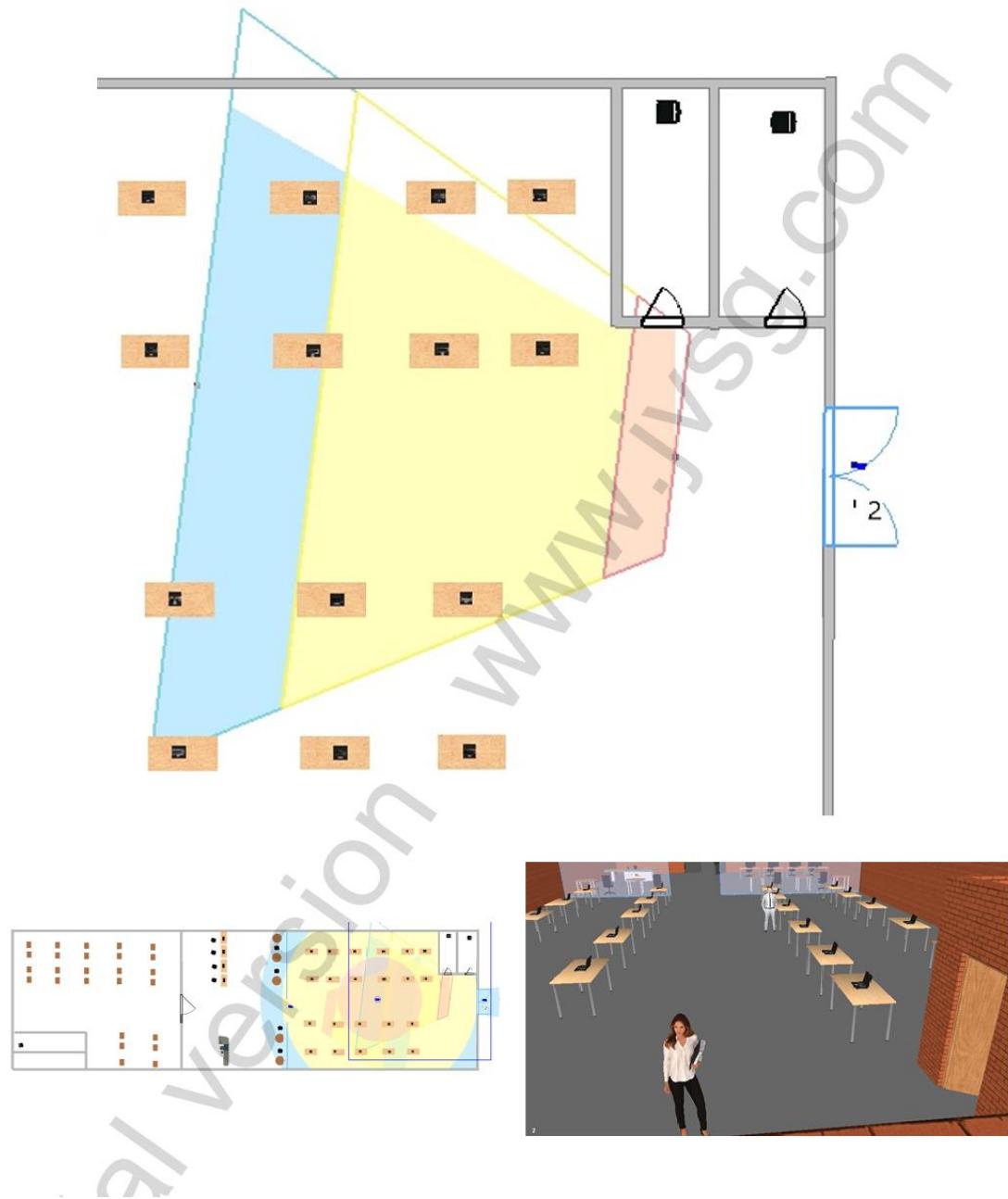
Camera 1 PTZ



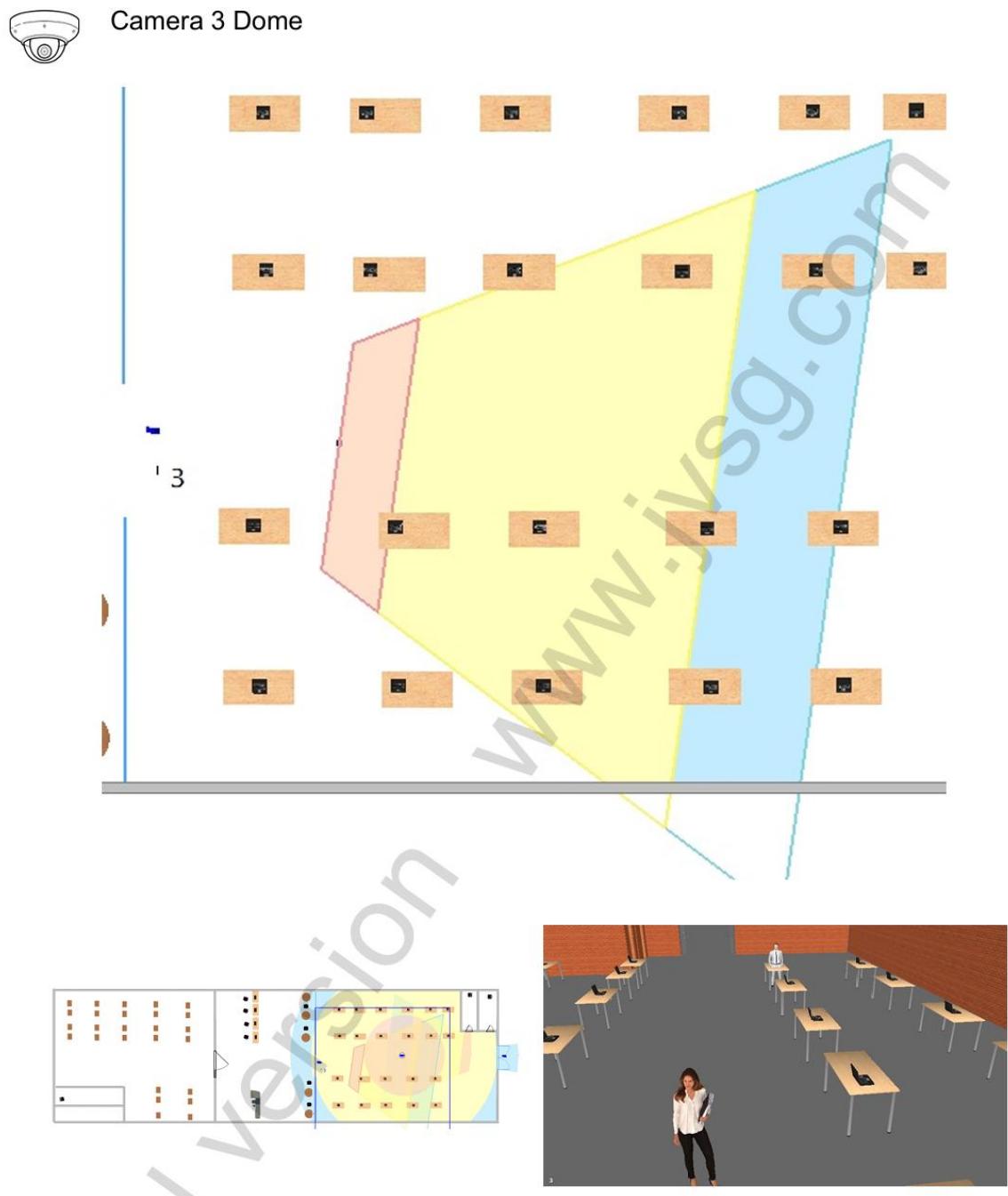
Hình 46. Cam 1 cửa



Camera 2 Dome



Hình 47. Cam 2 cửa

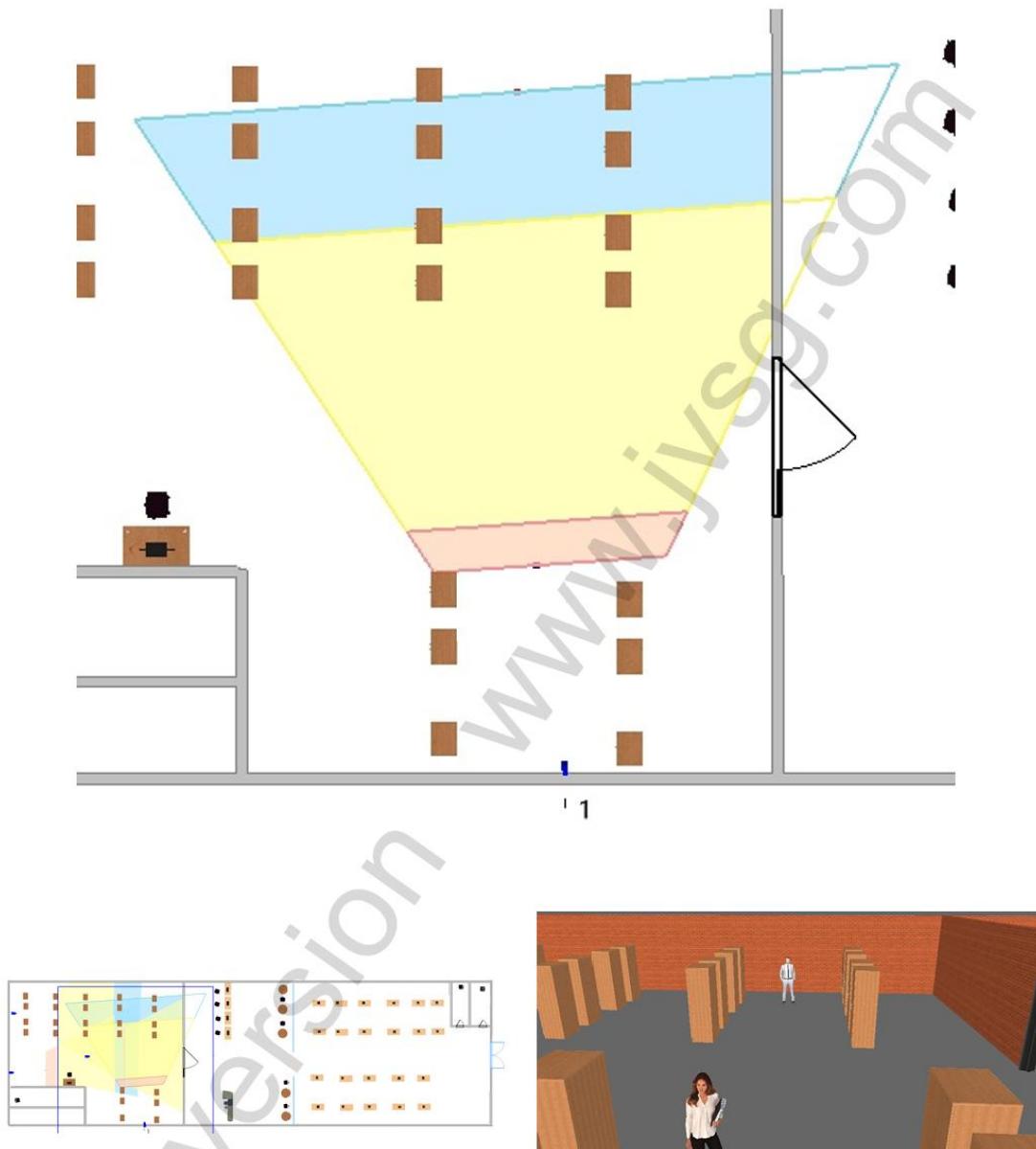


Hình 48. Cam 3 cửa

- giảm góc chết



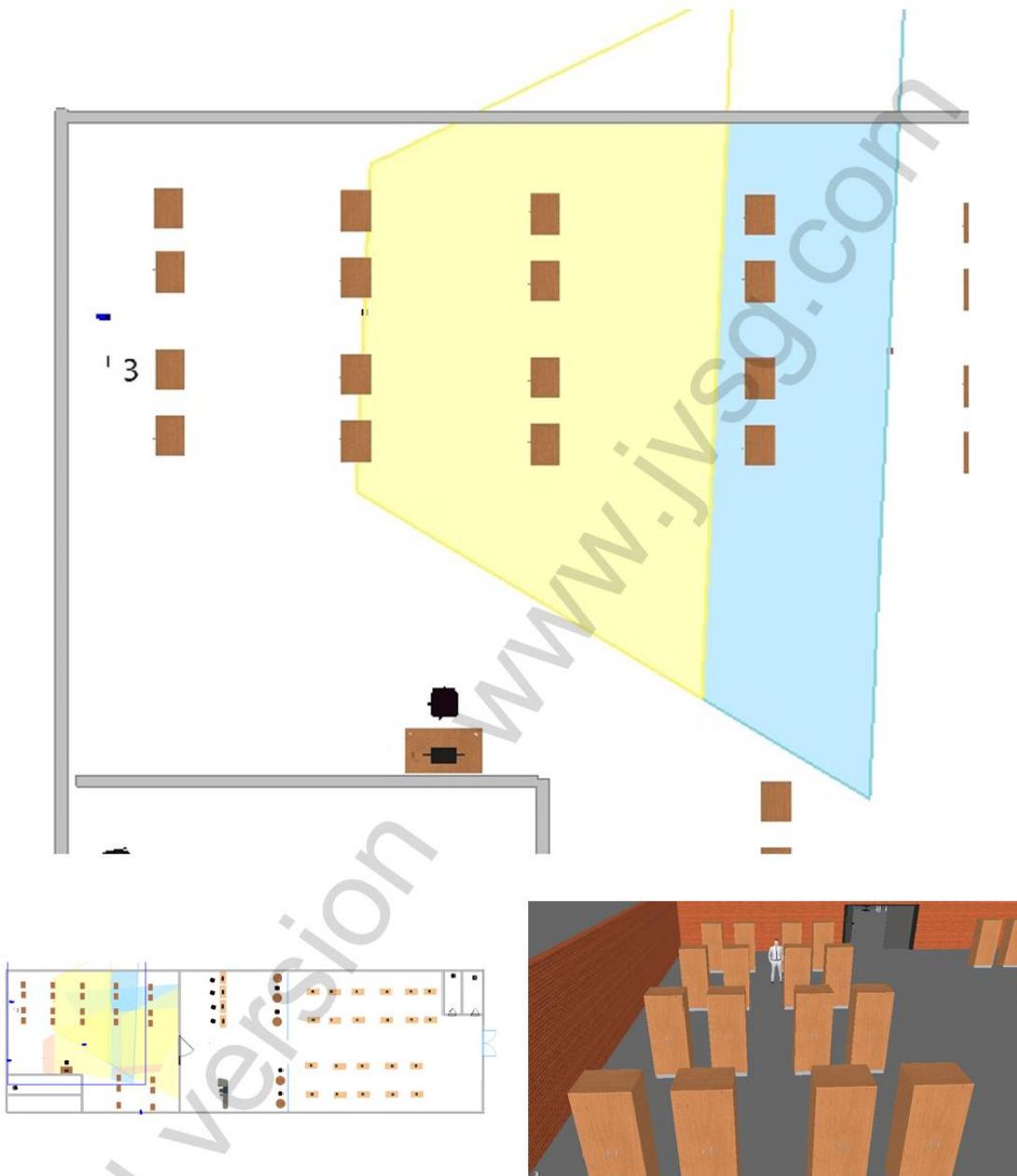
Camera 1 Turret



Hình 49. Cam 1 giảm góc chết



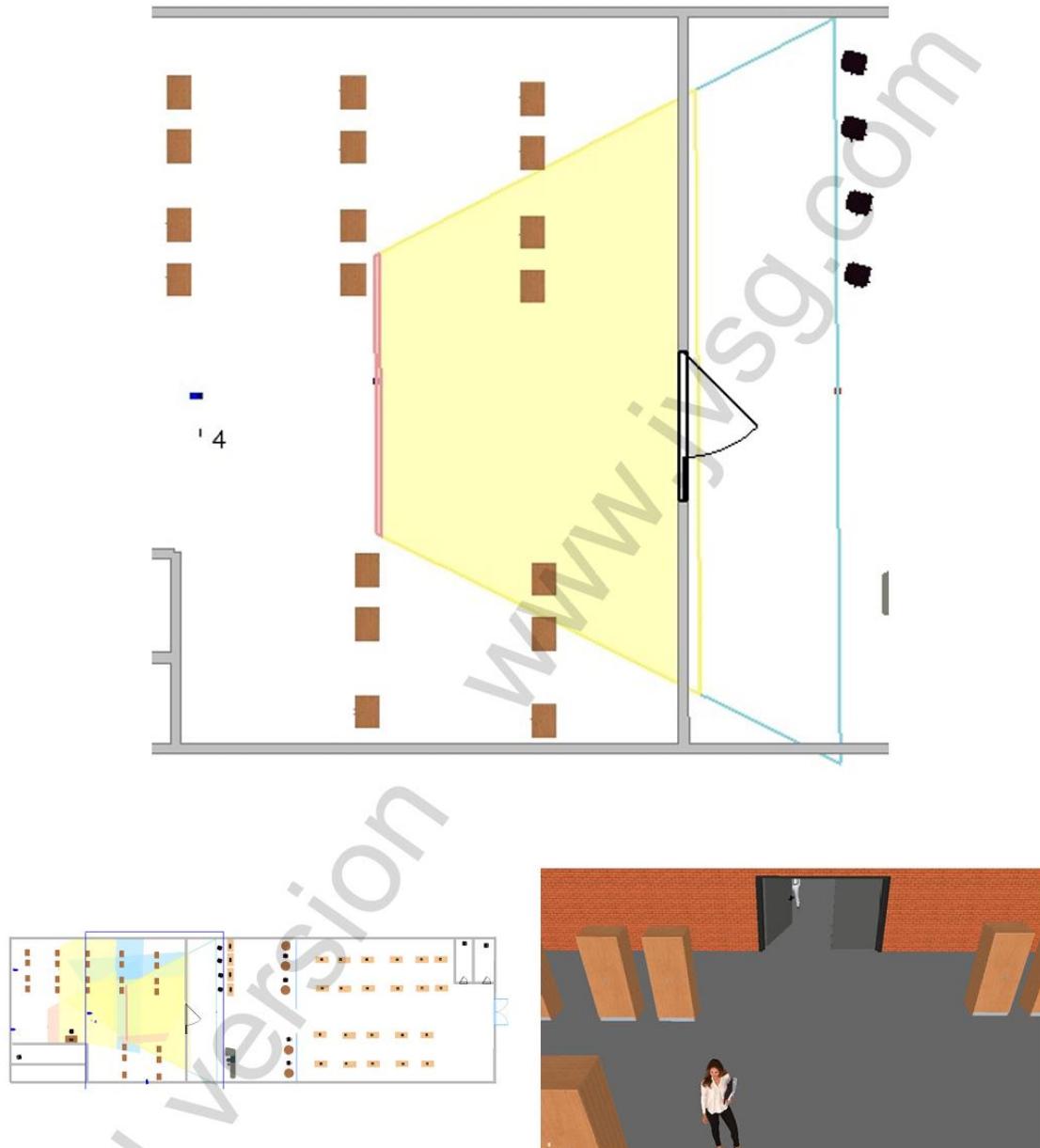
Camera 3 Turret



Hình 50. Cam 3 giảm góc chết



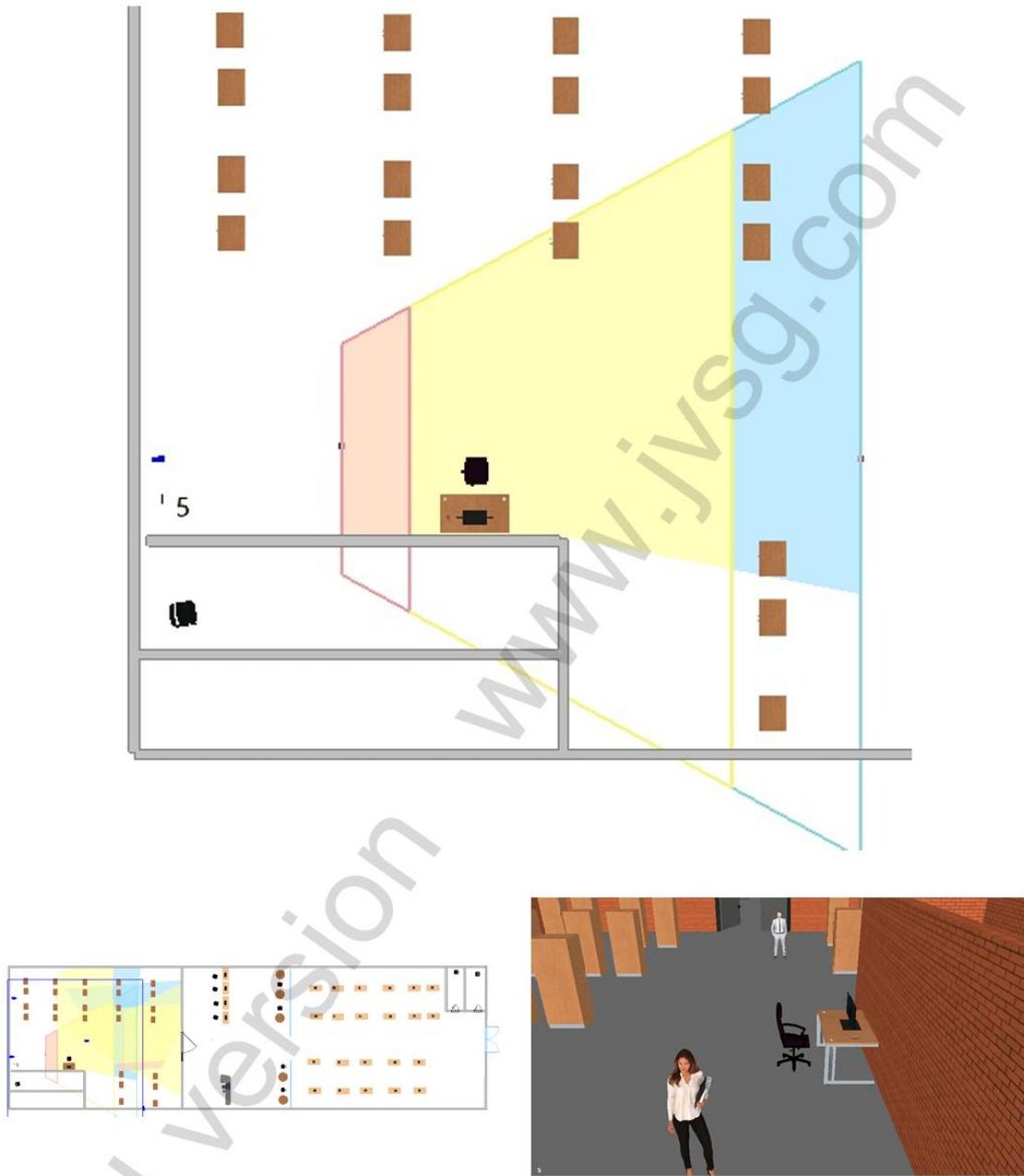
Camera 4 Dome



Hình 51. Cam 4 giảm góc chét



Camera 5 Box

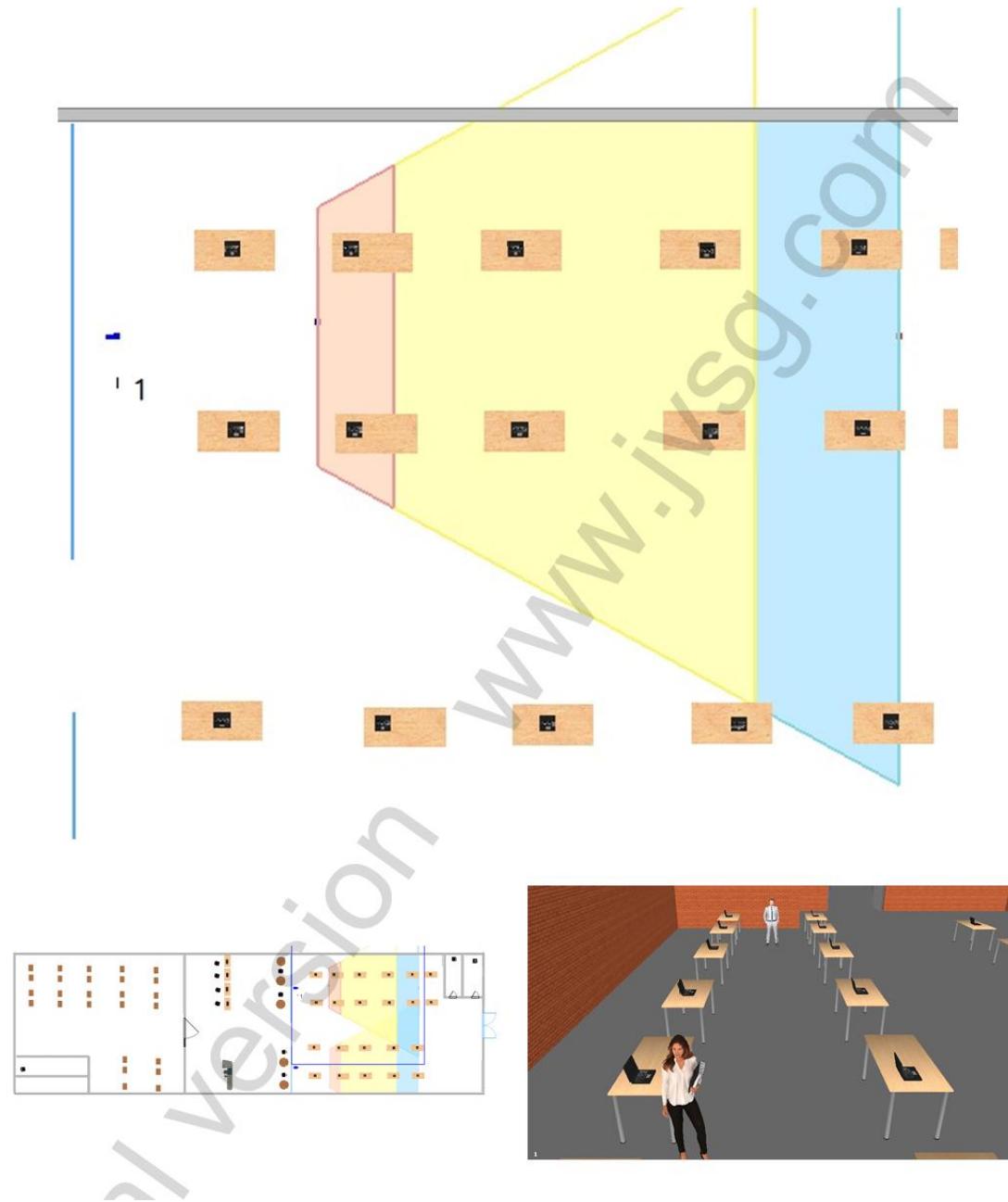


Hình 52. Cam 5 giảm góc chết

- Quan sát khu trưng bày



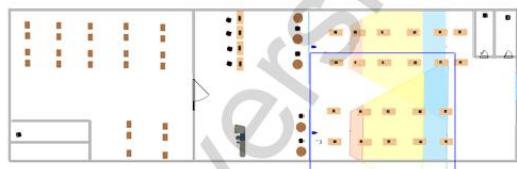
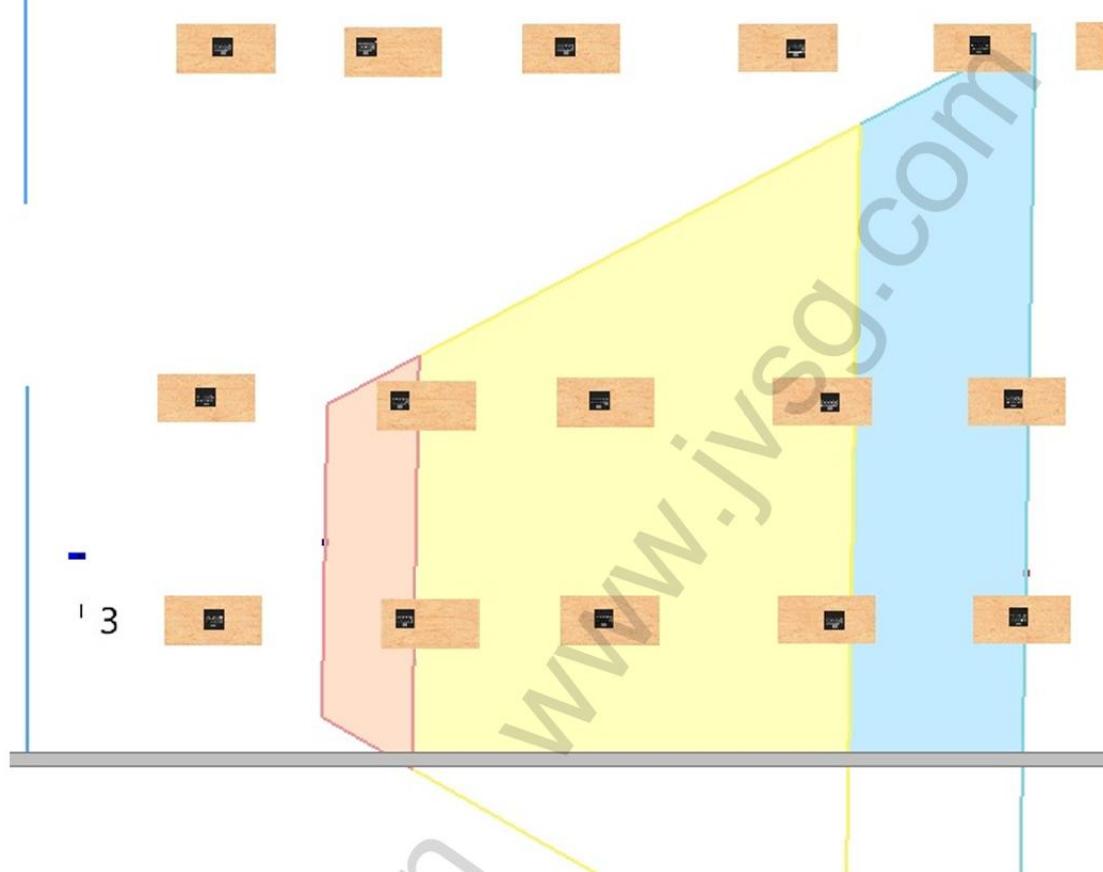
Camera 1 Turret



Hình 53. Cam 4 trung bày



Camera 3 Turret

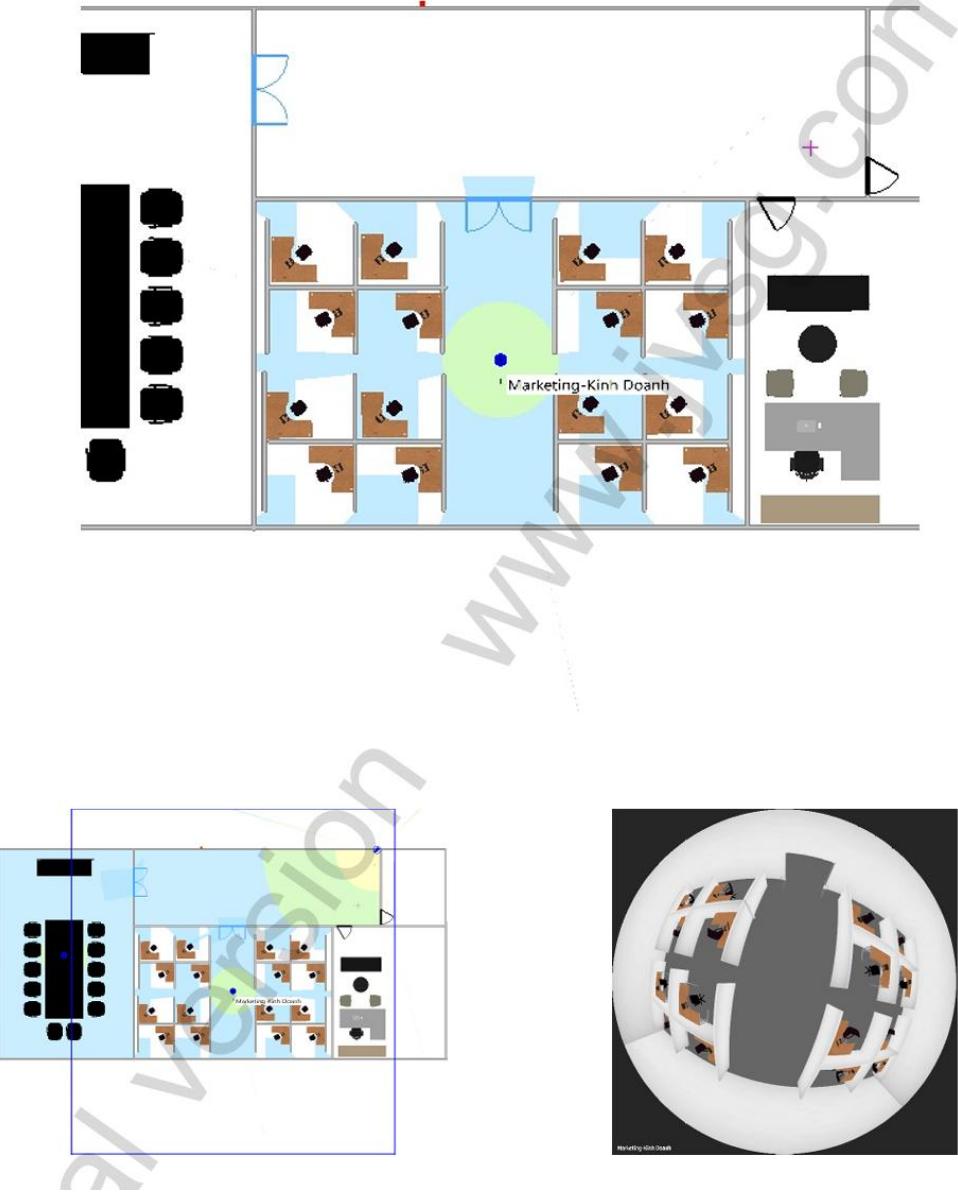


Hình 54. Cam 3 trung bày

- **Tầng 2**



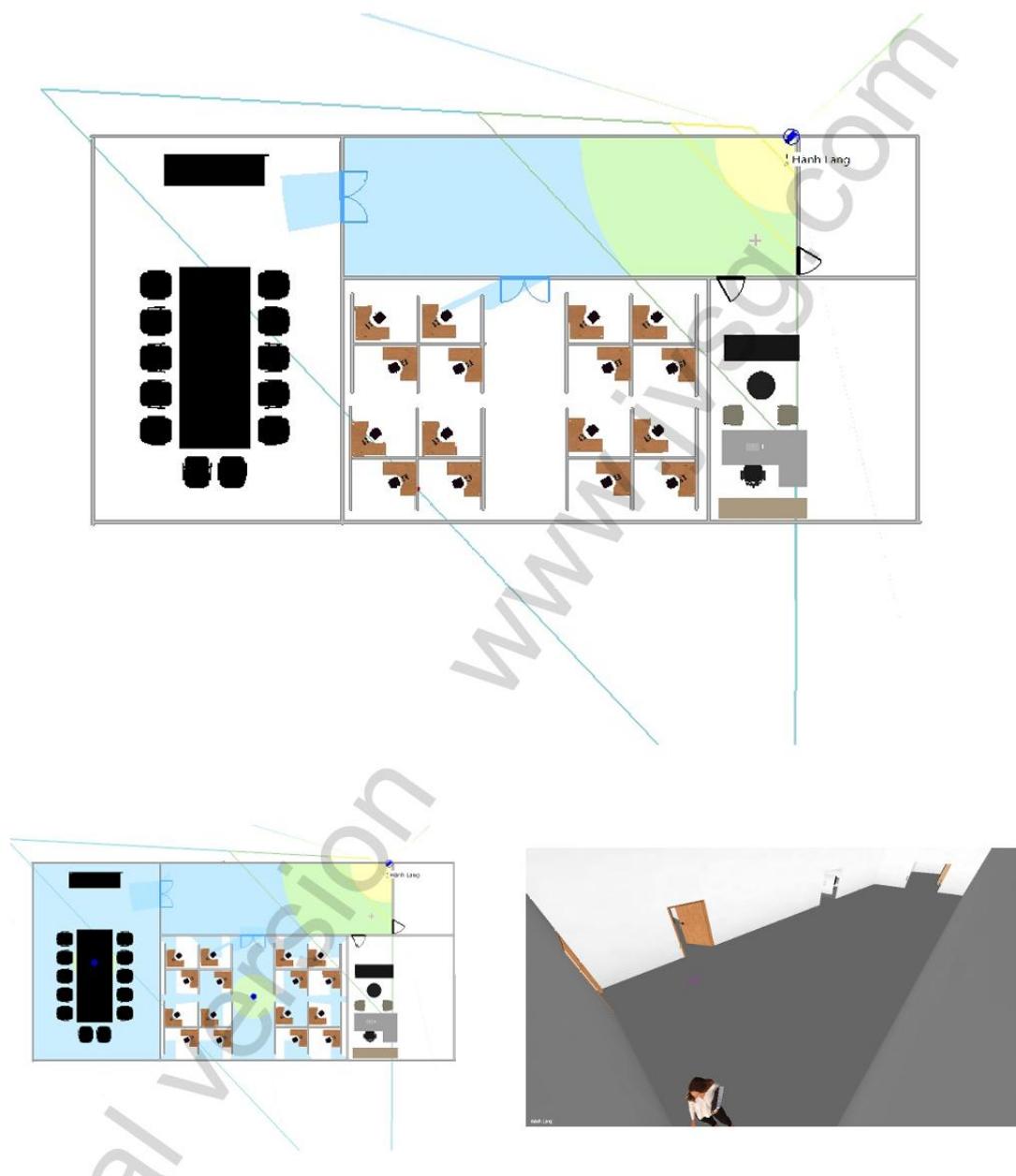
Camera Marketing-Kinh Doanh Fisheye



Hình 55. Camera marketing- kinh doanh



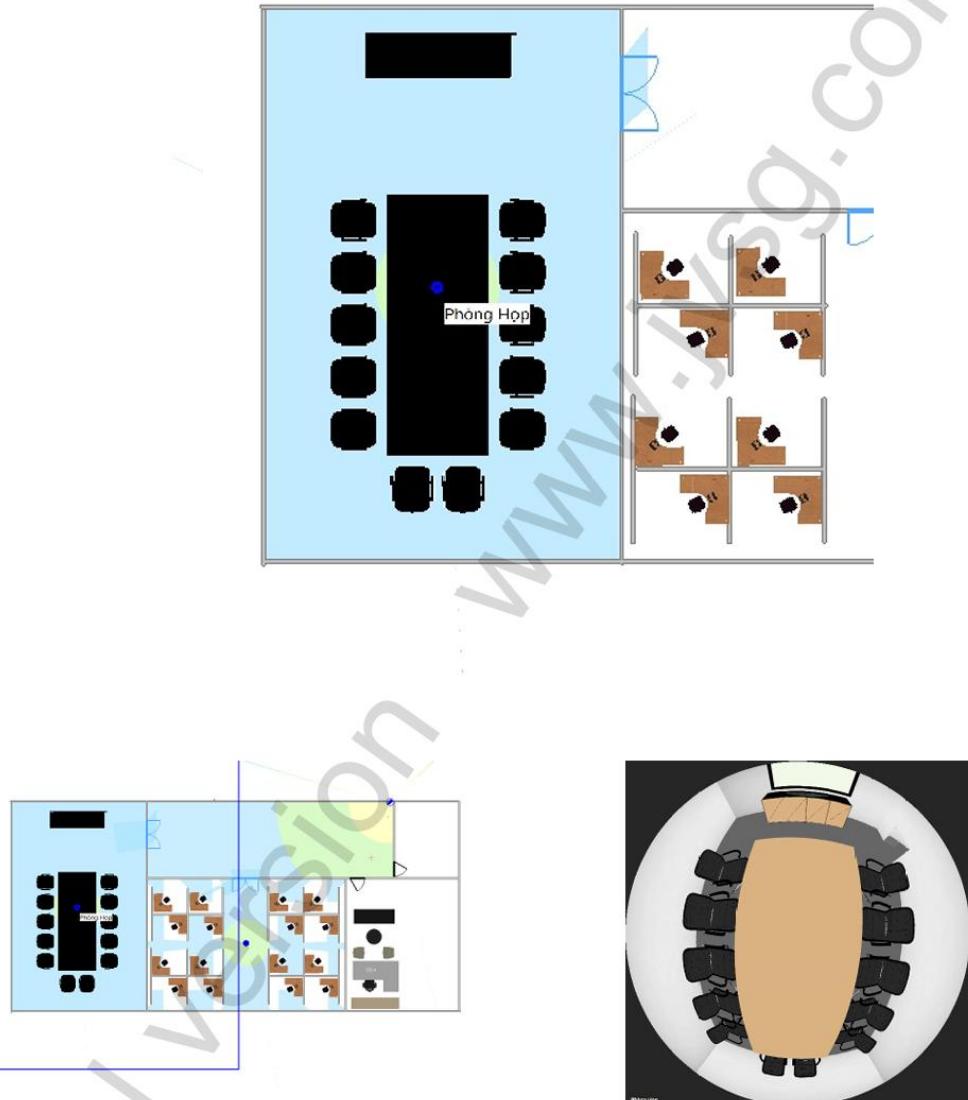
Camera Hành Lang PTZ



Hình 56. Cam hành lang tầng 2



Camera Phòng Hp Fisheye

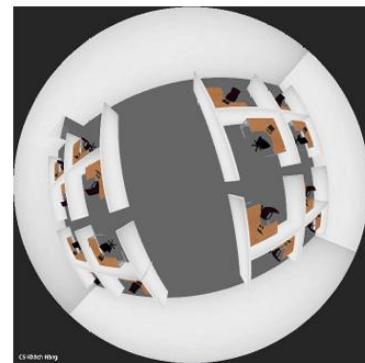
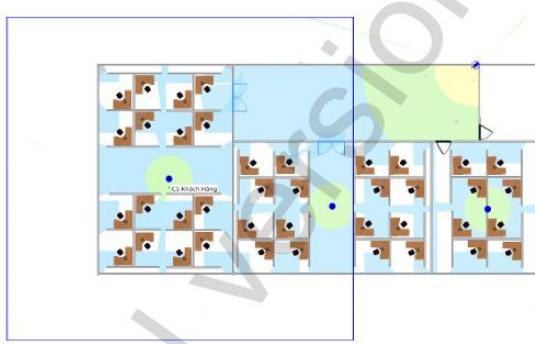
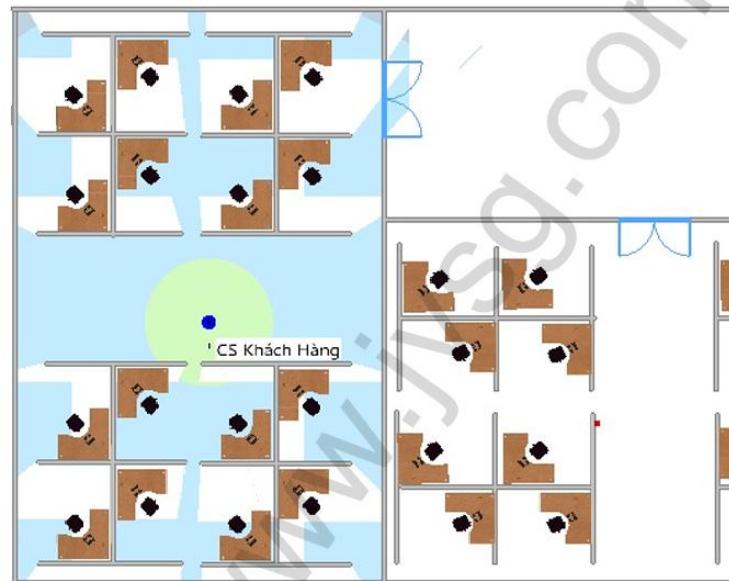


Hình 57. Cam phòng họp

- Tầng 3



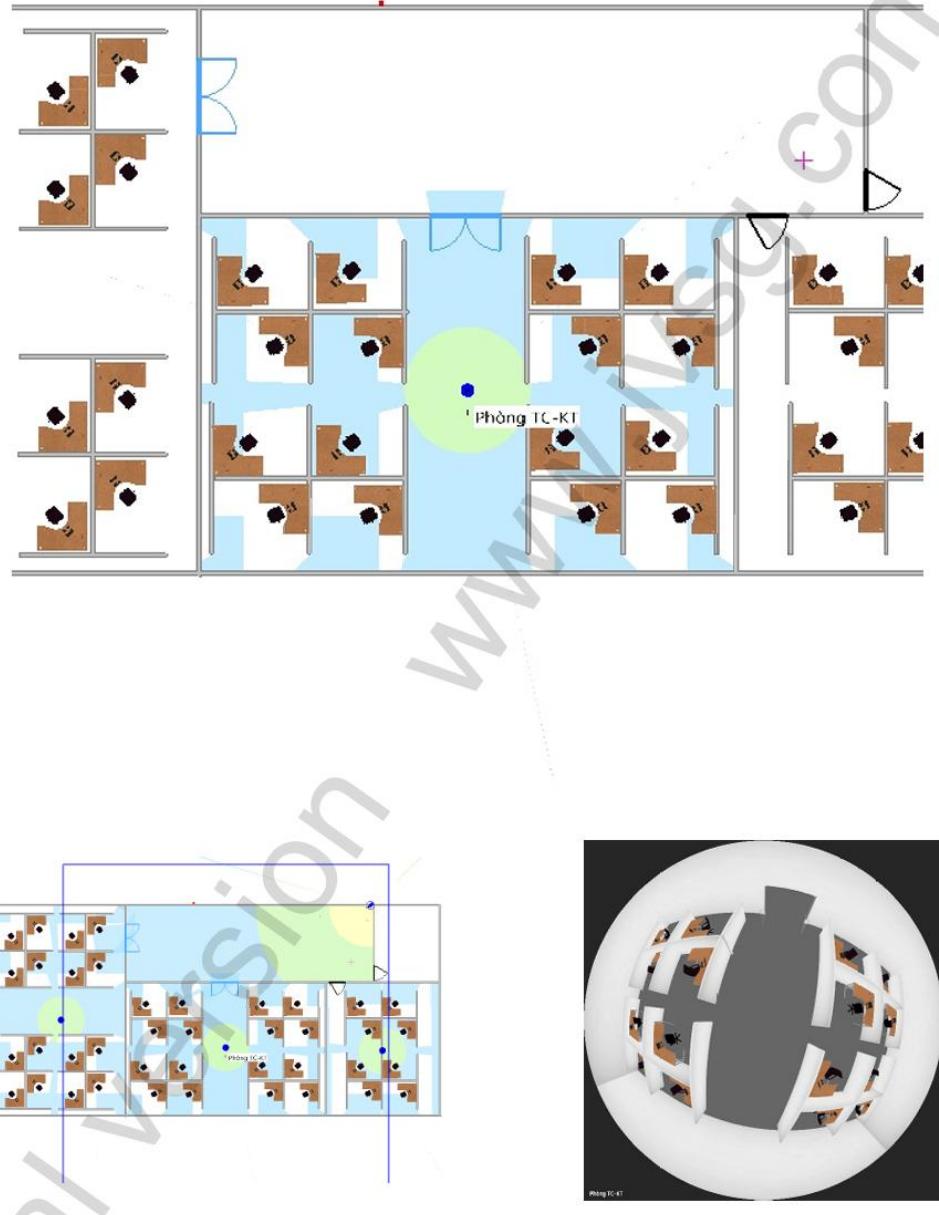
Camera CS Khách Hàng Fisheye



Hình 58. Cam chăm sóc khách hàng



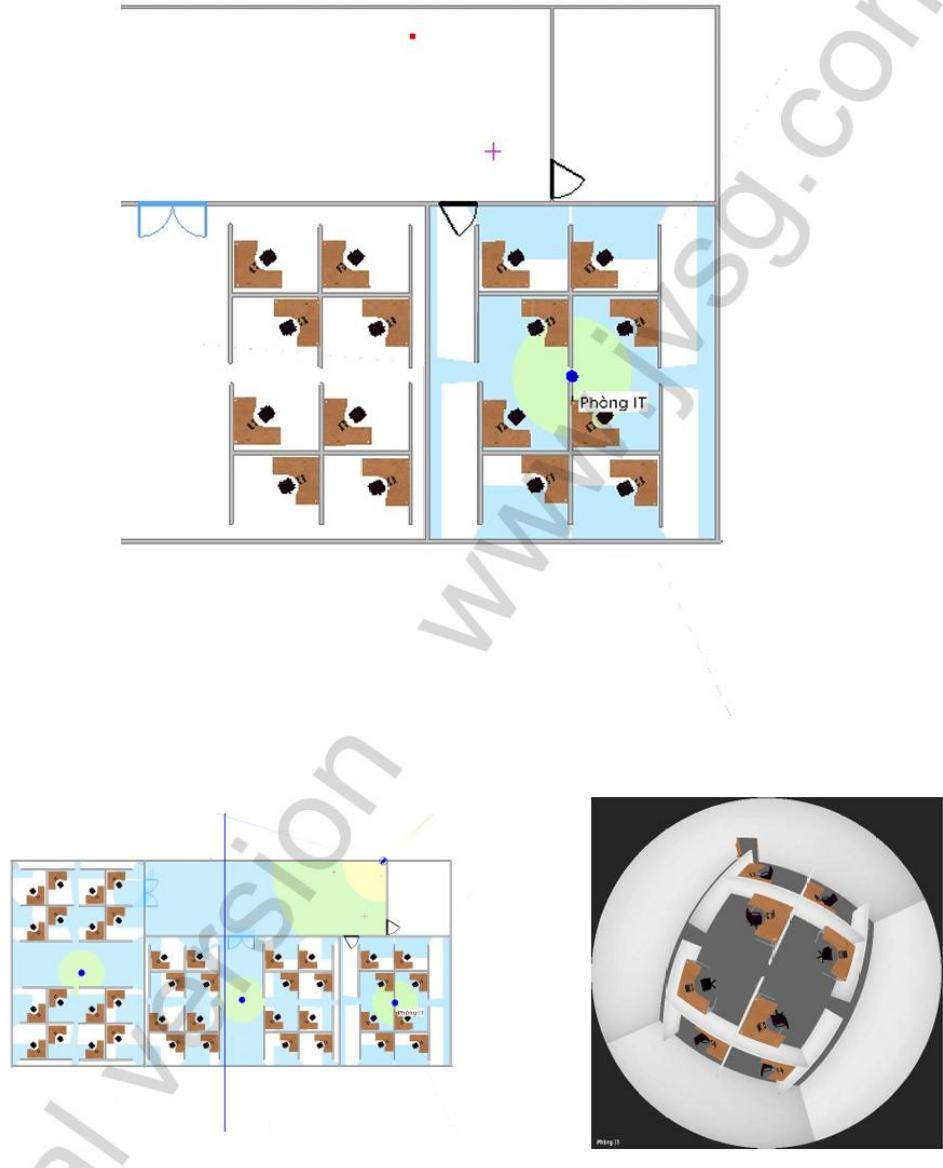
Camera Phòng TC-KT Fisheye



Hình 59. Cam tài chính kề toán



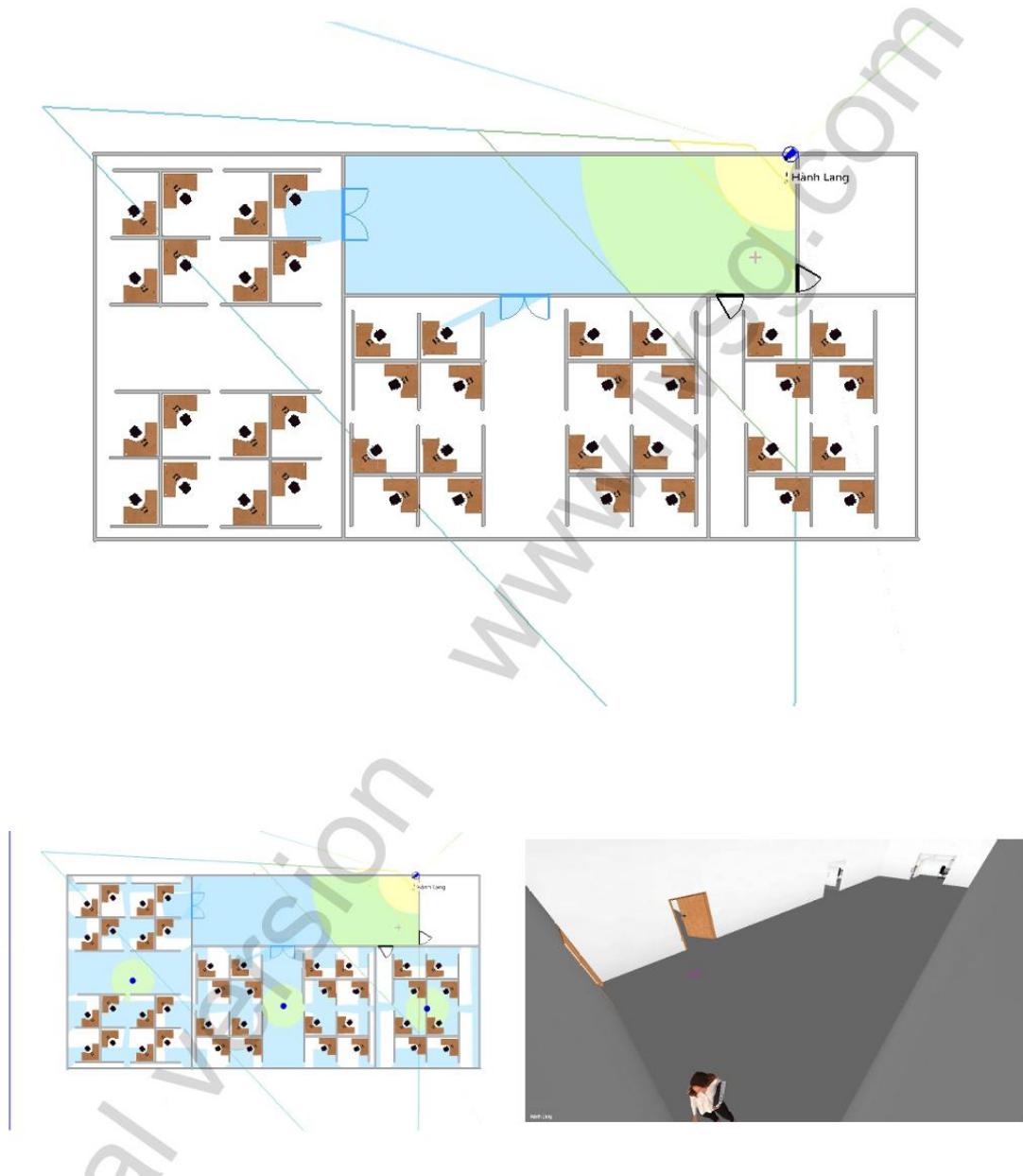
Camera Phòng IT Fisheye



Hình 60. Cam phòng IT



Camera Hành Lang PTZ

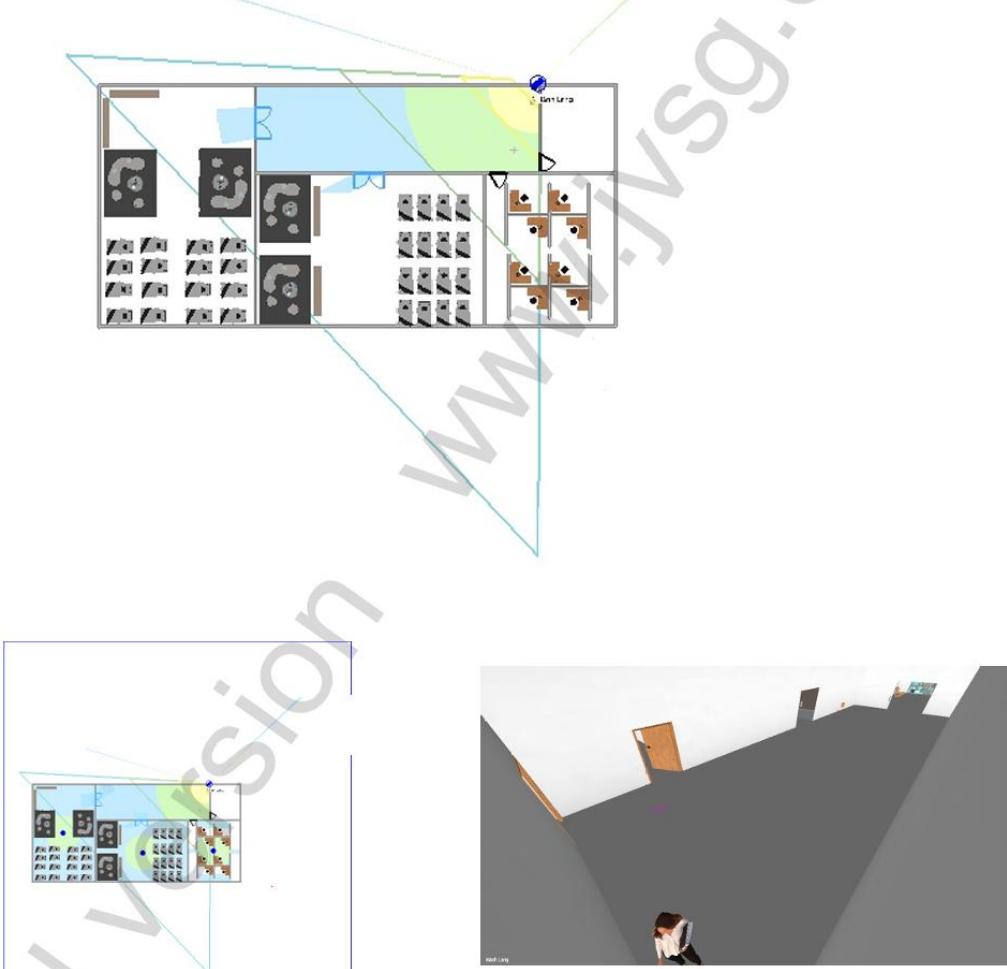


Hình 61. Cam hành lang tầng 3

- Tầng 4



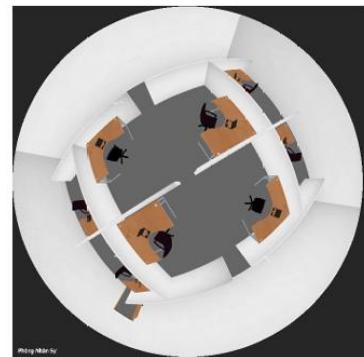
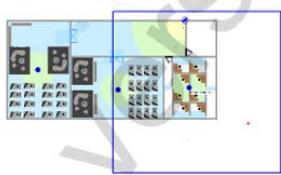
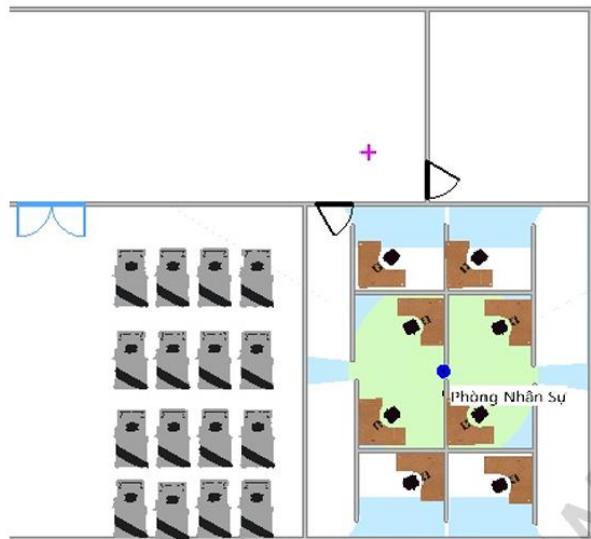
Camera Hành Lang PTZ



Hình 62. Cam hành lang tầng 4



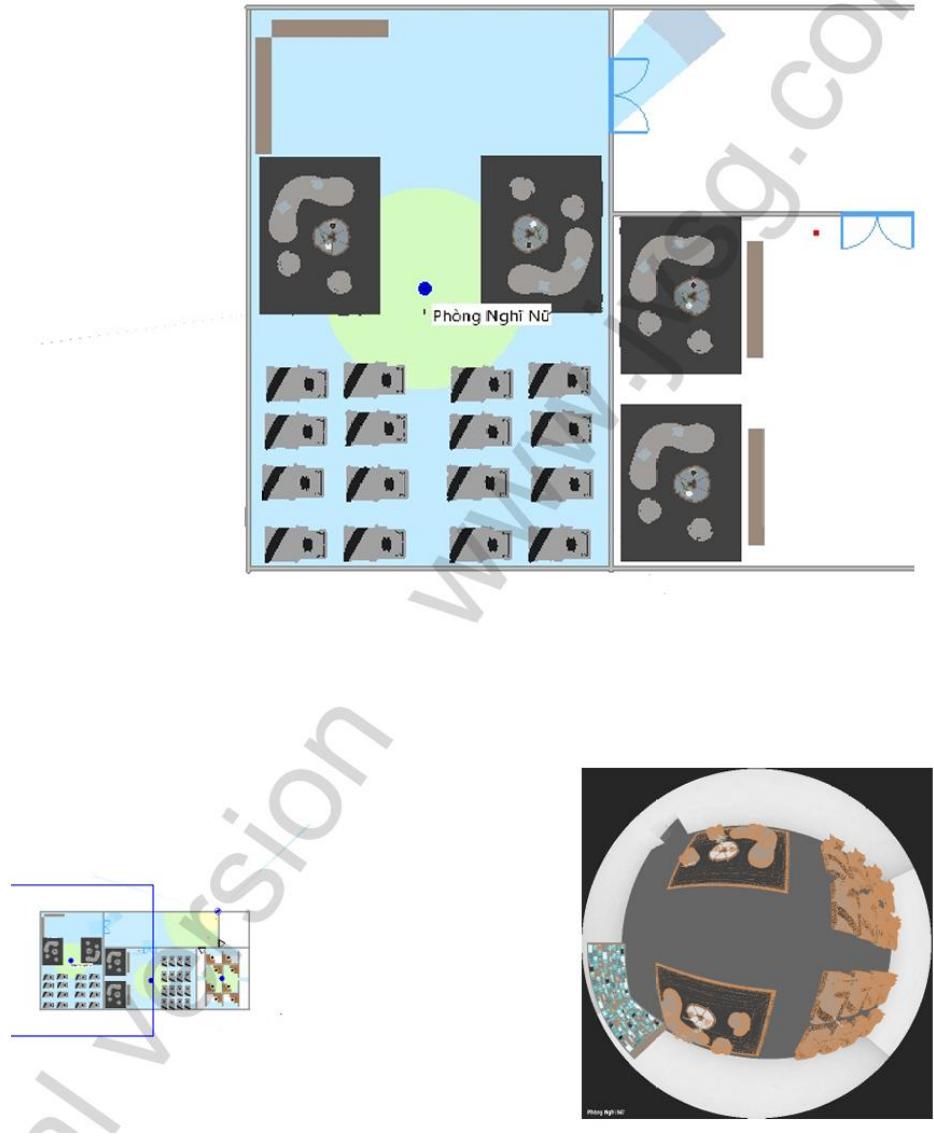
Camera Phòng Nhân S Fisheye



Hình 63. Cam phòng nhân sự



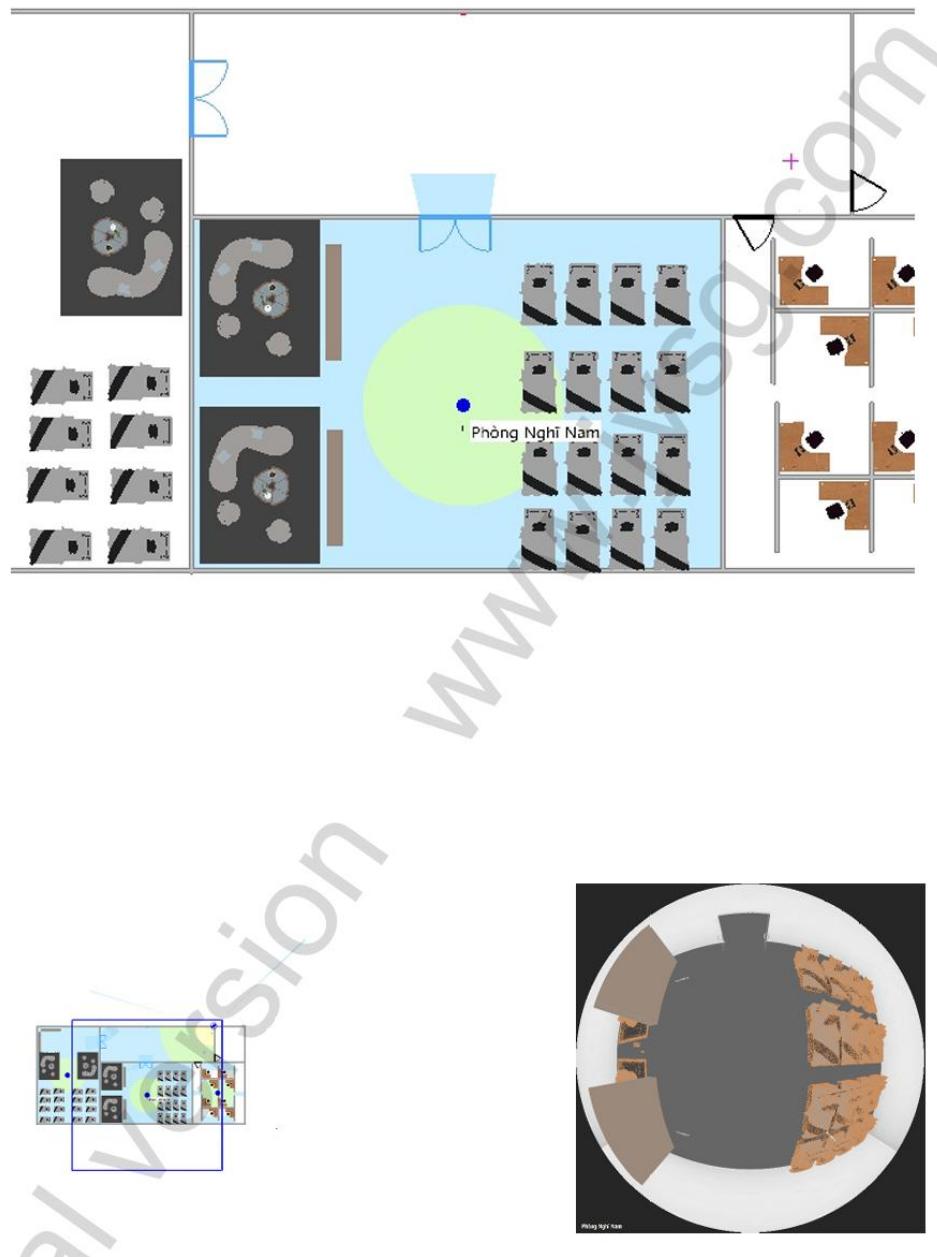
Camera Phòng Ngh N Fisheye



Hình 64. Cam phòng nghỉ nữ

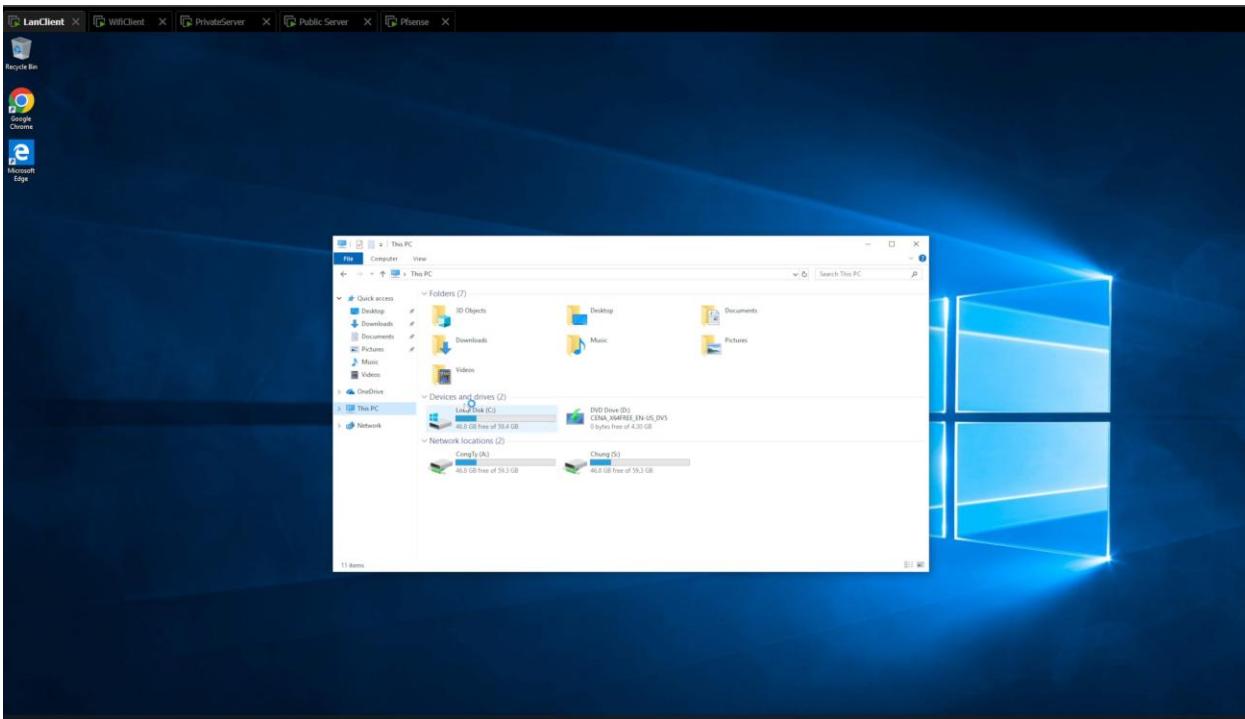


Camera Phòng Nghỉ Nam Fisheye

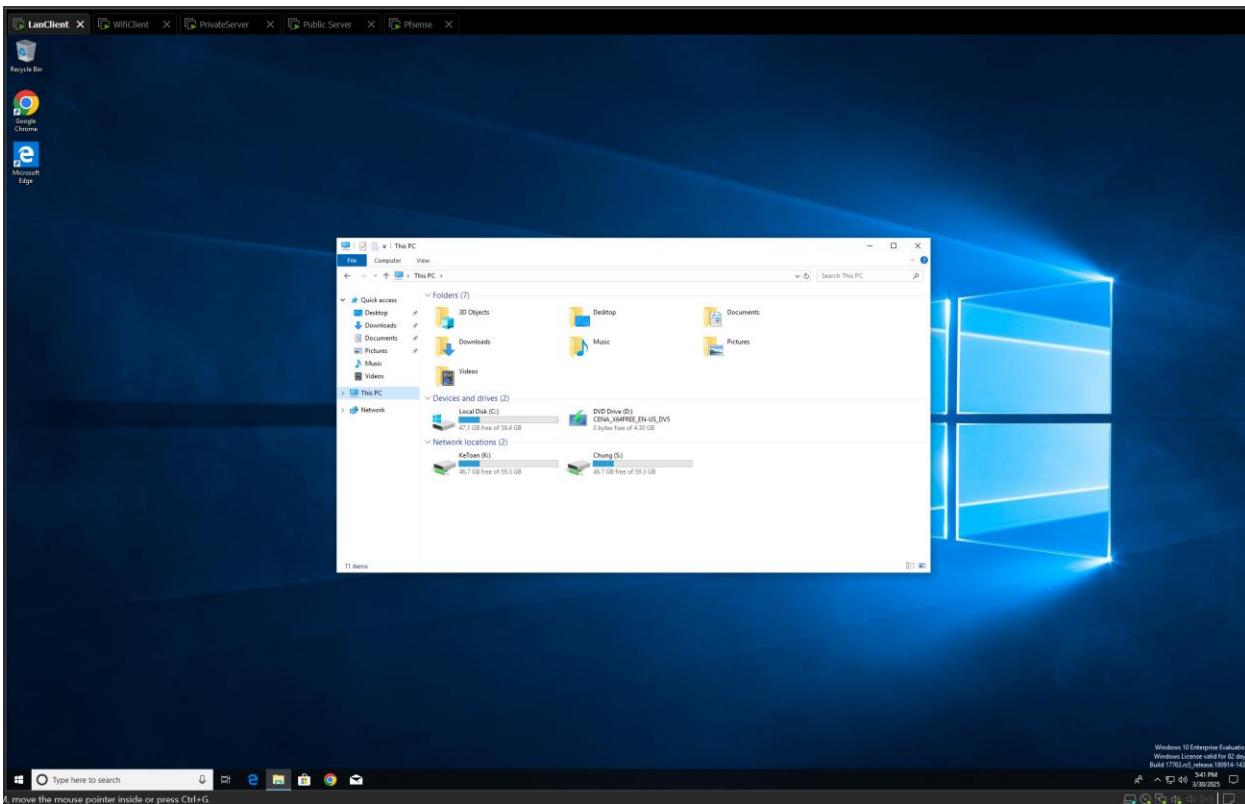


Hình 65. Cam phòng nghỉ nam

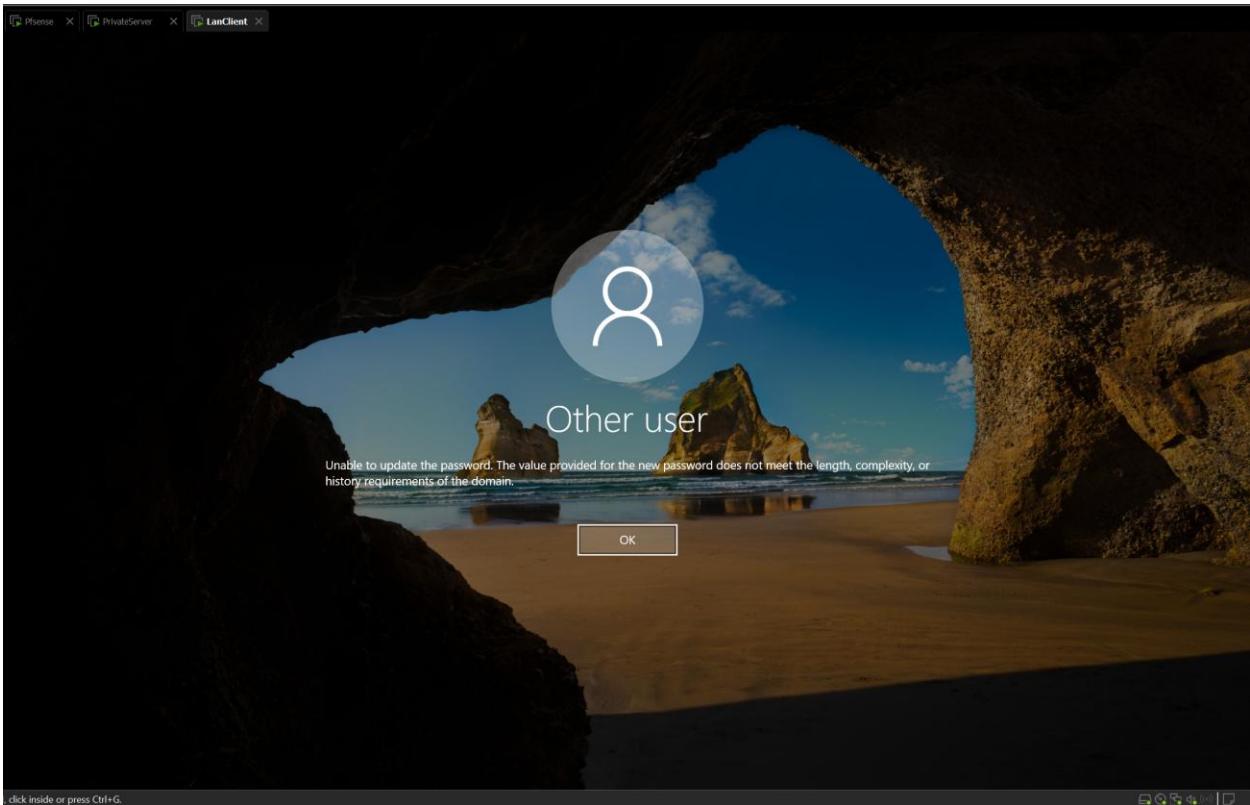
b. Bảo mật hệ điều hành



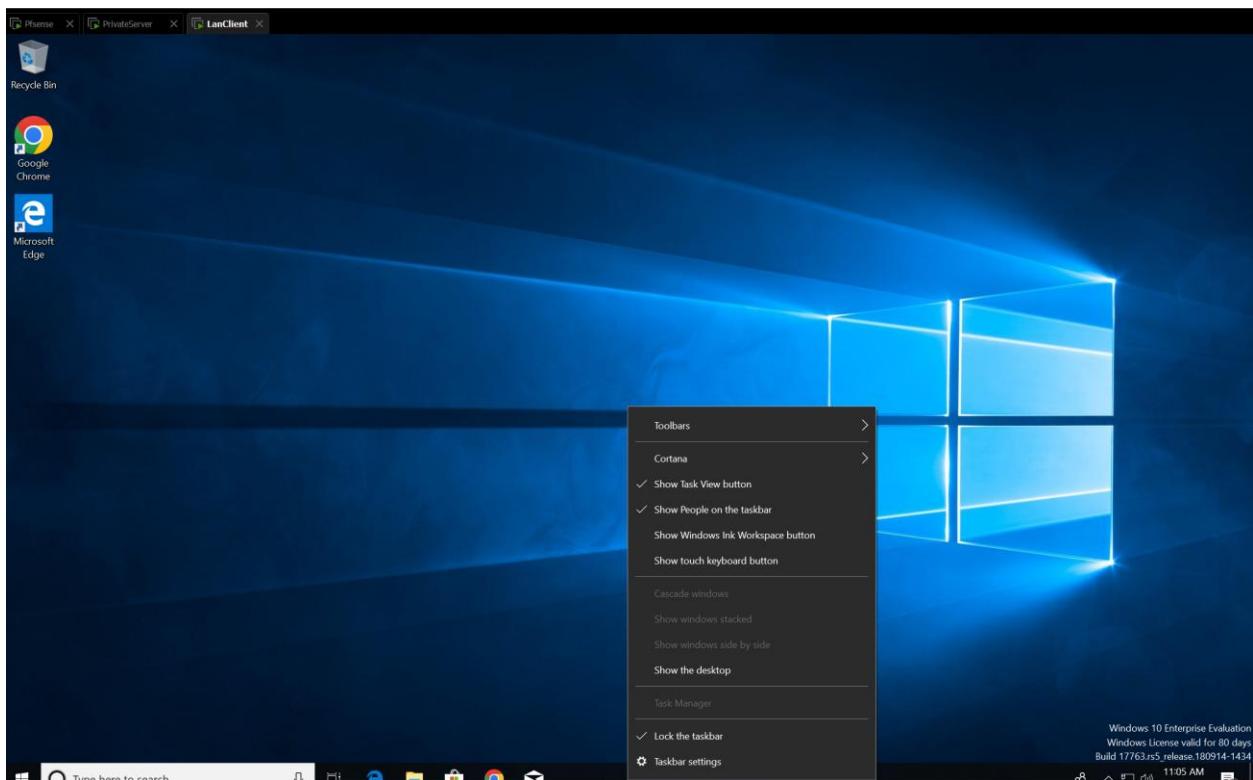
Hình 66. Kết quả triển khai map ổ đĩa



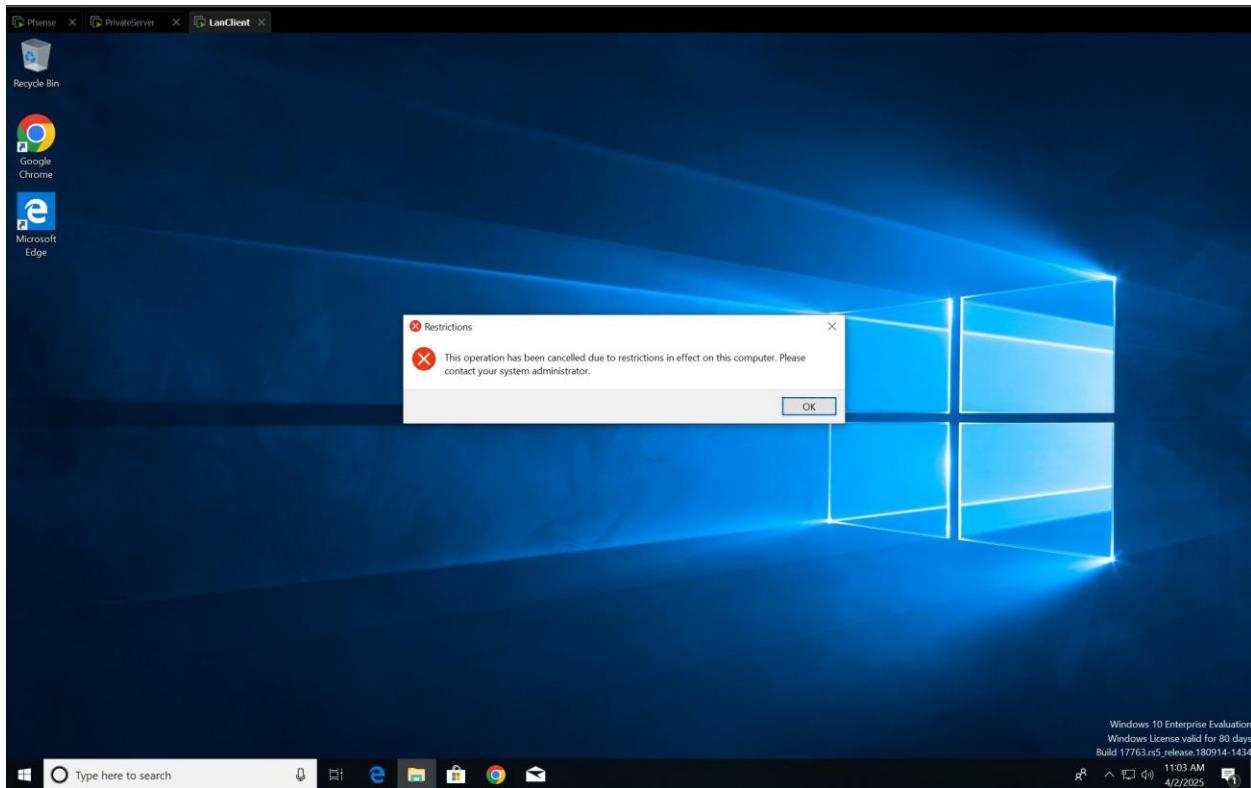
Hình 67. Thư mục share của kè toán



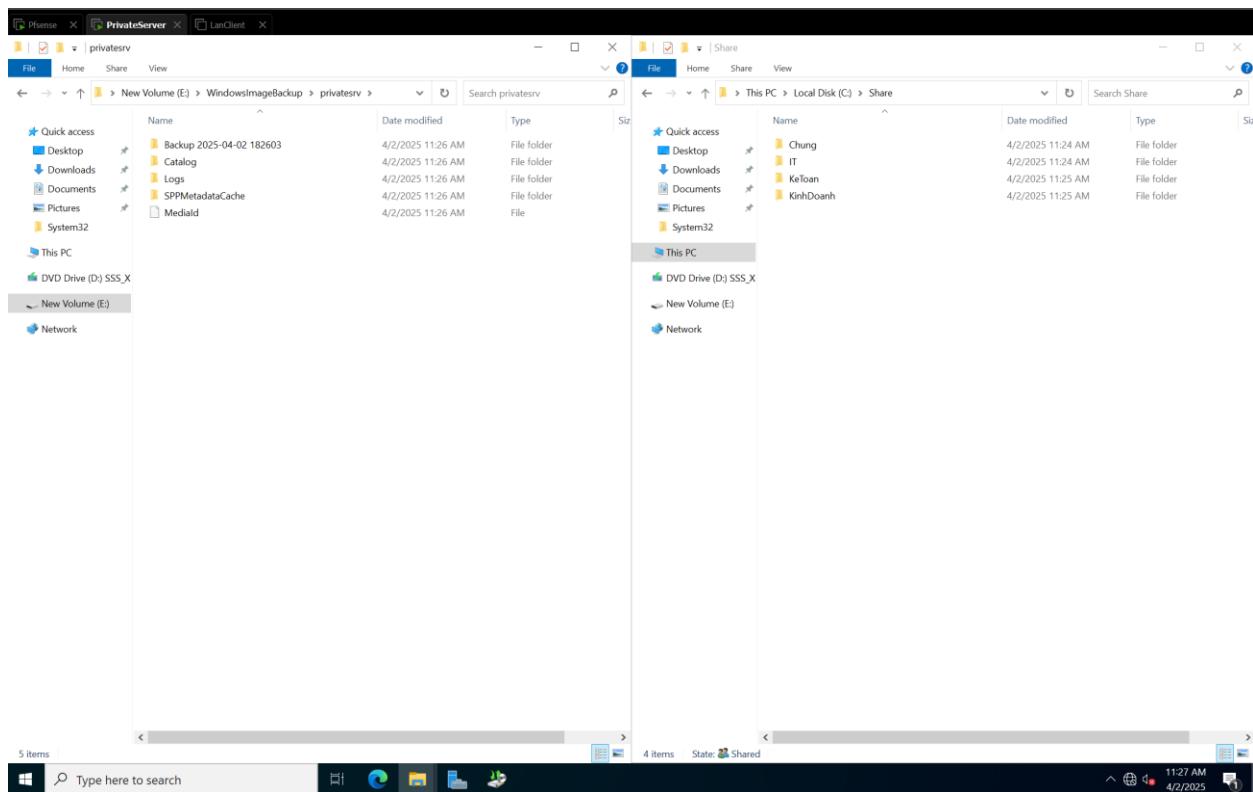
Hình 68. Mật khẩu đổi lại phải đúng định dạng



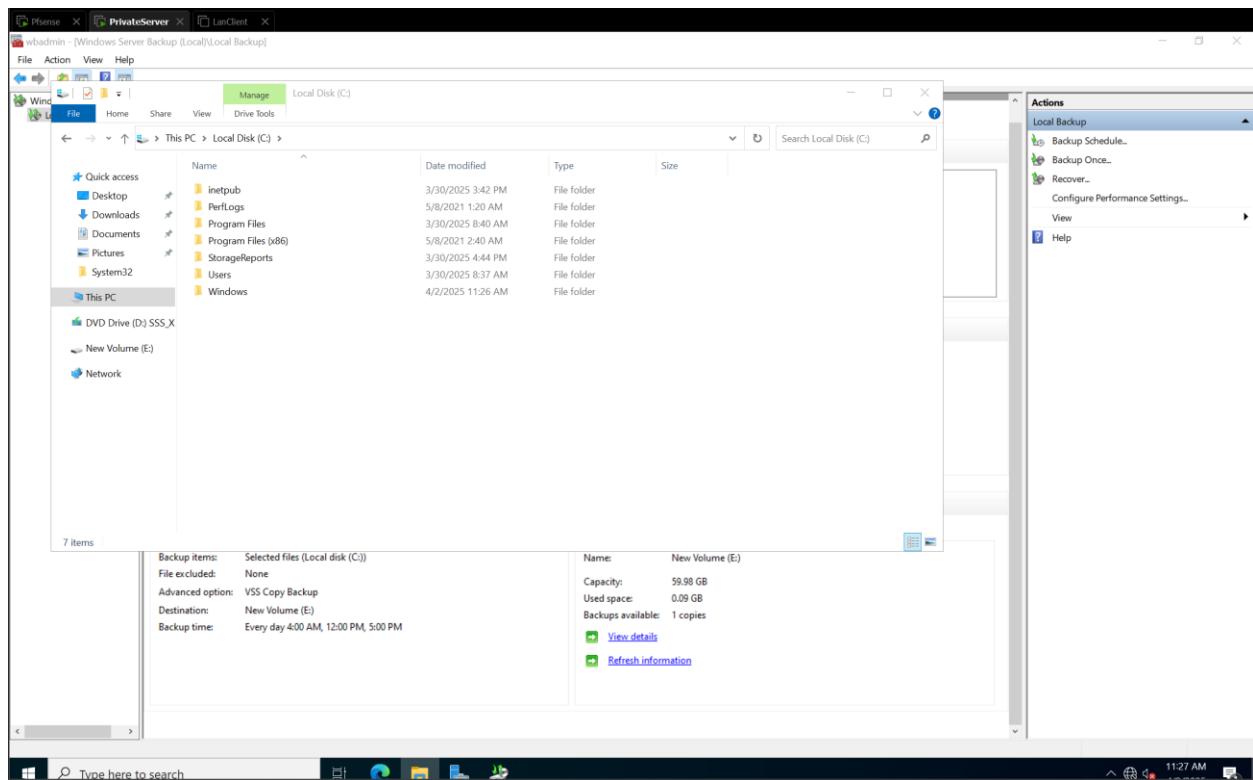
Hình 69. Tắt TaskManager



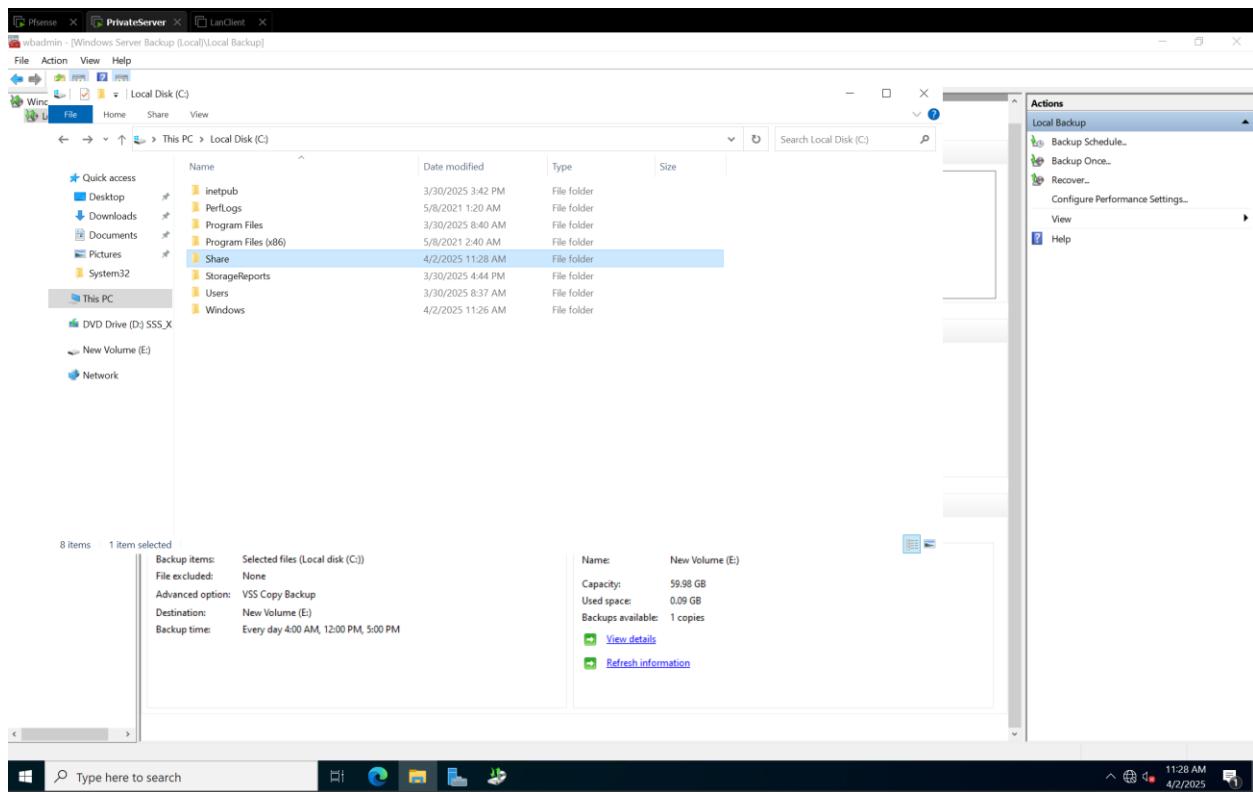
Hình 70. Không thể truy cập control panel



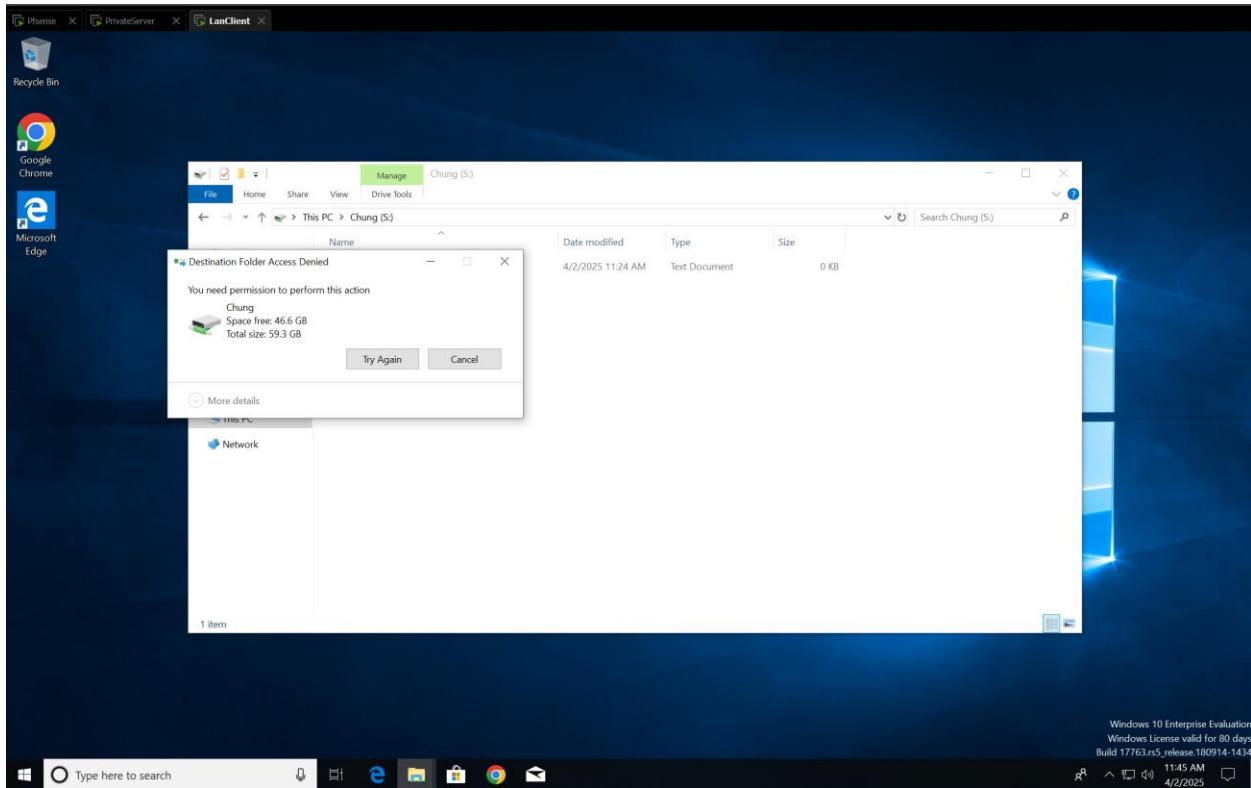
Hình 71. Back up theo ngày



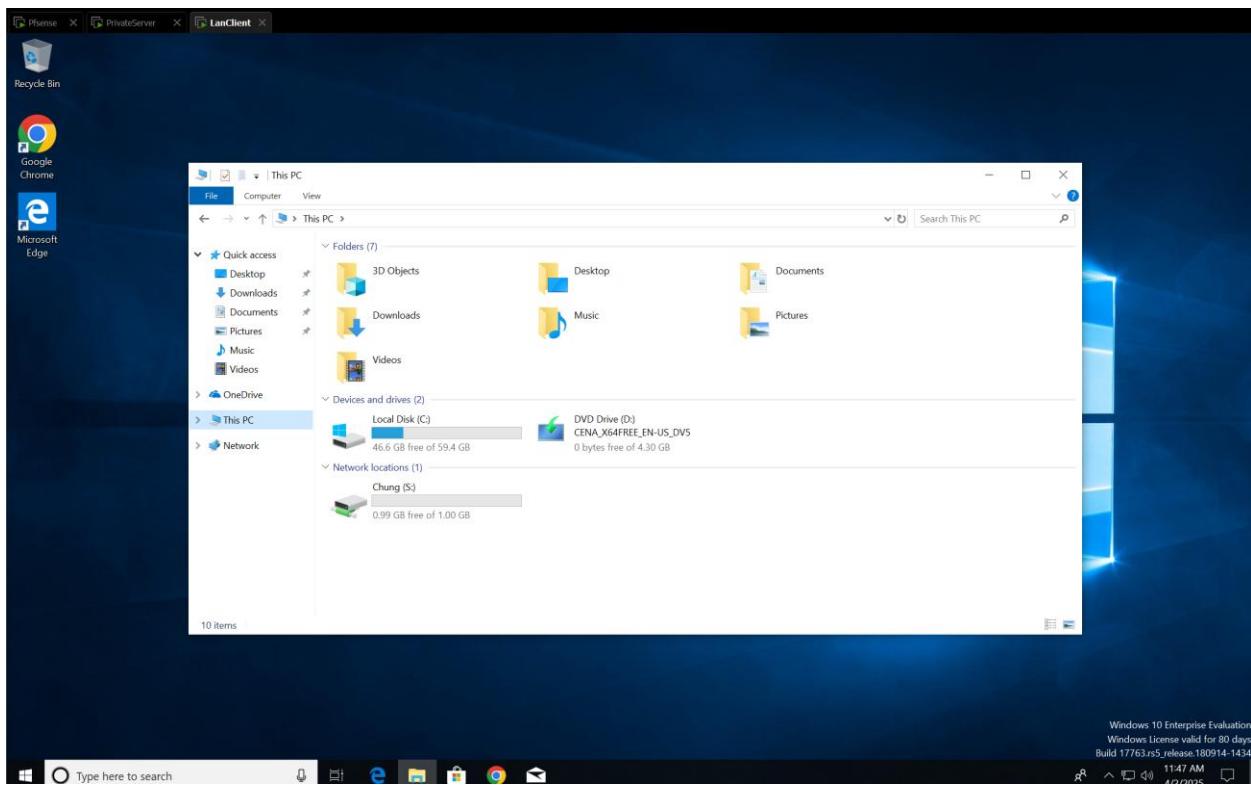
Hình 72. Khi dữ liệu chung bị mất



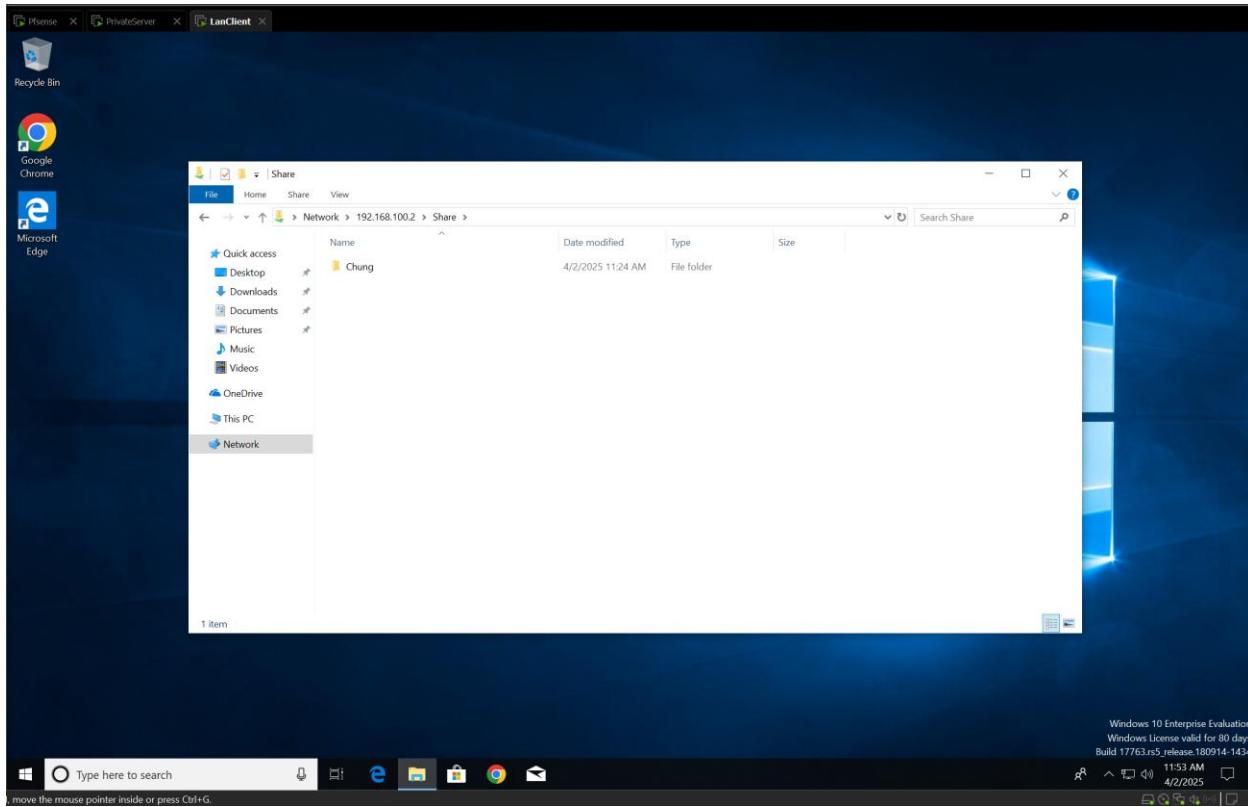
Hình 73. Khôi phục thành công



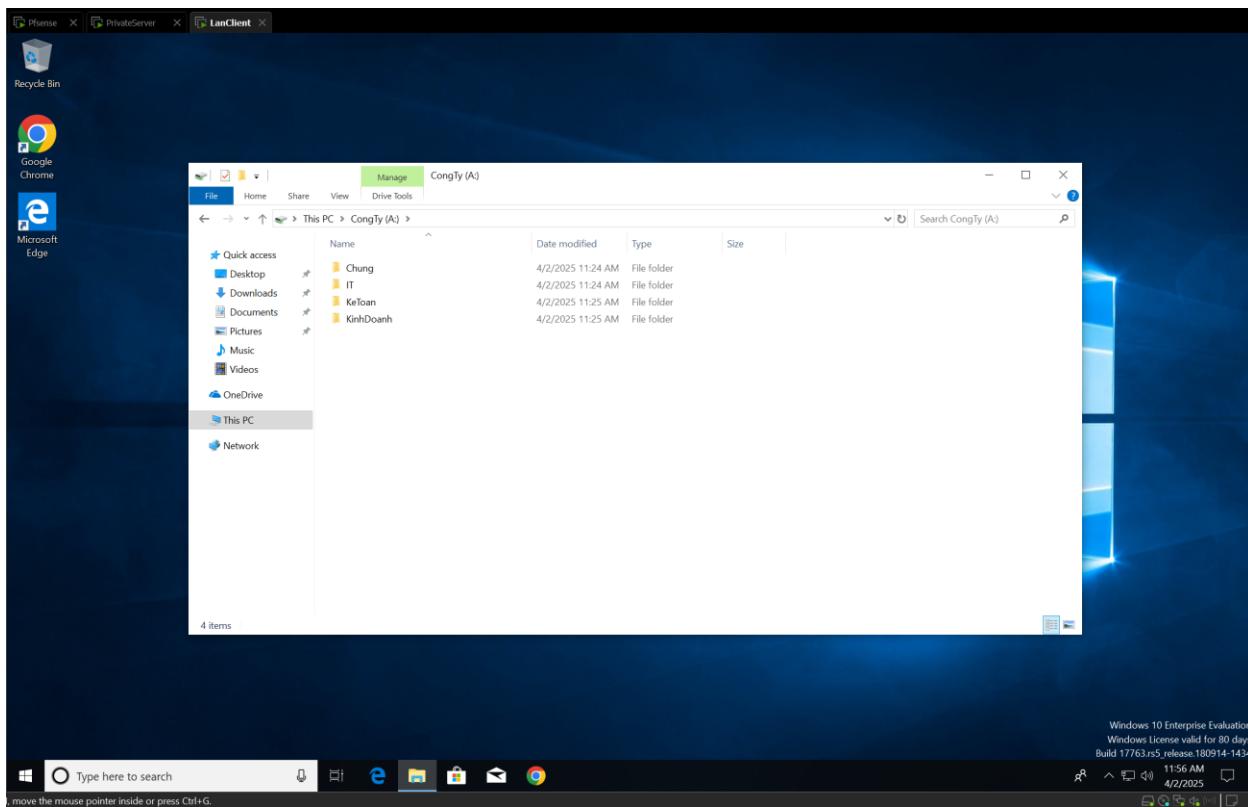
Hình 74. Không thể chép file thực thi vào thư mục của công ty



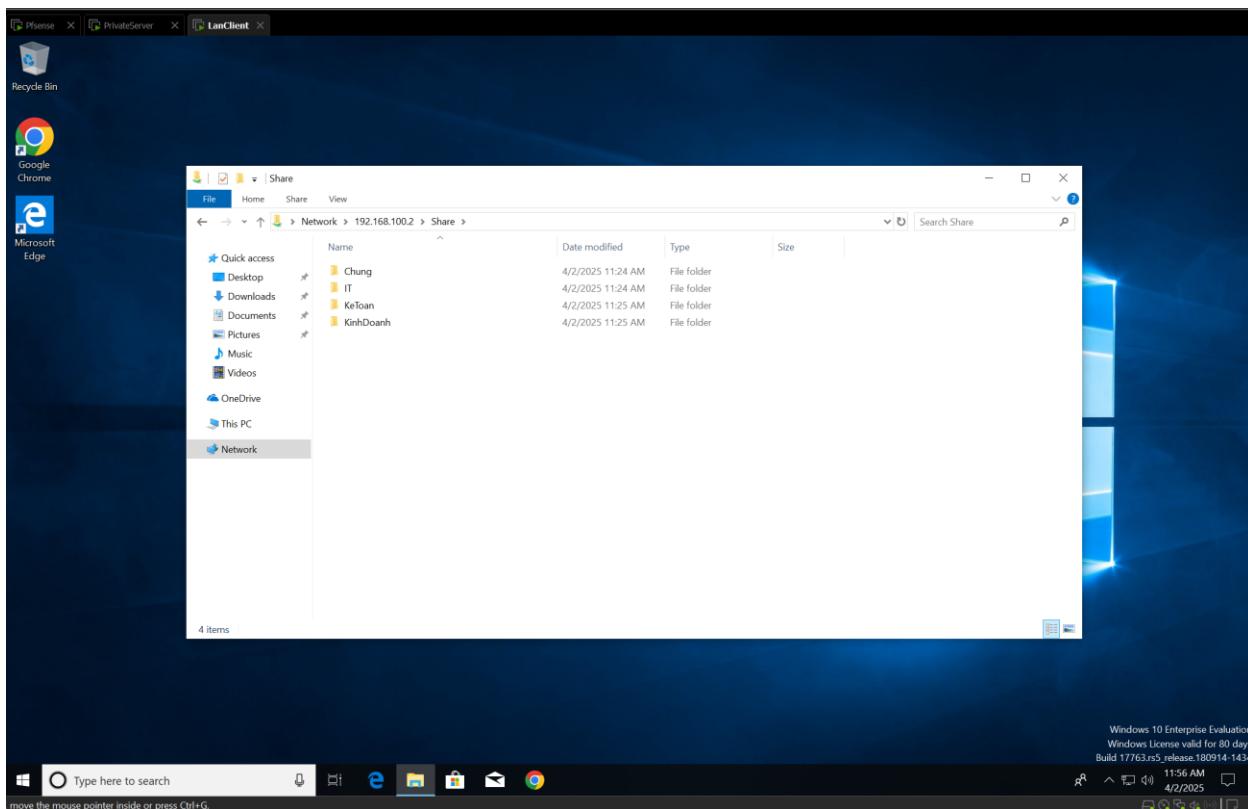
Hình 75. Giới hạn ngạch của từng phòng



Hình 76. Tài khoản không của phòng ban nào không thể truy cập tới thư mục của ban khác

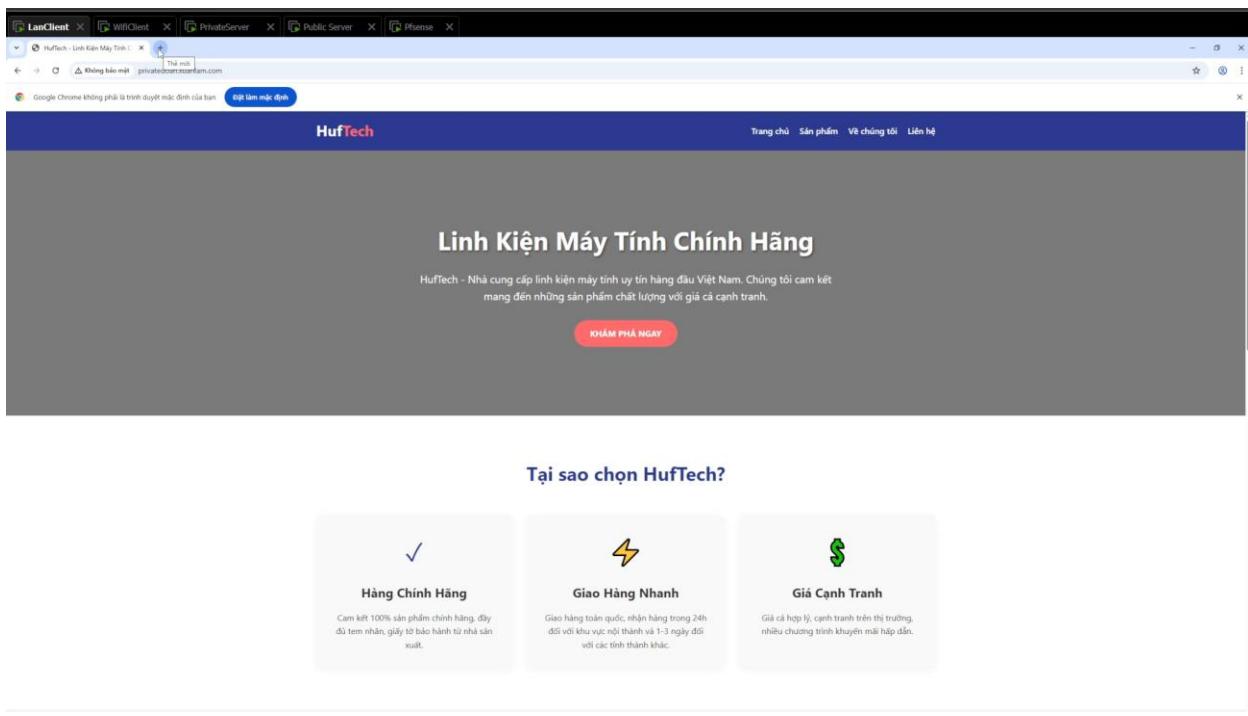


Hình 77. Giám đốc có thẻ xem toàn bộ dữ liệu nhân viên

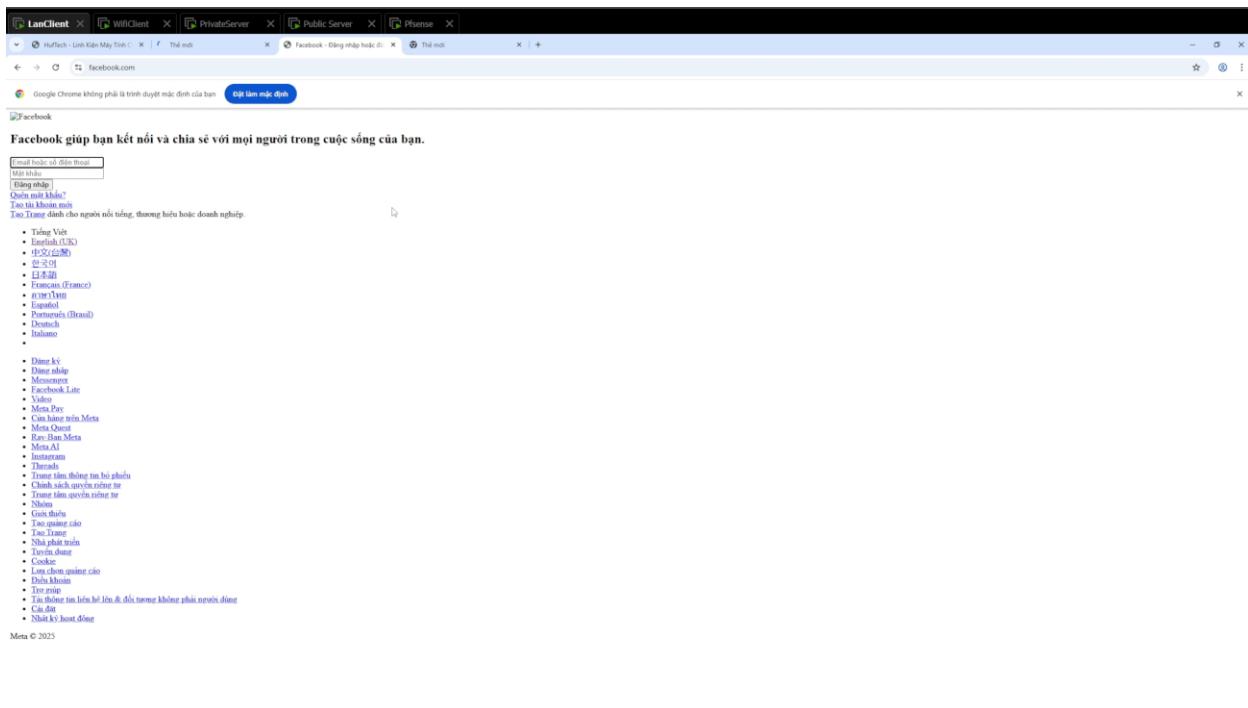


Hình 78. Truy cập bằng địa chỉ ip vẫn thấy được bằng tài khoản giám đốc

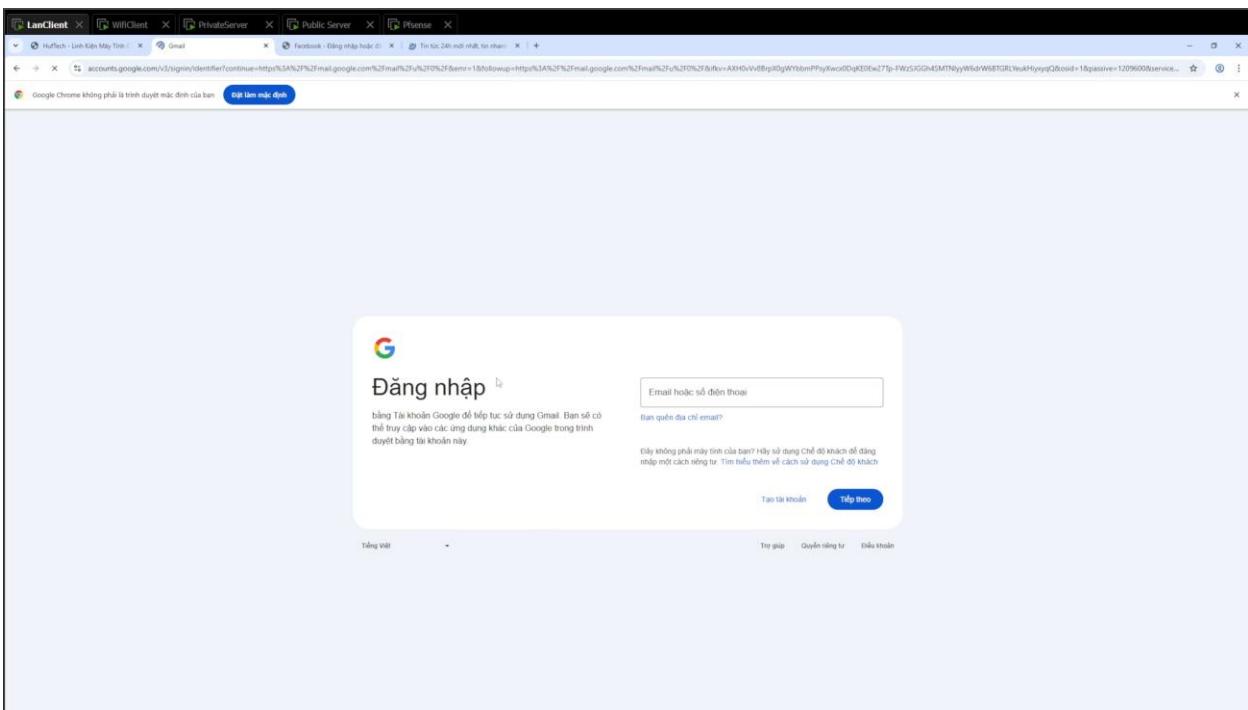
c. Bảo mật mạng



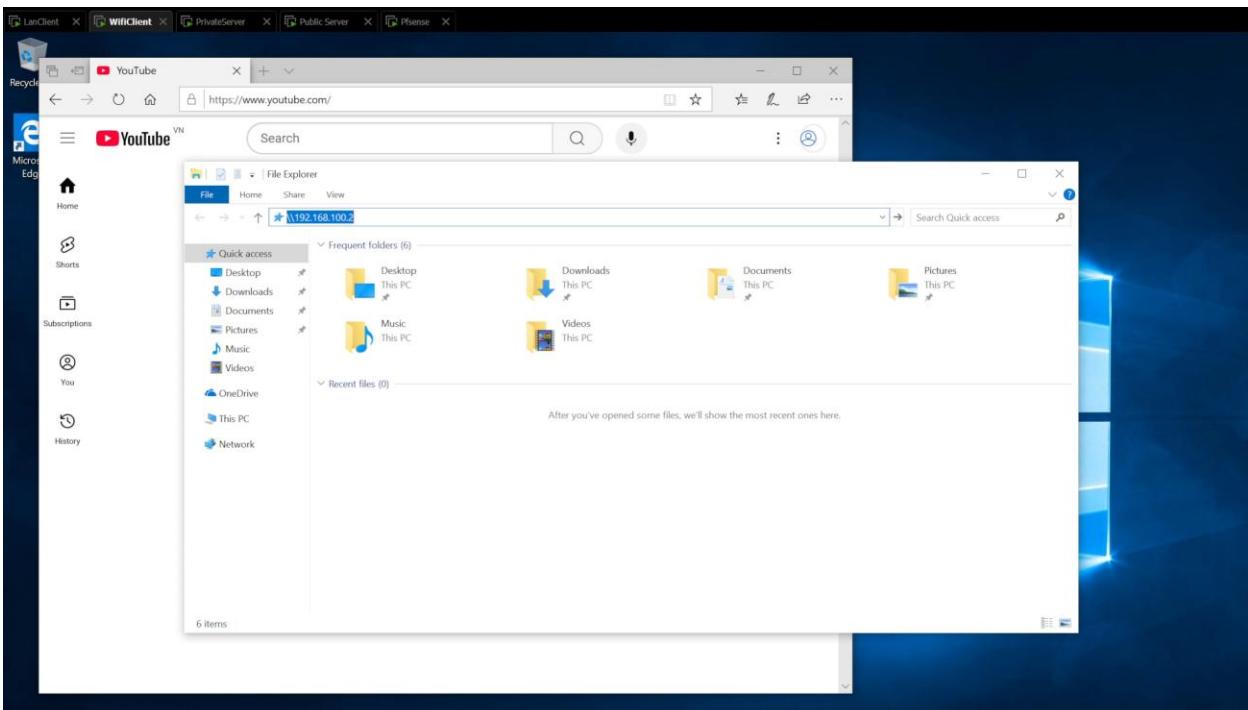
Hình 79. Mạng Lan có thẻ vô trang web của công ty



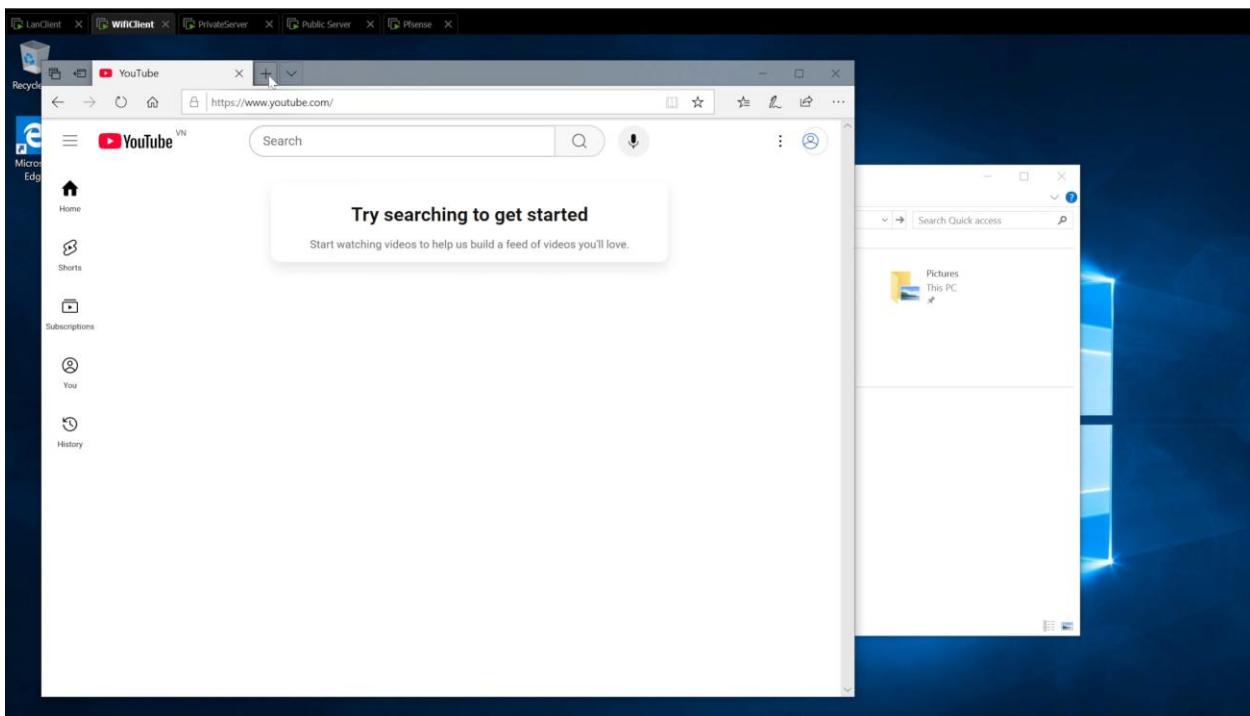
Hình 80. Mạng Lan vô được trang Facebook



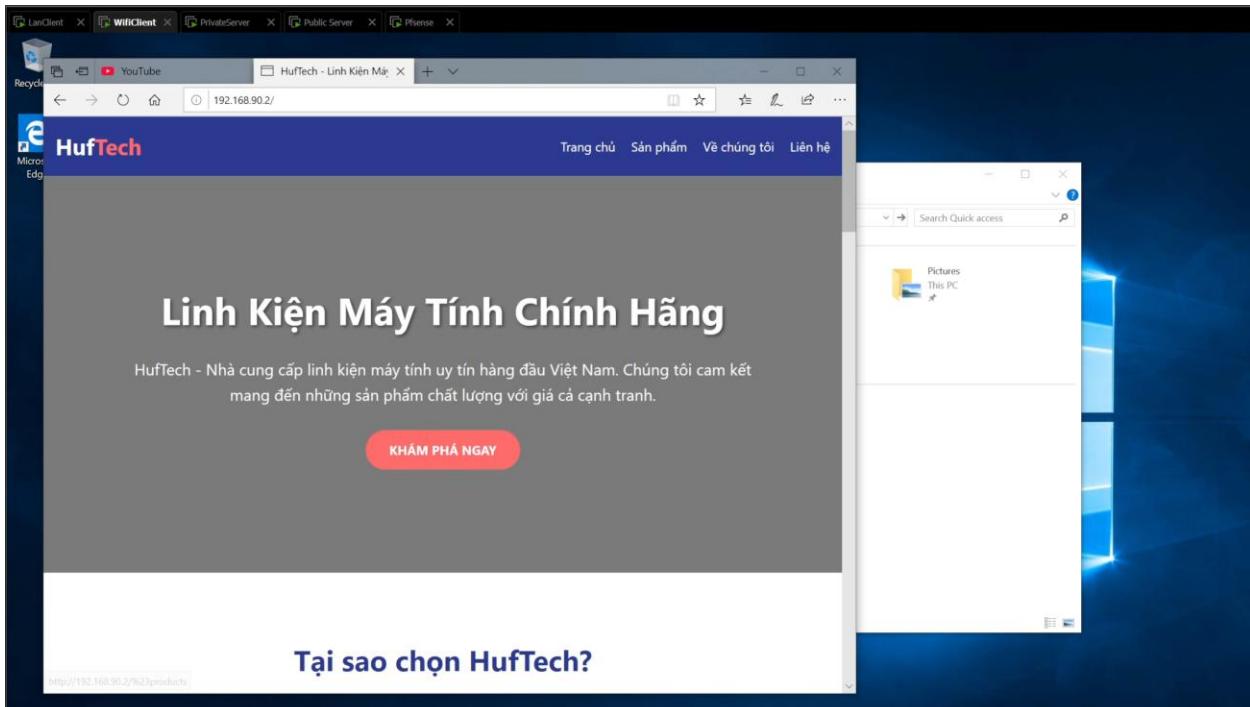
Hình 81. Mạng Lan có thẻ vô được trang gmail



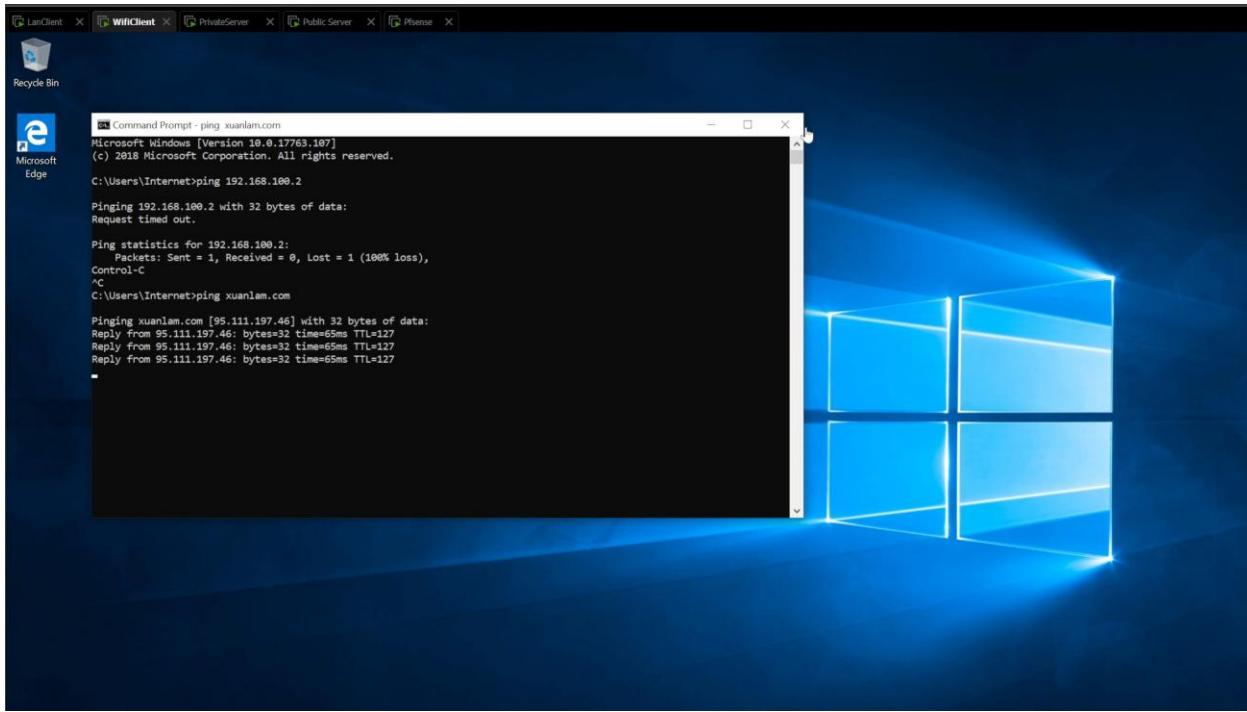
Hình 82. Máy wifi không thẻ truy cập tới file server



Hình 83. Máy wifi có thể truy cập tất cả web bình thường



Hình 84. Máy wifi có thể vô trang web của công ty



Hình 85. Máy wifi không thể ping tới domain và phân giải tên miền domain

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
OPT3 (em4)	OK C O	AUTO	DISABLED	OPT3	Add Edit Delete

Hình 86. Suricata chạy ở cổng wifi

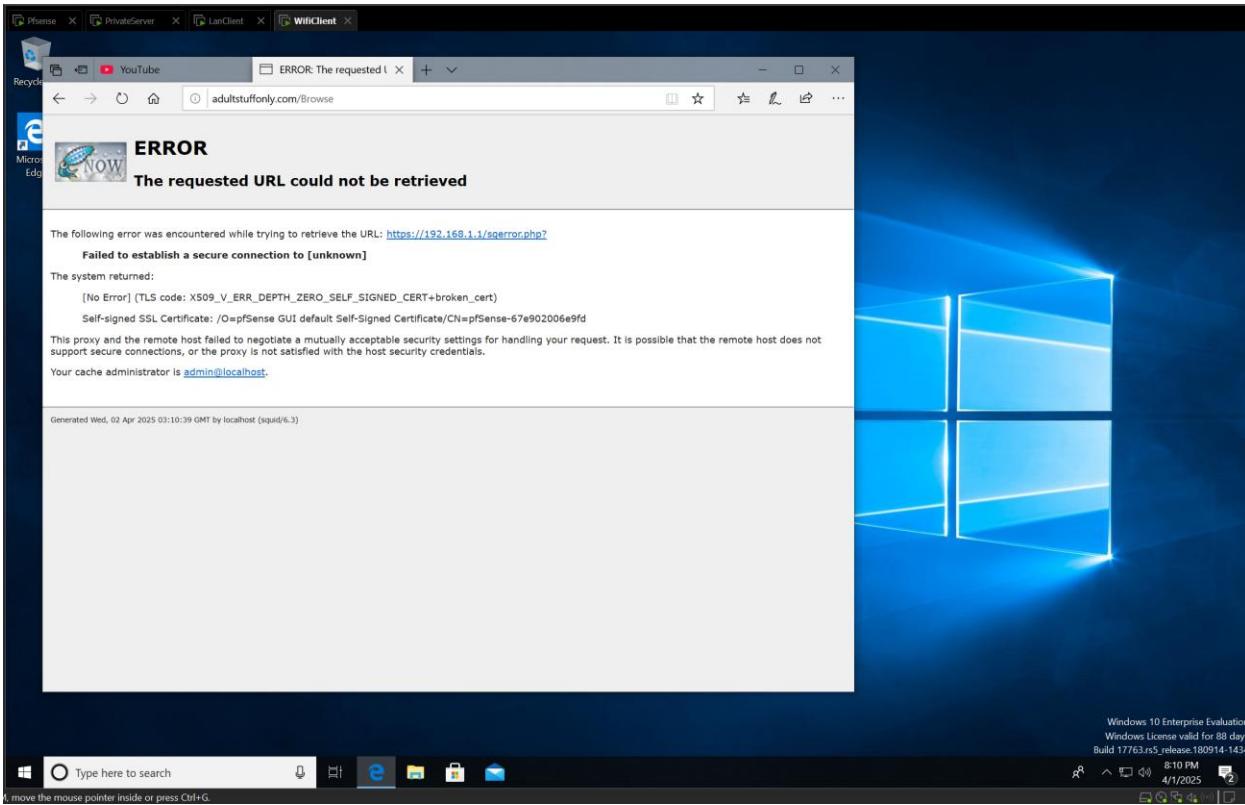
The screenshot shows a Microsoft Edge browser window displaying the pfSense web interface. The URL is https://192.168.1.1/suricata/suricata_alerts.php. The page title is "Services / Suricata / Alerts". The navigation bar includes links for Interfaces, Global Settings, Updates, **Alerts**, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. Below the navigation bar are buttons for Sync and IP Lists.

The main content area is titled "Alert Log View Settings". It includes a dropdown for "Instance to View" set to "(OPT3) OPT3", a "Save or Remove Logs" section with "Download" and "Clear" buttons, and a "Save Settings" section with a "Save" button, a "Refresh" checkbox (checked), and a "250" input field for the number of alerts to display (Default is ON).

Below this is the "Alert Log View Filter" section, which displays "Last 250 Alert Entries. (Most recent entries are listed first)". The table has columns: Date, Action, Prio, Proto, Class, Src, Sport, Dst, DPort, GID:SID, and Description. The table lists five entries from April 2, 2025, at 03:10:05, all categorized as "ALERT: YouTube Access Detected".

Date	Action	Pri	Proto	Class	Src	Sport	Dst	DPort	GID:SID	Description
04/02/2025 03:10:05	⚠️	3	TCP	Not Assigned	192.168.10.2	50024	192.168.10.1	3128	1:1000001 ⊕ ✘	ALERT: YouTube Access Detected
04/02/2025 03:10:05	⚠️	3	TCP	Not Assigned	192.168.10.2	50023	192.168.10.1	3128	1:1000001 ⊕ ✘	ALERT: YouTube Access Detected
04/02/2025 03:10:05	⚠️	3	TCP	Not Assigned	192.168.10.2	50022	192.168.10.1	3128	1:1000001 ⊕ ✘	ALERT: YouTube Access Detected
04/02/2025 03:10:05	⚠️	3	TCP	Not Assigned	192.168.10.2	50022	192.168.10.1	3128	1:1000002 ⊕ ✘	ALERT: YouTube Access Detected
04/02/2025 03:08:47	⚠️	3	TCP	Not Assigned	192.168.10.2	49978	192.168.10.1	3128	1:1000001 ⊕ ✘	ALERT: YouTube Access Detected

Hình 87. Cảnh báo của suricata



Hình 88. Chặn bằng squid

7. Kết luận

- **Làm được:**
 - Triển khai được camera để theo dõi hết tất cả các góc trưng bày của công ty
 - Triển khai được giải pháp cách ly mạng Lan đối các mối đe doạ từ internet
 - Triển khai được các giải pháp chống cài đặt Virus
 - Triển khai được đường mạng sử dụng cho khách riêng
 - Triển khai chống truy cập vào domain nếu không phải trong công ty
 - Triển khai việc khôi phục dữ liệu khi lỡ xoá dữ liệu của công ty
- **Không làm được:**
 - Triển khai tuồn thông tin của công ty thông qua việc chép dữ liệu vào usb
 - Triển khai chống cài các mã độc từ mạng
- **Những thứ phát triển trong tương lai:**
 - Triển khai VPN khi có nhiều cơ sở hơn
 - Đồng bộ giữa các server của các chi nhánh

BẢNG PHÂN CÔNG VIỆC

Bảng 1. Bảng phân công việc

Tên	Công Việc
Phạm Hoàng Gia Bảo	Viết báo cáo, lập các chính sách bảo mật, triển khai các dịch vụ mạng và tường lửa
Lê Thành Đạt	Vẽ sơ đồ vật lý + bảo mật vật lý tầng 1
Huỳnh Minh Nhựt	Vẽ sơ đồ vật lý + bảo mật vật lý tầng 2,3,4
Dương Lê Huy Hoàng	Vẽ sơ đồ logic, phân VLan, viết cơ sở lý thuyết

TÀI LIỆU THAM KHẢO

ZacsTech. (2023, 15 tháng 10). *How to Install Squid Proxy Server on pfSense*

[Video]. [How to Install Squid Proxy Server on pfSense - YouTube](#)

Aloui Hosni. (2022, 26 tháng 1). *SETUP SQUID and SQUIDGUARD PFSENSE*

[Video]. [SETUP SQUID and SQUIDGUARD PFSENSE](#)

IAMASUPERUSER. (2014, 19 tháng 7). *pfSense WEB FILTERING & Block Downloads w/ SQUIDGUARD / pfSense How-to/Guide/Tutorial*[Video]. [pfSense WEB FILTERING & Block Downloads w/ SQUIDGUARD | pfSense How-to/Guide/Tutorial](#)

atuanlab. (2024, 1 tháng 6). *[IDS/IPS] Cài đặt Suricata trên Pfsense 2.7.2*

[Video]. [\[IDS/IPS\] Cài đặt Suricata trên Pfsense 2.7.2](#)

MCT Đặng Đình Công. (2025, 7 tháng 1). *[Học MCSA 2022] Triển khai chính sách GPO cơ bản trên Windows Server 2022*[Video]. [\(32\) \[Học MCSA 2022\] Triển khai chính sách GPO cơ bản trên Windows Server 2022 - YouTube](#)

olbat. (2025, 27 tháng 3). *UT1 Blacklists*[Link]. [GitHub - olbat/ut1-blacklists: Collection of websites blacklists managed by the Université Toulouse Capitole](#)