**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

□□□□□

HCMUTE

# ĐỒ ÁN CUỐI KỲ

# AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG

**Wireless Access Control and Authentication**

**(KIỂM SOÁT VÀ TRUY CẬP XÁC THỰC KHÔNG DÂY)**


**GVHD:** ThS. Đinh Công Đoan

**SVTH:**

1. Bùi Nhật Thành 23162091
2. Nguyễn Gia Bảo 23162006
3. Phan Văn Tài 23162086


**MÃ LỚP HỌC**: WISE432380_05

**Thành phố Hồ Chí Minh, Tháng 12 năm 2025**

## DANH SÁCH PHÂN CÔNG NHIỆM VỤ

| STT | HỌ VÀ TÊN | MSSV | NHIỆM VỤ | HOÀN THÀNH |
|---|---|---|---|---|
| 1 | Bùi Nhật Thành | 23162091 | Nghiên cứu và phân tích đề tài; triển khai và thực nghiệm trên gns3 mục tiêu xác thực và kiểm soát truy cập cho nhân viên. | 100% |
| 2 | Nguyễn Gia Bảo | 23162006 | Nghiên cứu và phân tích đề tài; thiết kế và xây dựng mô hình hệ thống trên Cisco Packet. | 100% |
| 3 | Phan Văn Tài | 23162086 | Nghiên cứu và phân tích đề tài; quản lý cơ sở lý thuyết, viết báo cáo, thiết kế slide thuyết trình, cấu hình xác thực và kiểm soát truy cập cho khách. | 100% |

# LỜI CẢM ƠN

Với lòng biết ơn sâu sắc, chúng em xin gửi lời cảm ơn chân thành nhất đến Thầy ThS. Đinh Công Đoan, giảng viên Khoa Công nghệ Thông tin, đã tận tình hướng dẫn, truyền đạt kiến thức quý báu và tạo mọi điều kiện thuận lợi để chúng em hoàn thành đồ án môn học "An Toàn Mạng Không Dây và Di Động" này.

Trong suốt quá trình thực hiện đồ án, Thầy đã luôn theo sát, chỉ bảo chi tiết, giúp chúng em vượt qua những khó khăn về mặt chuyên môn và định hướng nghiên cứu. Những ý kiến đóng góp kịp thời và sự khích lệ của Thầy là nguồn động lực to lớn để đồ án của chúng em được hoàn thành đúng tiến độ và đạt được kết quả tốt nhất.

Chúng em xin kính chúc Thầy dồi dào sức khỏe và tiếp tục gặt hái nhiều thành công trong sự nghiệp trồng người.

Chúng em cũng xin gửi lời cảm ơn đến quý Thầy/Cô trong Khoa Công nghệ Thông tin, Trường Đại học Sư phạm Kỹ thuật TP. HCM đã giảng dạy và trang bị cho chúng em những kiến thức nền tảng vững chắc trong những năm học vừa qua.

Xin chân thành cảm ơn!

*TP. Hồ Chí Minh, ngày 24 tháng 12 năm 2025*

Nhóm Sinh viên thực hiện

Bùi Nhật Thành

Nguyễn Gia Bảo

Phan Văn Tài

Tóm tắt

Mục tiêu chính của đồ án là nghiên cứu và triển khai một mô hình hệ thống mạng không dây an toàn, có khả năng kiểm soát chặt chẽ quyền truy cập và thực hiện xác thực người dùng trước khi cấp phép vào mạng. Nhằm mục đích mô phỏng một giải pháp bảo mật toàn diện cho mạng Wifi, sử dụng các công cụ chuyên nghiệp để đảm bảo rằng chỉ người dùng hợp lệ mới có thể kết nối và truy cập tài nguyên mạng.

Đồ án được triển khai dưới dạng môi trường ảo, mô phỏng một mạng thực tế:

- Nền tảng: Sử dụng VM (Máy ảo) và GNS3 để giả lập môi trường ảo hóa, cho phép kết nối các hệ thống khác nhau một cách linh hoạt. Mô hình mạng được thiết kế ban đầu trên Cisco Packet Tracer.
- Các Thành phần Chính:
    - pfSense: Được cài đặt để đóng vai trò là Firewall chính, DHCP Server, và DNS Server của mạng.
    - Ubuntu Server: Cài đặt dịch vụ RADIUS Server (Remote Authentication Dial-In User Service) để thực hiện xác thực người dùng và chạy một Web Server nội bộ.
    - Ubuntu Desktop: Được dùng để cấu hình làm AP ảo và thực hiện nhiệm vụ chuyển tiếp cấp mạng cho mạng Guest (khách).
    - Thiết bị thực tế (Giả lập AP): Sử dụng một Router Wifi TP-Link WR822N và một USB Wifi để giả lập các điểm truy cập (Access Point) cung cấp mạng cho người dùng.

Đồ án tích hợp nhiều chức năng bảo mật và quản lý mạng:

- Kiểm soát Truy cập (Authentication):
    - Triển khai RADIUS Server trên Ubuntu Server để xác thực người dùng. Chỉ những người dùng có tài khoản hợp lệ mới được cấp quyền truy cập mạng.
- Bảo mật Tường lửa (Firewall):
    - pfSense được dùng để tạo các Rules chặn và cho phép truy cập, bảo vệ mạng nội bộ khỏi các mối đe dọa bên ngoài.

    - Sử dụng pfsense để ngăn chặn các địa chỉ IP bị xem là không phù hợp hoặc độc hại.
- Giám sát và Ghi Log (Logging & Monitoring):
    - pfSense thực hiện việc bắt các gói tin dữ liệu và đọc logs hoạt động của mạng.
    - Cấu hình Squid để bắt và đọc logs truy cập web của người dùng thông qua một trang web chuyên biệt do Squid tạo.
    - Có khả năng bắt các địa chỉ IP do người dùng truy cập.

Kết quả: Sản phẩm cuối cùng của đồ án là một mô hình mạng không dây an toàn đã được cấu hình và vận hành thành công

**Mục Lục**

**Phần mở đầu:**

## 1. Đặt vấn đề

Sự bùng nổ của mạng không dây (Wifi) đã biến công nghệ này trở thành xương sống của mọi hệ thống kết nối trong kỷ nguyên số, mang lại sự tiện lợi và linh hoạt không thể phủ nhận. Tuy nhiên, song hành với sự tiện lợi là những thách thức bảo mật nghiêm trọng. Các phương thức bảo mật truyền thống không còn đủ sức bảo vệ tài nguyên mạng khỏi các mối đe dọa phức tạp, đặc biệt là trong môi trường cần kiểm soát truy cập cá nhân hóa cao. Do đó, việc nghiên cứu và triển khai một giải pháp kiểm soát và xác thực truy cập không dây mạnh mẽ, linh hoạt và tập trung là một yêu cầu cấp thiết, đảm bảo rằng chỉ người dùng hợp lệ mới được cấp quyền, đồng thời cung cấp khả năng giám sát và truy vết đầy đủ hoạt động của người dùng trên mạng.

### 1.1. Tóm lược những nghiên cứu trong và ngoài nước liên quan đến đề tài

Trong những năm gần đây, Việt Nam đang chứng kiến sự gia tăng nhanh chóng nhu cầu triển khai mạng Wifi doanh nghiệp và campus có độ bảo mật cao tại các trường đại học, bệnh viện, khách sạn, văn phòng và khu công nghiệp. Nhiều tổ chức đã chuyển dần từ mô hình Wifi mở hoặc WPA2-PSK sang mô hình Wi-Fi Enterprise sử dụng chuẩn 802.1X kết hợp RADIUS để kiểm soát truy cập chặt chẽ theo từng người dùng. Các đồ án, luận văn và dự án thực tế tại các trường đại học lớn cùng doanh nghiệp trong nước đã tập trung nghiên cứu, triển khai và đánh giá hiệu quả của FreeRADIUS, Microsoft NPS, pfSense, OpenWrt và các giải pháp NAC mã nguồn mở, nhằm xây dựng hệ thống xác thực tập trung, kiểm soát thiết bị đầu cuối và bảo vệ mạng không dây với chi phí hợp lý, phù hợp điều kiện hạ tầng và nguồn nhân lực Việt Nam.

Trên thế giới, chuẩn IEEE 802.1X và các phương thức EAP đã liên tục được phát triển và hoàn thiện từ năm 2001 đến nay nhằm đáp ứng yêu cầu bảo mật ngày càng cao của mạng Wifi doanh nghiệp và môi trường BYOD, IoT. Các công trình nghiên cứu được công bố trên những tạp chí, hội nghị hàng đầu như IEEE, ACM, USENIX Security, NDSS và WiSec đã tập trung làm rõ các lỗ hổng thực tế trong quá trình cấu hình supplicant, phát triển kiến trúc Enterprise Wi-Fi an toàn (WPA3-Enterprise, certificate-based authentication, secure onboarding), đồng thời đề xuất các kỹ thuật giám sát lưu lượng không dây, phân tích log tập trung và hệ thống phát hiện xâm nhập chuyên

biệt, giúp giảm thiểu nguy cơ tấn công man-in-the-middle, evil twin, credential theft và khai thác mật khẩu trong môi trường Wifi quy mô lớn.

### 1.2. Tính cấp thiết cần nghiên cứu của đề tài

Việt Nam đang đẩy mạnh chuyển đổi số và xây dựng hạ tầng mạng không dây quy mô lớn (trường học, bệnh viện, khách sạn, khu công nghiệp, trung tâm thương mại, cơ quan nhà nước), mạng Wifi đã trở thành phương thức truy cập chính của hàng triệu người dùng và thiết bị mỗi ngày. Tuy nhiên, hầu hết các hệ thống Wifi hiện nay tại Việt Nam vẫn đang sử dụng chế độ WPA2/3-PSK (chia sẻ một mật khẩu chung) hoặc để mạng mở hoàn toàn, dẫn đến những rủi ro bảo mật nghiêm trọng.

Trong khi đó, các vụ tấn công mạng nhắm vào mạng Wifi doanh nghiệp và tổ chức tại Việt Nam ngày càng gia tăng: năm 2023–2025, Cục An toàn thông tin (AISO) ghi nhận hàng nghìn vụ đánh cắp dữ liệu qua Wifi công cộng và Wifi nội bộ yếu bảo mật; nhiều cơ quan, trường học, doanh nghiệp bị tấn công ransomware bắt đầu từ việc xâm nhập qua mạng không dây.

Chuẩn IEEE 802.1X kết hợp RADIUS (Wifi Enterprise) cùng các giải pháp NAC và firewall mã nguồn mở đã được chứng minh là phương thức bảo mật hiệu quả nhất hiện nay cho môi trường doanh nghiệp và tổ chức lớn trên thế giới. Tuy nhiên tại Việt Nam, việc triển khai thực tế vẫn còn rất hạn chế do thiếu tài liệu hướng dẫn chi tiết, thiếu mô hình mẫu phù hợp với hạ tầng trong nước và tâm lý e ngại về độ phức tạp, chi phí.

Vì vậy, việc nghiên cứu, thiết kế và triển khai thành công một hệ thống kiểm soát truy cập và xác thực không dây dựa trên 802.1X, RADIUS và pfSense không chỉ có ý nghĩa học thuật mà còn mang tính cấp thiết cao trong thực tiễn: góp phần nâng cao an toàn thông tin mạng không dây, đáp ứng yêu cầu pháp lý, bảo vệ tài sản thông tin của tổ chức, đồng thời cung cấp mô hình triển khai thực tế, chi phí thấp, dễ nhân rộng cho các trường đại học, doanh nghiệp và cơ quan nhà nước Việt Nam trong giai đoạn hiện nay.

### 1.3. Lý do chọn đề tài

Mạng Wifi đã trở thành hạ tầng thiết yếu tại hầu hết trường học, bệnh viện, khách sạn, văn phòng và khu công nghiệp Việt Nam. Tuy nhiên, phần lớn các hệ thống Wifi hiện nay vẫn sử dụng mật khẩu chung (WPA2/3-PSK) hoặc để mạng mở hoàn toàn mở,

dẫn đến nguy cơ bị tấn công rất cao: dò mật khẩu, lập AP giả (evil twin), KRACK, đánh cắp dữ liệu, lây lan ransomware… Một khi mật khẩu bị lộ hoặc nhân viên cũ nghỉ việc, toàn bộ mạng nội bộ đều có thể bị xâm phạm mà không thể truy vết.

Các vụ tấn công mạng qua Wifi tại Việt Nam ngày càng gia tăng. Theo báo cáo của Cục An toàn thông tin (AISO) giai đoạn 2023–2025, hàng nghìn tổ chức bị xâm nhập bắt đầu từ mạng không dây yếu bảo mật. Đồng thời, Luật An ninh mạng 2018 và Thông tư 03/2024/TT-BTTTT đã đặt ra yêu cầu bắt buộc về kiểm soát truy cập, xác thực người dùng và ghi nhật ký hoạt động đối với các hệ thống thông tin cấp độ 3 trở lên.

Trong khi đó, giải pháp chuẩn quốc tế là Wi-Fi Enterprise với IEEE 802.1X + RADIUS + NAC đã được chứng minh hiệu quả và bắt buộc áp dụng tại các tổ chức lớn trên thế giới, nhưng tại Việt Nam vẫn rất ít đơn vị triển khai thành công do thiếu tài liệu chi tiết, mô hình mẫu phù hợp hạ tầng giá rẻ và nhân sự có kinh nghiệm.

Vì những lý do trên, tôi chọn đề tài "Thiết kế và triển khai hệ thống kiểm soát truy cập và xác thực không dây sử dụng chuẩn IEEE 802.1X, RADIUS và pfSense" nhằm xây dựng một giải pháp bảo mật Wi-Fi thực tế, chi phí thấp, dễ nhân rộng, góp phần nâng cao an toàn thông tin mạng không dây, đáp ứng yêu cầu pháp lý và bảo vệ tài sản thông tin của các tổ chức Việt Nam trong thời kỳ chuyển đổi số hiện nay.

### 1.4. Mục tiêu đề tài

Đề tài hướng đến thiết kế và triển khai thành công một hệ thống kiểm soát truy cập và xác thực không dây hoàn chỉnh dựa trên chuẩn IEEE 802.1X, cụ thể là xây dựng mô hình mạng ảo mô phỏng môi trường thực tế trên GNS3 và máy ảo với đầy đủ các thành phần gồm pfSense làm firewall trung tâm, Ubuntu Server chạy FreeRADIUS làm máy chủ xác thực tập trung, Access Point giả lập và các thiết bị đầu cuối; triển khai thành công cơ chế xác thực 802.1X để chỉ người dùng hợp lệ mới được cấp quyền truy cập mạng; cấu hình các quy tắc tường lửa hiệu quả trên pfSense nhằm kiểm soát lưu lượng, phân đoạn mạng và bảo vệ vùng nội bộ; đồng thời tích hợp hệ thống giám sát, ghi log chi tiết cùng Squid proxy trong suốt để theo dõi, lưu trữ nhật ký truy cập web và gói tin của từng người dùng, từ đó đáp ứng yêu cầu quản trị, kiểm toán và truy vết sự cố an ninh mạng.

## 1.5. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của đồ án là việc thiết kế, triển khai và đánh giá hiệu quả của một Hệ thống Kiểm soát Truy cập và Xác thực Không dây. Cụ thể, đối tượng tập trung vào sự tương tác và vận hành của các thành phần công nghệ tiêu chuẩn nhằm đảm bảo an toàn cho mạng Wi-Fi, bao gồm: chuẩn IEEE 802.1X, giao thức xác thực tập trung RADIUS (sử dụng FreeRADIUS trên Ubuntu Server), và giải pháp tường lửa/quản lý mạng pfSense.

Phạm vi nghiên cứu của đề tài được giới hạn trong môi trường mô phỏng ảo hóa và một số thiết bị vật lý giả lập với môi trường được triển khai sử dụng VM (Máy ảo) và GNS3, nhằm mô phỏng lại một mạng doanh nghiệp hoặc trường học thực tế với chi phí thấp và tính linh hoạt cao. Tập trung vào việc cấu hình các dịch vụ mạng cốt lõi trên pfSense (Firewall, DHCP, DNS). Triển khai thành công cơ chế xác thực 802.1X giữa Access Point giả lập và RADIUS Server (Ubuntu Server). Tích hợp hệ thống Giám sát và Ghi Log thông qua các chức năng của pfSense và cấu hình Squid proxy trong suốt để theo dõi và lưu trữ nhật ký truy cập web của người dùng.

## 1.6. Phương pháp nghiên cứu

Phương pháp nghiên cứu lý thuyết, tập trung phân tích nguyên lý hoạt động của các tiêu chuẩn cốt lõi như IEEE 802.1X và giao thức RADIUS, bao gồm các phương thức xác thực mở rộng EAP. Đồng thời, nhóm nghiên cứu tiến hành tìm hiểu chi tiết về cấu hình và chức năng của các công nghệ nền tảng là tường lửa pfSense (các chức năng Firewall, DHCP, DNS), dịch vụ FreeRADIUS (quản lý người dùng, giao tiếp AP), và nguyên tắc hoạt động của Squid Proxy trong suốt nhằm phục vụ việc ghi log truy cập.

Phương pháp thiết kế và mô phỏng bằng cách sử dụng Cisco Packet Tracer để phác thảo sơ đồ mạng logic ban đầu, xác định kiến trúc tổng thể và phân đoạn mạng. Tiếp theo, quá trình thực nghiệm và triển khai được tiến hành trong môi trường ảo hóa sử dụng VM (Máy ảo) và GNS3, đây là bước quan trọng để xây dựng môi trường lab mô phỏng thực tế.

Phương pháp đánh giá và kiểm chứng để xác nhận hệ thống đã đạt được các mục tiêu đề ra. Các thử nghiệm được tiến hành nhằm kiểm tra tính hiệu quả của cơ chế xác thực (chặn người dùng không hợp lệ và cấp quyền cho người dùng hợp lệ), tính chặt chẽ của các quy tắc tường lửa (đảm bảo các truy cập bị cấm đã được ngăn chặn), và tính đầy đủ, chính xác của hệ thống ghi log (xác nhận Squid và pfSense thu thập logs thành công, phục vụ cho nhu cầu quản trị và truy vết sự cố an ninh mạng).

## 1.7. Nội dung Đồ án

Giới thiệu tổng quan về thực trạng bảo mật mạng Wifi tại Việt Nam, những lỗ hổng nghiêm trọng của mô hình mật khẩu chung (WPA2/3-PSK), vai trò then chốt của chuẩn IEEE 802.1X và mô hình Wi-Fi Enterprise trong việc kiểm soát truy cập từng người dùng, đáp ứng yêu cầu pháp lý và bảo vệ mạng nội bộ tổ chức.

Phân tích cơ sở lý thuyết liên quan bao gồm nguyên lý hoạt động của chuẩn 802.1X, các phương thức EAP phổ biến (PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS), giao thức RADIUS, cơ chế kiểm soát cổng mạng, VLAN động, cùng các công cụ mã nguồn mở chính như pfSense, FreeRADIUS, hostapd, wpa_supplicant và Squid proxy.
Phân tích yêu cầu và thiết kế hệ thống: xác định yêu cầu chức năng, phi chức năng cho môi trường doanh nghiệp vừa và nhỏ/trường đại học; thiết kế kiến trúc mạng tổng thể, phân vùng (Staff – Guest – IoT), chính sách xác thực, phân quyền VLAN và quy tắc tường lửa trên pfSense.

Triển khai thực tế: hướng dẫn chi tiết từng bước xây dựng mô hình trên GNS3 kết hợp máy ảo và một số thiết bị thật, bao gồm cài đặt và cấu hình pfSense, FreeRADIUS, Access Point hỗ trợ 802.1X, switch tầng 2, tích hợp proxy trong suốt và hệ thống ghi log tập trung; đồng thời kiểm thử xác thực trên các hệ điều hành phổ biến (Windows, Android, iOS, Linux).

Đánh giá kết quả: đo đạc hiệu năng xác thực, độ trễ, khả năng chịu tải; thử nghiệm các kịch bản tấn công thường gặp; so sánh mức độ bảo mật trước và sau khi triển khai; rút ra kết luận, hạn chế còn tồn tại và đề xuất hướng phát triển tiếp theo nhằm nhân rộng mô hình ra thực tế tại các tổ chức Việt Nam.

**Phần nội dung:**

# Chương 1: Tổng quan về KIỂM SOÁT VÀ TRUY CẬP XÁC THỰC KHÔNG DÂY

## 1.1. Khái niệm cơ bản

### 1.1.1. Giới thiệu về kiểm soát truy cập không dây

Kiểm soát Truy cập Mạng Không dây  là việc áp dụng các biện pháp và giao thức bảo mật để quản lý và hạn chế quyền truy cập vào một mạng không dây (Wifi/WLAN). Mục tiêu là bảo vệ mạng khỏi sự truy cập trái phép và đảm bảo chỉ những người dùng được xác thực mới có thể kết nối với Internet hoặc các tài nguyên mạng nội bộ. Mục tiêu chính là: chống truy cập trái phép, kiểm soát và theo dõi và bảo vệ dữ liệu

### 1.1.2. Giới thiệu về xác thực

Xác thực là quá trình xác minh danh tính của một người dùng, thiết bị, hoặc quy trình đang yêu cầu quyền truy cập vào một mạng hoặc hệ thống. Trong bối cảnh mạng không dây, xác thực là bước đầu tiên và quan trọng nhất để đảm bảo rằng chỉ các thiết bị và người dùng hợp pháp mới có thể kết nối với Điểm truy cập (Access Point - AP) và sử dụng tài nguyên mạng. Các cơ chế xác thực chính bao gồm: Xác thực Dựa trên Tiêu chuẩn 802.11 (Lớp MAC) và Xác thực Nâng cao (Tiêu chuẩn 802.1X và EAP)

### 1.1.3. Khái niệm về kiểm soát và truy cập xác thực không dây

Kiểm soát và Truy cập Xác thực Không dây là một giải pháp bảo mật toàn diện được thiết kế để xác minh danh tính của từng người dùng và quản lý quyền truy cập của họ vào mạng không dây. Thay vì sử dụng mật khẩu chia sẻ chung (WPA2-PSK) dễ bị lộ, hệ thống này dựa trên chuẩn IEEE 802.1X để yêu cầu người dùng phải xác thực thông qua một Máy chủ RADIUS (Authentication Server). Khi xác thực thành công, máy chủ sẽ cấp một khóa phiên duy nhất (session key) cho người dùng đó, đồng thời cho phép hệ thống áp dụng các chính sách bảo mật chi tiết, bao gồm Phân đoạn Mạng (Network Segmentation) để tách biệt các nhóm người dùng (ví dụ: Staff và Guest) và kiểm soát những tài nguyên nội bộ họ có thể truy cập, từ đó giảm thiểu rủi ro tấn công và tăng cường khả năng giám sát mạng.

## 1.2. Vai trò chung của kiểm soát và xác thực trong mạng không dây

Kiểm soát và Xác thực là hai trụ cột thiết yếu và bổ sung cho nhau trong việc thiết lập an ninh cho mạng không dây. Xác thực (Authentication) thực hiện vai trò là tuyến phòng thủ đầu tiên, tập trung vào việc xác minh danh tính của mọi người dùng hoặc thiết bị yêu cầu kết nối, nhằm ngăn chặn truy cập trái phép ngay từ cổng vào mạng. Quá trình này không chỉ đảm bảo rằng người dùng là hợp pháp (ví dụ: người gửi X không mạo

danh người gửi Y) mà còn thiết lập cơ sở để tạo ra các khóa mật mã cần thiết cho các giao thức bảo mật nâng cao (như 802.1X), từ đó bảo vệ luồng dữ liệu sắp tới.

Trong khi đó, Kiểm soát (Control) tập trung vào việc duy trì sự an toàn và ổn định của mạng sau khi danh tính đã được xác minh. Vai trò này bao gồm việc cấp Ủy quyền (Authorization), đảm bảo người dùng chỉ có thể truy cập những tài nguyên đã được phân bổ cho họ, đồng thời đảm bảo Tính toàn vẹn của Dữ liệu (Data Integrity) (ngăn chặn thao túng hoặc lỗi truyền dẫn) và Tính sẵn sàng (Availability) của hệ thống. Bằng cách hoạt động cùng nhau, Kiểm soát và Xác thực biến mạng không dây thành một môi trường bảo mật, đáp ứng ba yêu cầu cơ bản của chiến lược an ninh: Nhận dạng, Xác thực, và Ủy quyền.

## 1.3. Các mô hình hệ thống mạng không dây hiện nay

### 1.3.1. Mạng LAN Không dây (WLAN)

Mô hình Mạng LAN Không dây (WLAN) đại diện cho một bước tiến trong giao tiếp mạng bằng cách loại bỏ nhu cầu về cáp và cung cấp tính di động cao. Nền tảng của WLAN là việc tuân thủ các tiêu chuẩn IEEE 802.11. Trong đó, Mạng Ad hoc (IBSS) là kiến trúc cơ bản nhất, cho phép các thiết bị khách giao tiếp trực tiếp với nhau (client-to-client) để tạo ra các mạng tự phát và tạm thời, nhưng lại là mô hình kém bảo mật nhất.

Ngược lại, Mạng Cơ sở hạ tầng (Infrastructure Networks) là chế độ vận hành chủ đạo trong các tổ chức, nơi một Điểm truy cập (AP) đóng vai trò là trung tâm để định tuyến lưu lượng truy cập và liên kết mạng không dây với mạng có dây (LAN). Việc kết nối nhiều AP lại với nhau tạo ra Hệ thống Phân phối (DS), hình thành Extended Service Set (ESS), cho phép người dùng di chuyển liên tục (Roaming) trong phạm vi rộng lớn mà vẫn duy trì kết nối.

### 1.3.2. Mạng Cá nhân Không dây (WPAN) và Mạng Hồng ngoại (IrDA)

Mô hình mạng cá nhân không dây (WPAN) nổi bật với công nghệ Bluetooth, được thiết kế để truyền dữ liệu trong khoảng cách rất ngắn. Cấu trúc mạng cơ bản của Bluetooth là Piconet, nơi một thiết bị hoạt động như master và quản lý tối đa bảy thiết bị slaves hoạt động tích cực.

Song song với đó là mô hình Hồng ngoại (Infra Red - IrDA), sử dụng bức xạ hồng ngoại để tạo ra kết nối điểm-nối-điểm (point-to-point) có hướng trong phạm vi rất hẹp (khoảng 1m) và phải ở trong tầm nhìn thẳng. Một điểm khác biệt quan trọng là, không giống như WLAN và Bluetooth, giao thức IrDA không cung cấp các cơ chế xác thực hay mã hóa ở lớp liên kết dữ liệu, khiến việc triển khai bảo mật phải hoàn toàn dựa vào lớp ứng dụng.

### 1.3.3. Mạng Di động (Mobile Networks)

Mạng di động (ví dụ: GSM, UMTS) hoạt động dựa trên mô hình mạng tế bào (cellular network) có cấu trúc phân cấp để cung cấp dịch vụ liên lạc trên diện rộng. Trong mô hình này, các khu vực được chia thành các ô (cell), mỗi ô được phục vụ bởi một Trạm Cơ sở (Base Station - BTS), và việc định tuyến được quản lý bởi Nút Chuyển mạch Di động (Mobile Switching Center - MSC). Điều quan trọng là, không giống như mạng ad hoc của WLAN, giao tiếp giữa các thiết bị di động thường không phải là kết nối đầu cuối (end-to-end) mà luôn được định tuyến qua mạng của nhà cung cấp. Ngoài ra, các thiết bị thông minh hiện đại (Smartphones) đang thúc đẩy sự hội tụ với WLAN, cho phép chúng kết nối trực tiếp với mạng WLAN qua Điểm truy cập, mở ra các dịch vụ mới như VoIP nhưng đồng thời tạo ra các rủi ro bảo mật bổ sung.

## Chương 2: Cơ sở lý thuyết và công nghệ nền tảng

### 2.1. Chuẩn IEEE 802.1X và cơ chế kiểm soát truy cập cổng mạng (Port Access Control)

Chuẩn IEEE 802.1X là một giao thức được phát triển bởi IEEE, định nghĩa Cơ chế Kiểm soát Truy cập Cổng mạng (Port Access Control), được thiết kế để cung cấp khả năng xác thực người dùng và thiết bị trước khi chúng được cấp quyền truy cập vào các dịch vụ mạng, áp dụng cho cả mạng có dây (Ethernet) và mạng không dây (WLAN). Mục tiêu cốt lõi của 802.1X là đảm bảo rằng chỉ các thực thể đã được xác minh danh tính và ủy quyền mới có thể kết nối với mạng và trao đổi lưu lượng dữ liệu. Với kiến trúc Hoạt động (3 Thực thể) Cơ chế 802.1X hoạt động dựa trên sự tương tác của ba thành phần chính:

**Supplicant (Người yêu cầu):**

- Là thiết bị khách (client) muốn kết nối và truy cập vào mạng (ví dụ: máy tính xách tay, điện thoại thông minh).
- Nó gửi thông tin xác thực (thường là tên người dùng/mật khẩu) để chứng minh danh tính.

**Authenticator (Bộ xác thực):**

- Là thực thể mạng trung gian kiểm soát cổng truy cập. Trong mạng có dây, đó là Switch Ethernet, và trong mạng không dây, đó là Điểm truy cập (Access Point - AP).
- Nhiệm vụ của nó là chặn tất cả lưu lượng truy cập từ Supplicant (trừ lưu lượng xác thực) cho đến khi quá trình xác thực hoàn tất, và chuyển tiếp các thông điệp xác thực giữa Supplicant và Máy chủ Xác thực.

**Authentication Server (Máy chủ Xác thực):**

- Là hệ thống lưu trữ thông tin đăng nhập của người dùng và các chính sách kiểm soát truy cập.
- Nó đưa ra quyết định cuối cùng về việc cấp quyền (Access-Accept) hay từ chối (Access-Reject) truy cập.
- Trong thực tế, đây thường là một máy chủ RADIUS (Remote Authentication Dial-In User Service), như mô hình sẽ được triển khai trong đồ án.

## 2.2. Giao thức RADIUS (Remote Authentication Dial-In User Service)

### 2.2.1. Cấu trúc và nguyên lý hoạt động

RADIUS (Remote Authentication Dial-In User Service) là một tiêu chuẩn *thực tế* (de facto standard) cho các hệ thống xác thực, ban đầu được thiết kế cho các kết nối dial-in, nhưng hiện nay được sử dụng rộng rãi trong các mạng 802.1X, đặc biệt là WLAN.

#### 2.2.1.1 Cấu trúc

Giao thức RADIUS hoạt động trong mô hình ba bên (Supplicant, Authenticator, Authentication Server) của 802.1X, với RADIUS Server đóng vai trò là Máy chủ Xác thực (Authentication Server):

- Client (Máy chủ RADIUS Client): Trong bối cảnh mạng không dây, đây là Bộ Xác thực (Authenticator), tức là Điểm truy cập (Access Point - AP).
- Máy chủ (RADIUS Server): Là hệ thống xác minh thông tin và cấp quyền truy cập.

#### 2.2.1.2 Nguyên lý Hoạt động (Trong quy trình 802.1X)

**Yêu cầu:** Thiết bị khách (Supplicant) cung cấp thông tin đăng nhập (tên người dùng và mật khẩu) cho AP.

**Chuyển tiếp:** AP (RADIUS Client) đóng gói thông tin này lại và chuyển tiếp đến RADIUS Server để xác minh và phê duyệt.

**Xác minh & Phản hồi:** RADIUS Server kiểm tra thông tin đăng nhập dựa trên cơ sở dữ liệu của mình. Sau đó, nó gửi lại thông báo:

- **Access-Accept:** Cấp quyền truy cập vào mạng (kèm theo các thông số cấu hình và khóa phiên).
- **Access-Reject:** Từ chối truy cập.

**Bảo mật:** Giao tiếp giữa RADIUS Client (AP) và RADIUS Server được thực hiện theo phương thức mã hóa (encrypted fashion). Do đó, dữ liệu người dùng (tên người dùng và mật khẩu) không bị truyền dưới dạng văn bản thuần túy (plain text), tăng cường tính bảo mật.

### 2.2.2. Các phương thức xác thực mở rộng EAP-TLS phổ biến

EAP (Extensible Authentication Protocol) là một giao thức xác thực linh hoạt, đóng vai trò là khung chứa (container) cho nhiều phương thức xác thực khác nhau được sử dụng trong chuẩn 802.1X. Các phương thức EAP được thiết kế để tăng cường bảo mật và tính linh hoạt so với xác thực mật khẩu đơn thuần.

Trong đó, EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) là một trong những phương thức được coi là tiêu chuẩn vàng về bảo mật trong các mạng 802.1X:

#### 2.2.2.1. EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)

Khái niệm: EAP-TLS là một tiêu chuẩn mở của IETF, sử dụng Chứng chỉ số (Digital Certificates) và giao thức TLS (phiên bản kế thừa của SSL) để xác thực lẫn nhau (mutual authentication) giữa máy khách và máy chủ.

Nguyên lý: Nó thiết lập một kênh bảo mật mã hóa (TLS tunnel) trước, sau đó trao đổi và xác minh chứng chỉ công khai (public key certificates) của cả hai bên.

Ưu điểm: Được coi là phương thức an toàn nhất cho mạng 802.1X vì nó không dựa vào mật khẩu do người dùng kiểm soát mà dựa vào hạ tầng khóa công khai (PKI), loại bỏ nguy cơ bị tấn công vét cạn (brute force) hoặc lừa đảo (phishing).

Hạn chế: Yêu cầu quản lý chứng chỉ phức tạp trên cả thiết bị client và máy chủ.

#### 2.2.2.2. Các Phương thức EAP Phổ biến Khác (Dựa trên Giao thức TLS)

Các phương thức này được phát triển để khắc phục nhược điểm về quản lý chứng chỉ của EAP-TLS, bằng cách chỉ yêu cầu chứng chỉ ở phía máy chủ:

- PEAP (Protected EAP): Được phát triển bởi Cisco, Microsoft và RSA. Nó sử dụng chứng chỉ ở phía máy chủ để tạo một đường hầm mã hóa (TLS tunnel) an toàn. Sau đó, quá trình xác thực thực tế (thường là sử dụng mật khẩu/MS-CHAPv2) sẽ diễn ra bên trong đường hầm được bảo vệ đó.

- EAP-TTLS (Tunneled TLS): Tương tự như PEAP, EAP-TTLS thiết lập một kênh TLS bảo mật bằng chứng chỉ của máy chủ trước. Sau khi kênh bảo mật được thiết lập, các phương thức xác thực kém an toàn hơn (như PAP, CHAP) có thể được truyền an toàn qua đường hầm này. EAP-TTLS đơn giản hóa việc quản lý chứng chỉ phía client, vì chúng không bắt buộc.
- EAP-FAST (Flexible Authentication via Secure Tunneling): Được Cisco phát triển để thay thế EAP-TLS mà không cần PKI. Thay vào đó, nó sử dụng một "khóa bí mật chia sẻ mạnh" gọi là Protected Access Credential (PAC), duy nhất cho mỗi client và được phân phối trước.

## 2.3. Phân tích các công nghệ mã nguồn mở ứng dụng trong đề tài

### 2.3.1. Máy chủ xác thực FreeRADIUS

Khái niệm:

- FreeRADIUS là một triển khai mã nguồn mở phổ biến và mạnh mẽ của giao thức RADIUS (Remote Authentication Dial-In User Service).
- Nó hoạt động như Máy chủ Xác thực tập trung (Central Authentication Server), cho phép quản trị viên kiểm soát quyền truy cập mạng thông qua một cơ sở dữ liệu người dùng duy nhất.

Ứng dụng trong Đề tài:

- Vị trí: FreeRADIUS được cài đặt trên một Ubuntu Server riêng biệt.
- Chức năng chính: Thực hiện xác thực người dùng cho mạng Staff (Nhân viên) thông qua chuẩn 802.1X (Wifi Enterprise).

Cấu hình:

- Nó được cấu hình để thêm các thiết bị như Access Point (AP) và pfSense làm Client bằng cách định nghĩa địa chỉ IP và Shared Secret ('Testing123') trong file clients.conf.
- Nó chứa cơ sở dữ liệu người dùng nội bộ (ví dụ: staff01 với mật khẩu 'P@ssw0rd123') trong file users để thực hiện xác thực.

Vai trò bảo mật: Đảm bảo chỉ những người dùng có tài khoản hợp lệ mới được cấp quyền truy cập mạng Staff, nâng cao bảo mật so với việc sử dụng mật khẩu chia sẻ WPA2-PSK.

### 2.3.2. Tường lửa và Quản lý mạng pfSense (Firewall, DHCP, DNS)

Khái niệm:

- pfSense là một hệ điều hành tường lửa (firewall/router) mã nguồn mở dựa trên FreeBSD, nổi tiếng với khả năng cung cấp nhiều dịch vụ mạng nâng cao như tường lửa, VPN, DHCP, DNS, và proxy.
- Nó được coi là "trái tim" của hệ thống mạng trong đồ án.

Ứng dụng trong Đề tài:

- Firewall chính (Lớp bảo vệ):
    - pfSense được cài đặt để đóng vai trò là Firewall trung tâm, kiểm soát toàn bộ lưu lượng ra/vào giữa các phân đoạn mạng (Staff, Guest, Server) và mạng ngoài (WAN).
    - Nó được dùng để tạo các Rules chặn và cho phép truy cập, bảo vệ vùng nội bộ (như Server) khỏi các mối đe dọa từ mạng Guest.
- DHCP Server:
    - Cung cấp dịch vụ cấp phát địa chỉ IP tự động (DHCP).
    - Nó được cấu hình để cấp phát IP cho các mạng riêng biệt: Staff (VLAN 10: 10.10.10.0/24) và Guest (VLAN 20: 10.10.20.0/24).
- DNS Server:
    - Cung cấp dịch vụ phân giải tên miền (DNS Resolver) cho các máy khách trong mạng, giúp các thiết bị Staff và Guest có thể truy cập Internet bằng tên miền thay vì địa chỉ IP.

### 2.3.3. Proxy trong suốt Squid và cơ chế ghi log truy cập web

Khái niệm:

- Squid là một proxy web cache và forwarder mã nguồn mở, hỗ trợ nhiều giao thức mạng.
- Lightsquid là một công cụ tạo báo cáo (report) dựa trên nhật ký truy cập của Squid.

Ứng dụng trong Đề tài:

- Vị trí: Squid được cài đặt dưới dạng một Package trên pfSense.
- Proxy trong suốt (Transparent Proxy):
    - Squid được cấu hình ở chế độ Transparent Proxy. Điều này cho phép lưu lượng truy cập web của người dùng tự động đi qua Proxy mà không cần cấu hình thủ công trên trình duyệt của máy khách.
- Ghi log truy cập (Logging & Visibility):
    - Mục tiêu chính là khắc phục vấn đề "Lack of Visibility" (thiếu khả năng quan sát). Nếu chỉ dùng Router thông thường, bạn không thể biết người dùng đang truy cập URL nào.

    - Squid giải quyết vấn đề này bằng cách ghi lại chi tiết các giao dịch HTTP/HTTPS của người dùng.
- Cơ chế MITM (Man-in-the-Middle) cho HTTPS:
    - Để giám sát logs truy cập web bảo mật (HTTPS), Squid sử dụng tính năng SSL Man In the Middle.
    - Quá trình này yêu cầu tạo một Chứng chỉ CA (Internal-CA) trên pfSense, sau đó xuất ra và cài đặt vào máy của nhân viên (Staff/Guest) dưới dạng Trusted Root Store để tránh lỗi cảnh báo SSL.
    - Logs truy cập chi tiết được lưu trữ trong file /var/squid/logs/access.log và có thể được xem qua giao diện Lightsquid.

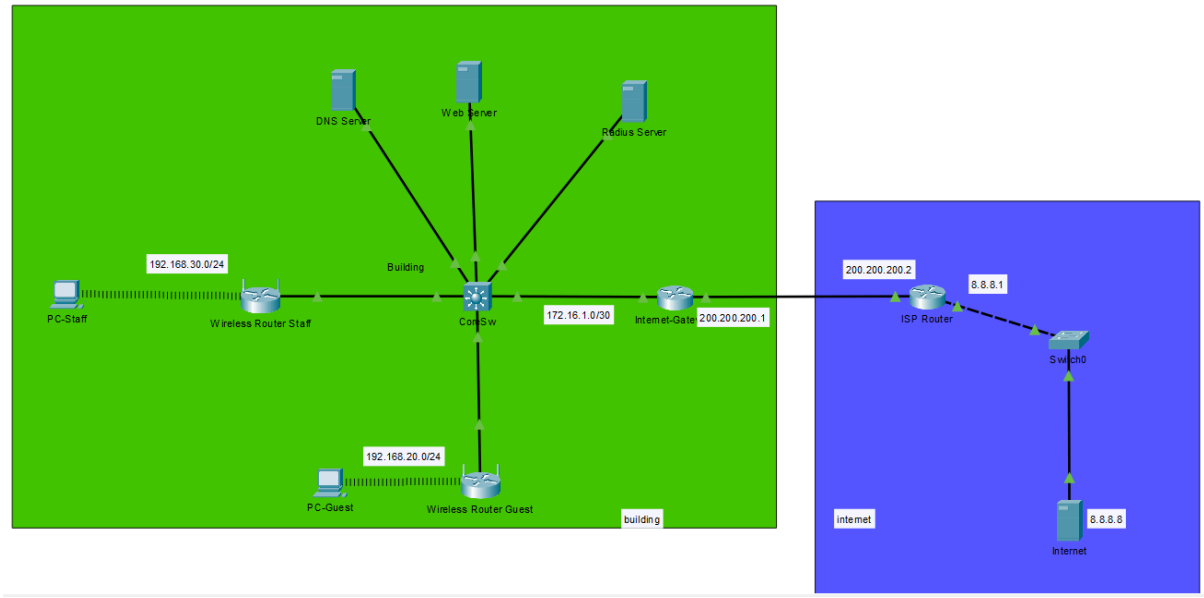
## Chương 3: Phân tích yêu cầu và Thiết kế mô hình hệ thống

### 3.1. Phân tích yêu cầu bảo mật và quản lý mạng

Yêu cầu chức năng định nghĩa những tính năng bắt buộc mà hệ thống phải thực hiện để kiểm soát truy cập và phân phối dịch vụ mạng. Cốt lõi của mô hình nằm ở khả năng kiểm soát truy cập cổng mạng, phải thực thi chuẩn IEEE 802.1X để xử lý quá trình xác thực, chỉ cho phép luồng xác thực (EAP) đi qua cổng không được kiểm soát. Hệ thống phải tích hợp thành công Máy chủ RADIUS (FreeRADIUS) để thực hiện xác thực tập trung cho người dùng nội bộ, đồng thời quản lý các dịch vụ mạng cơ bản như DHCP và DNS thông qua tường lửa pfSense. Cuối cùng, hệ thống cần phải có khả năng thiết lập các quy tắc lọc gói tin (Firewalling) chi tiết giữa các phân đoạn mạng logic (VLAN Staff, VLAN Guest, VLAN Server) để đảm bảo cô lập các vùng mạng và ngăn chặn sự xâm nhập trái phép vào tài nguyên nội bộ.

Yêu cầu phi chức năng mô tả các tiêu chí về chất lượng, hiệu suất và độ tin cậy của hệ thống, đóng vai trò quyết định tính hiệu quả của giải pháp bảo mật. Về mặt Bảo mật, hệ thống phải sử dụng cơ chế mã hóa mạnh (WPA2/WPA3 Enterprise) và hỗ trợ xác thực lẫn nhau để chống lại các cuộc tấn công mạo danh AP. Về mặt Giám sát, hệ thống phải cung cấp khả năng ghi log (Logging) chuyên sâu cho mọi hoạt động truy cập web (HTTP/HTTPS) thông qua Proxy Squid, đảm bảo khả năng kiểm toán và truy vết người dùng một cách minh bạch. Về mặt Quản lý, hệ thống phải đơn giản hóa quy trình vận hành, cho phép quản lý tập trung các dịch vụ mạng thông qua giao diện tường lửa (pfSense) và duy trì Tính Sẵn sàng (Availability) cao để đảm bảo kết nối ổn định và nhanh chóng cho người dùng.

## 3.2. Thiết kế kiến trúc mạng tổng thể




## 3.3. Thiết kế phân vùng mạng và chính sách phân quyền

### 3.3.1. Phân vùng mạng (Staff – Guest - Server)

Bảng hoạch định địa chỉ ip:

| VLAN | Tên | Network/Subnet | Gateway | Địa chỉ IP máy chủ (Tĩnh) |
|---|---|---|---|---|
| 10 | Staff (Nhân viên) | 192.168.30.0/24 | 192.168.30.1 | N/A |
| 20 | Guest (Khách) | 192.168.20.0/24 | 192.168.20.1 | N/A |
| 30 | Servers (Máy chủ) | 192.168.30.0/24 | 192.168.30.1 | **Radius Server:** 192.168.30.10<br>**Web Server:** 192.168.30.11<br>**DNS Server:** 192.168.30.12 |

| | | | | |
|---|---|---|---|---|
| 99 | Uplink to ASA | 172.16.1.0/30 | N/A | **CoreSw:** 172.16.1.2<br>**ASA:** 172.16.1.1 |

### 3.3.2. Chính sách xác thực theo người dùng

Chính sách xác thực được xây dựng nhằm đảm bảo tính định danh cá nhân (per-user identity) và tính bảo mật cao nhất cho các tài nguyên nội bộ, đặc biệt là mạng Staff và Servers, đồng thời cung cấp khả năng truy cập Internet có kiểm soát cho mạng Guest.

Chính sách Mạng Staff (VLAN 30)

| **Tiêu chí** | **Mô tả Chính sách** | **Vai trò Bảo mật** |
|---|---|---|
| **Xác thực** | Bắt buộc sử dụng chuẩn IEEE 802.1X Enterprise (WPA2/WPA3-Enterprise) với giao thức EAP (ví dụ: PEAP/EAP-TTLS). | Đảm bảo tính định danh cá nhân cho từng nhân viên. Thông tin xác thực được kiểm tra tập trung bởi Radius Server (192.168.30.10). |
| **Kiểm soát truy cập** | Truy cập không giới hạn đến tất cả các tài nguyên nội bộ thuộc VLAN Servers và các dịch vụ mạng:<br><br>Web Server (192.168.30.11)<br><br>DNS Server (192.168.30.12)<br><br>Internet (thông qua Uplink 172.16.1.0/30) | Hỗ trợ công việc nghiệp vụ của nhân viên, cho phép truy cập:<br><br>- Dữ liệu kinh doanh và ứng dụng nội bộ.<br><br>- Dịch vụ phân giải tên miền.<br><br>- Giao tiếp bên ngoài. |

| | | |
|---|---|---|
| **Ghi log** | Toàn bộ lưu lượng truy cập Web (HTTP/HTTPS) phải đi qua Proxy trong suốt (Transparent Proxy) của pfSense để ghi lại nhật ký truy cập theo từng người dùng. | Cung cấp khả năng kiểm toán (auditing) và truy vết hoạt động của nhân viên. |

Chính sách Mạng Guest (VLAN 20):

| Tiêu chí | Mô tả Chính sách | Vai trò Bảo mật |
|---|---|---|
| **Xác thực** | Sử dụng WPA2/WPA3-PSK (Pre-Shared Key) hoặc Cổng Bắt buộc (Captive Portal) đơn giản. | Cung cấp khả năng truy cập đơn giản mà không yêu cầu tài khoản Radius. |
| **Kiểm soát truy cập** | Truy cập bị giới hạn hoàn toàn theo các nguyên tắc Firewalling sau:<br><br>- Cho phép truy cập Internet (ra ngoài WAN).<br><br>- Cho phép truy cập Internet (ra ngoài WAN). | Đảm bảo cô lập mạng và ngăn chặn tấn công:<br><br>- Đáp ứng nhu cầu truy cập Internet cơ bản.<br><br>- Ngăn chặn tấn công mở rộng (Lateral Movement) vào tài nguyên nội bộ. |
| **Ghi log** | Tùy chọn: Lưu lượng truy cập Internet nên được ghi log để đáp ứng yêu cầu pháp lý về quản lý người dùng công cộng (nếu có). | - Đảm bảo tuân thủ pháp luật và truy vết hoạt động bất hợp pháp. |

Chính sách Mạng Servers (VLAN 30)

| Tiêu chí | Mô tả Chính sách | Vai trò Bảo mật |
|---|---|---|
| **Bảo vệ** | Mạng Servers là vùng bảo mật cao và không cho phép bất kỳ thiết bị không phải Server nào kết nối trực tiếp. | Đảm bảo tính cô lập (isolation) và bảo mật vật lý cho các máy chủ quan trọng. |
| **Luồng vào (Inbound)** | Chỉ cho phép các luồng giao tiếp sau:<br><br>- Từ VLAN 30 (Staff) đến Web Server (192.168.30.11).<br><br>- Từ VLAN 30 (Staff) đến Radius Server (192.168.30.10).<br><br>- Chặn hoàn toàn luồng từ VLAN 20 (Guest). | Đảm bảo chức năng và hạn chế rủi ro:<br><br>- Truy cập ứng dụng hợp pháp.<br><br>- Giao tiếp xác thực của AP.<br><br>- Bảo vệ cốt lõi hệ thống khỏi khách truy cập. |
| **Luồng ra (Outbound)** | Các máy chủ không được phép tự do truy cập Internet mà không có lý do nghiệp vụ chính đáng (nguyên tắc Least Privilege). | Ngăn chặn rò rỉ dữ liệu hoặc tấn công Command and Control (C2). |

## Chương 4: Triển khai thực tế và Cấu hình hệ thống

### 4.1. Chuẩn bị và xây dựng môi trường ảo hóa (VM và GNS3)

Môi trường thí nghiệm được xây dựng dựa trên sự kết hợp của phần mềm ảo hóa và mô phỏng mạng để tạo ra một hệ thống mạng thực tế:

**Nền tảng Ảo hóa:**

- Sử dụng VMware Workstation để cài đặt các máy chủ và tường lửa (pfSense, Ubuntu Server, Client Desktop).
- Sử dụng GNS3 để mô phỏng Topology mạng, kết nối các máy ảo với nhau thông qua các switch ảo (Core Switch) và giả lập luồng Uplink (WAN) đi ra ngoài.

**Thiết kế Topology:** Mô hình mạng được thiết kế ban đầu trên Cisco Packet Tracer, sau đó chuyển sang GNS3, bao gồm các interface vật lý và VLAN logic.

**Các Thành phần Chính:**

- pfSense VM: Đóng vai trò là Router, Firewall, DHCP, DNS Resolver và Squid Proxy.
- Ubuntu Server VM: Đóng vai trò là FreeRADIUS Server và Web Server nội bộ.
- Thiết bị Giả lập AP: Sử dụng Router Wi-Fi thực tế (TP-Link) hoặc Ubuntu Desktop được cấu hình làm AP ảo để cung cấp kết nối 802.1X cho các máy khách.
- Client VM: Máy khách Windows/Ubuntu/Mobile để kiểm thử các kết nối.

### 4.2. Triển khai và cấu hình pfSense:

PfSense là thành phần trung tâm, đóng vai trò giao tiếp chính giữa các phân đoạn mạng.

#### 4.2.1. Cấu hình các dịch vụ cốt lõi (DHCP, DNS)

**Gán Interface và IP Tĩnh:**

- Truy cập WebGUI của pfSense.
- Tạo ra các cổng nhằm tạo tương ứng với các vlan ra từng mạng cho staff , guest và server cấu hình static ip cho từng cổng tương ứng.

**Cấu hình DHCP Server:**

- Vào Services -> DHCP Server.
- VLAN 10 (Staff):
    - Kích hoạt DHCP.
    - Thiết lập dải IP: 10.10.10.100 đến 10.10.10.200.
    - DNS Servers: Trỏ về 8.8.8.8 && 1.1.1.1 và 10.10.10.120 (pfSense).
- VLAN 20 (Guest):
    - Kích hoạt DHCP.
    - Thiết lập dải IP:10.10.20.100 đến 10.10.20.200.
    - DNS Servers: Trỏ về 8.8.8.8 && 1.1.1.1(pfSense).

Cấu hình DNS Resolver:

- Vào Services -> DNS Resolver.
- Kích hoạt dịch vụ để pfSense có thể phân giải tên miền cho các client và forward query ra Internet.

### 4.2.2. Cấu hình Quy tắc Tường lửa và NAT

Quy tắc NAT (Network Address Translation):

- Firewall -> NAT -> Outbound.
- Thiết lập chế độ Automatic Outbound NAT để cho phép tất cả lưu lượng từ các mạng LAN (VLAN 10, 20, 30) đi ra Internet thông qua interface WAN.

Quy tắc Tường lửa (Firewall Rules):

- Áp dụng nguyên tắc "Mặc định chặn" (Default Deny).
- Trên Interface LAN_GUEST (VLAN 20):
    - *Rule 1 (Allow Outbound):* Cho phép lưu lượng từ VLAN 20 (10.10.20.0/24) đi ra WAN (qua Gateway).
    - *Rule 2 (Block Internal):* Chặn lưu lượng từ VLAN 20 đi đến VLAN 10 (10.10.20.0/24) và VLAN 30 (10.10.30.100).
- Trên Interface LAN_STAFF (VLAN 30):
    - *Rule 1 (Allow Outbound):* Cho phép lưu lượng từ VLAN 10 đi ra WAN.
    - *Rule 2 (Allow Server Access):* Cho phép lưu lượng từ VLAN 10 truy cập các Server cụ thể trong VLAN 30 tại các địa chỉ 10.10.30.100
- Trên Interface LAN_SERVER (VLAN 30):
    - *Rule 1 (Allow Radius):* Cho phép lưu lượng RADIUS (UDP/1812, 1813) từ VLAN 10 (AP/pfSense) đến 10.10.30.100

## 4.3. Cài đặt và cấu hình máy chủ xác thực FreeRADIUS (Ubuntu Server)

### 4.3.1. Quản lý tài khoản người dùng

Tài khoản người dùng được định nghĩa trong file cấu hình người dùng của FreeRADIUS (thường là /etc/freeradius/3.0/certs).

### 4.3.2. Cấu hình giao tiếp với Access Point

Các thiết bị trung gian (AP, Switch) đóng vai trò là Client của RADIUS Server. Chúng phải được định nghĩa trong file client.cnf.

## 4.4. Triển khai Access Point giả lập và kiểm thử kết nối 802.1X

Thiết bị Access Point (AP) đóng vai trò là **Bộ Xác thực (Authenticator)** trong mô hình 802.1X.

Cấu hình AP (TP-Link/Virtual AP):

Chế độ Bảo mật: Cài đặt Wifi SSID cho mạng Staff (ví dụ: STAFF-Secure) ở chế độ WPA2-Enterprise.

Cấu hình RADIUS:

- RADIUS Server IP: 10.10.30.100
- RADIUS Port:1812 (Authentication)
- Shared Secret: Testing123.

Kiểm thử Kết nối 802.1X:

    - Sử dụng máy khách (Client VM) cố gắng kết nối với SSID STAFF-Secure.
    - Khi được yêu cầu, nhập tên người dùng và mật khẩu (ví dụ: staff và test).
    - Kết quả mong đợi:

      Máy khách kết nối thành công, nhận IP từ DHCP của VLAN 10 (dải 10.10.10.0/24).

      Trên FreeRADIUS Server, nhật ký ghi lại quá trình Access-Accept.

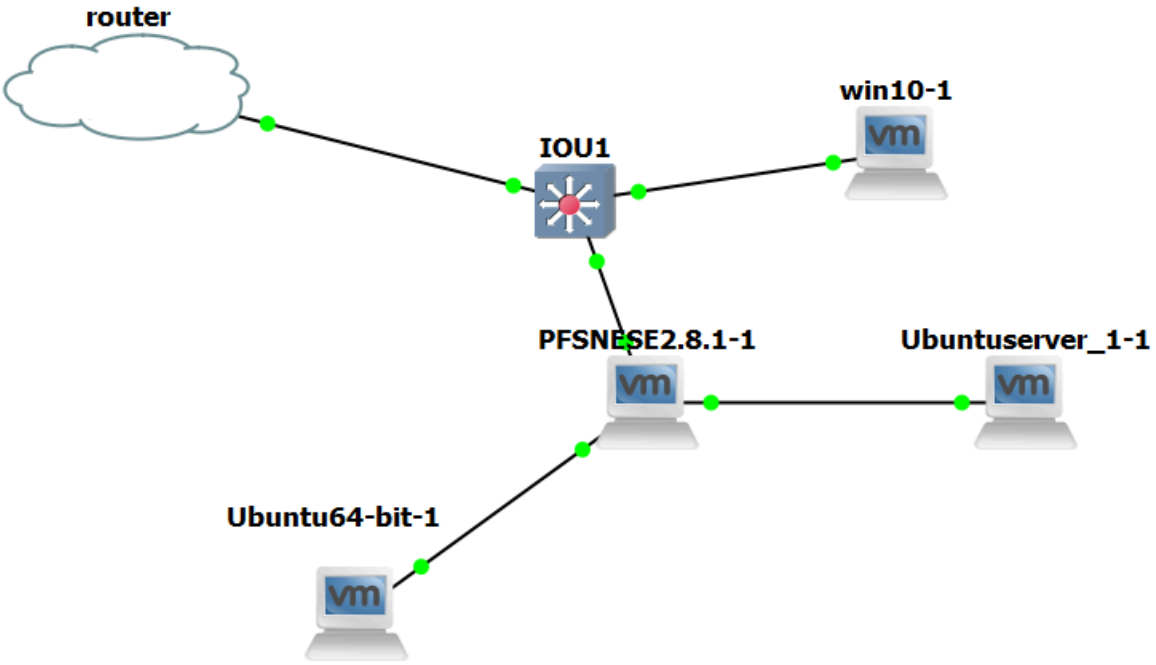
      Máy khách có thể truy cập Internet và Web Server nội bộ (10.10.30.100).

## Chương 5: Thực nghiệm chi tiết:

### 5.1: Thiết kế Topology & Addressing

Bạn cần quy hoạch IP trước khi cấu hình để tránh conflict.

- **VLAN 10 (STAFF):** 10.10.10.0/24 - GW: 10.10.10.120 (pfSense)
- **VLAN 20 (GUEST):** 10.10.20.0/24 - GW: 10.10.20.100 (pfSense)
- **VLAN 30 (SERVER):** 10.10.30.0/24 - GW: 10.10.30.10 (pfSense).
- **WAN:** IP NAT từ GNS3/VMware.



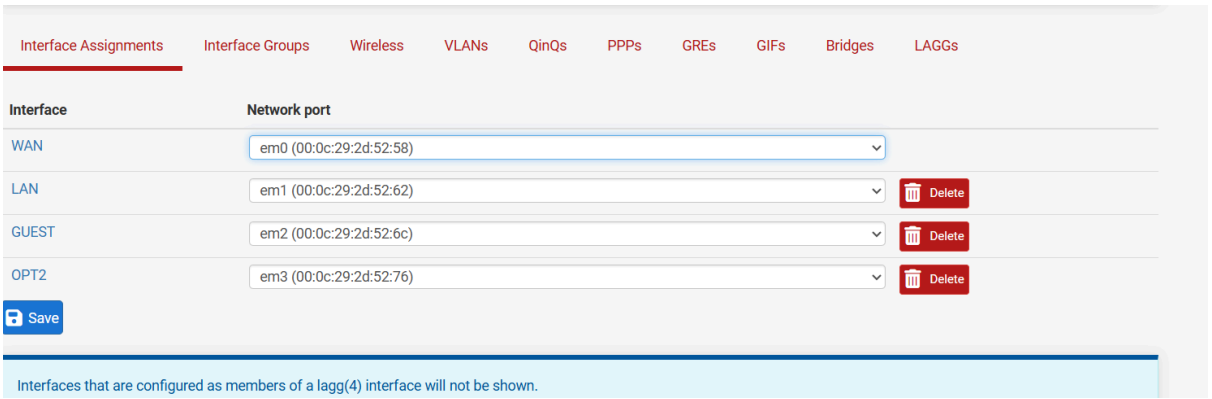

### 5.2: Cấu hình pfSense (The Core)

Đây là trái tim của hệ thống: Firewall, Router, Proxy.

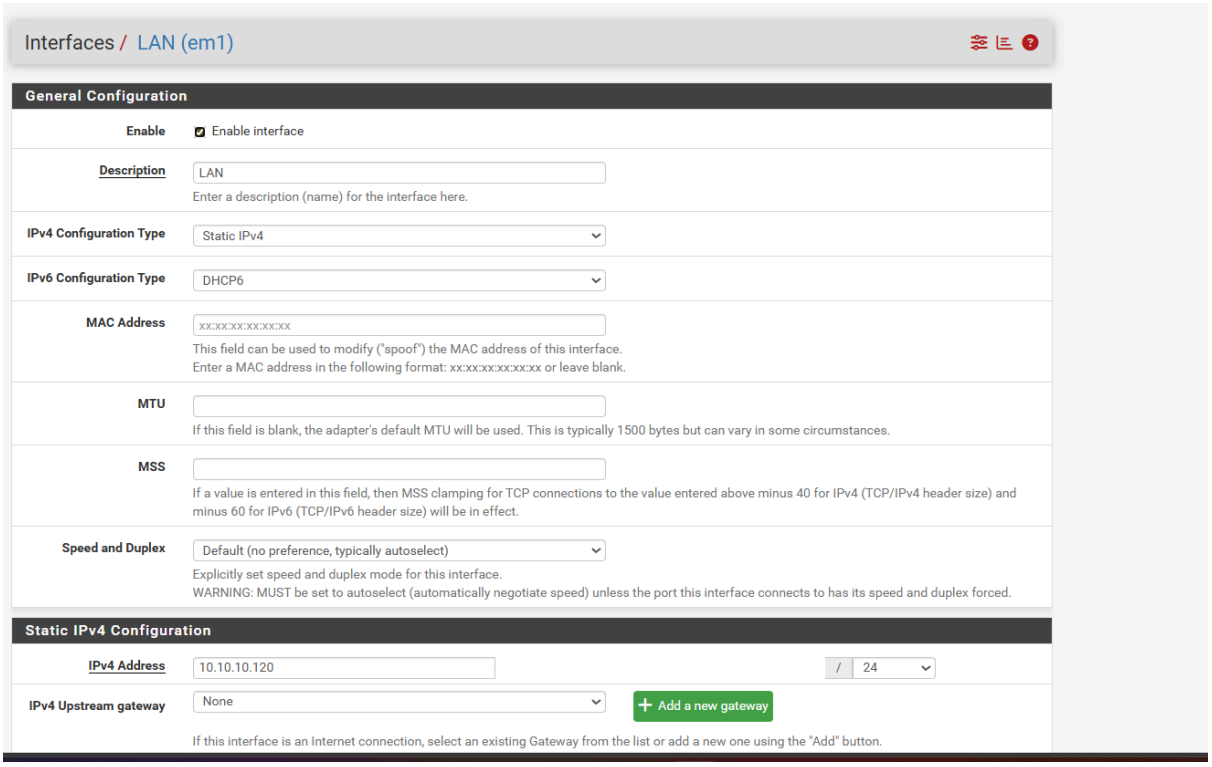
### 1. Interface & IP:

- Truy cập WebGUI pfSense.
- Assign Interfaces: Map các port từ GNS3 vào LAN_STAFF, LAN_GUEST, LAN_SERVER [7].

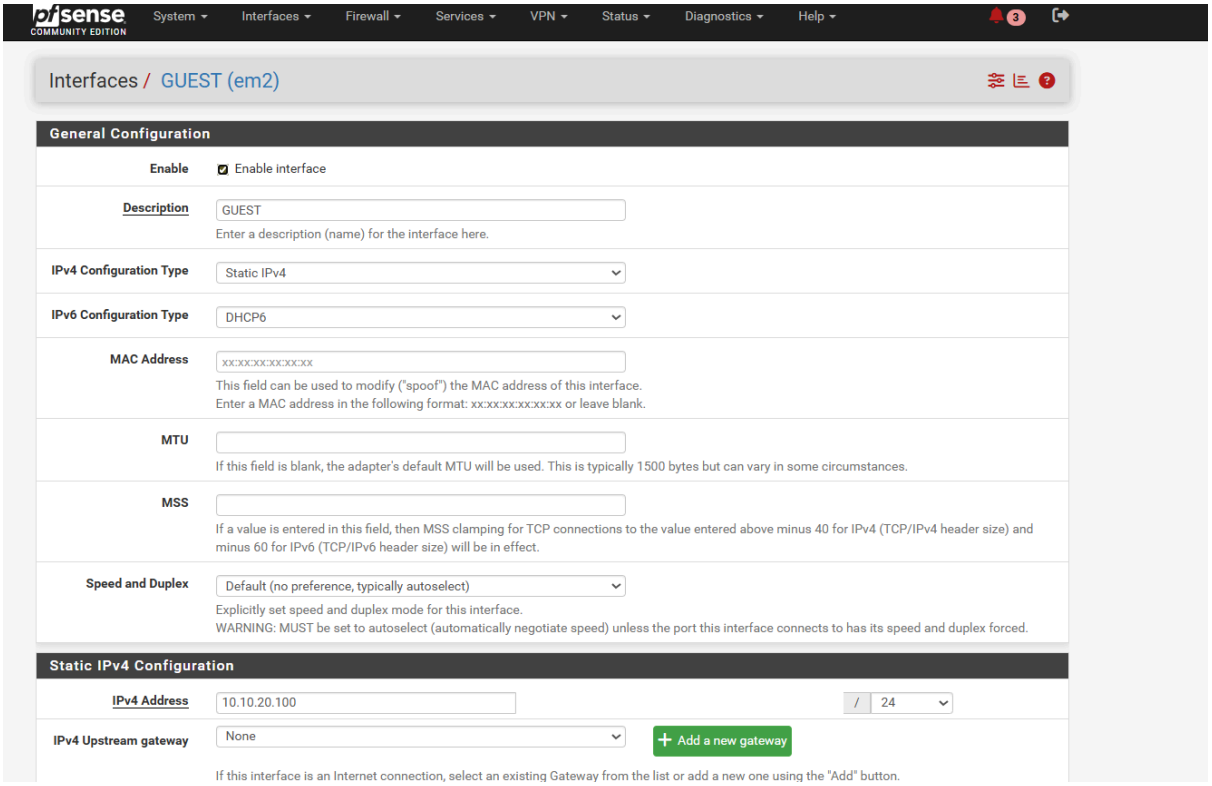
- Set Static IP cho từng interface theo quy hoạch Phần 1.



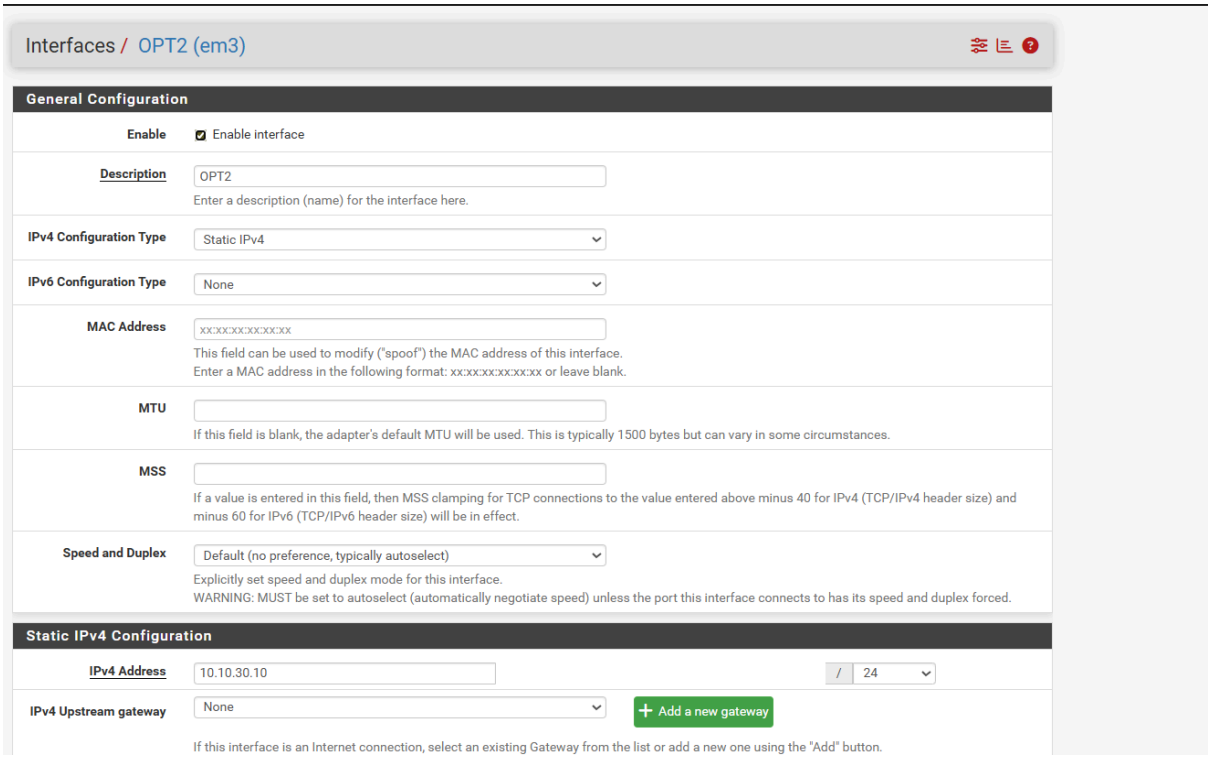

Mạng LAN :




Mạng GUEST:

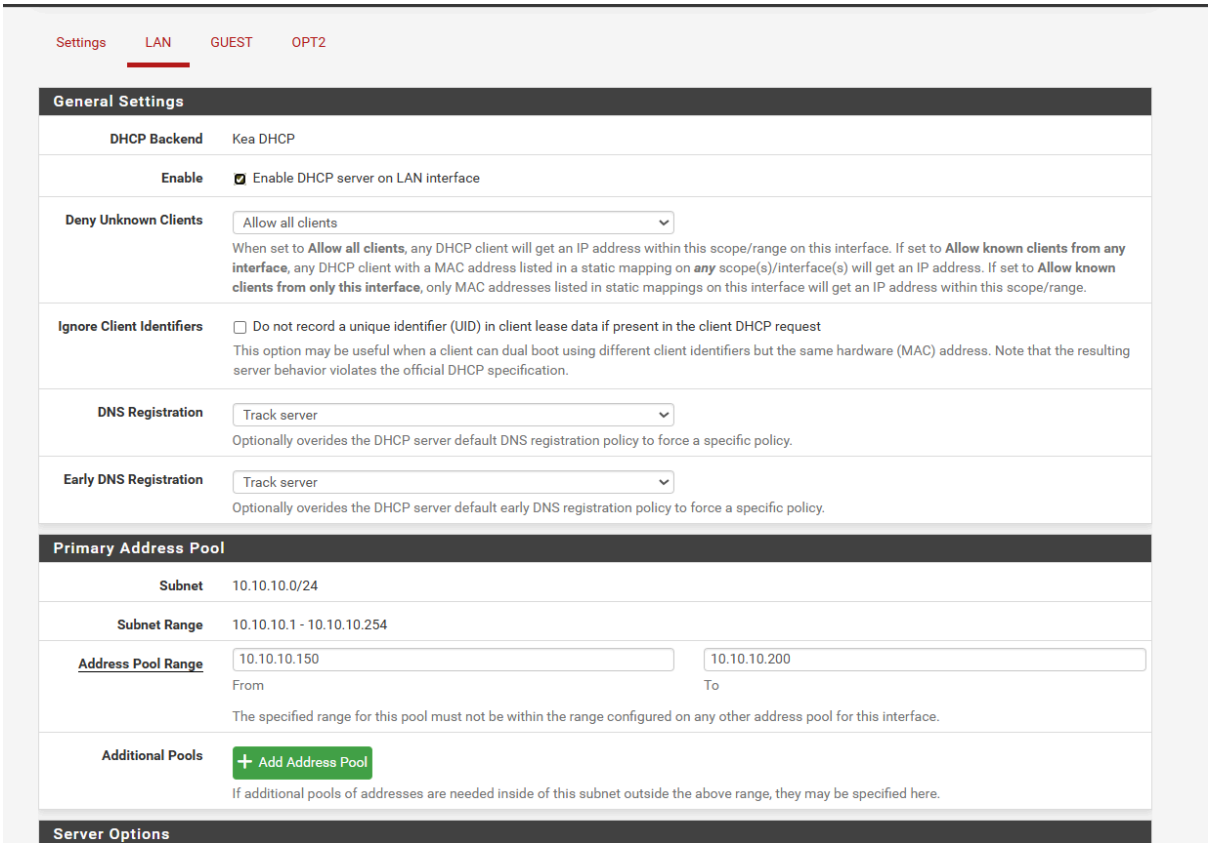



Mạng Server :

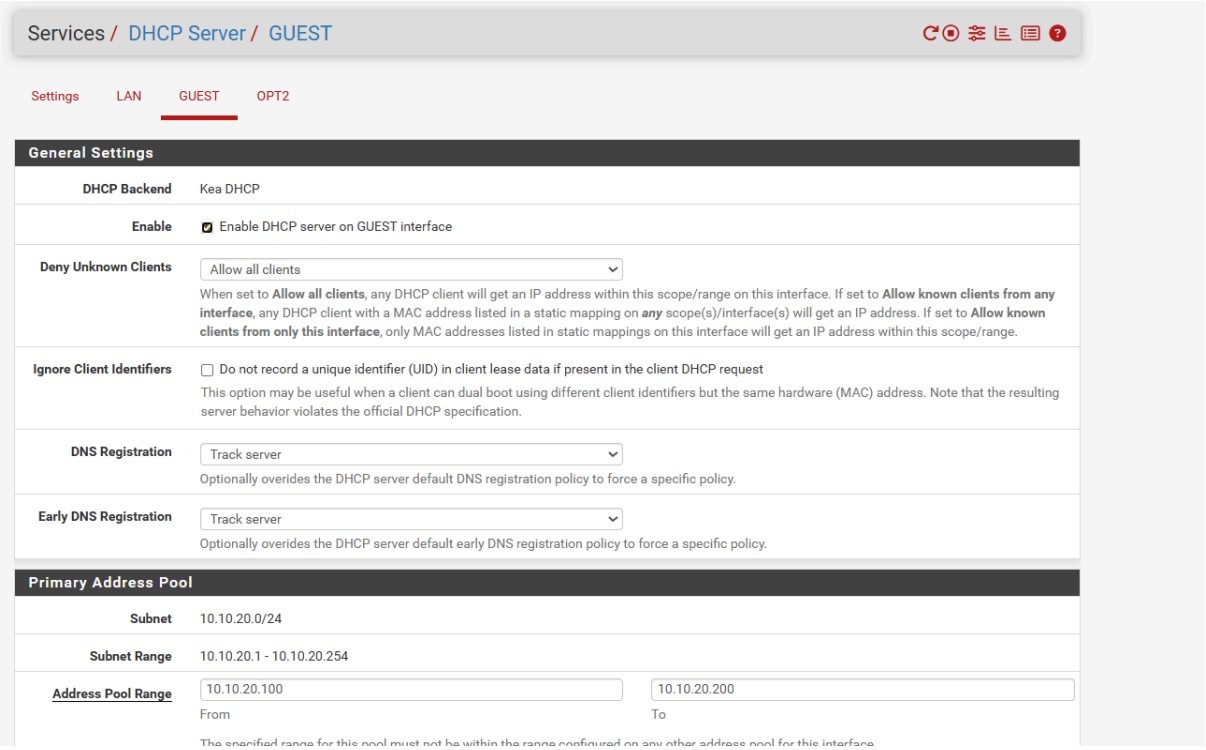



## 2. DHCP & DNS Server:

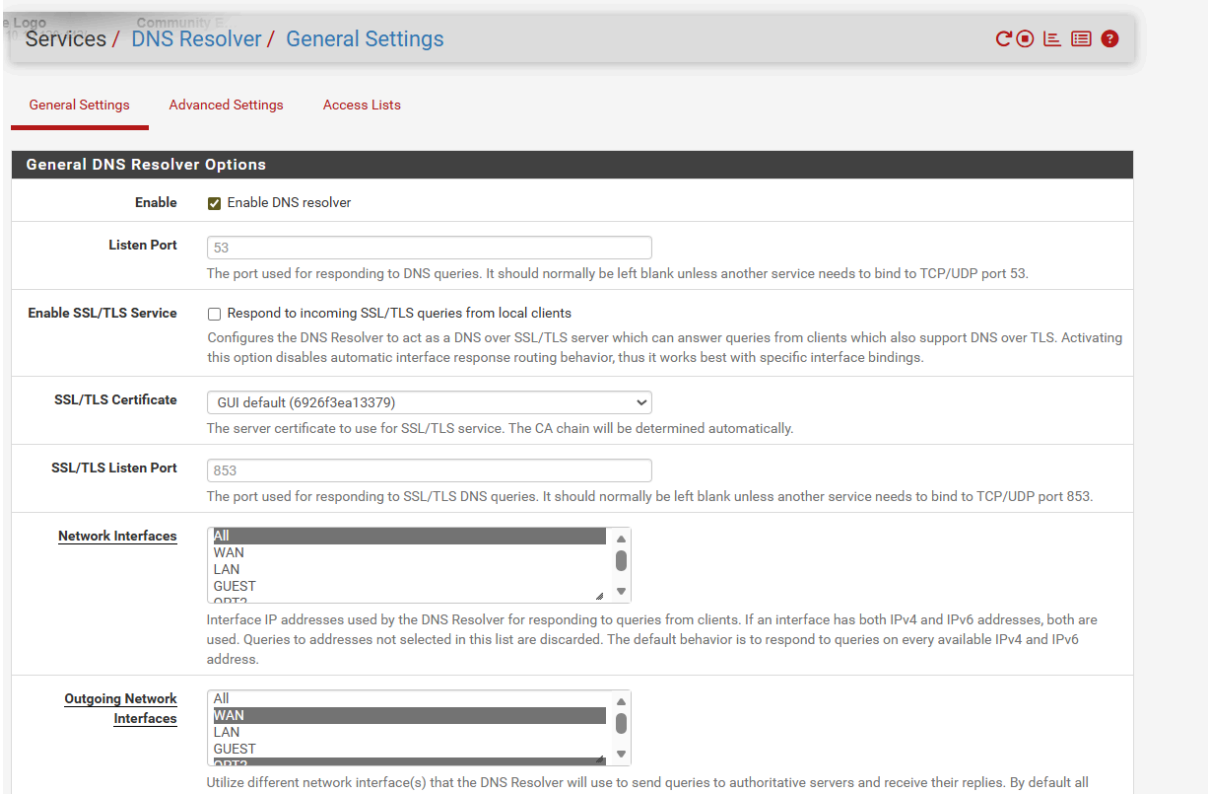
- **DHCP:** Vào Services -> DHCP Server. Enable cho từng interface (Staff, Guest).
  staff:




guest:




- **DNS:** Vào Services -> DNS Resolver. Enable lên để pfSense phân giải tên miền cho client.

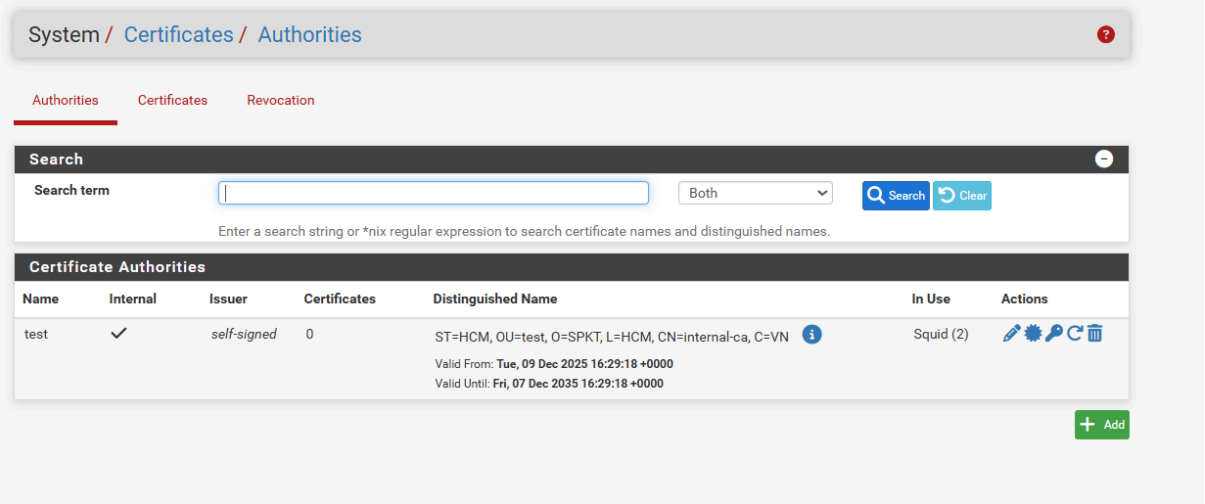



3. Squid Proxy (Logging & Filtering):

Để bắt logs nhân viên truy cập web (HTTPS):

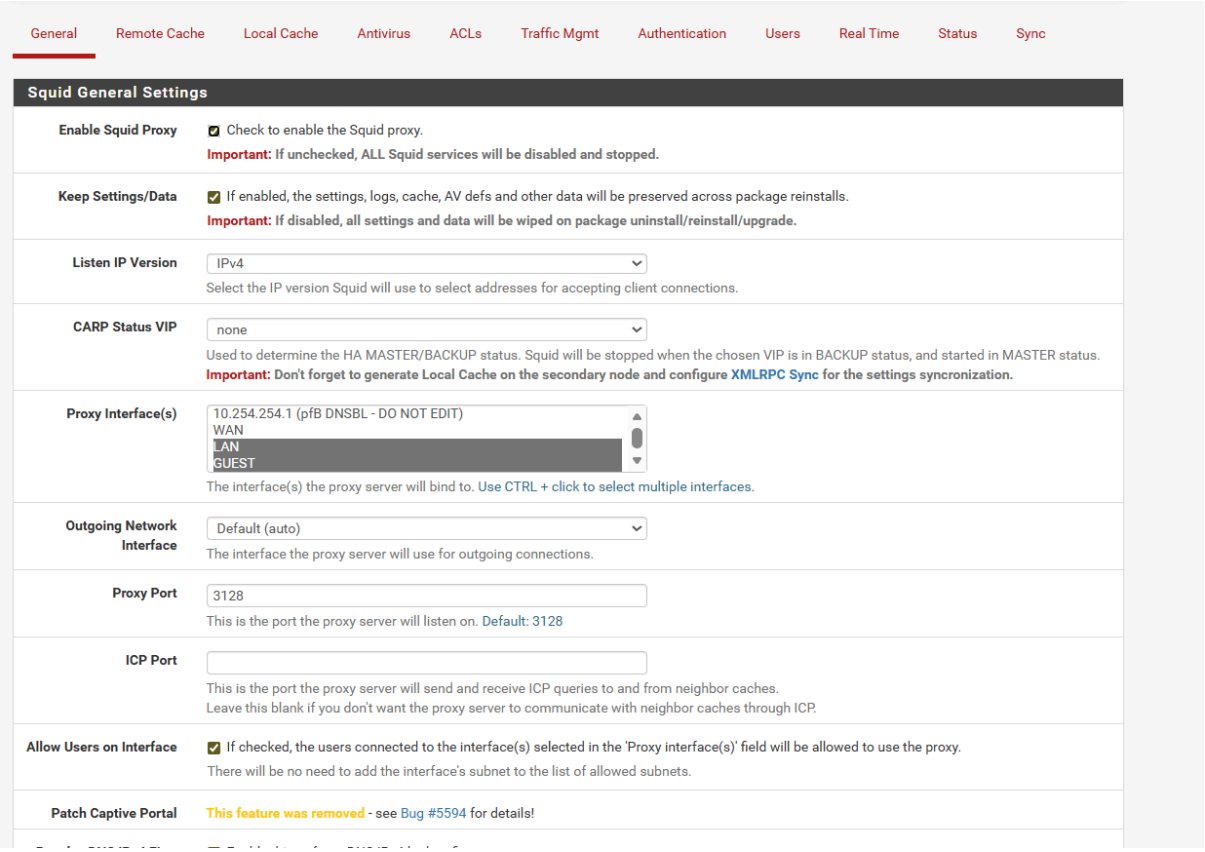
- Cài package: System -> Package Manager -> Install **Squid** và **Lightsquid** (để xem report).
- **Tạo CA:** System -> Cert. Manager. Tạo 1 CA mới (Internal-CA).

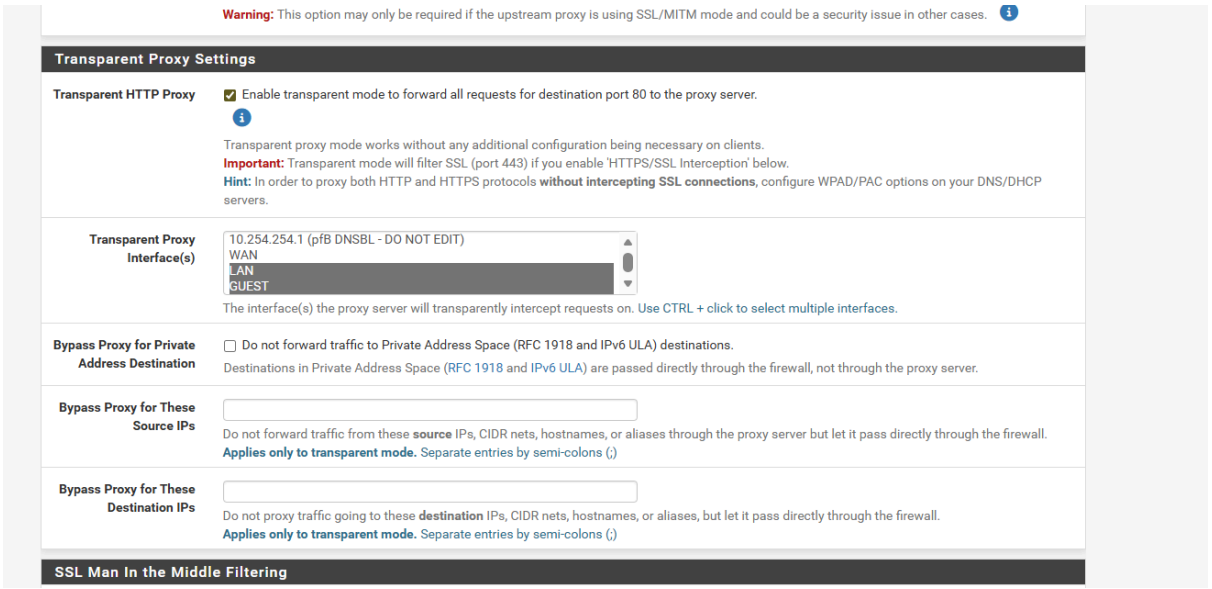
- *Lưu ý:* Export file CA .crt này ra, **cài vào máy Staff/Guest** (Trusted Root Store) thì mới không bị lỗi SSL Warning.
  cấu hình CA nhằm cái vào máy stafff để không bị lỗi ssl:



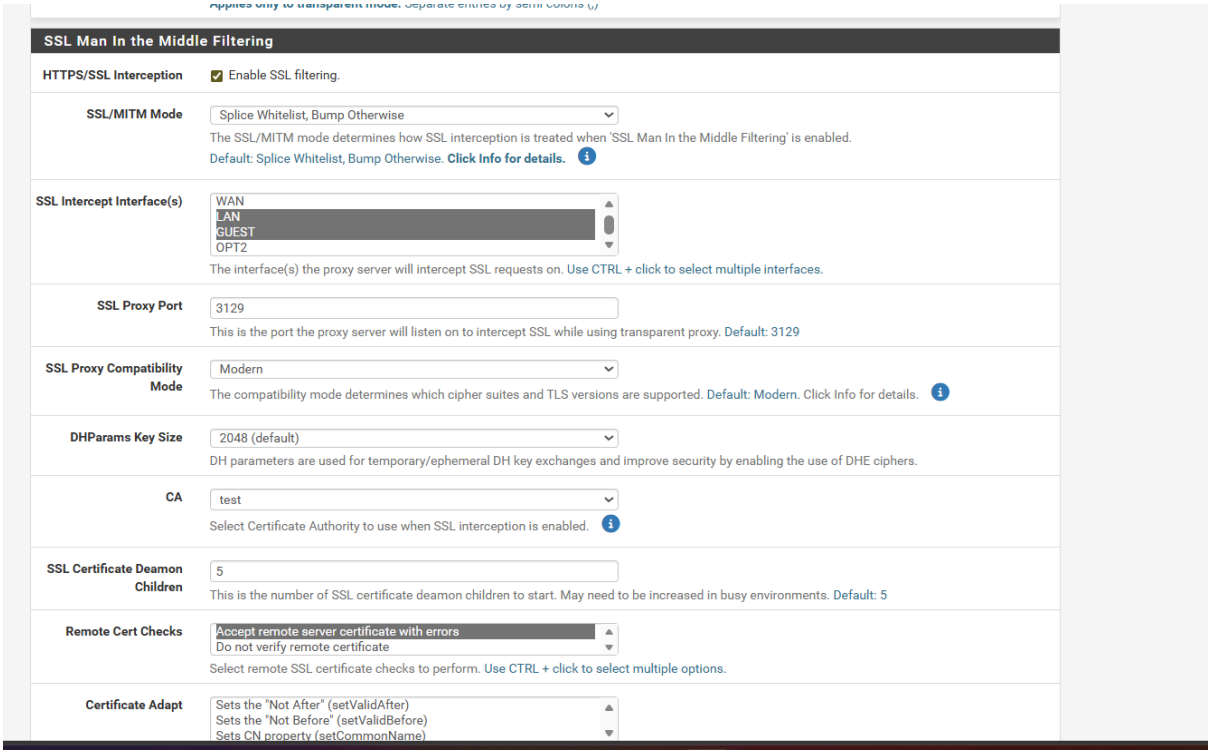

- **Cấu hình Squid:** Services -> Squid Proxy Server:
  - Tab **General**: Enable Squid, chọn Interface (Staff, Guest), Tick "Transparent Proxy".

    cấu hình nhằm đảm bảo có thể bắt được những cổng nào mà tôi muốn :

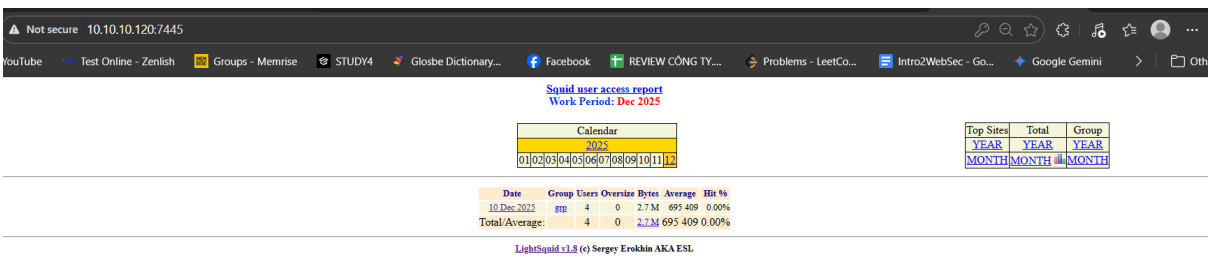





- Tab **SSL Man In the Middle**: Enable, chọn CA vừa tạo ở trên. Log Pages Denied: Enable.




- **Log View:** Kiểm tra logs tại /var/squid/logs/access.log hoặc xem qua giao diện Lightsquid.



### 5.3: Cấu hình Ubuntu Server (Backend)

Đóng vai trò Radius xác thực và Web Server nội bộ.

**1. Networking:**

- Set IP tĩnh: 10.10.30.100.
- Gateway: 10.10.30.10 (pfSense).

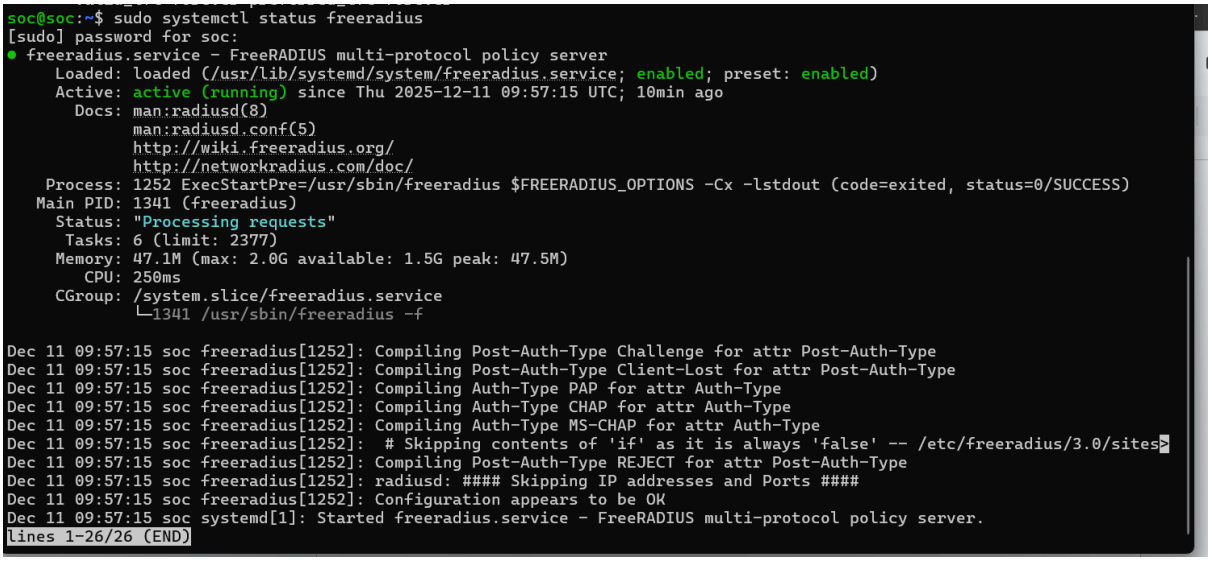
**2. Web Server:**

- Cài Apache2: sudo apt install apache2.
- Tạo trang index demo để test: "Welcome to Internal Secure Server".

**3. FreeRADIUS:**

- Cài đặt: sudo apt install freeradius freeradius-utils.
- Cấu hình Client (cho phép TP-Link AP và pfSense kết nối tới Radius):
  - Edit file /etc/freeradius/3.0/clients.conf.
  - Thêm block client cho mạng Staff (subnet 10.10.10.0/24) với secret = 'Testing123'.
- Tạo User:
  - Edit file /etc/freeradius/3.0/users.
  - Thêm dòng: staff01 Cleartext-Password := "test".
- Restart service: sudo systemctl restart freeradius.

cấu hình systemctl trên freeradius:




cấu hình trên server:

```
root@soc: /etc/freeradius/3.0
 GNU nano 7.2                                        server.cnf *
#req_extensions         = v3_req

[server]
countryName             = VN
stateOrProvinceName     = BinhDuong
localityName            = DiAn
organizationName        = DoAn_Wifi_Staff
emailAddress            = test@hcmute.edu.vn
commonName              = "radius_server"
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names
subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid:always,issuer:always

[alt_names]
DNS.1 = radius.test.local

otherName.0 = 1.3.6.1.5.5.7.8.8;FORMAT:UTF8,UTF8:*.example.com

^G Help      ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
```

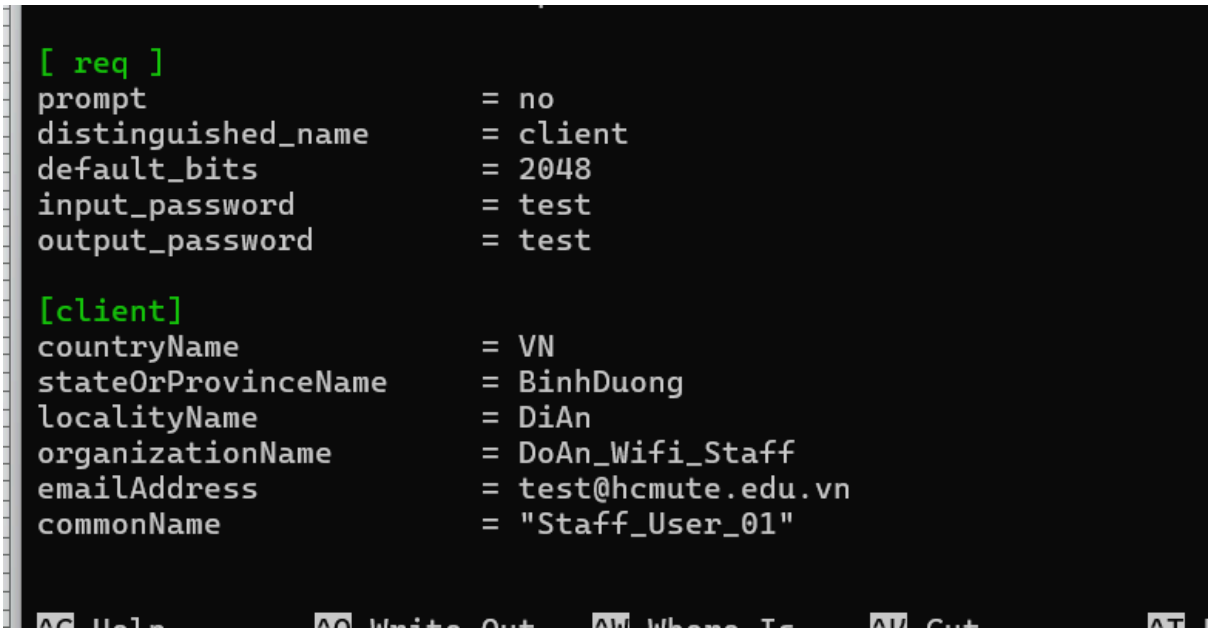
cấu hình trên staff :

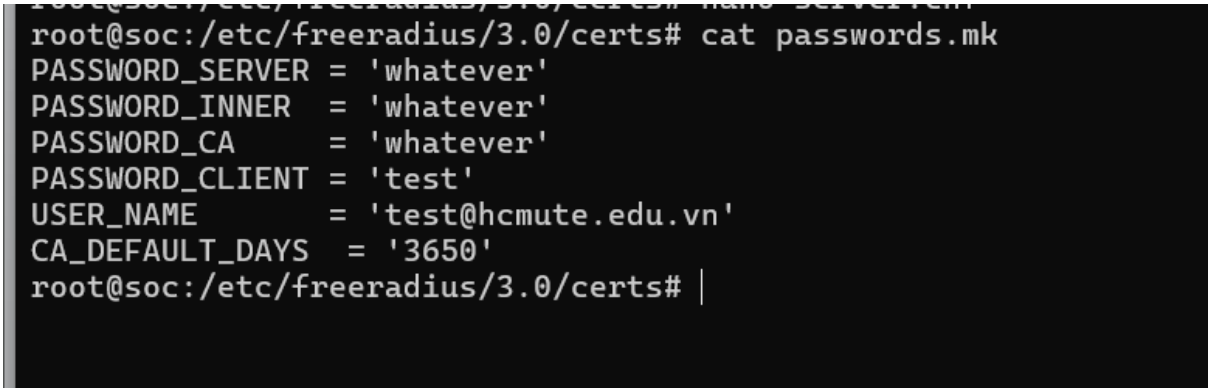
```
[certificate_authority]
# ĐÂY MỚI LÀ CHỖ ĐIỀN THÔNG TIN ĐỒ ÁN
countryName             = VN
stateOrProvinceName     = BinhDuong
localityName            = DiAn
organizationName        = DoAn_Wifi_Staff
emailAddress            = test@hcmute.edu.vn
commonName              = "DoAn Root CA"

[v3_ca]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always
basicConstraints        = critical,CA:true
crlDistributionPoints   = URI:http://www.example.org/example_ca.crl

^G Help      ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit      ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

cấu hình certs để xác thực :

```
#
#clients per_socket_clients {
#       client socket_client {
#               ipaddr = 192.0.2.4
#               secret = testing123
#       }
#}
# --- BAT DAU CAU HINH CUA TOI ---
client Router_Wifi_staff {
    # Cho phep moi IP ket noi (De test cho de, production thi thay bang IP Router)
    ipaddr = 10.10.10.0/24

    # Giao thuc
    proto = *

    # MAT KHAU QUAN TRONG (Phai cau hinh y het tren Router Wifi)
    secret = Testing123

    # Ten ngan gon de hien trong log
    shortname = TL-WR820N
}
# --- KET THUC CAU HINH CUA TOI ---
root@soc:/etc/freeradius/3.0#
```

cấu hình để nhận diện client:




### 5.4: Cấu hình Ubuntu Desktop (Virtual Guest AP)

Dùng USB Wifi biến máy này thành trạm phát sóng cho Guest.

**1. Chuẩn bị:**

- Cắm USB Wifi, Passthrough vào máy ảo Ubuntu Desktop.
- Cài hostapd: sudo apt install hostapd.

**2. Cấu hình Hostapd:**

- Tạo file /etc/hostapd/hostapd.conf:
- Bridging (Quan trọng): Để pfSense cấp DHCP, bạn cần bridge wlan0 (wifi) với eth0 (dây nối về pfSense Guest LAN). Cấu hình Bridge.
  các lệnh :

```
sudo systemctl stop NetworkManager
sudo killall wpa_supplicant
```

```
sudo ip link set wlx00127b216237 down
sudo ip addr flush dev wlx00127b216237

sudo ip link set br0 down
sudo brctl delbr br0

sudo brctl addbr br0
sudo brctl addif br0 ens38

sudo ip link set ens38 up
sudo ip link set br0 up

sudo dhclient br0
sudo ip link set wlx00127b216237 up
sudo killall wpa_supplicant

sudo hostapd -dd test.conf
```

**5.5: Kết nối TP-Link (Staff AP) & GNS3**

Giả lập mạng Staff dùng thiết bị thật.

1. Cấu hình TP-Link: Mode Access Point. Tắt DHCP Server trên TP-Link.

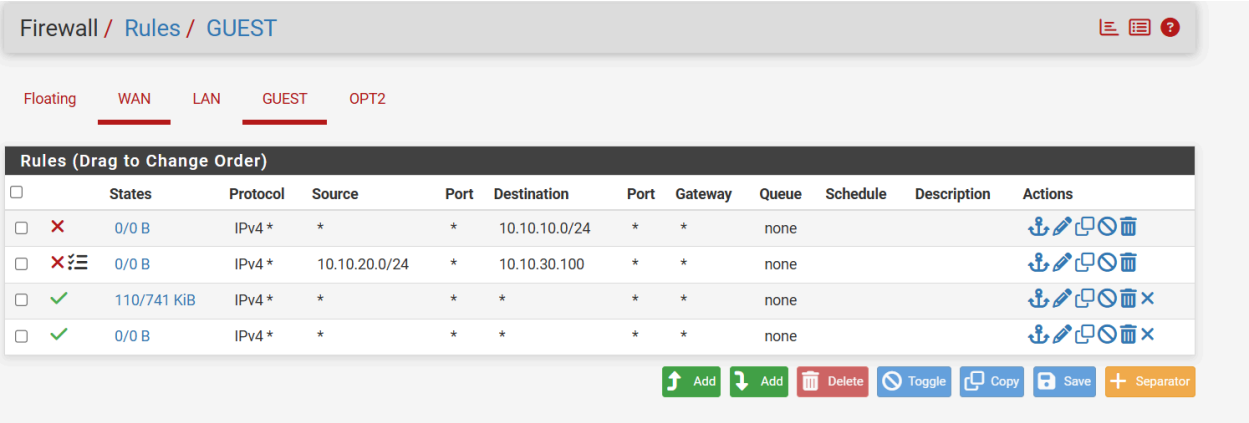
2. SSID: Company_Staff. Security: **WPA2-Enterprise**.
   - Radius IP: 10.10.10.150
   - Radius Secret: Testing123
3. Đấu nối: Cổng LAN TP-Link -> Cổng Ethernet PC -> Cloud Node GNS3-> pfSense LAN_STAFF.

**5.6: Firewall Rules & Hardening**

Thiết lập luật chơi  trên pfSense.

**1. Tab LAN_GUEST:**

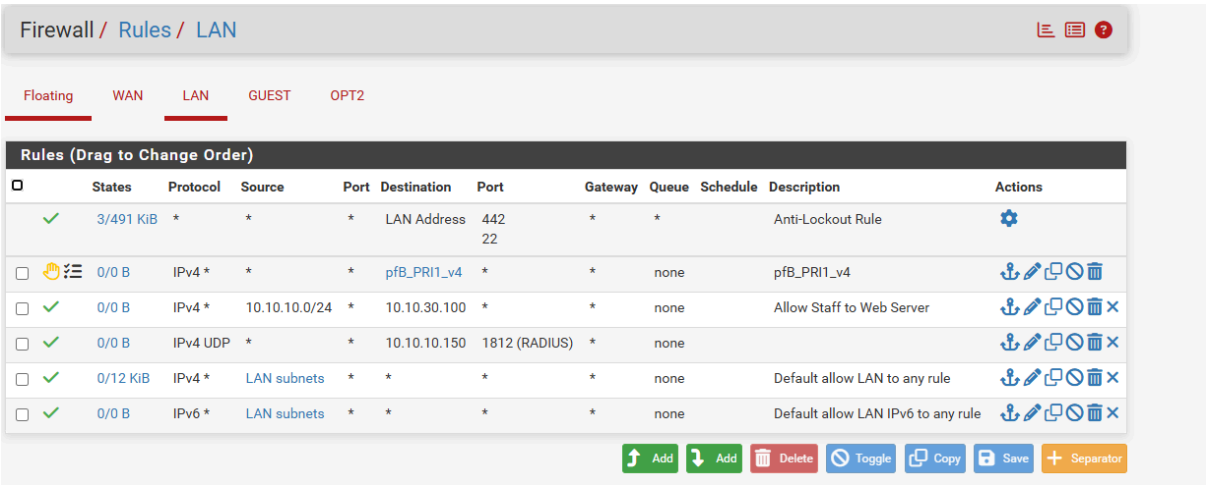
- **Rule 1 (Block Internal) và cho ra internet**




## 2. Tab LAN_STAFF:

- **Rule 1 (Allow Server):** Action: Pass | Proto: TCP | Port: 80/443 | Dst: 10.10.30.10 [15].

- **Rule 2 (Allow Internet):** Action: Pass | Proto: Any | Src: Staff Net | Dst: Any.




## 5.7: Kiểm thử & Logs (Minh chứng kết quả)

1. **Test Staff:** Kết nối wifi Company_Staff -> dùng Ca được tải về để kiểm tra -> Vào được web 10.10.30.100.
2. **Test Guest:** Kết nối wifi Company_Guest -> Vào được Google, ping 10.10.30.10 bị **Request Timed Out** (Block).
3. **Check Logs:** Vào pfSense xem Squid Access Log, thấy rõ máy Staff vừa truy cập trang web nào.

Log hiển thị truy cập của lan và guest :
Lan : Bắt được truy vấn của việc nhân viên gọi đến dns.google nhằm phân giải tên miền và biết được nhân viên khi nào sẽ viết câu search.


**Squid user access report**

User: 10.10.10.151 (?)
Group: ?
Date: **10 Dec 2025**

**Total** **2.4 M**

| # | Accessed site | Connect | Bytes | Cumulative | % |
|---|---|---|---|---|---|
| 1 | sider.ai | 1 | 1.8 M | 1.8 M | 74.4% |
| 2 | www.googletagmanager.com | 1 | 148 148 | 1.9 M | 5.9% |
| 3 | accounts.google.com | 2 | 94 068 | 2.0 M | 3.7% |
| 4 | www-varonis-com.translate.goog | 1 | 90 235 | 2.1 M | 3.5% |
| 5 | e8.c.lencr.org | 1 | 56 751 | 2.2 M | 2.2% |
| 6 | e7.c.lencr.org | 1 | 54 692 | 2.2 M | 2.1% |
| 7 | www.google-analytics.com | 2 | 22 748 | 2.2 M | 0.9% |
| 8 | pusha.viblo.asia | 4 | 22 074 | 2.2 M | 0.8% |
| 9 | beacons.gcp.gvt2.com | 19 | 19 549 | 2.3 M | 0.7% |
| 10 | tt-convers-wpa.chat.zalo.me | 1 | 16 129 | 2.3 M | 0.6% |
| 11 | steamcommunity.com | 4 | 10 499 | 2.3 M | 0.4% |
| 12 | api.steampowered.com | 5 | 9 866 | 2.3 M | 0.3% |
| 13 | encrypted-tbn0.gstatic.com | 3 | 6 925 | 2.3 M | 0.2% |
| 14 | tt-profile-wpa.chat.zalo.me | 11 | 6 348 | 2.3 M | 0.2% |
| 15 | fonts.googleapis.com | 2 | 5 918 | 2.3 M | 0.2% |
| 16 | ws4-msg.chat.zalo.me | 10 | 5 630 | 2.3 M | 0.2% |
| 17 | lh3.googleusercontent.com | 1 | 5 580 | 2.3 M | 0.2% |
| 18 | ws1-msg.chat.zalo.me | 9 | 5 067 | 2.3 M | 0.2% |
| 19 | ws5-msg.chat.zalo.me | 9 | 5 067 | 2.3 M | 0.2% |
| 20 | images.dmca.com | 2 | 4 807 | 2.3 M | 0.1% |
| 21 | login.microsoftonline.com | 2 | 4 593 | 2.3 M | 0.1% |
| 22 | ws2-msg.chat.zalo.me | 8 | 4 504 | 2.4 M | 0.1% |
| 23 | www.helloworldsaigon.com:443 | 1 | 4 289 | 2.4 M | 0.1% |
| 24 | b1.nel.goog | 2 | 4 224 | 2.4 M | 0.1% |
| 25 | cdn.jsdelivr.net | 1 | 4 142 | 2.4 M | 0.1% |
| 26 | ws3-msg.chat.zalo.me | 6 | 3 378 | 2.4 M | 0.1% |
| 27 | www.msftncsi.com | 10 | 2 610 | 2.4 M | 0.1% |
| 28 | recentsearch.chat.zalo.me | 1 | 2 571 | 2.4 M | 0.1% |
| 29 | event.sider.ai | 4 | 1 976 | 2.4 M | 0.0% |
| 30 | clientconfig.akamai.steamstatic.com | 1 | 1 957 | 2.4 M | 0.0% |
| 31 | www.bing.com | 1 | 1 670 | 2.4 M | 0.0% |
| 32 | twemoji.maxcdn.com | 1 | 1 551 | 2.4 M | 0.0% |
| 33 | translate.google.com | 1 | 1 282 | 2.4 M | 0.0% |
| 34 | stats.g.doubleclick.net | 1 | 905 | 2.4 M | 0.0% |

Guest : thì chỉ bắt được mỗi tên miền :

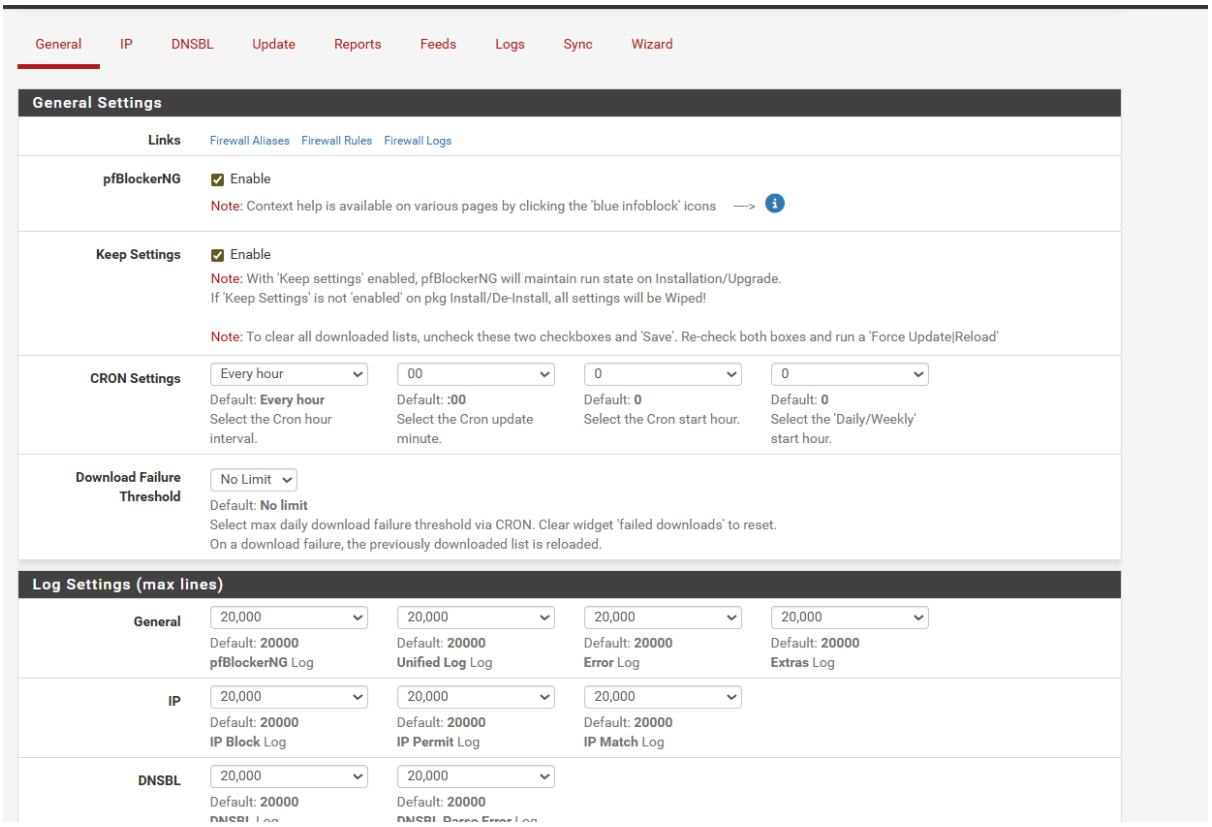
**Squid user access report**

User: 10.10.20.101 (?)
Group: ?
Date: **10 Dec 2025**

| Total | | | 246 282 | | |
|---|---|---|---|---|---|
| # | Accessed site | Connect | Bytes | Cumulative | % |
| 1 | sildo.com | 11 | 202 753 | 202 753 | 82.3% |
| 2 | connectivitycheck.gstatic.com | 103 | 20 703 | 223 456 | 8.4% |
| 3 | c.whatsapp.net | 5 | 5 950 | 229 406 | 2.4% |
| 4 | ire-dsu.shalltry.com | 17 | 5 151 | 234 557 | 2.0% |
| 5 | clientservices.googleapis.com | 1 | 2 390 | 236 947 | 0.9% |
| 6 | log.api.zaloapp.com | 5 | 1 785 | 238 732 | 0.7% |
| 7 | open.boomplaymusic.com | 3 | 1 482 | 240 214 | 0.6% |
| 8 | clients2.google.com | 1 | 1 251 | 241 465 | 0.5% |
| 9 | ssl.google-analytics.com | 1 | 937 | 242 402 | 0.3% |
| 10 | dantricdn.com | 1 | 799 | 243 201 | 0.3% |
| 11 | device-api.palmplaystore.com | 2 | 746 | 243 947 | 0.3% |
| 12 | df.infra.sz.shopee.vn | 1 | 562 | 244 509 | 0.2% |
| 13 | ire-oneid.shalltry.com | 1 | 522 | 245 031 | 0.2% |
| 14 | ire-dsc.shalltry.com | 2 | 470 | 245 501 | 0.1% |
| 15 | nehaaj-inapps.appsflyersdk.com | 1 | 411 | 245 912 | 0.1% |
| 16 | newsaggreg.shalltry.com | 1 | 370 | 246 282 | 0.1% |
| 17 | 142.250.71.170:443 | 1 | 0 | 246 282 | 0.0% |
| 18 | 74.125.68.190:443 | 2 | 0 | 246 282 | 0.0% |
| 19 | 47.245.138.185:443 | 3 | 0 | 246 282 | 0.0% |
| 20 | 142.250.198.227:443 | 1 | 0 | 246 282 | 0.0% |
| 21 | 142.250.198.234:443 | 1 | 0 | 246 282 | 0.0% |
| 22 | 142.251.10.102:443 | 4 | 0 | 246 282 | 0.0% |
| 23 | 34.36.65.236:443 | 1 | 0 | 246 282 | 0.0% |
| 24 | 23.59.80.65:443 | 2 | 0 | 246 282 | 0.0% |
| 25 | 103.176.145.87:443 | 1 | 0 | 246 282 | 0.0% |
| 26 | 143.92.73.201:443 | 6 | 0 | 246 282 | 0.0% |
| 27 | 108.157.34.108:443 | 1 | 0 | 246 282 | 0.0% |
| 28 | 57.144.14.145:443 | 3 | 0 | 246 282 | 0.0% |
| 29 | 142.250.4.94:443 | 55 | 0 | 246 282 | 0.0% |
| 30 | 27.77.82.139:443 | 1 | 0 | 246 282 | 0.0% |
| 31 | 163.70.159.42:443 | 81 | 0 | 246 282 | 0.0% |
| 32 | 125.234.51.74:443 | 1 | 0 | 246 282 | 0.0% |
| 33 | 142.250.76.10:443 | 3 | 0 | 246 282 | 0.0% |

---

Còn phần chặn traffic dựa trên địa chỉ ip nhằm không cho nhân viên truy cập đến những trang web không phù hợp gây mất an toàn bằng cách sử dụng công cụ pfBlockerNG:


General
IP
DNSBL
Update
Reports
Feeds
Logs
Sync
Wizard
General Settings
Links
Firewall Aliases
Firewall Rules
Firewall Logs
pfBlockerNG
Enable
Note: Context help is available on various pages by clicking the 'blue infoblock' icons
Keep Settings
Enable
Note: With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade.
If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!
Note: To clear all downloaded lists, uncheck these two checkboxes and 'Save'. Re-check both boxes and run a 'Force Update|Reload'
CRON Settings
Every hour
Default: Every hour
Select the Cron hour interval.
00
Default: :00
Select the Cron update minute.
0
Default: 0
Select the Cron start hour.
0
Default: 0
Select the 'Daily/Weekly' start hour.
Download Failure Threshold
No Limit
Default: No limit
Select max daily download failure threshold via CRON. Clear widget 'failed downloads' to reset.
On a download failure, the previously downloaded list is reloaded.
Log Settings (max lines)
General
20,000
Default: 20000
pfBlockerNG Log
20,000
Default: 20000
Unified Log Log
20,000
Default: 20000
Error Log
20,000
Default: 20000
Extras Log
IP
20,000
Default: 20000
IP Block Log
20,000
Default: 20000
IP Permit Log
20,000
Default: 20000
IP Match Log
DNSBL
20,000
Default: 20000
20,000
Default: 20000

# PHẦN KẾT LUẬN

## 1. Tóm tắt các kết quả đạt được

Mô hình đã được thiết kế và triển khai thành công trong môi trường ảo hóa (VM và GNS3) với đầy đủ các thành phần cốt lõi:

- Xác thực mạnh mẽ (802.1X): Triển khai FreeRADIUS trên Ubuntu Server để thực hiện xác thực tập trung, đảm bảo chỉ người dùng có tài khoản hợp lệ mới được cấp quyền truy cập mạng Staff. Cơ chế này loại bỏ hoàn toàn nguy cơ rò rỉ dữ liệu khi sử dụng một mật khẩu chung.
- Kiểm soát truy cập và Phân đoạn mạng (pfSense Firewall): Sử dụng pfSense làm tường lửa trung tâm và cổng mạng, thiết lập các vùng mạng logic (VLAN 10 Staff, VLAN 20 Guest, VLAN 30 Server). Các quy tắc Firewalling chi tiết đã được cấu hình thành công để cô lập hoàn toàn mạng Guest khỏi tài nguyên nội bộ (mạng Servers và Staff), ngăn chặn các cuộc tấn công mở rộng (Lateral Movement).
- Giám sát và Ghi Log chuyên sâu (Squid Proxy): Tích hợp thành công Squid Transparent Proxy và cơ chế SSL Man In the Middle trên pfSense. Điều này giúp hệ thống có khả năng ghi lại chi tiết URL truy cập của từng người dùng (cả HTTP và HTTPS), cung cấp bằng chứng kiểm toán (auditing) và khả năng truy vết sự cố an ninh mạng một cách minh bạch, đáp ứng yêu cầu pháp lý về quản lý người dùng.
- Hệ thống dịch vụ mạng cốt lõi: Cấu hình hoàn chỉnh các dịch vụ DHCP và DNS trên pfSense để quản lý việc cấp phát và phân giải tên miền cho từng phân đoạn mạng.

## 2. Ý nghĩa và Giá trị thực tiễn

Đồ án không chỉ dừng lại ở việc chứng minh tính khả thi của các công nghệ tiêu chuẩn quốc tế mà còn cung cấp một mô hình triển khai thực tế, chi phí thấp (sử dụng hoàn toàn các giải pháp mã nguồn mở như pfSense và FreeRADIUS) và dễ dàng nhân rộng. Giải pháp này góp phần nâng cao an toàn thông tin mạng không dây, đáp ứng các tiêu chí bảo mật: Nhận dạng, Xác thực, và Ủy quyền cho mọi kết nối.

## 3. Hạn chế và Hướng phát triển

Mặc dù hệ thống đã đạt được các mục tiêu đề ra, vẫn còn một số hạn chế và hướng phát triển tiềm năng:

- **Quản lý Chứng chỉ:** Mô hình hiện tại tập trung vào xác thực mật khẩu qua PEAP/EAP-TTLS. Hướng phát triển tiếp theo là triển khai đầy đủ EAP-TLS dựa

trên Public Key Infrastructure (PKI) để đạt được mức độ bảo mật cao nhất (không phụ thuộc vào mật khẩu), mặc dù yêu cầu quản lý chứng chỉ phức tạp hơn.

- **Tích hợp NAC:** Nghiên cứu và tích hợp các giải pháp Network Access Control (NAC) mã nguồn mở để kiểm tra tình trạng bảo mật (ví dụ: Antivirus, Patch Level) của thiết bị đầu cuối trước khi cấp quyền truy cập.
- **Tính sẵn sàng cao (High Availability):** Triển khai pfSense và FreeRADIUS dưới dạng cặp HA (High Availability) để đảm bảo mạng không bị gián đoạn dịch vụ khi một máy chủ gặp sự cố.

## 4. Kết luận và kiến nghị

Tóm lại, đồ án của nhóm đã chứng minh thành công tính hiệu quả và tính khả thi của việc thiết kế và triển khai một hệ thống Wi-Fi chuẩn Enterprise (802.1X + RADIUS) với chi phí tối ưu, sử dụng các công nghệ mã nguồn mở hàng đầu (pfSense và FreeRADIUS). Hệ thống này không chỉ nâng cao đáng kể mức độ bảo mật mạng không dây bằng cách cung cấp cơ chế xác thực cá nhân hóa và cô lập mạng, mà còn đáp ứng được các yêu cầu pháp lý về kiểm toán và truy vết hoạt động người dùng. Thành công của đồ án mở ra một mô hình thực tiễn, chi phí thấp và dễ dàng nhân rộng, góp phần vào công cuộc chuyển đổi số an toàn và bảo vệ tài sản thông tin cho các tổ chức tại Việt Nam trong thời kỳ mới.

## TÀI LIỆU THAM KHẢO

[1] W. Osterhage, *Wireless Network Security*. Tài liệu khóa học không công bố, Goethe-Universität Frankfurt, Frankfurt, Germany, 2018. [Truy cập: 16-Dec-2025]

[2] IEEE Standards Association. Local and metropolitan area networks—Port-Based Network Access Control, IEEE Std 802.1X-20

[3] The FreeRADIUS Project, "FreeRADIUS Documentation," 2024. [Trực tuyến]. Có sẵn: https://www.freeradius.org/documentation/freeradius-server/3.2.9/ . [Truy cập: 16-Dec-2025]

[4] Netgate, "pfSense Documentation," 2024. [Trực tuyến]. Có sẵn: https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf. [Truy cập: 16-Dec-2025]

[5] D. Wessels and k. claffy, "ICP and the Squid Web Cache," Báo cáo Kỹ thuật, CAIDA, 13 August 1997. [Trực tuyến]. Có sẵn: https://www.caida.org/catalog/papers/1998_icp_sq/icp-sq.pdf](https://www.caida.org/catalog/papers/1998_icp_sq/icp-sq.pdf . [Truy cập: 16-Dec-2025].