ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

--------o0o--------

BÁO CÁO ĐỒ ÁN

ĐỀ TÀI: RADIUS AND LDAP

Giảng viên hướng dẫn : Lê Đức Thịnh

Sinh viên thực hiện:

1. Nguyễn Trọng Nhân – 19520801
2. Bùi Quốc Huy– 21520911
3. Nguyễn Long Vũ– 21522800

Lớp : **NT330.O21.ANTT**

TP. Hồ Chí Minh, 25 tháng 5 năm 2024

# LỜI CẢM ƠN

Lời đầu tiên, xin chân thành cảm ơn Ban Giám hiệu Trường Đại học Công nghệ thông tin,khoa Mạng máy tính và truyền thông và quý thầy Lê Đức Thịnh đã tạo nền tảng, điều kiện giúp chúng tôi có hội tiếp cận và nghiên cứu chủ đề này.

Chúng tôi cũng muốn bày tỏ lòng biết ơn sâu sắc đến các tác giả của bài báo khoa học mà chúng tôi đã sử dụng làm cơ sở cho nghiên cứu của mình. Công trình nghiên cứu của quý vị đã cung cấp cho tôi cơ sở lý thuyết và dữ liệu quan trọng để phát triển và thực hiện dự án này.

Trong quá trình nghiên cứu về chủ đề này, có thể do hiểu biết còn nhiều hạn chế nên bài làm khó tránh khỏi những thiếu sót. Chúng tôi rất mong nhận được những lời góp ý chân thành của thầy để bài báo cáo ngày càng hoàn thiện hơn.

Trân trọng.

# NHẬN XÉT CỦA GIẢNG VIÊN

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

**MỤC LỤC**

[LỜI CẢM ƠN 2](#_Toc167734576)

[NHẬN XÉT CỦA GIẢNG VIÊN 3](#_Toc167734577)

[MỤC LỤC 4](#_Toc167734578)

[DANH MỤC HÌNH ẢNH 5](#_Toc167734579)

[DANH MỤC BẢNG 6](#_Toc167734580)

[DANH MỤC VIẾT TẮT 7](#_Toc167734581)

[1. Giới thiệu 8](#_Toc167734582)

[1.1. Tổng quan đề tài 8](#_Toc167734583)

[1.2. Mục tiêu và Phạm vi nghiên cứu 8](#_Toc167734584)

[1.3. Phương pháp nghiên cứu 8](#_Toc167734585)

[2. Cơ sở lý thuyết 8](#_Toc167734586)

[2.1. Khái niệm về 802.1X 8](#_Toc167734587)

[2.2. Khái niệm về RADIUS 9](#_Toc167734588)

[2.3. Khái niệm về LDAP 9](#_Toc167734589)

[3. Phân tích thiết kế hệ thống 11](#_Toc167734590)

[3.1. Tổng quan hệ thống 11](#_Toc167734591)

[3.2. Cấu hình RADIUS server trên Windows server 12](#_Toc167734592)

[3.3. Cấu hình Radius server trên kali linux 14](#_Toc167734593)

[3.4. Cấu hình pfsense để xác thực RADIUS 15](#_Toc167734594)

[4. Thực nghiệm và Kết quả 17](#_Toc167734595)

[4.1. Chuẩn bị 17](#_Toc167734596)

[4.2. Kết quả thực nghiệm 18](#_Toc167734597)

[4.3. Đánh giá 19](#_Toc167734598)

[5. Kết luận và Đề xuất 19](#_Toc167734599)

[5.1. Tóm tắt kết quả nghiên cứu 19](#_Toc167734600)

[5.2. Thách thức và hạn chế 20](#_Toc167734601)

[5.3. Đề xuất cho nghiên cứu tương lai 20](#_Toc167734602)

[6. Tài liệu tham khảo 21](#_Toc167734603)

# DANH MỤC HÌNH ẢNH

[Hình 1: Minh họa RADIUS 9](#_Toc167734555)

[Hình 2: Minh họa LDAP 10](#_Toc167734556)

[Hình 3: Minh họa cách hoạt động dự kiến của hệ thống 11](#_Toc167734557)

[Hình 4: Thiết kế hệ thống với RADIUS server trên Windows server 11](#_Toc167734558)

[Hình 5: Hệ thống freeRadius trên ubuntu 22.04 12](#_Toc167734559)

[Hình 6: Tạo domain 12](#_Toc167734560)

[Hình 7: Tạo certificate doanh nghiệp 13](#_Toc167734561)

[Hình 8: User test thuộc nhóm wlan users 13](#_Toc167734562)

[Hình 9: RADIUS client (Win Server) 13](#_Toc167734563)

[Hình 9: Chính sách xác định nhóm người dùng cần xác thực 14](#_Toc167734564)

[Hình 10: RADIUS client (FreeRADIUS) 14](#_Toc167734565)

[Hình 11: Cấu hình EAP 15](#_Toc167734566)

[Hình 12: Cấu hình Auth Server on pfsense 15](#_Toc167734567)

[Hình 13: Cấu hình CP 15](#_Toc167734568)

[Hình 14: Cấu hình CP - Sử dụng html tùy chỉnh 16](#_Toc167734569)

[Hình 15: Cấu hình CP - Chọn RADIUS Server 16](#_Toc167734570)

[Hình 16: Giao diện html tùy chỉnh 17](#_Toc167734571)

[Hình 17: Ảnh thực tế Router Wifi 17](#_Toc167734572)

[Hình 18: Máy ảo pfsense 18](#_Toc167734573)

[Hình 19: Máy ảo win server 18](#_Toc167734574)

[Hình 20: Log CP (RADIUS win server) 18](#_Toc167734575)

# DANH MỤC BẢNG

# DANH MỤC VIẾT TẮT

|  |  |
| --- | --- |
| Viết tắt | Viết đầy đủ |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |
| EAP | Extensible Authentication Protocol |
| LDAP | Lightweight Directory Access Protocol |
| RADIUS | Remote Authentication Dial-In User Service |
| IEEE | Institute of Electrical and Electronics Engineers |
| RFC | Request for Comments |
| SSL | Secure Sockets Layer |
| SSO | Single Sign-On |
| IETF | Internet Engineering Task Force |
| AD DS | Active Directory Domain Services |
| AD CS | Active Directory Certificate Services |
| NPS | Network Policy Server |
| TLS | Transport Layer Security |
| CP | Captive Portal |
| DHCP | Dynamic Host Configuration Protocol |
| LAN | Local Area Network |
| GUI | Graphical User Interface |

# 1. Giới thiệu

## 1.1. Tổng quan đề tài

Trong lĩnh vực bảo mật mạng không dây, việc triển khai mạng WLAN với giao thức xác thực cơ bản như WPA/WPA 2 là không đủ để đáp ứng nhu cầu kiểm soát người dùng WLAN của doanh nghiệp. Để đáp ứng nhu cầu đó chuẩn 802.1X và giao thức xác thực mở rộng (EAP) xuất hiện.

802.1X/EAP sử dụng một server xác thực để xác thực người dùng WLAN và cấp quyền truy cập tài nguyên mạng cho WLAN.

Server xác thực thường sẽ là RADIUS server và giao tiếp trực tiếp với một cơ sở dữ liệu LDAP.

Đồ án này nhóm sẽ cố gắng triển khai mạng 802.1X có tích hợp RADIUS server và LDAP. Với RADIUS server chạy trên Windows và Linux.

## 1.2. Mục tiêu và Phạm vi nghiên cứu

Mục tiêu của đồ án là triển khai 2 mạng 802.1X có tích hợp RADIUS server (một chạy trên Windows, một chạy trên Linux) và LDAP.

Phạm vị nghiên cứu: hạ tầng mạng, chuẩn 802.1X, Windows Server, freeRadius.

## 1.3. Phương pháp nghiên cứu

Nhóm đọc, nghiên cứu tài liệu: Sách CWSP (Coleman, D., Westcott, D., & Harkins, B. (2016). CWSP, 2nd Edition. Sybex.), tài liệu và các video trên internet.

Thực hành và thử nghiệm trên các router wifi TP-LINK, các máy ảo, pfsense ảo.

# 2. Cơ sở lý thuyết

## 2.1. Khái niệm về 802.1X

Chuẩn 802.1x là chuẩn IEEE liên quan đến điều khiển truy cập hệ thống qua port. Tiêu chuẩn 802.1x cung cấp sự chứng thực và bảo mật thông tin mạnh mẽ, và đó chỉ là một phần trong framework mở rộng an toàn và đầy tiềm năng của mình.

Một hệ thống 802.1x chỉ cần 3 thành tố chính để hoạt động, mỗi thành phần đều riêng biệt không thể tách rời:

* Supplicant: phần mềm được cài đặt phía client với tiêu chuẩn 802.1x và hoạt động trong cả hai môi trường có dây và không dây. Supplicant được tải lên thiết bị của người dùng để gửi yêu cầu truy cập hệ thống
* Authenticator: một thành phần nằm giữa người dùng bên ngoài, nơi cần được chứng thực và kết cấu hạ tầng dùng để thực hiện việc chứng thực. Switch và điểm truy cập mạng không dây (wireless access point) có thể dùng làm Authenticator.
* Authentication Server: một server nhận thông tin RADIUS và dùng chúng kiểm tra chứng thực của người dùng hay thiết bị, thường dùng với chứng thực đầu cuối nơi lưu trữ thông tin như Microsoft Active Directory, LDAP, hay một loại cơ sở dữ liệu nào khác

## 2.2. Khái niệm về RADIUS

RADIUS (Remote Authentication Dial-In User Service) là một giao thức mạng được phát triển bởi Livingston Enterprises vào năm 1991, sử dụng để quản lý việc xác thực, ủy quyền và kế toán người dùng truy cập vào mạng. Nó được sử dụng phổ biến trong mạng không dây, mạng di động và mạng điện thoại từ xa (dial-up). RADIUS hoạt động dựa trên mô hình client-server, trong đó RADIUS server là trung tâm xác thực và ủy quyền, và các thiết bị khách (supplicants) gửi yêu cầu xác thực đến server. RADIUS sử dụng giao thức UDP để truyền tải thông tin xác thực và ủy quyền.

Chức năng Chính:

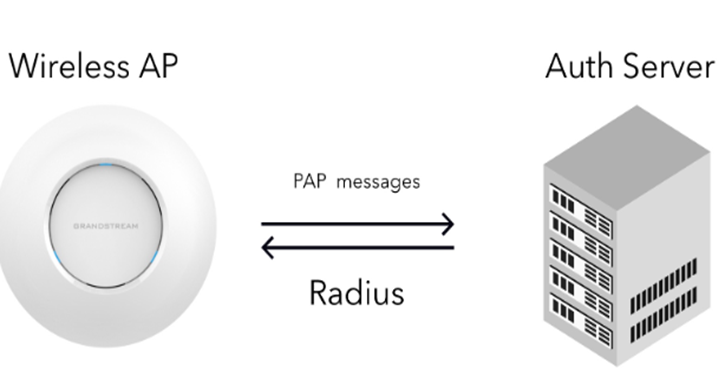
* Authentication: Xác thực danh tính người dùng trước khi cho phép truy cập.
* Authorization: Cấp quyền truy cập và xác định mức độ truy cập của người dùng.
* Accounting: Ghi nhận và theo dõi các hoạt động truy cập của người dùng.

Kiến trúc và Hoạt động của RADIUS hoạt động theo mô hình client-server, trong đó:

* Client: Thiết bị truy cập hoặc máy chủ truy cập mạng yêu cầu xác thực.
* Server: Máy chủ RADIUS xử lý yêu cầu xác thực, ủy quyền và kế toán.

Các RFC Liên quan:

* RFC 2865: Định nghĩa các chức năng Authentication và Authorization cho RADIUS.
* RFC 2866: Định nghĩa chức năng Accounting cho RADIUS.



Hình 1: Minh họa RADIUS

## 2.3. Khái niệm về LDAP

LDAP (Lightweight Directory Access Protocol) là một giao thức cho phép truy cập và duy trì dịch vụ thư mục qua mạng IP. LDAP được phát triển vào những năm 1990 bởi Tim Howes và các cộng sự tại Đại học Michigan. LDAP là một giao thức ứng dụng được sử dụng để cung cấp dịch vụ thư mục (directory) trên mạng IP. LDAP cung cấp phương thức truy cập và quản lý thông tin trong thư mục. Nó hoạt động trên giao thức TCP/IP và sử dụng cổng 389 (hoặc cổng 636 khi sử dụng LDAP qua SSL).

Chức năng Chính và Ứng dụng:

* Chức năng Chính: Cung cấp cơ sở dữ liệu phân tán để lưu trữ và truy xuất thông tin người dùng, nhóm, thiết bị, và các tài nguyên mạng khác.
* Ứng dụng: Được sử dụng rộng rãi trong quản lý thông tin người dùng và xác thực truy cập trong các hệ thống lớn, như hệ thống đăng nhập một lần (SSO), thư mục nhân sự, và quản lý thông tin tài nguyên mạng.

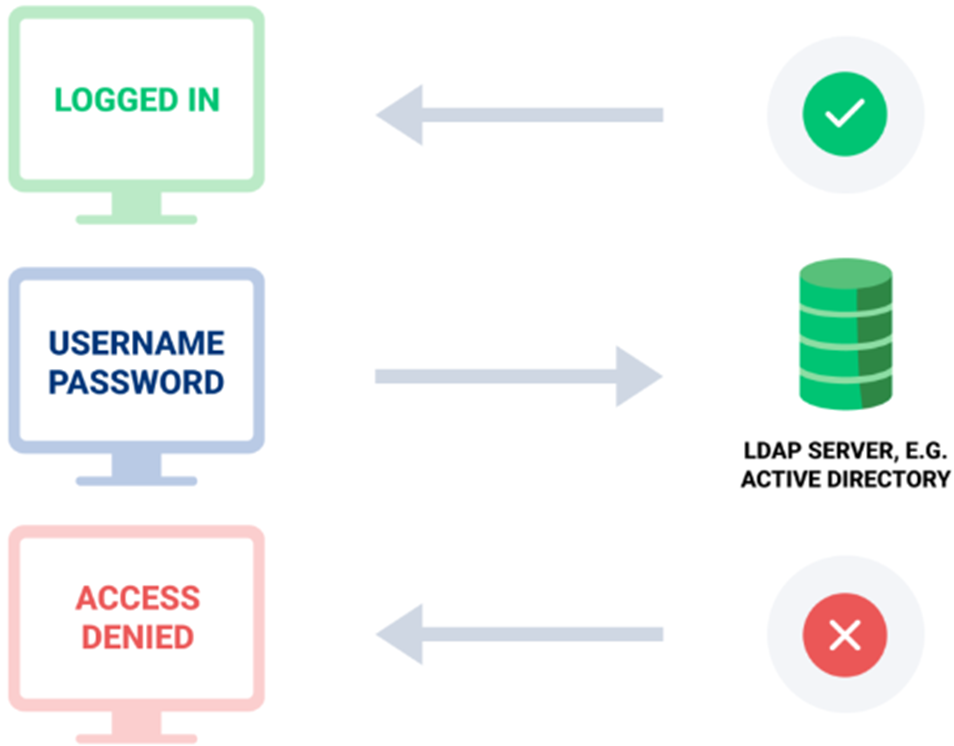
Kiến trúc của LDAP hoạt động theo mô hình client-server, trong đó:

* Client: Gửi các yêu cầu truy cập hoặc sửa đổi thông tin đến máy chủ LDAP.
* Server: Xử lý các yêu cầu và trả về kết quả phù hợp từ cơ sở dữ liệu thư mục.

Cấu trúc dữ liệu của LDAP được tổ chức dưới dạng cây thư mục (directory tree), với các nút (entry) chứa các thuộc tính (attributes) và giá trị (values).

Các Phiên bản và RFC Liên Quan:

* LDAPv3: Phiên bản hiện tại của LDAP, được chuẩn hóa trong IETF RFC 4511, định nghĩa giao thức truyền thông giữa client và server LDAP.

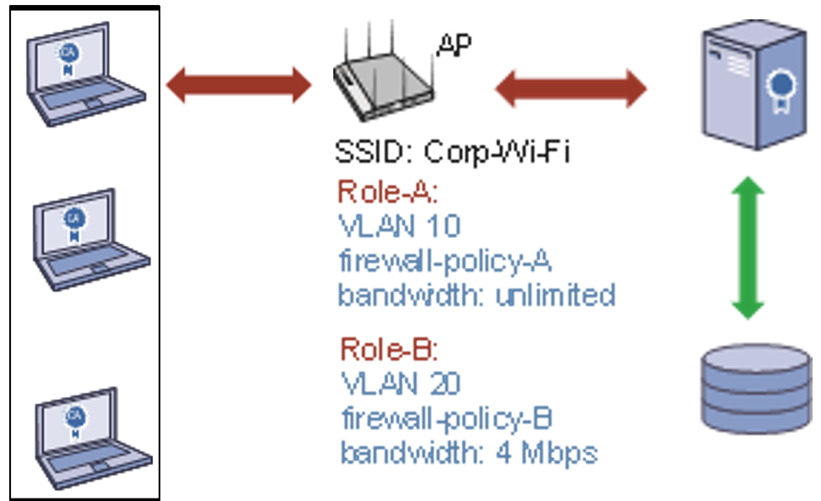


Hình 2: Minh họa LDAP

# 3. Phân tích thiết kế hệ thống

## 3.1. Tổng quan hệ thống

Tổng quan cách hoạt động dự kiến của hệ thống: Yêu Cầu Truy Cập từ Client > Yêu Cầu Gửi Đến Máy Chủ RADIUS > Máy Chủ RADIUS Truy Vấn LDAP > Máy Chủ LDAP Xác Thực Người Dùng > Máy Chủ RADIUS Quyết Định Cấp Quyền > Access Point Cấp Quyền Truy Cập > Ghi Nhận và Kế Toán (Accounting).



Hình 3: Minh họa cách hoạt động dự kiến của hệ thống

Thiết kế hệ thống thực tế với RADIUS server trên Windows Server:

* Các WLAN client sẽ kết nối với router wifi.
* Router wifi được kết nối với cổng LAN của pfsense qua cổng LAN của nó (không dùng cổng WAN).
* Pfsense (máy ảo) triển khai dịch vụ Captive Port và xác thực RADIUS với Windows Server. Cổng WAN của pfsense kết nối tới internet qua mạng ảo NAT.
* Windows server (máy ảo) thực hiện vai trò là RADIUS server.

A computer screen with text and symbols

Description automatically generated with medium confidence

Hình 4: Thiết kế hệ thống với RADIUS server trên Windows server

Thiết kế hệ thống thực tế với RADIUS server trên Kali Linux:

* Các WLAN client sẽ kết nối với router wifi.
* Router wifi được kết nối cổng LAN qua cổng LAN của server freRadiu
* Trên máy server triển khai các dịch vụ của freeRadius
* Cấu hình kết nối xác thực Router wifi thông qua server freeRadius
* Các máy client muốn vào được mạng wifi local phải xác thực được với server freeRadius

A computer and a monitor

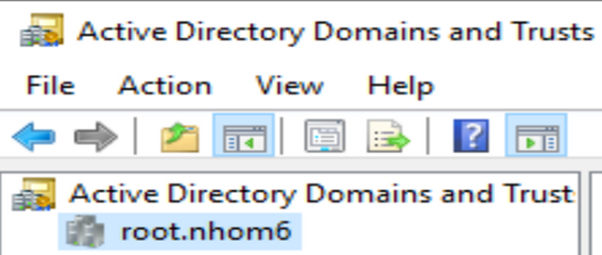
Description automatically generated

Hình 5: Hệ thống freeRadius trên ubuntu 22.04

## 3.2. Cấu hình RADIUS server trên Windows server

Video cấu hình window server: [Config WinServer.mp4](https://drive.google.com/file/d/1wSJXkFUyTMUCMFhEMUw4UEWkJm0UuHKI/view)

Bước 1: Cấu hình AD DS (Active Directory Domain Services). Tạo domain để quản lý người dùng.



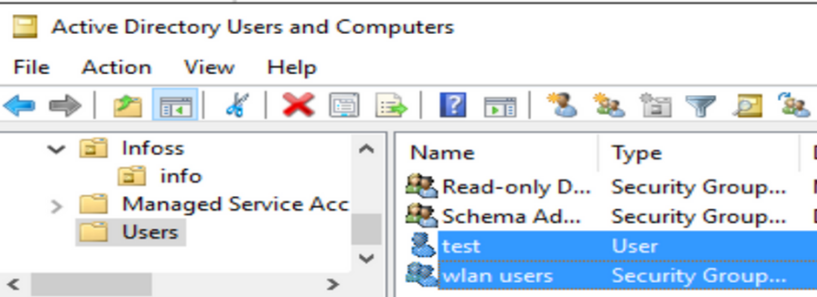
Hình 6: Tạo domain

Bước 2: Cấu hình AD CS (Active Directory Certificate Services). Tạo chứng chỉ doanh nghiệp (cần có domain) để thực hiện RADIUS trên Windows server.



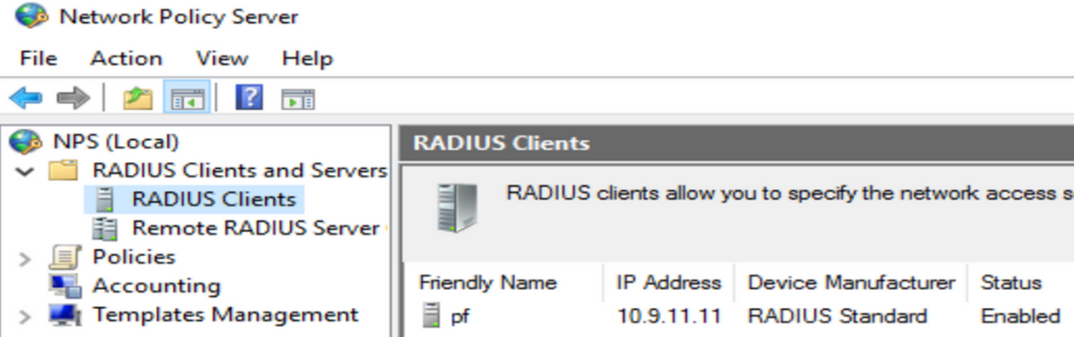
Hình 7: Tạo certificate doanh nghiệp

Bước 3: Tạo User và nhóm User cho khách kết nối Wifi.



Hình 8: User test thuộc nhóm wlan users

Bước 4: Cấu hình Network Policy Server (NPS). Tạo RADIUS client và thêm chính sách để xác định nhóm người dùng cần xác thực. Sau bước này Windows Server đã có chức năng của RADIUS Server, đồng thời cũng có mở cổng và chức năng của LDAP. Có thể hiểu Windows server vừa có thể xác thực RADIUS vừa lưu trữ LDAP.



Hình 9: RADIUS client (Win Server)

A computer screen shot of a computer

Description automatically generated

Hình 10: Chính sách xác định nhóm người dùng cần xác thực

Bước 5: Chỉnh sửa rules của tường lửa hoặc tắt sao cho RADIUS Server hoạt động không bị cản trở.

## 3.3. Cấu hình Radius server trên kali linux

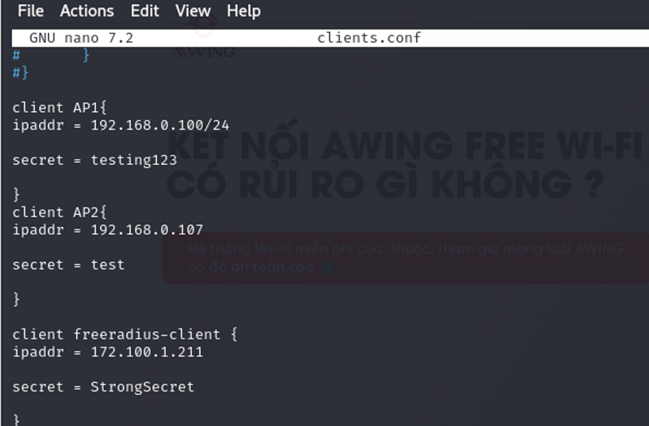
Bước 1: Cài đặt freeradius qua lệnh apt trên kali linux.

sudo apt update

sudo apt install freeradius freeradius-utils

Bước 2: Chỉnh sửa cấu hình cấu hình máy khách FreeRADIUS.

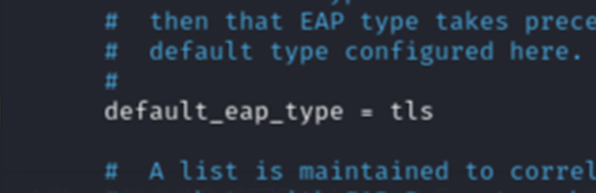
sudo nano /etc/freeradius/3.0/clients.conf



Hình 11: RADIUS client (FreeRADIUS)

Bước 3: Chỉnh sửa cấu hình eap bật tls.

sudo nano /etc/freeradius/3.0/epa



Hình 12: Cấu hình EAP

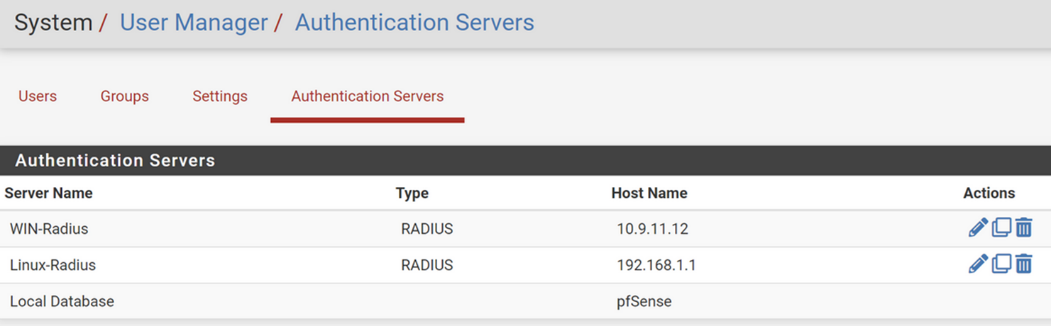
Bước 4: Chạy máy chủ FreeRADIUS.

sudo systemctl start freeradius

sudo systemctl enable freeradius

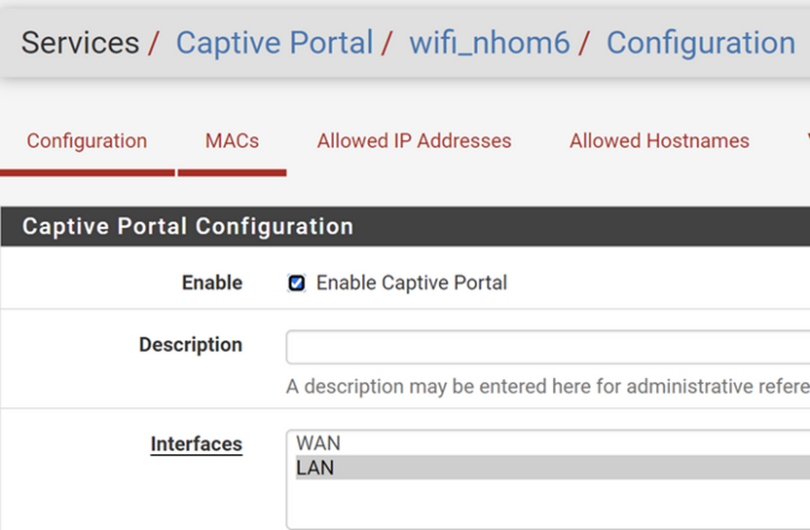
## 3.4. Cấu hình pfsense để xác thực RADIUS

Bước 1: Cấu hình System/User Manager/Authentication Servers.

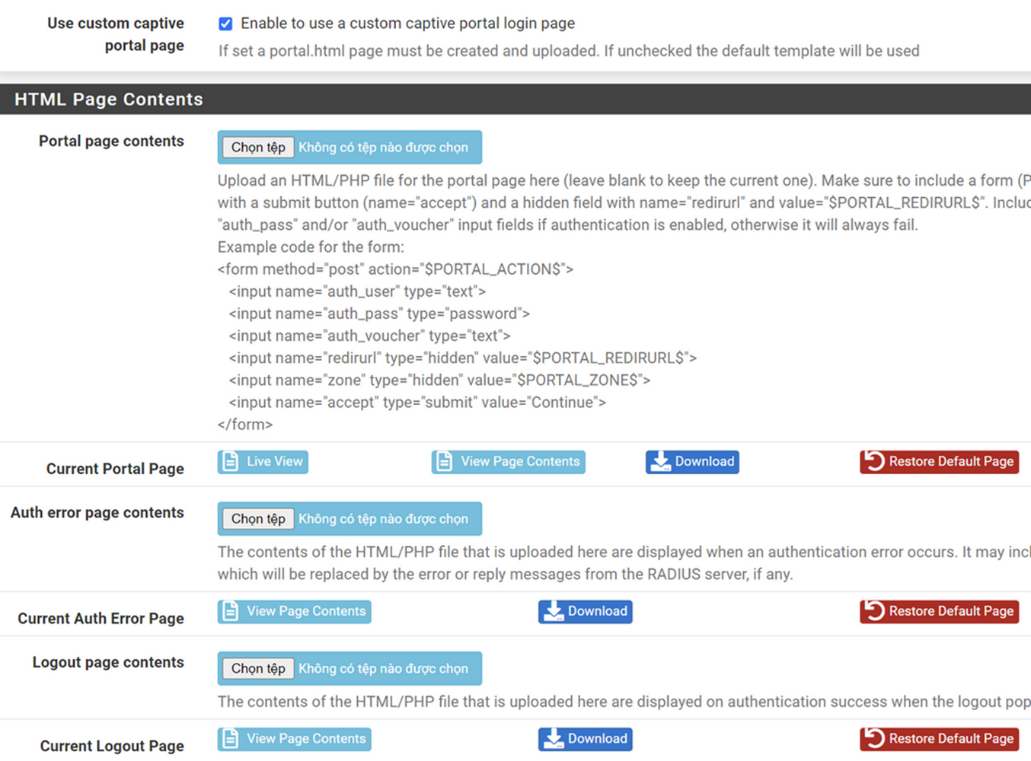


Hình 13: Cấu hình Auth Server on pfsense

Bước 2: Cấu hình Captive Portal. Ở đây Captive Portal Zones của nhóm là wifi\_nhom6.



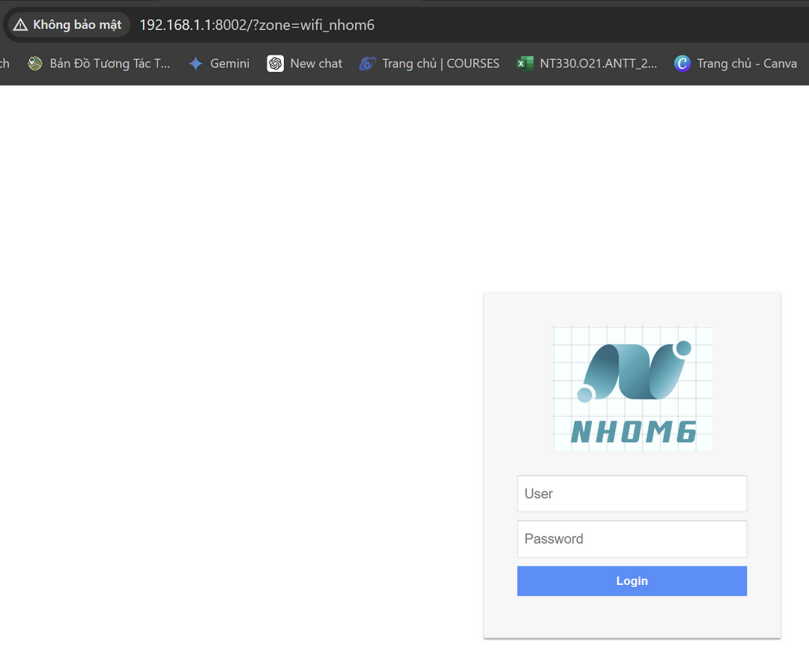
Hình 14: Cấu hình CP



Hình 15: Cấu hình CP - Sử dụng html tùy chỉnh



Hình 16: Cấu hình CP - Chọn RADIUS Server



Hình 17: Giao diện html tùy chỉnh

# 4. Thực nghiệm và Kết quả

## 4.1. Chuẩn bị

Phần cứng:

* 1 router wifi (tắt dịch vụ DHCP).
* 1 dây cáp mạng LAN.
* 1 laptop có kết nối internet.
* 1 LAN-to-USB Adaptor (nếu máy không có cổng LAN)

Phần mềm:

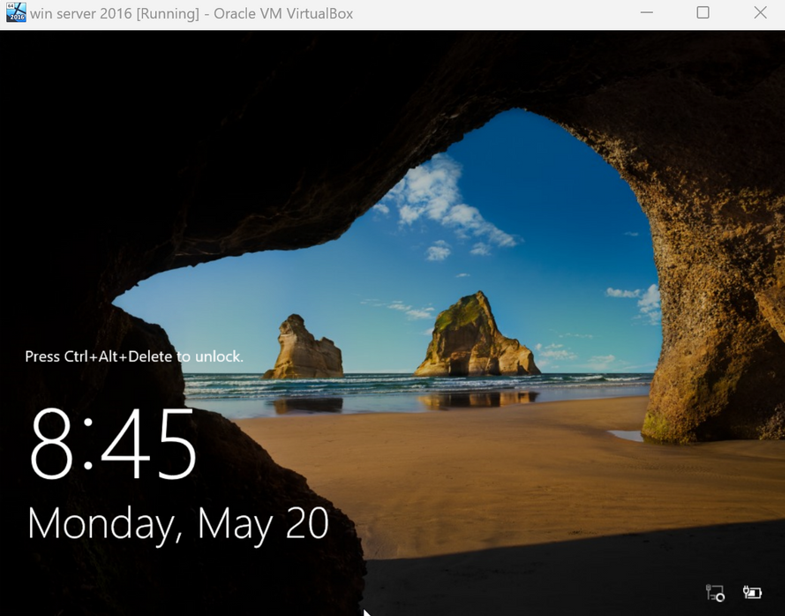
* 1 máy ảo pfsense.
* 1 máy ảo Window server 2016.
* 1 máy ảo kali linux 22.04



Hình 18: Ảnh thực tế Router Wifi



Hình 19: Máy ảo pfsense

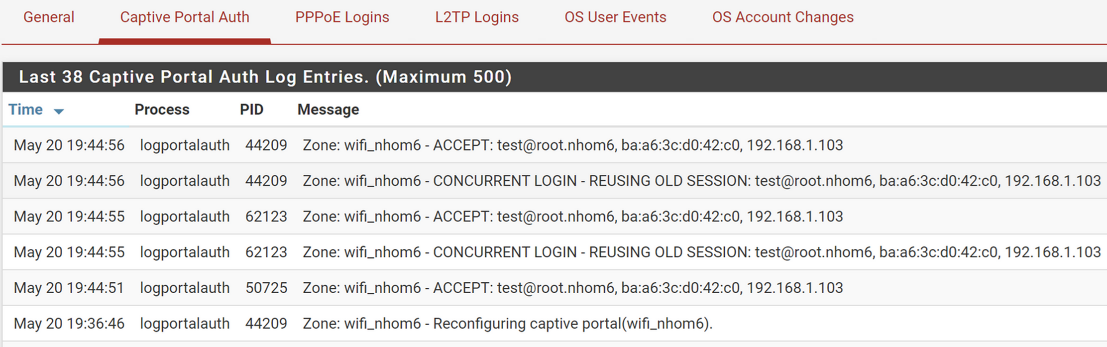


Hình 20: Máy ảo win server

## 4.2. Kết quả thực nghiệm

Triển khai thành công mô hình mạng 802.1X với Windows Server thực hiện xác thực RADIUS và lưu LDAP (dịch vụ mặc định của Windows Server khi triển khai RADIUS):

* Video demo xác thực RADIUS với Windows Server: [demo radius win server.mp4](https://drive.google.com/file/d/1KtpMXzWgZ-WDNoCYMwB7JG11yFgOv6HZ/view)



Hình 21: Log CP (RADIUS win server)

- Video demo xác thực RADIUS với kali linux: [demo freeRadius kali](https://drive.google.com/file/d/1t2TAGiJ2No8q41RQfzgdDuEzqal2jCco/view?usp=sharing)

## 4.3. Đánh giá

Mô hình mạng 802.1X với Windows Server:

* Ưu điểm: Bảo mật cao; các User được phân quyền, phân cấp, gom nhóm rõ ràng, chặt chẽ; tự triển khai LDAP không bắt buộc LDAP từ bên ngoài; có các chứng chỉ rõ ràng đáng tin cậy, có giá trị doanh nghiệp.
* Nhược điểm: Việc tạo user mất khá nhiều thời gian do yêu cầu chặt chẽ từ các chính sách bảo mật của Windows Server; bản thân tường lửa của win server đôi lúc chặn cả dịch vụ của mình; phải trải qua nhiều bước để thiết lập 1 RADIUS client và nhóm người dùng WLAN mới; LDAP mặc định của win server không phù hợp với nhu cầu triển khai lượng lơn User trong thời gian ngắn.

Mô hình mạng 802.1X với FreeRADIUS trên kali linux:

* Ưu điểm: Mã nguồn mở, miễn phí; dễ tùy chỉnh, thêm các thành phần (như web GUI, …); dễ triển khai các user với số lượng lớn nếu có danh sách trước; tạo RADIUS client dễ dàng.
* Nhược điểm: Không có sẵn các chính sách bảo mật; bảo mật không quá cao; khó tương tác. Khó cấu hình với terminal, khó tạo them liên kết với phần mềm thứ 3 (ex. LDAP)

# 5. Kết luận và Đề xuất

## 5.1. Tóm tắt kết quả nghiên cứu

Qua đề tài này nhóm đã trình bày chi tiết về giao thức RADIUS và LDAP, cũng như cách thức triển khai và kết hợp hai giao thức này để cung cấp dịch vụ xác thực và ủy quyền người dùng trong mạng không dây. Qua quá trình nghiên cứu và triển khai, nhóm đã đạt được các mục tiêu chính:

* Hiểu rõ nguyên lý hoạt động và giao thức của RADIUS và LDAP.
* Xây dựng và cấu hình mô hình mạng 802.1X với RADIUS chạy trên Windows và linux, tuy nhiên vẫn chưa thành công với lưu trữ LDAP ngoài RADIUS server.
* Đánh giá hiệu quả, lợi ích và hạn chế của hệ thống.

Các bước triển khai cụ thể bao gồm cấu hình RADIUS Server trên hệ điều hành Windows và linux, cấu hình pfsense để kết nối đến RADIUS Server, và cấu hình Proxy Server sử dụng xác thực LDAP. Nhóm đã thực hiện các thử nghiệm và đánh giá hiệu suất, bảo mật và khả năng mở rộng của hệ thống, qua đó rút ra được các kết luận quan trọng và bài học kinh nghiệm.

## 5.2. Thách thức và hạn chế

Thách thức:

* Phức tạp trong cấu hình và triển khai: Quá trình cấu hình RADIUS và LDAP yêu cầu sự hiểu biết sâu rộng về các giao thức mạng, bảo mật, và cách thức hoạt động của các dịch vụ liên quan. Việc này đòi hỏi nhiều thời gian và công sức để đảm bảo hệ thống hoạt động đúng và hiệu quả.
* Khả năng tương thích: Một trong những thách thức lớn là đảm bảo tính tương thích giữa các thiết bị và phần mềm khác nhau khi triển khai hệ thống. Đặc biệt là khi sử dụng các thiết bị Access Point và Wi-Fi controllers từ nhiều nhà cung cấp khác nhau.
* Bảo mật và hiệu suất: Bảo mật là một vấn đề quan trọng cần được chú trọng, đặc biệt là khi xử lý thông tin xác thực của người dùng. Đồng thời, đảm bảo hiệu suất của hệ thống trong các mạng lớn với số lượng yêu cầu xác thực đồng thời lớn cũng là một thách thức không nhỏ.

Hạn chế:

* Giới hạn về thời gian và nguồn lực: Do hạn chế về thời gian và nguồn lực, nhóm chỉ tập trung vào cấu hình cơ bản và thử nghiệm trên một số mô hình nhất định. Điều này có thể không phản ánh hết được các tình huống và kịch bản thực tế.
* Khả năng mở rộng: Mặc dù hệ thống có thể mở rộng, việc triển khai trong các mạng lớn hoặc phân tán vẫn còn nhiều thách thức cần giải quyết, như tối ưu hóa hiệu suất và quản lý thông tin xác thực tập trung.
* Thiếu tính năng tự động hóa: Quá trình cấu hình và quản lý hệ thống còn phụ thuộc nhiều vào các thao tác thủ công, thiếu các công cụ và giải pháp tự động hóa để giảm thiểu sai sót và tăng hiệu quả quản lý.

## 5.3. Đề xuất cho nghiên cứu tương lai

Tối ưu hóa hiệu năng và bảo mật của RADIUS:

* Hiệu năng: Nghiên cứu các phương pháp cải thiện tốc độ phản hồi của máy chủ RADIUS trong các mô hình mạng phân tán, đặc biệt là khi phải xử lý số lượng lớn yêu cầu xác thực đồng thời.

Phát triển và ứng dụng công nghệ mới:

* Machine Learning và AI: Áp dụng machine learning và AI để phát hiện và ngăn chặn các hành vi bất thường hoặc tiềm ẩn nguy cơ trong mạng không dây. Điều này có thể giúp cải thiện khả năng bảo mật tổng thể của mạng.

Khả năng ứng dụng và mở rộng giải pháp trong các môi trường doanh nghiệp lớn với nhiều chi nhánh:

* Mô hình phân tán: Áp dụng các mô hình phân tán với các máy chủ RADIUS tại mỗi chi nhánh, nhưng vẫn duy trì một cơ sở dữ liệu LDAP tập trung để quản lý xác thực. Điều này giúp cải thiện hiệu suất và đảm bảo tính khả dụng cao khi có sự cố mạng WAN​​.
* Caching: Sử dụng cơ chế caching của RADIUS để lưu trữ tạm thời thông tin xác thực, giúp người dùng vẫn có thể truy cập mạng ngay cả khi kết nối WAN gặp sự cố​​.

# 6. Tài liệu tham khảo

* Sách CWSP: Coleman, D., Westcott, D., & Harkins, B. (2016). CWSP, 2nd Edition. Sybex.
* Hướng dẫn cấu hình pfsense xác thực RADIUS: <https://www.youtube.com/watch?v=A0rAasVhkvY>
* Hướng dẫn cấu hình win server xác thực RADIUS: <https://www.youtube.com/watch?v=oOmIOG1eu3w&t=1078s>
* Thiết kế trang đăng nhập Captive Portal: <https://github.com/felixhaeberle/pfsense-captive-portal>