**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ THÀNH PHỐ HỒ CHÍ MINH**

**Khoa Công Nghệ Thông Tin 2**

**AN TOÀN MẠNG**



**BÀI BÁO CÁO**

**ĐỀ TÀI: CAPTIVE PORTAL**

**Giảng viên: ThS. Trần Thị Dung**

**Sinh viên thực hiện:**

**Nguyễn Tuấn Kiệt N18DCAT035**

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

LỚP: POLI1100109

NHÓM 7

GV HƯỚNG DẪN: ĐỖ THỊ THÚY YẾN

Thành phố Hồ Chí Minh – Năm 2021

# MỤC LỤC

[MỤC LỤC 2](#_Toc86246435)

[I. Cơ Sở Lý Thuyết 3](#_Toc86246436)

[A. Pfsense 3](#_Toc86246437)

[B. Tính Năng Pfsense 3](#_Toc86246438)

[1. Pfsense Aliases 3](#_Toc86246439)

[2. NAT 3](#_Toc86246440)

[3. Firewall Rules 4](#_Toc86246441)

[4. Firewall Schdules 4](#_Toc86246442)

[5. Traffic Sharper 4](#_Toc86246443)

[6. Virtual IPS 4](#_Toc86246444)

[C. Một số dịch vụ Pfsense 5](#_Toc86246445)

[1. Captive Portal 5](#_Toc86246446)

[2. Các dịch vụ khác 6](#_Toc86246447)

[II. Nội dung bài lab 6](#_Toc86246448)

[A. Chuẩn bị 6](#_Toc86246449)

[B. Thực hiện 8](#_Toc86246450)

[1. Thiết lập Pfsense có 3 card mạng. 8](#_Toc86246451)

[2. Cấu hình từng interface cho pfsense 9](#_Toc86246452)

[3. Cấu hình các thông tin cơ bản bằng web config 10](#_Toc86246453)

[4. Cấu hình Interface WIFI để thực hiện Captive Portal 15](#_Toc86246454)

[5. Thiết lập Firewall Rules cho interface WIFI. 16](#_Toc86246455)

[6. Thiết lập captive portal. 20](#_Toc86246456)

[7. Phần Cơ Bản 22](#_Toc86246457)

[8. Phần Nâng Cao (Vouchers) 23](#_Toc86246458)

[9. Phân Nâng Cao (Authentication dùng Raidus Server) 28](#_Toc86246459)

[III. Tài Liệu Tham Khảo. 34](#_Toc86246460)

# PHẦN I. Cơ Sở Lý Thuyết

## Pfsense

* Một cách ngắn gọn PfSense là một ứng dụng có chức năng định tuyến và tường lửa mạnh mà miễn phí, ứng dụng này sẽ cho phép mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật.
* Đây là một dự án bảo mật tập trung vào các hệ thống nhúng, pfSense được sử dụng để bảo vệ các mạng ở tất cả kích cỡ, từ các mạng gia đình đến các mạng lớn của của các công ty.

## Tính Năng Pfsense

### Pfsense Aliases

Một Aliases ngăn cho phép sử dụng cho một host, công hoặc mạng có thể được sử dụng khi tạo các rules trong pfSense. Sử dụng Aliases sẽ giúp cho phép lưu trữ nhiều mục trong một nơi duy nhất có nghĩa là không cần tạo ra nhiều rules cho nhóm các máy hoặc cổng.

### NAT

PfSense cung cấp network address translation (NAT) và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng này vẫn còn một số hạn chế với Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE) và Session Initiation Protocol (SIP) khi sử dụng NAT.

Trong Firewall có thể cấu hình các thiết lập NAT nếu cần sử dụng công chuyên tiếp cho các dịch vụ hoặc cấu hình NAT tĩnh (1:1) cho các host cụ thể. Thiết lập mặc định của NAT cho các kết nối outbound là automatic/dynamic, tuy nhiên có thể thay đổi kiểu manual nếu cần.

### Firewall Rules

Nơi lưu các rules của Firewall. Để vào Rules của pfsense vào Firewall – Rules. Mặc định pfsense cho phép mọi trafic ra vào hệ thống, chúng ta phải tạo ra các rules để quản lí mạng bên trong firewall.

### Firewall Schdules

Các Firewall rules có thể được sắp xếp để nó có chỉ hoạt động vào các thời điểm nhất định trong ngày hoặc vào những ngày nhất định cụ thể hoặc các ngày trong tuần.

Ví dụ: Tạo lịch tên GioLamViec của tháng 12 từ thứ hai đến thứ 7 và thời gian từ 8 giờ tới 17 giờ.

### Traffic Sharper

Traffic Sharper giúp theo dõi và quản lý băng thông mạng dễ dàng và hiệu quả hơn Traffic Shaping là phương pháp tối ưu hóa kết nối Internet. Nó tăng tối đa tốc độ trong khỉ đảm bảo tối thiểu thời gian trễ Khi sử dụng những gói dữ liệu ACK được sắp xếp thứ tự ưu tiên trong đường truyền tải lên, điều này cho phép tiến trình tải về được tiếp tục với tốc độ tối đa.

Quản lí băng thông của một số ứng dụng khác như Remote Service VPN, Messengers, Web, Mail, Miscellaneous

### Virtual IPS

Một Virtual IPS có thể sử dụng bất kỳ địa chỉ IP của pfSense, đó không phải là một địa chỉ IP chính. Trong các tình huống khác nhau, mỗi trong số đó có các tính năng riêng của nó. Virtual IP được sử dụng để cho phép pfSense đúng cách chuyển tiếp lưu lượng cho những việc như chuyển tiếp công NAT, NAT Outbound và NAT 1:1. Họ cũng cho phép các tính năng như failover, và có thể cho phép các dịch vụ trên router để gắn kết với địa chỉ IP khác nhau.

## Một số dịch vụ Pfsense

### Captive Portal

Đây là dịch vụ mà nhóm sẽ thực hiện chính trong bài Lab này, Captive portal là 1 tính năng thuộc dạng flexible, chỉ có trên các thiết bị firewall thương mại lớn, tuy nhiên trên Pfsense tính năng này được cung cấp miễn phí. Tính năng này giúp chuyển hướng trình duyệt của người dùng vào 1 trang web định sẵn, từ đó giúp chúng ta có thể quản lý được người dùng. Tính năng này tiên tiến hơn các kiểu đăng nhập như WPA, WPA2 ở chỗ người dùng sẽ thao tác trực tiếp với 1 trang web (http, https) chứ không phải là bảng đăng nhập khô khan như kiểu authentication WPA, WPA2.

Dịch vụ Captive Portal của Pfsense có các chức năng sau:

* Pass-though MAC: Các MAC address được cấu hình trong mục này sẽ được bỏ qua, không authentication.
* Allowed IP addres: Các IP address được cấu hình sẽ không authentication.
* Users: Tạo local user để dùng kiểu authentication: local user.
* File Manager: Upload trang quản lý của Captive portal lên pfsense.
* Enable captive portal: Đánh dấu chọn nếu muốn sử dụng captive portal.
* Maximum concurrent connections: Giới hạn các connection trên mối ip/user/mac.
* Idle timeout:Nêu mối ip không còn truy cập mạng trong 1 thời gian xác định thì sẽ ngắt kết nối của ip/user/mac.
* Hard timeout: Giới hạn thời gian kết nối của mối ip/users/mac.
* Logout popup windows: Xuất hiện 1 popup thông báo cho ip/users/mac.
* Redirect URL: Địa chỉ URL mà người dùng sẽ được direct tới sau khi đăng nhập.
* MAC filtering: Đánh dấu vào nếu pfsense năm trước router. Bởi vì pfsense quản lý kết nối theo MAC (mặc định). Mà chi dữ liệu qua Router sẽ bị thay đổi mac address nên nếu timeout thì toàn bộ người dùng sẽ mất kết nối
* Authentication: Chọn kiểu chứng thực khi kết nối vào mạng. Pfsense hỗ trợ 3 kiểu:
* No authentication: pfsense sẽ điều hướng người dùng tới 1 trang nhất định mà không chứng thực.
* Local user manager: pfsense hỗ trợ tạo user để chứng thực.
* Radius authentication: Chứng thực bằng radius server (Cần chỉ ra địa chỉ ip của radius, port, ...).

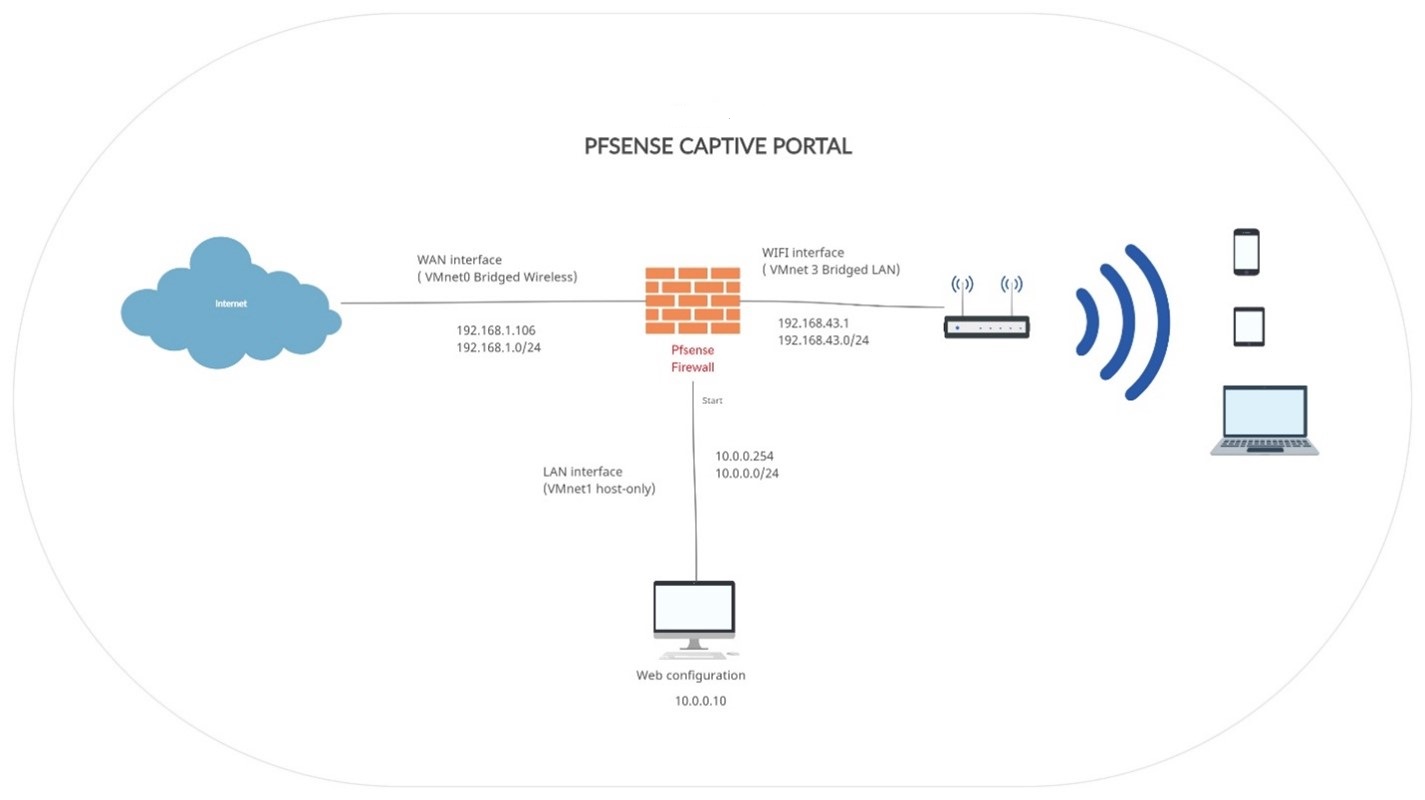
### Các dịch vụ khác

* + DHCP Server.
  + Load Balance.
  + VPN trên Pfsense.
  + VPN PPTP.
  + Open VNP Site to Site.

# PHẦN II. Nội dung bài lab

## Chuẩn bị

* 1 máy cài Pfsense 3 card mạng.
* 1 máy client win 10
* File ISO cài Pfsense.



Card 1: Kết nối wifi ra ngoài Internet (Vmnet0)

IP: 192.168.1.106 – 192.168.1.0/24

Card 2: Kết nối đến mạng lan để cấu hình Pfsense(Vmnet1)

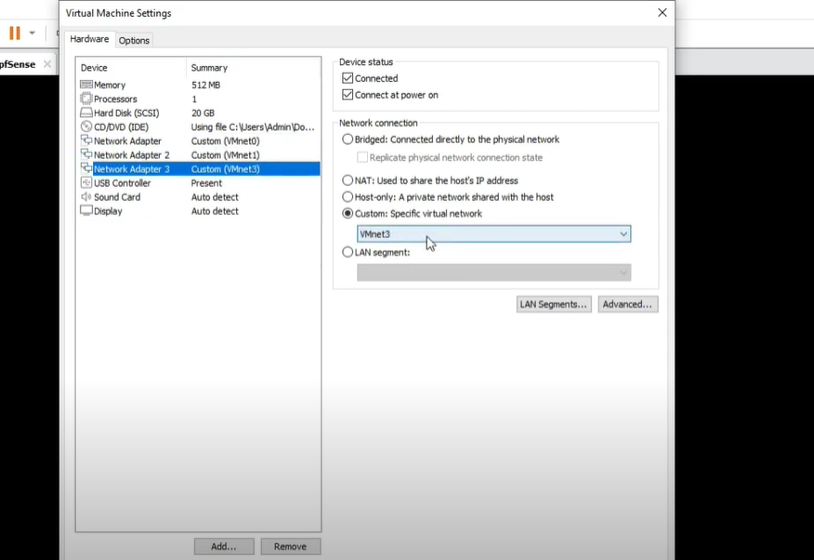
IP: 10.0.0.254 – 10.0.0.0/24

Card 3: Kết nối tới AccessPoint để phát Wifi cho máy khác kết nối tới(Vmnet3)

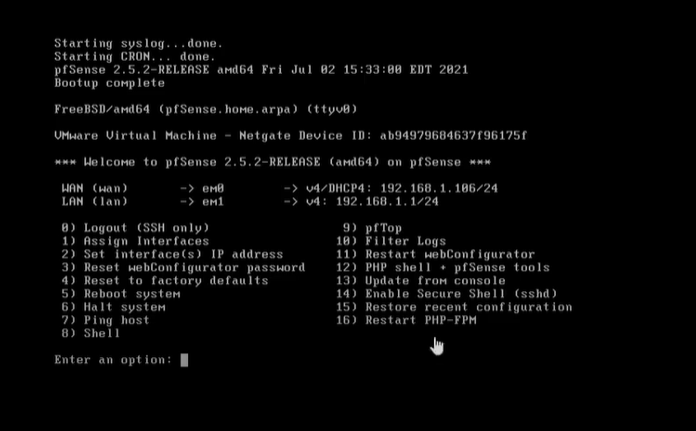
IP: 192.168.43.1 – 192.168.43.0/24

## Thực hiện

### Thiết lập Pfsense có 3 card mạng.



### Cấu hình từng interface cho pfsense

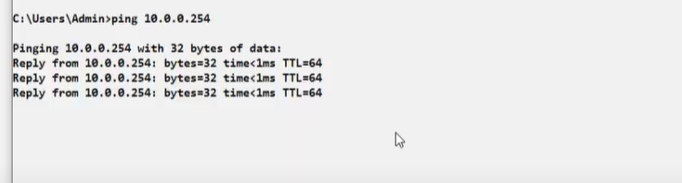


Cài IP cho Lan 10.0.0.254



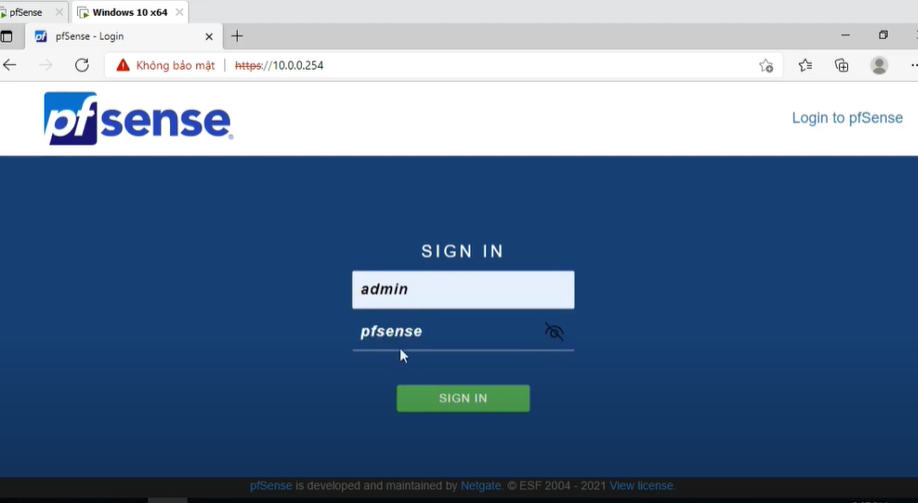
### Cấu hình các thông tin cơ bản bằng web config

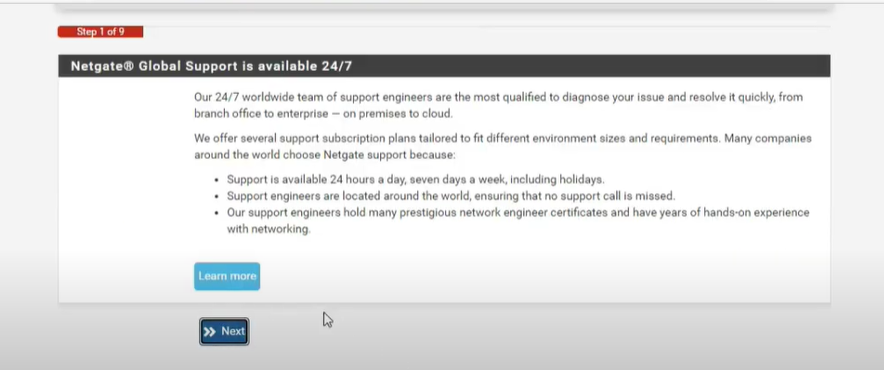
Máy Client win 10 sử dụng card Vmnet 1.



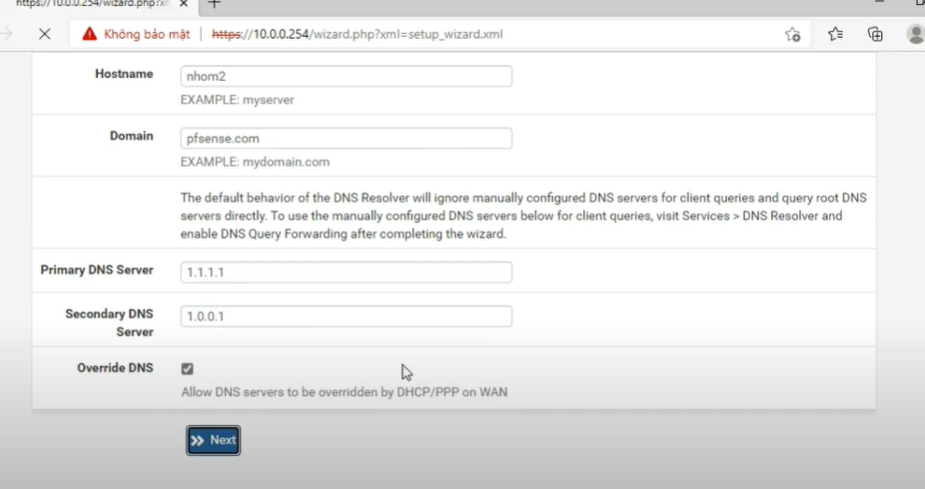
Truy cập vào Pfsense với địa chỉ 10.0.0.254 trên máy Clinet

Với user: admin và password: pfsense

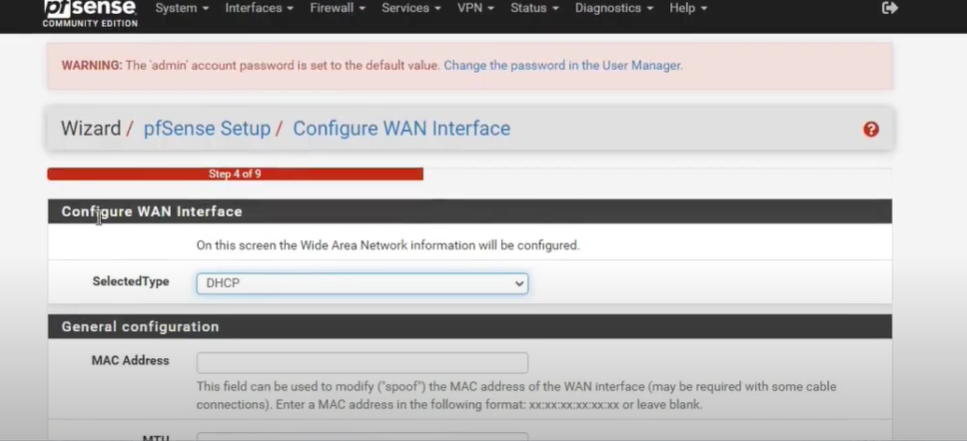




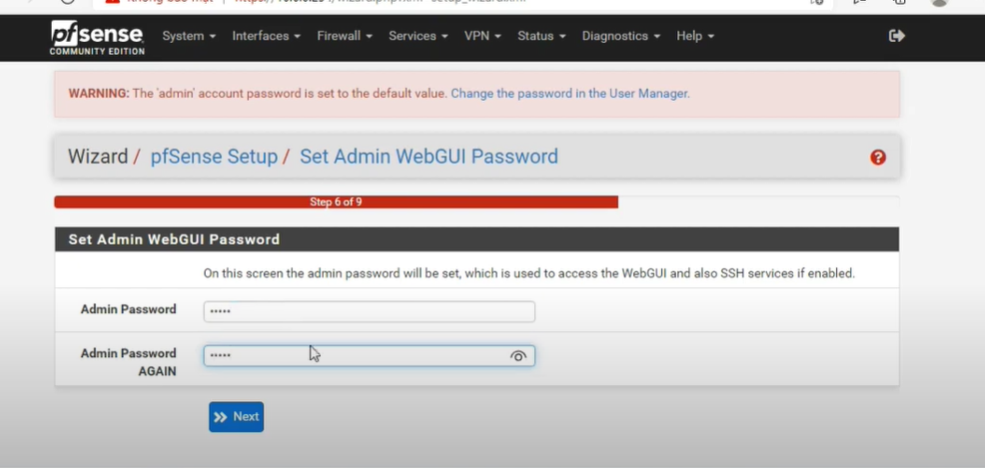
Đặt hostname và domain.



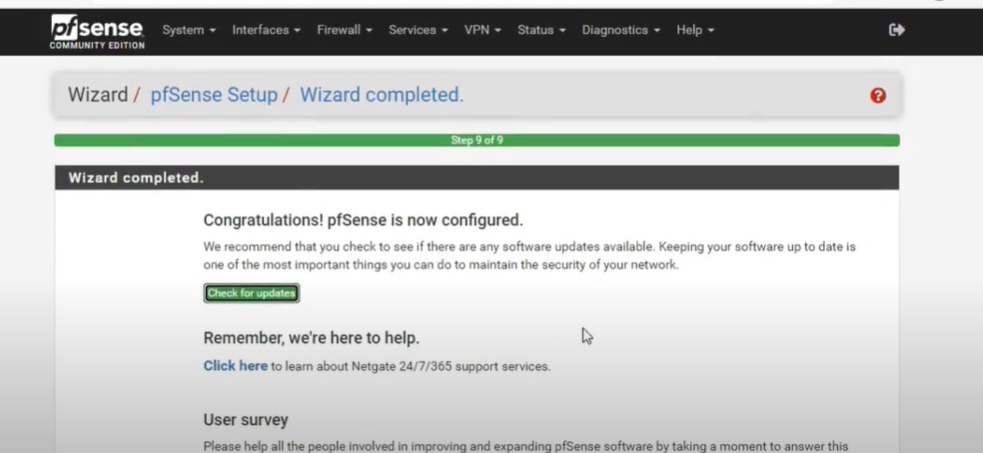




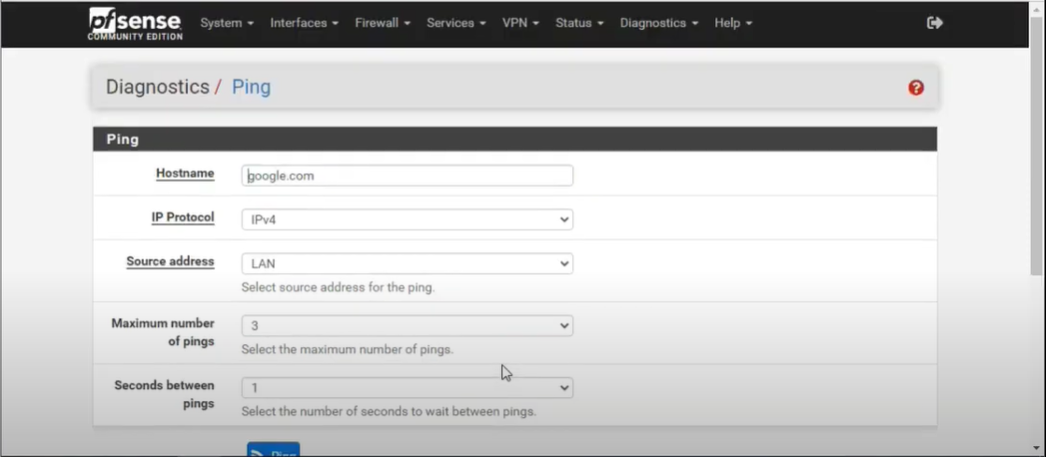


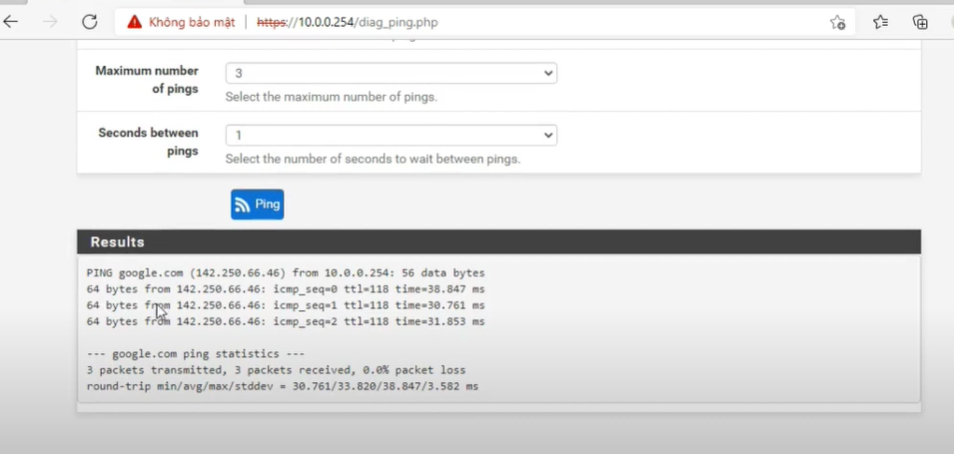


Cấu hình thành công Pfsense.



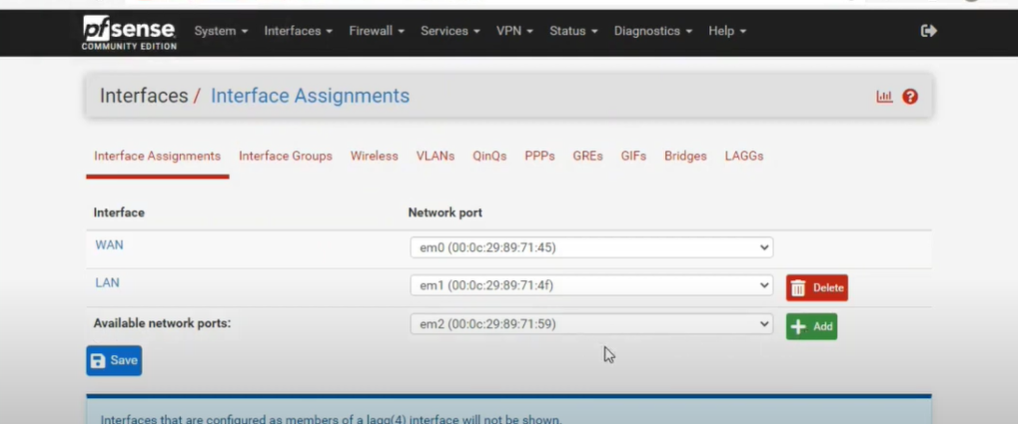
Vào Diagnostics -> Ping từ Lan tới google.com để kiểm tra kết nối internet của mạng LAN



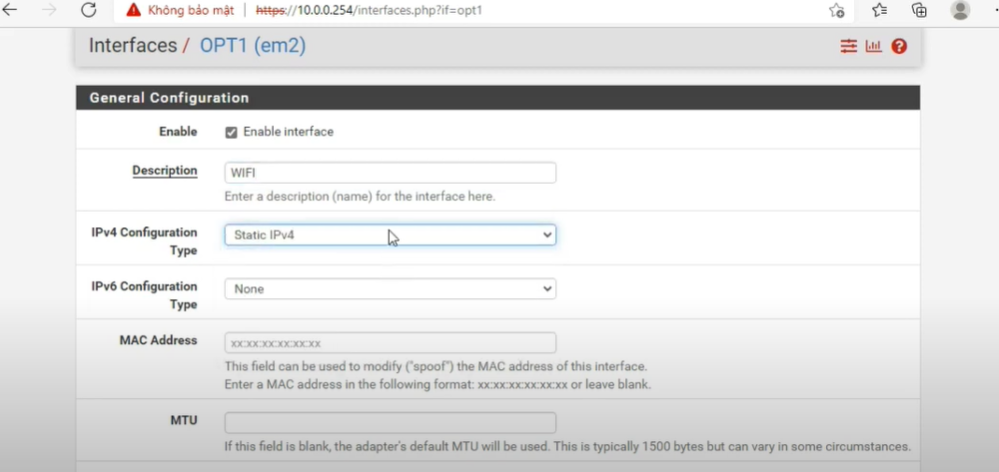


### Cấu hình Interface WIFI để thực hiện Captive Portal

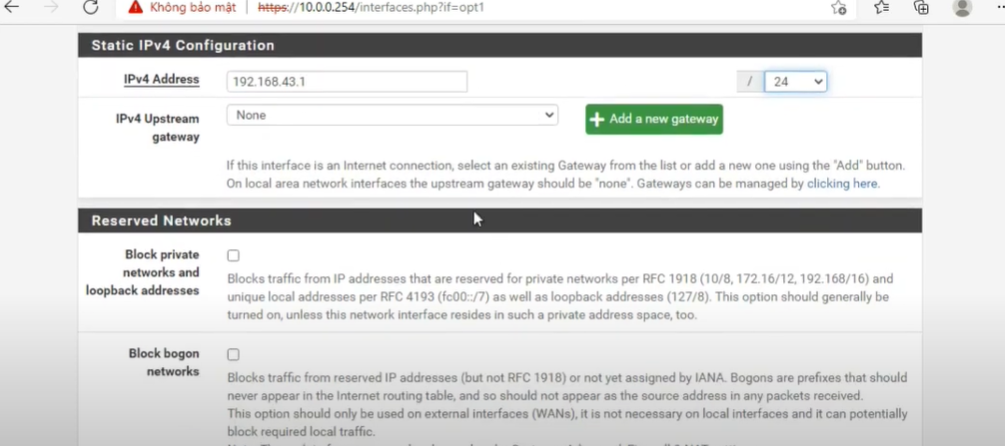
Vào Interfaces -> Assignments -> Add



Sửa OPT1 -> WIFI và chọn Static IPv4.

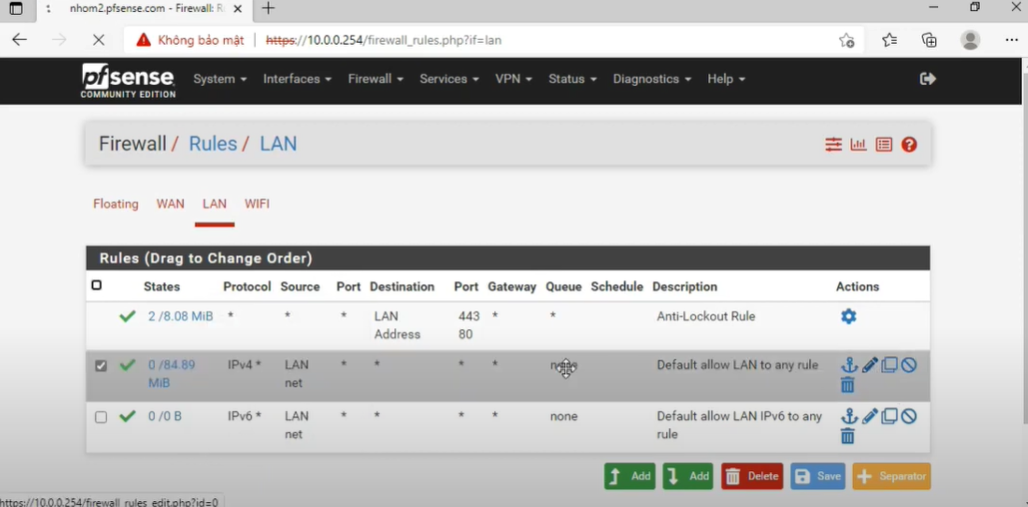


Đặt IP 192.168.43.1 /24, Sau đó Save lại.

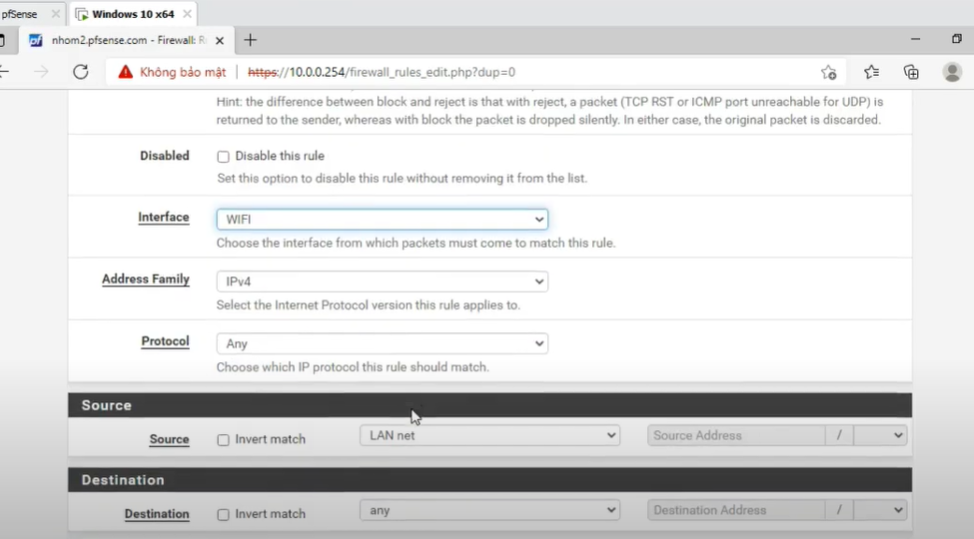


### Thiết lập Firewall Rules cho interface WIFI.

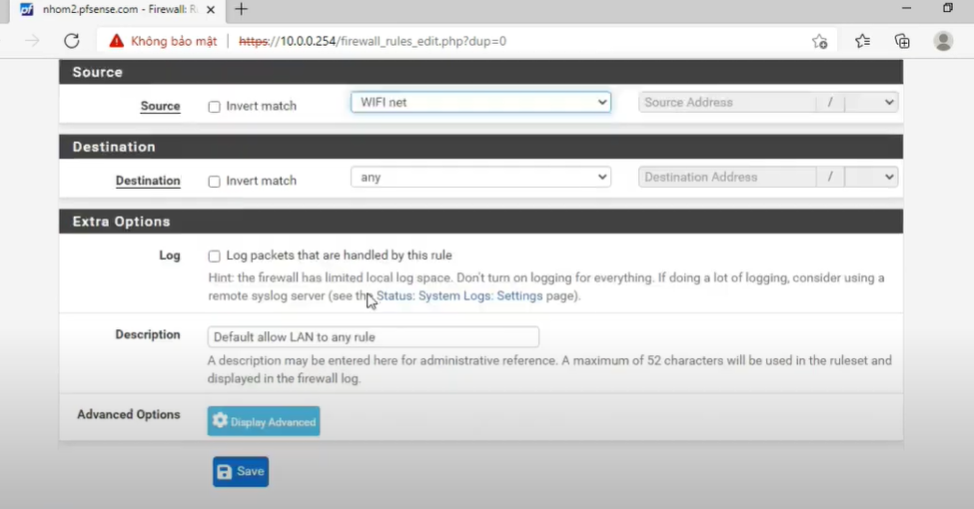
Vào Firewall -> Rules -> LAN -> chọn Copy dòng Ipv4

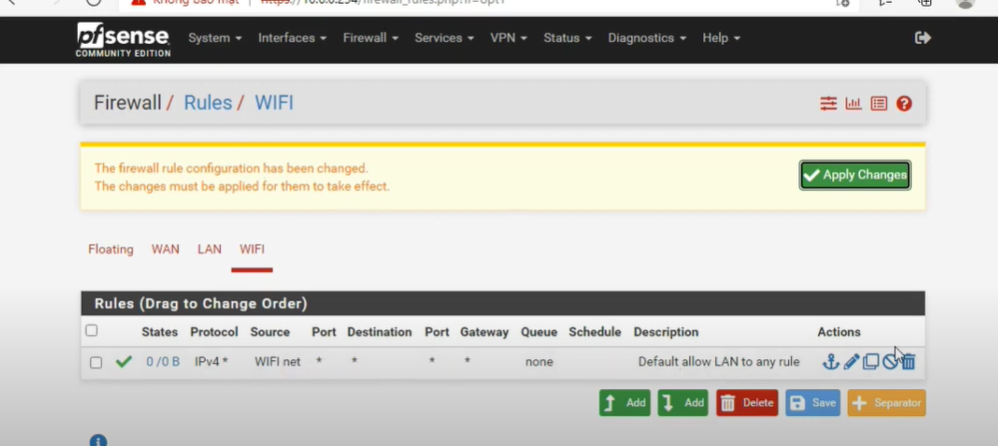


Interface chọn WIFI

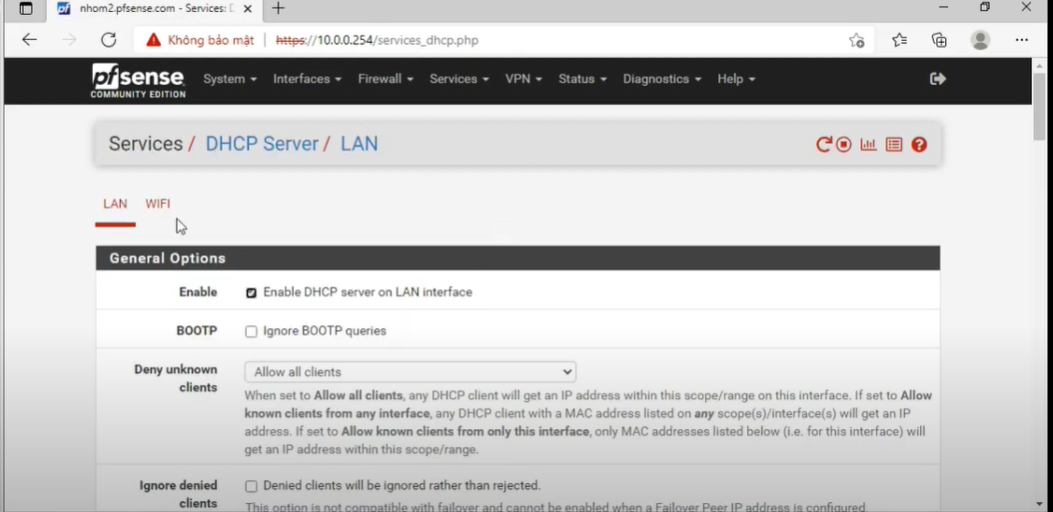


Source chọn WIFI net. Sau đó chọn Save.

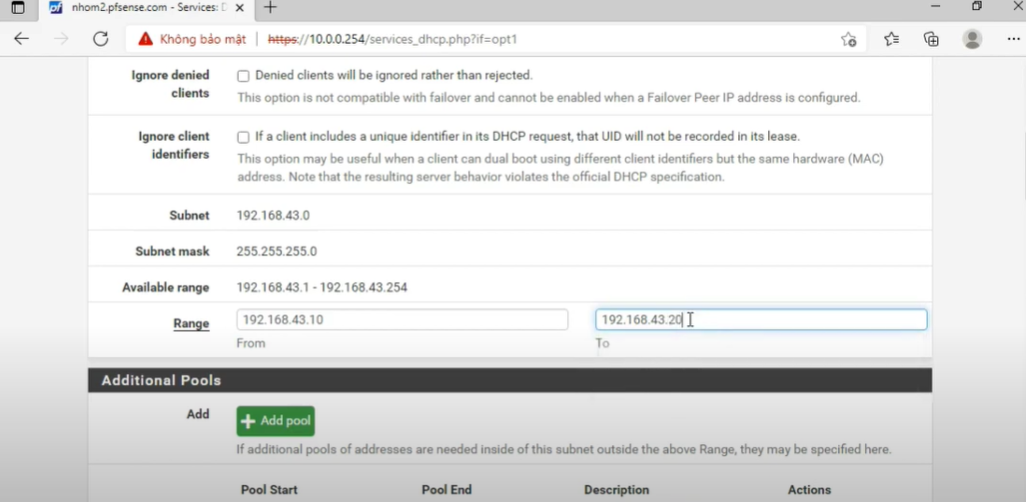




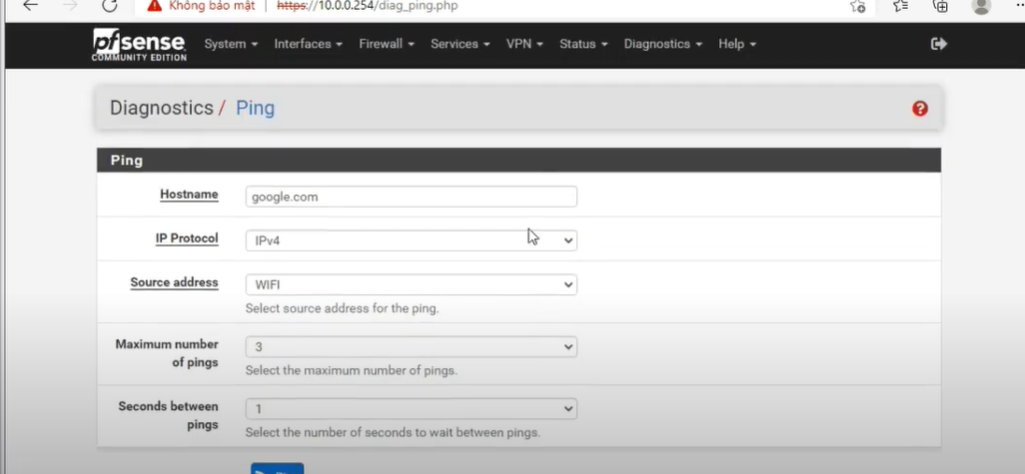
Tiếp theo vào Services -> DHCP Server -> WIFI -> Enable DHCP server

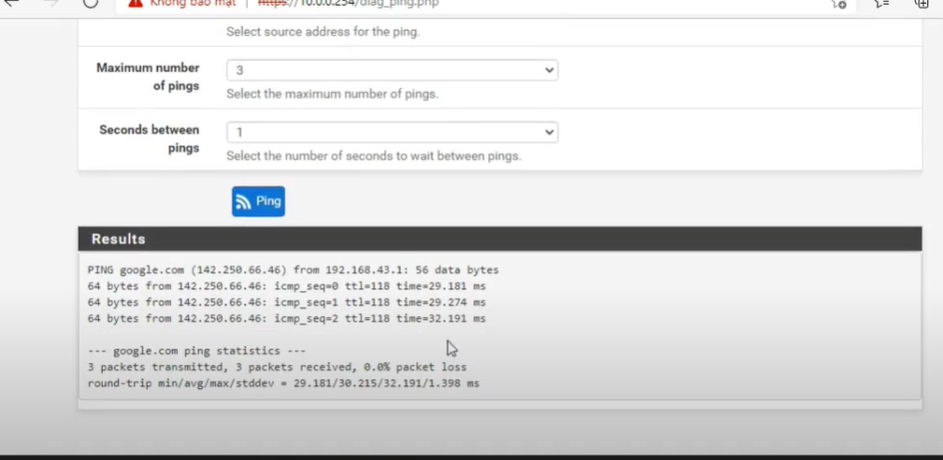


Cấp IP từ 192.168.43.10 -> 192.168.43.20



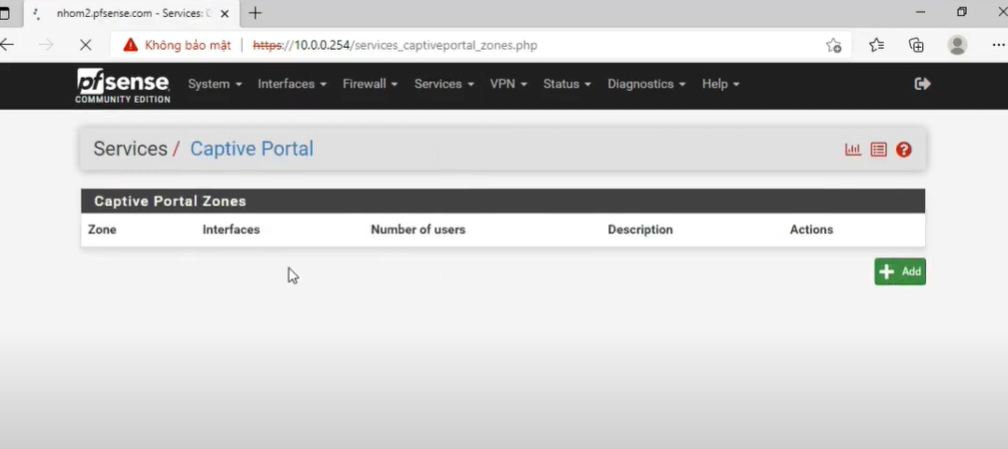
Diagnostics -> Ping từ WIFI tới google.com



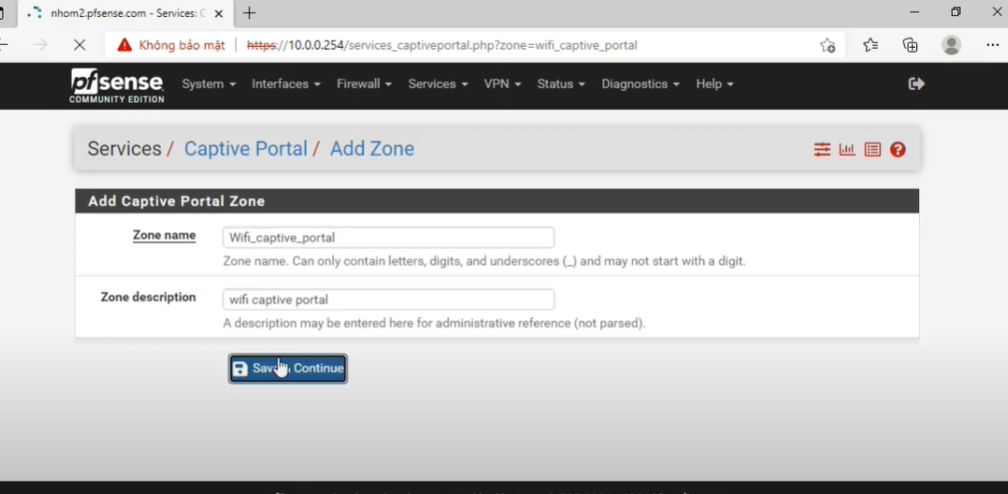


### Thiết lập captive portal.

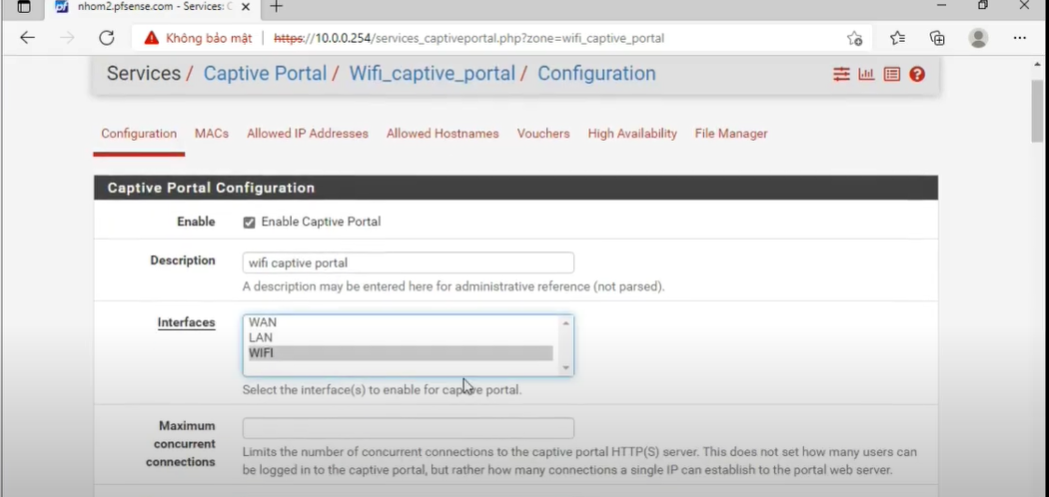
Vào Services -> Captive Portal -> Add



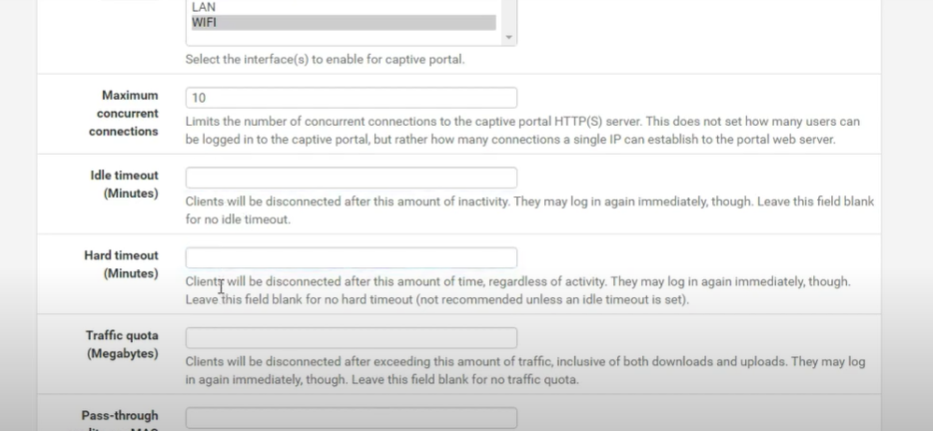
Đặt Zone name và Zone description. Sau đó chọn Save.



Enable Captive Portal và Interface chọn WIFI.

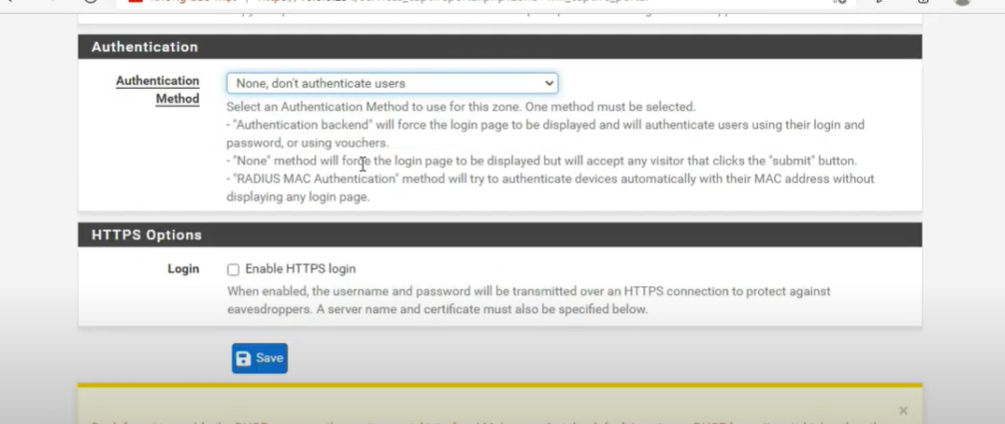


Cho tối đa 10 kết nối cùng lúc.

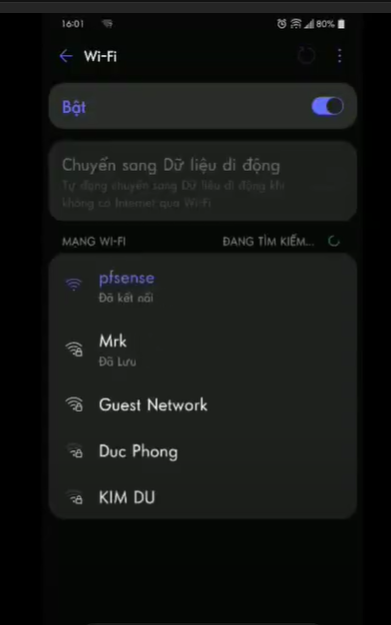
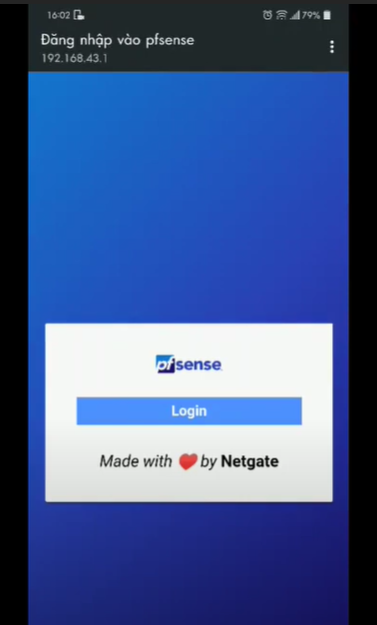
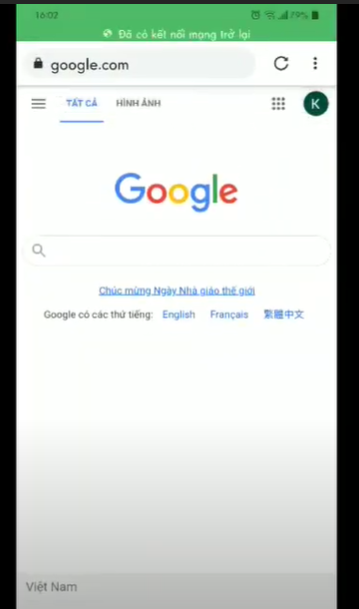


### Phần Cơ Bản

Authentication Method chọn None, don’t authentication users. Sau đó chọn Save.

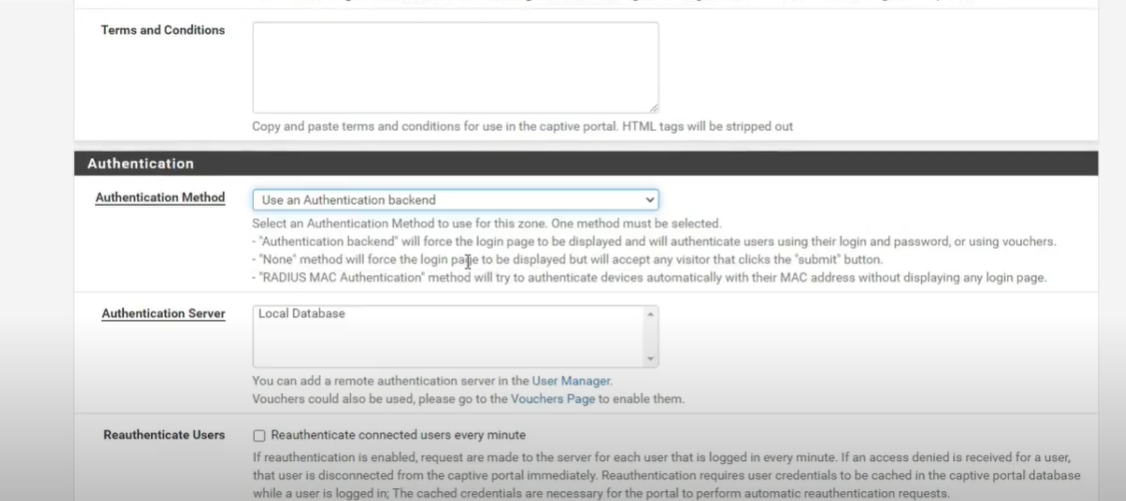


Kết nối trên điện thoại kiểm tra

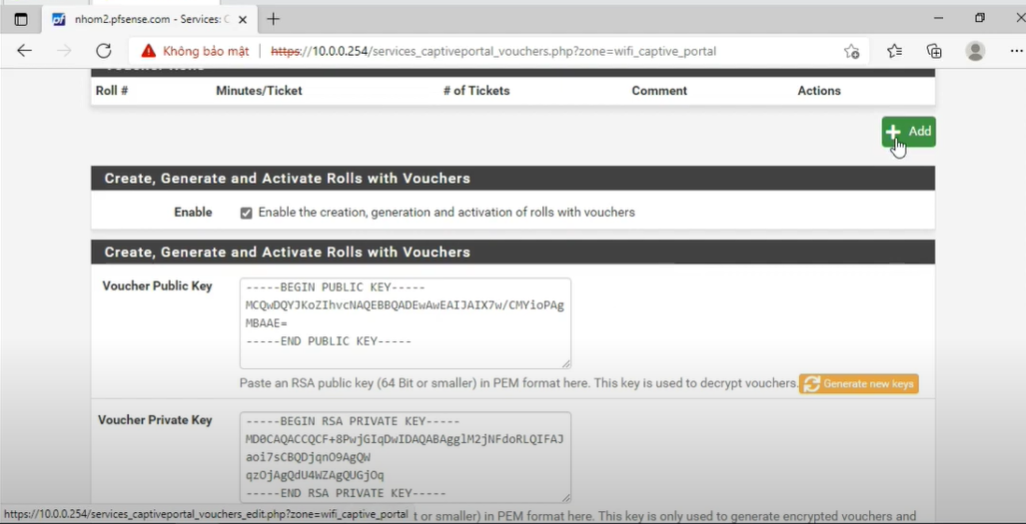


### Phần Nâng Cao (Vouchers)

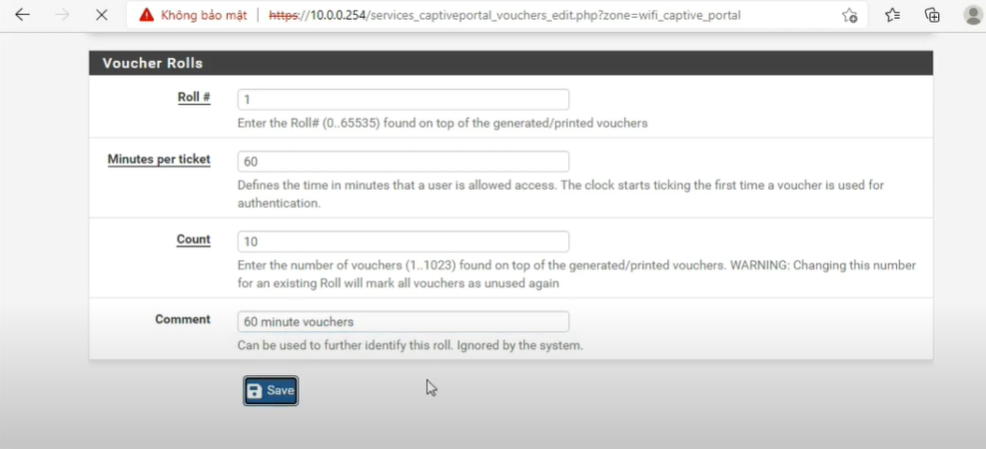
Authentication Method chọn User an Authentication backend. Sau đó chọn Save.



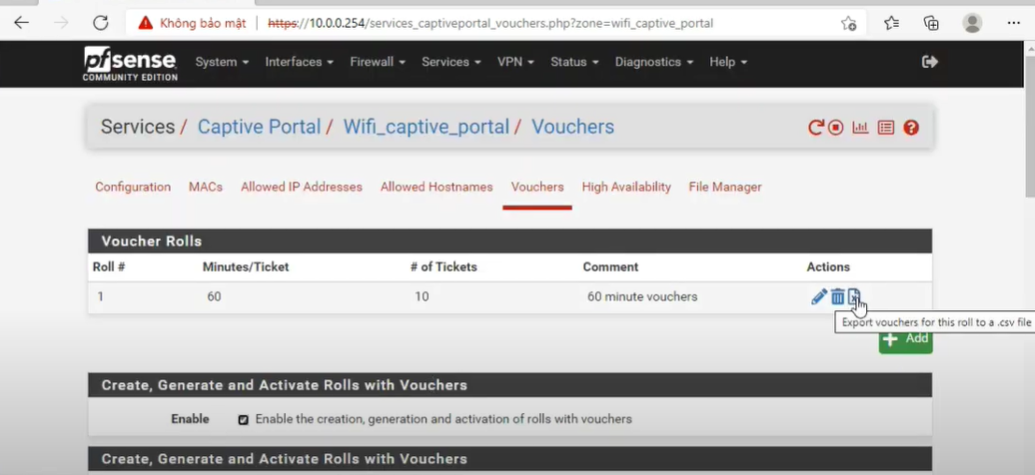
Chọn Vouchers > Chọn Generate new keys > Chọn Add.

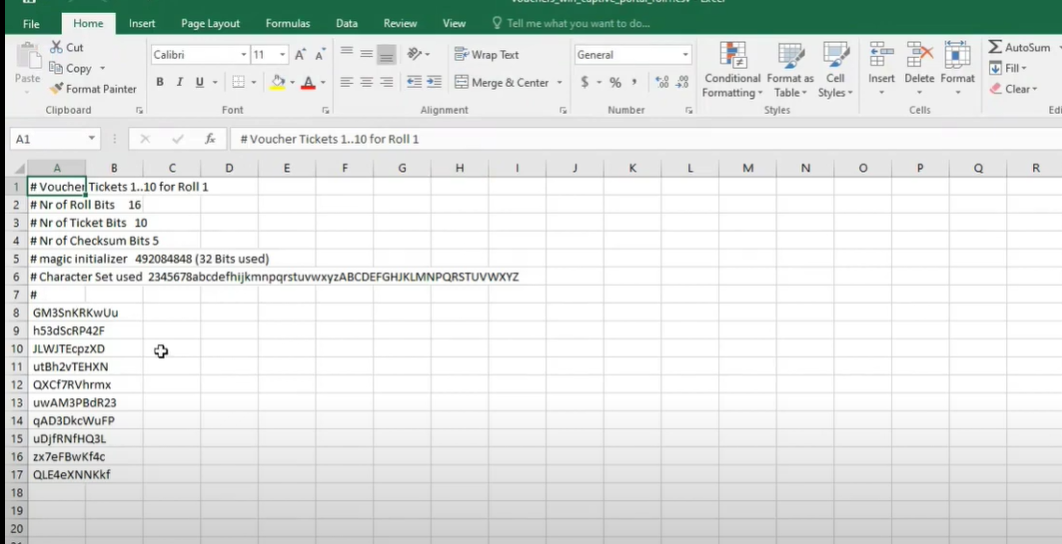


Tạo 10 Voucher có thời gian sử dụng là 60 phút. Sau đó chọn Save.

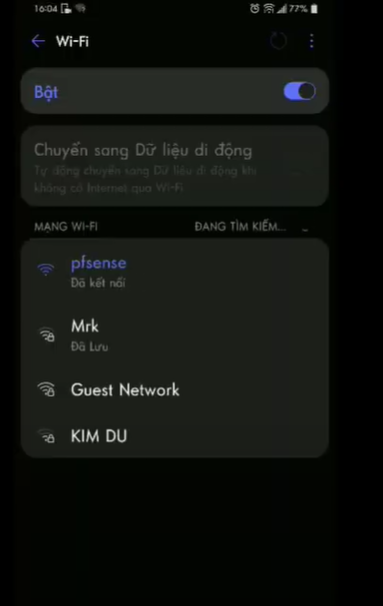
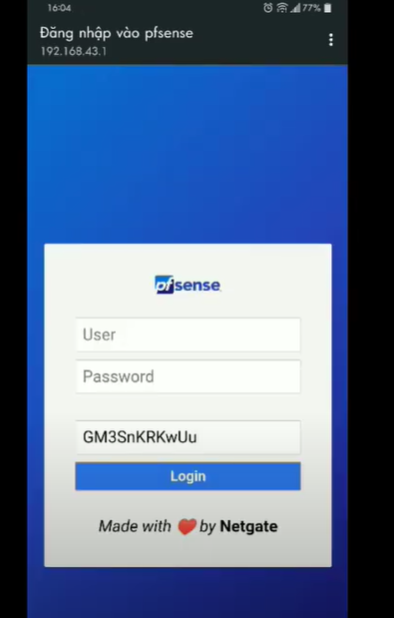
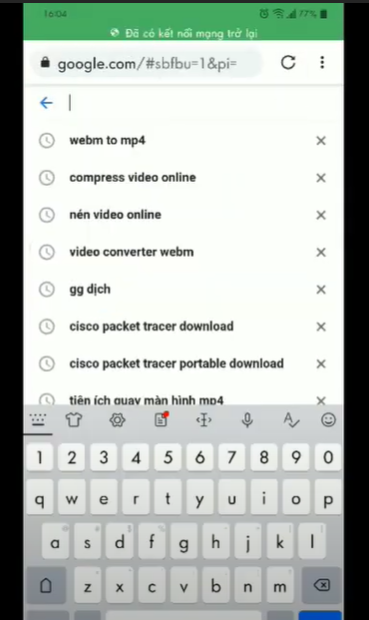


Sau đó xuất Voucher ra.



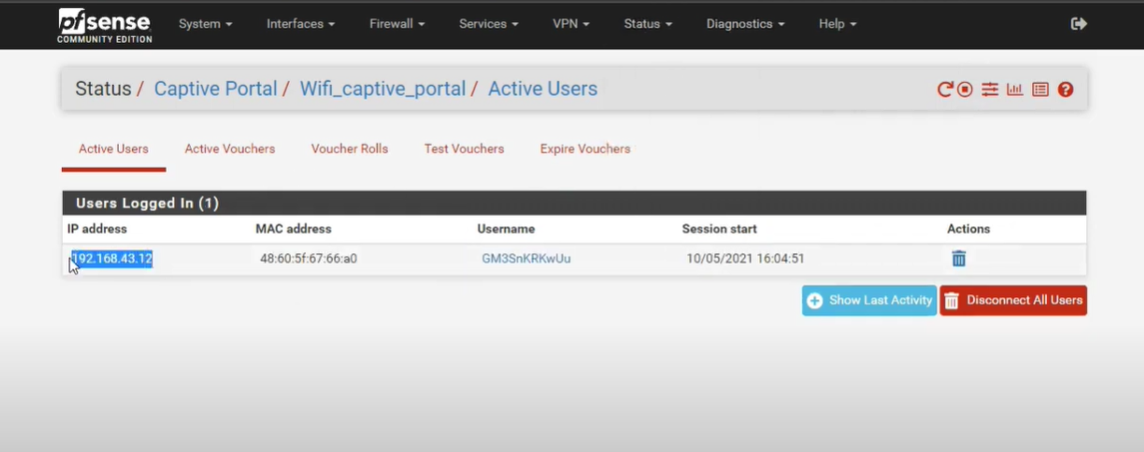


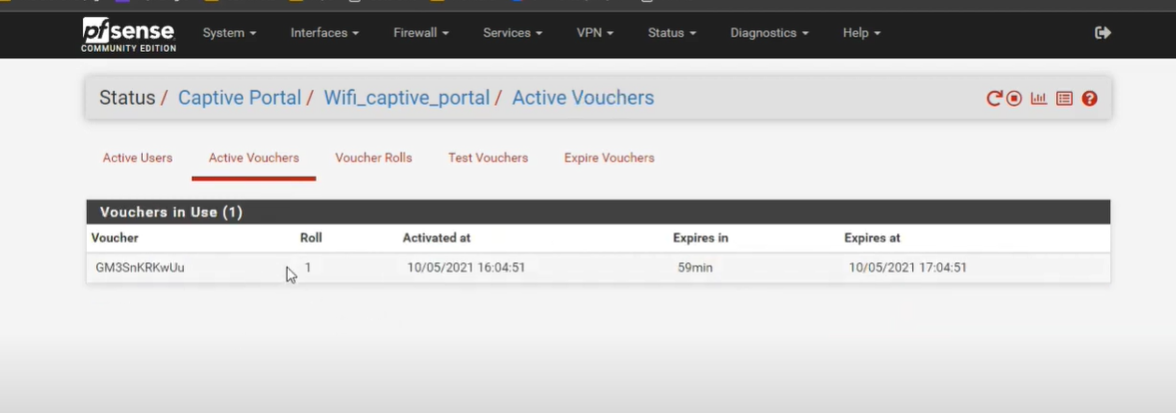
Kết nối.

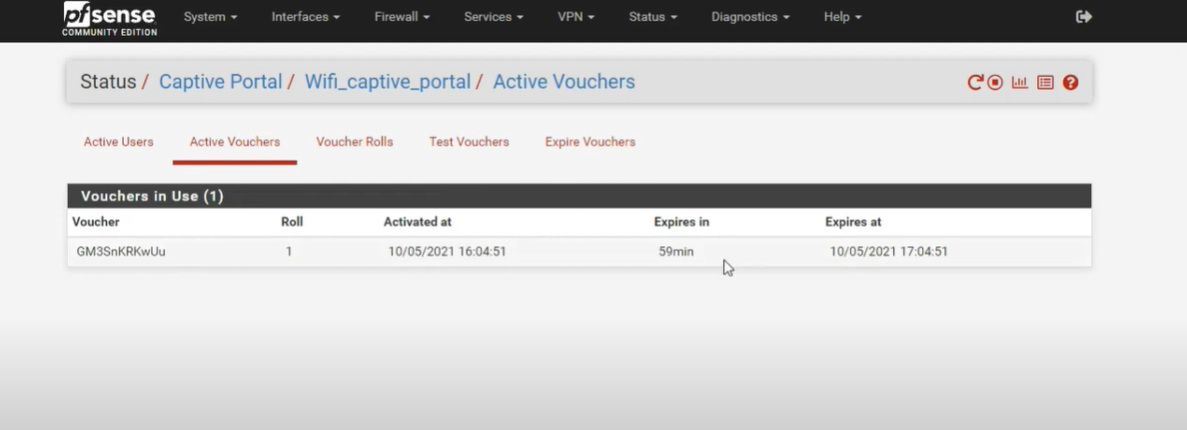


Quản lí các thiết bị kết nối.

Vào Status -> Captive Portal.



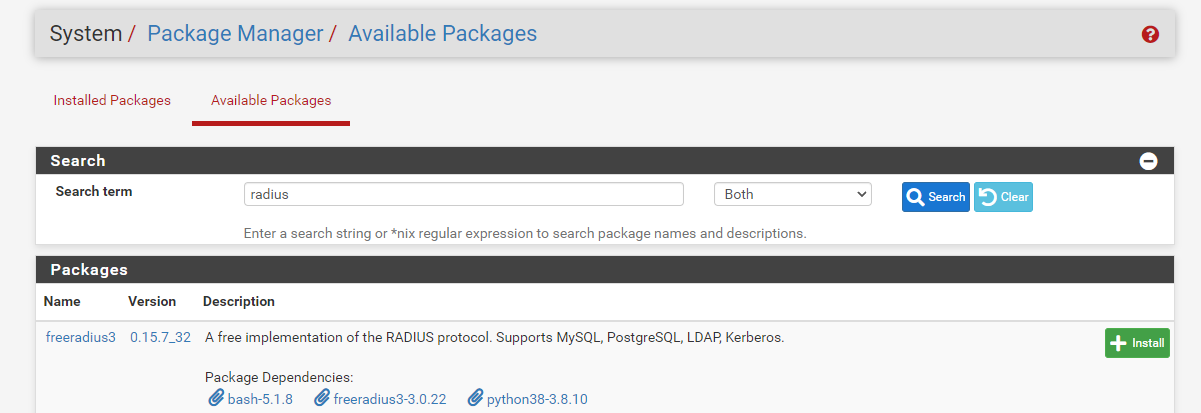




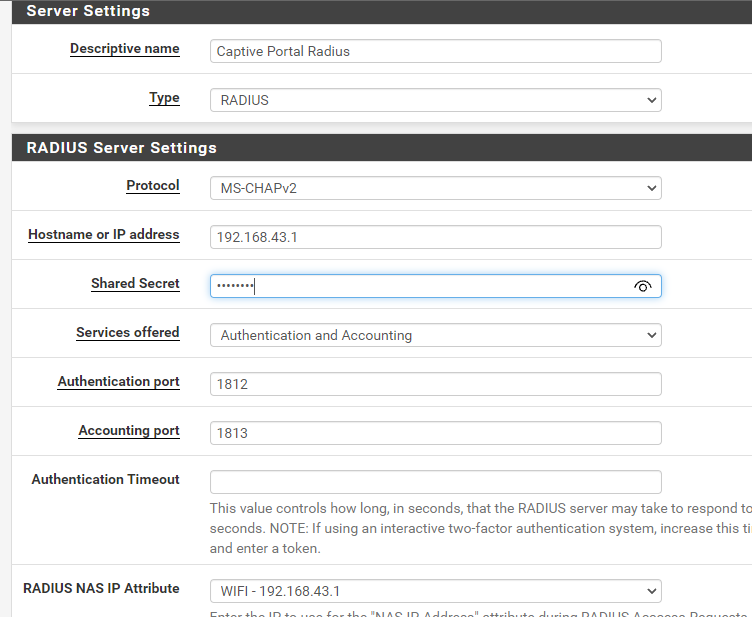
### Phân Nâng Cao (Authentication dùng Raidus Server)

Vào System > Package Manager

Tìm và cài đặt gói “freeradius3”



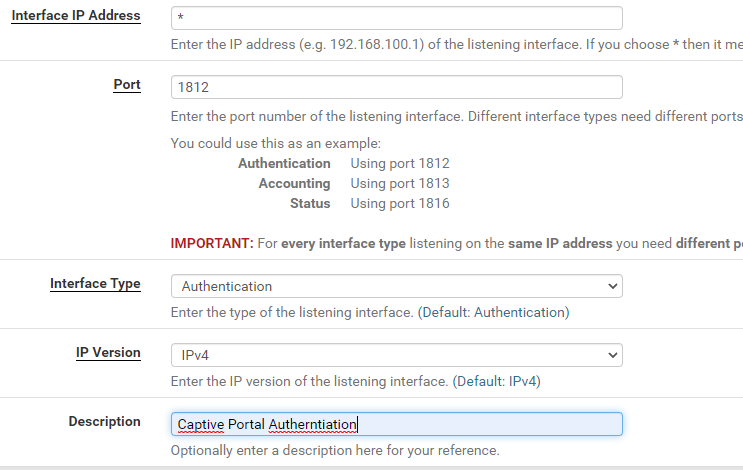
Vào System > User Manager > Authentication Servers > Add > thiết lập thông tin của Authentication Server. Phần quan trọng nhất là IP, ta phải để IP WIFI interface

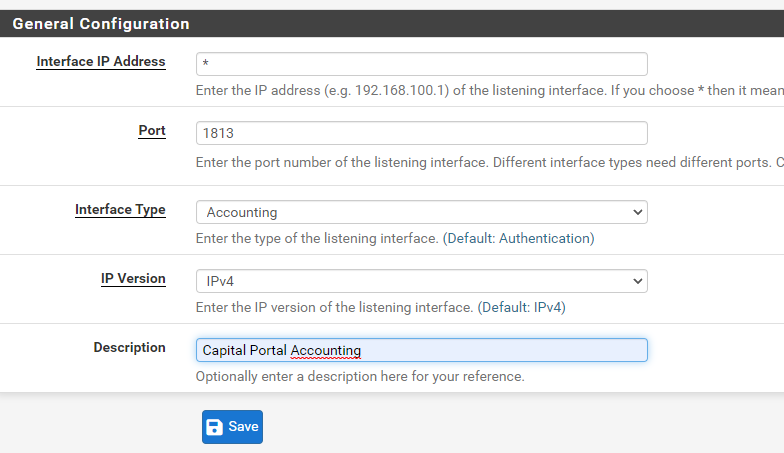


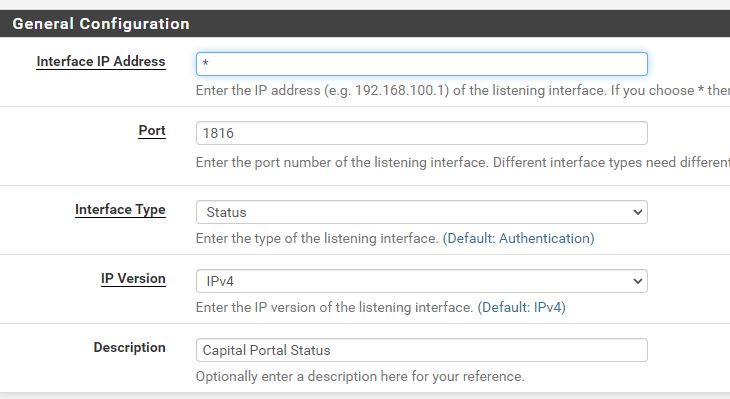
Vào Service > Free Radius > Interfaces

Lần lượt thiết lập các interface:

* Authentication port 1812
* Accounting port 1813
* Status port 1816



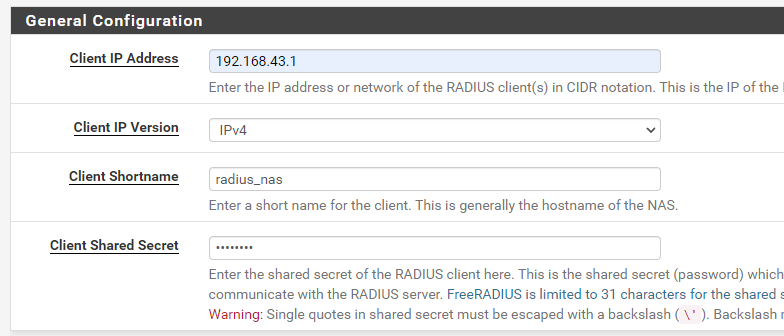




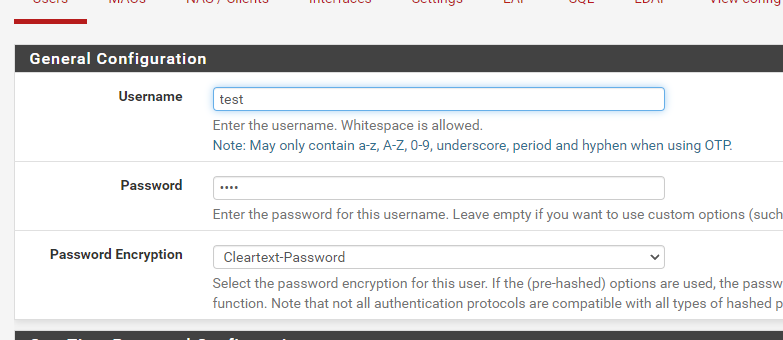
Ở Service Free Radius > chọn tiếp NAS/Client

Client IP là IP của Radius Client, ở đây ta nhập vào 192.168.43.1

Client Shared Secret là mật khẩu đã nhập khi thêm Authentication Server bên trên, mục đích là để kết nối với Radius Server xác thực tài khoản



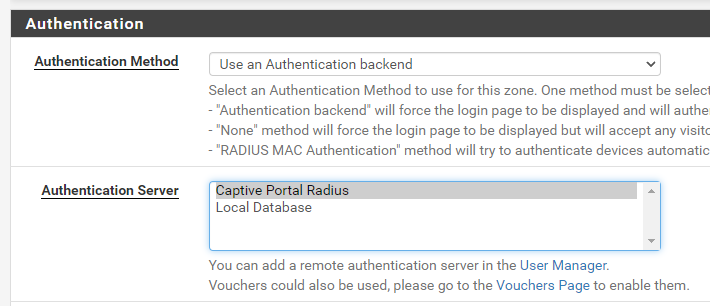
Sau khi xong ta chọn tiếp mục Users để thêm tài khoản cho client



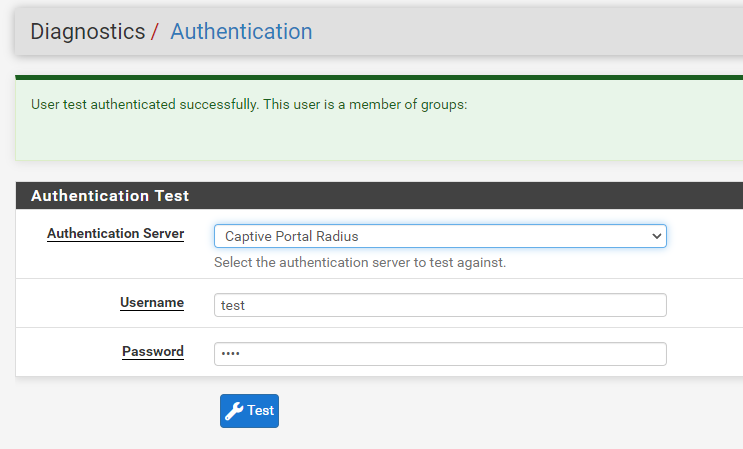
Như vậy là hoàn tất thiết lập Radius Authentication Server

Quay lại Service Captive Portal ở phần Authentication Method > Use an backend Authentication backend

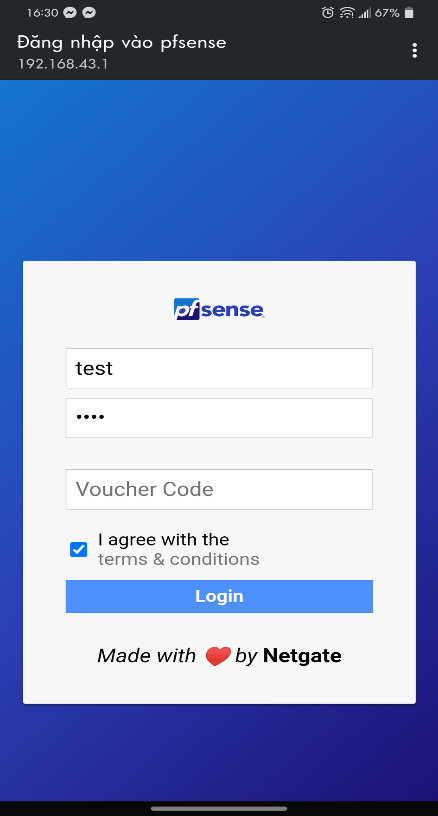
Authentication Server chọn tên Radius Authentication Server đã tạo trước đó



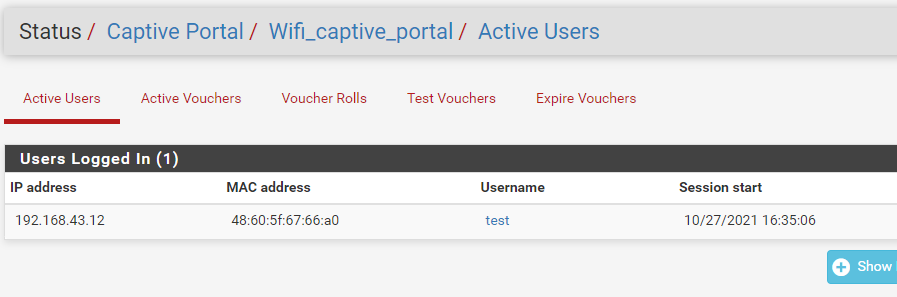
Kiểm tra kết nối trên pfsense với tài khoản “test”



Kiểm tra trên thiết bị của Client



Trên Pfsense phần Status đã xuất hiện user “test”



# PHẦN III. Tài Liệu Tham Khảo.

[1] Video Youtube: [pfsense Captive Portal](https://www.youtube.com/watch?v=hdHDCafeFdU)

[2] Video Youtube: [Pfsense 2.5 tutorial: how to create captive portal on Pfsense](https://www.youtube.com/watch?v=OrcIczjd5ww)

[3] Video Youtube: [Update: FreeRadius and Captive Portal Customization on Pfsense 2.4.4](https://youtu.be/m5oyxGenUxY)