

**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:**

<b>Nguyễn Tuấn Kiệt</b>	<b>N18DCAT035</b>
<b>Trần Khang</b>	<b>N18DCAT037</b>
<b>Nguyễn Quốc Huy</b>	<b>N18DCAT029</b>
<b>Phạm Viết Học</b>	<b>N18DCAT026</b>
<b>Phan Hoài Phương</b>	<b>N18DCAT061</b>

Thành phố Hồ Chí Minh – Năm 2021

## MỤC LỤC

<b>MỤC LỤC .....</b>	<b>2</b>
<b>PHẦN I. Cơ Sở Lý Thuyết.....</b>	<b>3</b>
<b>A. Pfsense.....</b>	<b>3</b>
<b>B. Tính Năng Pfsense.....</b>	<b>3</b>
1. Pfsense Aliases .....	3
2. NAT .....	3
3. Firewall Rules.....	4
4. Firewall Schedules .....	4
5. Traffic Shaper.....	4
6. Virtual IPS .....	4
<b>C. Một số dịch vụ Pfsense.....</b>	<b>5</b>
1. Captive Portal .....	5
2. Các dịch vụ khác.....	6
<b>PHẦN II. Nội dung bài lab.....</b>	<b>6</b>
<b>A. Phân Công.....</b>	<b>6</b>
<b>B. Chuẩn bị.....</b>	<b>7</b>
<b>C. Thực hiện .....</b>	<b>8</b>
1. Thiết lập Pfsense có 3 card mạng. ....	8
2. Cấu hình từng interface cho pfsense.....	9
3. Cấu hình các thông tin cơ bản bằng web config.....	10
4. Cấu hình Interface WIFI để thực hiện Captive Portal .....	15
5. Thiết lập Firewall Rules cho interface WIFI. ....	16
6. Thiết lập captive portal. ....	20
7. Phần Cơ Bản .....	22
8. Phần Nâng Cao (Vouchers) .....	23
9. Phần Nâng Cao (Authentication dùng Radius Server) .....	28
<b>PHẦN III. Tài Liệu Tham Khảo.....</b>	<b>34</b>

## **PHẦN I. Cơ Sở Lý Thuyết**

### **A. Pfsense**

- Một cách ngắn gọn PfSense là một ứng dụng có chức năng định tuyến và tường lửa mạnh mẽ 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 các công ty.

### **B. Tính Năng Pfsense**

#### **1. 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 công.

#### **2. NAT**

PfSense cung cấp network address translation (NAT) và tính năng chuyển tiếp công, 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 chuyển 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.

### **3. Firewall Rules**

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

### **4. Firewall Schedules**

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.

### **5. Traffic Shaper**

Traffic Shaper 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 khi 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 lý băng thông của một số ứng dụng khác như Remote Service VPN, Messengers, Web, Mail, Miscellaneous

### **6. 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.

## C. Một số dịch vụ Pfsense

### 1. 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-through MAC: Các MAC address được cấu hình trong mục này sẽ được bỏ qua, không authentication.
- Allowed IP address: 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 mỗi ip/user/mac.
- Idle timeout: Nếu mỗi 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 mỗi 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 nằm trước router. Bởi vì pfsense quản lý kết nối theo MAC (mặc định). Mà chỉ 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, ...).

## 2. Các dịch vụ khác

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

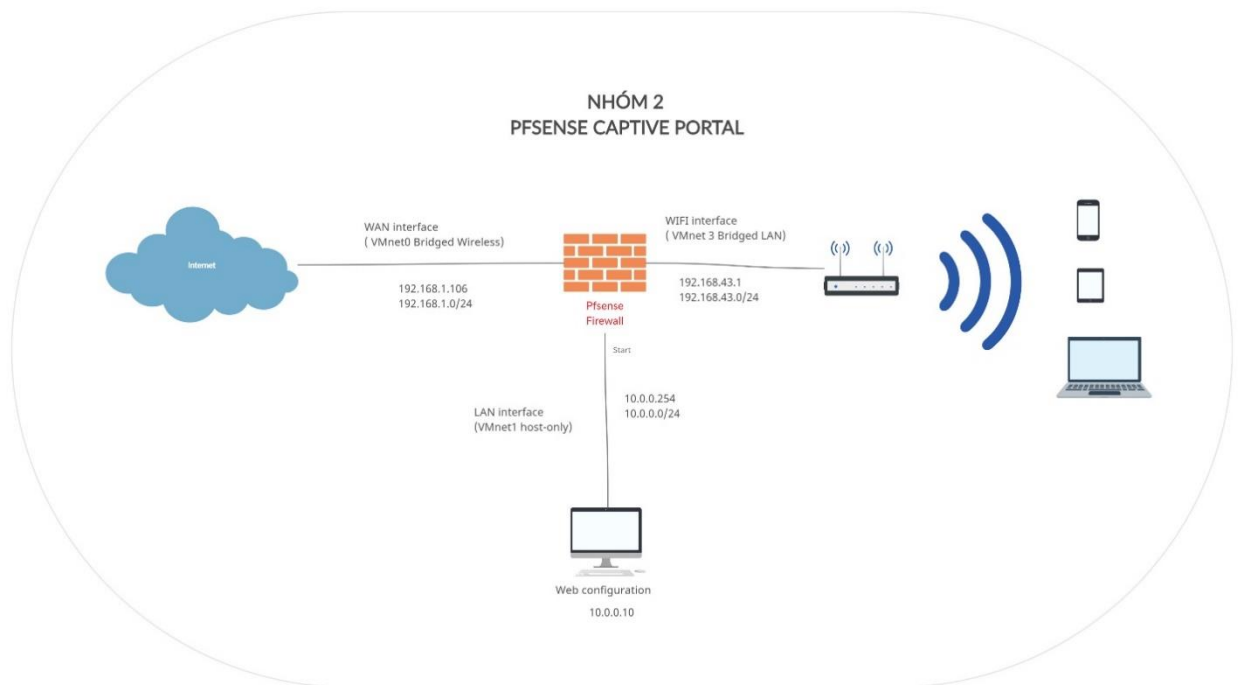
## PHẦN II. Nội dung bài lab

### A. Phân Công

STT	Tên	Nhiệm vụ
1	Trần Khang	Tìm hiểu lý thuyết, Xây dựng mô hình, chuẩn bị phần cứng (router phát wifi), Cài đặt nội dung Cơ Bản.
2	Nguyễn Quốc Huy	Cấu hình card mạng cho VMWare, Cấu hình DHCP LAN.
3	Nguyễn Viết Học	Setup pfsense khi đăng nhập lần đầu, Thiết lập WIFI Interface.
4	Phan Hoài Phương	Cấu hình Firewall Rule cho WIFI, Cấu hình DHCP WIFI.
5	Nguyễn Tuấn Kiệt	Cài đặt nội dung Nâng Cao (vouchers + password)

## B. 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)

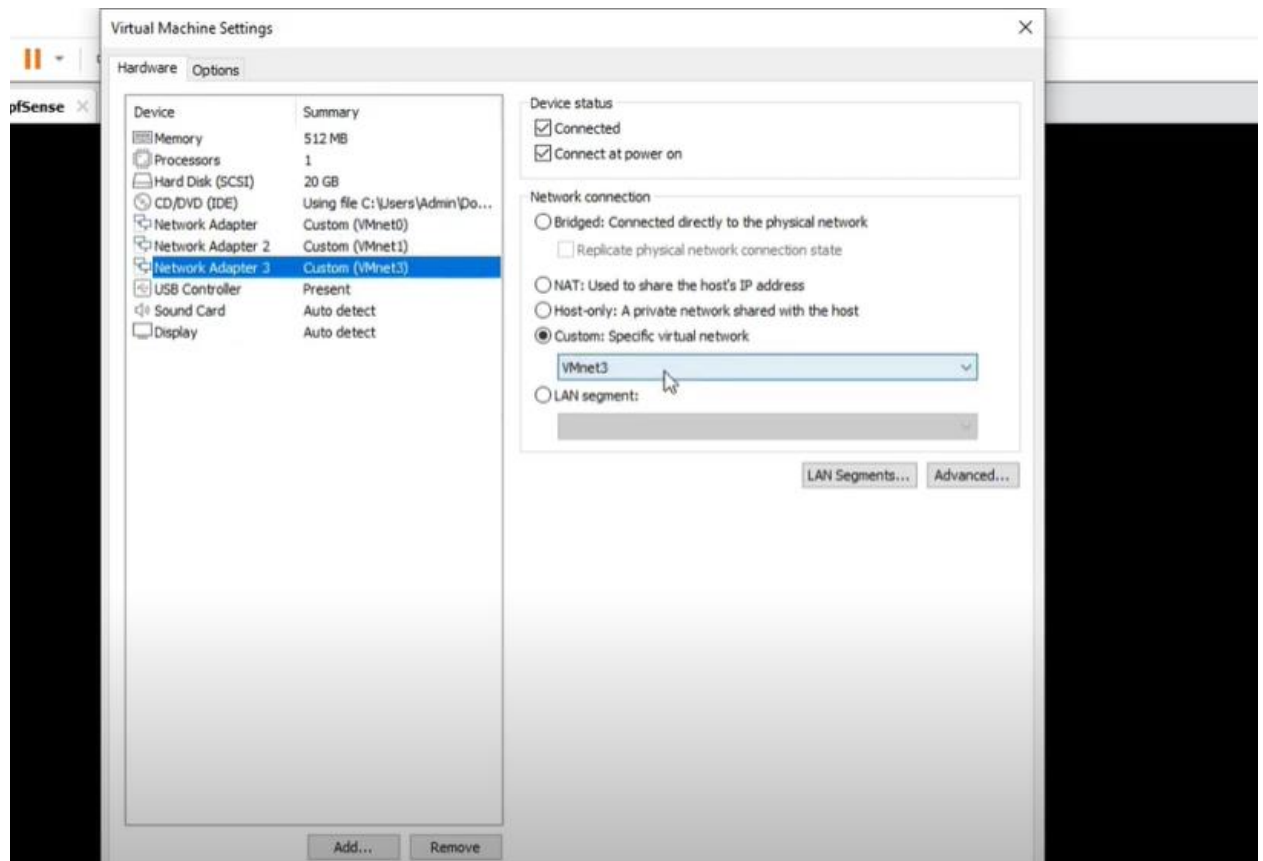
IP: 10.0.0.254 – 10.0.0.0/24

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

## C. Thực hiện

### 1. Thiết lập Pfsense có 3 card mạng.





## 2. Cấu hình từng interface cho pfsense

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: ab94979684637f96175f

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.106/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Cài IP cho Lan 10.0.0.254

```
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.10
Enter the end address of the IPv4 client address range: 10.0.0.20█
```

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

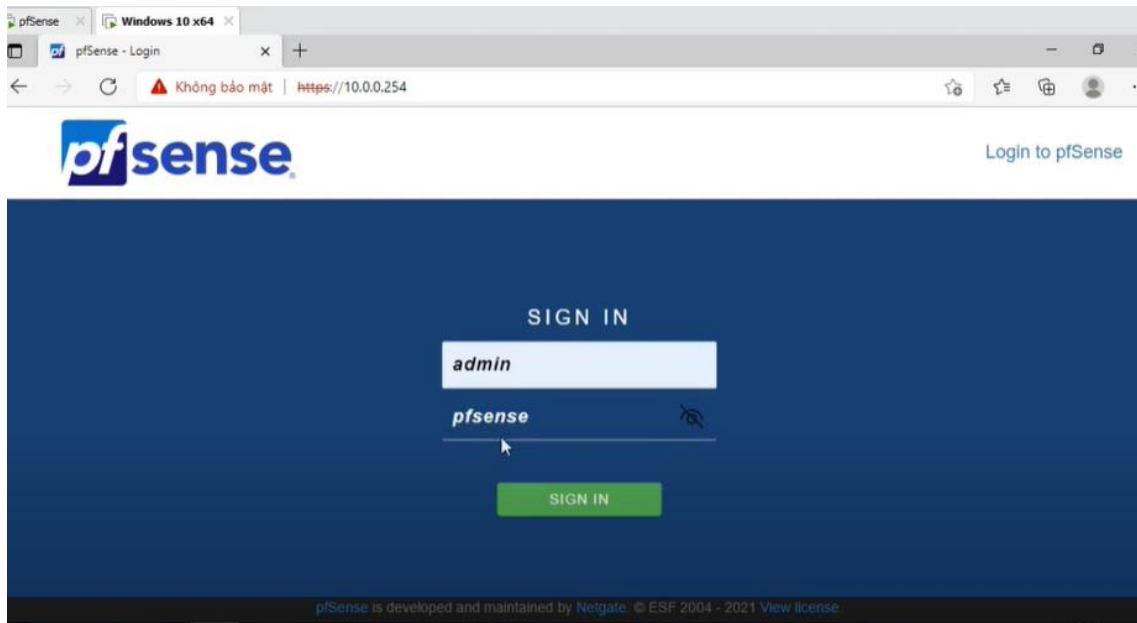
Máy Client win 10 sử dụng card Vmnet 1.

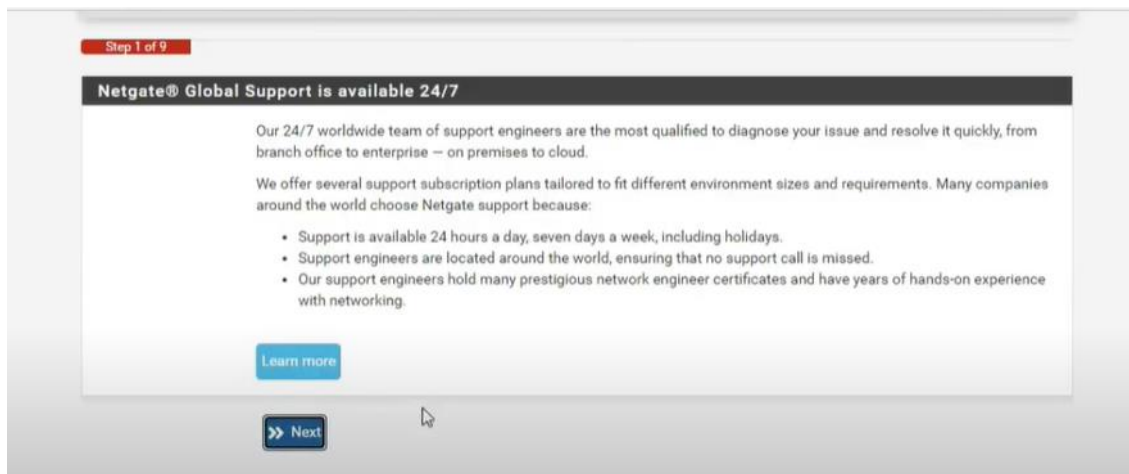
```
C:\Users\Admin>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:
Reply from 10.0.0.254: bytes=32 time<1ms TTL=64
Reply from 10.0.0.254: bytes=32 time<1ms TTL=64
Reply from 10.0.0.254: bytes=32 time<1ms TTL=64
```

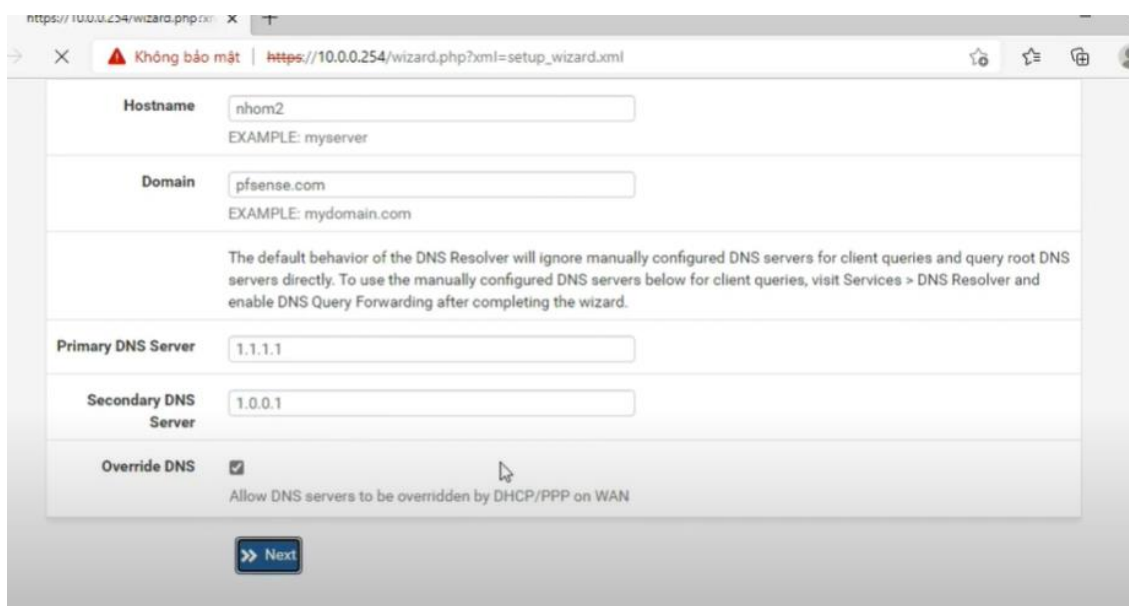
Truy cập vào Pfsense với địa chỉ 10.0.0.254 trên máy Client

Với user: admin và password: pfsense





Đặt hostname và domain.



pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

Time server hostname   
Enter the hostname (FQDN) of the time server.

Timezone

Next

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

### Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

### General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

← → × ⚠ Không bảo mật | https://10.0.0.254/wizard.php?xml=setup\_wizard.xml

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

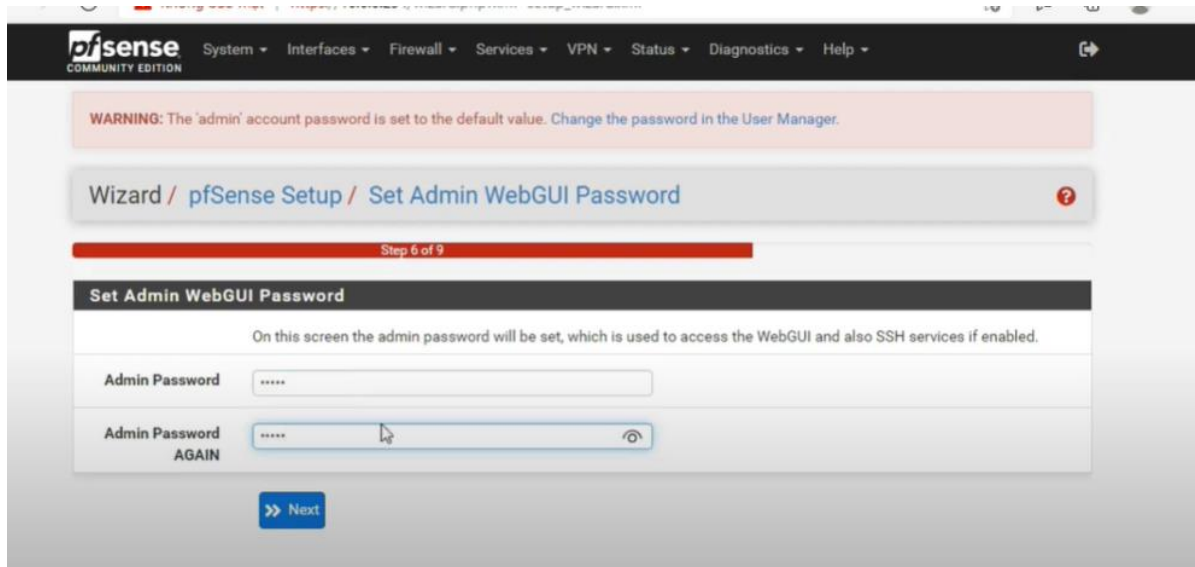
### Configure LAN Interface

On this screen the Local Area Network information will be configured.

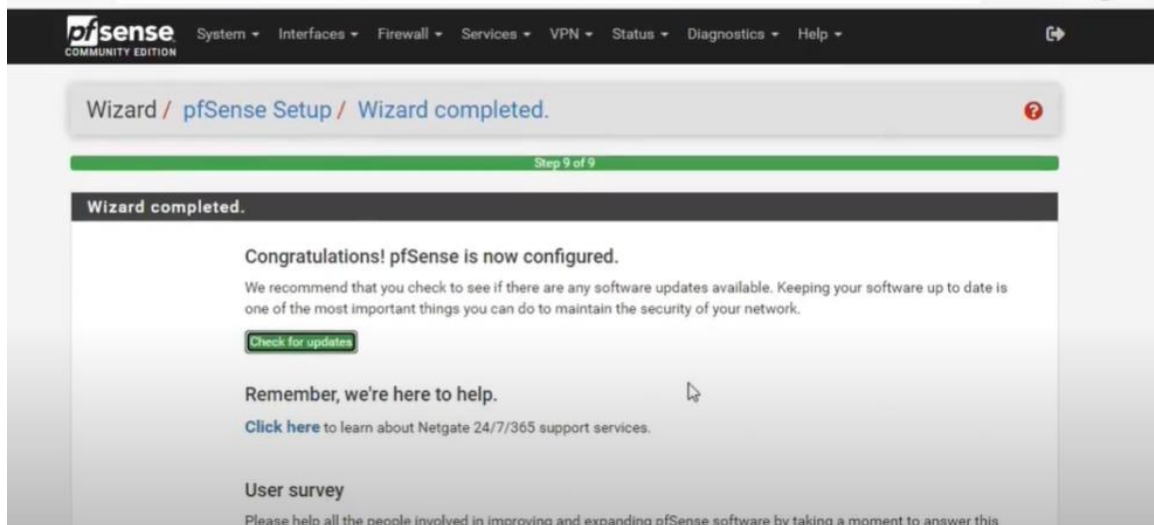
LAN IP Address   
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

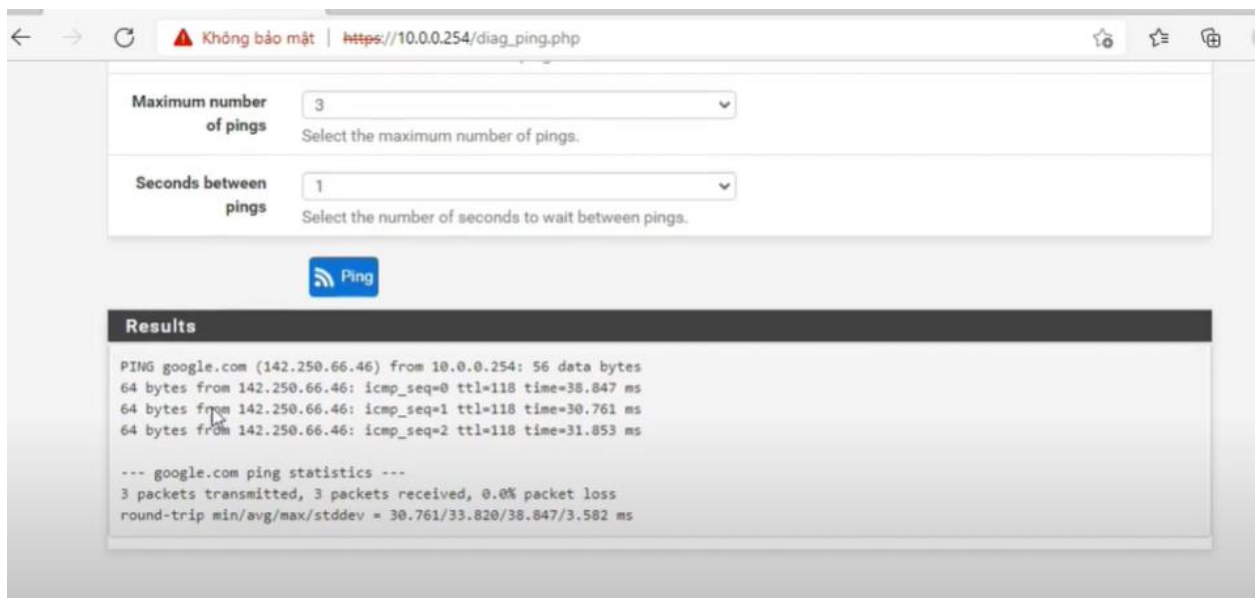
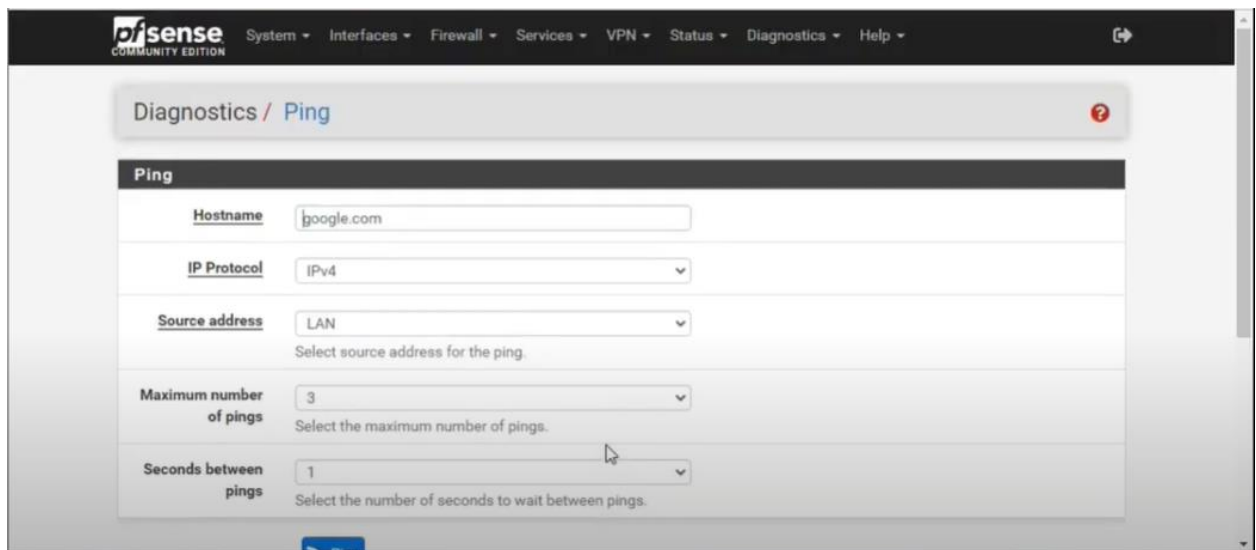
Next



Cấu hình thành công Pfsense.

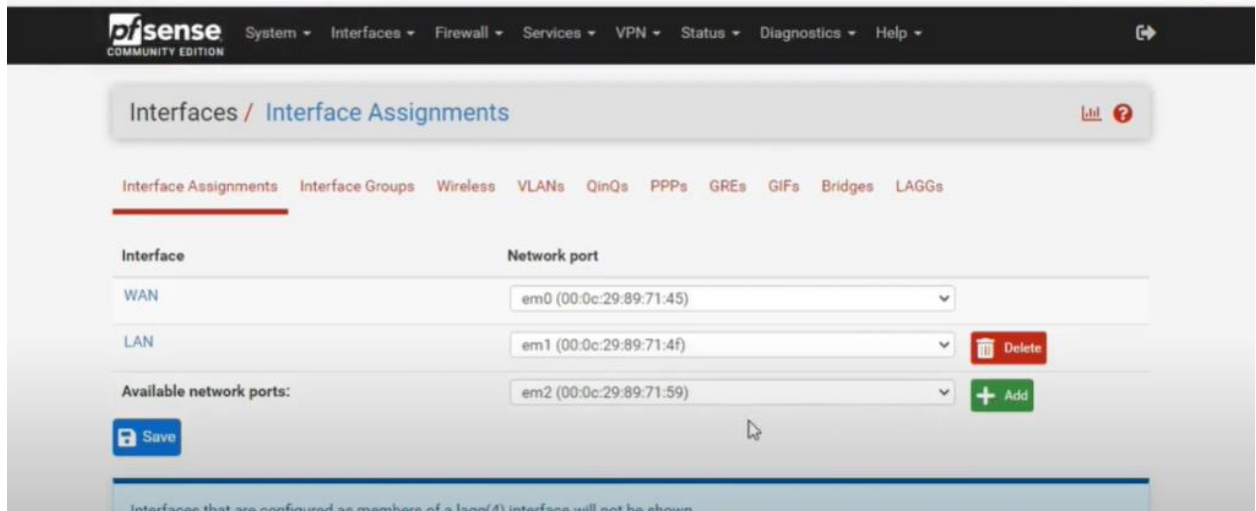


Vào Diagnostics -> Ping từ Lan tới google.com để kiểm tra kết nối internet của mạng LAN

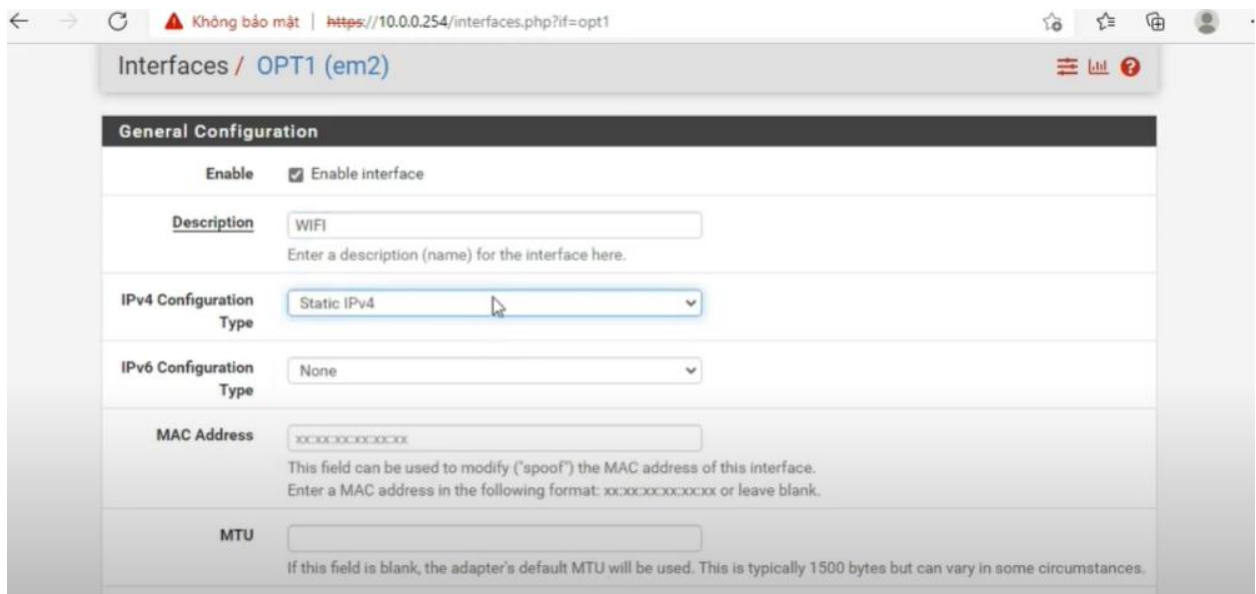


#### 4. Cấu hình Interface WIFI để thực hiện Captive Portal

Vào Interfaces -> Assignments -> Add



Sửa OPT1 -> WIFI và chọn Static IPv4.



Đặt IP 192.168.43.1 /24, Sau đó Save lại.

**Static IPv4 Configuration**

IPv4 Address: 192.168.43.1 / 24

IPv4 Upstream gateway: None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking [here](#).

**Reserved Networks**

☐ **Block private networks and loopback addresses**  
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

☐ **Block bogon networks**  
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.

## 5. Thiết lập Firewall Rules cho interface WIFI.

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

**Firewall / Rules / LAN**

Floating WAN LAN WIFI

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 2 / 8.06 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	<a href="#">Settings</a>
<input checked="" type="checkbox"/> 0 / 84.89 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	<a href="#">Copy</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Lock</a> <a href="#">Unlock</a>
<input type="checkbox"/> 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<a href="#">Copy</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Lock</a> <a href="#">Unlock</a>

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)



## Interface chọn WIFI

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

**Interface** WIFI  
Choose the interface from which packets must come to match this rule.

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

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

**Source**

**Source** ☐ Invert match LAN net Source Address /

**Destination**

**Destination** ☐ Invert match any Destination Address /

Source chọn WIFI net. Sau đó chọn Save.

**Source**

**Source** ☐ Invert match WIFI net Source Address /

**Destination**

**Destination** ☐ Invert match any Destination Address /

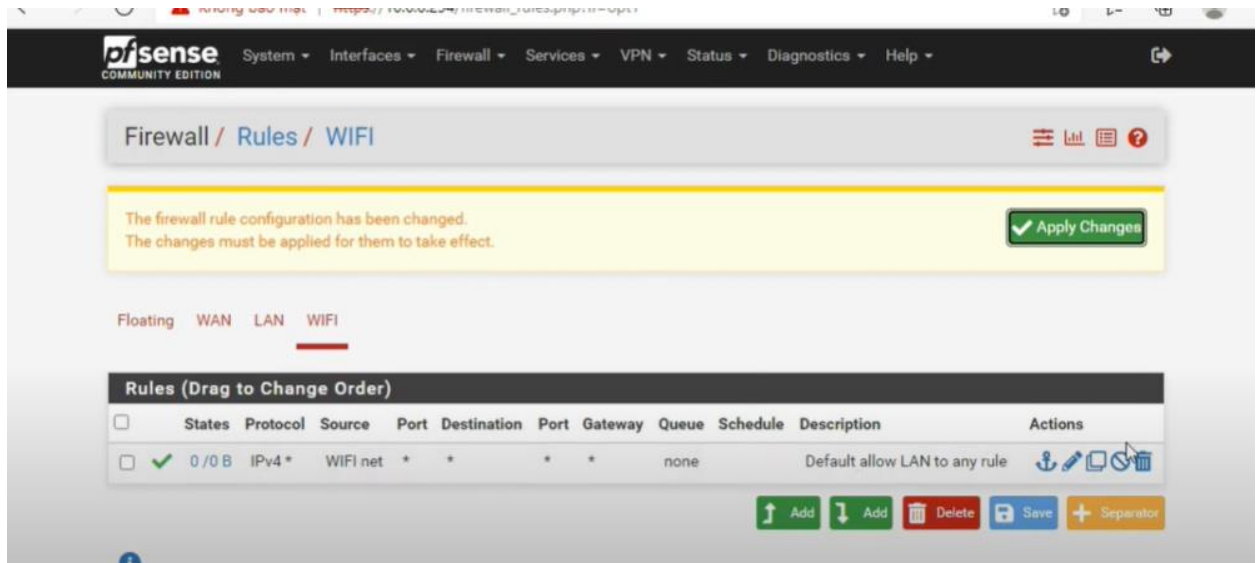
**Extra Options**

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

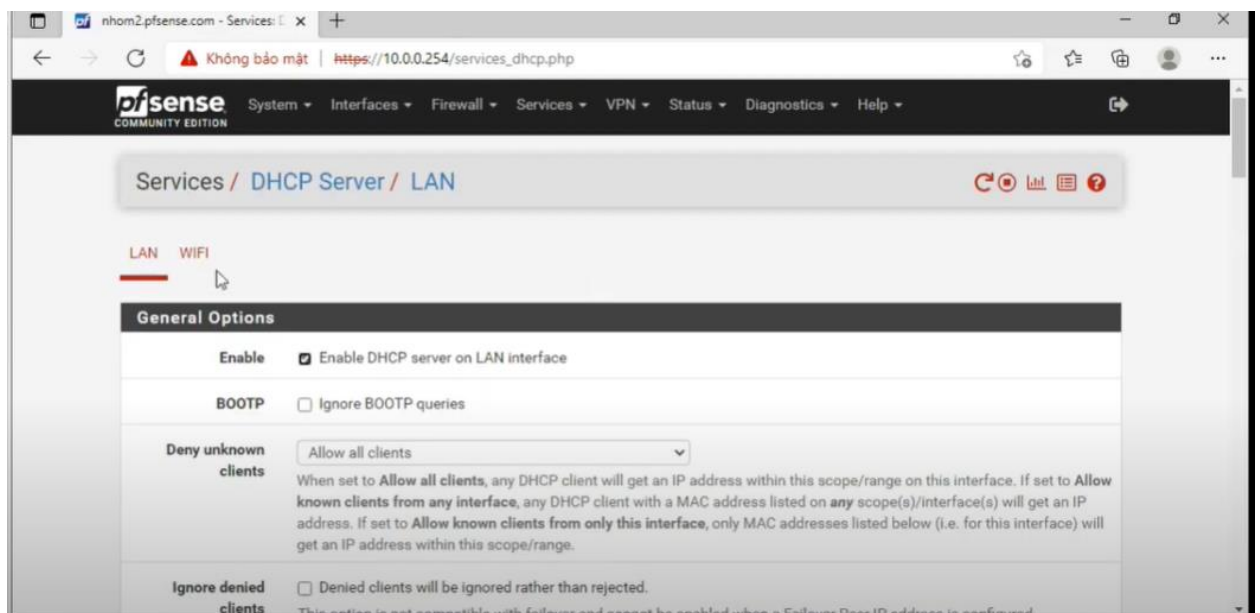
**Description** Default allow LAN to any rule  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)



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



Cấp IP từ 192.168.43.10 -> 192.168.43.20

Ignore denied clients ☐ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 192.168.43.0

Subnet mask 255.255.255.0

Available range 192.168.43.1 - 192.168.43.254

Range 192.168.43.10 192.168.43.20

From To

Additional Pools

Add [+ Add pool](#)

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions
------------	----------	-------------	---------

Diagnostics -> Ping từ WIFI tới google.com

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help

Diagnostics / Ping

Ping

Hostname google.com

IP Protocol IPv4

Source address WIFI

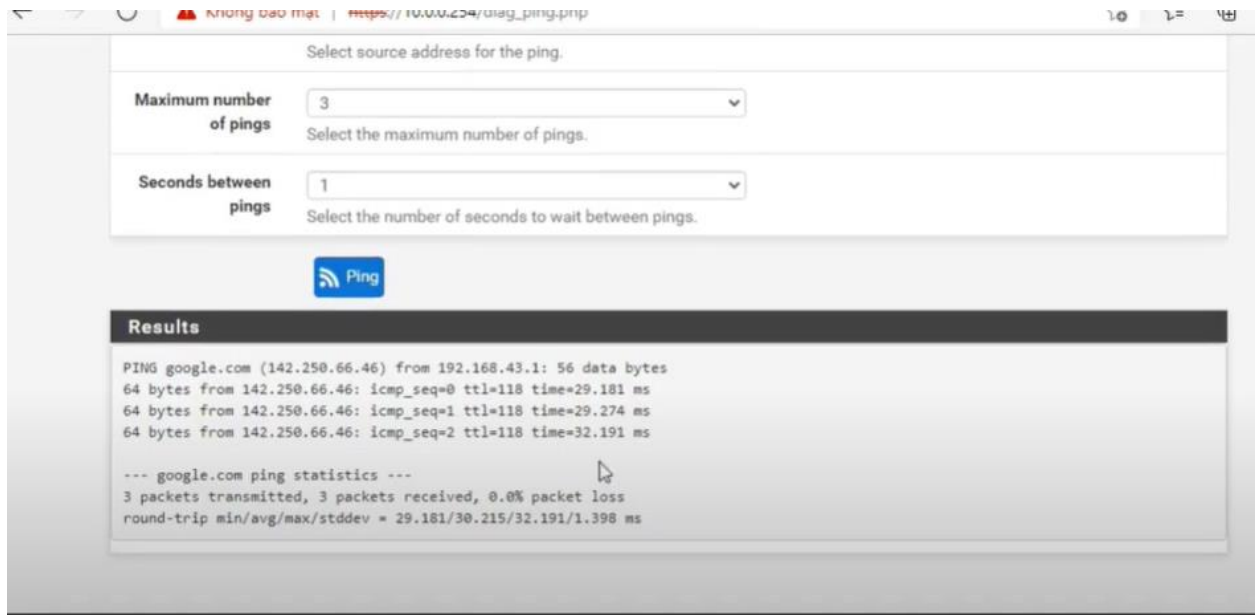
Select source address for the ping.

Maximum number of pings 3

Select the maximum number of pings.

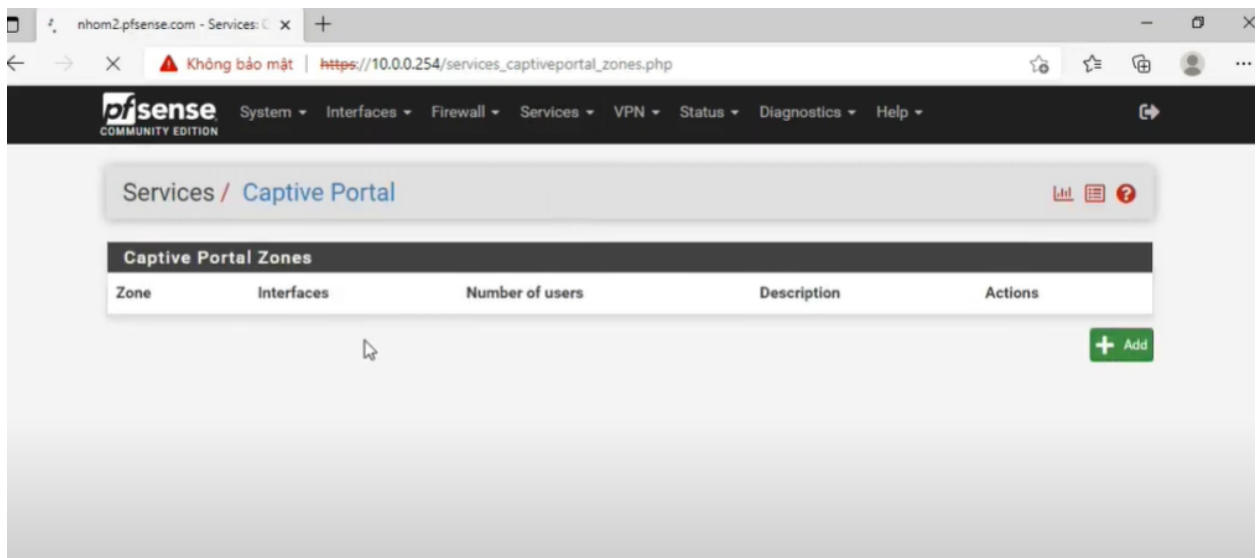
Seconds between pings 1

Select the number of seconds to wait between pings.



## 6. Thiết lập captive portal.

Vào Services -> Captive Portal -> Add



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

The screenshot shows the 'Add Captive Portal Zone' configuration page in the pfSense web interface. The breadcrumb trail is 'Services / Captive Portal / Add Zone'. The page has a title bar 'Add Captive Portal Zone'. Below it, there are two input fields: 'Zone name' with the value 'Wifi\_captive\_portal' and 'Zone description' with the value 'wifi captive portal'. Below the fields is a 'Save & Continue' button.

Services / Captive Portal / Add Zone

**Add Captive Portal Zone**

**Zone name** Wifi\_captive\_portal  
Zone name. Can only contain letters, digits, and underscores (\_) and may not start with a digit.

**Zone description** wifi captive portal  
A description may be entered here for administrative reference (not parsed).

Save & Continue

Enable Captive Portal và Interface chọn WIFI.

The screenshot shows the 'Captive Portal Configuration' page in the pfSense web interface. The breadcrumb trail is 'Services / Captive Portal / Wifi\_captive\_portal / Configuration'. The page has a title bar 'Captive Portal Configuration'. Below it, there are several sections: 'Enable' with a checked 'Enable Captive Portal' checkbox, 'Description' with the value 'wifi captive portal', 'Interfaces' with a dropdown menu showing 'WAN', 'LAN', and 'WIFI' (selected), and 'Maximum concurrent connections' with an empty input field.

Services / Captive Portal / Wifi\_captive\_portal / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

**Captive Portal Configuration**

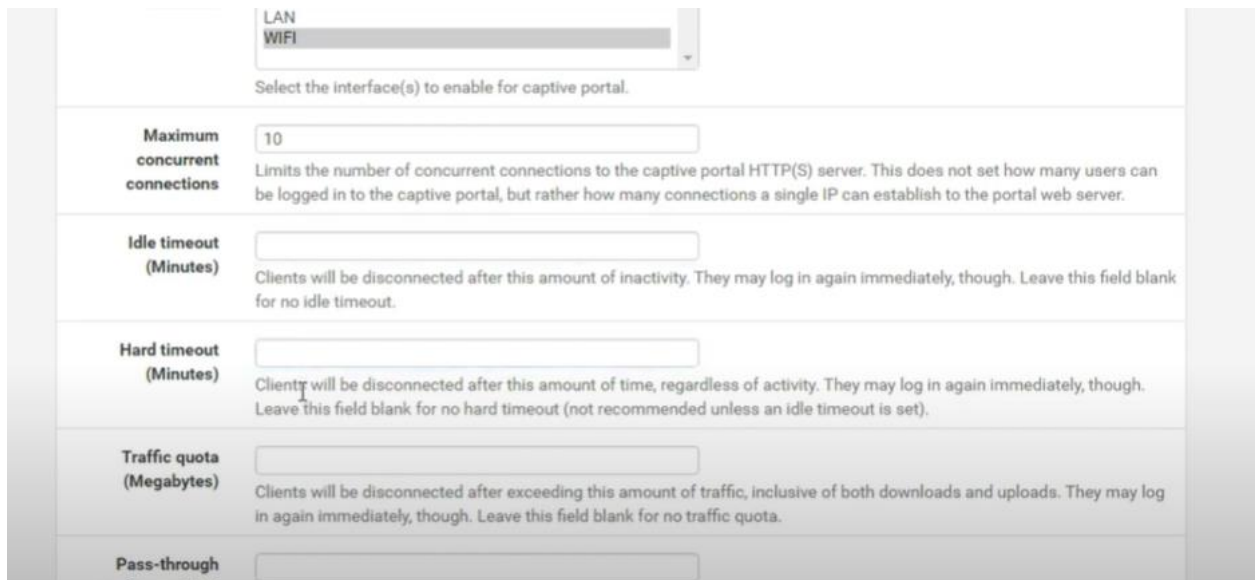
**Enable** ☒ Enable Captive Portal

**Description** wifi captive portal  
A description may be entered here for administrative reference (not parsed).

**Interfaces** WAN LAN WIFI  
Select the interface(s) to enable for captive portal.

**Maximum concurrent connections**  
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Cho tối đa 10 kết nối cùng lúc.



LAN  
WIFI

Select the interface(s) to enable for captive portal.

**Maximum concurrent connections**  
10  
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

**Idle timeout (Minutes)**  
  
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

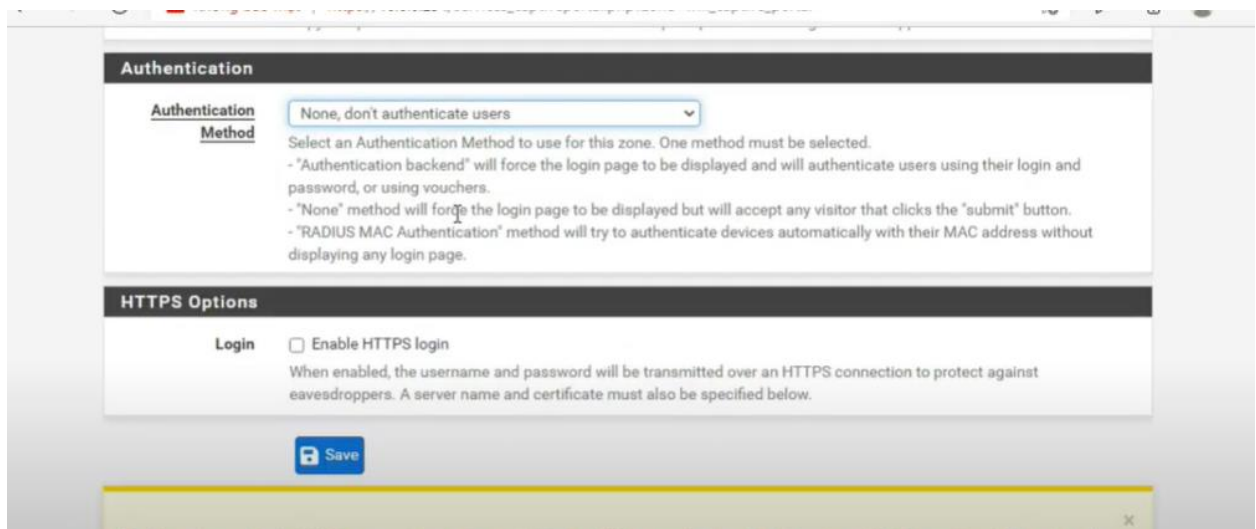
**Hard timeout (Minutes)**  
  
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

**Traffic quota (Megabytes)**  
  
Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

**Pass-through**

## 7. Phần Cơ Bản

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



**Authentication**

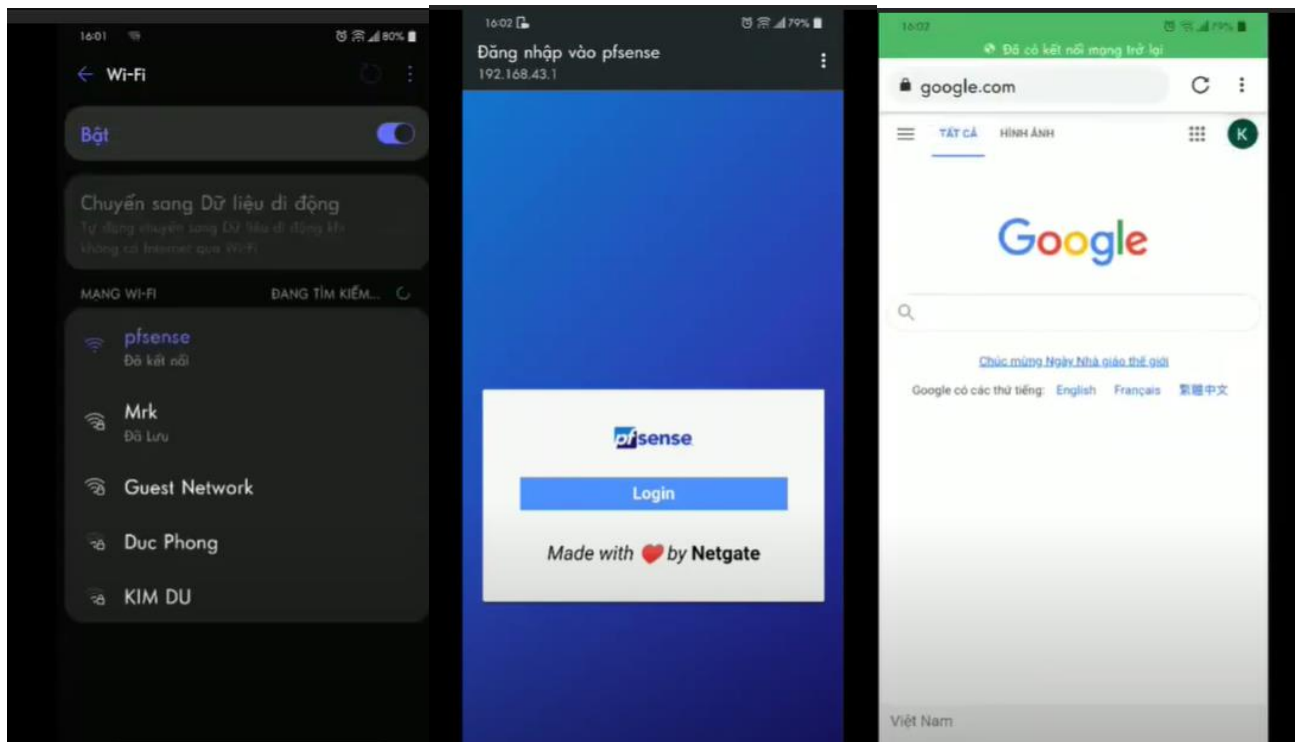
**Authentication Method**  
None, don't authenticate users  
Select an Authentication Method to use for this zone. One method must be selected.  
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.  
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.  
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

**HTTPS Options**

**Login**  
☐ Enable HTTPS login  
When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

**Save**

Kết nối trên điện thoại kiểm tra



## 8. Phần Nâng Cao (Vouchers)

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

Terms and Conditions	<div></div> <p>Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out</p>
<b>Authentication</b>	
Authentication Method	<div>Use an Authentication backend</div> <p>Select an Authentication Method to use for this zone. One method must be selected.</p> <ul style="list-style-type: none"><li>- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.</li><li>- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.</li><li>- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.</li></ul>
Authentication Server	<div>Local Database</div> <p>You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.</p>
Reauthenticate Users	<input type="checkbox"/> Reauthenticate connected users every minute <p>If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in. The cached credentials are necessary for the portal to perform automatic reauthentication requests.</p>

Chọn Vouchers > Chọn Generate new keys > Chọn Add.

Roll # Minutes/Ticket # of Tickets Comment Actions

**Create, Generate and Activate Rolls with Vouchers**

Enable ☒ Enable the creation, generation and activation of rolls with vouchers

**Create, Generate and Activate Rolls with Vouchers**

Voucher Public Key

```
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADAwEAJIAIX7w/CHY1oPag
MBAAE=
-----END PUBLIC KEY-----
```

Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers. [Generate new keys](#)

Voucher Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MD8CAQACCQCF+8PwJGIQDwIDAQABAgg1M2jNFdoRLQIFAJ
ao17sCBQDjqn09AgQW
qz0jAgQdu4WZAgQUGjOq
-----END RSA PRIVATE KEY-----
```

[Generate new keys](#)

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

**Voucher Rolls**

Roll #   
Enter the Roll# (0..65535) found on top of the generated/printed vouchers

Minutes per ticket   
Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.

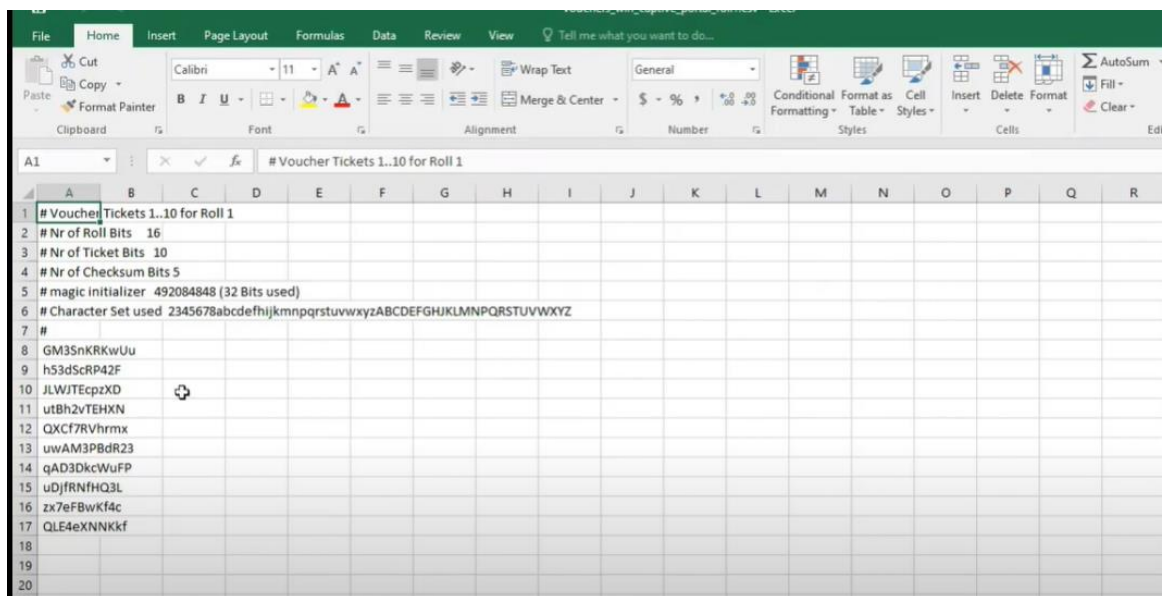
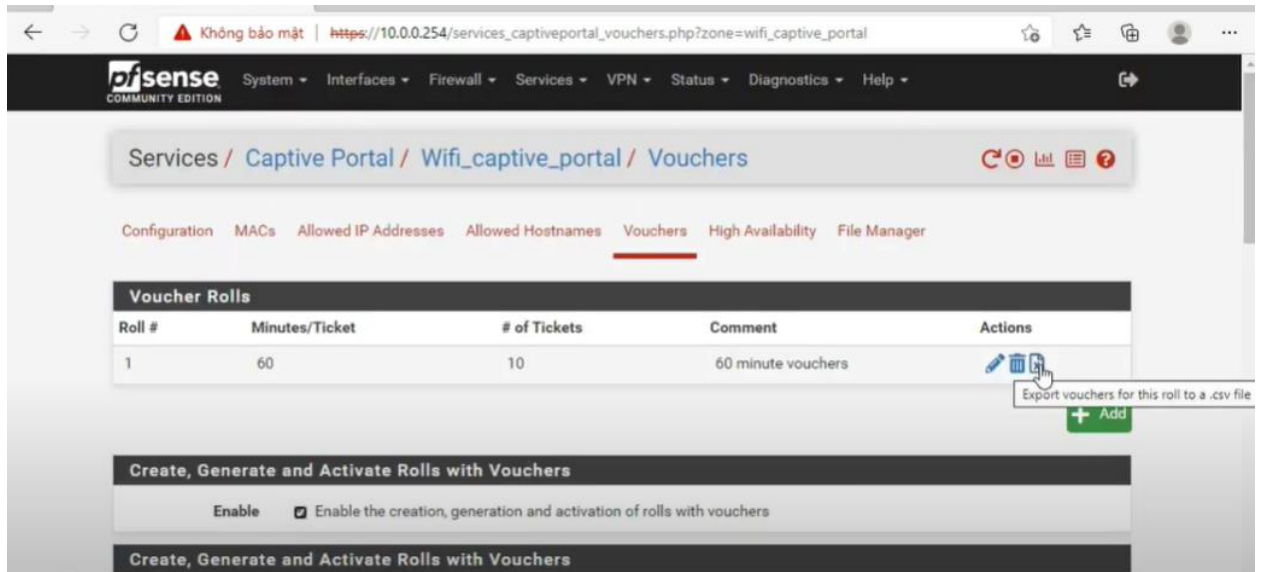
Count   
Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again

Comment   
Can be used to further identify this roll. Ignored by the system.

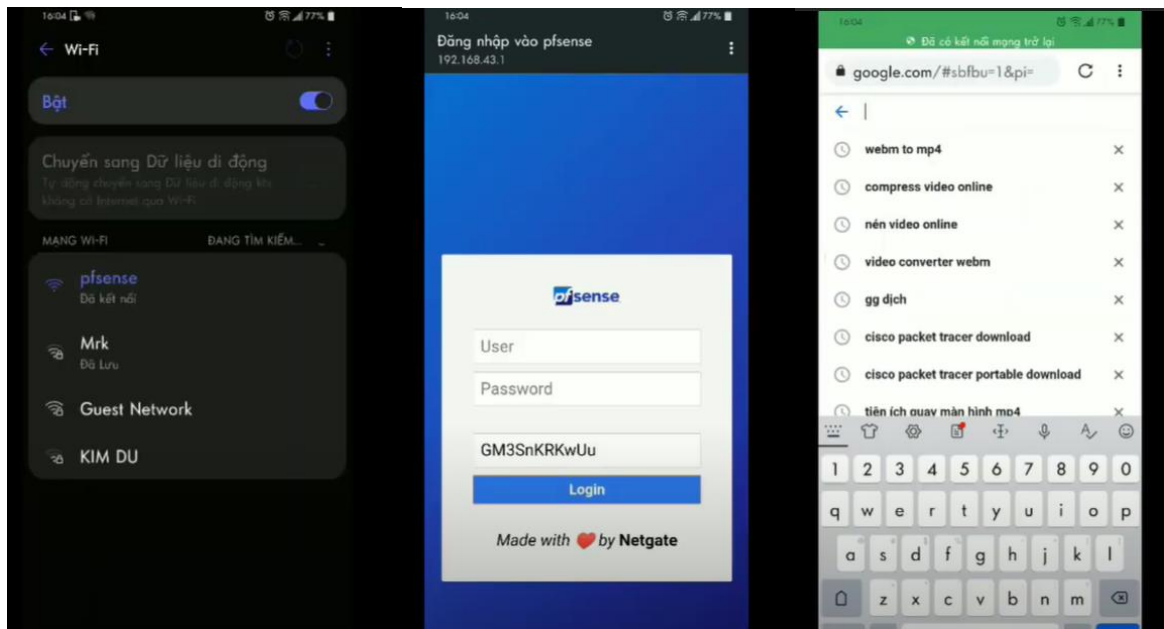
[Save](#)



Sau đó xuất Voucher ra.



Kết nối.



Quản lí các thiết bị kết nối.

Vào Status -> Captive Portal.

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Status / Captive Portal / Wifi\_captive\_portal / Active Users'. Below the breadcrumb, there are tabs for 'Active Users', 'Active Vouchers', 'Voucher Rolls', 'Test Vouchers', and 'Expire Vouchers'. The 'Active Users' tab is selected. The main content area is titled 'Users Logged In (1)' and contains a table with the following data:

IP address	MAC address	Username	Session start	Actions
192.168.43.12	48:60:5f:67:66:a0	GM3SnKRKwUu	10/05/2021 16:04:51	

At the bottom right of the table, there are two buttons: 'Show Last Activity' (blue) and 'Disconnect All Users' (red).

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Status / Captive Portal / Wifi\_captive\_portal / Active Vouchers'. Below the breadcrumb, there are tabs for 'Active Users', 'Active Vouchers', 'Voucher Rolls', 'Test Vouchers', and 'Expire Vouchers'. The 'Active Vouchers' tab is selected. The main content area is titled 'Vouchers in Use (1)' and contains a table with the following data:

Voucher	Roll	Activated at	Expires in	Expires at
GM3SnKRKwUu	1	10/05/2021 16:04:51	59min	10/05/2021 17:04:51

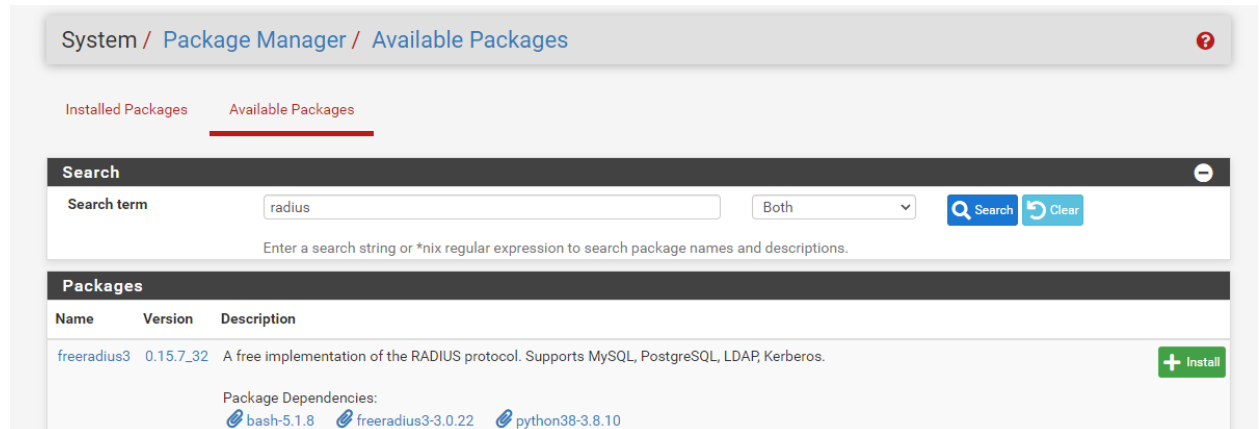
This screenshot is identical to the previous one, showing the 'Active Vouchers' tab in the pfSense interface. The table displays one voucher with the following details:

Voucher	Roll	Activated at	Expires in	Expires at
GM3SnKRKwUu	1	10/05/2021 16:04:51	59min	10/05/2021 17:04:51

## 9. Phân Nâng Cao (Authentication dùng Radius 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

The screenshot shows the 'Server Settings' form for adding a new Authentication Server. The form is divided into two main sections: 'Server Settings' and 'RADIUS Server Settings'.

**Server Settings:**

- Descriptive name:** Captive Portal Radius
- Type:** RADIUS

**RADIUS Server Settings:**

- Protocol:** MS-CHAPv2
- Hostname or IP address:** 192.168.43.1
- Shared Secret:** (masked with dots)
- Services offered:** Authentication and Accounting
- Authentication port:** 1812
- Accounting port:** 1813
- Authentication Timeout:** (empty field)
- RADIUS NAS IP Attribute:** WIFI - 192.168.43.1

Below the 'Authentication Timeout' field, there is a note: 'This value controls how long, in seconds, that the RADIUS server may take to respond to seconds. NOTE: If using an interactive two-factor authentication system, increase this ti and enter a token.'

Vào Service > Free Radius > Interfaces

Lần lượt thiết lập các interface:

- Authentication port 1812
- Accounting port 1813
- Status port 1816

---

<b><u>Interface IP Address</u></b>	<input type="text" value="*"/>
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means any IP address.	

---

<b><u>Port</u></b>	<input type="text" value="1812"/>						
Enter the port number of the listening interface. Different interface types need different ports. You could use this as an example: <table><tr><td><b>Authentication</b></td><td>Using port 1812</td></tr><tr><td><b>Accounting</b></td><td>Using port 1813</td></tr><tr><td><b>Status</b></td><td>Using port 1816</td></tr></table>		<b>Authentication</b>	Using port 1812	<b>Accounting</b>	Using port 1813	<b>Status</b>	Using port 1816
<b>Authentication</b>	Using port 1812						
<b>Accounting</b>	Using port 1813						
<b>Status</b>	Using port 1816						

---

**IMPORTANT:** For every interface type listening on the same IP address you need different ports.

---

<b><u>Interface Type</u></b>	<input type="text" value="Authentication"/>
Enter the type of the listening interface. (Default: Authentication)	

---

<b><u>IP Version</u></b>	<input type="text" value="IPv4"/>
Enter the IP version of the listening interface. (Default: IPv4)	

---

<b><u>Description</u></b>	<input type="text" value="Captive Portal Authentication"/>
Optionally enter a description here for your reference.	

---

### General Configuration

**Interface IP Address**

\*

Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose \* then it means

**Port**

1813

Enter the port number of the listening interface. Different interface types need different ports. C

**Interface Type**

Accounting

Enter the type of the listening interface. (Default: Authentication)

**IP Version**

IPv4

Enter the IP version of the listening interface. (Default: IPv4)

**Description**

Capital Portal Accounting

Optionally enter a description here for your reference.

 Save

### General Configuration

**Interface IP Address**

\*

Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose \* then it means

**Port**

1816

Enter the port number of the listening interface. Different interface types need different

**Interface Type**

Status

Enter the type of the listening interface. (Default: Authentication)

**IP Version**

IPv4

Enter the IP version of the listening interface. (Default: IPv4)

**Description**

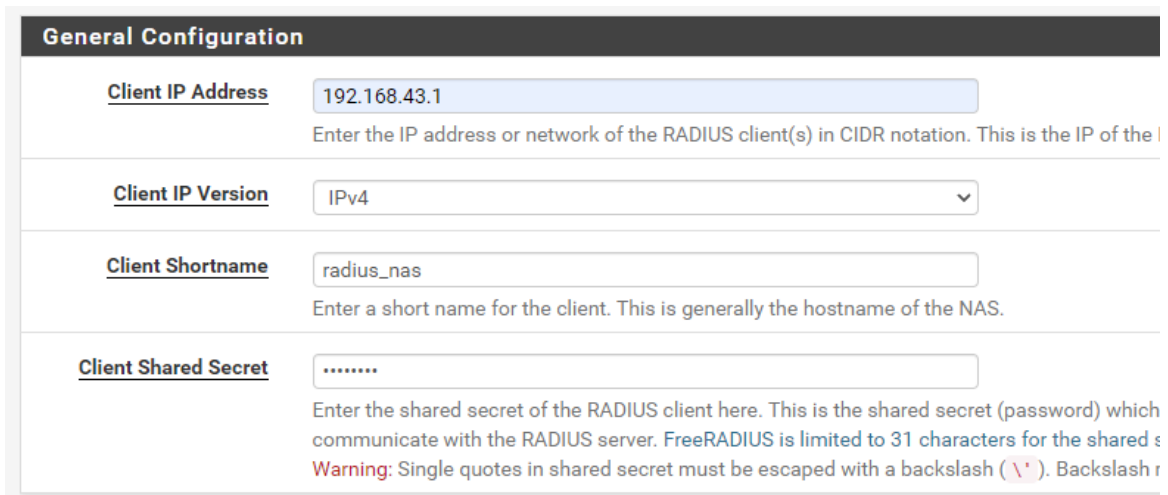
Capital Portal Status

Optionally enter a description here for your reference.

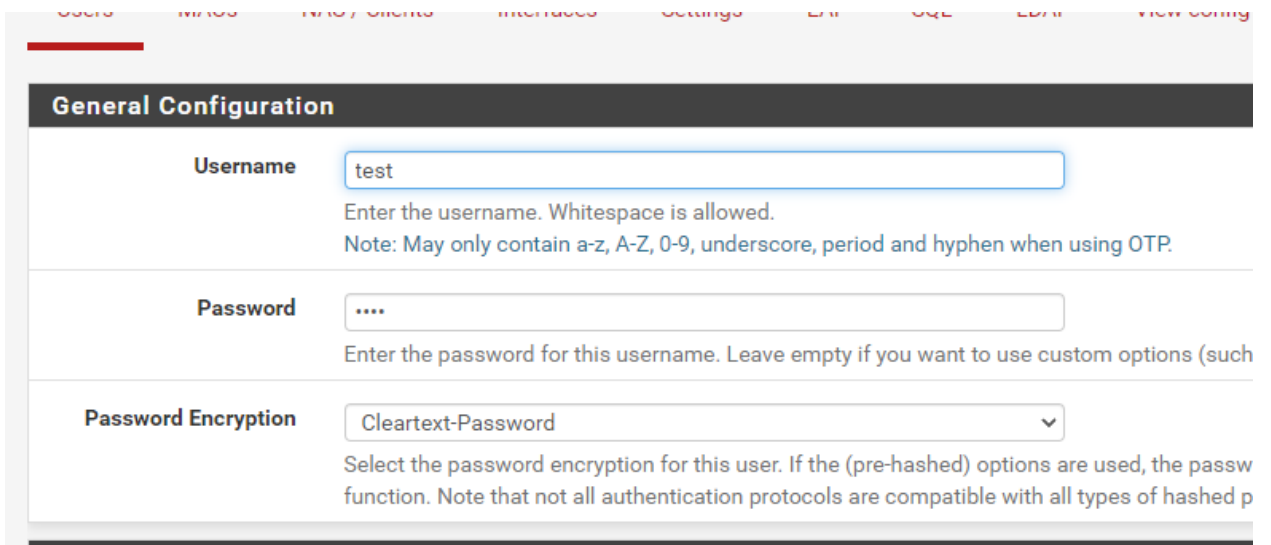
Ở Service Free Radius > chọn tiếp NAS/Client

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

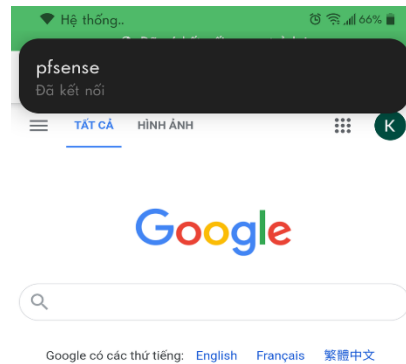
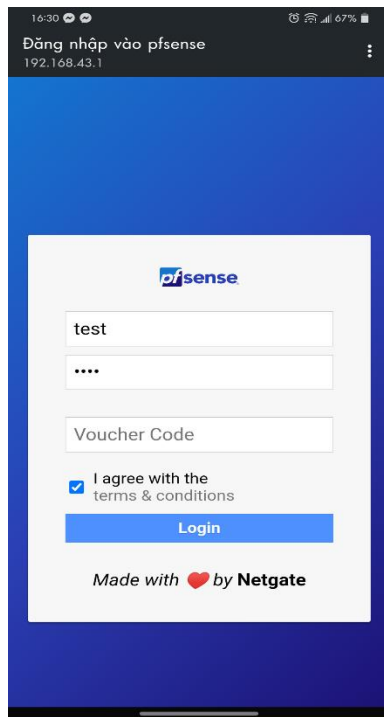
The screenshot shows the 'Authentication' configuration page in PfSense. It has two main sections: 'Authentication Method' and 'Authentication Server'. In the 'Authentication Method' section, a dropdown menu is set to 'Use an Authentication backend'. Below it, instructions state that one method must be selected, and lists three options: 'Authentication backend' (forces login page and authenticates), 'None' (forces login page but accepts any visitor), and 'RADIUS MAC Authentication' (tries to authenticate devices automatically). In the 'Authentication Server' section, a dropdown menu shows 'Captive Portal Radius' as the selected option, with 'Local Database' as an alternative. Below this, a note says 'You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.'

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

The screenshot shows the 'Authentication Test' page in PfSense. At the top, a green message box states 'User test authenticated successfully. This user is a member of groups:'. Below this is the 'Authentication Test' section. It contains three fields: 'Authentication Server' (a dropdown menu set to 'Captive Portal Radius'), 'Username' (a text box containing 'test'), and 'Password' (a text box with masked characters '....'). At the bottom of the section is a blue button with a key icon and the text 'Test'.



## Kiểm tra trên thiết bị của Client



## Trên Pfsense phần Status đã xuất hiện user “test”

Status / Captive Portal / Wifi\_captive\_portal / Active Users

Active UsersActive VouchersVoucher RollsTest VouchersExpire Vouchers

Users Logged In (1)

IP address	MAC address	Username	Session start
192.168.43.12	48:60:5f:67:66:a0	test	10/27/2021 16:35:06

+ Show

### **PHẦN III. Tài Liệu Tham Khảo.**

- [1] Video Youtube: [pfsense Captive Portal](#)
- [2] Video Youtube: [Pfsense 2.5 tutorial: how to create captive portal on Pfsense](#)
- [3] Video Youtube: [Update: FreeRadius and Captive Portal Customization on Pfsense 2.4.4](#)