

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG CƠ SỞ
THÀNH PHỐ HỒ CHÍ MINH**



Cấu Hình Captive Portal pfSense

Báo Cáo Cuối Kỳ

Nhóm 11:

N18DCAT014: Lê Khánh Duy (Nhóm trưởng)

N18DCAT074: Lê Phạm Công Toàn

N18DCAT089: Lê Xuân Thu

N18DCAT034: Phạm Chí Kiên

N18DCAT049: Huỳnh Lê Minh Luân

TP.HCM - 2021

Mục lục

| | |
|--|----|
| 1. Giới thiệu về Captive Portal | 2 |
| 2. Tính năng, ứng dụng của Captive Portal..... | 2 |
| 3. Cách thực hiện cấu hình Captive Portal pfSense | 4 |
| ○ Đầu tiên, hãy cùng nhìn mô hình mà chúng ta sẽ triển khai..... | 4 |
| ○ Cấu hình chung cho tất cả các loại chứng thực | 5 |
| ○ Cấu hình Captive Portal xác thực người dùng sử dụng Local Database | 7 |
| ○ Cấu hình Captive Portal xác thực người dùng sử dụng Voucher | 15 |
| ○ Cấu hình Captive Portal xác thực người dùng sử dụng DaloRadius..... | 18 |

Nội dung

1. Giới thiệu về Captive Portal

- **Captive Portal** là một trang Web trung gian, dùng để bảo vệ hệ thống mạng. Khi người dùng muốn tham gia vào hệ thống mạng sẽ được yêu cầu nhập tên và mật khẩu hợp lệ (đôi khi chỉ cần click tham gia), chức năng này thường được sử dụng ở những hệ thống mạng không dây.
- **Captive portal pfsense** mang đến một giải pháp cấu hình dễ dàng. Sử dụng một trang trung gian để yêu cầu người dùng chứng thực, giúp nâng cao khả năng bảo mật. Trang Web trung gian này có thể thiết kế đơn giản, với hướng dẫn và điều khoản sử dụng, hoặc sử dụng ô Username và Password để đăng nhập.
- Như đã trình bày ở trên, những hệ thống mạng Wifi thường sử dụng **Captive portal** nhiều nhất. Tại những sân bay hoặc khách sạn, khi kết nối vào hệ thống mạng Wifi, thường xuất hiện màn hình Captive portal, chúng ta phải bấm vào nút truy cập để có thể truy cập Internet. Ngày càng phổ biến hơn, captive portal cũng có thể được dùng tại văn phòng, quán cafe, hoặc nhà ở.
- Khi đã **cấu hình captive portal pfsense**, bất cứ máy tính nào sử dụng pfSense làm gateway đều được chuyển hướng đến trang portal đích.

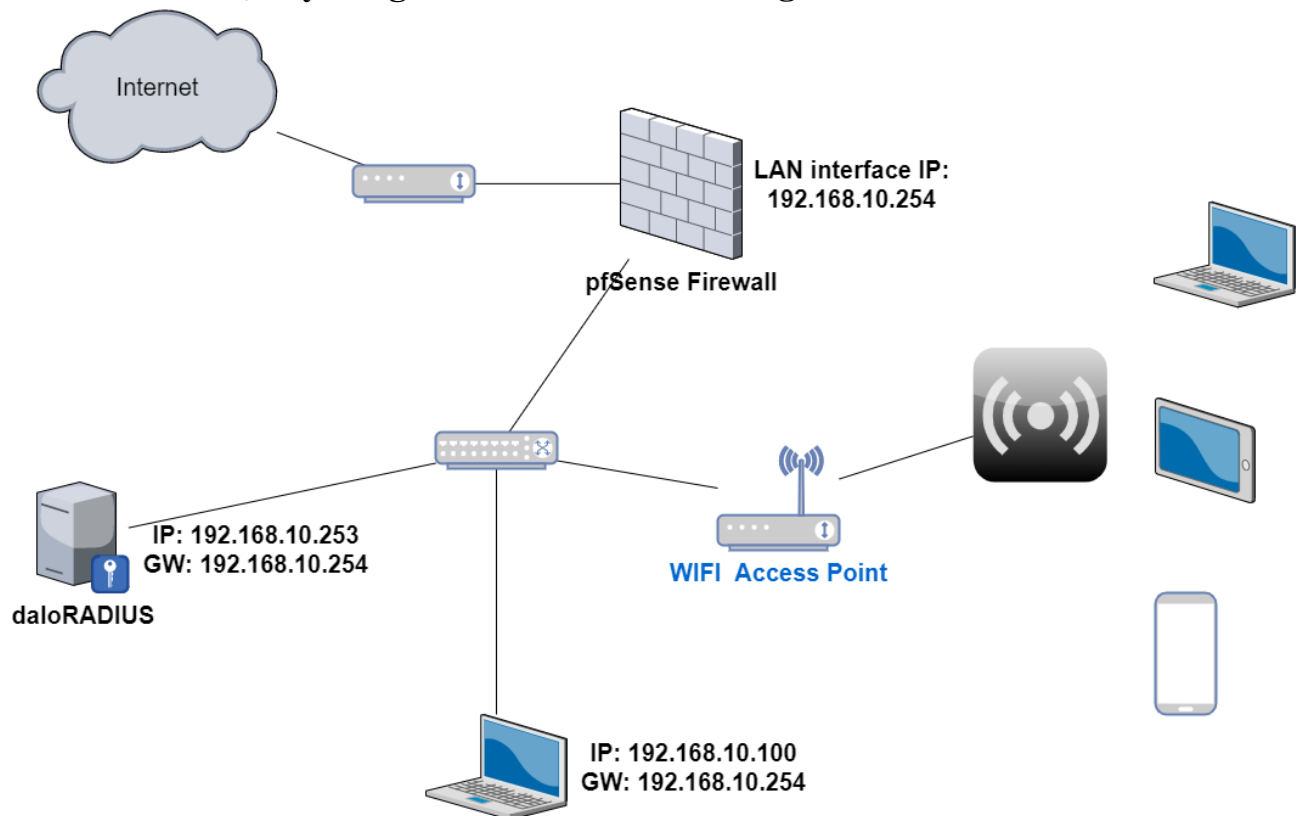
2. Tính năng, ứng dụng của Captive Portal

- Trong thực tế, **Captive Portal** được biết đến với cái tên đầy hoa mỹ **Wi-Fi Marketing** bởi vì nó được ứng dụng khá nhiều trong vai trò marketing. Ngày nay, **Wi-Fi Marketing** được cung cấp và sử dụng trong nhiều doanh nghiệp từ lớn tới nhỏ. **WiFi Marketing** là một trong những cách sáng tạo và hiệu quả nhất để quảng cáo thương hiệu. Bằng cách truyền đạt thông điệp hoặc nội dung trực tiếp tới khách hàng tiềm năng hoặc người dùng gần điểm phát.

- Như đã được đề cập ở nội dung phần giới thiệu về **Captive Portal**. Qua việc tạo ra một vùng phủ sóng dựa trên công nghệ không dây WiFi cho phép bất cứ ai có thiết bị di động (laptop, điện thoại smartphone, máy tính bảng Tablet...) Được trang bị công nghệ WiFi để kết nối và truy cập các dịch vụ hoặc nội dung đã được được cung cấp sẵn.
- Hệ thống trong giải pháp **WiFi Marketing** tạo điều kiện cho khách hàng truy cập miễn phí. Nhưng trước tiên họ phải điều hướng request tới nội dung của một trang website mà chúng ta đã chuẩn bị sẵn. Ở đây chúng ta sẽ có cơ hội hiển thị cho họ sản phẩm, dịch vụ của ta đã và đang cung cấp, khuyến mãi hoặc đơn giản là thông tin liên quan đến doanh nghiệp của mình.
- Những lợi ích của giải pháp **Captive Portal** đem lại khi được ứng dụng vào thực tế:
 - Xây dựng thương hiệu:
 - Các tin tức, thông tin, hình ảnh về doanh nghiệp sẽ nằm dưới quyền kiểm soát của mình bằng việc tùy chỉnh trang website mà người buộc phải truy cập tới khi muốn sử dụng internet.
 - Tiếp cận quảng cáo của khách hàng:
 - Quảng cáo sẽ được tiếp cận tới người sử dụng khi họ truy cập và sử dụng Wi-Fi
 - Là giải pháp đa giải pháp:
 - Được thể hiện qua việc cung cấp website được hỗ trợ bởi nhiều thiết bị Table, Smartphone và Laptop, PC.
 - Giới hạn băng thông người sử dụng:
 - Để tránh các vấn đề có thể bị lạm dụng. Ta có thể kiểm soát lưu lượng sử dụng internet của người dùng. Nhờ vậy mà băng thông sẽ được chia sẻ một cách hợp lý tới người sử dụng.
 - Quản lý phiên hoạt động:
 - Thời gian kết nối của một người sử dụng có thể điều chỉnh bất cứ lúc nào. Có thể thiết lập thời gian sử dụng khác nhau cho mọi người. Ta luôn có sự lựa chọn để thay đổi các thiết lập.
 - Công thông tin điện tử:
 - Ta có thể lợi dụng website mà Captive Portal sử dụng để xác thực để tạo lên một trang tin tức nội bộ.

3. Cách thực hiện cấu hình Captive Portal pfSense

- Đầu tiên, hãy cùng nhìn mô hình mà chúng ta sẽ triển khai.



- Máy **pfSense** có 2 card mạng:
 - **Card 1:** Kết nối ra Internet (VMnet 0 Bridge với tùy chọn **Intel(R) Wireless-AC 9560 160MHz**). IP sẽ do modem ra Internet cấp tự động
 - **Card 2:** Kết nối với Access Point để phát WIFI và dùng để cấu hình **pfSense** bằng giao diện (VMnet 8 Bridge với tùy chọn **Realtek PCIe GbE Family Controller**). Đặt IP là 192.168.100.1/24, cấp **DHCP** tự động cho Access Point và phát Wifi
- Máy **Client** có 1 card mạng:
 - **Card 1:** Kết nối với **LAN**, dùng để cấu hình **pfSense** (VMnet 8 Bridge với tùy chọn **Realtek PCIe GbE Family Controller**)
- Máy **daloRADIUS** có 1 card mạng:
 - **Card 1:** Kết nối với **LAN**, dùng để tạo mới, lưu trữ và quản lý các tài khoản đăng nhập vào **Captive Portal** (VMnet 8 Bridge với tùy chọn **Realtek PCIe GbE Family Controller**)
- Em có thử tìm cách phát WIFI bằng card **Intel(R) Wireless-AC 9560 160MHz** nhưng trong máy ảo Vmware sẽ không thể phát đc WIFI do Vmware không có quyền truy cập trực tiếp vào bộ điều hợp mạng WIFI.



MOD **wila** Leadership

08-27-2021 02:47 AM



Hi,

That's expected...

Your Windows 10 VM does not get direct access to the wifi network adapter.

Instead it is presented a virtual wired network adapter, where the wire is also virtual.

If you want to use this feature then you would have to use an external usb wifi adapter and pass the USB wifi directly to the the virtual machine.

The easier alternative is to use your mac as a hotspot instead:

<https://www.howtogeek.com/214053/HOW-TO-TURN-YOUR-MAC-INTO-A-WI-FI-HOTSPOT/>

edit: note that the article mentions that you cannot create a hotspot if you are only connected by WiFi (I don't know if this still applies, I never used this myself)

--

Wil

| Author of Vimalin. The virtual machine Backup app for VMware Fusion, VMware Workstation and Player |

| More info at vimalin.com | Twitter [@wilva](https://twitter.com/wilva)



- **Cấu hình chung cho tất cả các loại chứng thực**
 - Thực hiện enable DHCP Server. Điều này là cần thiết nếu như ta cung cấp sử dụng tính năng kết hợp với Wi-Fi cho các thiết bị không dây và tránh trường hợp các thiết bị sử dụng có địa chỉ IP giống nhau gây phát sinh lỗi. Tại giao diện Web Interface quản lý của pfSense. Ta chọn **Services** rồi chọn **DHCP Server**. Hãy thực hiện điền thông tin tương tự như hình dưới sau đó chọn **Save** để lưu lại cấu hình.

Services / DHCP Server / LAN

LAN

General Options

| | |
|---------------------------|---|
| Enable | <input checked="" type="checkbox"/> Enable DHCP server on LAN interface |
| BOOTP | <input type="checkbox"/> Ignore BOOTP queries |
| Deny unknown clients | <input type="text" value="Allow all clients"/> <p>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</p> |
| Ignore denied clients | <input type="checkbox"/> 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 | <input type="checkbox"/> 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 | 192.168.10.0 |
| Subnet mask | 255.255.255.0 |
| Available range | 192.168.10.1 - 192.168.10.254 |
| Range | <input type="text" value="192.168.10.100"/> <input type="text" value="192.168.10.200"/> From To |

| Additional Pools | | | |
|-------------------------------|---|-------------|---------|
| Add | <div>+ Add pool</div> <p>If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.</p> | | |
| Pool Start | Pool End | Description | Actions |
| | | | |
| Servers | | | |
| WINS servers | <div>WINS Server 1</div> <div>WINS Server 2</div> | | |
| DNS servers | <div>DNS Server 1</div> <div>DNS Server 2</div> <div>DNS Server 3</div> <div>DNS Server 4</div> <p>Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.</p> | | |
| Other Options | | | |
| Gateway | <div>192.168.10.254</div> <p>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.</p> | | |
| Domain name | <div></div> <p>The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.</p> | | |
| Domain search list | <div></div> <p>The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.</p> | | |
| Default lease time | <div></div> <p>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</p> | | |
| Maximum lease time | <div></div> <p>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</p> | | |
| Failover peer IP | <div></div> <p>Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).</p> | | |
| Static ARP | <input type="checkbox"/> Enable Static ARP entries This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface. | | |
| Time format change | <input type="checkbox"/> Change DHCP display lease time from UTC to local time By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time. | | |
| Statistics graphs | <input type="checkbox"/> Enable RRD statistics graphs Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default. | | |
| Ping check | <input type="checkbox"/> Disable ping check When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default. | | |
| Dynamic DNS | <div>⚙ Display Advanced</div> | | |
| MAC address control | <div>⚙ Display Advanced</div> | | |
| NTP | <div>⚙ Display Advanced</div> | | |
| TFTP | <div>⚙ Display Advanced</div> | | |
| LDAP | <div>⚙ Display Advanced</div> | | |
| Network Booting | <div>⚙ Display Advanced</div> | | |
| Additional BOOTP/DHCP Options | <div>⚙ Display Advanced</div> | | |
| <div>💾 Save</div> | | | |

Trong đó:

- `192.168.10.254` là địa chỉ IP của pfSense trong LAN
- `192.168.10.100 - 10.10.10.200` là dải địa chỉ IP tự động cấp cho người dùng khi kết nối

○ Cấu hình Captive Portal xác thực người dùng sử dụng Local Database

- Bước 1: Tạo tài khoản người dùng cung cấp cho người sử dụng có thể xác thực để truy cập internet. Cách thực hiện như sau:
 - Chọn **System**, sau đó chọn **User Manager**, tiếp tục chọn **Add** rồi nhập thông tin giống như hình sau:

The screenshot shows the 'Edit' page for a user in the pfSense User Manager interface. The breadcrumb trail at the top is 'System / User Manager / Users / Edit'. The 'Users' tab is selected in the top navigation bar. The 'User Properties' section contains the following fields: 'Defined by' (USER), 'Disabled' (checkbox, unchecked), 'Username' (lkduy), 'Password' (masked with dots), 'Full name' (Le Khanh Duy), 'Expiration date' (empty), 'Custom Settings' (checkbox, unchecked), and 'Group membership' (admins). Below the 'Group membership' field are two buttons: 'Move to "Member of" list' and 'Move to "Not member of" list'. The 'Effective Privileges' section is empty. The 'User Certificates' section is empty. The 'Keys' section contains 'Authorized SSH Keys' (empty) and 'IPsec Pre-Shared Key' (empty). A 'Save' button is at the bottom.

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username lkduy

Password

Full name Le Khanh Duy
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership admins

Not member of Member of

» Move to "Member of" list « Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Effective Privileges

| Inherited from | Name | Description | Action |
|----------------|------|-------------|--------|
|----------------|------|-------------|--------|

+ Add

User Certificates

| Name | CA |
|------|----|
|------|----|

+ Add

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Save

Trong đó, **Username**, **Password** và **Confirm Password** là Tài khoản, Mật khẩu, Nhập lại mật khẩu.

- Chọn **Save** để lưu lại thông tin

Cấu Hình Captive Portal pfSense

- Bước 2. Cấu hình **Captive Portal** bằng các thực hiện như sau:
 - Chọn **Services**, tiếp tục chọn **Captive Portal** sau đó chọn Add. Nhập thông tin tương tự như hình sau để tạo ra Captive Portal Zone:

Services / Captive Portal / Add Zone

Add Captive Portal Zone

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

Zone description
A description may be entered here for administrative reference (not parsed).

- Chọn **Save & Continue** để lưu lại thông tin.
- Tiếp tục nhập thông tin tương tự như hình dưới đây:

Services / Captive Portal / Nhom11CaptivePortalWifi / Configuration

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

Interfaces
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.

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 credits per MAC address.
Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Waiting period to restore pass-through credits. (Hours)
Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period ☐ Enable waiting period reset on attempted access
If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window ☒ Enable logout popup window
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication redirect URL
Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURL\$ variable in captiveportal's HTML pages.

After authentication Redirection URL
Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address redirect URL
Blocked MAC addresses will be redirected to this URL when attempting access.

Preserve users database ☐ Preserve connected users across reboot
If enabled, connected users won't be disconnected during a pfSense reboot.

Concurrent user logins
Disabled: Do not allow concurrent logins per username or voucher.
Multiple: No restrictions to the number of logins per username or voucher will be applied.
Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected.
First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.

MAC filtering ☐ Disable MAC filtering
If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Pass-through MAC Auto Entry ☐ Enable Pass-through MAC automatic additions
When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the **MAC** tab or send a POST from another system. If this is enabled, the logout window will not be shown.

Per-user bandwidth restriction ☒ Enable per-user bandwidth restriction

Default download (Kbit/s)

Default upload (Kbit/s)
If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS servers can override the default settings. Leave empty for no limit.

Use custom captive portal page ☐ Enable to use a custom captive portal login page
If set a portal.html page must be created and uploaded. If unchecked the default template will be used

Cấu Hình Captive Portal pfSense

| Captive Portal Login Page | |
|---------------------------------|---|
| Display custom logo image | <input type="checkbox"/> Enable to use a custom uploaded logo |
| Logo Image | <div>Chọn tệp Không tệp nào được chọn</div> <p>Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, it can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.</p> |
| Display custom background image | <input type="checkbox"/> Enable to use a custom uploaded background image |
| Background Image | <div>Chọn tệp Không tệp nào được chọn</div> <p>Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.</p> |
| 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> |
| Authentication | |
| 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">- "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. |
| Authentication Server | <div>daloRADIUS 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> |
| Secondary authentication Server | <div>daloRADIUS Local Database</div> <p>You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.</p> |
| Reauthenticate Users | <input type="checkbox"/> Reauthenticate connected users every minute 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. |
| Local Authentication Privileges | <input type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set |
| HTTPS Options | |
| Login | <input type="checkbox"/> 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

Trong đó:

- **Maximum concurrent connections:** chỉ số lượng người dùng có thể kết nối đồng thời. Ở đây là 50 người.
- **Hard timeout (Minutes):** chỉ thời gian người dùng sẽ tự động bị ngắt kết nối. Ở đây là 60 phút, nếu không muốn dùng tính năng này thì để trống không nhập giá trị nào cả.

- **Logout popup window:** Cho phép một cửa sổ hiện lên để người dùng có thể tự ngắt kết nối.
- **Concurrent user logins:** Quy định tài khoản người dùng chỉ có thể đăng nhập trên một thiết bị vào cùng một thời điểm. Nếu trong một thời điểm mà có nhiều hơn một tài khoản cùng **Username** được đăng nhập thì thiết bị trước đó sẽ được tự động ngắt kết nối.
- **Per-user bandwidth restriction:** Giới hạn băng thông người dùng. Ở đây, ta giới hạn tốc độ Download là 2048 Kb/s và Upload là 1024 Kb/s cho người dùng.
- **Authentication Method:** Quy định cách thức xác thực người dùng sử dụng Internet. Ở đây ta chọn **Use an Authentication backend** quy định người dùng phải có tài khoản tương tự như Bước 1 ta đã tạo thì mới có thể sử dụng Internet. Chọn **None, Authenticate users** nếu như không cần thiết quá trình xác thực người dùng phải xảy ra.
- Tại mục **Authentication**, ta có thấy dòng nội dung "Allow only users/groups with "Captive portal login" privilege set". Hãy bỏ tích ở ô vuông nếu như ta muốn tất cả mọi người sử dụng đều có thể sử dụng tính năng Captive Portal để có thể truy cập internet. Ngược lại, khi nội dung này được tích, ta cần phải cấp quyền cho người dùng.

Authentication

Authentication Method

Use an Authentication backend

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.

Authentication Server

daloRADIUS
Local Database

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.

Secondary authentication Server

daloRADIUS
Local Database




You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users
☐ Reauthenticate connected users every minute

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.

Local Authentication Privileges
☐ Allow only users/groups with "Captive portal login" privilege set

- Chọn **Save** để lưu lại cấu hình. Kết quả ta thu được:

| Services / Captive Portal | | | | |
|---------------------------|------------|-----------------|--|---|
| Captive Portal Zones | | | | |
| Zone | Interfaces | Number of users | Description | Actions |
| Nhom11CaptivePortalWifi | LAN | 0 | Chung thuc Captive Portal voi Wifi Nhom 11 |   |
| | | | |  Add |

- Để cấp quyền cho người dùng chỉ sử dụng tính năng **Captive Portal**, ta thực hiện như sau:
 - Bước 1. Chọn menu **System**, sau đó chọn **User Manager**. Tại đây, ta sẽ thực hiện cấp quyền cho người dùng có **Username** là **lkduy** đã tạo ra trước đó. Nhấp double vào dòng người dùng **lkduy**. Tại mục Effective Privileges ta thấy:

| Effective Privileges | | | |
|----------------------|------|-------------|--------|
| Inherited from | Name | Description | Action |
| | | | |

- Chọn **Add** để thêm mới một quyền.
- Bước 2. Tại đây, ta thấy được như sau:

System / User Manager / Users / Edit / Add Privileges

Users
Groups
Settings
Authentication Servers

User Privileges

User

lkduy (Le Khanh Duy)

Assigned privileges

System - HA node sync
User - Config: Deny Config Write
User - Notices: View
User - Notices: View and Clear
User - Services: Captive Portal login
User - System: Copy files (scp)
User - System: Copy files to home directory (chrooted scp)
User - System: Shell account access
User - System: SSH tunneling
User - VPN: IPsec xauth Dialin
User - VPN: L2TP Dialin
User - VPN: PPPoE Dialin
WebCfg - AJAX: Get Queue Stats
WebCfg - AJAX: Get Service Providers
WebCfg - AJAX: Get Stats
WebCfg - All pages
WebCfg - Crash reporter
WebCfg - Dashboard (all)
WebCfg - Dashboard widgets (direct access).
WebCfg - Diagnostics: ARP Table

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter

Show only the choices containing this term

Privilege information

The following privileges effectively give the user administrator-level access because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:

User - System: Copy files (scp)
User - System: Shell account access
System - HA node sync
WebCfg - All pages
WebCfg - Diagnostics: Backup & Restore
WebCfg - Diagnostics: Command
WebCfg - Diagnostics: Configuration History
WebCfg - Diagnostics: Edit File
WebCfg - Diagnostics: Factory defaults
WebCfg - OpenVPN: Servers Edit Advanced
WebCfg - OpenVPN: Client Specific Override Edit Advanced
WebCfg - OpenVPN: Clients Edit Advanced
WebCfg - System: Authentication Servers
WebCfg - System: Group Manager
WebCfg - System: Group Manager: Add Privileges
WebCfg - System: User Manager
WebCfg - System: User Manager: Add Privileges
WebCfg - System: User Manager: Settings

Please take care when granting these privileges.

Save

Filter

Clear

- Tìm tới **Filter** ta nhập **Captive Portal login** nhấn Enter để thực hiện tìm kiếm quyền. Sau đó nhấp chuột vào **User - Services: Captive Portal login** để chọn quyền:

System / User Manager / Users / Edit / Add Privileges

Users Groups Settings Authentication Servers

User Privileges

User Ikduy (Le Khanh Duy)

Assigned privileges

User - Services: Captive Portal login

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Filter Captive Portal login
Show only the choices containing this term

Privilege information

The following privileges effectively give the user administrator-level access because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:

- User - System: Copy files (scp)
- User - System: Shell account access
- System - HA node sync
- WebCf - All pages
- WebCf - Diagnostics: Backup & Restore
- WebCf - Diagnostics: Command
- WebCf - Diagnostics: Configuration History
- WebCf - Diagnostics: Edit File
- WebCf - Diagnostics: Factory defaults
- WebCf - OpenVPN: Servers Edit Advanced
- WebCf - OpenVPN: Client Specific Override Edit Advanced
- WebCf - OpenVPN: Clients Edit Advanced
- WebCf - System: Authentication Servers
- WebCf - System: Group Manager
- WebCf - System: Group Manager: Add Privileges
- WebCf - System: User Manager
- WebCf - System: User Manager: Add Privileges
- WebCf - System: User Manager: Settings

Please take care when granting these privileges.

Save **Filter** **Clear**

- Sau đó chọn **Save** để lưu lại. Kết quả, ta nhận được:

| Effective Privileges | | | |
|----------------------|---------------------------------------|--|--------------|
| Inherited from | Name | Description | Action |
| | User - Services: Captive Portal login | Indicates whether the user is able to login on the captive portal. | |
| | | | + Add |

Tiếp tục chọn **Save** để lưu lại.

- Về cơ bản, thì chúng ta đã thực hiện cấu hình thành công đối với **Captive Portal**. Nhấp double chuột vào dòng **Nhom11CaptivePortalWifi** để chỉnh sửa cấu hình nâng cao nếu như chúng ta muốn. Tại giao diện, ta sẽ thấy 3 tab là **Allowed IP Addresses** và **Allowed Hostnames**, **MACs**. Chức năng trong hai tab này là gì?

Services / Captive Portal / Nhom11CaptivePortalWifi / Configuration

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

- Thứ nhất, đối với tab **Allowed IP Addresses** ta có thể thực hiện quy định dải các địa chỉ IP hoặc các IP có thể tự do truy cập internet mà không cần phải trải qua quá trình xác thực và có thể thực hiện giới hạn băng thông đối với IP hay dải IP ta quy định. Thông thường, ta sẽ thực hiện cấu hình với từng địa chỉ IP nhiều hơn so với dải địa chỉ IP. Để thực hiện cấu hình, tại tab **Allowed IP Addresses** ta chọn **Add**. Nhập thông tin tương tự như hình sau:

Edit Captive Portal IP Rule

| | | |
|-----------------------|---|------|
| IP Address | <input type="text" value="192.168.10.100"/> | / 24 |
| Description | <input type="text" value="Cho phép ip này không cần xác thực"/> <small>Enter a description here for reference only. (Not parsed)</small> | |
| Direction | Both <small>Use "From" to always allow access to an address through the captive portal (without authentication). Use "To" to allow access from all clients (even non-authenticated ones) behind the portal to this IP.</small> | |
| Bandwidth up | <input type="text"/> <small>Enter an upload limit to be enforced on this address in Kbit/s</small> | |
| Bandwidth down | <input type="text"/> <small>Enter a download limit to be enforced on this address in Kbit/s</small> | |

Save

Trong hình, ta thực hiện cho phép thiết bị có địa chỉ IP 192.168.10.100/24 tự do truy cập Internet mà không cần phải xác thực. Không có giới hạn về băng thông đối với IP này.

- Thứ hai, đối với tab **Allowed Hostnames** có chức năng tương tự như **Allowed IP Addresses** nhưng áp dụng đối với các **Hostnames** được sử dụng trong trường hợp thiết bị không sử dụng địa chỉ IP tĩnh vì vậy mà ta không thể biết được địa chỉ IP để của thiết bị mà cấu hình trong tab **Allowed IP Addresses**. Để thực hiện cấu hình, tại tab **Allowed Hostnames** ta chọn **Add**. Nhập thông tin tương tự như hình sau:

Captive Portal Hostname Settings

| | |
|-----------------------|---|
| Direction | Both <small>Use "From" to always allow a Hostname through the captive portal (without authentication). Use "To" to allow access from all clients (even non-authenticated ones) behind the portal to this Hostname.</small> |
| Hostname | <input type="text" value="DESKTOP-8B3EU46"/> |
| Description | <input type="text" value="Đây là hostname của máy client dùng để cấu hình pfSense"/> <small>A description may be entered here for administrative reference (not parsed).</small> |
| Bandwidth up | <input type="text"/> <small>Enter an upload limit to be enforced on this Hostname in Kbit/s</small> |
| Bandwidth down | <input type="text"/> <small>Enter a download limit to be enforced on this Hostname in Kbit/s</small> |

Save

Trong hình, ta thực hiện cho phép thiết bị có tên là **DESKTOP-8B3EU46** không cần phải xác thực khi truy cập internet.

- Thứ ba, đối với tab **MACs**. có chức năng tương tự như **Allowed IP Addresses** nhưng áp dụng đối với MAC thay vì IP.
- Lưu ý:
 - Để cấu hình thành công, các thiết bị khi kết nối phải xác thực, các thiết bị trong kết nối đến phải có DNS là địa chỉ của pfSense trong mạng LAN.

```
C:\Users\lkduy>hostname
DESKTOP-8B3EU46

C:\Users\lkduy>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:




    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::79fa:876c:9b75:d717%14
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254
```

Đây là hostname và ip của máy client đã cấu hình trong các bước **Allowed IP Addresses** và **Allowed Hostnames**



- Kiểm tra kết quả**
 - Nhập thông tin tài khoản người dùng mà ta đã tạo được ở Bước 1. Kết quả là client đã có thể truy cập internet. Thực hiện truy cập internet tới 1 website bất kỳ, ta thấy được như sau:

The screenshot shows a mobile device screen with a captive portal login page on the left and a website on the right. The login page has a blue header with the pfSense logo and a white box containing the username 'lkduy' and a masked password '.....'. Below the password field is a blue 'Login' button. At the bottom of the login page, it says 'Made with ❤ by Netgate'. The website on the right is the homepage of the Hanoi University of Technology (HUT), featuring a blue header with the university's name in Vietnamese and English, and a white body with various news items and a large announcement about the 2020-2021 academic year.

- **Cấu hình Captive Portal xác thực người dùng sử dụng Voucher**
- Xác thực người dùng trong Captive Portal sử dụng Voucher là quá trình cho phép người dùng trong LAN truy cập internet khi sở hữu một khóa - tương ứng với một ticket trong voucher mà không cần đến phải có tài khoản người dùng.
- Để thực hiện cấu hình sử dụng voucher, ta bắt buộc phải làm các công việc cấu hình Captive Portal như bên trên (ngoại trừ việc tạo mới người dùng) trước tiên. Sau đó thực hiện cấu hình xác thực tài khoản người dùng như sau:
 - Bước 1. Tại giao diện **Captive Portal**, thực hiện nhấp double chuột vào **Captive Portal Zones** muốn sử dụng để cấu hình cho tính năng Voucher. Ví dụ ở đây là zone **Nhom11CaptivePortalWifi**:

| Services / Captive Portal | | | | |
|---------------------------|------------|-----------------|--|---|
| Captive Portal Zones | | | | |
| Zone | Interfaces | Number of users | Description | Actions |
| Nhom11CaptivePortalWifi | LAN | 2 | Chung thuc Captive Portal voi Wifi Nhom 11 |   |
| | | | |  Add |

- Bước 2. Ta chuyển sang tab **Vouchers**. Tích chọn vào **Enable the creation, generation and activation of rolls with vouchers** để sử dụng tính năng cho zone. Ta thấy được như sau:

| Create, Generate and Activate Rolls with Vouchers | |
|--|---|
| Voucher Public Key | <pre>-----BEGIN PUBLIC KEY----- MCQWdQYJKoZIhvcNAQEBBQADAwEAIJAI2nc5tt1J1ZagMBAAE= -----END PUBLIC KEY-----</pre> <p>Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers. </p> |
| Voucher Private Key | <pre>-----BEGIN RSA PRIVATE KEY----- MD4CAQACCQCNp30bbZ5dlwQIDAQABAggF8zgZCaMZFWIFAMjULp8CBQC0 ekKHAgQq 4gKbAgR3xP9ZAgUatqJAMQ== -----END RSA PRIVATE KEY-----</pre> <p>Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline.</p> |
| Character set | <input type="text" value="0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"/> <p>Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.</p> |
| # of Roll bits | <input type="text" value="16"/> <p>Reserves a range in each voucher to store the Roll # it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size.</p> |
| # of Ticket bits | <input type="text" value="16"/> <p>Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage.</p> |
| # of Checksum bits | <input type="text" value="16"/> <p>Reserves a range in each voucher to store a simple checksum over Roll # and Ticket#. Allowed range is 0..31.</p> |
| Magic number | <input type="text" value="367534305"/> <p>Magic number stored in every voucher. Verified during voucher check. Size depends on how many bits are left by Roll+Ticket+Checksum bits. If all bits are used, no magic number will be used and checked.</p> |
| Invalid voucher message | <input type="text" value="Voucher invalid"/> <p>Error message displayed for invalid vouchers on captive portal error page (\$PORTAL_MESSAGES).</p> |
| Expired voucher message | <input type="text" value="Voucher expired"/> <p>Error message displayed for expired vouchers on captive portal error page (\$PORTAL_MESSAGES).</p> |
|  Save | |

- Tại mục **Character set**, ta thay đổi các giá trị sẵn có bởi giá trị sau:
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#\$%^&()_~
đây là dãy các ký tự sẽ được sử dụng để sinh ra key - voucher.
- Lần lượt thay các giá trị tương ứng giống với hình sau đây hoặc giữ nguyên hoặc thay đổi các giá trị sao cho tổng của 3 giá trị nhỏ hơn 64 một cách tùy ý:

| | | |
|--------------------|---------------------------------|---|
| # of Roll bits | <input type="text" value="16"/> | Reserves a range in each voucher to store the Roll # it belongs to. Allowed range: 1..31. Sum of Roll+Ticket+Checksum bits must be one Bit less than the RSA key size. |
| # of Ticket bits | <input type="text" value="16"/> | Reserves a range in each voucher to store the Ticket# it belongs to. Allowed range: 1..16. Using 16 bits allows a roll to have up to 65535 vouchers. A bit array, stored in RAM and in the config, is used to mark if a voucher has been used. A bit array for 65535 vouchers requires 8 KB of storage. |
| # of Checksum bits | <input type="text" value="16"/> | Reserves a range in each voucher to store a simple checksum over Roll # and Ticket#. Allowed range is 0..31. |

chọn **Save** để lưu lại.

- Tiếp theo, ta cần phải tạo ra một **roll** chứa các ticket - là một chuỗi ký tự sẽ cung cấp cho người sử dụng để có thể truy cập internet thay vì ta cung cấp tài khoản. Tại phần **Voucher Rolls**, ta chọn **Add**:

| Voucher Rolls | | | | |
|---------------|----------------|--------------|---------|-----------------------|
| Roll # | Minutes/Ticket | # of Tickets | Comment | Actions |
| | | | | + Add |




- Nhập các giá trị tương ứng giống như hình sau:

| | |
|---------------------------|--|
| Voucher Rolls | |
| Roll # | <input type="text" value="1"/> Enter the Roll# (0..65535) found on top of the generated/printed vouchers |
| Minutes per ticket | <input type="text" value="60"/> 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 | <input type="text" value="1000"/> Enter the number of vouchers (1..65535) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again |
| Comment | <input type="text"/> Can be used to further identify this roll. Ignored by the system. |
| Save | |




trong đó:

- Roll:** Định danh cho roll.
- Minutes per ticket:** Quy định thời gian có hiệu lực của mỗi voucher đó kể từ khi nó được sử dụng. Ở đây là 60 phút.
- Count:** Quy định số voucher sẽ được tạo ra. Ở đây là 1000 voucher. Nếu như of Ticket bits ta đã cấu hình có giá trị là 16 thì số voucher có thể được sinh ra lên đến 65536 voucher.

Chọn **Save** để lưu lại, kết quả ta thu được tương tự như sau:

| Voucher Rolls | | | | |
|---------------|----------------|--------------|---------|---|
| Roll # | Minutes/Ticket | # of Tickets | Comment | Actions |
| 1 | 60 | 1000 | |    |

- Export roll để có thể biết được thông tin về các voucher được tạo ra bằng việc thực hiện chọn **Export vouchers for this roll to a .csv file** tương ứng của mỗi roll:

| Voucher Rolls | | | | |
|---------------|----------------|--------------|---------|---|
| Roll # | Minutes/Ticket | # of Tickets | Comment | Actions |
| 1 | 60 | 1000 | |    |

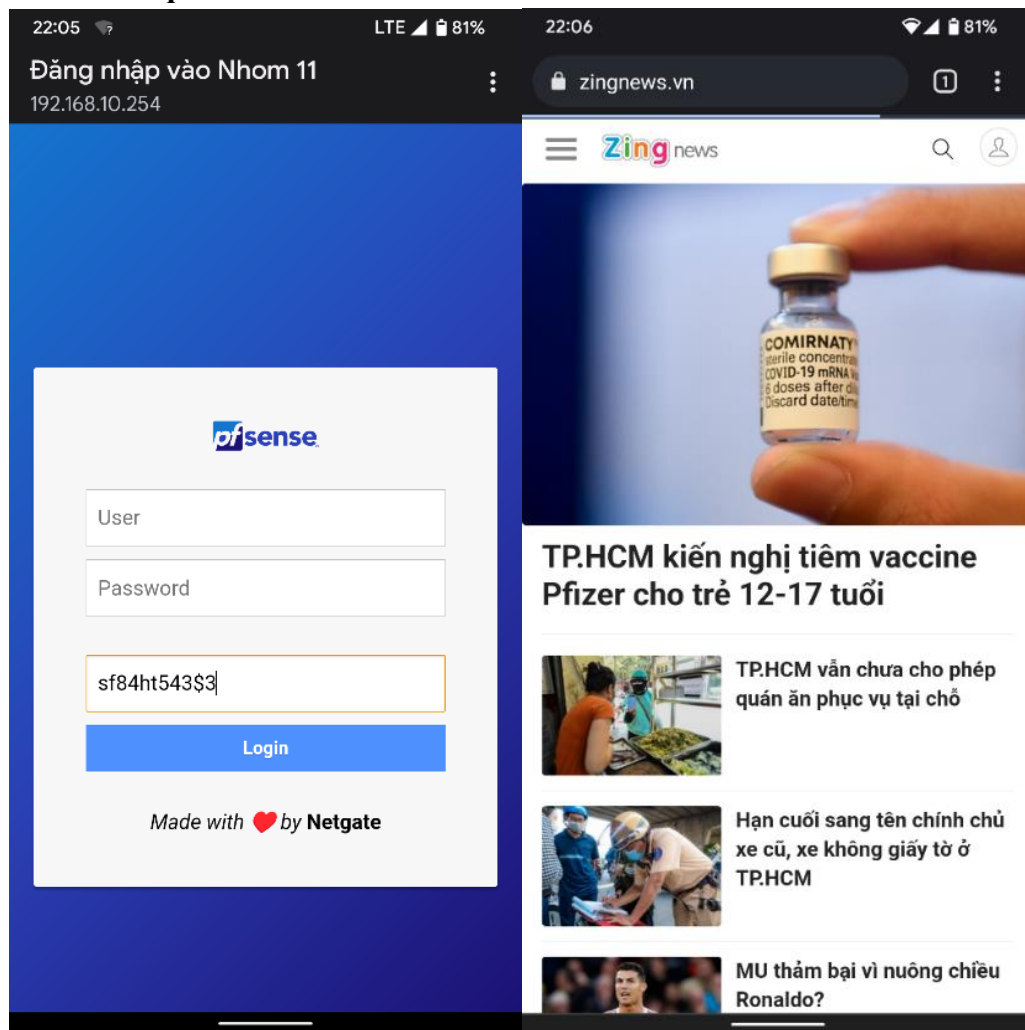
Ta sẽ cần tải về một file *.csv có tên theo dạng "vouchers_zoneName_rollid.csv". Trong đó zoneName và rollid lần lượt là tên của Captive Portal Zone và định danh của roll.

- Mở file đã download bằng Microsoft Excel hoặc các phần mềm soạn thảo khác như Notepad(Wordpad) đối với Windows hay Vim đối với Linux để có thể thu được giá trị của các voucher. Ta thu được kết quả tương tự như sau:

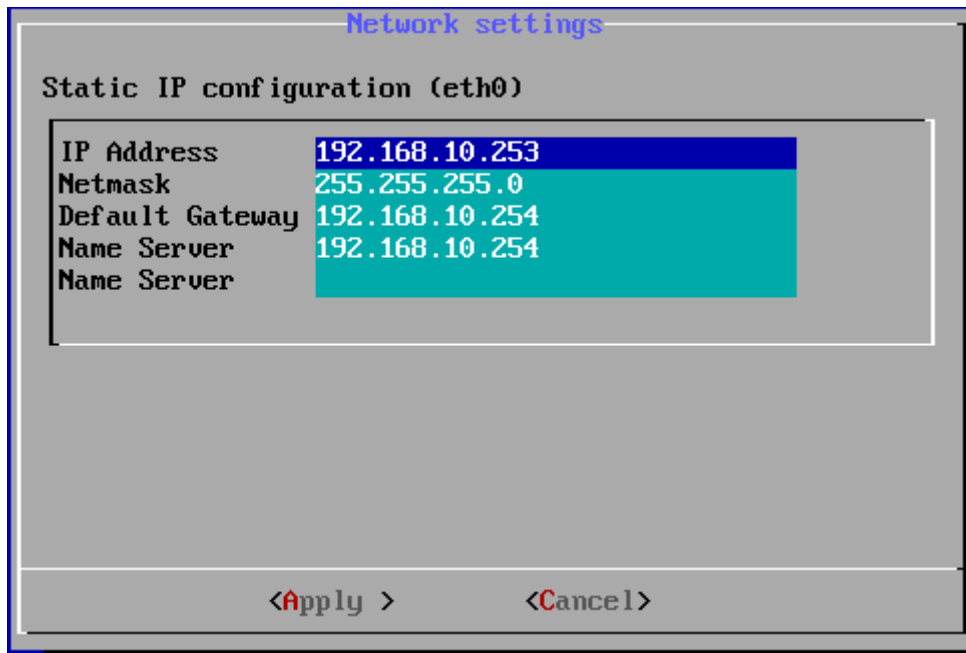
```
# Voucher Tickets 1..1000 for Roll 1
# Nr of Roll Bits      16
# Nr of Ticket Bits   16
# Nr of Checksum Bits 16
# magic initializer    8417 (15 Bits used)
# Character Set used   0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#$%^&()._~
#
" MdVKM&JBwR2"
" C~bV9@KTv(1"
" PHj!Hz21Gc"
" evHFGt~mpF2"
" ^M@w@AJe0K"
" hC_Bt2%6j41"
" QrsFM&F9Ke3"
" reh(Wc@LmS3"
" ku2WdtzKxG2"
" ^D0dv1D9KD"
" 8N78)U6zAq1"
" D8xtE)m)4m2"
" njYLvGJMf21"
" 461NFsNuT(2"
" $wJFq~!8uH2"
" xF~z_MtU^D3"
" $_SXExuyuG"
" UKR_$HVGAX"
" 7dy@!ivfca1"
" )J$jcTc^#f"
" 9!4&SfdjDL3"
" MPNP4JLyNm2"
" RSHvL%^!a"
```

Ta thấy được các chuỗi voucher được quy định bắt đầu từ dòng thứ 8 cho đến hết. Mỗi voucher tương ứng với 1 dòng. Chúng sẽ được ta sử dụng để cung cấp cho người có nhu cầu sử dụng internet trong WIFI.

- **Kiểm tra kết quả**



- **Cấu hình Captive Portal xác thực người dùng sử dụng DaloRadius**
- Dịch vụ Captive Portal trên PfSense có thể sử dụng các phương thức chứng thực như local user và RADIUS với Domain User trên Windows. Ngoài ra chúng ta còn có thể triển khai dịch vụ Captive Portal chứng thực bằng freeRADIUS. Về bản chất, freeRADIUS hoạt động tương tự như RADIUS. FreeRADIUS là dịch vụ được phát triển trên nền tảng nguồn mở nên việc sử dụng cũng tương đối phức tạp hơn so với nền tảng Windows. Để đơn giản trong sử dụng người ta phát triển các ứng dụng quản lý cho freeRADIUS, trong bài này chúng ta sẽ làm quen với một ứng dụng như vậy đó là daloRadius.
- DaloRadius là phần mềm được phát triển trên nền web php và mysql, ta có thể tự cài đặt chúng bằng tay, tuy nhiên việc cài đặt hơi phức tạp nên trong bài này chúng ta sẽ sử dụng ứng dụng đã được cài đặt sẵn trên máy ảo.
- Sau khi import máy ảo daloRADIUS, chúng ta khởi động máy này lên và thiết lập IP cho máy ảo:



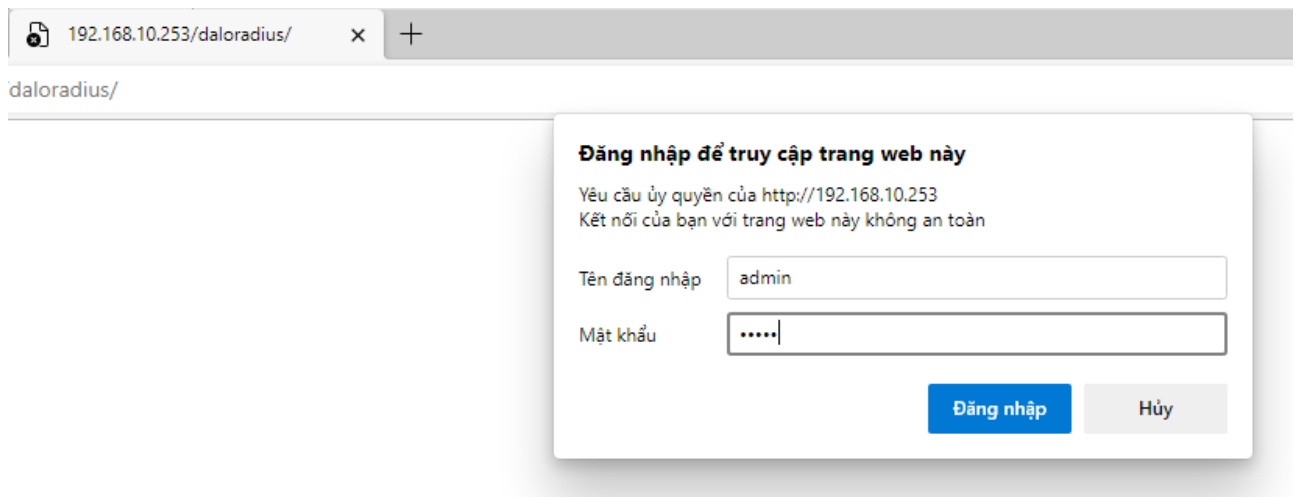
Network settings

Static IP configuration (eth0)

| | |
|-----------------|----------------|
| IP Address | 192.168.10.253 |
| Netmask | 255.255.255.0 |
| Default Gateway | 192.168.10.254 |
| Name Server | 192.168.10.254 |
| Name Server | |

<Apply> <Cancel>

- Sau khi **ban** thiết lập xong địa chỉ IP, ta có thể kết nối đến máy ảo bằng giao diện web, username và password mặc định là admin. Bước này chứng thực của web service trên máy ảo daloRADIUS.



192.168.10.253/daloradius/

daloradius/

Đăng nhập để truy cập trang web này

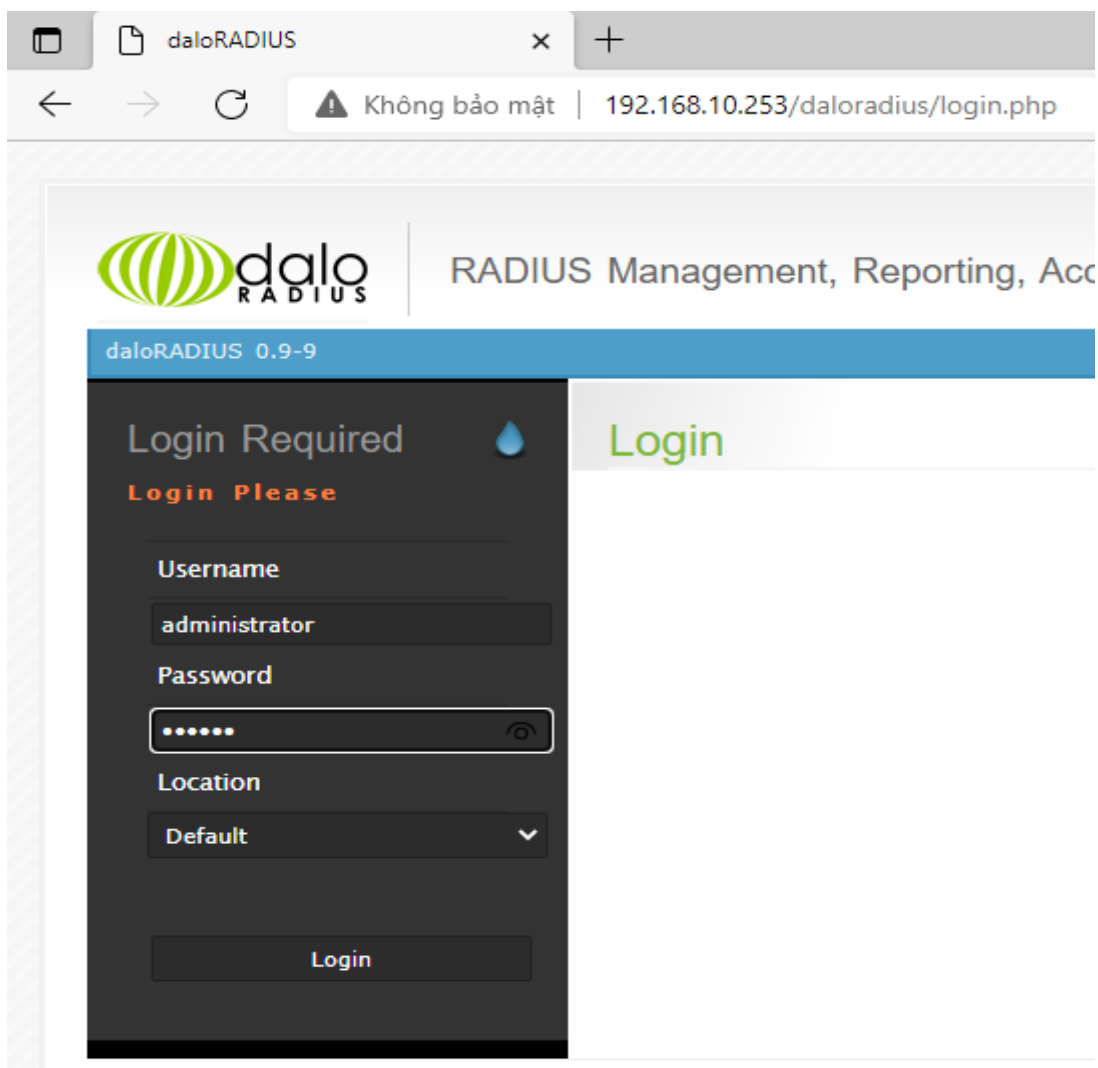
Yêu cầu ủy quyền của http://192.168.10.253
Kết nối của bạn với trang web này không an toàn

Tên đăng nhập: admin

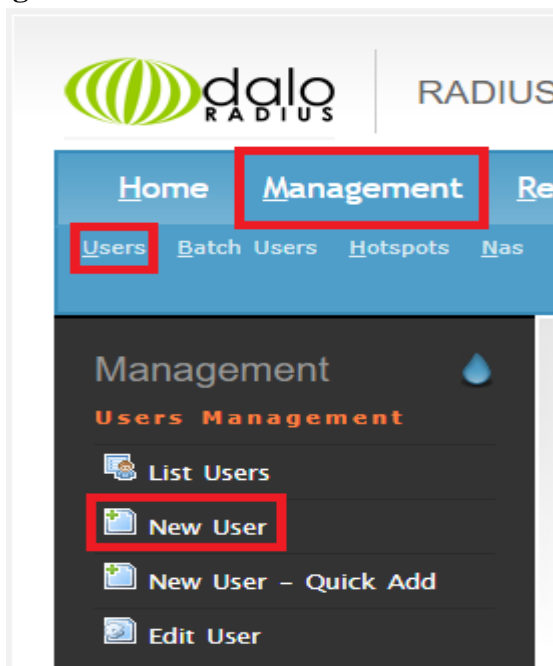
Mật khẩu:

Đăng nhập Hủy

- Tiếp theo, ta sẽ vào giao diện quản lý của daloRADIUS với username **administrator** và password mặc định là **radius**. Bước này chứng thực để vào ứng dụng quản lý daloRADIUS.



- Tiếp theo, ta có thể thêm các user dùng để chứng thực người dùng thông qua daloRADIUS bằng cách vào **Management > Users > New User**



- Ta điền các thông tin user:

New User +

Account Info User Info Billing Info Attributes

☐ Username Authentication

Username: user1 [Random]

Password: 123456789 [Random]

Password Type: Cleartext-Password

Group: Select Groups [Add]

[Apply]

- Tiếp theo, chúng ta đưa RADIUS client, chính là máy Pfsense, vào hệ thống quản lý của daloRADIUS, vào menu **Management** > **Nas** > **New NAS**. Chúng ta cần chú ý **NAS Secret** chính là key ta sẽ phải điền trong mục **Share secret** trên Pfsense.

daloRADIUS | RADIUS Management, Reporting, Accounting and Billing by Enginx

Home **Management** Reports Accounting Billing GIS Graphs Config Help

Users Batch Users Hotspots **Nas** User-Groups Profiles HuntGroups Attributes Realms/Proxys IP-Pool

Management

NAS Management

List NAS

New NAS

Edit NAS

Remove NAS

New NAS Record +

NAS Info NAS Advanced

NAS IP/Host: 192.168.10.254

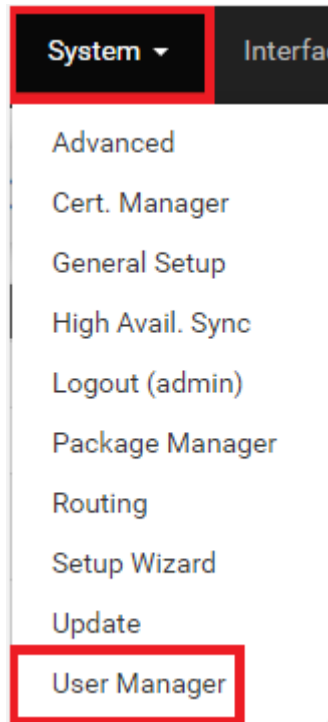
NAS Secret: 123456789

NAS Type: Select Type...

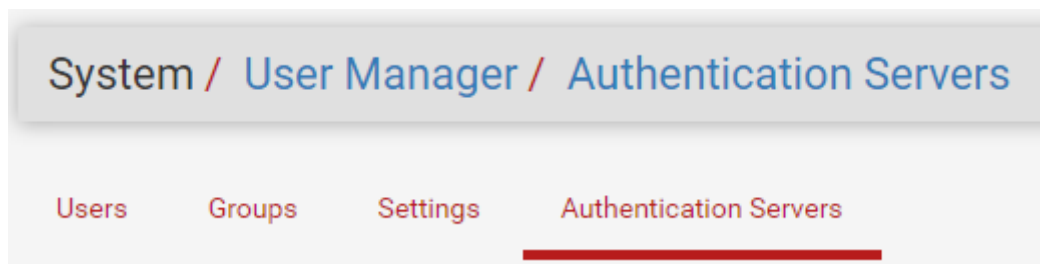
NAS Shortname: pfsense

[Apply]

- Sau khi tạo xong tài khoản và đưa máy Pfsense vào daloRADIUS, chúng ta sẽ cần khởi động máy ảo daloRADIUS một lần để đảm bảo dịch vụ sẽ chạy.
- Thêm phương thức chứng thực bằng daloRADIUS vào pfSense**
 - Truy cập pfSense **System** -> **User Manager**



- Ở màn hình **User Manager**, truy cập tab **Authentication Servers** và bấm vào nút **Add** :



- Ở mục Server settings, thực hiện những cấu hình sau :
 - Descriptive name: daloRADIUS
 - Type: RADIUS

| Server Settings | |
|-------------------------|---|
| <u>Descriptive name</u> | <input type="text" value="daloRADIUS"/> |
| <u>Type</u> | <input type="text" value="RADIUS"/> |

- Ở mục RADIUS Server setting, thực hiện những cấu hình sau :
 - Protocol – PAP
 - Hostname or IP address – 192.168.10.253 đây là địa chỉ IP của máy daloRADIUS
 - Shared Secret – 123456789 đây **NAS Secret** đã tạo ở trên
 - Services Offered – Authentication and Accounting
 - Authentication Port – 1812
 - Accounting Port – 1813

▪ Authentication Timeout – 5

RADIUS Server Settings



| | |
|---|-------------------------------|
| <u>Protocol</u> | PAP |
| <u>Hostname or IP address</u> | 192.168.10.253 |
| <u>Shared Secret</u> | |
| <u>Services offered</u> | Authentication and Accounting |
| <u>Authentication port</u> | 1812 |
| <u>Accounting port</u> | 1813 |
| <u>Authentication Timeout</u> | 5 |
| This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. NOTE: If using an interactive two-factor authentication system, increase this timeout and enter a token. | |
| <u>RADIUS NAS IP Attribute</u> | LAN - 192.168.10.254 |
| Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server. | |

Save

- Bấm vào nút **Save** để kết thúc cấu hình.

- Để thực hiện cấu hình sử dụng daloRADIUS, ta bắt buộc phải làm các công việc cấu hình Captive Portal như sử dụng **Local database** (ngoại trừ việc tạo mới người dùng) trước tiên. Sau đó thực hiện cấu hình xác thực tài khoản người dùng như sau:
 - Bước 1. Tại giao diện **Captive Portal**, thực hiện nhấp double chuột vào **Captive Portal Zones** muốn sử dụng để cấu hình cho tính năng Voucher. Ví dụ ở đây là zone **Nhom11CaptivePortalWifi**:

Services / Captive Portal

| Captive Portal Zones | | | | |
|-------------------------|------------|-----------------|--|---|
| Zone | Interfaces | Number of users | Description | Actions |
| Nhom11CaptivePortalWifi | LAN | 2 | Chung thuc Captive Portal voi Wifi Nhom 11 |   |

+ Add

- Bước 2. Kéo xuống mục **Authentication**, trong **Authentication Method** chọn **Authentication backend** và **Authentication Server** chọn **daloRADIUS**

Cấu Hình Captive Portal pfSense

| Authentication | |
|--|---|
| 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">- "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. |
| Authentication Server | <div>daloRADIUS 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> |
| Secondary authentication Server | <div>daloRADIUS Local Database</div> <p>You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.</p> |
| NAS Identifier | <div></div> <p>Specify a NAS identifier to override the default value (CaptivePortal-nhom11captiveportalwifi)</p> |
| Reauthenticate Users | <div><input type="checkbox"/> Reauthenticate connected users every minute</div> <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> |
| Session timeout | <div><input type="checkbox"/> Use RADIUS Session-Timeout attributes</div> <p>When enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute.</p> |
| Traffic quota | <div><input type="checkbox"/> Use RADIUS pfSense-Max-Total-Octets attribute</div> <p>When enabled, clients will be disconnected after exceeding the amount of traffic, inclusive of both downloads and uploads, retrieved from the RADIUS pfSense-Max-Total-Octets attribute.</p> |
| Per-user bandwidth restrictions | <div><input type="checkbox"/> Use RADIUS pfSense-Bandwidth-Max-Up and pfSense-Bandwidth-Max-Down attributes</div> <p>When enabled, the bandwidth assigned to a client will be limited to the values retrieved from the RADIUS pfSense-Bandwidth-Max-Up and pfSense-Bandwidth-Max-Down attributes or from the comparable WISPr attributes.</p> |
| MAC address format | <div>Default</div> <p>This option changes the MAC address format used when performing a RADIUS authentication.</p> <p>Default: 00:11:22:33:44:55 Single dash: 001122-334455 IETF: 00-11-22-33-44-55 Cisco: 0011.2233.4455 Unformatted: 001122334455</p> |

- Bước 3. Để RADIUS server có thể kiểm toán và report được client, ta tích vào ô **Send RADIUS accounting packet** trong mục **Accounting**.

| Accounting | |
|--------------------------------|--|
| RADIUS | <div><input checked="" type="checkbox"/> Send RADIUS accounting packets.</div> <p>If enabled, accounting request will be made for users identified against any RADIUS server.</p> |
| Accounting Server | <div>daloRADIUS</div> <p>You can add a Radius Accounting server in the User Manager.</p> |
| Send accounting updates | <div><input type="radio"/> No updates <input type="radio"/> Stop/Start <input type="radio"/> Stop/Start (FreeRADIUS) <input type="radio"/> Interim</div> <p>This field set the way Accounting Updates should be done :</p> <ul style="list-style-type: none">- If "No updates" is selected, then only one "Accounting Start" and one "Accounting Stop" request will be sent, when any user get connected and disconnected.- If "Interim" is selected, then "Accounting Update" requests will be send regularly (every minute) to the RADIUS server, for each connected user.- In some rare cases, you would like to simulate users to disconnect and reconnect every minute (eg, to send an Accounting Stop then an Accounting Start) instead of sending Accounting updates, this is the purpose of "Stop/Start" option. FreeRADIUS does not support this option very well, you should select "Stop/Start (FreeRADIUS)" instead. |
| Accounting style | <div><input type="checkbox"/> Invert Acct-Input-Octets and Acct-Output-Octets</div> <p>When enabled, data counts for RADIUS accounting packets will be taken from the client perspective, not the NAS. Acct-Input-Octets will represent download, and Acct-Output-Octets will represent upload.</p> |
| Idle time accounting | <div><input type="checkbox"/> Include idle time when users get disconnected due to idle timeout</div> <p>This setting change the stop time that will be send in the Accounting Stop request, when a user get disconnected after exceeding the idle timeout. If not checked, the sent stop time will be the last activity time.</p> |

- Kiểm tra kết quả

