

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

System / Certificate / Authorities / Edit

Authorities
Certificates
Revocation

Create / Edit CA

Descriptive name

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, '

Method

Import an existing Certificate Authority ▾

Trust Store

☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial

☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
RiIDzjCCAKgAwIBAgIQh9BQJgfhTwwDQYJKoZIhvc
NAQELBQAwZ1EIMCGA1UE
AxQcSVRFU3lzdGVtX0NBX0F19Db21tb25fcmFTZTA
eFwByNTEwMDgwNjQ0NTBa
-----
```

Certificate Private Key (optional)

```
-----BEGIN PRIVATE KEY-----
RiIEvQIBADANBgkqhkiG9w0BAQEFAASCBCkgwSjAgE
AAoIBAQo=BlKc46jQKZz
dtIQXGjYkIqzOD98vlygpXWVzt4j3oZdHGzgdeHf
0FL187WKnPpfx+RXTG5A
-----
```

Next Certificate Serial

Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

Save

Bước 1.2: Tạo Chứng chỉ cho Máy chủ OpenVPN (Server Certificate)

Chứng chỉ này được máy chủ OpenVPN sử dụng để xác định danh tính của nó với các máy khách kết nối đến.

1. Truy cập **System > Cert. Manager > Certificates**.
2. Nhấn **Add/Sign**.
3. **Method**: Chọn "Create an internal Certificate".
4. **Descriptive name**: Đặt tên cho chứng chỉ, ví dụ: IT_System_CA_CER.
5. **Certificate authority**: Chọn CA đã tạo ở Bước 1.1 (IT_System_CA_AU).

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, '.

Internal Certificate

Certificate authority IT_System_CA_AU

Key type RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

6. Điền các thông tin cần thiết. Trong **Common Name**, có thể đặt tên miền hoặc tên của máy chủ pfSense.
7. **Certificate Type**: Chọn "Server Certificate".

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname

Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as

8. Nhấn **Save**.

Lý do: Đảm bảo các máy khách đang kết nối đến đúng máy chủ OpenVPN, tránh các cuộc tấn công xen giữa (Man-in-the-Middle).

Bước 1.3: Tạo Chứng chỉ cho Người dùng (User Certificates)

Mỗi người dùng kết nối VPN sẽ cần một chứng chỉ riêng.

1. Truy cập **System > Cert. Manager > Certificates**.
2. Nhấn **Add/Sign**.
3. **Method**: "Create an internal Certificate".
4. **Descriptive name**: Đặt tên định danh cho người dùng, ví dụ: giahung_client_to_site.
5. **Certificate authority**: Chọn CA đã tạo ở Bước 1.1.
6. **Common Name**: Đặt tên của người dùng, ví dụ: giahung.
7. **Certificate Type**: Chọn "User Certificate".
8. Nhấn **Save**. Lặp lại cho tất cả người dùng khác (quandhp, hiennv, vuongpb).

Lý do: Chứng chỉ người dùng là một yếu tố xác thực, đảm bảo chỉ những người dùng sở hữu chứng chỉ hợp lệ mới có thể khởi tạo kết nối.

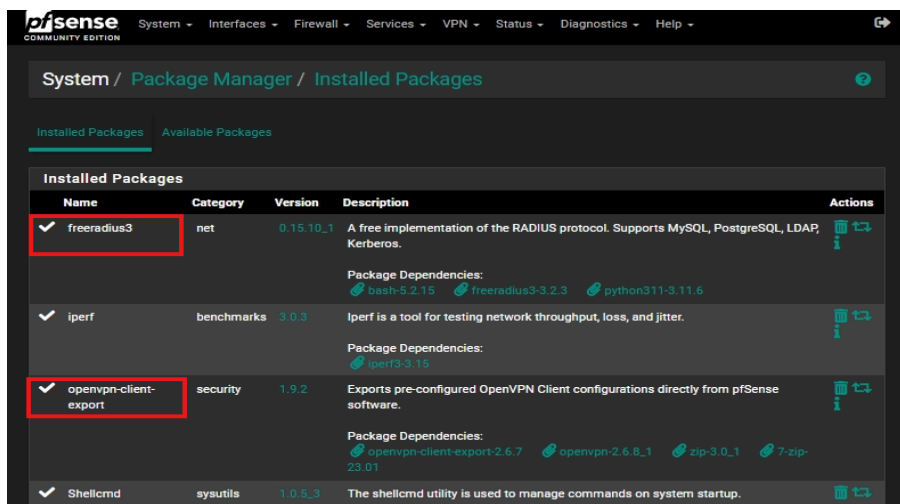
Thật ra khi xác thực bằng Radius thì cái này không cần thiết lắm vì nó chỉ sử dụng cho Client To Site thuần túy, hiện tại sẽ chuyển sang xác thực với Radius Server

Phần 2: Cài đặt và Cấu hình FreeRADIUS

Gói FreeRADIUS trên pfSense sẽ hoạt động như một máy chủ xác thực, quản lý người dùng và quy trình 2FA.

Bước 2.1: Cài đặt gói FreeRADIUS

1. Truy cập **System > Package Manager > Available Packages**.
2. Tìm kiếm freeradius3 và nhấn **Install** để cài đặt.



Bước 2.2: Cấu hình Interfaces của FreeRADIUS

Định cấu hình cổng mà FreeRADIUS sẽ lắng nghe các yêu cầu xác thực.

1. Truy cập **Services > FreeRADIUS > Interfaces**.
2. Nhấn **Add**.
3. **Interface IP Address**: Đặt là * (hoặc 127.0.0.1) để lắng nghe trên tất cả các giao diện (hoặc chỉ giao diện loopback). Trong hạ tầng công ty mình, nó lắng nghe trên 127.0.0.1 vì OpenVPN và FreeRADIUS đều chạy trên cùng một máy pfSense.
4. **Port**: 1812 cho **Authentication** và 1813 cho **Accounting**.
5. Nhấn **Save**.

Lý do: Cần chỉ định cổng để máy chủ OpenVPN biết nơi gửi yêu cầu xác thực người dùng đến FreeRADIUS.

The screenshot shows the 'Services / FreeRADIUS / Edit / Interfaces' page in pfSense. The 'General Configuration' section is highlighted with a red box. It contains the following fields:

- Interface IP Address**: A text input field with a cursor, containing an asterisk (*). Below it is a hint: 'Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)'.
- Port**: A text input field containing '1812'. Below it is a hint: 'Enter the port number of the listening interface. Different interface types need different ports. Click Info for details.'
- Interface Type**: A dropdown menu set to 'Authentication'. Below it is a hint: 'Enter the type of the listening interface. (Default: Authentication)'.
- IP Version**: A dropdown menu set to 'IPv4'. Below it is a hint: 'Enter the IP version of the listening interface. (Default: IPv4)'.
- Description**: A text input field containing 'Radius Auth'. Below it is a hint: 'Optionally enter a description here for your reference.'

A green 'Save' button is at the bottom left of the configuration section.

The screenshot shows the same 'Services / FreeRADIUS / Edit / Interfaces' page, but for an Accounting interface. The 'General Configuration' section is highlighted with a red box. It contains the following fields:

- Interface IP Address**: A text input field with a cursor, containing an asterisk (*). Below it is a hint: 'Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)'.
- Port**: A text input field containing '1813'. Below it is a hint: 'Enter the port number of the listening interface. Different interface types need different ports. Click Info for details.'
- Interface Type**: A dropdown menu set to 'Accounting'. Below it is a hint: 'Enter the type of the listening interface. (Default: Authentication)'.
- IP Version**: A dropdown menu set to 'IPv4'. Below it is a hint: 'Enter the IP version of the listening interface. (Default: IPv4)'.
- Description**: A text input field containing 'Radius Acc'. Below it is a hint: 'Optionally enter a description here for your reference.'

Bước 2.3: Cấu hình NAS / Clients

Định nghĩa máy chủ OpenVPN là một "client" hợp lệ được phép gửi yêu cầu tới FreeRADIUS.

1. Truy cập **Services > FreeRADIUS > NAS / Clients**.
2. Nhấn **Add**.
3. **Client IP Address:** 127.0.0.1 (vì OpenVPN server chạy trên chính pfSense).
4. **Client Shortname:** pfsense_radius_2FA.
5. **Client Shared Secret:** Nhập một chuỗi bí mật phức tạp. Trong cấu hình này là Novaon@#\$2025.

Services / FreeRADIUS / Edit / NAS / Clients

Users MACs **NAS / Clients** Interfaces Settings EAP SQL LDAP View Config XMLRPC Sync

General Configuration

Client IP Address 127.0.0.1
Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).

Client IP Version IPv4

Client Shortname pfsense_radius_2FA
Enter a short name for the client. This is generally the hostname of the NAS.

Client Shared Secret *****
Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.
Warning: Single quotes in shared secret must be escaped with a backslash ('). Backslash must be escaped by using two backslashes (\\).

Miscellaneous Configuration

6. Nhấn **Save**.

Lý do: Shared Secret này giống như một mật khẩu giữa OpenVPN và FreeRADIUS để đảm bảo rằng các yêu cầu xác thực là hợp lệ và đến từ một nguồn đáng tin cậy.

Bước 2.4: Tạo và Cấu hình Người dùng với 2FA

Đây là bước quan trọng nhất để kích hoạt 2FA cho từng người dùng.

1. Truy cập **Services > FreeRADIUS > Users**.
2. Nhấn **Add**.
3. **Username**: Nhập tên người dùng
4. **Password Encryption**: Để là "Cleartext-Password" (RADIUS sẽ xử lý việc mã hóa sau đó).
5. **Kích hoạt One-Time Password (OTP)**: Tích vào ô Enable one-time password (MOTP).
6. **Authentication Method**: Chọn googleauth. Một mã QR và một chuỗi "MOTP init secret" sẽ tự động được tạo.
7. **User PIN**: Đặt một mã PIN cho người dùng (ví dụ: 2025). Đây là phần mật khẩu tĩnh.

One-Time Password Configuration

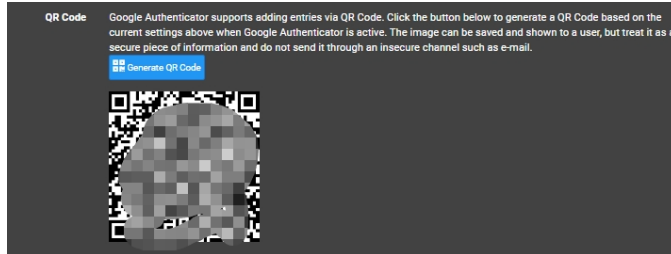
One-Time Password ☒ Enable One-Time Password (OTP) for this user
This enables the possibility to authenticate with username and one-time-password.
The client used to generate OTP can be installed on various mobile device platforms like Android, iOS and others. (Default: unchecked)
IMPORTANT: For MOTP, mOTP must be enabled at [FreeRADIUS > Settings](#).
The RADIUS NAS / Client must use PAP, otherwise the authenticator script cannot use the authentication data.

OTP Auth Method Google-Authenticator
Select the OTP authentication method for this user. Default: mOTP

Init-Secret [REDACTED]
This is the generated init secret you get when you initialize the token for the first time on a client (mobile device).
Note: For mOTP this may only contain 0-9 and a-f. For Google Authenticator, it must be A-Z and 2-7. Must contain at least 16 characters.
[Generate OTP Secret](#) [Show OTP Secret](#)

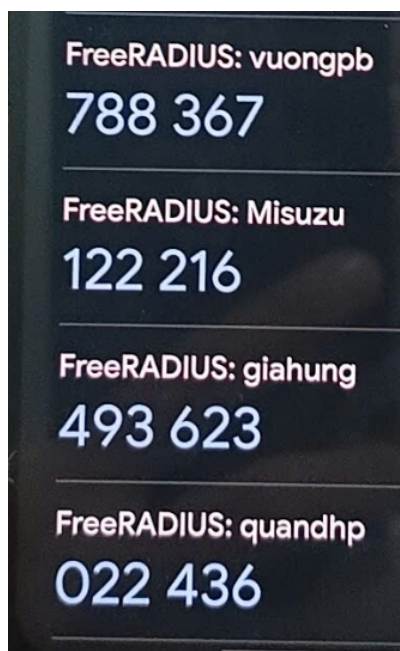
PIN [REDACTED]
This is the PIN the user has to enter on his mobile device to generate a one-time-password.
For Google Authenticator, the user must prepend this PIN to the one-time password generated by the authenticator when logging in (e.g. OTP code "990990", user enters "1234990990" as the password).
[Show OTP PIN](#)

8. **Quét mã QR:** Người dùng cần sử dụng ứng dụng Google Authenticator (hoặc tương tự) trên điện thoại để quét mã QR này. Thao tác này sẽ thêm tài khoản vào ứng dụng của họ để tạo mã OTP.



9. Nhấn **Save**. Lặp lại cho các người dùng khác (vuongpb, hiennv, quandhp).

*Lý do: Bằng cách này, mật khẩu để đăng nhập VPN sẽ là sự kết hợp của **PIN + Mã OTP** (ví dụ: 2025123456). Điều này bổ sung yếu tố "thứ mình có" (điện thoại tạo OTP) vào yếu tố "thứ mình biết" (mã PIN), tăng cường bảo mật đáng kể.*



Phần 3: Cấu hình pfSense Authentication Server

Bước này kết nối hệ thống pfSense với dịch vụ FreeRADIUS vừa cấu hình.

1. Truy cập **System > User Manager > Authentication Servers**.
2. Nhấn **Add**.
3. **Descriptive name**: OpenVPN_Radius_2FA.
4. **Type**: Chọn RADIUS.
5. **Hostname or IP address**: 127.0.0.1.
6. **Shared Secret**: Nhập lại chính xác chuỗi bí mật đã đặt ở Bước 2.3 (Novaon@#\$2025).
7. **Services offering RADIUS authentication**: Ports 1812 (Auth) và 1813 (Acct).
8. **Authentication protocol**: Chọn PAP.
9. Nhấn **Save**.

Lý do: Bước này đăng ký FreeRADIUS như một phương thức xác thực hợp lệ trên pfSense, để các dịch vụ khác (như OpenVPN) có thể sử dụng nó.

pfSense COMMUNITY EDITION

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name OpenVPN_Radius_2FA

Type RADIUS

RADIUS Server Settings

Protocol PAP

Hostname or IP address 127.0.0.1

Shared Secret

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout 5

This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute VLAN11 - 192.168.11.251

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

Phần 4: Cấu hình Máy chủ OpenVPN

Bây giờ chúng ta sẽ tạo máy chủ OpenVPN và liên kết tất cả các thành phần đã thiết lập.

1. Truy cập **VPN > OpenVPN > Servers**.
2. Nhấn **Add**.
3. **Server mode**: "Remote Access (User Auth)".
4. **Backend for Authentication**: Chọn máy chủ RADIUS đã tạo ở Phần 3 (OpenVPN_Radius_2FA).
5. **Protocol**: UDP on IPv4 only.
6. **Interface**: Chọn Gateway Group VNPT_FPT. Điều này cho phép VPN hoạt động trên cả hai đường truyền WAN.

Endpoint Configuration

Protocol

Interface
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port
The port used by OpenVPN to receive client connections.

7. **Local port**: 1194.
8. **Peer Certificate Authority**: Chọn CA đã tạo (IT_System_CA_AU).
9. **Server certificate**: Chọn chứng chỉ máy chủ đã tạo (IT_System_CA_CER).

Cryptographic Settings

TLS Configuration ☒ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

☒ Automatically generate a TLS Key.

Peer Certificate Authority

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check ☐ Check client certificates with OCSP

Server certificate
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

10. **Data Encryption Algorithms:** Chọn các thuật toán mã hóa mong muốn như AES-256-GCM.
11. **Auth digest algorithm:** SHA256.
12. **Tunnel Network:** Nhập dải IP sẽ cấp cho các client khi kết nối, ví dụ: 18.9.6.0/24.
Dải IP này không được trùng với bất kỳ mạng nội bộ nào.

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

13. **Local Network:** Nhập dải IP của mạng nội bộ mà bạn muốn client truy cập sau khi kết nối VPN, ví dụ: 192.168.11.0/24.

IPv4 Local network(s)




IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

14. Nhấn **Save**.

Lý do: Cấu hình này tạo ra một "cổng" VPN, chỉ định cách client kết nối (giao diện, cổng), cách xác thực (RADIUS 2FA), cách mã hóa dữ liệu, và quyền truy cập mạng sau khi kết nối thành công.

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
GW Group VNPT_FPT	UDP4 / 1194 (TUN)	18.9.6.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	IT System OpenVPN Client to Site	  

+ Add

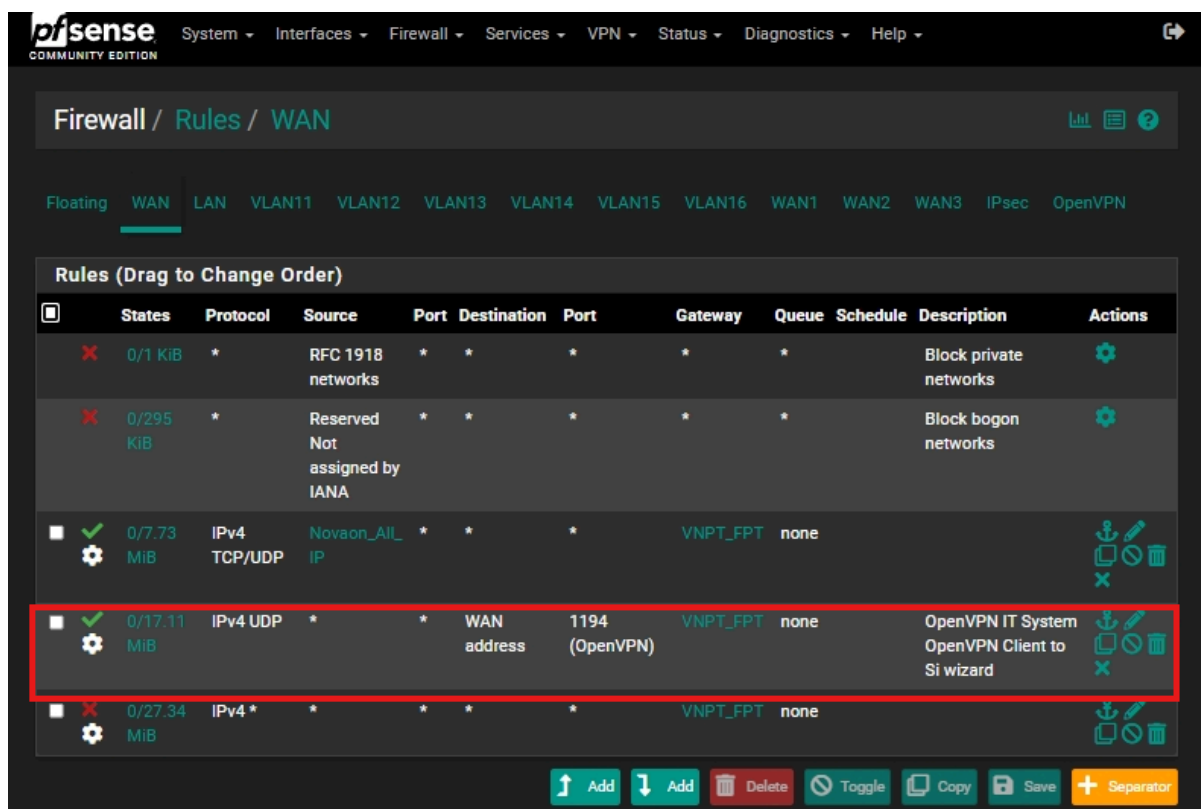
Phần 5: Cấu hình Firewall Rules

Chúng ta cần tạo các quy tắc tường lửa để cho phép lưu lượng truy cập VPN.

Bước 5.1: Tạo Rule trên WAN Interface

Cho phép các kết nối từ Internet đến cổng OpenVPN.

1. Truy cập **Firewall > Rules > WAN**.
2. Nhấn **Add**.
3. **Action:** Pass.
4. **Interface:** WAN.
5. **Protocol:** UDP.
6. **Source:** any.
7. **Destination:** WAN address.
8. **Destination Port Range:** 1194.
9. **Description:** Allow OpenVPN connections.
10. Nhấn **Save**. Lặp lại cho giao diện WAN1 (opt7).



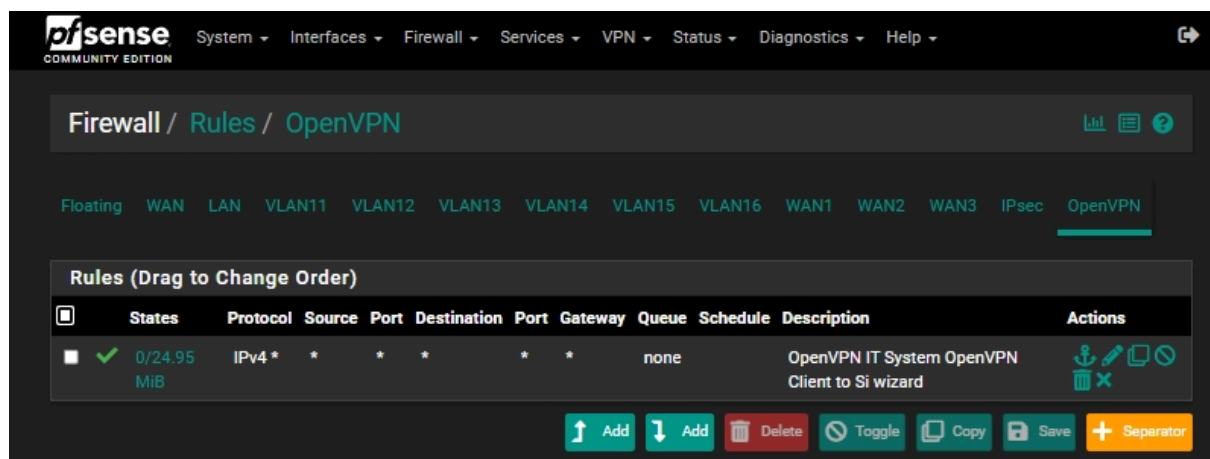
Lý do: Nếu không có quy tắc này, tường lửa pfSense sẽ chặn tất cả các yêu cầu kết nối VPN từ bên ngoài, khiến người dùng không thể kết nối.

Bước 5.2: Tạo Rule trên OpenVPN Interface

Cho phép lưu lượng từ các client đã kết nối VPN đi vào mạng nội bộ.

1. Truy cập **Firewall > Rules > OpenVPN**.
2. Nhấn **Add**.
3. **Action:** Pass.
4. **Interface:** OpenVPN.
5. **Protocol:** any.
6. **Source:** any.
7. **Destination:** any.
8. **Description:** Allow traffic from VPN clients.
9. Nhấn **Save**.

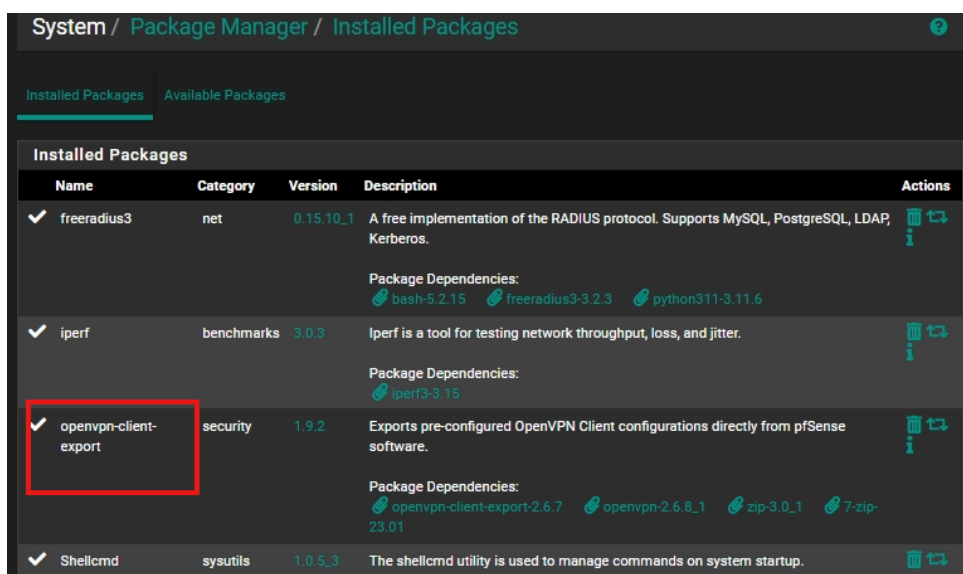
Lý do: Quy tắc này xác định những gì người dùng VPN được phép làm sau khi kết nối thành công. Cấu hình "any to any" cho phép họ truy cập mọi thứ, nhưng có thể giới hạn lại (ví dụ: chỉ cho phép truy cập một số máy chủ nhất định) để tăng cường bảo mật.



Phần 6: Xuất Cấu hình cho Client

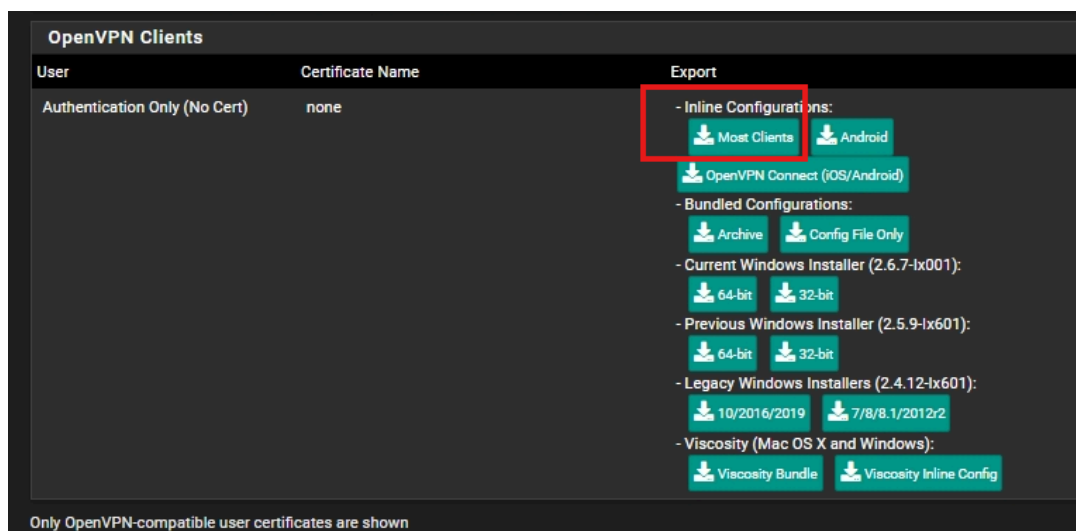
Để người dùng dễ dàng kết nối, hãy sử dụng gói Client Export.

1. Cài đặt gói `openvpn-client-export` từ **System > Package Manager**.



2. Truy cập **VPN > OpenVPN > Client Export**.
3. Tìm người dùng tương ứng trong danh sách và tải về gói cấu hình phù hợp (ví dụ: "Most Clients" cho file .ovpn hoặc "Viscosity" cho macOS).
4. Gửi tệp cấu hình này cho người dùng.

Lý do: Gói này tự động gom chứng chỉ CA, chứng chỉ người dùng, và các thiết lập máy chủ vào một tệp duy nhất, giúp người dùng cuối cài đặt dễ dàng mà không cần cấu hình thủ công.



Phần 7: Quy trình Đăng nhập của Người dùng

1. Người dùng cài đặt OpenVPN client trên máy tính/điện thoại và nhập (import) tệp cấu hình .ovpn.
2. Khi kết nối, ứng dụng sẽ hỏi **Username** và **Password**.
3. **Username:** Nhập tên người dùng của họ (ví dụ: giahung).
4. **Password:** Nhập **PIN** nối liền với **mã OTP** đang hiển thị trên ứng dụng Google Authenticator. Ví dụ, nếu PIN là 2025 và mã OTP là 123456, họ sẽ nhập mật khẩu là 2025123456.
5. Kết nối thành công.

