

**TRIỂN KHAI PHƯƠNG ÁN BACKUP SITE TO SITE TRÊN PFSENSE**

Mục lục

[I. Mô hình triển khai 3](#_Toc88659522)

[II. Mục đích 3](#_Toc88659523)

[III. Cấu hình 3](#_Toc88659524)

[1. Thông tin địa chỉ IP 3](#_Toc88659525)

[2. Cấu hình Pfsense tòa nhà 3A 4](#_Toc88659526)

[3. Cấu hình Pfsense tòa nhà AC 5](#_Toc88659527)

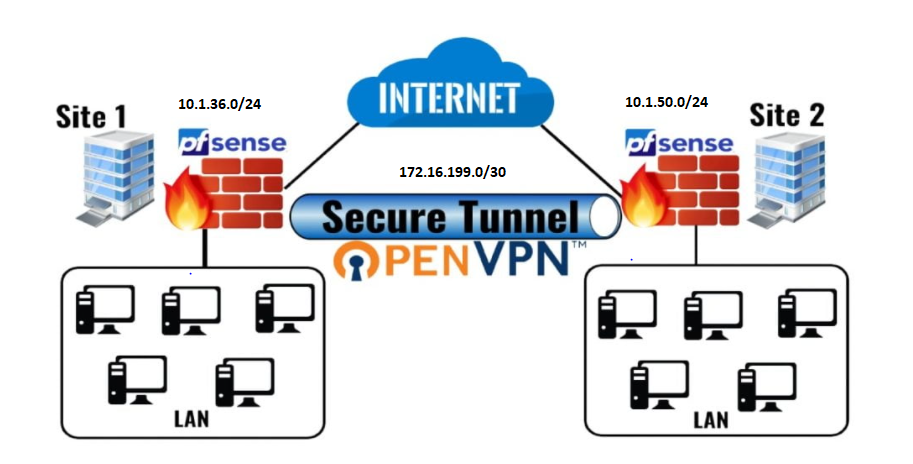
[4. Mở Rule trên Pfsense tòa nhà AC 7](#_Toc88659528)

[5. Mở Rule trên Pfsense tòa nhà 3A 8](#_Toc88659529)

[6. Kiểm tra 8](#_Toc88659530)

[9](#_Toc88659531)

1. **Mô hình triển khai**



1. **Mục đích**

- Cấu hình VPN site-to site trên 2 Firewall Pfsense, khi đường cáp quang mất kết nối  
- Đảm bảo các PC trong LAN của tòa nhà 3A và tòa nhà AC có thể truy cập lẫn nhau sau khi cấu hình VPN thành công

**III. Cấu hình**

* 1. Thông tin địa chỉ IP

|  |  |  |  |
| --- | --- | --- | --- |
| Site A | | Site B | |
| Name | Tòa nhà 3A | Name | Tòa nhà AC |
| WAN IP | 113.164.228.221 | WAN IP | 118.70.128.119 |
| LAN Subnet | 10.1.0.0/24 | LAN Subnet | 10.1.50.0/24 |
| LAN IP | 10.1.36.1 | LAN IP | 10.1.50.1 |
| Tunnel Network | 172.16.199.1 | Tunnel Network | 172.16.199.2 |

* 1. Cấu hình Pfsense tòa nhà 3A

Điều hướng đến VPN -> OpenVPN, Server Tab

Chọn + Add thêm 1 server mới

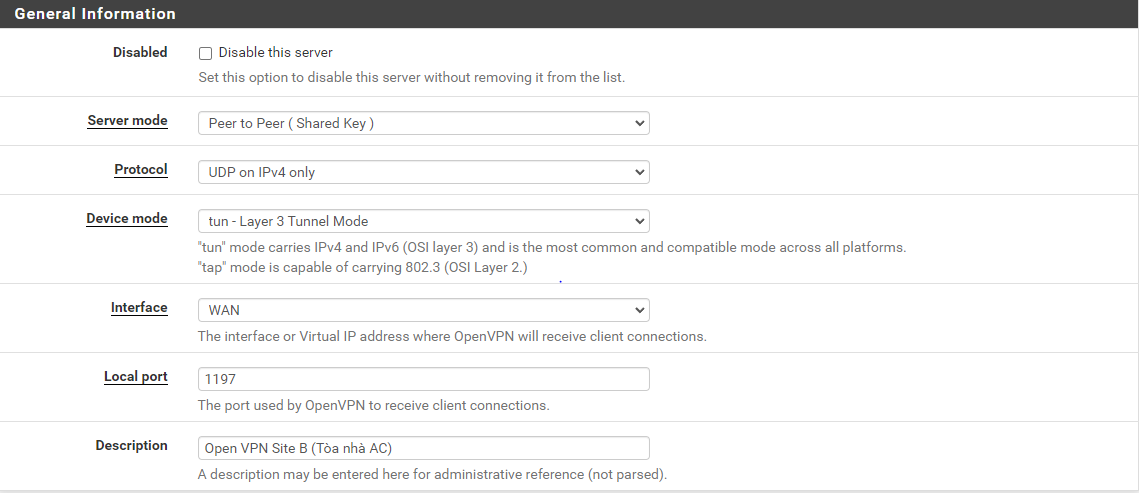


Điền các trường như sau, với các trường khác để ở giá trị mặc định:

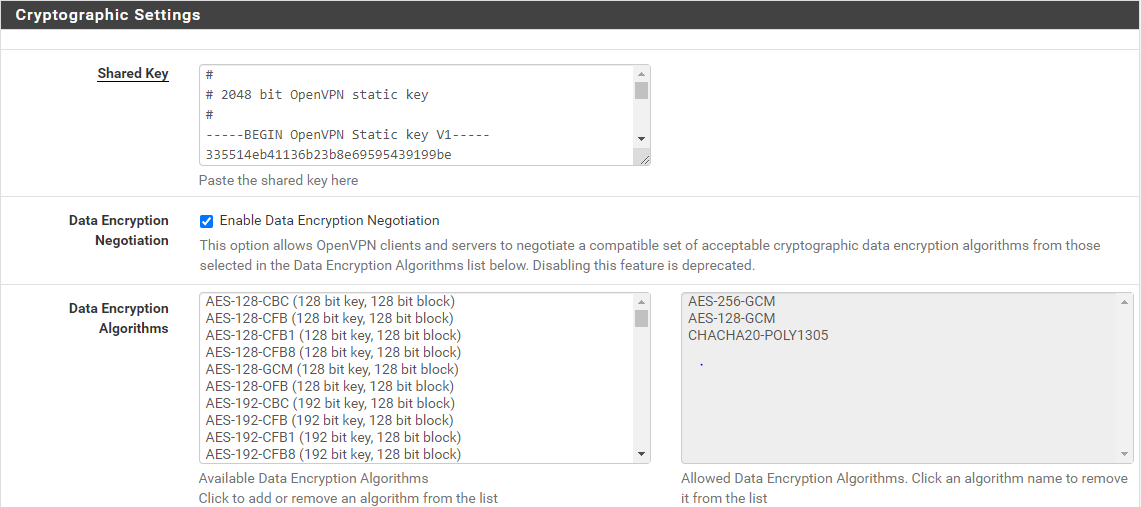
Server Mode: Chọn Peer to Peer (Shared Key)

Local port: 1197

Description: Open VPN Site B (Tòa nhà AC)



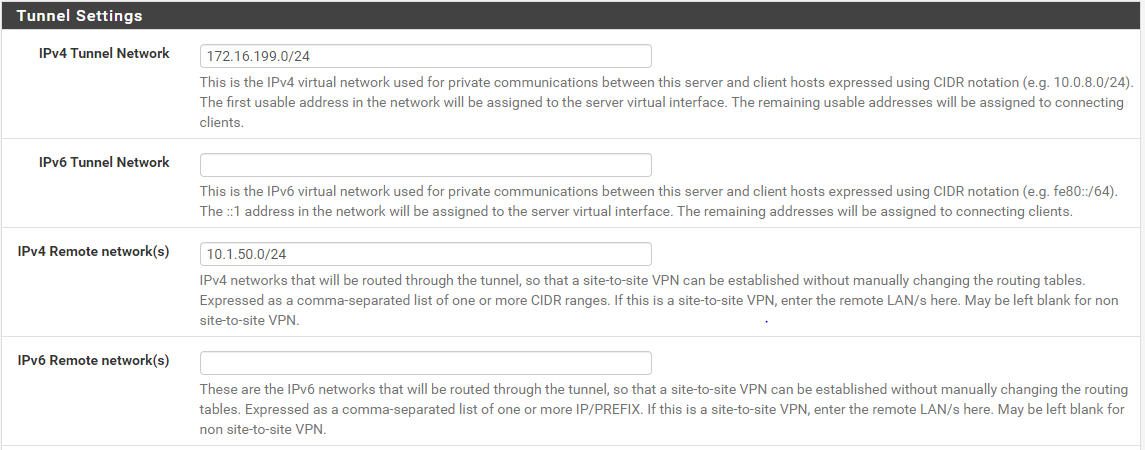
Shared Key: Chọn Automatically generate a shared key



IPv4 Tunnel Network: 172.16.199.0/30

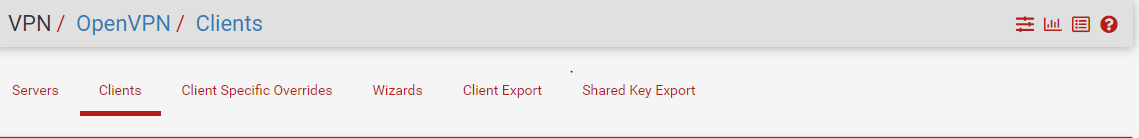
Remote Network: Nhập IP LAN Subnet tòa nhà AC, 10.1.50.0/24

Chọn Save và cấu hình sẽ giống như hình dưới



* 1. Cấu hình Pfsense tòa nhà AC

Điều hướng đến VPN -> OpenVPN, Client Tab



Chọn fa-level-up và tạo 1 OpenVPN Client

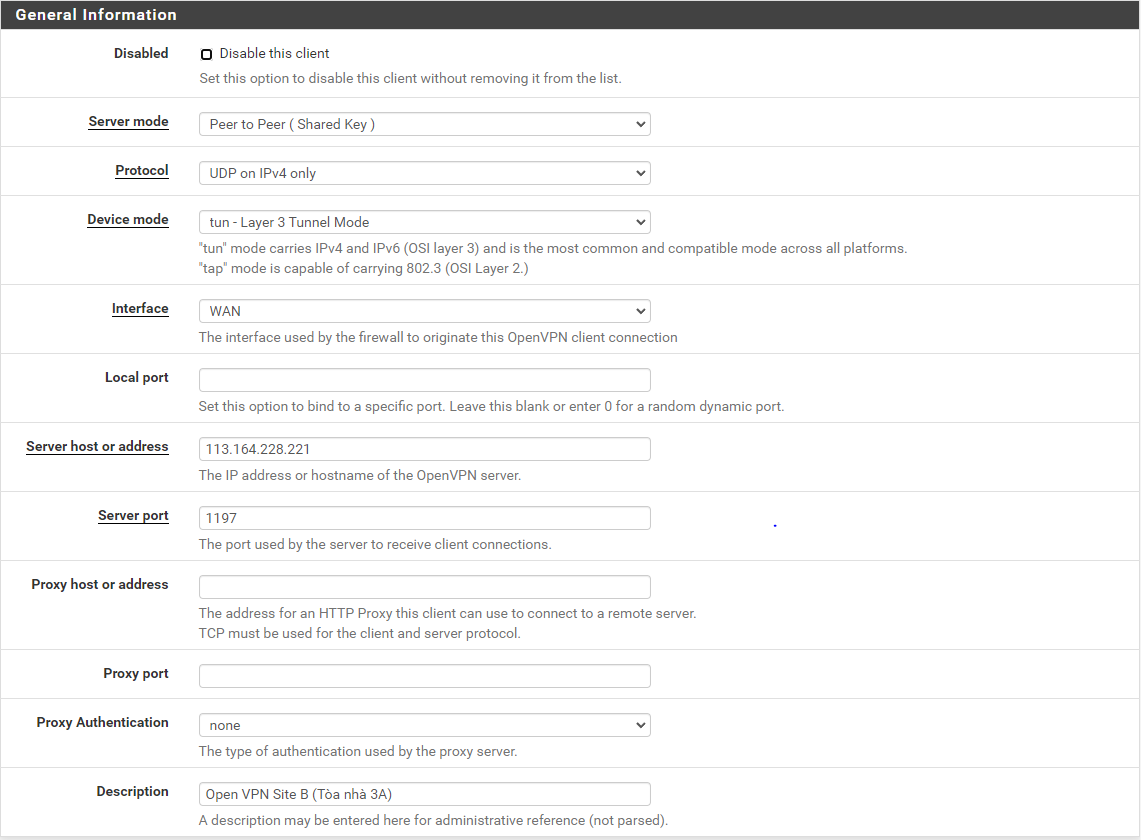
Điền các trường như sau, với các trường khác để ở giá trị mặc định:

Server Mode: Chọn Peer to Peer (Shared Key)

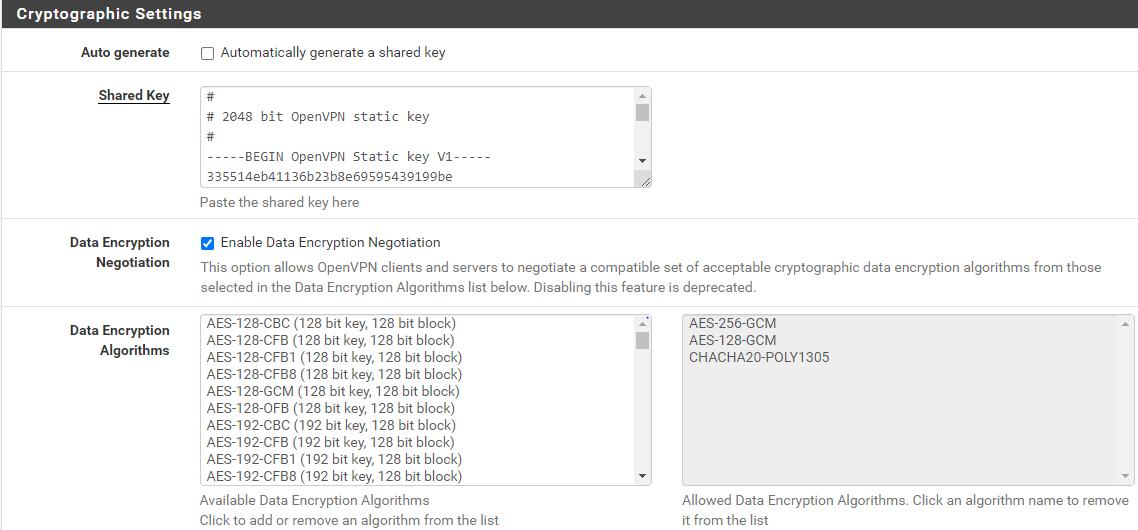
Server host or address: 113.164.228.221

Server port: 1197

Description: Open VPN Site B (Tòa nhà 3A)



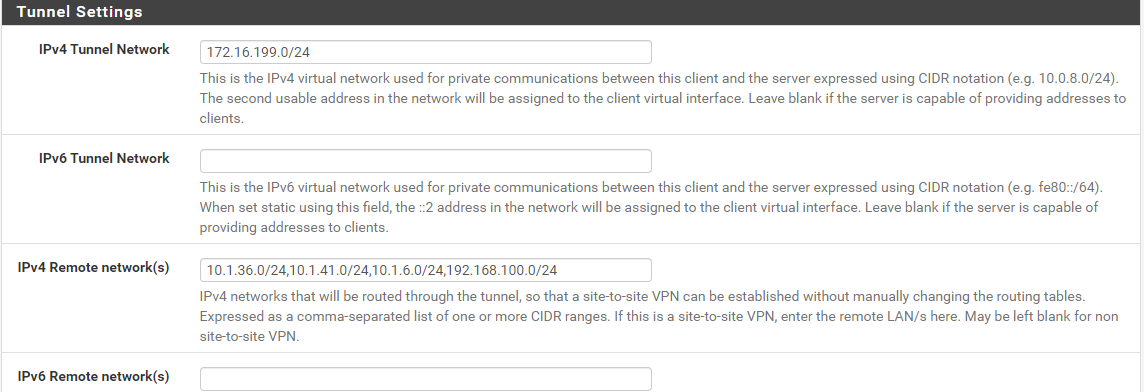
Shared Key: Bỏ check tự động tạo Key sau đó copy Key từ máy chủ tòa nhà 3A



IPv4 Tunnel Network: 172.16.199.0/30

Remote Network: Nhập IP LAN Subnet tòa nhà 3A định tuyến qua đường hầm, 10.1.32.0/24, 10.1.41.0/24, 10.1.36.0/24, 192.168.100.0/24, 10.1.6.0/24….

Chọn Save và cấu hình sẽ giống như dưới



* 1. Mở Rule trên Pfsense tòa nhà AC

Cấu hình quy tắc tường lửa trên WAN cho phép truy cập vào máy chủ OpenVPN.

Mở port 1197 trên Wan

Điều hướng đến Firewall -> Rules, WAN tab

Chọn fa-level-up và tạo 1 rule mới ở đầu danh sách

Protocol: UDP

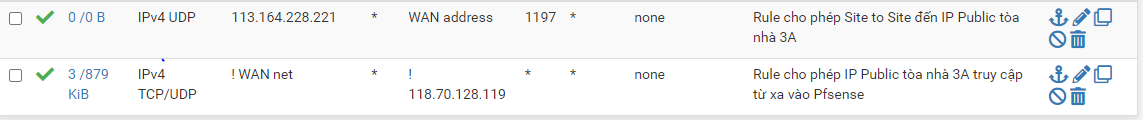
Source: Single host alias, 113.164.228.221

Destination: Wan address

Destination Port Range: Other, 1197

Description: OpenVPN Site to Site

Chọn Save và quy tắc sẽ giống như hình OpenVPN Ví dụ Quy tắc Tường lửa WAN Site to Site



Ví dụ Quy tắc Tường lửa WAN Site to Site

Cấu hình quy tắc tường lửa trên VPN\_Site cho phép chuyển lưu lượng truy cập VPN từ mạng LAN

Điều hướng đến Firewall -> Rule, OpenVPN tab

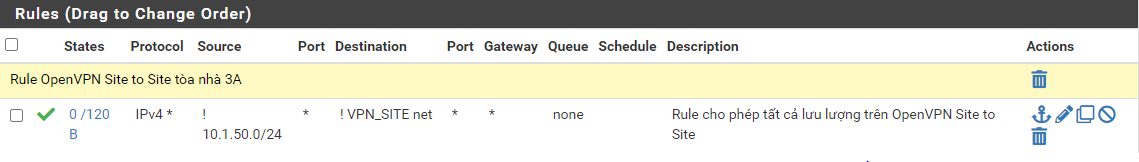
Chọn fa-level-up và tạo 1 rule mới ở đầu danh sách

Protocol: Any, Tích vào Invert match

Destination: Any, Tích vào Invert match

Description: Rule cho phép tất cả lưu lượng trên OpenVPN Site to Site

Chọn Save và quy tắc sẽ giống như hình OpenVPN Ví dụ Quy tắc tương lửa LAN Site to Site

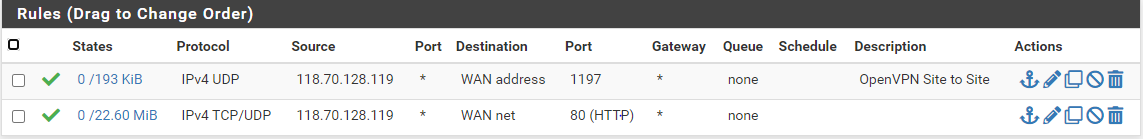


Ví dụ Quy tắc tường lửa LAN Site to Site

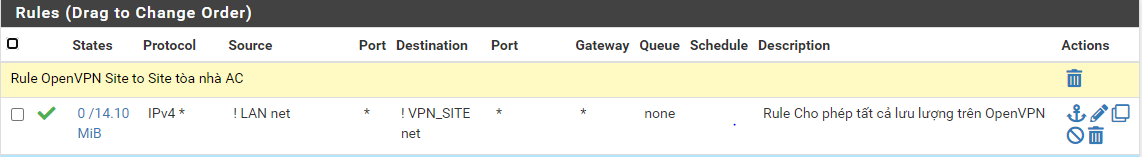
* 1. Mở Rule trên Pfsense tòa nhà 3A

Làm tương tự quy tắc tường lửa trên WAN và OpenVPN của tòa nhà AC

Cấu hình quy tắc tường lửa trên WAN cho phép truy cập vào máy chủ OpenVPN.



Cấu hình quy tắc tường lửa trên VPN\_Site cho phép chuyển lưu lượng truy cập VPN từ mạng LAN



* 1. Kiểm tra

IP Site AC: 10.1.50.11

Site tòa nhà AC thông với mang LAN và Server Site 3A

Internet đi theo đường WAN của Site AC

