

Triển Khai Aliases và Firewall Rules trên pfSense

Phần 1: Quản lý Định danh bằng Aliases

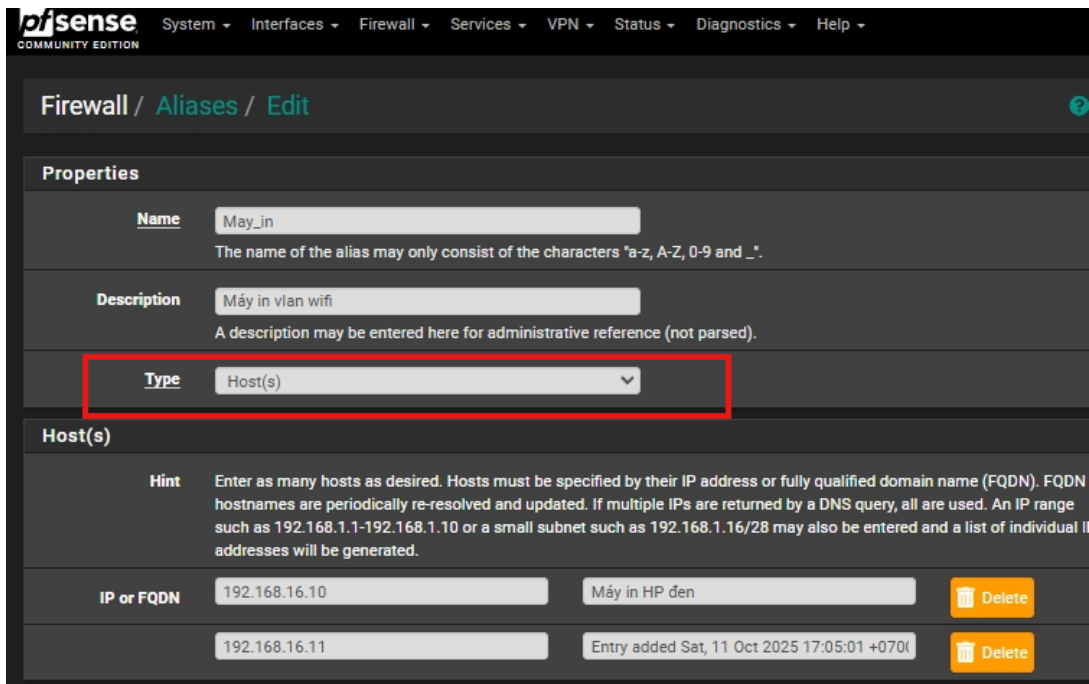
Bước 1.1: Tạo các Alias cho Thiết bị và Mạng

Thao tác thực hiện trên giao diện web pfSense:

1. Truy cập **Firewall > Aliases**.
2. Chọn tab tương ứng (IP, Networks, Ports) và nhấn **Add**.

Phân tích các Aliases đã được cấu hình:

- **Alias May_in (Loại: Host):**
 - **Nội dung:** 192.168.16.10, 192.168.16.11.
 - **Mục đích:** Nhóm địa chỉ IP của các máy in trong công ty. Thay vì phải tạo quy tắc riêng cho từng máy in, giờ đây chúng ta có thể tạo một quy tắc duy nhất áp dụng cho alias May_in.



- **Alias Vlan12_block, Vlan13_block, Vlan14_block, Vlan15_block, Vlan16_block (Loại: Network):**
 - **Nội dung (ví dụ Vlan12_block):** 192.168.11.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.15.0/24, 192.168.16.0/24.
 - **Mục đích:** Để thực thi chính sách cấm giao tiếp giữa các VLAN. Alias này định nghĩa "tất cả các VLAN khác ngoại trừ chính nó". Nó sẽ được dùng trong một quy tắc Block để ngăn VLAN 12 truy cập vào các VLAN còn lại.

Firewall / Aliases / Edit

Properties

Name
Vlan12_block

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
Chặn Vlan12 tới các Vlan còn lại

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

Type
Network(s)

Network(s)

Hint
Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN				
192.168.11.0	/	24	Entry added Sat, 11 Oct 2025 17:02:41 +0700	Delete
192.168.13.0	/	24	Entry added Sat, 11 Oct 2025 17:02:41 +0700	Delete
192.168.14.0	/	24	Entry added Sat, 11 Oct 2025 17:02:41 +0700	Delete
192.168.15.0	/	24	Entry added Sat, 11 Oct 2025 17:02:41 +0700	Delete
192.168.16.0	/	24	Entry added Sat, 11 Oct 2025 17:02:41 +0700	Delete

- **Alias Novaon_All_IP (Loại: Host):**

- **Nội dung:** 118.70.81.114, 118.70.179.9, 118.69.187.183, ...
- **Mục đích:** Tập hợp tất cả các địa chỉ IP WAN tĩnh của các văn phòng khác thuộc Novaon. Alias này hữu ích để tạo các quy tắc bảo mật, ví dụ như "Chỉ cho phép truy cập vào giao diện quản lý pfSense từ các IP thuộc Novaon_All_IP".

The screenshot shows the 'Firewall / Aliases / Edit' page in pfSense. The 'Name' field is 'Novaon_All_IP'. The 'Description' is 'Các IP văn phòng khác'. The 'Type' is set to 'Host(s)'. Below this, there is a 'Host(s)' section with a hint: 'Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.' Below the hint, there are two rows of IP addresses: '118.70.81.114' with 'HN NC' and '118.70.179.9' with 'HN TK'. Each row has a 'Delete' button.

Lý do: Thay vì nhìn vào một địa chỉ IP vô nghĩa, quản trị viên có thể ngay lập tức hiểu được mục đích của quy tắc, ví dụ "Chặn VLAN12 tới các VLAN khác" hoặc "Cho phép VLAN13 truy cập Máy in".

The screenshot shows the 'Firewall / Aliases / IP' page in pfSense. It displays a table of aliases with columns: Name, Type, Values, Description, and Actions. The table lists various aliases, including 'May_in', 'Nguyen_Chinh_HN', 'Novaon_All_IP', 'Phap_Van_HN', 'Tan_Huong_HCM', 'Trung_Kinh_HN', and several 'VlanX_block' entries. Each entry has a 'Delete' button in the 'Actions' column.

Name	Type	Values	Description	Actions
May_in	Host(s)	192.168.16.10, 192.168.16.11	Máy in văn phòng	[Edit] [Copy] [Delete]
Nguyen_Chinh_HN	Host(s)	116.98.214.17, 118.70.81.114	Nguyễn Chính Hà Nội	[Edit] [Copy] [Delete]
Novaon_All_IP	Host(s)	118.70.81.114, 118.70.179.9, 118.70.233.162, 118.69.52.224, 118.69.187.183, 113.161.80.147, 116.98.214.17, 118.69.52.224	Các IP văn phòng khác	[Edit] [Copy] [Delete]
Phap_Van_HN	Host(s)	171.244.15.35	Pháp Văn Hà Nội	[Edit] [Copy] [Delete]
Tan_Huong_HCM	Host(s)	118.69.187.183, 118.69.52.224, 118.69.152.59	Tân Hương HCM	[Edit] [Copy] [Delete]
Trung_Kinh_HN	Host(s)	118.70.179.9, 118.70.233.162	Trung Kinh Hà Nội	[Edit] [Copy] [Delete]
Vlan12_block	Network(s)	192.168.11.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.15.0/24, 192.168.16.0/24	Chặn Vlan12 tới các Vlan còn lại	[Edit] [Copy] [Delete]
Vlan13_block	Network(s)	192.168.11.0/24, 192.168.12.0/24, 192.168.14.0/24, 192.168.15.0/24, 192.168.16.0/24	Chặn Vlan 13 tới Vlan còn lại	[Edit] [Copy] [Delete]
Vlan14_block	Network(s)	192.168.11.0/24, 192.168.12.0/24, 192.168.13.0/24, 192.168.15.0/24, 192.168.16.0/24	Chặn Vlan14 tới các Vlan còn lại	[Edit] [Copy] [Delete]
Vlan15_block	Network(s)	192.168.11.0/24, 192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.16.0/24	Chặn Vlan 15 tới Vlan còn lại	[Edit] [Copy] [Delete]
Vlan16_block	Network(s)	192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.15.0/24, 192.168.11.0/24	Chặn Vlan 16 tới Vlan còn lại	[Edit] [Copy] [Delete]

Phần 2: Firewall Rules

Bước 2.1: Rule trên các Giao diện VLAN (Ví dụ: OPT2 - VLAN 12)

Đây là nơi chính sách phân đoạn mạng được thực thi một cách rõ ràng nhất. Các quy tắc trên tab **Firewall > Rules > OPT2** được xử lý theo thứ tự sau:

- Rule 1 (Ưu tiên cao nhất): Cho phép In ấn**
 - Action:** Pass
 - Source:** opt2 net (Bất kỳ IP nào trong mạng VLAN 12)
 - Destination:** May_in (Alias chứa IP các máy in)
 - Giải thích:** Quy tắc này được đặt lên đầu tiên để đảm bảo rằng yêu cầu in ấn luôn được cho phép trước khi bị các quy tắc chặn bên dưới xử lý.
- Rule 2: Chặn truy cập đến các VLAN khác**
 - Action:** Block
 - Source:** any (Bất kỳ nguồn nào từ VLAN 12)
 - Destination:** Vlan12_block (Alias chứa tất cả các mạng VLAN khác)
 - Giải thích:** Đây là quy tắc an ninh cốt lõi. Sau khi đã cho phép các truy cập cần thiết (như in ấn), quy tắc này sẽ chặn tất cả các nỗ lực truy cập từ VLAN 12 sang các phòng ban khác, giúp cô lập các phân đoạn mạng với nhau.
- Rule 3 (Ưu tiên thấp nhất): Cho phép đi ra Internet**
 - Action:** Pass
 - Source:** any
 - Destination:** any
 - Gateway:** VNPT_FPT (Sử dụng nhóm gateway cân bằng tải)
 - Giải thích:** Quy tắc này là cuối cùng. Nếu một gói tin không phải là đi đến máy in (Rule 1) và cũng không phải đi đến các VLAN khác (Rule 2), thì nó sẽ khớp với quy tắc này. Đây chính là lưu lượng đi ra Internet.

Lý do: Cấu trúc 3 quy tắc này (Allow Specific -> Block Inter-VLAN -> Allow Internet) là một mô hình kinh điển và rất hiệu quả để triển khai bảo mật theo lớp. Nó đảm bảo chỉ những gì được phép tường minh mới có thể diễn ra, còn lại sẽ bị chặn hoặc cho phép ra ngoài Internet.

Firewall / Rules / VLAN16											
Floating WAN LAN VLAN11 VLAN12 VLAN13 VLAN14 VLAN15 <u>VLAN16</u> WAN1 WAN2 WAN3 IPsec OpenVPN											
Rules (Drag to Change Order)											
<input checked="" type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	VLAN16 subnets	*	May_in	*	*	none			
<input checked="" type="checkbox"/>	0/50 KiB	IPv4 *	*	*	Vlan16_block	*	*	none			
<input checked="" type="checkbox"/>	5.837K/176.79 GiB	IPv4 *	*	*	*	*	VNPT_FPT	none			

Bước 2.2: Phân tích Rule trên Giao diện WAN

Các quy tắc trên giao diện WAN kiểm soát những gì được phép đi từ Internet vào hệ thống mạng.

1. Rule Pass UDP port 1194:

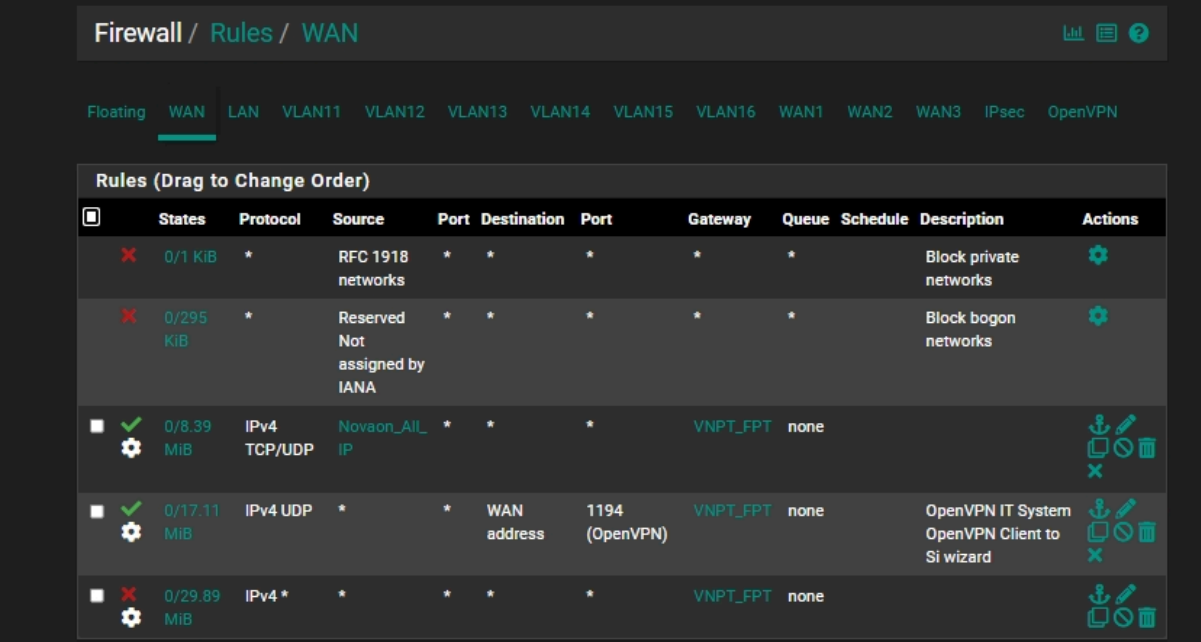
- **Mục đích:** Cho phép các kết nối OpenVPN từ bên ngoài vào. Đây là quy tắc bắt buộc để dịch vụ VPN hoạt động.

2. Rule Pass từ Novaon_All_IP:

- **Mục đích:** Đây là một quy tắc Policy-Based Routing. Nó đảm bảo rằng bất kỳ lưu lượng nào có nguồn từ các văn phòng khác của Novaon sẽ được định tuyến qua nhóm gateway VNPT_FPT, tận dụng cơ chế cân bằng tải.

3. Rule Block any to any:

- **Mục đích:** Quy tắc này chặn tất cả các truy cập còn lại từ Internet vào. Mặc dù pfSense có cơ chế "implicit deny", việc thêm một quy tắc chặn tường minh ở cuối giúp việc đọc log và xác định các truy cập bị từ chối trở nên rõ ràng hơn.



Firewall / Rules / WAN											
Floating WAN LAN VLAN11 VLAN12 VLAN13 VLAN14 VLAN15 VLAN16 WAN1 WAN2 WAN3 IPsec OpenVPN											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/1 KIB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
	0/295 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
	0/8.39 MIB	IPv4 TCP/UDP	Novaon_All_IP	*	*	*	VNPT_FPT	none			
	0/17.11 MIB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	VNPT_FPT	none		OpenVPN IT System OpenVPN Client to Si wizard	
	0/29.89 MIB	IPv4 *	*	*	*	*	VNPT_FPT	none			

Thông tin thêm: Vlan 11 là Vlan System cho quản trị viên, nên các rules được thiết kế để đảm bảo các Client trong Vlan 11 có thể truy cập tất cả vlan còn lại và cả hệ thống hạ tầng để quản trị. 2 Rules Pass all, rule trên đầu để dùng default gateway, chỉ có như thế mới có thể quản trị được các Vlan còn lại, Rules 2 là pass all nhưng gateway lại là VNPT_FPT, là để áp dụng cân bằng tải đã có.