

Lab 10: Tạo alias IP/group và áp dụng vào firewall rules – giúp tối ưu quản lý firewall rule trên pfSense. Lab này phù hợp với người đã có kiến thức cơ bản về pfSense và đang muốn nâng cao khả năng quản trị firewall.

Mục tiêu lab

- Tạo alias (bí danh) IP và nhóm IP.
- Áp dụng alias vào firewall rule để:
 - Quản lý dễ hơn.
 - Tối ưu hóa số lượng rule.
 - Dễ cập nhật nếu có thay đổi IP.

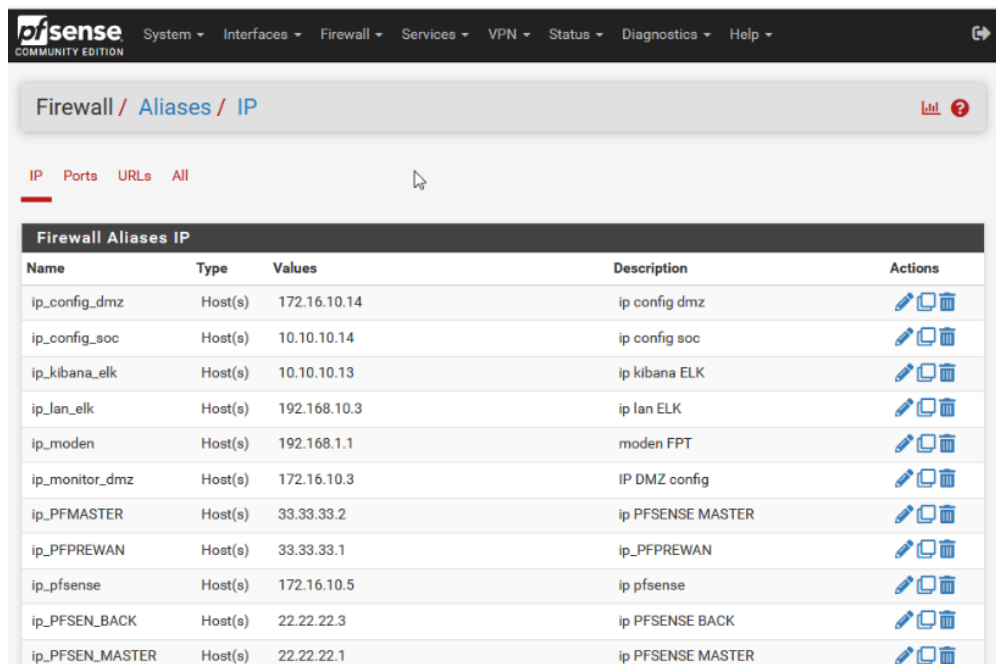
Yêu cầu

- pfSense đã cài đặt và truy cập được Web GUI.
- Có ít nhất 1 interface đang hoạt động (LAN hoặc OPT).
- Có sẵn vài IP cần chặn hoặc cho phép.


































Các bước thực hiện

Bước 1: Tạo Alias cho IP

1. Truy cập **pfSense Web GUI**.
2. Vào menu: Firewall → Aliases.



The screenshot shows the pfSense Web GUI interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Firewall / Aliases / IP'. Below the breadcrumb, there are tabs for 'IP', 'Ports', 'URLs', and 'All', with 'IP' being the active tab. The main content area is titled 'Firewall Aliases IP' and contains a table with the following data:

Name	Type	Values	Description	Actions
ip_config_dmz	Host(s)	172.16.10.14	ip config dmz	  
ip_config_soc	Host(s)	10.10.10.14	ip config soc	  
ip_kibana_elk	Host(s)	10.10.10.13	ip kibana ELK	  
ip_lan_elk	Host(s)	192.168.10.3	ip lan ELK	  
ip_moden	Host(s)	192.168.1.1	moden FPT	  
ip_monitor_dmz	Host(s)	172.16.10.3	IP DMZ config	  
ip_PFMMASTER	Host(s)	33.33.33.2	ip PFSense MASTER	  
ip_PFPREWAN	Host(s)	33.33.33.1	ip_PFPREWAN	  
ip_pfsense	Host(s)	172.16.10.5	ip pfsense	  
ip_PFSense_BACK	Host(s)	22.22.22.3	ip PFSense BACK	  
ip_PFSense_MASTER	Host(s)	22.22.22.1	ip PFSense MASTER	  

3. Click + **Add**.

Firewall / Aliases / Edit ?

Properties

Name

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

Description

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

Type

Host(s)

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.

IP or FQDN

4. Điền thông tin:

- **Name:** Blocked_IPs (ví dụ)
- **Type:** Host (s)
- **Description:** Danh sách IP bị chặn

Firewall / Aliases / Edit ?

Properties

Name

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

Description

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

Type

Host(s)

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.

IP or FQDN

5. Ở phần **IP or FQDN**, thêm các IP muốn đưa vào nhóm. Ví dụ:

- 192.168.10.10
- 192.168.10.20
- 192.168.10.20

Host(s)

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.

IP or FQDN		
192.168.10.10	Chan IP .10	Delete
192.168.10.20	Chan IP .20	Delete
192.168.10.30	Chan IP .30	Delete

Save Add Host

6. Click **Save**, sau đó **Apply Changes**.

Firewall Aliases IP					
Name	Type	Values	Description	Actions	
Blocked_IPs	Host(s)	192.168.10.10, 192.168.10.20, 192.168.10.30	danh sach chan IP		

✓ Có thể tạo nhiều alias: IP, network, port, hay cả domain.

◆ Bước 2: Áp dụng Alias vào Firewall Rule

Tôi sẽ áp dụng alias vừa tạo để chặn IP trong danh sách đã tạo.

- Vào menu: Firewall → Rules → Chọn tab tương ứng (LAN, OPT...). ở đây tôi đang có 1 vùng area là LAN với giải IP là 192.168.10.0/24

Firewall / Rules / LAN

Floating WAN LAN SOC

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	ip_PFMMASTER	*	*	none		Block LAN to 33.33.33.2	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	ip_PFPREWAN	*	*	none		Block LAN to 33.33.33.1	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	ip_PFPREWAN	*	*	none		Block LAN to 33.33.33.3	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	ip_PFSEN_MASTER	*	*	none		Block LAN to 22.22.22.1	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	LAN subnets	*	ip_PFSEN_BACK	*	*	none		Block LAN to 22.22.22.3	

- Click + **Add** (thường đặt ở đầu hoặc cuối tùy mục đích).
- Thiết lập rule:**

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

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

Protocol TCP
Choose which IP protocol this rule should match.

- **Action:** Block (hoặc Pass, tùy mục đích).
- **Interface:** Chọn interface áp dụng (ví dụ: LAN).

Source

Source ☐ Invert match Address or Alias blo /
Blocked_IPs

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

- **Source:**
 - **Type:** Single host or alias
 - **Address:** chọn Blocked_IPs (alias vừa tạo).

Destination

Destination ☐ Invert match Any Destination Address /
Destination Address

Destination Port Range From (other) Custom To (other) Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- **Destination:** any (hoặc cụ thể).

Extra Options

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

Description Chặn nhóm IP đã định nghĩa
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

- Description:** Chặn nhóm IP đã định nghĩa

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	Blocked_ IPs	*	*	*	*	none		Chặn nhóm IP đã định nghĩa	

5. Click **Save**, sau đó **Apply Changes**.

Check LOG trên Pfsense

	Jul 5 08:39:14	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57946	142.250.71.170:443	TCP:S
	Jul 5 08:39:14	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57943	142.250.71.170:443	TCP:S
	Jul 5 08:39:14	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57944	142.250.71.202:443	TCP:S
	Jul 5 08:39:15	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57945	142.250.71.202:443	TCP:S
	Jul 5 08:39:15	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57946	142.250.71.170:443	TCP:S
	Jul 5 08:39:15	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57939	142.250.71.170:443	TCP:S
	Jul 5 08:39:17	LAN	Chặn nhóm IP đã định nghĩa (1751678700)	192.168.10.20:57941	142.250.197.206:443	TCP:S

Có thể thấy rule chặn nhóm IP đã định nghĩa đang hoạt động

◆ Bước 3: Kiểm tra và tối ưu

- Truy cập tab **Diagnostics** → **States**, kiểm tra các IP bị chặn đã có trong bảng trạng thái chưa.

LAN	udp	192.168.10.20:57668 -> 142.250.198.164:443	MULTIPLE:MULTIPLE	10 / 11	5 KIB / 7 KIB
LAN	udp	192.168.10.20:57963 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	62 B / 103 B
LAN	udp	192.168.10.20:57890 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	72 B / 124 B
LAN	udp	192.168.10.20:55419 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	72 B / 124 B
LAN	udp	192.168.10.20:54835 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	73 B / 125 B
LAN	udp	192.168.10.20:54480 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	70 B / 122 B
LAN	udp	192.168.10.20:51992 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	70 B / 122 B
LAN	udp	192.168.10.20:58082 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	66 B / 118 B
LAN	udp	192.168.10.20:51305 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	69 B / 121 B
LAN	udp	192.168.10.20:52642 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	71 B / 123 B
LAN	udp	192.168.10.20:62057 -> 172.16.10.30:53	SINGLE:MULTIPLE	1 / 1	62 B / 78 B

Phân tích nội dung kết quả

- Giao diện: LAN
- Protocol: tcp, udp
- Nguồn: hầu hết là 192.168.10.20
- Đích:
 - 172.16.10.30:53 → DNS server nội bộ.
 - 142.250.198.164:443 443 → dịch vụ HTTPS (có thể là Google,...).

✓ Ứng dụng Alias trong trường hợp này

1. 📄 Tạo Alias IP để quản lý client

Giả sử muốn **theo dõi, giới hạn hoặc chặn client 192.168.10.20**, bạn có thể:

- Tạo alias tên Client_Test:
 - Kiểu: Host(s)
 - IP: 192.168.10.20
- Dùng alias này trong rule để:
 - **Giới hạn truy cập DNS.**
 - **Chặn HTTP/HTTPS** đi ra ngoài.
 - **Giám sát bằng log.**

2. 🌐 Tạo Alias Network hoặc IP đích

Thấy client truy cập đến:

- 142.250.198.164 (Google Cloud / YouTube?)

Nếu muốn **block hoặc redirect** những kết nối ra ngoài các địa chỉ này, hãy:

- Tạo alias Blocked_HTTPS_Cloud:
 - Thêm IP hoặc subnet của dịch vụ cloud đó.
- Rule chặn: Source: Client_Test, Destination: Blocked_HTTPS_Cloud, Port: 443, Action: Block.
- Vào Firewall → Aliases, nếu cần thêm IP, chỉ cần sửa alias Blocked_IPs, rule vẫn hoạt động mà không cần chỉnh sửa lại.

✓ Lợi ích khi dùng Alias

Lợi ích	Giải thích
🔧 Dễ bảo trì	Thay IP trong alias là đủ, không cần chỉnh nhiều rule.
📄 Tối ưu rule	Ít rule hơn, dễ đọc và giảm lỗi cấu hình.
🔒 An toàn hơn	Tăng độ chính xác khi quản lý tập trung.
📊 Thống kê tốt hơn	Rule rõ ràng, dễ theo dõi trong logs.