

□ Lab 4: Tạo Firewall Rule cơ bản – ICMP & HTTP

🎯 Mục tiêu

- Hiểu và thao tác với hệ thống rule firewall của pfSense.
- Tạo rule để cho phép hoặc chặn:
 - ICMP (ping)
 - HTTP (port 80)
- Kiểm tra logic "First match wins" trong firewall pfSense.

📋 Kiến thức nền tảng

- Firewall rule **áp dụng theo chiều INCOMING (Inbound)** của mỗi interface.
- Rule được **đọc từ trên xuống** → Rule nào khớp đầu tiên sẽ được áp dụng.
- Mặc định, pfSense **cho phép toàn bộ từ LAN ra ngoài**, không cho gì vào từ WAN.

🔧 Bước 1: Xóa rule mặc định (nếu cần)

Mặc định pfSense có rule “Allow all from LAN to any”.

1. Truy cập GUI: <https://192.168.20.1>
2. Vào **Firewall** → **Rules** → **LAN**
3. Tìm rule mặc định:
 - Action: Pass | Protocol: Any | Source: LAN net | Destination: any
4. **Tắt (Disable)** hoặc **Xóa** rule này để test theo từng dịch vụ

```
PS C:\Users\admin> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=116
Reply from 8.8.8.8: bytes=32 time=25ms TTL=116
Reply from 8.8.8.8: bytes=32 time=25ms TTL=116
Reply from 8.8.8.8: bytes=32 time=25ms TTL=116

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 25ms, Average = 25ms
PS C:\Users\admin>
```

Trước khi tạo rule vẫn ping được 8.8.8.8 từ máy client.

Tạo rule chặn ICMP đến 8.8.8.8

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 ICMP
 Choose which IP protocol this rule should match.

ICMP Subtypes any
 Alternate Host
 Datagram conversion error
 Echo reply
 For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Add rule trên interface LAN

Action: tùy chọn hoạt động này của rule, cho qua (PASS), hay chặn lượng lưu đi qua (BLOCK)

Interface: chọn LAN, trên giao diện LAN

Protocol: giao thức được rule áp dụng, có rất nhiều giao thức mà pfsense áp dụng, đối với chặn ICMP đến 8.8.8.8, thì ta sử dụng protocol ICMP.

Source

☒ Source ☐ Invert match LAN subnets Source Address /

Destination

☐ Destination ☐ Invert match Address or Alias 8.8.8.8 /

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 block ICMP LAN to 8.8.8.8
 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.

Đến với phần tiếp theo của rule:

Source là nguồn của gói tin trong rule

Destination là đích đến của gói tin trong rule

Và nên ghi là mô tả cho rule trong phần Description

➔ SAVE

<input type="checkbox"/>		0/0 B	IPv4	LAN	*	8.8.8.8	*	*	none	block ICMP LAN to 8.8.8.8	
			ICMP	subnets						8.8.8.8	
			any								

```

PS C:\Users\admin> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
PS C:\Users\admin>

```

Như vậy là rule chặn ICMP đến 8.8.8.8 đã hoạt động

Tạo rule chặn client truy cập HTTP từ client đến firewall

Source

Source

☐ Invert match

LAN subnets

Source Address

/

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**.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

HTTP (80)

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

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

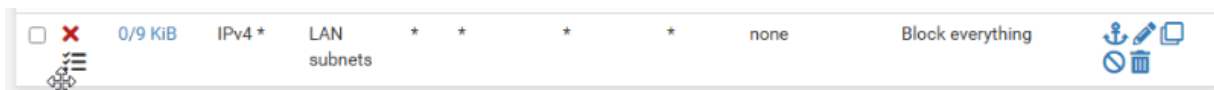
block HTTP client to firewall

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.

		0/312 B	IPv4 TCP	LAN subnets	*	*	80 (HTTP)	*	none	block HTTP client to firewall	
<input type="checkbox"/>		0/180 B	IPv4 ICMP	LAN subnets	*	8.8.8.8	*	*	none	block ICMP LAN to 8.8.8.8	

Tạo rule chặn tất cả còn lại

- Thêm rule **Block all** cuối cùng:
 - Action:** Block
 - Protocol:** Any
 - Source:** LAN net
 - Destination:** any
 - Description:** Block everything else
- Save → Apply




✓ Kết quả đạt được


- Tạo rule chi tiết cho phép ICMP và HTTP.
- Chặn toàn bộ traffic khác (theo mô hình "Allow specific, deny all").
- Hiểu rõ nguyên tắc "top-down, first match wins".


□ Gợi ý nâng cao

- Tạo rule chỉ cho HTTPS đi qua vào giờ hành chính (Schedule)
- Áp dụng rule chỉ cho 1 máy cụ thể (theo IP hoặc MAC)
- Log riêng các gói bị chặn để theo dõi hành vi bất thường

Tạo rule chỉ cho HTTPS đi qua vào giờ hành chính (Schedule)

Schedules			
Name	Range: Date / Times / Name	Description	Actions
 https_pass	June 5 - 6 June 9 - 13 June 16 - 20 June 23 - 27 June 30 / 7:00-11:00 / AM June 5 - 6 June 9 - 13 June 16 - 20 June 23 - 27 June 30 / 13:00-17:00 / PM June 5 - 6 June 9 - 13 June 16 - 20 June 23 - 27 June 30 / 19:00-23:00 / Night	Pass https in 8:00-11:00 & 13:00-17:00	 

 Indicates that the schedule is currently active.

 Add