

Lab 7 – Cấu hình Firewall Rules nâng cao: Lọc theo IP, Port, Time-based Rule

Mục tiêu

- Lọc truy cập theo **IP nguồn/đích**
- Lọc truy cập theo **cổng (Port)**
- Cấu hình **rule theo thời gian** (Time-based firewall rule)

Yêu cầu

- 1 máy chủ pfSense (đã cài và truy cập được qua WebGUI)
- 1 máy client (trong LAN)
- Địa chỉ IP cho pfSense:
 - WAN: DHCP hoặc tĩnh từ mạng ngoài
 - LAN: 192.168.20.1/24
- Client IP: 192.168.20.100

Phần 1: Lọc theo IP (IP Filtering)

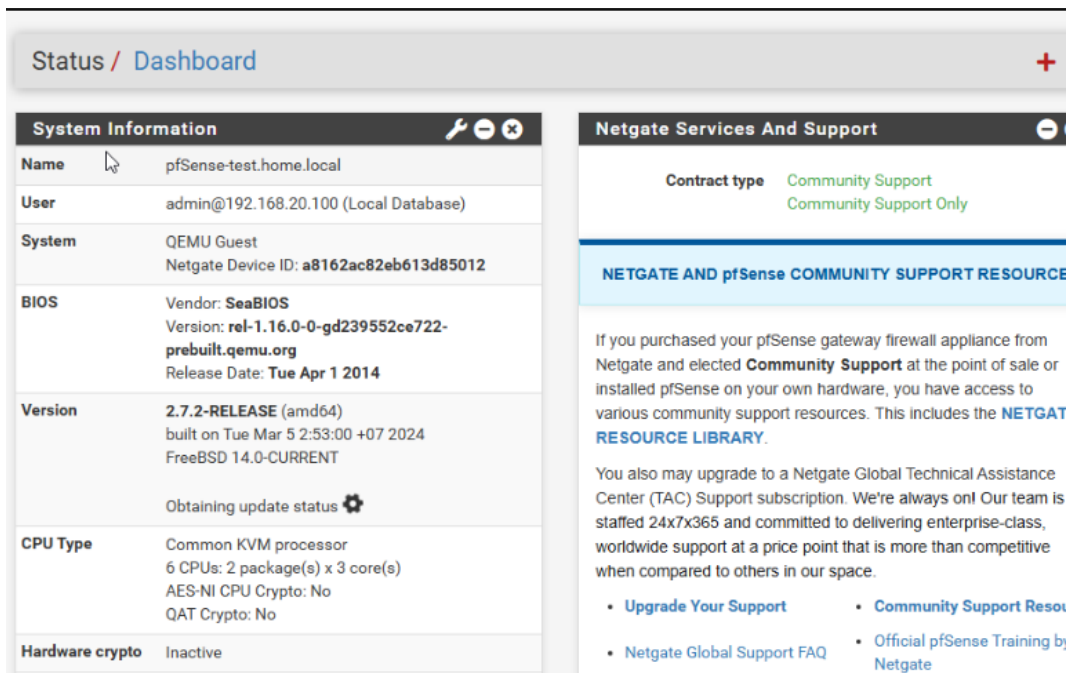
Mục tiêu:

Chặn máy 192.168.20.100 truy cập internet (HTTP/HTTPS)

Thực hiện:

1. Vào WebGUI của pfSense

Truy cập <https://192.168.20.1> → Đăng nhập






The screenshot displays the pfSense WebGUI interface. The top navigation bar shows 'Status / Dashboard'. The main content area is divided into two panels. The left panel, titled 'System Information', contains a table with the following details:

System Information	
Name	pfSense-test.home.local
User	admin@192.168.20.100 (Local Database)
System	QEMU Guest Netgate Device ID: a8162ac82eb613d85012
BIOS	Vendor: SeaBIOS Version: rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org Release Date: Tue Apr 1 2014
Version	2.7.2-RELEASE (amd64) built on Tue Mar 5 2:53:00 +07 2024 FreeBSD 14.0-CURRENT Obtaining update status
CPU Type	Common KVM processor 6 CPUs: 2 package(s) x 3 core(s) AES-NI CPU Crypto: No QAT Crypto: No
Hardware crypto	Inactive

The right panel, titled 'Netgate Services And Support', shows the 'Contract type' as 'Community Support' and 'Community Support Only'. Below this, there is a section for 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCE' with text explaining the support resources available. At the bottom, there are links for 'Upgrade Your Support', 'Community Support Resources', 'Netgate Global Support FAQ', and 'Official pfSense Training by Netgate'.

2. Vào Firewall → Rules → LAN

3. Click "Add" ở đầu danh sách (để tạo rule đứng đầu, ưu tiên cao)
4. Cấu hình rule:

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/67 KiB	IPv4 *	ip_201 client_1	*	*	*	*	none		Block Client1- 192.168.20.100 access internet	  

- **Action:** Block
 - **Interface:** LAN
 - **Address Family:** IPv4
 - **Protocol:** Any
 - **Source:** Single host or alias → nhập: 192.168.20.100
 - **Destination:** any
 - **Description:** Block Internet for 192.168.20.100
5. Save → Apply Changes

✓ Phần 2: Lọc theo cổng (Port Filtering)

◆ Mục tiêu:

Chỉ cho phép truy cập cổng HTTP (80) và HTTPS (443), chặn tất cả các cổng khác.

🔧 Thực hiện:

1. Tạo rule **ALLOW** trước:
 - **Action:** Pass
 - **Protocol:** TCP
 - **Source:** LAN net
 - **Destination:** any
 - **Destination Port Range:** HTTP (80)
 - **Description:** Allow HTTP

→ Lặp lại để tạo rule tương tự cho HTTPS (443)
2. Tạo rule **BLOCK** sau cùng:
 - **Action:** Block
 - **Protocol:** Any
 - **Source:** LAN net
 - **Destination:** any
 - **Description:** Block all other ports
3. Sắp xếp rule:
Đảm bảo 2 rule **ALLOW** ở trên, **BLOCK** nằm cuối.
4. Save → Apply Changes

<input type="checkbox"/>		0/0 B	IPv4	LAN	*	*	80	*	none	Allow LAN to internet HTTP	
			TCP	subnets			(HTTP)				
<input type="checkbox"/>		0/0 B	IPv4	LAN	*	*	443	*	none	Allow LAN to internet HTTPS	
			TCP	subnets			(HTTPS)				
<input type="checkbox"/>		0/481 KiB	IPv4 *	LAN	*	*	*	*	none	Block everything	
				subnets							

✓ Phần 3: Rule theo thời gian (Time-based rule)

◆ Mục tiêu:

Chỉ cho phép máy 192.168.20.100 truy cập internet từ **8h đến 17h**

🔧 Thực hiện:

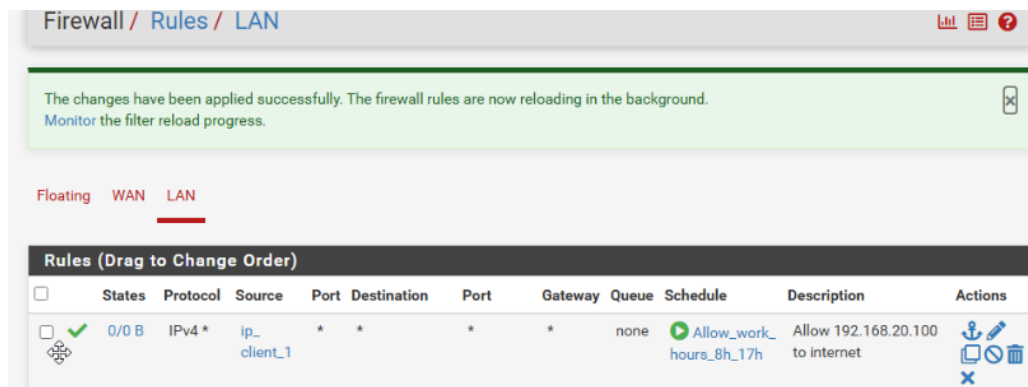
Bước 1: Tạo Time Schedule

- Vào **Firewall** → **Schedules** → Click "Add"
- Cấu hình:**
 - Name:** allow_work_hours_8h_17h
 - Description:** Cho phép truy cập từ 8h-17h
 - Chọn ngày:** Monday to Friday
 - Thời gian:** From: 08:00 → To: 17:00
- Save**

Firewall / Schedules			
Schedules			
Name	Range: Date / Times / Name	Description	Actions
Allow_work_hours_8h_17h	Mon - Sun / 8:00-17:59 / Time	Allow 8h-17h	

Bước 2: Tạo Rule sử dụng Schedule

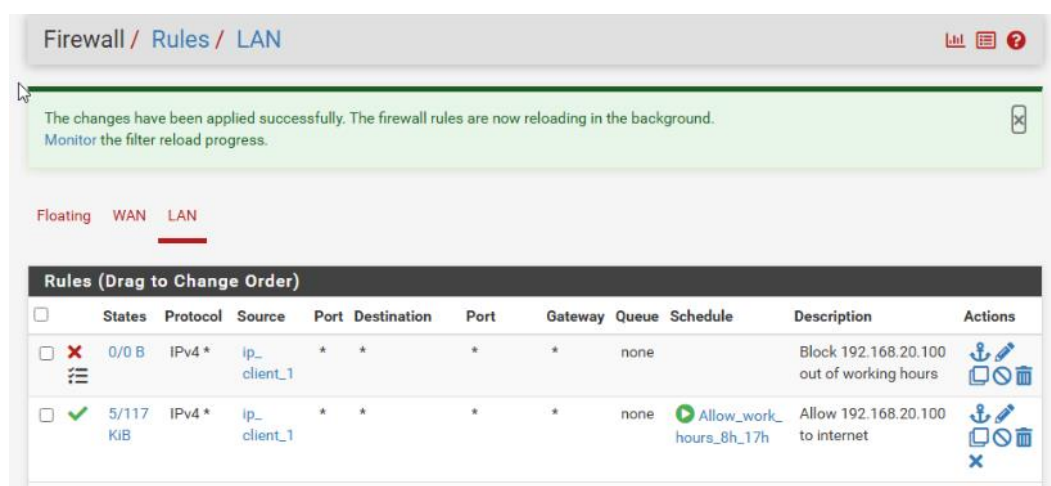
- Vào **Firewall** → **Rules** → **LAN** → Click "Add" ở đầu
- Cấu hình:**
 - Action:** Pass
 - Source:** 192.168.1.100
 - Destination:** any
 - Schedule:** chọn allow_work_hours_8h_17h
 - Description:** Allow 192.168.1.100 in working hours



3. Tạo rule BLOCK ngay dưới:

- **Action:** Block
- **Source:** 192.168.1.100
- **Destination:** any
- **Description:** Block out of working hours

4. Save → Apply Changes



□ Kiểm tra

- Từ client 192.168.20.100, kiểm tra:
 - Có vào được internet trong giờ cho phép không?
 - Có bị chặn ngoài giờ?
 - Có bị chặn nếu truy cập port khác (ví dụ SSH - port 22)?

🔑 Ghi chú

- Các rule xử lý **từ trên xuống** – hãy đặt rule có độ ưu tiên cao hơn ở trên.
- Time-based rules **phụ thuộc vào giờ hệ thống pfSense**, hãy đảm bảo đã cấu hình đúng timezone (System → General Setup).
- Có thể dùng **Aliases** nếu muốn áp dụng cho nhiều IP hoặc nhóm port.