

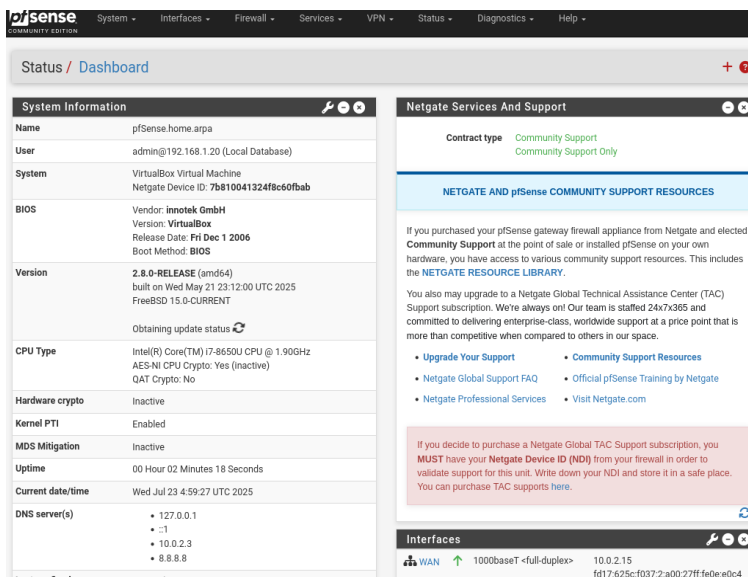
Firewall Setup and Configuration (pfSense)

➤ Introduction

In this, we will configure the pfSense firewall to secure a network by creating rules, blocking suspicious traffic, and documenting the setup using screenshots. pfSense is a powerful, open-source firewall and router software used for network protection.

• **Step 1: Access pfSense Web Interface**

1. Open a web browser in your system.
2. Type the IP address of your pfSense system (e.g., <http://192.168.1.1>).
3. Enter your username and password to log in.



pfSense Dashboard after Login

• **Step 2: Configure Basic Firewall Rules**

1. Navigate to 'Firewall' > 'Rules'.
2. Select the interface (LAN).
3. Click the 'Add' button to create a new rule.
4. Set the following parameters:
 - Action: Pass or Block
 - Interface: LAN
 - Protocol: TCP/UDP
 - Source: Any
 - Destination: Any or specific IP
 - Destination Port: (Optional - e.g., 80 for HTTP, 443 for HTTPS)
5. Click 'Save'.
6. Click 'Apply Changes' at the top.

Kali Linux [Running] - Oracle VirtualBox

FileMachineViewInputDevicesHelp

pfSense.home.arpa - Sta

https://192.168.1.1

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DB

pfSense
COMMUNITY EDITION

System

Interfaces

Firewall

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Services

VPN

https://www.kali.org/docs/

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.

Source

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

FloatingWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	D
<input checked="" type="checkbox"/>	✓ 1/176 KIB	*	*	*	LAN Address	443	*	*		A
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	*	*	none		
<input type="checkbox"/>	✓ 3/3.13 MiB	IPv4 *	LAN subnets	*	*	*	*	none		C
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		C

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

💾 Save

➕ Separator

i

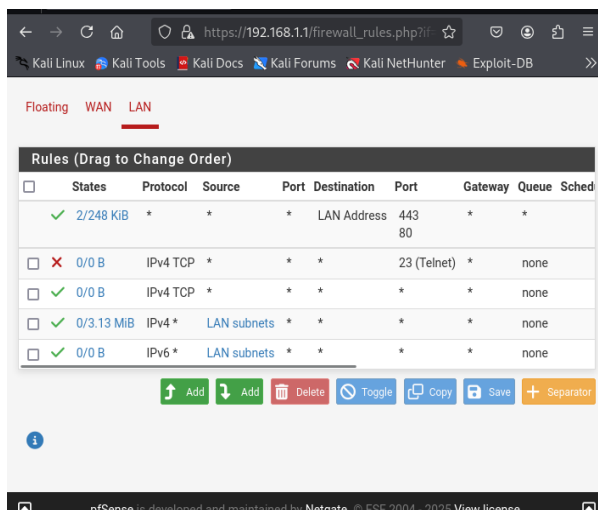
Right Ctrl

Rules Page after Saving Changes

- **Step 3: Block Suspicious Traffic**

Example: Block access to Telnet (port 23):

1. Click 'Add' at the top of the LAN rules list.
2. Set:
 - Action: Block
 - Protocol: TCP
 - Source: Any
 - Destination: Any
 - Destination Port Range: From 23 to 23
3. Save and Apply Changes.



Block Rule for Telnet

- **Step 4: Verify Configuration**

1. Go to 'Status' > 'System Logs' > 'Firewall'.
2. Check logs to see blocked or allowed traffic.
3. You can also test connectivity from another system.