# Step-by-Step Guide: Installing and Configuring pfSense Virtual Firewall on Kali Linux VM (VMware Workstation Pro)

## 1. Introduction

In cybersecurity and network administration, firewalls play a critical role in protecting systems from unauthorized access and malicious activity. pfSense, a free and open-source firewall and router platform based on FreeBSD, provides enterprise-grade security features suitable for virtualized environments. This guide offers a step-by-step walkthrough for installing, configuring, and using pfSense as a virtual firewall between a Kali Linux VM and other network nodes within VMware Workstation Pro.

## 2. Project Background

In modern cybersecurity labs, simulating real-world network environments is essential for learning and testing. Virtual firewalls like pfSense provide a controlled, flexible way to manage and analyze network traffic between virtual machines. By integrating pfSense with Kali Linux, users can practice intrusion detection, packet inspection, and intrusion prevention using actual network data without impacting real systems.

## 3. Importance and Uses

Implementing pfSense as a virtual firewall serves several key purposes;

1. Network Segmentation: Isolate and secure different virtual networks within a single host.
2. Traffic Monitoring: Analyze incoming and outgoing packets for security evaluation.
3. Intrusion Detection/Prevention: Use tools like Suricata and rule sets such as Emerging Threats Open (ETOpen) to detect and block malicious activities.
4. Learning Environment: Provides hands-on experience with enterprise-level firewall and IDS/IPS configurations.

## 4. Step-by-Step Setup Guide

Step 1: Download pfSense ISO  
1. Visit the official pfSense website: <https://www.pfsense.org/download/>   
2. Select AMD64 (64-bit) architecture and ISO Installer.  
3. Choose the nearest mirror and download the file.  
  
Step 2: Create a New Virtual Machine in VMware Workstation Pro  
1. Open VMware Workstation Pro.  
2. Click Create a New Virtual Machine.  
3. Select Typical (recommended) setup and click Next.  
4. Choose Installer disc image file (ISO) and browse to the downloaded pfSense ISO.  
5. Set OS type to FreeBSD 64-bit.  
6. Assign 2 GB RAM and 1 CPU core (minimum recommended).  
7. Create a new 20 GB virtual disk.  
8. Complete the wizard and power on the VM.  
  
Step 3: pfSense Installation  
1. Boot the VM and follow on-screen instructions.  
2. Choose Install pfSense, accept defaults, and continue.  
3. After installation, reboot the system.  
4. Log in to the pfSense console (default username: admin, password: pfsense).  
  
Step 4: Configure Network Interfaces  
1. Assign interfaces:  
 - WAN Interface: Connects to the internet (e.g., NAT or Bridged).  
 - LAN Interface: Connects to the internal lab network (e.g., Host-Only).  
2. From the pfSense console, go to Interfaces > Assignments to adjust as needed.  
3. Ensure the LAN network uses a private IP range (e.g., 192.168.10.1/24).  
  
Step 5: Connect Kali Linux VM  
1. In VMware, edit Kali VM settings.  
2. Add a second network adapter and set it to the same Host-Only network as pfSense LAN.  
3. Start Kali and confirm connectivity:  
 ping 192.168.10.1  
  
Step 6: Access pfSense Web Interface  
1. Open a browser in Kali.  
2. Visit https://192.168.10.1.  
3. Login with credentials (admin / pfsense).  
4. Follow the setup wizard to configure WAN, LAN, hostname, DNS, and password.  
  
Step 7: Install and Configure Suricata  
1. Navigate to System > Package Manager > Available Packages.  
2. Search and install Suricata.  
3. After installation, go to Services > Suricata.  
4. Click Add Interface and select LAN.  
  
Step 8: Download Emerging Threats Open (ETOpen)  
1. In Suricata interface settings, enable EVE JSON Logging.  
2. Under Rules Update Settings, enable ETOpen Rules.  
3. Click Update Rules.  
  
Step 9: Enable Intrusion Prevention (IPS Mode)  
1. Go to Interfaces > LAN > Settings in Suricata.  
2. Enable IPS Mode (block offenders).  
3. Save and apply changes.  
  
Step 10: Monitor Logs and Alerts  
1. Navigate to Services > Suricata > Logs View.  
2. Select Alerts, Blocked, or EVE JSON tabs to review traffic events.  
3. Use Status > System Logs > Firewall to view blocked and allowed traffic.

## 5. Conclusion

With pfSense deployed as a virtual firewall, your Kali Linux lab now has a professional-grade network security layer. By integrating Suricata and ETOpen rules, you can detect, block, and analyze threats in real time. This setup is ideal for learning intrusion detection, firewall management, and incident analysis in a controlled environment.

Author: Matthew E. Bello

*Jr. SOC Analyst (Entry Level)*

[belloematthew@gmail.com](mailto:belloematthew@gmail.com)

Date: October 2025

Version: 1.0