Home-Lab Walk-Through: pfSence ↔ Kali ↔ Ubuntu (Do5 Defense Demo)

1. Objectives

- Stand up a pfSense firewall in VirtualBox with separate WAN (bridged) and LAN (internal) segments.
- Put Kali Linux on the WAN side to simulate an external attacker.
- Put Ubuntu Desktop on the LAN side as the victim host.
- Demonstrate DoS traffic with hping3 and show it in Wireshark.
- Mitigate the attack using pfSense firewall rules and view the resulting logs.

2. Topology G IP Plan

Device / Segment	VirtualBox Adapter	Interface	IP / Subnet	Role
Home LAN (physical)	— (host network)	—	192.168.0.0/24	Provides Internet & bridges to lab
pfSense WAN	Bridged	vtnet0	Eg. 192.168.0.254/24 → GW 192.168.0.1	Edge firewall toward home LAN
Kali Linux (Attacker)	Bridged	eth0	Eg. 192.168.0.200/24	External attacker host
Lab LAN (internal `LabNet`)	Internal Network	—	192.168.1.0/24	Isolated subnet behind pfSense
pfSense LAN	Internal `LabNet`	vtnet1	192.168.1.1/24 (DHCP .100-.199)	Default GW & DHCP/DNS relay
Ubuntu Desktop (Victim)	Internal `LabNet`	eth0	192.168.1.100/24	Victim workload

3. Prerequiiitei

- VirtualBox ≥ 7.x installed on host (Windows/macOS/Linux)
- ISO images (download whatever is the latest ISO on the respective download sites)

  pfSense-CE-2.7.x-amd64.iso

  kali-linux-current-amd64.iso

  ubuntu-22.04-desktop-amd64.iso

- Minimum host resources: 8 GB RAM, 40 GB free disk
- Administrative rights on the host (to create bridged adapters)

4. Lab Environment 5etup

4.1 Create pfSense VM

Name pfSense

OS Type FreeBSD 64-bit

CPUs / RAM 2 vCPU / 2 GB

Disk 20 GB VDI (dynamically-allocated)

Adapter 1 Bridged → Physical NIC

Adapter 2 Internal Network → LabNet

Attach the pfSense ISO under Settings ▸ Storage and start the VM

4.2 Create Kali VM (Attacker)

Debian 64‑bit, 2 vCPU, 2 GB RAM, 15 GB disk.

Adapter 1: Bridged.

Choose the ISO image downloaded and set up the Kali Linux on VBOX. After install you must delete the ISO image and boot from the virtual disk.

4.3 Create Ubuntu VM (Victim)

Ubuntu 64‑bit, 2 vCPU, 2 GB RAM, 15 GB disk.

Adapter 1: Internal Network → LabNet.

Create LabNet once: in any VM's Network ▸ Internal Network drop‑down type the name LabNet; VirtualBox auto‑creates it.

Choose the ISO image downloaded and set up the Ubuntu on VBOX. After install you must delete the ISO image and boot from the virtual disk.

5. pf5enıe 5ET UP

- Install pfSense (accept defaults).
- Console menu → 1) Assign Interfaces: vtnet0 = WAN (Bridged) vtnet1 = LAN (LabNet).
- Leave WAN as DHCP – pfSense pulls an address from the home router automatically. Watch the console; note the WAN IP (e.g. 192.168.0.58).

5.1 Reaching pfSense from the WAN

- Via the pfsense you will have to enter the shell and then disable the pfsense firewall by running the following command: pfsense -d
- Now log into the PFSENSE over the WAN using the WAN IP address. Default credentials are admin and pfsense.

- You will need to add a firewall rule to allow WAN GUI access, which can be done as follows:
- Firewall ▸ Rules ▸ WAN ▸ Add: Action Pass, Protocol TCP, Source <home network>, Destination <pfsense WAN>, Port 443, Description “Allow GUI access from home network”.
- Apply and save the rule and now you should have WAN access

5.2 Configure LAN DHCP

- You can do so by navigating to Services ▸ DHCP Server ▸ LAN.
- Tick “Enable DHCP server on LAN interface.”
- Range: 192.168.1.100 – 192.168.1.199
- DNS servers: 192.168.0.1 (home router)
- Save → Apply Changes.

5.3 Add rule to allow Kali access to Internal LAN network

This is being done purely to demonstrate the flood attack which we will then block by adding another rule later on.

Add the rule on the WAN interface as follows:

- Firewall ▸ Rules ▸ WAN ▸ Add: Action Pass, Protocol Any, Source <Kali Linux IP>, Destination <Ubuntu LAN IP>, Description “Allow Kali access to Ubuntu”.

Note- To check the Ubuntu LAN IP you would need to run step 7, alternatively you can perform this section after you complete booting the ubuntu and checking its IP.

6. Kali Linux 5etup (Attacker)

Kali gets its address from the home router automatically.

On the CLI on the Kali Machine, you can check the IP address by running the below command

Ifconfig

- Next we will add a route on the Kali to provide reachability to the Internal subnet where the Ubuntu sits

sudo ip route add 192.168.1.0/24 via <PFSENSE_WAN_IP>

Replace <PFSENSE_WAN_IP> with the real value (e.g. 192.168.0.58).

Tip: if the WAN IP ever changes, update this route or script it.

7. Ubuntu 5etup (Victim)

Ubuntu boots, grabs 192.168.1.100 from pfSense DHCP, and sets pfSense (192.168.1.1) as gateway & DNS.

Verify:

ifconfig

ping -c3 google.com # Test Internet reachability on the Ubuntu

Note - Once all devices have gotten IP's and you have the necessary firewall rules and static routes in place, test connectivity by pinging from Kali to the Ubuntu machine and it should succeed.

8. Launching the Do5 (hping3)

- Start Wireshark on Ubuntu
- sudo apt update && sudo apt install -y wireshark
- sudo wireshark & # capture on eth0
- Start the flood from Kali
- sudo hping3 -1 --flood 192.168.1.100 # ICMP flood
- # or SYN flood: sudo hping3 --flood -S -p 80 192.168.1.100
- View Packets spike in Wireshark.

9. Blocking the Attack G Verifying

- Now we will navigate to the PFSENSE WebGUI and add a new security rule to block traffic from the Kali to the Ubuntu Machine
- pfSense Firewall ▸ Rules ▸ WAN ▸ Add (TOP): Action Block, Source Kali−IP, Destination 192.168.1.100/24 (Ubuntu IP), Log ✓, Description “Block Kali DoS”.
- Apply – traffic halts, check wireshark on the Ubuntu machine and you shouldn't see the flood anymore.
- On the PFSENSE go the firewall rule and you can check the logs for the rule where you enabled logging to verify that malicious flood traffic is being blocked.

10. Wrap-Up G Next 5tepı

- You have built a two-zone pfSense lab using DHCP on the WAN, attacked it, and then blocked it using a firewall
- You have configured the networking for this home lab using different types of network adapters in virtual box as well as static routes, DHCP scopes etc.
- **Security Best Practices**: Keep your homelab isolated from production networks.
- **Maintenance**: Regularly update Ubuntu, Kali, and SafeLine WAF to patch vulnerabilities.