Escuela Colombiana de Ingeniería Julio Garavito

Demo Company
IT Security and Privacy

Security Architecture

Students:

Laura Sofia Gil Chaves

Camilo Castaño Quintanilla

Teacher:

Ing. Daniel Vela

Business Confidential

December 4th , 2024

Project 01-11

Version 1.0

Table of Contests

Assessment Overview

From Thursday, November 28 to Tuesday, December 4 we configured and tested pfSense, a highly versatile open-source firewall and router. During this lab, we followed a series of detailed steps that included downloading the appropriate installation image, configuring a virtual machine in VirtualBox with specific network interfaces, and customizing firewall rules to manage traffic and access. We configured essential services such as the DHCP server to automatically assign IP addresses to devices on our internal network and tested connectivity between virtual machines using custom rules. In addition, we implemented and verified a firewall rule to block ICMP requests to the public DNS server 8.8.8.8, demonstrating the granular control that pfSense allows over network traffic.

1.Planning: We define the objectives of the lab, organizing the necessary steps to install and configure pfSense in a virtual environment. Identified the key tools, such as VirtualBox, Kali Linux and Ubuntu, for the simulations. We plan the virtual network structure with WAN and LAN interfaces to emulate a realistic environment.

2.Discovery: We explore the initial pfSense configuration, verifying IP address assignment and basic connectivity. We confirmed DHCP server operation and web console accessibility. We performed connectivity tests through pings to evaluate the functionality of the configured network.

3.Attacking: We implement firewall rules to block and allow specific traffic, such as ICMP protocol. We test these rules from internal virtual machines to validate their effectiveness and tuning. We verify the order of the rules in the firewall to prioritize blocking over configured exceptions.

4.Reporting: Documentation of attack and possible mitigation options.

Plan → Discovery → Attack →Report

Assessment Components

External Penetration Test

We configured and tested pfSense, an open-source firewall and router. We downloaded the installation image, configured a virtual machine in VirtualBox with specific network interfaces and customized firewall rules to manage traffic. We configured essential services such as the DHCP server to automatically assign IPs and tested connectivity between virtual machines. In addition, we implemented and verified a firewall rule to block ICMP requests to the public DNS server 8.8.8.8, demonstrating the granular control that pfSense offers over network traffic.

Scope

Assessment	Details
External Penetration Test	Index of /mirror/downloads/

Scope Exclusions

There will be no scope exclusions regarding Security Architecture, as all testing will be conducted in a secure and controlled laboratory environment.

Client Allowances

The permissions required to perform the tests will be provided by the laboratory teacher, which will allow full access to all necessary files and resources.

Executive Summary

In this lab we configure and evaluate pfSense, an open-source firewall and router, to understand its capabilities in network management. We installed pfSense on a virtual machine configured in VirtualBox, defining a network structure with WAN and LAN interfaces. We configured essential services such as the DHCP server, which enabled automatic assignment of IP addresses to devices on the internal network. In addition, we customized firewall rules to control traffic, including the implementation of a specific rule to block ICMP requests to the public DNS server 8.8.8.8. We performed extensive connectivity testing between virtual machines to verify the correct operation of the configured rules and services.

Attack Summary

The following table describes how we built the firewall, step by step:

Step	Action	Recommendation
1	We set up virtual machines in VirtualBox: pfSense with two network interfaces (WAN: bridge adapter, LAN: PrivNet internal network), Kali Linux and Ubuntu connected to the PrivNet internal network.	Verify that the network interfaces are correctly configured and connected before starting the tests.
2	We created a rule in pfSense to block ICMP traffic directed to the DNS server 8.8.8.8 from the internal network. This rule was applied on the LAN interface firewall.	Document and test firewall rules before applying them in production environments to avoid unexpected disruptions to legitimate traffic.

3	From the Kali Linux and Ubuntu machines, we performed connectivity tests by pinging 8.8.8.8 to validate ICMP traffic blocking. We observed “Destination Host Unreachable” responses.	Use tools such as pfSense logs to audit and monitor the blocked traffic, ensuring that the rule meets its objective without affecting other services.
4	Validated that pfSense correctly implemented blocking and allowed granular control over internal network traffic, highlighting its effectiveness.	Perform periodic simulations to ensure that security rules and configurations remain up-to-date and effective in the face of new threats.

Security Weaknesses

The following is a description of the weaknesses that a system may have in the absence of a firewall:

Unauthorized access

Without a firewall, any device connected to the network can be accessible from the outside. This allows attackers to exploit open ports and vulnerabilities to gain unauthorized access to internal systems.

Denial of Service Attacks (DoS/DDoS)

Firewalls help filter and limit unwanted traffic. Without them, the network is vulnerable to DoS/DDoS attacks, where an attacker can overload servers with malicious traffic, causing service interruptions and failures.

Malware propagation

Firewalls block suspicious traffic, including malware infiltration attempts. Without this protection, networks can easily be infected with viruses, ransomware or other malicious software through uncontrolled external connections.

Lack of segmentation and control of internal traffic

Without firewalls, it is not possible to segment the network or monitor internal traffic. This makes it easy for an attacker who compromises an internal device to move laterally within the network, escalating privileges and accessing critical resources.

External Penetration Test Findings

External Penetration Test Findings

Description:	We configured pfSense, creating a virtual network with custom firewall rules, a DHCP server and connectivity testing. We verified the blocking

	of ICMP requests to DNS 8.8.8.8.8, highlighting its control over network traffic on the other Kali Linux and Ubuntu virtual machines.
Impact:	Critical
System:	Windows
References:	Index of /mirror/downloads/

Exploit Proof of Concept

After installing the pfSense DVD image (ISO) installer, configure your virtual machine property.

Machine name: pfSense.

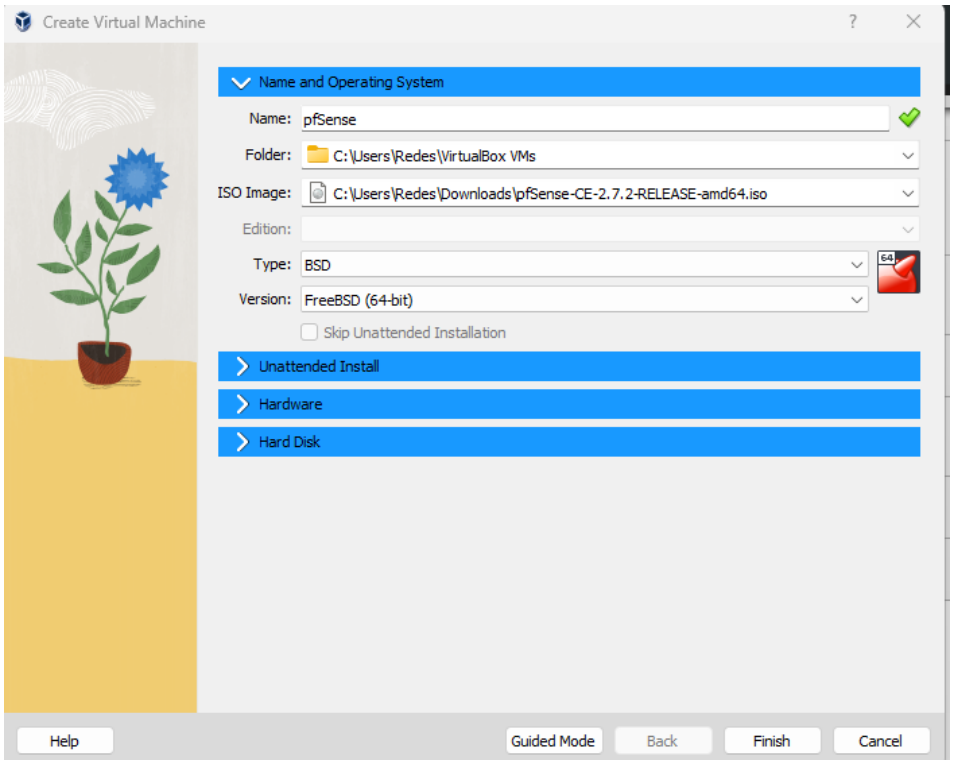
Accept the default folder location.

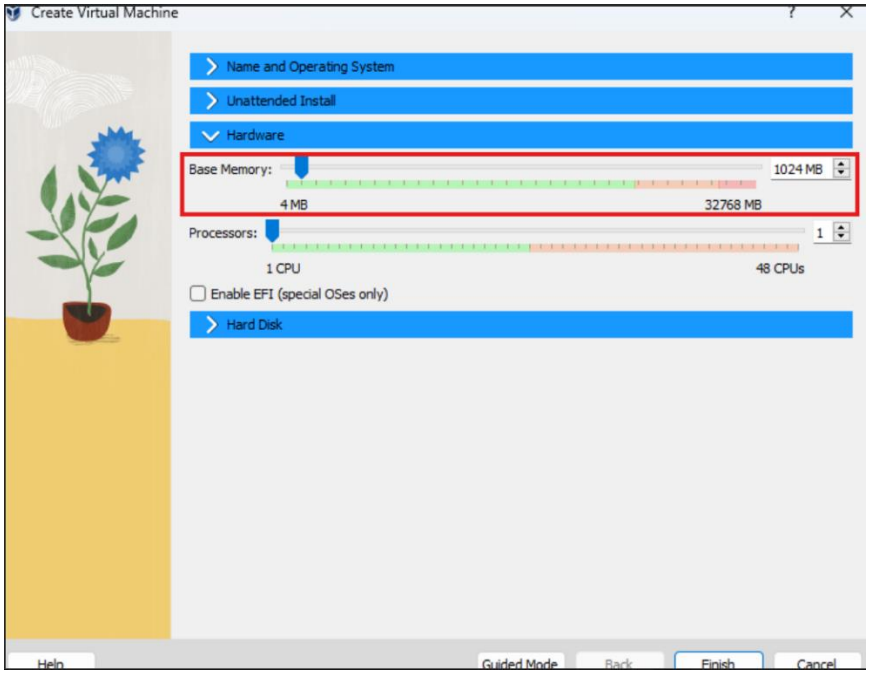
Type: BSD

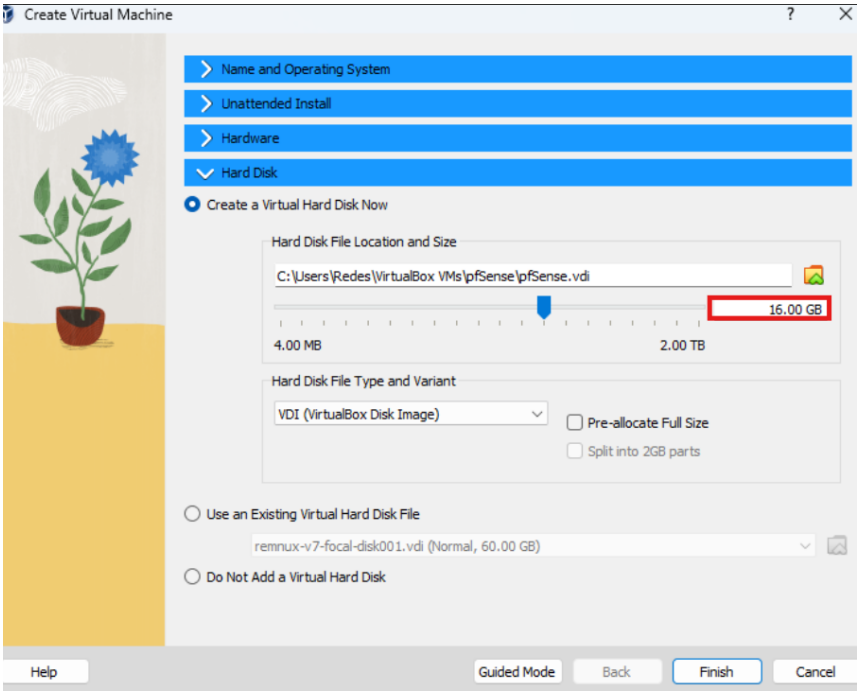
Version: FreeBSD (64-bit).

Memory size: 1024 GB.

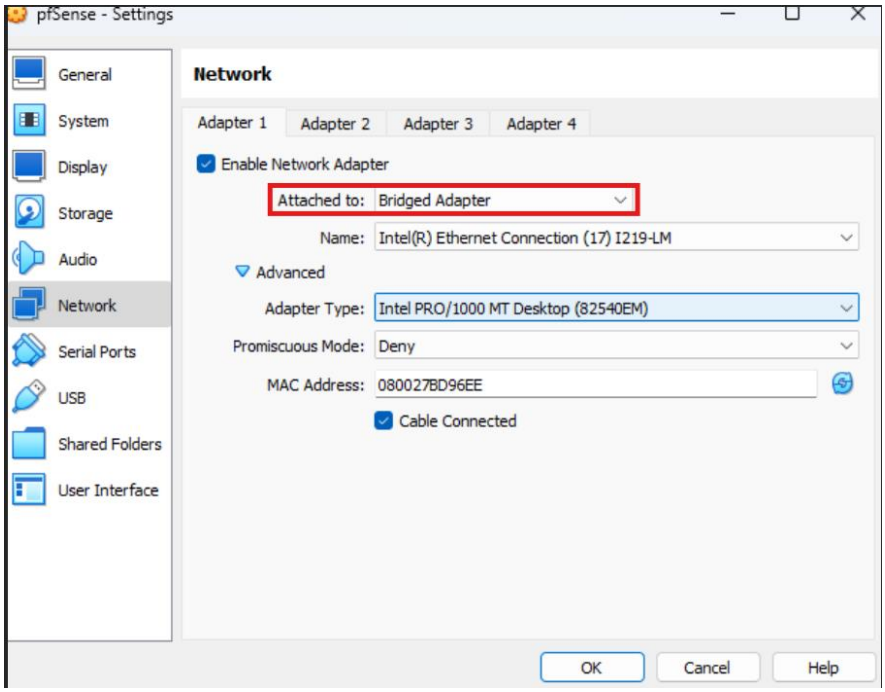
Hard Disk size: 16 GB.



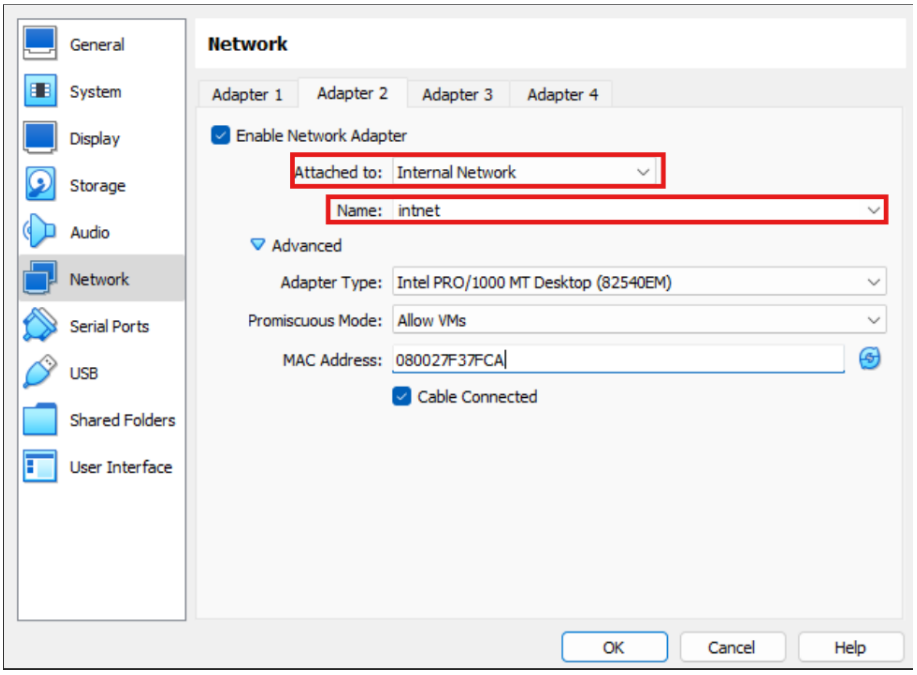




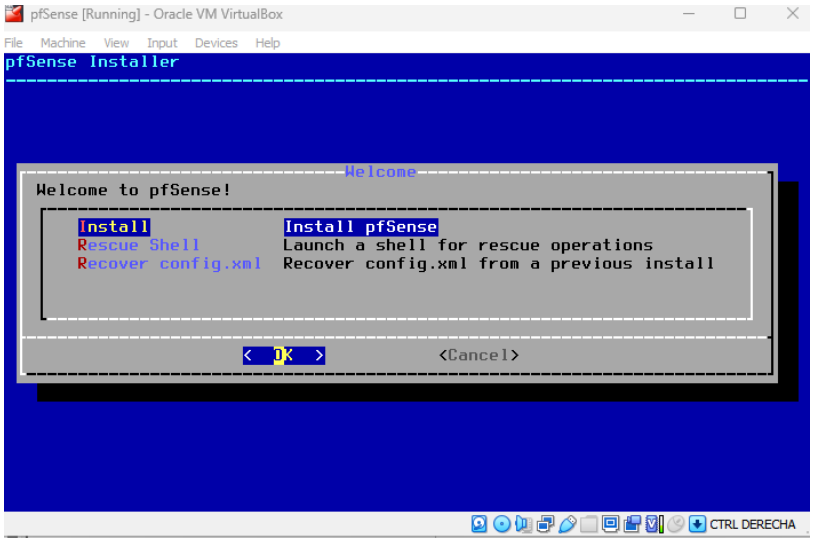
Set adapter 1 to **Bridge Adapter,** this adapter will be the WAN adapter and will connect to the internet.



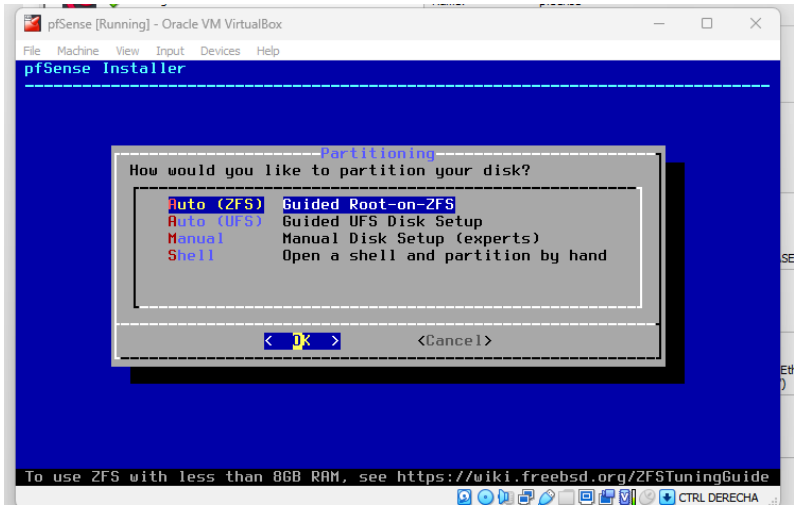
Enable Adapter 2 and set it to Internal Network. Then, change the name to **Privnet,** this adapter will be the LAN interface.



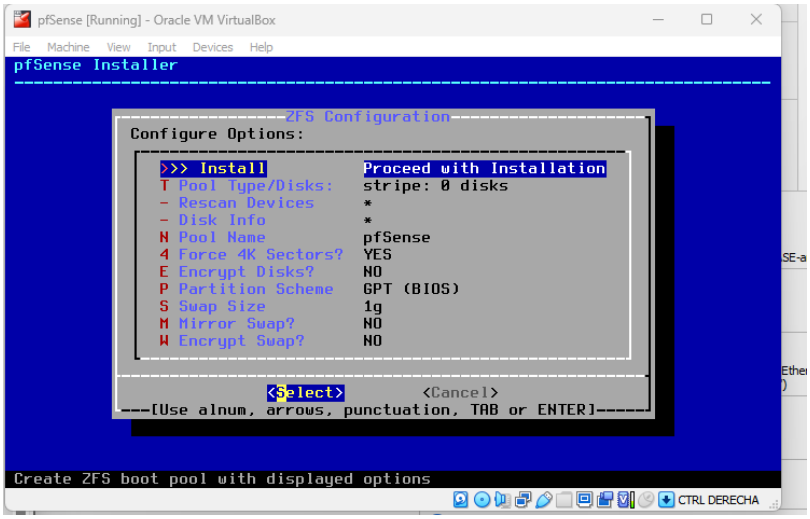
Select **Intall pfSense** and click OK.



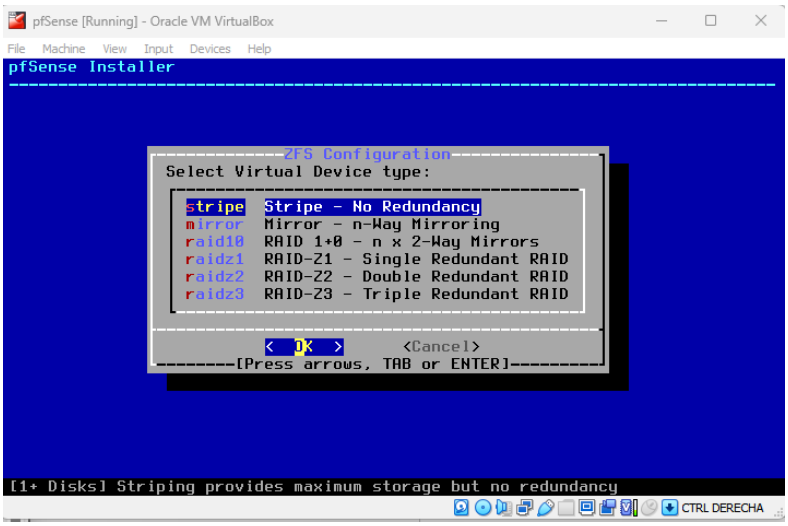
Select **Auto (2FS) Guided Root-on-ZFS** and click ok.



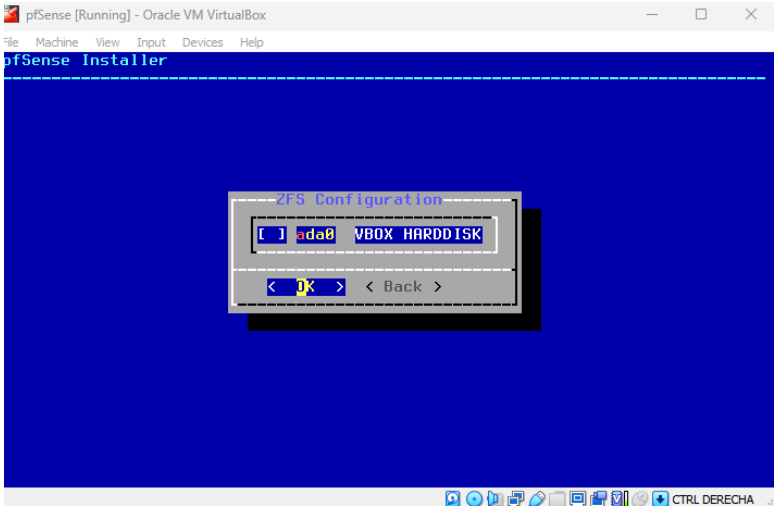
Select **Install Proceed with installation** and click Select.



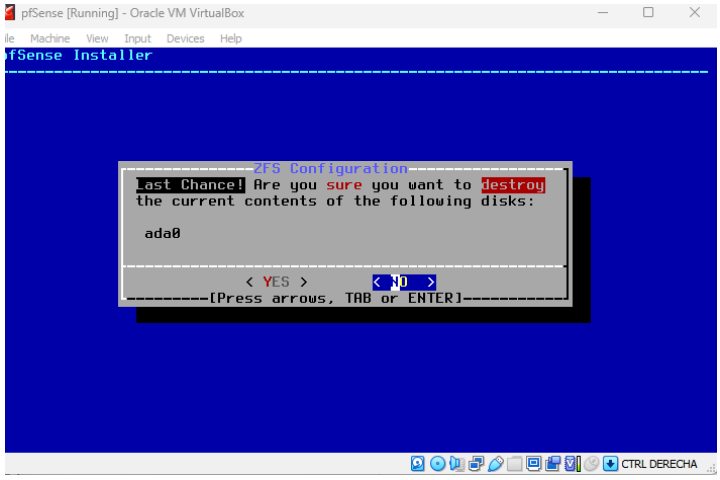
Select **stripe Stripe – No Redudancy** and then select OK.



Select **ada0 VBOX HARDDISK** and then OK.



In the ZFS configuration select YES.

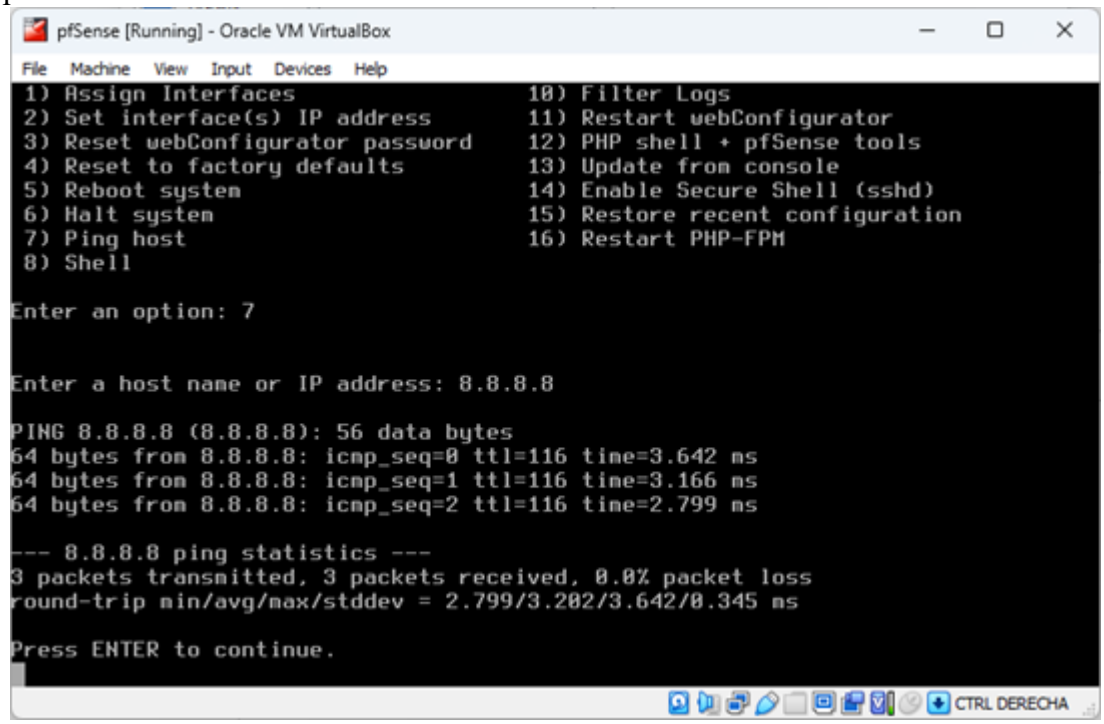


Once the installation is finished, retire the ISO and reboot the machine. Then, configure the WAN and LAN interfaces.

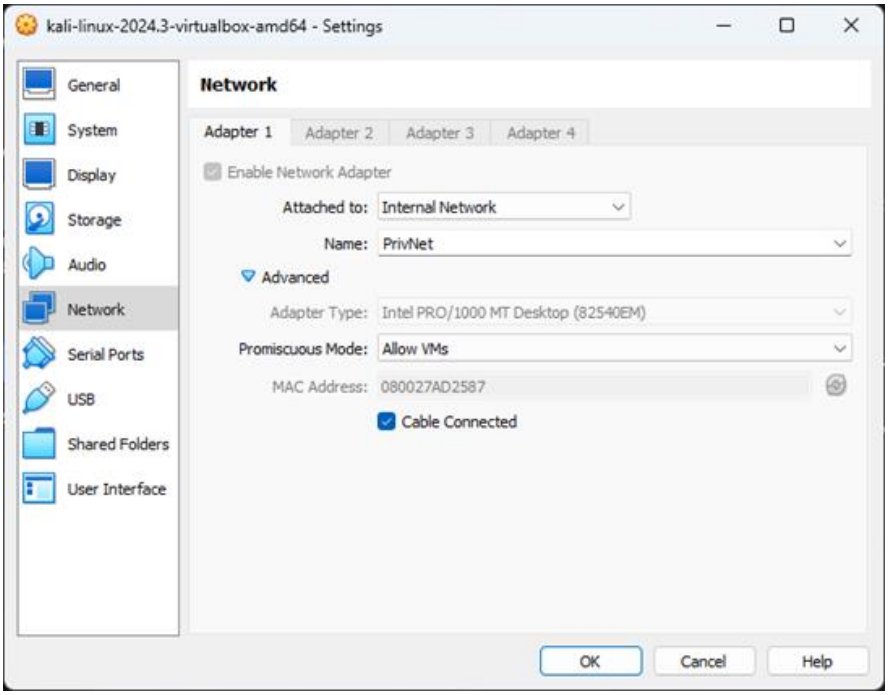
- **WAN:** 10.2.65.102/16
- **LAN:** 172.16.1.1/16

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 10.2.65.102/16
 LAN (lan)       -> em1        -> v4: 172.16.1.1/16

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Nov 28 23:17:17 ...
php-fpm[394]: /index.php: Successful login for user 'admin' from: 172.16.1.100 (
Local Database)

Message from syslogd@pfSense at Nov 28 23:29:00 ...
php-fpm[17598]: /index.php: Successful login for user 'admin' from: 172.16.1.100
 (Local Database)
```

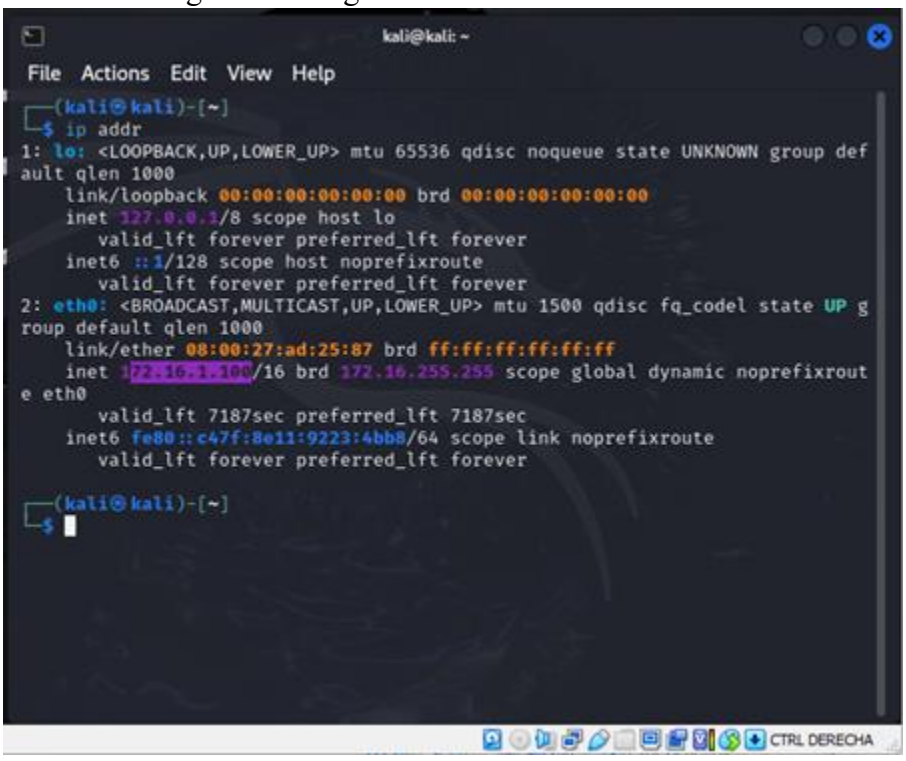
To verify connectivity, perfom a ping from **pfSense** to **8.8.8.8**, receiving a successful response.



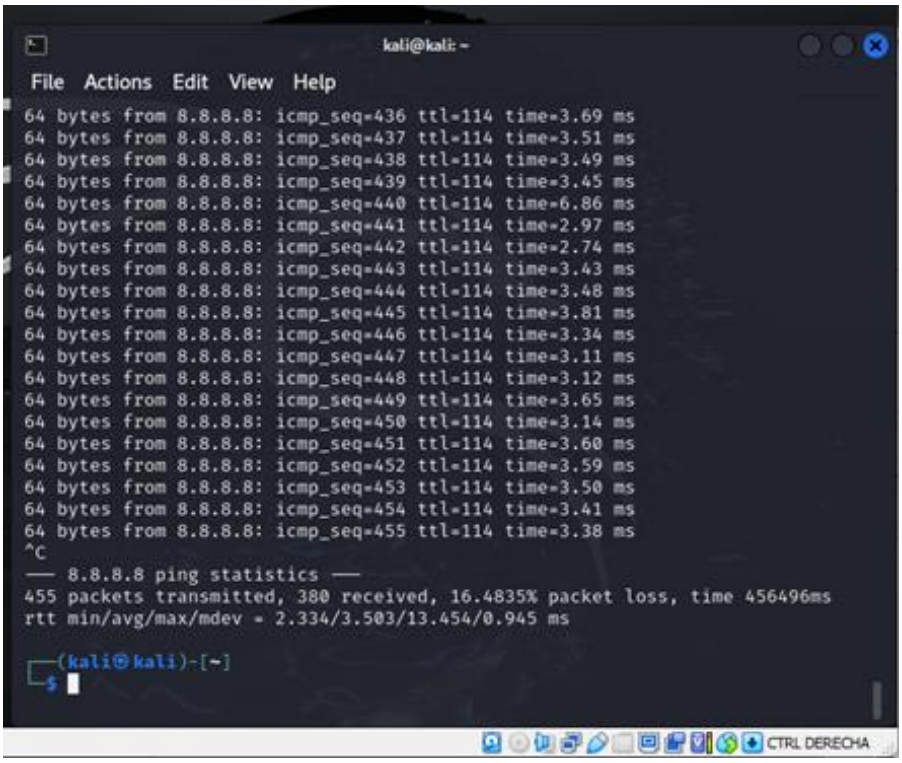
Connect the Kali Linux machine to the "PrivNet" network. On this machine, the **Automatic (DHCP)** option isenabled to automatically obtain an IP address from the **pfSense** DHCP server.



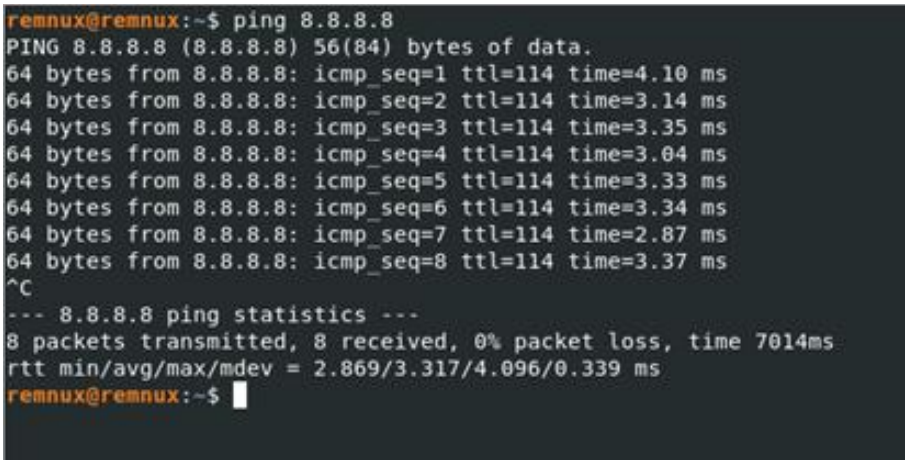
Verify the IP address assignation using **addr** command.



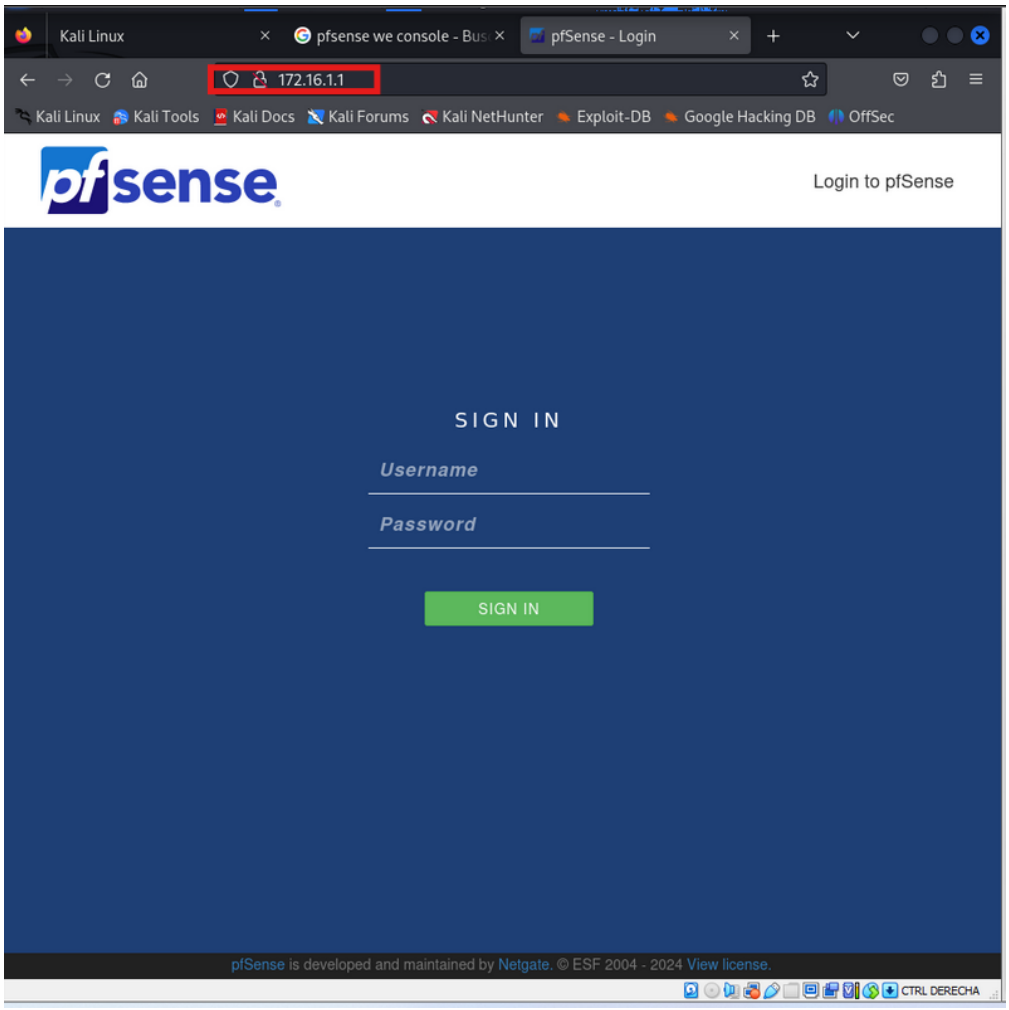
Verify the connection, with **ping** to 8.8.8.8



Repeat the process on Ubuntu machine.



In the Kali Linux machine, access the pfSense web console via a browser using the LAN IP 172.16.1.1



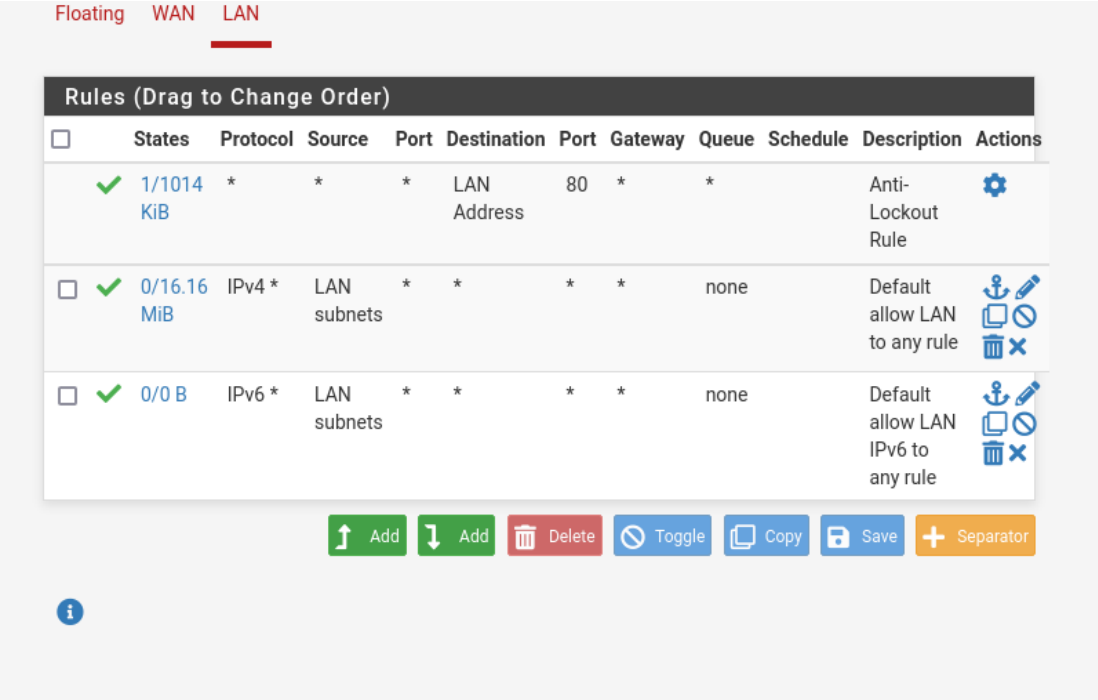
Enter the credentials:

- **Username:** admin.
- **Password:** psfense.

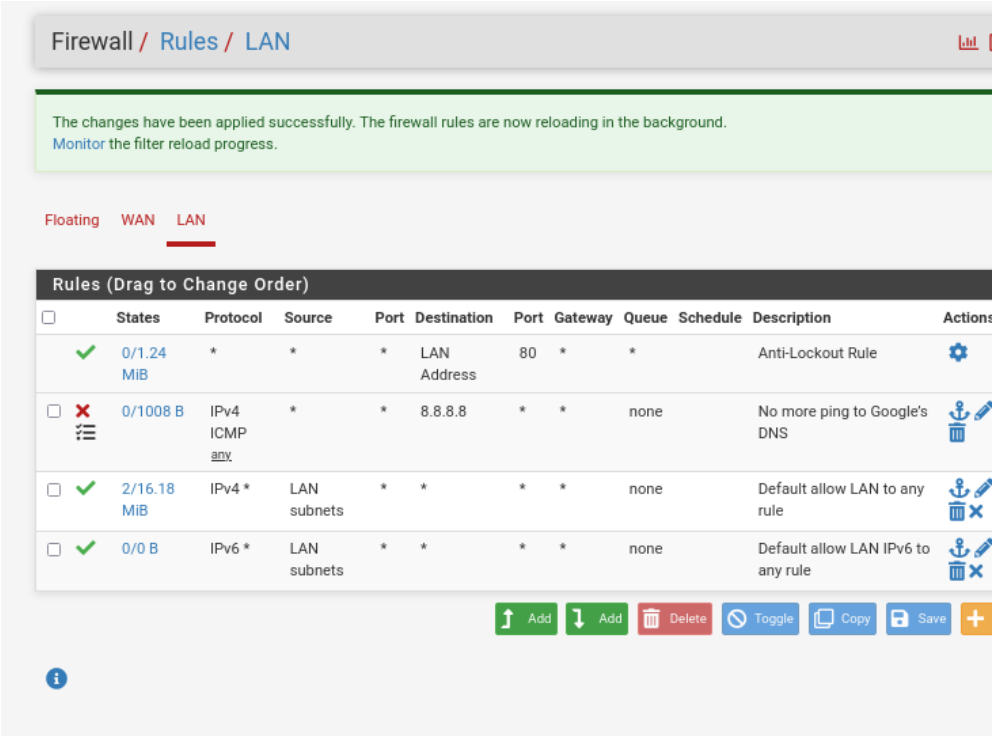
in pfSense configure the firewall rules. Create a rule on the **LAN interface** to block ICMP packets directed to **8.8.8.8**, enabling the logging of blocked packets, following conditions were implemented for the rule:

- **Interface**: LAN
- **Protocol**: ICMP
- **Source**: Any
- **Destination**: 8.8.8.8
- **Logging**: Enabled for blocked packets.

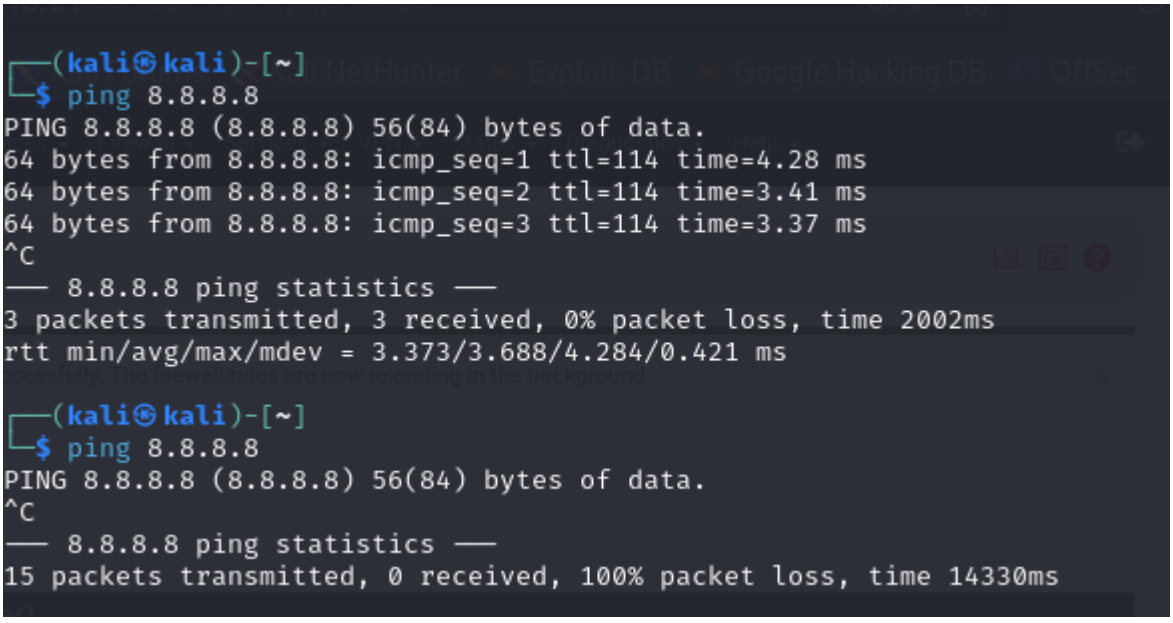
Save the changes



and look at the changes made to the site



If you test the rule, you will notice that the destination is unreachable, so the firewall was configured successfully.



```
remnux@remnux:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=3.45 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=3.40 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 3.403/3.427/3.452/0.024 ms
remnux@remnux:~$ ping 8.8.8.8
ping: connect: Network is unreachable
remnux@remnux:~$
```

Recommendation:

Who:	The system security team and developers of the programs.
Vector:	Remote.
Action:	*Item 1*: Make sure the firewall is configured at the entry/exit point of the network to control incoming and outgoing traffic. Use strict policies to block unauthorized traffic and allow only necessary connections. *Item 2*: Set up custom rules to block unnecessary ports, restrict insecure protocols (such as Telnet or FTP) and allow only legitimate traffic based on network requirements. Keep these rules updated regularly. *Item 3*: Configure the firewall to log and monitor both successful and failed access attempts. Implement alerts to detect suspicious activity, such as multiple failed access attempts or unusual traffic spikes. *Item 4*: Use internal firewalls to segment the network into isolated subnets. This limits lateral movement of attackers within the network and protects critical data in specific areas from unauthorized access.