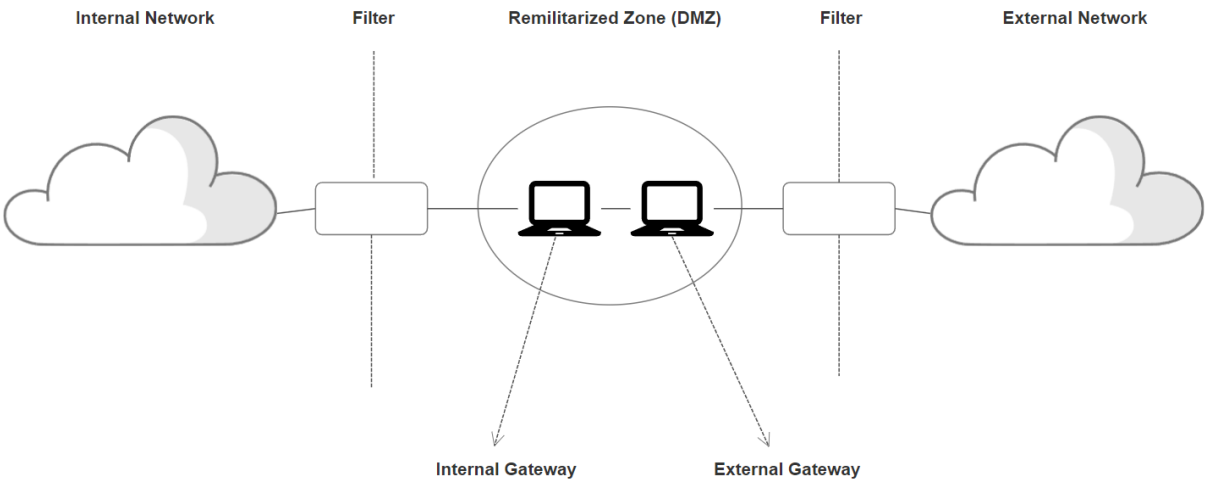
FIREWALL

Introduction

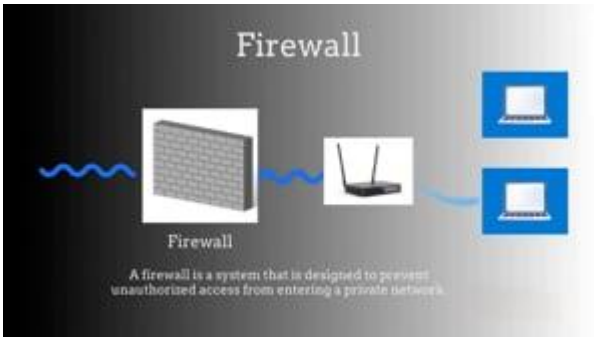
A firewall is a type of network security that analyzes and regulates all incoming and outgoing network data based on rules that have already been set. It stands between an internal network that you can trust and an outward network that you can't, like the Internet. A firewall's main job is to set up a security barrier and stop people from getting in without permission or doing illicit activities.

Firewalls can be implemented both in hardware and software forms.

The figure below tells you that a firewall has various basic components like host, router filters, and services.



Remilitarized Zone is a wall between the internal and external network used to secure the internal network. This is a basic firewall used to protect the network. The internal gateway refers to the specific interface or designated area within a firewall system that establishes a connection to an organization's internal network. The side of the firewall that is oriented towards the network encompassing the organization's devices, servers, and other resources is referred to as the internal-facing side. The internal gateway assumes a critical function in the prevention of unlawful intrusion from external sources into the internal network. The application of security policies to regulate the flow of traffic from external sources into the internal network is typical. External gateway is the part of the firewall that connects to the outside network, which is usually the Internet. This is the part of the firewall that faces the outside world. Its job is to filter Internet traffic and only allow safe, authorized traffic into the internal network. The external gateway helps keep the internal network safe from threats that come from the outside, like attacks from hackers, people trying to break in without authorization, and other security risks that come from the Internet.



How Firewalls work?

The basic overview of how firewall works:

1. Packet filtering Firewalls:
    - Operates at layer 3 (network layer) of the OSI model.
    - Packet filtering is based on the criteria such as destination Ip address, port numbers, and protocols.
2. Stateful Inspection Firewalls:
    - Keep track of the status of active connections and make decisions depending on traffic situations.
    - Analyze the connection's state to determine whether to allow or stop traffic.
    - They know what's going on with the network links, which makes them safer than packet-filtering firewalls.
3. Proxy Firewalls:
    - Intermediaries between client and server connections.
    - Examine and filter communications at the application layer (Layer 7) of the OSI model.
    - By masking the main network's topology, it is possible to provide content filtering and increased security.
4. Application Layer Firewalls:
    - These, like proxy firewalls, operate at the application layer.
    - Data packets are monitored, filtered, and blocked based on the application or service generating the traffic.
    - Precise control over user access to apps and services is provided.
5. Next-Generation Firewalls (NGFW):
    - Integrate standard firewall functions with advanced security features like application awareness, VPN support, and intrusion prevention.
    - Offer enhanced capabilities for detecting and preventing threats.

Firewall Deployment scenarios

1. **Perimeter or network edge firewall**
   Placed at the network perimeter, between the internal network and the internet. It protects the internal network from external threats. Filters incoming and outgoing traffic based on defined security rules.
2. **Internal Firewalls:**
   Placed within the internal network to separate different segments or departments. Its purpose is to Segments the internal network into zones for added security. It Controls traffic between internal network segments, providing an additional layer of protection.

3. **Demilitarized Zone firewall (DMZ):**
   Placed between the internal network and the DMZ, hosting public-facing services. Its purpose is to Secures the area between the internal network and external-facing services. It Controls traffic to and from the DMZ, allowing limited access to internal resources.
4. **Application Layer Gateway (Proxy):**
   Often integrated into firewalls or as standalone proxies. It Controls and inspects traffic at the application layer. It Acts as an intermediary between users and the internet, filtering and caching content.
5. **Host-Based Firewall:**
   It is installed on every individual device. It protects individual devices. It monitors and controls incoming traffic on the specific host.

Tools and technologies used

1. **Pfsense:**
   pfSense is a FreeBSD-based open-source firewall and router software distribution. It is intended to provide network administrators and IT professionals with a robust, versatile, and secure platform for building and managing network infrastructures. pfSense is well-known for its feature set, ease of use, and ability to transform an ordinary PC into a powerful network appliance.
   Key features:
   - Firewall protection
   - Routing and networking
   - VPN support
   - Web based GUI
   - Intrusion detection and prevention

   pfSense provides a variety of functions in a variety of situations. It is a popular solution for individuals seeking advanced network security control at home. Its powerful features make it ideal for small to medium-sized enterprises, and it offers cost-effective alternatives to commercial firewall solutions. pfSense is smoothly integrated into

complicated network architectures in larger companies, providing scalability and high availability characteristics. The open-source nature of the platform, as well as its vast documentation, make it a valuable tool for educational institutions, where it is used to teach networking and cybersecurity concepts. Furthermore, pfSense is useful in organizational settings, enabling secure VPN connections for remote access by employees and providing secure connections across different sites. Because of its versatility and scalability, pfSense is a go-to solution in a variety of scenarios, fulfilling the needs of users ranging from home enthusiasts to major organizations.

2. **Kali Linux:**
   Kali Linux is the leading operating system for cybersecurity and penetration testing. Kali Linux, well-known for its extensive array of tools for ethical hacking, security testing, and forensics, empowers cybersecurity experts, ethical hackers, and hobbyists alike. This open-source platform, derived from Debian, provides a full environment for testing and enhancing network security. Kali Linux, with its user-friendly interface and extensive documentation, is not only a strong tool for experienced practitioners but also a learning resource for cybersecurity and ethical hacking. Its frequent updates and active community add to its standing as a go-to solution for anyone navigating the ever-changing field of information security, ensuring that it remains at the cutting edge of technologies designed to protect digital environments.

TOOL USED: Pfsense

In this workshop, we are using Pfsense, a firewall/router software.

pfSense is a firewall and router software that operates on the FreeBSD operating system. It is an open-source solution intended for use on actual hardware or virtual computers. The software functions as a comprehensive security solution, offering many features such as firewall control, routing capabilities, and an intuitive web-based interface. pfSense offers a diverse selection of supplementary components and modules, thereby broadening its capabilities to encompass virtual private network (VPN) services, traffic management, and other features. The adaptability of this technology renders it appropriate for diverse network configurations, encompassing multi-WAN setups and high-availability scenarios. With a vibrant community and accessible commercial support, pfSense presents itself as a robust option for those in search of a highly customizable and feature-laden firewall and routing system.

Configuration of Pfsense:

“Installation and configuring Pfsense is in the readme file provided.”

Step1: Open Pfsense in virtual machine and check for its Ip address.

Step2: open kali virtual box, check its Ip address, it should be in the same network as pfsense. If not, put the virtual machine in internal network mode.

Step 3: open 192.168.1.1, default gateway address and pfsense login page will be prompted. Login as username: admin, password: pfsense

Step 4: go to Services/dns resolver/general settings. In general settings section, Change network interface for incoming traffic to LAN and localhost from ALL.

Step 5: for outgoing services, change it to WAN. Save the settings.

Step 6: Go to services/dhcp server/lan. check the internal network IP address, it should be same as below seen. Save it.

Creating rules:

Go to Firewall/rules/LAN, we can find there are some predefined rules, we can change them or we can create our own rules using + operator.

Demonstration:

Figure 1

In Figure 1 you can see that pfsense was installed and is running successfully in a virtual setting. With choice 2, set interface IP addresses, we can change the web address or use local host: 192.168.1.1 to connect to pfSense in a web browser.

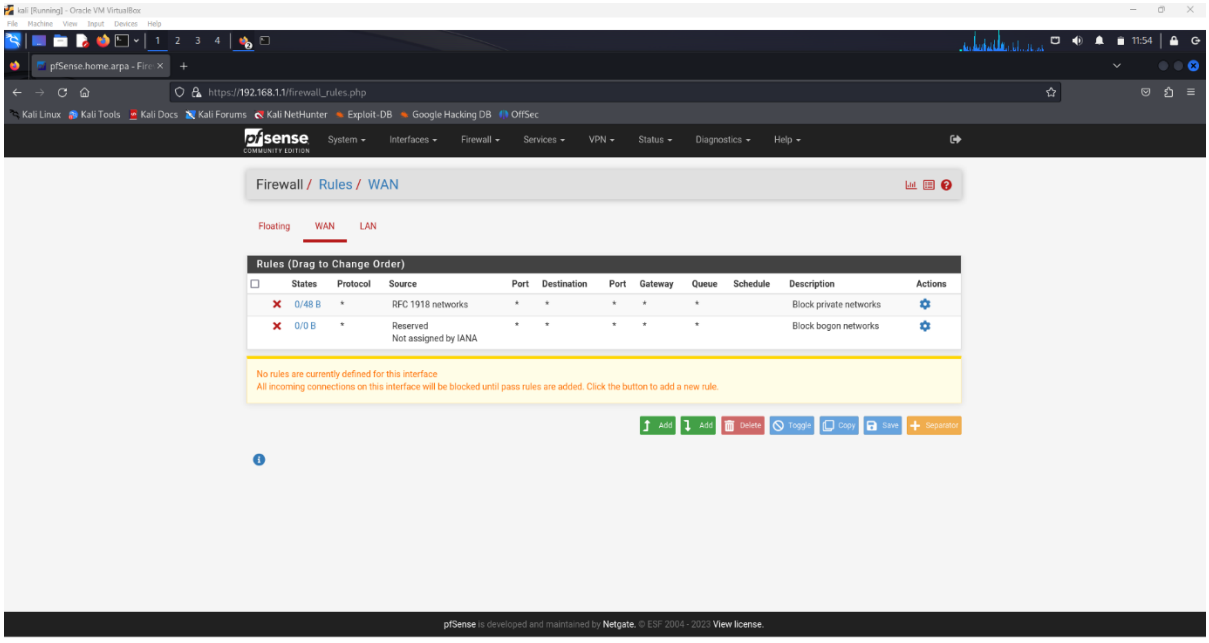


Figure 2

In Figure 2, you can see the local host pfsense website/interface. The rules that can be set up for LAN and WAN connections can be seen above. We can get around by going to firewall/rules/LAN or WAN.

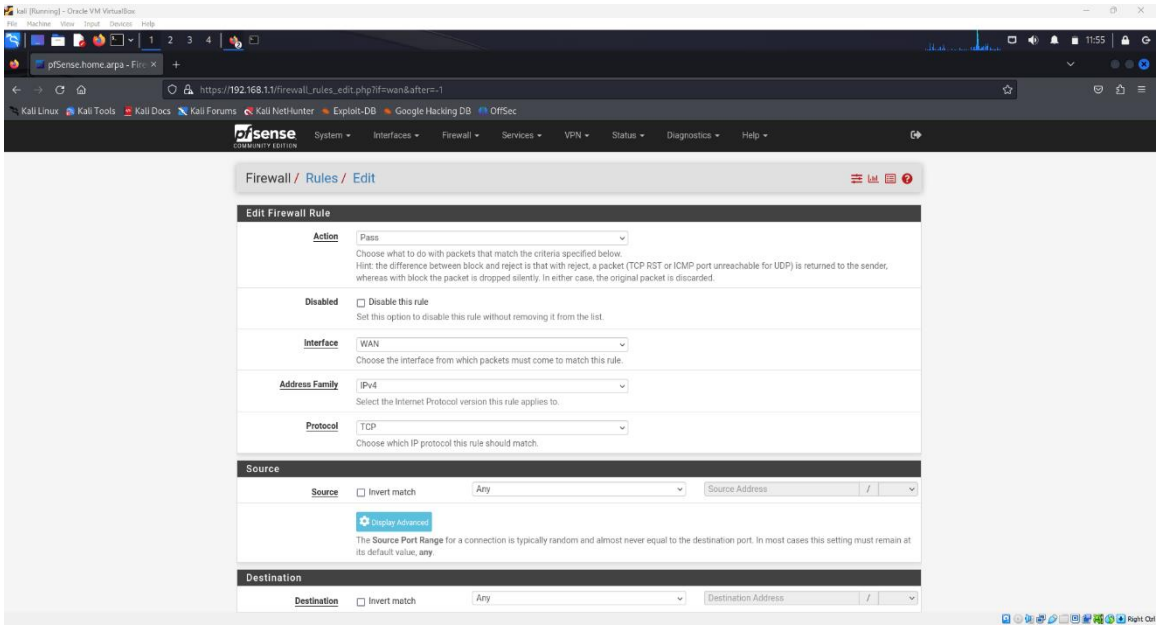


Figure 3

Figure 3 shows the rules generated by the pfsense software. Action options include block, allow, or limit, while interface options include WAN or LAN. The crucial aspect is the source and destination. Within the source, we can assign an IP address in particular for the purpose of restricting or allowing access. Similarly, in the destination address, we can perform the same action.

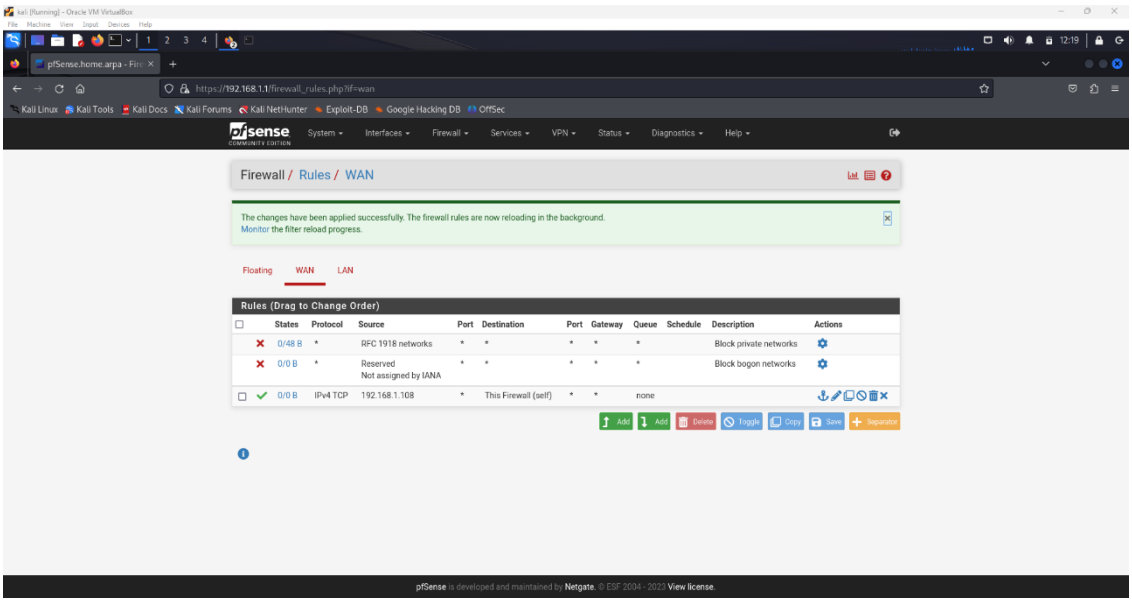


Figure 4

In figure 4, I implemented a rule that prohibits any ICMP and TCP connections linked to my VM machine.

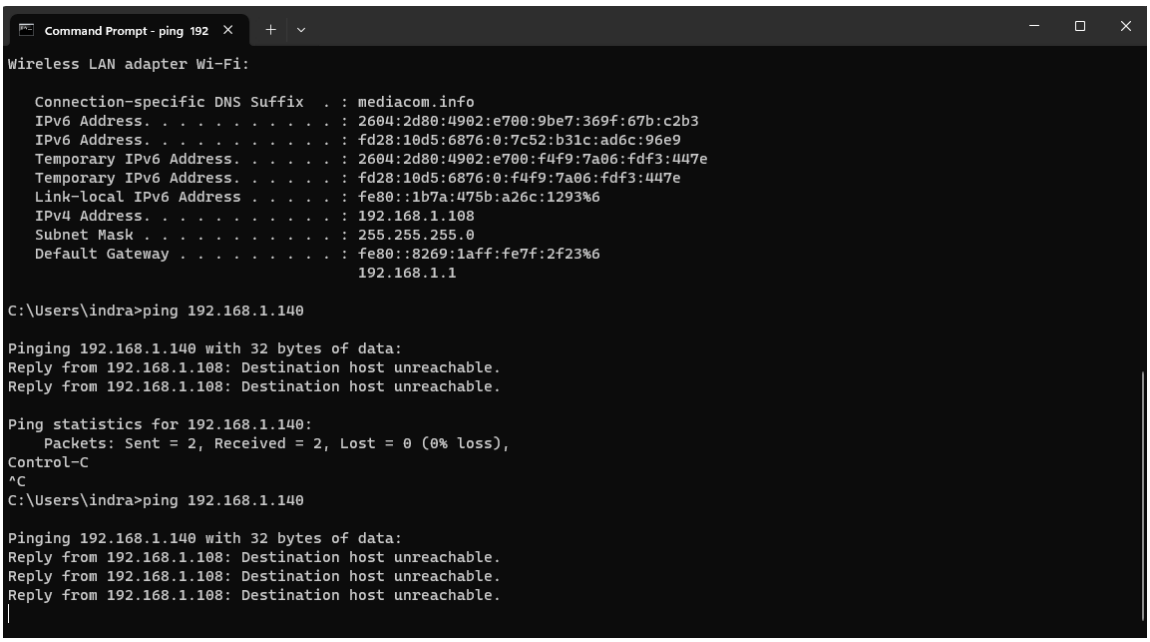


Figure 5

Figure 5 illustrates the failure of the ping command and the inability to reach the host. This occurs because ping utilizes ICMP packets to verify the availability of the destination host.

Therefore, pfsense is functioning perfectly, enabling us to generate more rules using this firewall.