

pfSense Firewall Lab Simulation: DoS Detection & Mitigation in a Virtual Environment

Author: Rishav Kumar Thapa

Platform: Oracle VirtualBox

Victim OS: Ubuntu

Server OS: Pfsense Firwall

Attacker Os : kali

Date : 6/17/2025

1. Introduction

This lab guide provides a comprehensive walkthrough for setting up a pfSense-based firewall environment using Oracle VirtualBox. It simulates a basic two-zone security setup with an internal LAN and an external WAN to demonstrate firewall configuration and DoS mitigation techniques. The lab is particularly beneficial for cybersecurity students and professionals aiming to understand perimeter defense using pfSense.

Through this setup, users will deploy pfSense as the firewall, Kali Linux as the attacker machine on the WAN side, and Ubuntu Desktop as the victim on the LAN. Using tools like hping3 and Wireshark, the guide walks through launching and detecting a simulated DoS attack and mitigating it using pfSense firewall rules.

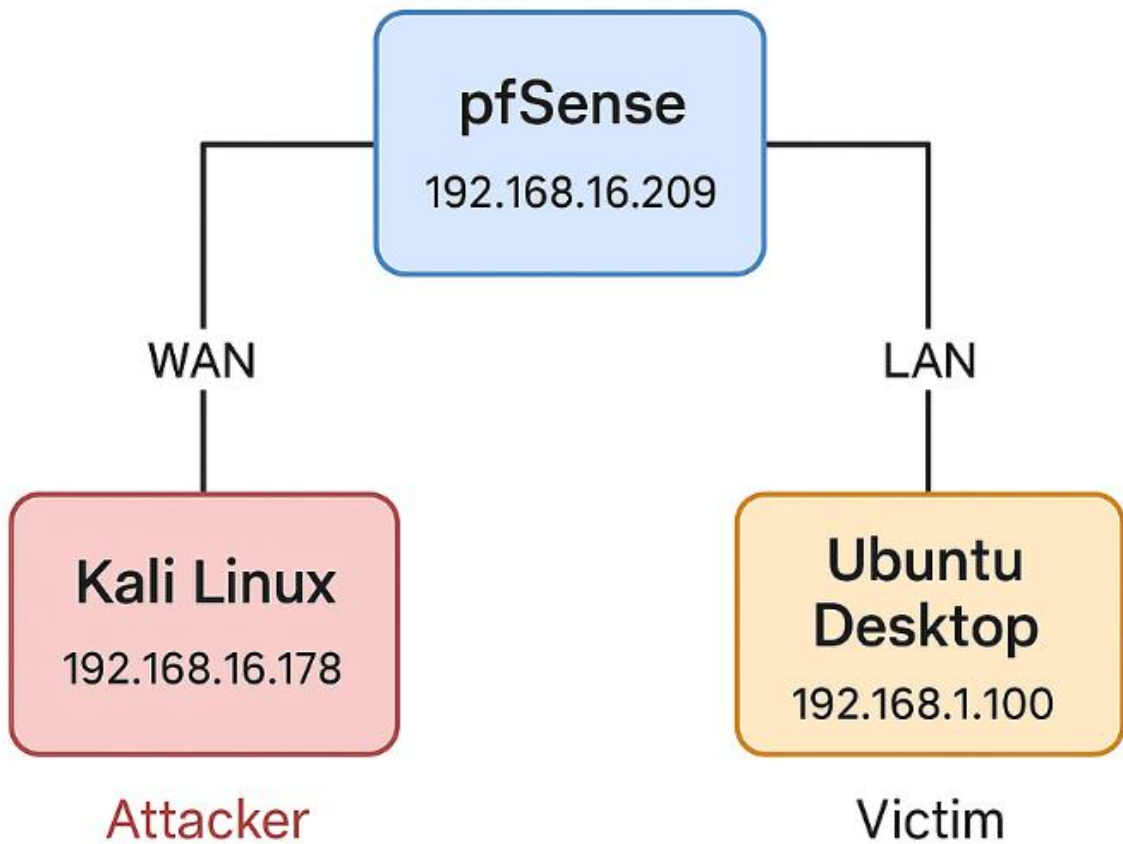
2. Objectives

- Deploy a pfSense firewall in VirtualBox with separate WAN (bridged) and LAN (internal) segments.
- Simulate an external attack from Kali Linux on the WAN interface.
- Configure Ubuntu Desktop as the internal victim machine.
- Demonstrate a DoS attack using hping3.
- Use pfSense firewall rules to mitigate and block the attack.

3. Network Topology & IP Plan

Device	Network Adapter	IP Address	Role
pfSense (WAN	Bridged	192.168.16.209/24	Edge Firewall
Kali Linux (Attacker)	Bridged	192.168.16.178/24	External Threat Source
pfSense (LAN)	Internal (intnet)	x.x.x.x/24	Default GW + DHCP
Ubuntu (Victim)	Internal (intnet)	192.168.1.100/24	Internal Host

4. Network Architecture Overview



5. Prerequisites

- Oracle VirtualBox (v7 or above)
- ISO files:
 - pfSense-CE-2.7.x-amd64.iso
 - kali-linux-current-amd64.iso
 - ubuntu-22.04-desktop-amd64.iso
- Minimum System Requirements:
 - 8 GB RAM
 - 40 GB disk space
 - Admin rights on host machine

6. Lab Setup Overview

1. Create pfSense VM

- OS Type: FreeBSD 64-bit
- Network:
 - Adapter 1: Bridged (WAN)
 - Adapter 2: Internal (LAN / LabNet)

2. Create Kali VM (Attacker)

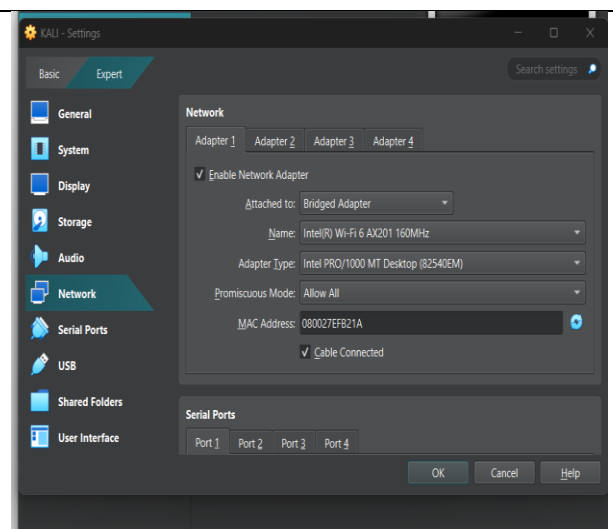
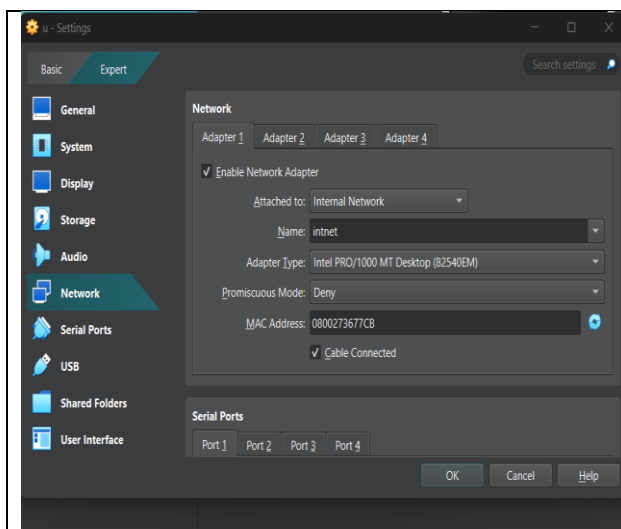
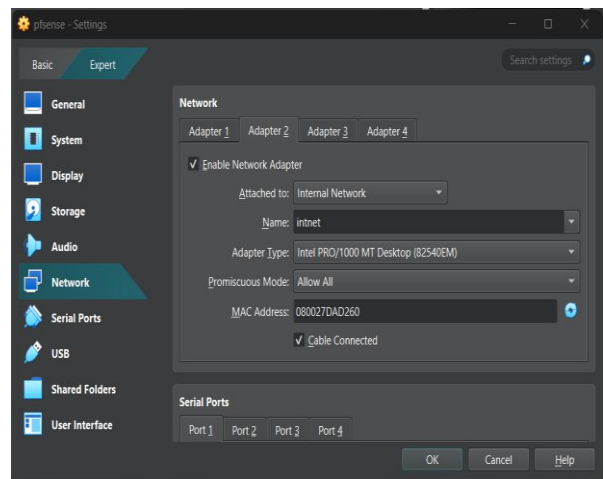
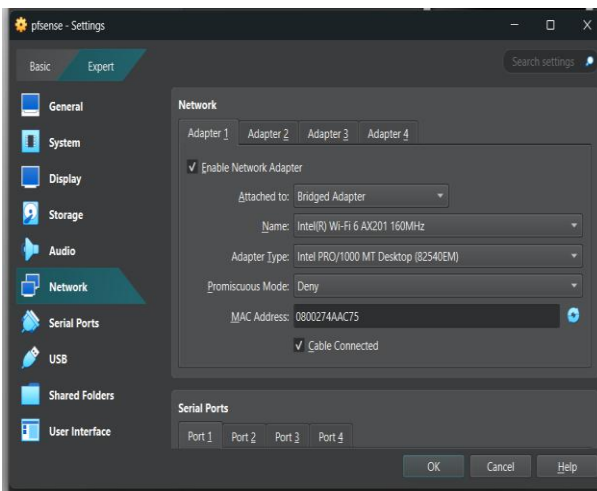
- OS Type: Debian 64-bit
- Network:
 - Adapter 1: Bridged

3. Create Ubuntu VM (Victim)

- OS Type: Ubuntu 64-bit
- Network:
 - Adapter 1: Internal (LabNet)

7. Firewall Lab Setup

This section outlines the step-by-step process of building a virtualized firewall environment using pfSense within Oracle VirtualBox. The lab setup is designed to replicate a real-world network infrastructure featuring an external (WAN) attacker and an internal (LAN) victim, protected by a pfSense firewall. Each virtual machine is carefully configured to simulate network segmentation, allowing for practical experimentation with firewall rules, attack simulations, and defense strategies. This foundational setup ensures that all components are correctly positioned for demonstrating and mitigating a Denial-of-Service (DoS) attack in a controlled and observable environment.



Step 1: Virtual Machine Network Configuration in VirtualBox

To simulate a real-world network with segmented zones, I configured three virtual machines within Oracle VirtualBox as follows:

- **Kali Linux** was assigned to the **Bridged Adapter** mode to simulate an external attacker connected to the public/WAN side of the network.
- **Ubuntu Desktop** was connected to an **Internal Network** named **intnet**, representing a secure internal LAN environment where the victim machine resides.
- **pfSense Firewall** was configured with two network adapters:
 - **Adapter 1 (WAN):** Set to **Bridged Adapter**, enabling pfSense to receive an IP address from the host's physical network and act as the network edge.
 - **Adapter 2 (LAN):** Set to **Internal Network (intnet)**, connecting it to the same LAN segment as the Ubuntu machine, allowing it to serve as the internal gateway and firewall.

This network segmentation allows controlled communication between the external attacker (Kali), the internal victim (Ubuntu), and the security appliance (pfSense), forming the foundation for simulating and analyzing a Denial-of-Service (DoS) attack scenario.

```

pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: f5916e9abb981186e14b

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.16.209/24
                                v6/DHCP6: fdef:2024:ef2f:0:a00:27ff:fe4a:ac75/
64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

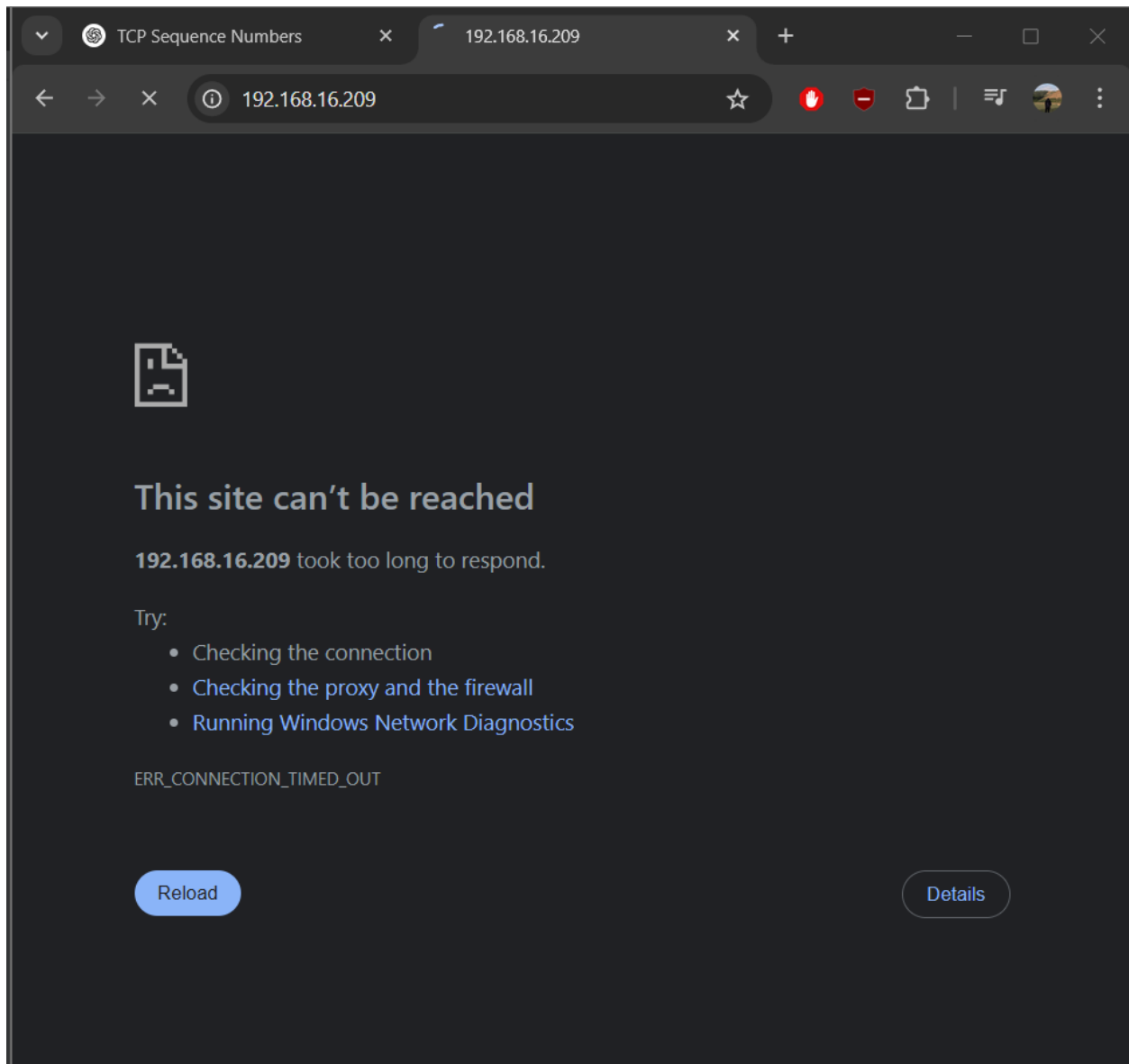
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: █

```

Step 2: Accessing the pfSense Terminal and Initial Setup

After booting the pfSense virtual machine, I accessed the built-in terminal interface to perform the initial configuration.



Step 3: Troubleshooting Connection to IP 192.168.16.209

While attempting to access the device at IP address **192.168.16.209** via a web browser,

```

VirtualBox Virtual Machine - Netgate Device ID: f5916e9abb981186e14b
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.16.209/24
                v6/DHCP6: fdef:2024:ef2f:0:a00:27ff:fe4a:ac75/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

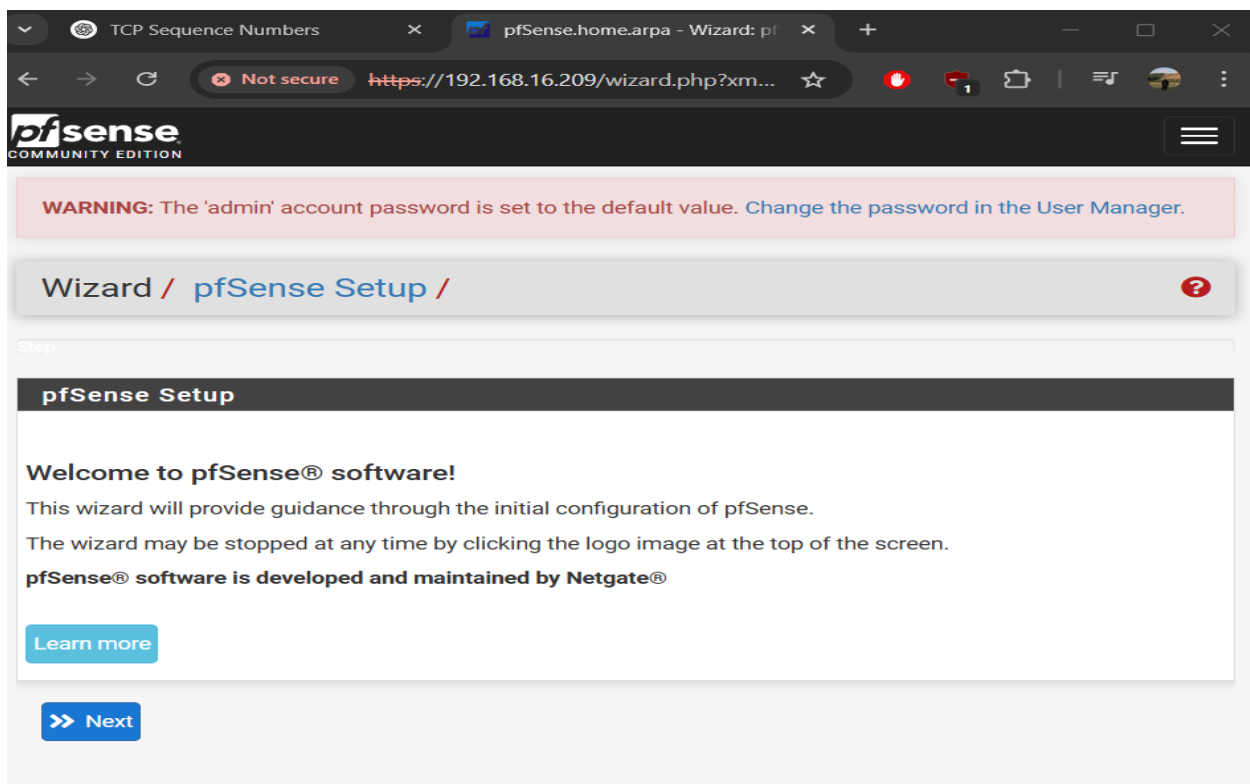
Enter an option: 8

[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: █

```

Step 4: Disable pfSense Firewall Temporarily

From the pfSense console shell, I ran the command `pfctl -d` to temporarily disable the firewall. This allowed me unrestricted access to the pfSense WebGUI for initial configuration without being blocked by firewall rules. This step is only temporary to avoid lockout during setup.



Step 5: Initial pfSense Setup Wizard

Upon accessing the pfSense WebGUI, the Setup Wizard welcomed me to the system and prompted for initial configuration. The wizard provides step-by-step guidance to configure essential settings such as hostname, domain, DNS servers, and admin password. It also issues a warning that the default admin password should be changed immediately for security purposes.

The screenshot shows a web browser window with the URL `https://192.168.16.209/wizard.php?xm...`. The page displays the 'PPTP Remote IP Address' field with the value '32'. Below it is the 'PPTP Dial on demand' section with an unchecked checkbox for 'Enable Dial-On-Demand mode' and a descriptive text. The 'PPTP Idle timeout' section has an empty input field and a description. The 'RFC1918 Networks' section contains two sub-sections: 'Block RFC1918 Private Networks' with a checked checkbox and a description, and 'Block bogon networks' with a checked checkbox and a description. At the bottom is a blue 'Next' button.

32

PPTP Remote IP Address

PPTP Dial on demand

☐ Enable Dial-On-Demand mode

This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks

☒ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

☒ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

Step 6: Observing Auto-Enabled WAN Firewall Settings

The WAN interface had the options to block RFC 1918 private networks and bogon networks enabled by default. Despite these settings being active, legitimate web pages loaded successfully, indicating that normal internet traffic was allowed while unwanted or suspicious packets were filtered automatically.

The screenshot shows a web browser window with the address bar displaying 'https://192.168.16.209/wizard.php?xm...'. The page is titled 'PPTP Remote IP Address' and contains several configuration sections. At the top, there is a dropdown menu showing '32'. Below it, the 'PPTP Remote IP Address' section has an empty input field. The 'PPTP Dial on demand' section includes a checkbox for 'Enable Dial-On-Demand mode' which is unchecked, followed by a descriptive paragraph. The 'PPTP Idle timeout' section has an empty input field and a descriptive paragraph. The 'RFC1918 Networks' section has a dark header and contains the 'Block RFC1918 Private Networks' checkbox, which is unchecked, with a descriptive paragraph. The 'Block bogon networks' section also has a dark header and contains the 'Block bogon networks' checkbox, which is unchecked, with a descriptive paragraph. At the bottom left, there is a blue button labeled '>> Next'.

32

PPTP Remote IP Address

PPTP Dial on demand

☐ Enable Dial-On-Demand mode

This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks

☐ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks

☐ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

Step 7: Disabling WAN Firewall Restrictions to Enable Web Access


I unticked the options to block RFC 1918 private networks and bogon networks on the WAN interface. This change allows traffic from private IP ranges and reserved IP blocks, which is necessary when the WAN itself uses such private addressing. Disabling these blocks enabled successful web page access through the WAN interface.


Additionally, the Dial-OnDemand mode remained disabled, ensuring the WAN connection stayed active continuously.

The screenshot shows a web browser window with the pfSense Setup Wizard. The browser's address bar shows the URL `https://192.168.16.209/wizard.php?xm...` and a "Not secure" warning. The pfSense logo and "COMMUNITY EDITION" are visible in the top left. A red warning banner at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation reads "Wizard / pfSense Setup / Configure LAN Interface". A progress bar indicates "Step 5 of 9". The main heading is "Configure LAN Interface". The instructions state: "On this screen the Local Area Network information will be configured." The "LAN IP Address" field contains "192.168.1.1". Below it, the text says "Type dhcp if this interface uses DHCP to obtain its IP address." The "Subnet Mask" field contains "24". At the bottom left is a blue button labeled ">> Next".


Step 8: Configuring the LAN Interface

In the pfSense setup wizard, I configured the LAN interface with the default IP address **192.168.1.1** and subnet mask /24. Since this interface uses a static IP, I left the DHCP option unchecked. I proceeded with these default settings without changing to ensure proper internal network configuration.

 COMMUNITY EDITION



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / [pfSense Setup](#) / [Set Admin WebGUI Password](#) 


Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

 Next

Step 9: Setting the Admin WebGUI Password

I set a strong admin password to secure access to the pfSense WebGUI and SSH services (if enabled). This password protects the firewall's management interface from unauthorized access. After entering and confirming the new password, I proceeded to the next configuration step.

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Step 10: Completing the pfSense Setup Wizard

After completing all configuration steps, the pfSense Setup Wizard confirms that the firewall is now configured. It recommends checking for software updates to ensure the latest security and feature improvements. The wizard also offers links to support resources, community forums, and product information. Finally, I clicked **Finish** to exit the wizard and start using the pfSense firewall.


```

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: 8

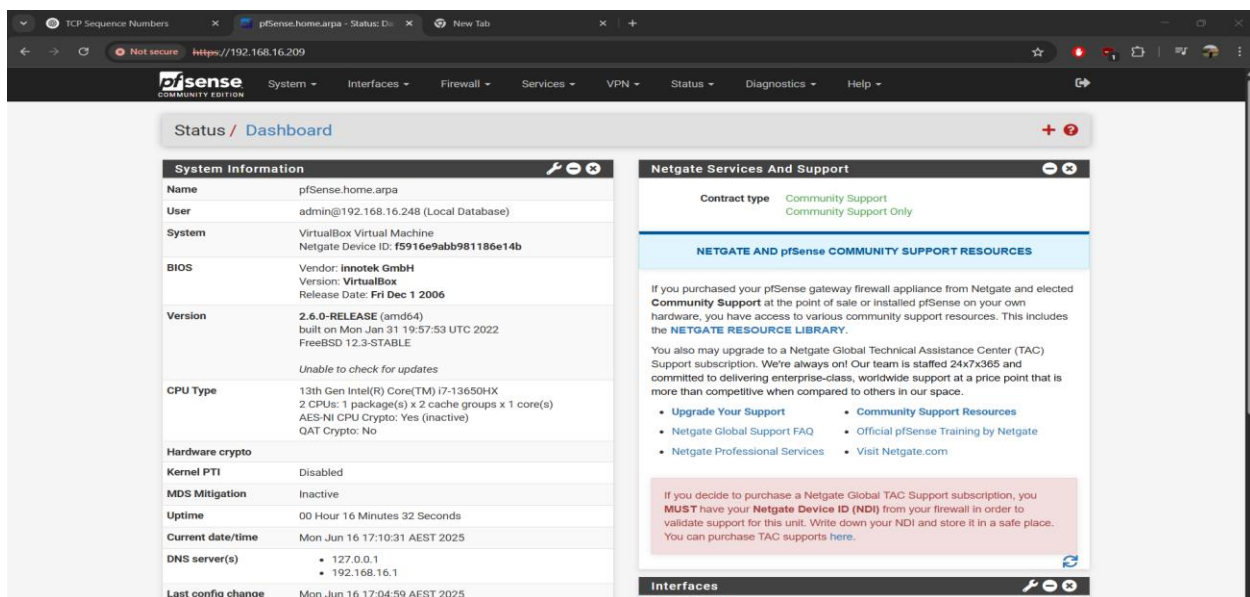
[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -d
pf disabled
[2.6.0-RELEASE][root@pfSense.home.arpal/root:
Message from syslogd@pfSense at Jun 16 07:00:24 ...
php-fpm[3591]: /index.php: Successful login for user 'admin' from: 192.168.16.248
(Local Database)

[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -d
pf disabled
[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -e
pf enabled
[2.6.0-RELEASE][root@pfSense.home.arpal/root:

```

Step 11: Temporarily Disable the pfSense Firewall via Console

From the pfSense console menu, I chose option 8 to access the shell. Then, I ran the command `pfctl -d` to disable the firewall temporarily, allowing unrestricted access to the WebGUI for initial configuration. The system confirmed that the packet filter (pf) was disabled. After completing the setup, I re-enabled the firewall by running `pfctl -e` to secure the system again.

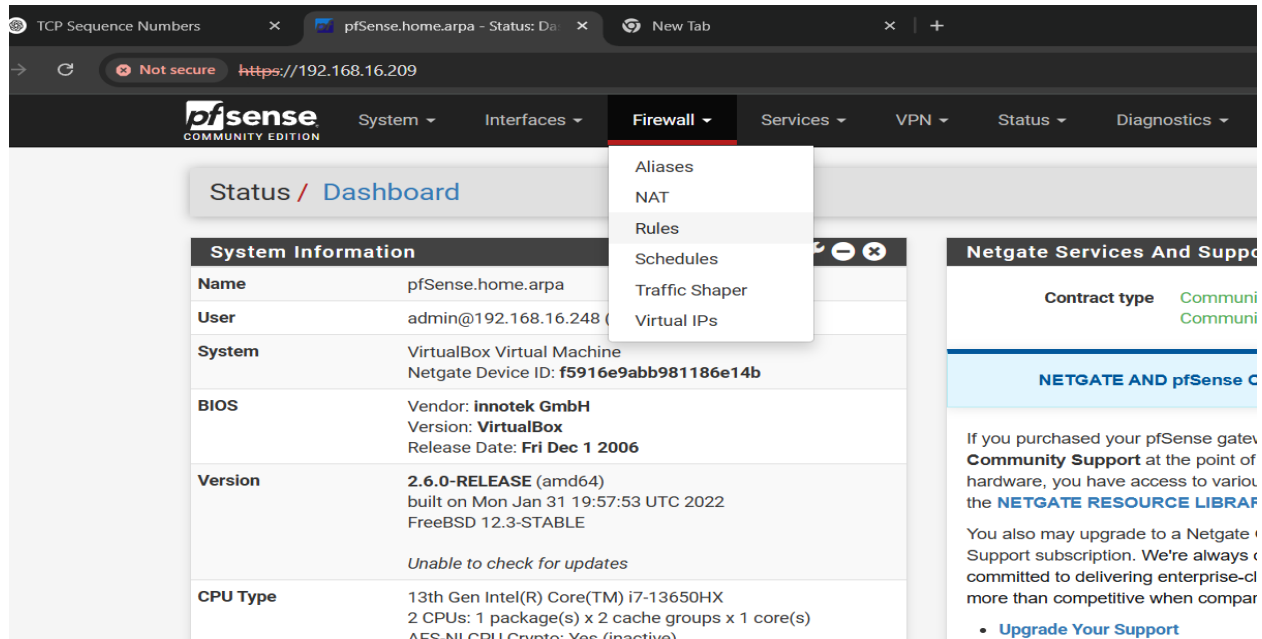


The screenshot shows the pfSense web interface with the following sections:

- System Information:**
 - Name: pfSense.home.arpal
 - User: admin@192.168.16.248 (Local Database)
 - System: VirtualBox Virtual Machine, Netgate Device ID: f5916e9abb981186e14b
 - BIOS: Vendor: innotek GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006
 - Version: 2.6.0-RELEASE (amd64), built on Mon Jan 31 19:57:53 UTC 2022, FreeBSD 12.3-STABLE
 - CPU Type: Unable to check for updates
 - CPU Type: 13th Gen Intel(R) Core(TM) i7-13650HX, 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s), AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No
 - Hardware crypto: Disabled
 - Kernel PTI: Disabled
 - MDS Mitigation: Inactive
 - Uptime: 00 Hour 16 Minutes 32 Seconds
 - Current date/time: Mon Jun 16 17:10:31 AEST 2025
 - DNS server(s): 127.0.0.1, 192.168.16.1
 - Last config change: Mon Jun 16 17:04:59 AEST 2025
- Netgate Services And Support:**
 - Contract type: Community Support, Community Support Only
 - NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**
 - If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).
 - You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
 - Upgrade Your Support:
 - Netgate Global Support FAQ
 - Netgate Professional Services
 - Community Support Resources:
 - Official pfSense Training by Netgate
 - Visit Netgate.com
 - If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).
- Interfaces:** (Section header visible)

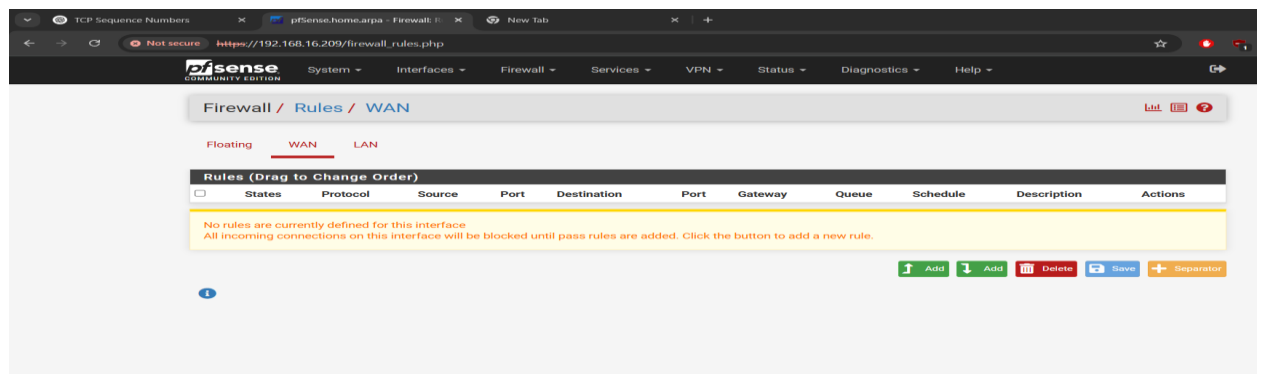
Step 12: Accessing the pfSense Dashboard

After disabling the firewall temporarily, I opened a web browser and navigated to the pfSense WAN IP address (e.g., <https://192.168.16.209>). The pfSense login page appeared. I logged in using the default credentials and was directed to the **Status Dashboard**, confirming successful access to the pfSense WebGUI for further configuration.



Step 13: Navigating to Firewall Rules

After logging into the pfSense WebGUI, I accessed the **Firewall** menu from the dashboard sidebar. Under this menu, I selected **Rules** to view and manage the firewall rules. This section allows configuring which traffic is allowed or blocked on various interfaces, such as WAN or LAN.



Step 14: Adding Firewall Rules on WAN Interface

In the pfSense WebGUI, I went to **Firewall > Rules > WAN** to add new rules. These rules allow

secure remote management by permitting HTTPS (port 443) traffic from trusted IPs on the WAN side. This helps control and restrict incoming connections while maintaining secure access.

192.168.16.209/firewall_rules_edit.php?if=wan&after=-1

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 WAN
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

Source ☐ Invert match Network 192.168.16.0 / 24

[Display Advanced](#)
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Single host or alias 192.168.16.209

Destination Port Range (other) (other)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

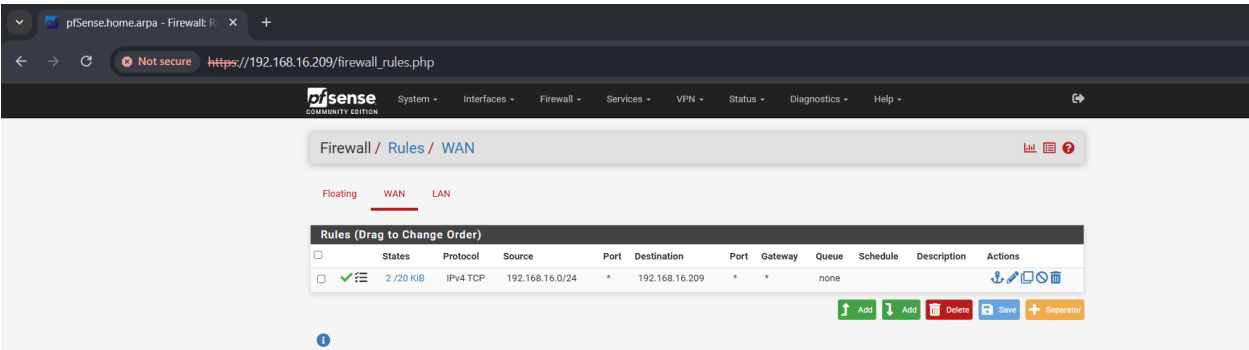
[Save](#)

Step 15: Creating a Firewall Rule to Allow Traffic from Source Network to Specific Destination

I configured a firewall rule on the WAN interface to **allow traffic from the source network 192.168.16.0/24 to the specific destination IP 192.168.16.209**. The rule was set to **pass** matching packets to permit communication. Key settings included:

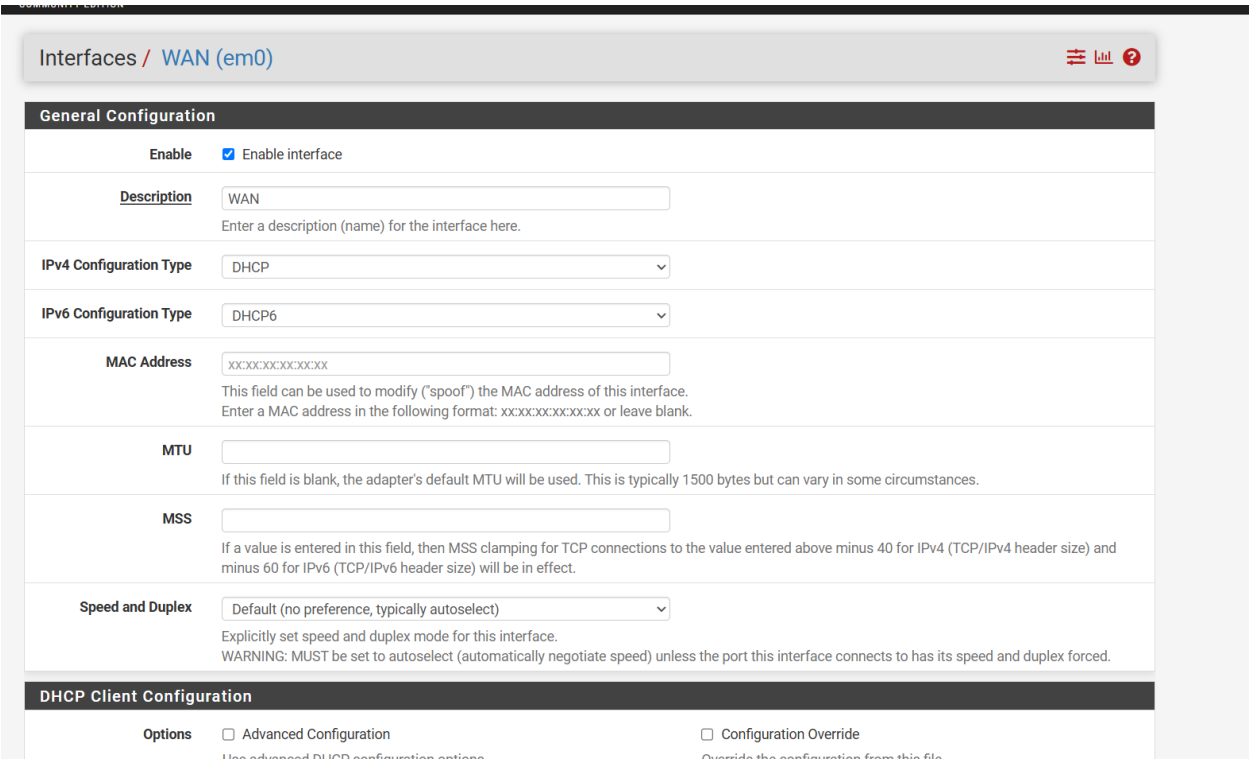
- Interface: WAN
- Protocol: Any (or specify if needed)
- Source: Network 192.168.16.0/24
- Destination: Single host 192.168.16.209
- Port Range: Default (any)
- Action: Pass

The rule was enabled to ensure traffic filtering applied correctly. This setup allows controlled access from the trusted local subnet to the designated IP address.



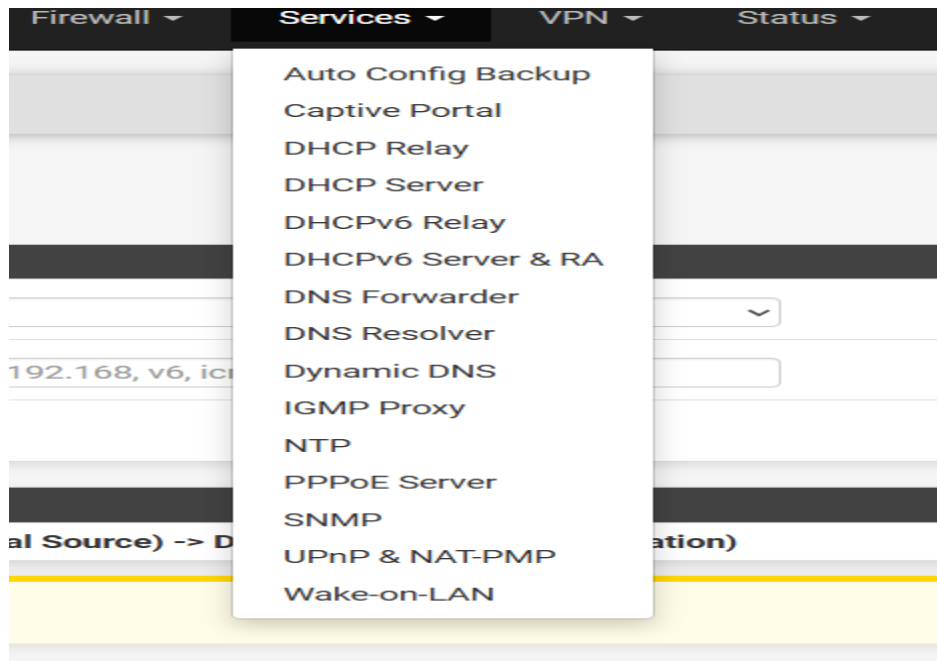
Step 16: Verifying Firewall Rules on WAN and LAN Interfaces

I navigated to **pfSense > Firewall > Rules** and confirmed that the new rule allowing traffic from the LAN network (192.168.16.0/24) to the destination IP (192.168.16.209) was successfully created under the **WAN** interface rules. This ensures proper filtering and access control for incoming traffic.



Step 17: Configuring WAN Interface Firewall Rules

I accessed **Firewall > Rules > WAN** in pfSense WebGUI and created a rule to allow traffic from the source network 192.168.16.0/24 to the destination IP 192.168.16.209. This rule ensures proper access control and allows the required communication through the WAN interface.



Step 18: Assign IP to LAN Interface Using DHCP

By enabling DHCP on the LAN interface, devices like the Ubuntu machine connected to the internal network will automatically receive an IP address. This allows the Ubuntu system to communicate on the LAN without manual IP configuration, simplifying network setup and management.

p.php

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet: 192.168.1.0

Subnet mask: 255.255.255.0

Available range: 192.168.1.1 - 192.168.1.254

Range: 192.168.1.10 To 192.168.1.245

From To

Additional Pools

Add [+ Add pool](#)

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Action

Servers

WINS servers:

DNS servers:

Leave blank to use the system default DNS servers this interface's IP. If DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

DMZAPI

DMZAPI Port:
Set the port that DMZAPI will listen on. The default port is 7911, leave blank to disable. Only the first DMZAPI configuration is used.

DMZAPI Key:
Enter a key matching the selected algorithm to secure connections to the DMZAPI endpoint.

☐ Generate New Key
Generate a new key based on the selected algorithm.

Key Algorithm:
Set the algorithm that DMZAPI key will use.

Other Options

Gateway:
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name:
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain search list:
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default lease time:
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum lease time:
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Refuse peer IP:
Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP interface's address to determine whether the DHCP process is Primary or Secondary. Ensure one machine's address is 20 (and the other is - 20).

Static ARP: ☐ Enable Static ARP entries
This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.

Time format change: ☐ Change DHCP display lease time from UTC to local time
By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.

Statistics graphs: ☐ Enable RRD statistics graphs
Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.

Ping check: ☐ Disable ping check
When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.

Dynamic DNS: [Display Advanced](#)

MAC address control: [Display Advanced](#)

NTP: [Display Advanced](#)

TFTP: [Display Advanced](#)

LDAP: [Display Advanced](#)

Network Booting: [Display Advanced](#)

Additional BOOTP/DHCP Options: [Display Advanced](#)

[Save](#)

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description

[+ Add](#)

Step 19: Configure LAN Subnet and DNS Settings

We set the LAN subnet to **192.168.1.0** with a subnet mask of **255.255.255.0**, providing an IP range from **192.168.1.1** to **192.168.1.254** for devices on the network. For DNS, we use the home router's DNS server to resolve domain names, ensuring proper internet connectivity and name resolution for devices on the LAN.

```
vboxuser@UBUNTU: ~  
vboxuser@UBUNTU:~$  
vboxuser@UBUNTU:~$  
vboxuser@UBUNTU:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
    inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fe36:77cb  prefixlen 64  scopeid 0x20<link>  
    ether 08:00:27:36:77:cb  txqueuelen 1000  (Ethernet)  
    RX packets 3120  bytes 1932266 (1.9 MB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 4898  bytes 435173 (435.1 KB)  
    TX errors 0  dropped 16 overruns 0  carrier 0  collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 34766  bytes 3311538 (3.3 MB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 34766  bytes 3311538 (3.3 MB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
vboxuser@UBUNTU:~$
```

Step 20: Verify Ubuntu Network Configuration

On the Ubuntu VM, the network interface **enp0s3** is configured on the internal network with IP **192.168.1.100** (via DHCP), subnet mask **255.255.255.0**, and is successfully transmitting and receiving packets. This confirms the DHCP service from pfSense is working correctly, assigning IPs in the LAN subnet. The pfSense firewall is connected with two adapters: one bridged (WAN) and one internal (LAN).

```
    inet 127.0.0.1  netmask 255.0.0.0  
    inet6 ::1  prefixlen 128  scopeid 0x10<host>  
    loop txqueuelen 1000  (Local Loopback)  
    RX packets 34766  bytes 3311538 (3.3 MB)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 34766  bytes 3311538 (3.3 MB)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
vboxuser@UBUNTU:~$ 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=116 time=32.6 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=29.3 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=32.5 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=32.4 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=29.2 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=28.5 ms
```

Step 21: Verify Internet Connectivity from Ubuntu VM

The Ubuntu VM successfully pings the external DNS server **8.8.8.8**, showing stable responses with low latency and no packet loss. This confirms that the Ubuntu VM has proper internet access through the pfSense firewall.

```
Downloads  logger  passwordsearch  shell.exe  Videos

(kali@vbox)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ef:b2:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.16.178/24 brd 192.168.16.255 scope global dynamic noprefixroute eth0
        valid_lft 39578sec preferred_lft 39578sec
    inet6 fdef:2024:ef2f::b25/128 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 2407:1400:aa7e:6978:f2fa:3e09:f443:37d3/64 scope global temporary dynamic
        valid_lft 259176sec preferred_lft 84067sec
    inet6 2407:1400:aa7e:6978:9001:af3e:790f:4407/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 259176sec preferred_lft 172776sec
    inet6 fdef:2024:ef2f:0:ee8b:620f:dd7e:8d41/64 scope global temporary dynamic
        valid_lft 602470sec preferred_lft 84066sec
    inet6 fdef:2024:ef2f:0:2dfa:172f:7fcd:a318/64 scope global mngtmpaddr noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::f494:c1d3:a834:dc9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@vbox)-[~]
$ ping 192.168.16.209
PING 192.168.16.209 (192.168.16.209) 56(84) bytes of data.
■
```

Step 22: Kali Linux Unable to Connect to pfSense LAN

The Kali Linux machine cannot reach the pfSense LAN IP (192.168.16.209) because no firewall rule/policy currently allows traffic from Kali's network. This step highlights the need to create appropriate firewall rules to enable communication.

pfSense.home.arpa - Firewall: R

Not secure https://192.168.16.209/firewall_rules_edit.php?if=wan&after...

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 WAN
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 ICMP
Choose which IP protocol this rule should match.

ICMP Subtypes
any
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source ☐ Invert match
Single host or alias 192.168.16.178 /

Destination

Destination ☐ Invert match
Single host or alias 192.168.16.209 /

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

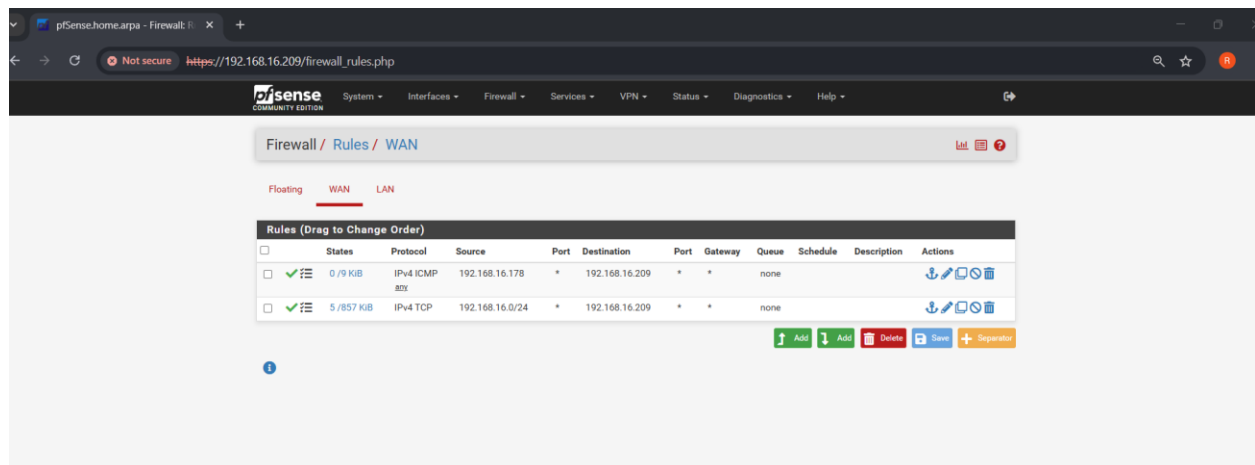
Step 23: Create Firewall Rule to Allow ICMP from Kali to pfSense

Add a new firewall rule on the pfSense WAN or LAN interface to allow ICMP traffic from Kali's IP (192.168.16.178) to pfSense LAN IP (192.168.16.209).

- Protocol: ICMP (IPv4)

- Source: Single host or alias — 192.168.16.178
- Destination: Single host or alias — 192.168.16.209
- Enable logging (optional) to monitor allowed packets
- Add a descriptive note like "Allow ICMP from Kali to pfSense"

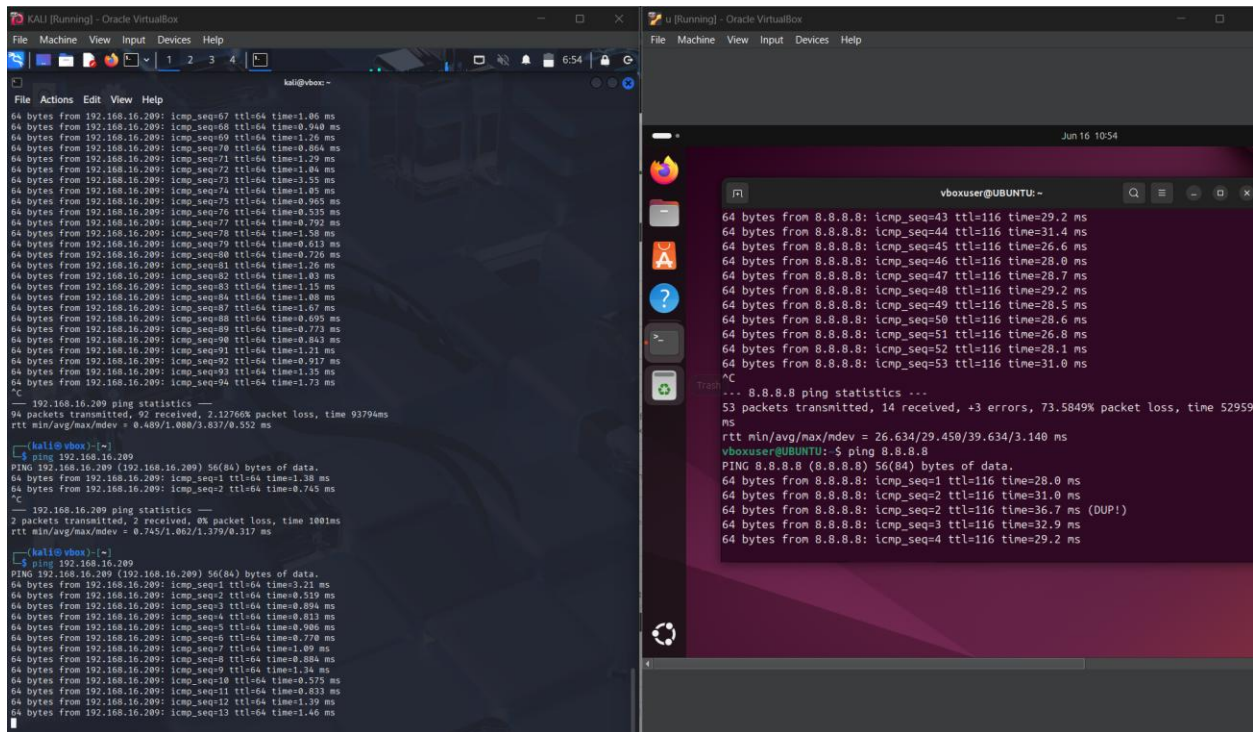
This rule enables ping and network diagnostics between Kali and the pfSense firewall.



Step 24: Review and Configure Firewall Rules on pfSense

- Navigate to **Firewall > Rules** and check the rules under **WAN** and **LAN** interfaces.
- Ensure there is a rule allowing traffic from the source IP (e.g., 192.168.16.178 or subnet 192.168.16.0/24) to the destination IP (192.168.16.209 — pfSense LAN).
- Confirm the rules specify correct protocols (e.g., TCP, ICMP) and ports if applicable.
- Use descriptions to clearly identify each rule's purpose for easier management.
- Adjust rule order if needed, as pfSense processes rules top-down.

This step ensures proper traffic flow through the firewall by configuring and verifying relevant rules.



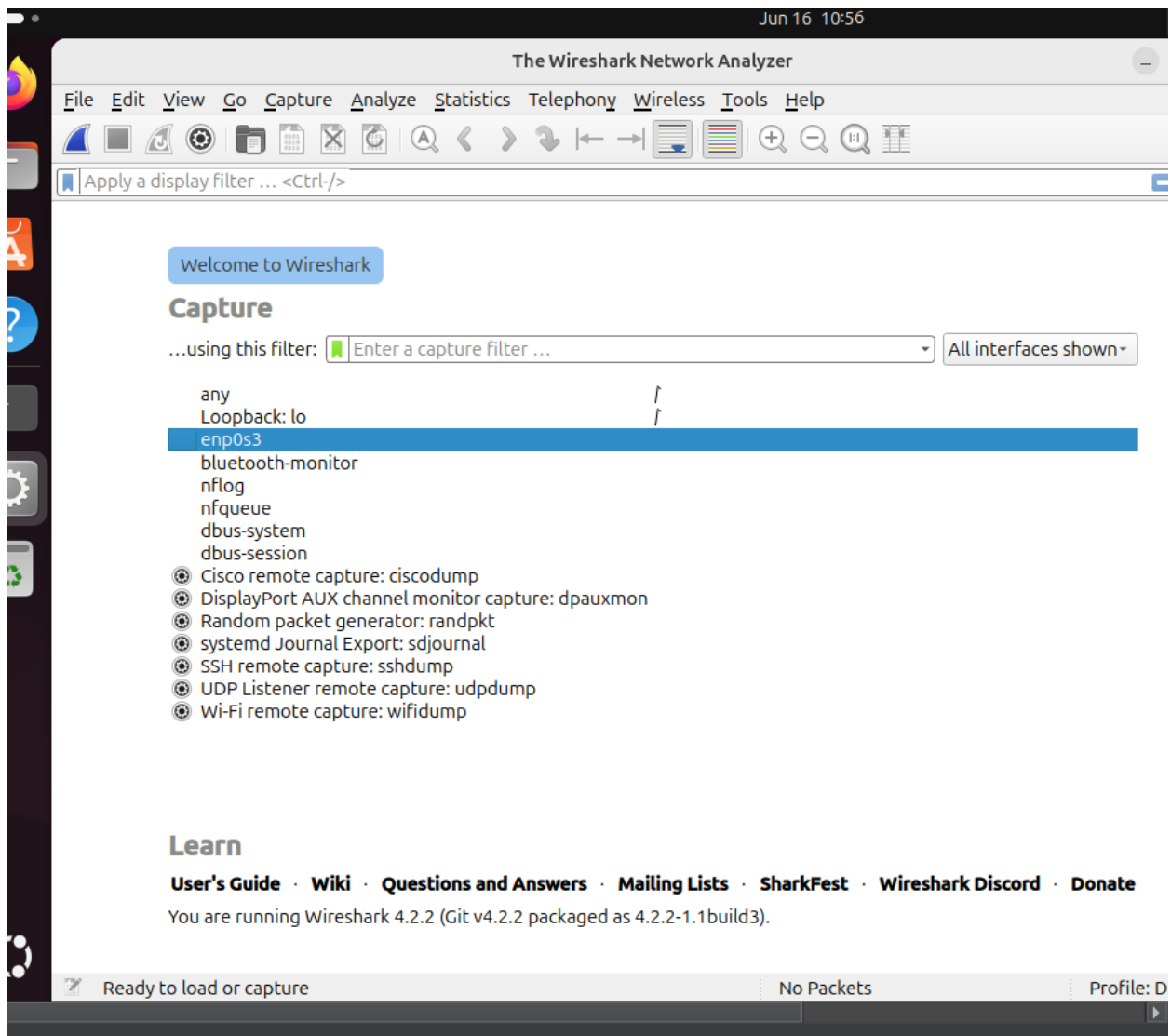
The image shows two terminal windows from Oracle VM VirtualBox. The left window is titled 'kali [Running] - Oracle VM VirtualBox' and shows a terminal session on a Kali Linux machine. It displays a series of ICMP echo requests (ping) from 192.168.16.209 to 192.168.16.209, with various sequence numbers and times. Below this, it shows '192.168.16.209 ping statistics' with 94 packets transmitted, 92 received, and 2.12766% packet loss. The right window is titled 'u [Running] - Oracle VM VirtualBox' and shows a terminal session on an Ubuntu machine. It displays a series of ICMP echo requests from 8.8.8.8 to 8.8.8.8, with various sequence numbers and times. Below this, it shows '8.8.8.8 ping statistics' with 53 packets transmitted, 14 received, and 73.5849% packet loss.

Step 25: Enable Communication Between Kali, pfSense Firewall, and Ubuntu

- Configure firewall rules on pfSense to allow traffic from Kali (e.g., 192.168.16.178) to the pfSense LAN IP (192.168.16.209) and to Ubuntu's IP on the internal network (e.g., 192.168.1.100).
- Ensure Ubuntu is configured to use DHCP or a static IP within the subnet managed by pfSense.
- Verify Kali and Ubuntu can ping pfSense and each other by allowing ICMP traffic in firewall rules.
- Confirm network interfaces on pfSense (bridge and internal) are properly configured to route traffic between Kali and Ubuntu.

8. Demonstration of a Basic DoS Attack within the Virtual Network Environment

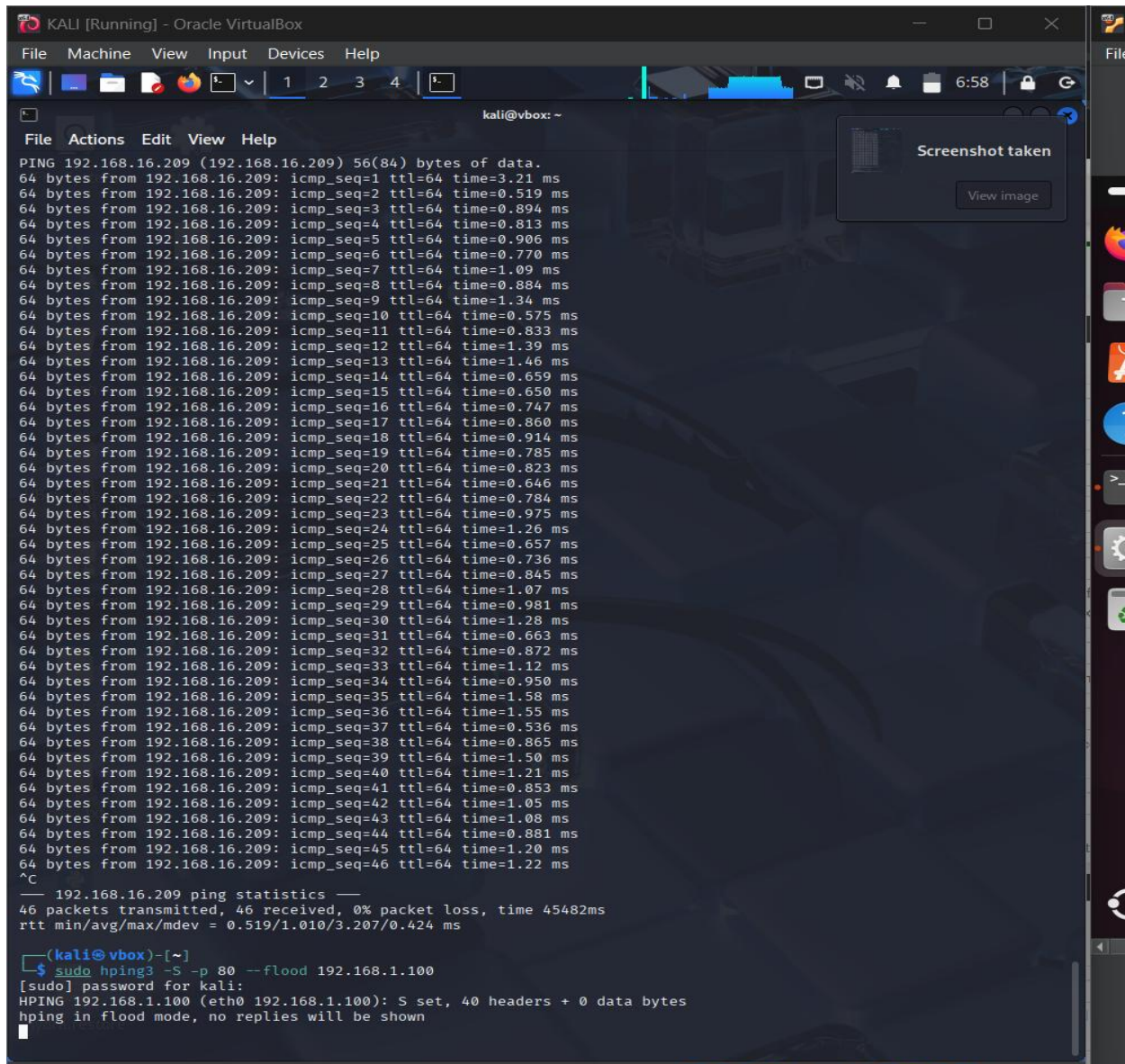
In this step, we demonstrate a simple Denial of Service (DoS) attack within the virtual network setup. We have already deployed a firewall rule allowing ICMP traffic from the Kali attacker to the Ubuntu victim, enabling them to successfully ping each other. This connectivity ensures that Kali can now perform DoS attacks by flooding ICMP requests to the Ubuntu machine, simulating network disruption for testing purposes.



Step 1: Launch Wireshark on Ubuntu

Open Wireshark from the applications menu or by typing `wireshark` in the terminal. Once

opened, you will see the main Wireshark window displaying available network interfaces. This tool will be used to capture and analyze network traffic during the DoS attack demonstration.



The screenshot shows a Kali Linux terminal window titled "KALI [Running] - Oracle VirtualBox". The terminal output displays the results of a normal ping test to 192.168.16.209, showing 46 packets transmitted with 0% packet loss and an average round-trip time of 1.010 ms. Below the ping statistics, the user has entered the command `sudo hping3 -S -p 80 --flood 192.168.1.100`. The terminal shows the password prompt and the hping3 tool starting in flood mode, sending 40 headers per second.

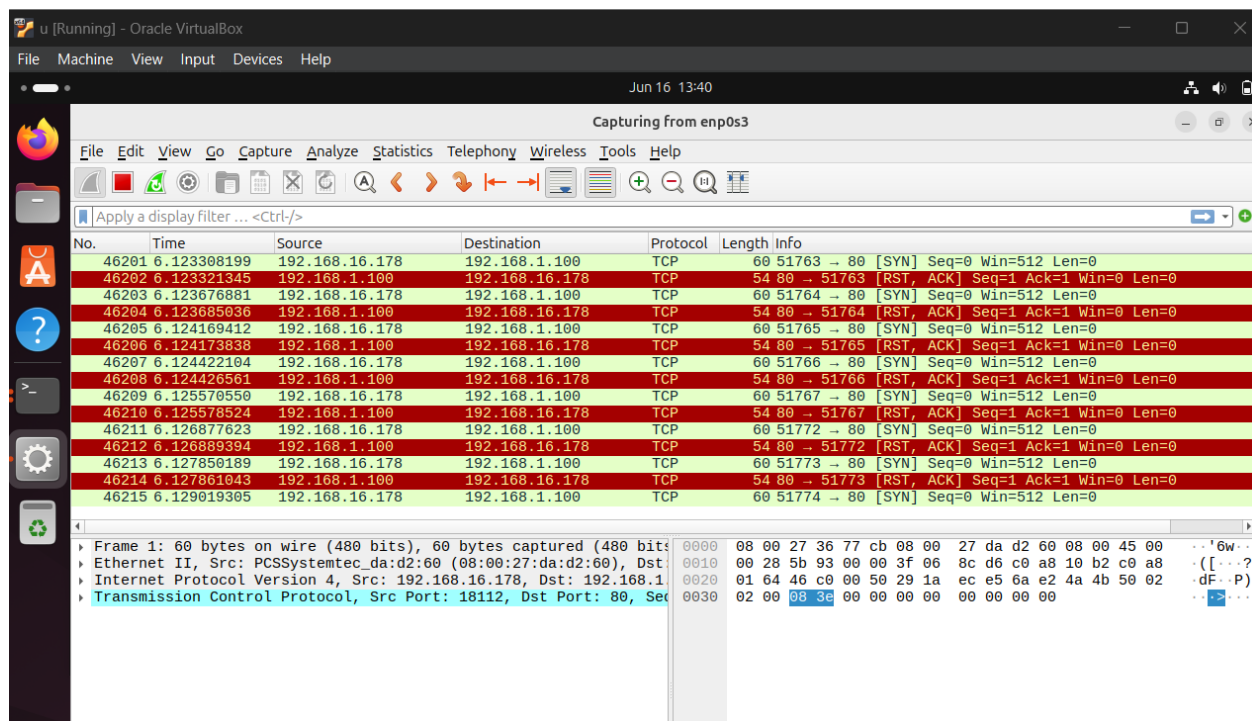
```
KALI [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

kali@vbox: ~
File Actions Edit View Help
PING 192.168.16.209 (192.168.16.209) 56(84) bytes of data:
64 bytes from 192.168.16.209: icmp_seq=1 ttl=64 time=3.21 ms
64 bytes from 192.168.16.209: icmp_seq=2 ttl=64 time=0.519 ms
64 bytes from 192.168.16.209: icmp_seq=3 ttl=64 time=0.894 ms
64 bytes from 192.168.16.209: icmp_seq=4 ttl=64 time=0.813 ms
64 bytes from 192.168.16.209: icmp_seq=5 ttl=64 time=0.906 ms
64 bytes from 192.168.16.209: icmp_seq=6 ttl=64 time=0.770 ms
64 bytes from 192.168.16.209: icmp_seq=7 ttl=64 time=1.09 ms
64 bytes from 192.168.16.209: icmp_seq=8 ttl=64 time=0.884 ms
64 bytes from 192.168.16.209: icmp_seq=9 ttl=64 time=1.34 ms
64 bytes from 192.168.16.209: icmp_seq=10 ttl=64 time=0.575 ms
64 bytes from 192.168.16.209: icmp_seq=11 ttl=64 time=0.833 ms
64 bytes from 192.168.16.209: icmp_seq=12 ttl=64 time=1.39 ms
64 bytes from 192.168.16.209: icmp_seq=13 ttl=64 time=1.46 ms
64 bytes from 192.168.16.209: icmp_seq=14 ttl=64 time=0.659 ms
64 bytes from 192.168.16.209: icmp_seq=15 ttl=64 time=0.650 ms
64 bytes from 192.168.16.209: icmp_seq=16 ttl=64 time=0.747 ms
64 bytes from 192.168.16.209: icmp_seq=17 ttl=64 time=0.860 ms
64 bytes from 192.168.16.209: icmp_seq=18 ttl=64 time=0.914 ms
64 bytes from 192.168.16.209: icmp_seq=19 ttl=64 time=0.785 ms
64 bytes from 192.168.16.209: icmp_seq=20 ttl=64 time=0.823 ms
64 bytes from 192.168.16.209: icmp_seq=21 ttl=64 time=0.646 ms
64 bytes from 192.168.16.209: icmp_seq=22 ttl=64 time=0.784 ms
64 bytes from 192.168.16.209: icmp_seq=23 ttl=64 time=0.975 ms
64 bytes from 192.168.16.209: icmp_seq=24 ttl=64 time=1.26 ms
64 bytes from 192.168.16.209: icmp_seq=25 ttl=64 time=0.657 ms
64 bytes from 192.168.16.209: icmp_seq=26 ttl=64 time=0.736 ms
64 bytes from 192.168.16.209: icmp_seq=27 ttl=64 time=0.845 ms
64 bytes from 192.168.16.209: icmp_seq=28 ttl=64 time=1.07 ms
64 bytes from 192.168.16.209: icmp_seq=29 ttl=64 time=0.981 ms
64 bytes from 192.168.16.209: icmp_seq=30 ttl=64 time=1.28 ms
64 bytes from 192.168.16.209: icmp_seq=31 ttl=64 time=0.663 ms
64 bytes from 192.168.16.209: icmp_seq=32 ttl=64 time=0.872 ms
64 bytes from 192.168.16.209: icmp_seq=33 ttl=64 time=1.12 ms
64 bytes from 192.168.16.209: icmp_seq=34 ttl=64 time=0.950 ms
64 bytes from 192.168.16.209: icmp_seq=35 ttl=64 time=1.58 ms
64 bytes from 192.168.16.209: icmp_seq=36 ttl=64 time=1.55 ms
64 bytes from 192.168.16.209: icmp_seq=37 ttl=64 time=0.536 ms
64 bytes from 192.168.16.209: icmp_seq=38 ttl=64 time=0.865 ms
64 bytes from 192.168.16.209: icmp_seq=39 ttl=64 time=1.50 ms
64 bytes from 192.168.16.209: icmp_seq=40 ttl=64 time=1.21 ms
64 bytes from 192.168.16.209: icmp_seq=41 ttl=64 time=0.853 ms
64 bytes from 192.168.16.209: icmp_seq=42 ttl=64 time=1.05 ms
64 bytes from 192.168.16.209: icmp_seq=43 ttl=64 time=1.08 ms
64 bytes from 192.168.16.209: icmp_seq=44 ttl=64 time=0.881 ms
64 bytes from 192.168.16.209: icmp_seq=45 ttl=64 time=1.20 ms
64 bytes from 192.168.16.209: icmp_seq=46 ttl=64 time=1.22 ms
^C
— 192.168.16.209 ping statistics —
46 packets transmitted, 46 received, 0% packet loss, time 45482ms
rtt min/avg/max/mdev = 0.519/1.010/3.207/0.424 ms

(kali@vbox)-[~]
$ sudo hping3 -S -p 80 --flood 192.168.1.100
[sudo] password for kali:
HPING 192.168.1.100 (eth0 192.168.1.100): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 2: A Basic DoS Attack Using Ping and hping3 Flood

In this step, we perform a simple DoS attack by flooding the target IP 192.168.16.209 with ICMP echo requests (ping) and TCP SYN packets using the hping3 tool. First, a normal ping test shows the target's response times and packet statistics. Then, using hping3 with the --flood and -S (SYN flag) options on port 80, a rapid stream of TCP SYN packets is sent to overwhelm the target's resources, simulating a SYN flood attack. This helps illustrate how a DoS attack can disrupt network availability.



Step3: Capturing Attack Traffic

During this step, we capture the network traffic while the attack is in progress using Wireshark on the relevant interface. The capture reveals TCP packets with SYN flags set, indicating the initiation of multiple connection requests typical in a DoS attack. The detailed packet information includes source and destination IPs, ports, sequence numbers, and protocol headers, allowing us to analyze the attack pattern and its impact on the network.

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
 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 WAN
 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

Source ☐ Invert match Single host or alias 192.168.16.178 /
[Display Advanced](#)
 The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Single host or alias 192.168.1.100 /
Destination Port Range any any
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Step 4: Adding a Firewall Rule to Block DoS Attack

In this step, we create a firewall rule on pfSense to block traffic from the Kali Linux attacker IP to the Ubuntu victim IP. The rule is set to block the specific source IP (Kali) targeting the destination IP (Ubuntu) on all ports and protocols, effectively stopping the DoS attack. Optional logging is enabled to monitor blocked packets for further analysis.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

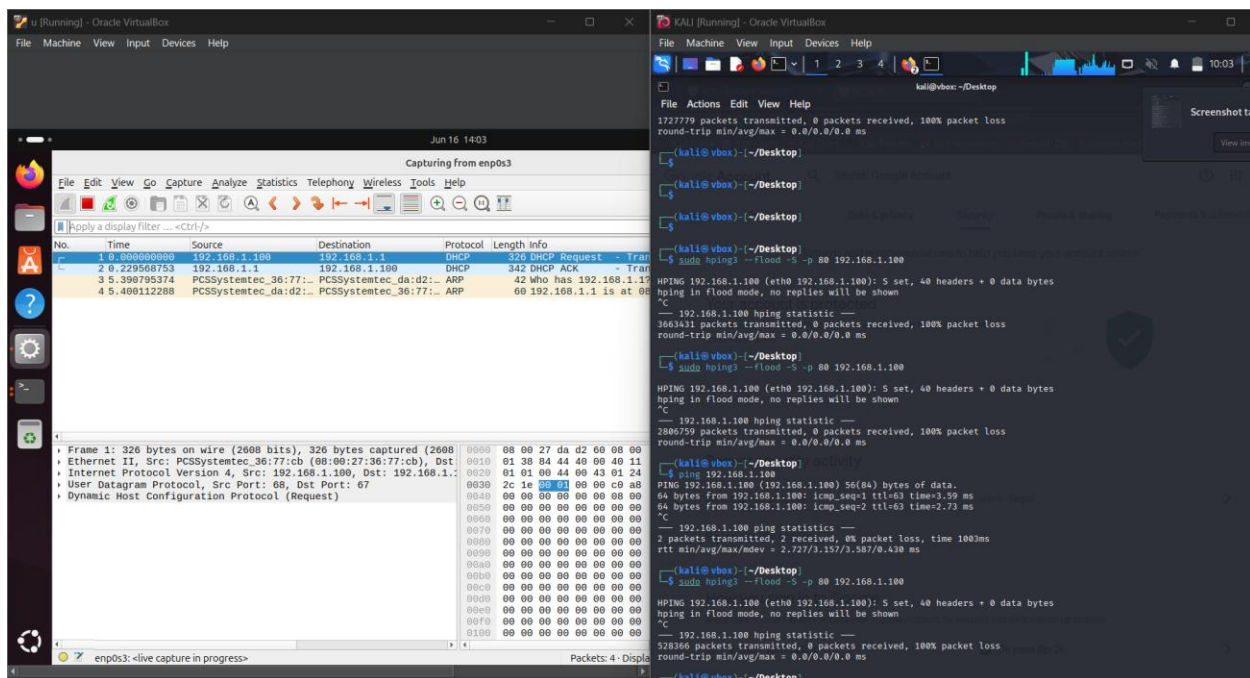
Floating WAN LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 / 11.95 MiB	IPv4 TCP	192.168.16.178	*	192.168.1.100	*	*	none			
<input type="checkbox"/>	✓ 0 / 3 KiB	IPv4 ICMP any	192.168.16.178	*	192.168.1.100	*	*	none		Allow Kali ICMP to Ubuntu	
<input type="checkbox"/>	✓ 0 / 43.78 MiB	IPv4 TCP	192.168.16.178	*	192.168.1.100	*	*	none			
<input type="checkbox"/>	✓ 0 / 1008 B	IPv4 ICMP any	192.168.16.178	*	192.168.16.209	*	*	none			
<input type="checkbox"/>	✓ 2 / 11.56 MiB	IPv4 TCP	192.168.16.0/24	*	192.168.16.209	*	*	none			

Add Add Delete Save Separator

Step 5: Deploying and Verifying Firewall Rule on WAN

We deployed a firewall rule on the pfSense WAN interface to block traffic from the attacker IP (192.168.16.178) targeting the victim IP (192.168.16.209). After applying the rule, the firewall successfully reloaded the configuration. Monitoring the rule shows active state entries, confirming the rule is enforced and blocking the specified traffic as intended.



Step 6: Limited Traffic Observed After Adding Firewall Rule

After adding the firewall rule to allow traffic from the Kali attacker to the Ubuntu victim, only minimal network traffic was observed. This indicates that although basic connectivity was established, no significant attack activity or malicious packets were detected on the network at this stage. Further configuration or attack steps may be required to generate noticeable traffic.

9. Pros and Cons

Category	Pros (Strengths)	Cons (Challenges & Fixes)
Setup	-Realistic network segmentation (WAN/LAN). -Isolated VMs (Kali, Ubuntu, pfSense) for safe testing.	-Initial DHCP misconfiguration on LAN. - Fix: Enabled DHCP server on pfSense (192.168.1.1/24).
Attack Simulation	-Successfully demonstrated DoS attacks using hping3 and Wireshark for analysis.	-SYN flood bypassed rules initially due to incorrect rule order.
Firewall Rules	-Granular control over traffic (ICMP/TCP blocking, IP-based filtering).	-Rule misplacement caused conflicts (e.g., allow rules overriding blocks).
Connectivity	-Ubuntu accessed the internet via pfSense NAT; Kali bridged to host network.	-Kali lost connectivity when host WiFi changed (required adapter reconfiguration).
Scalability	-Easy to expand (e.g., adding IDS like Suricata or VPN support).	-Manual traffic logging made forensic analysis tedious.
Ease of Use	-pfSense WebGUI is user-friendly for beginner	-Default WAN rules blocked private IPs, requiring manual adjustment.

10. Future Enhancements

1. Advanced Security Features

- Suricata IDS/IPS: Add intrusion detection for deeper attack analysis.
- GeoIP Blocking: Block traffic from high-risk regions.
- Rate Limiting: Throttle ICMP/SYN packets to prevent floods.

2. Network Resilience

- Failover WAN: Add a secondary ISP link for redundancy.
- VPN Integration: Secure remote management (OpenVPN/WireGuard).

3. Monitoring & Logging

- ELK Stack: Centralize logs for attack forensics.
- Grafana Dashboards: Visualize traffic patterns in real-time.

11. Critical Lessons Learned

- **Rule Order Matters:** pfSense processes rules top-down; place blocks before allows.
- **Test Rules Incrementally:** Avoid lockouts by testing one rule at a time.
- **Document Changes:** Label rules (e.g., "Allow Admin HTTPS") for easier troubleshooting.
- **Backup Configs:** Export pfSense settings before major changes.

12. Conclusion

This lab successfully demonstrated the setup and configuration of a pfSense-based firewall environment within Oracle VirtualBox, simulating a real-world network with distinct WAN and LAN segments. By deploying Kali Linux as the attacker, Ubuntu Desktop as the victim, and pfSense as the firewall, the lab effectively showcased the execution, detection, and mitigation of a Denial-of-Service (DoS) attack using tools like hping3 and Wireshark. The step-by-step configuration of pfSense firewall rules highlighted its robust capabilities in controlling network traffic and securing internal hosts against external threats. Key lessons learned, such as the importance of rule order, incremental testing, and clear documentation, underscore the practical challenges and solutions in firewall management. The lab provided valuable hands-on experience for cybersecurity enthusiasts, reinforcing the critical role of perimeter defense in protecting network infrastructure.