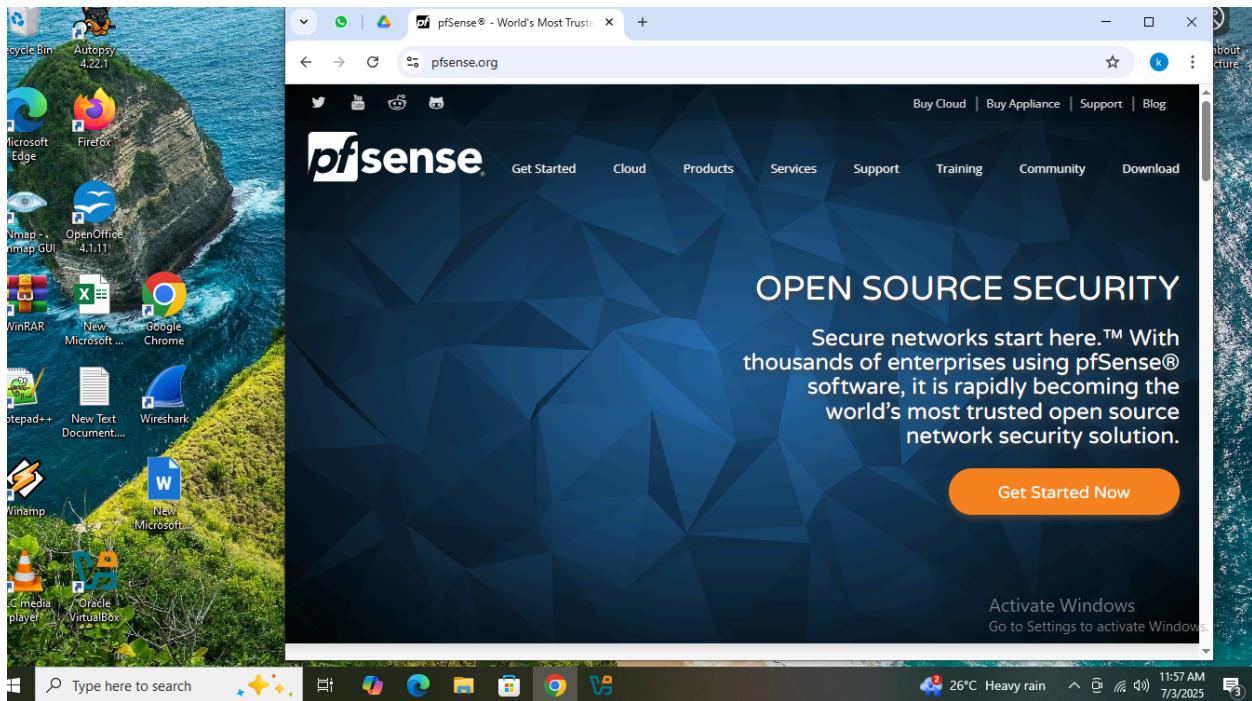


## VIRTUAL FIREWALL IMPLEMENTATION

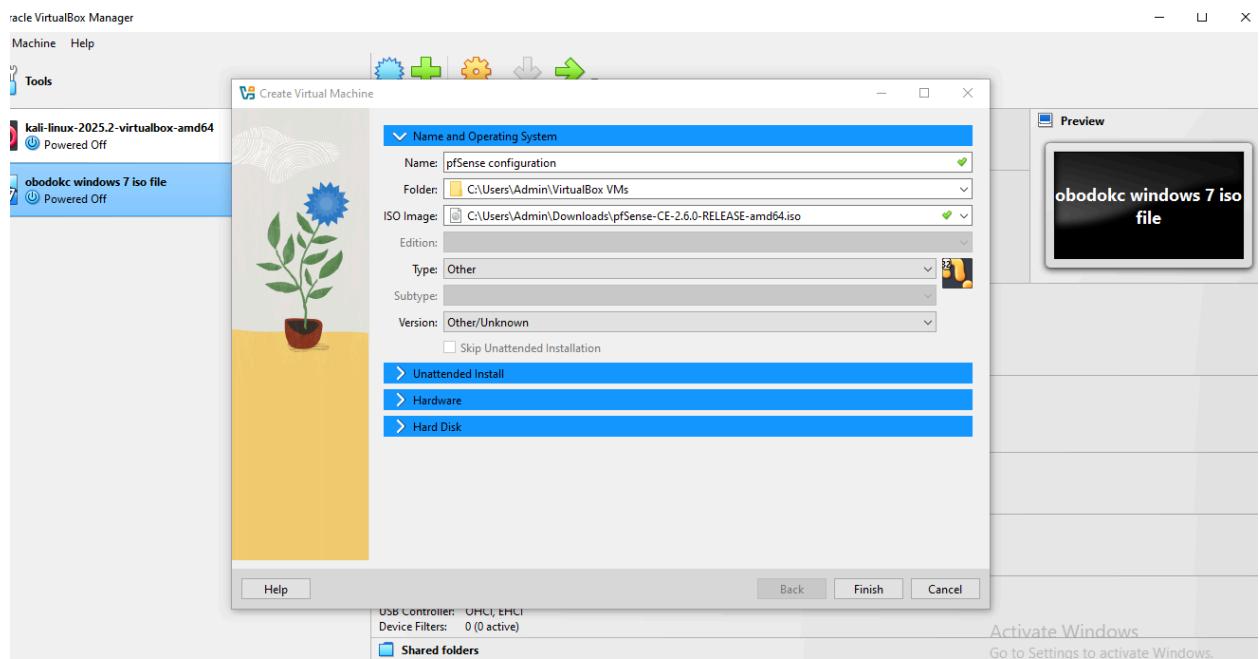
### USING PFSENSE

A Pfsense is s Virtual Firewall, a free open-source firewall and router distribution. It is used to build dedicated network security solutions for businesses of all sizes and home networks. pfSense offers a wide range of features, including Firewalling, Routing, VPN, DHCP, DNS, and many more. In this project, I am going to create a virtual firewall and perform some needed tasks.l

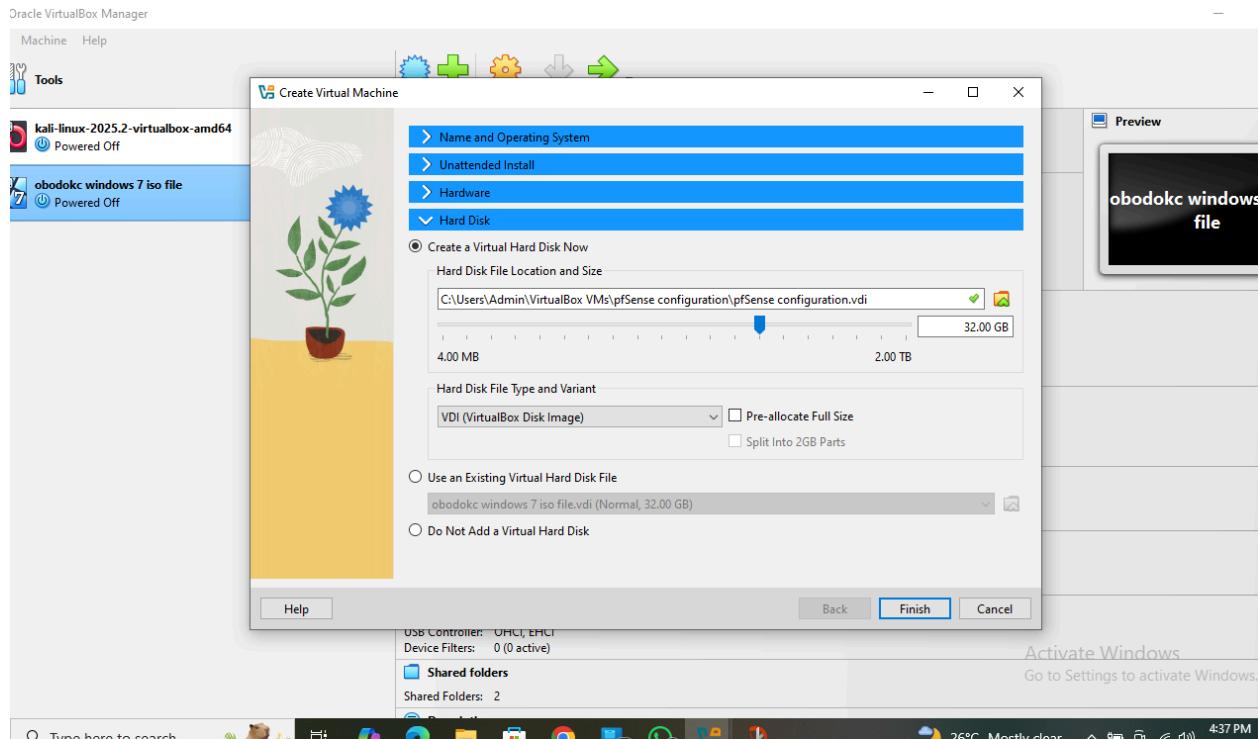
To start with, I downloaded the pfSense ISO

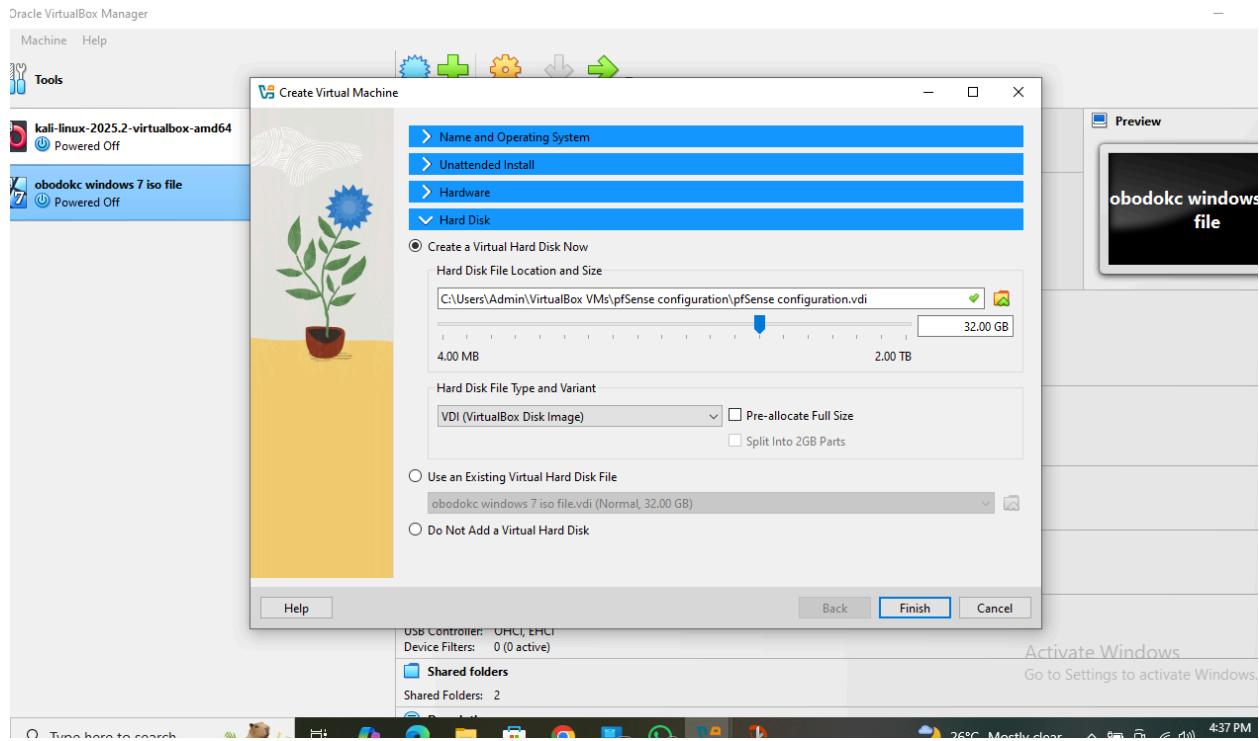


The pfSense was downloaded successfully, and 7zip was used to extract it to the file that will be compatible with the virtualbox. What I did next was to import the extracted ISO file into the virtualbox

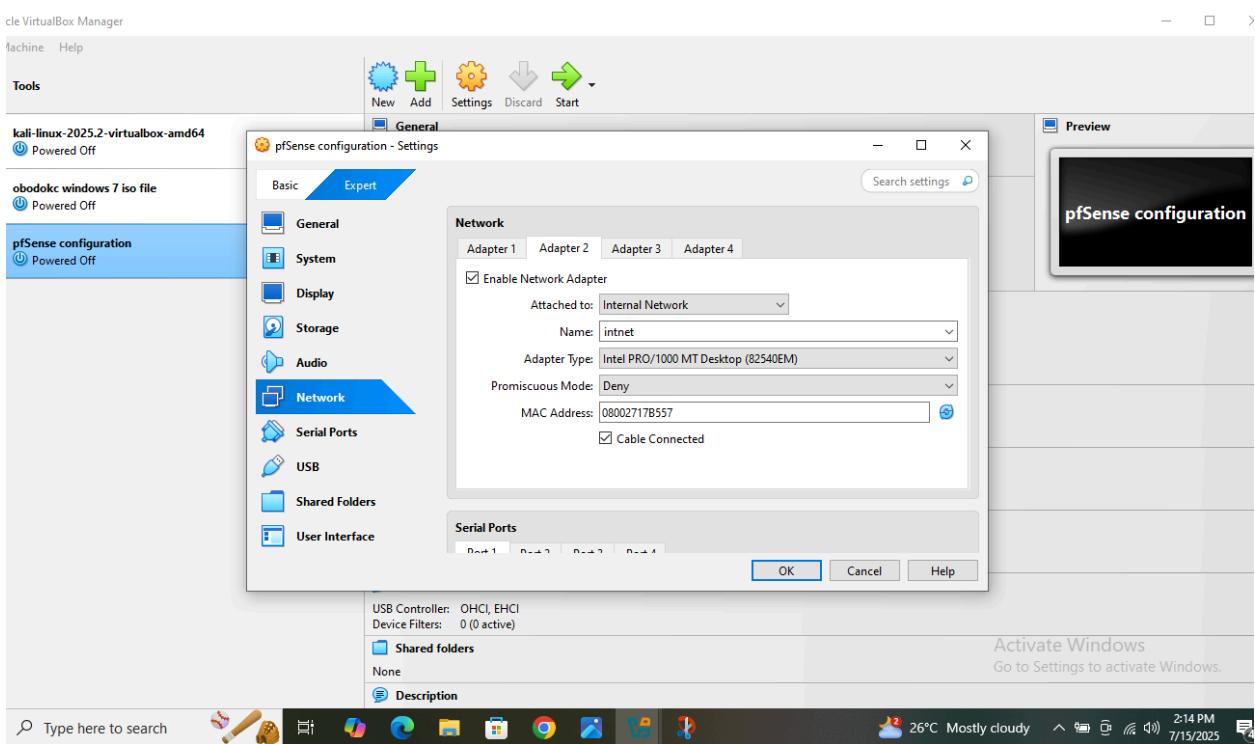
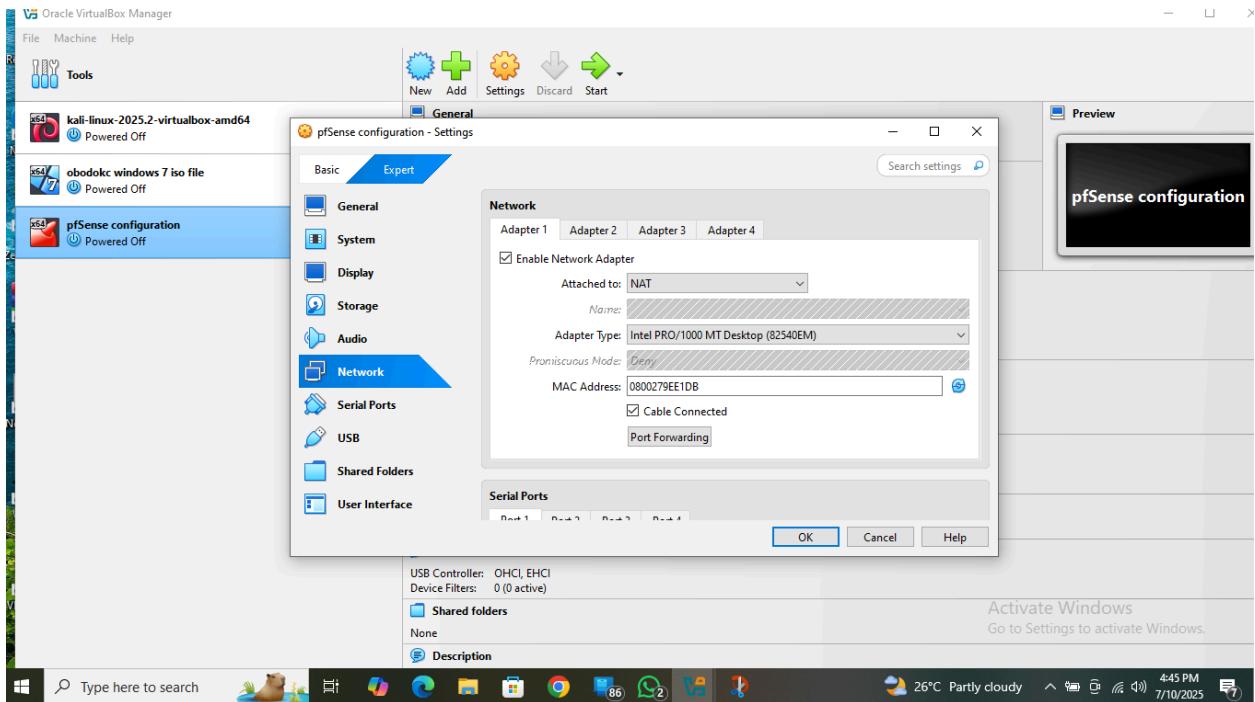


The above screenshot shows the process of importing the pfSense ISO file into the virtualbox. I named the pfSense 'pfSense configuration'. When I clicked on the folder icon, it took me to the location of the extracted ISO file, i selected and imported it and did some settings on the hardware and the hard disk.

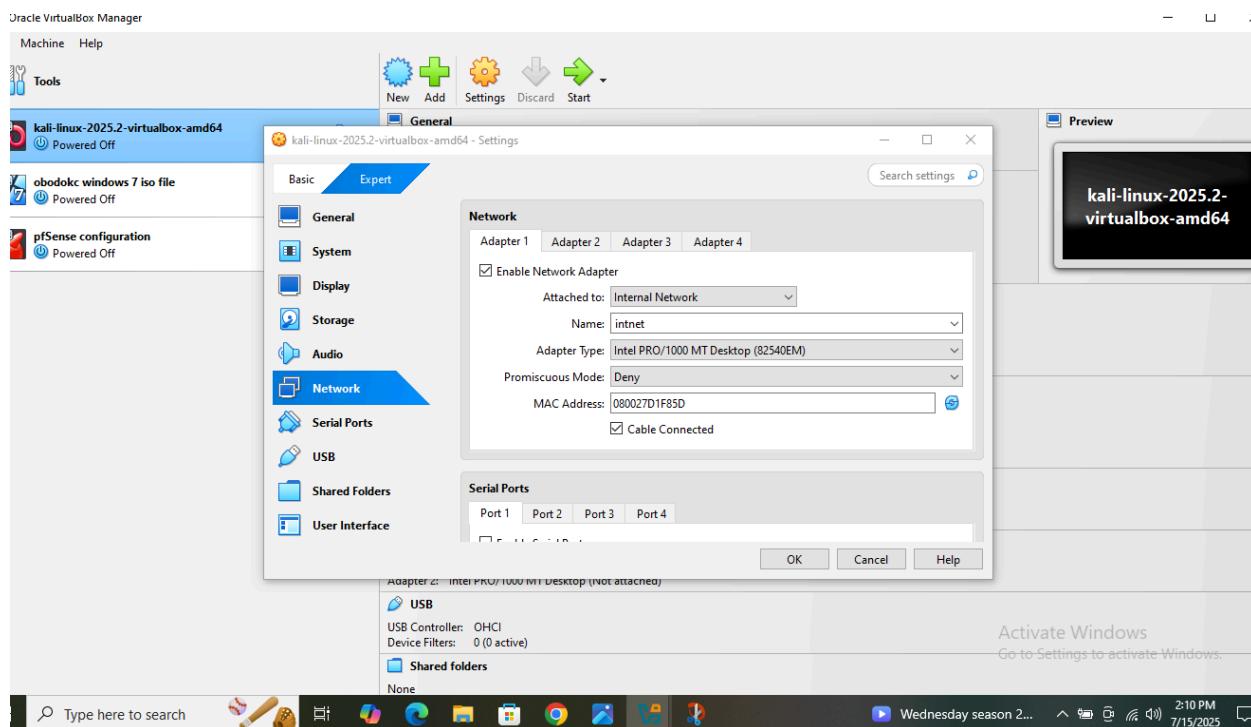
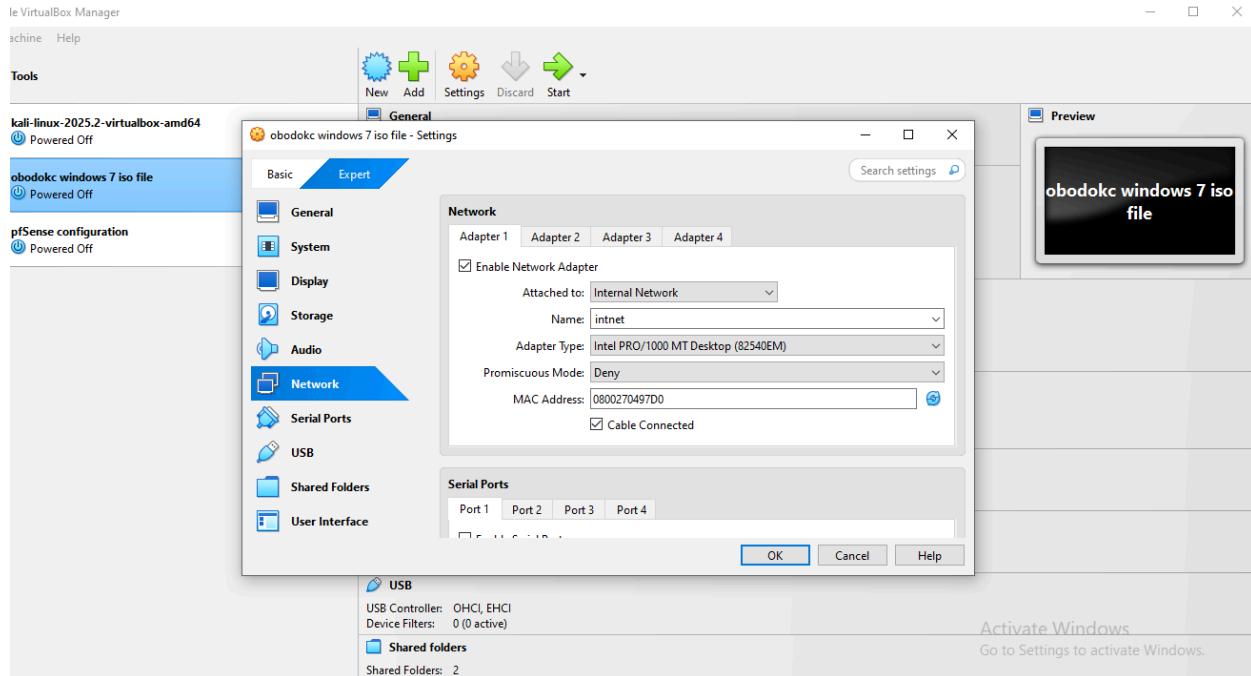




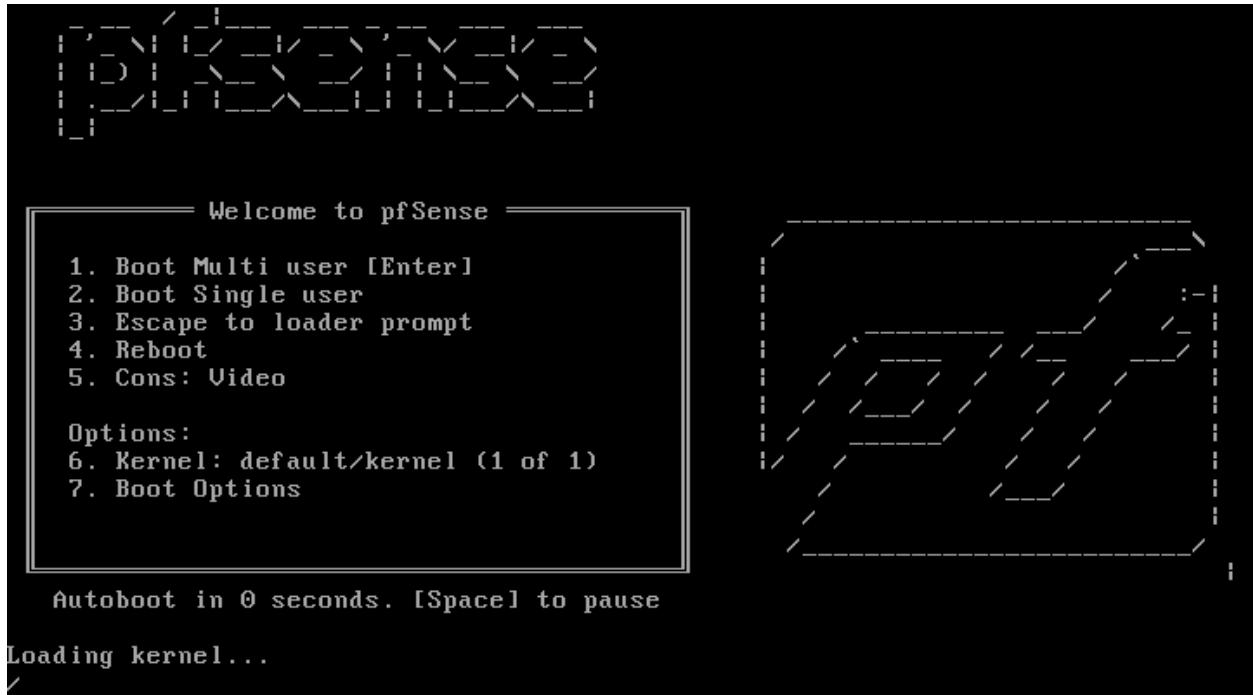
After the hardware and the hard disc settings, I started the configuration process of the pfSense ISO. In the processing of configuration process a prompt will come just select UFS(BIOS) and continue the pfSense configuration. After the installation is completed, the pfSense may start reinstalling itself again. To stop this, I went to the virtualbox after powering off the pfSense VM. I clicked on the settings and to the storage to remove the disk from the file. After removing the disk from the file I did some network adapter settings as shown below:



The network adapter that I did for the two VMs (kali and window7) are shown below:



From the above screenshot, I only set network adapter 1 for the VMs on internal network, while for pfSense, adapter 1 was set on NAT. While adapter 2 was set on internal network so it could communicate with the two VMs. Then I restarted the pfSense and it finally came to this;



And then to this:

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

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

VirtualBox Virtual Machine - Netgate Device ID: ea07e94970f5eecd17581

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

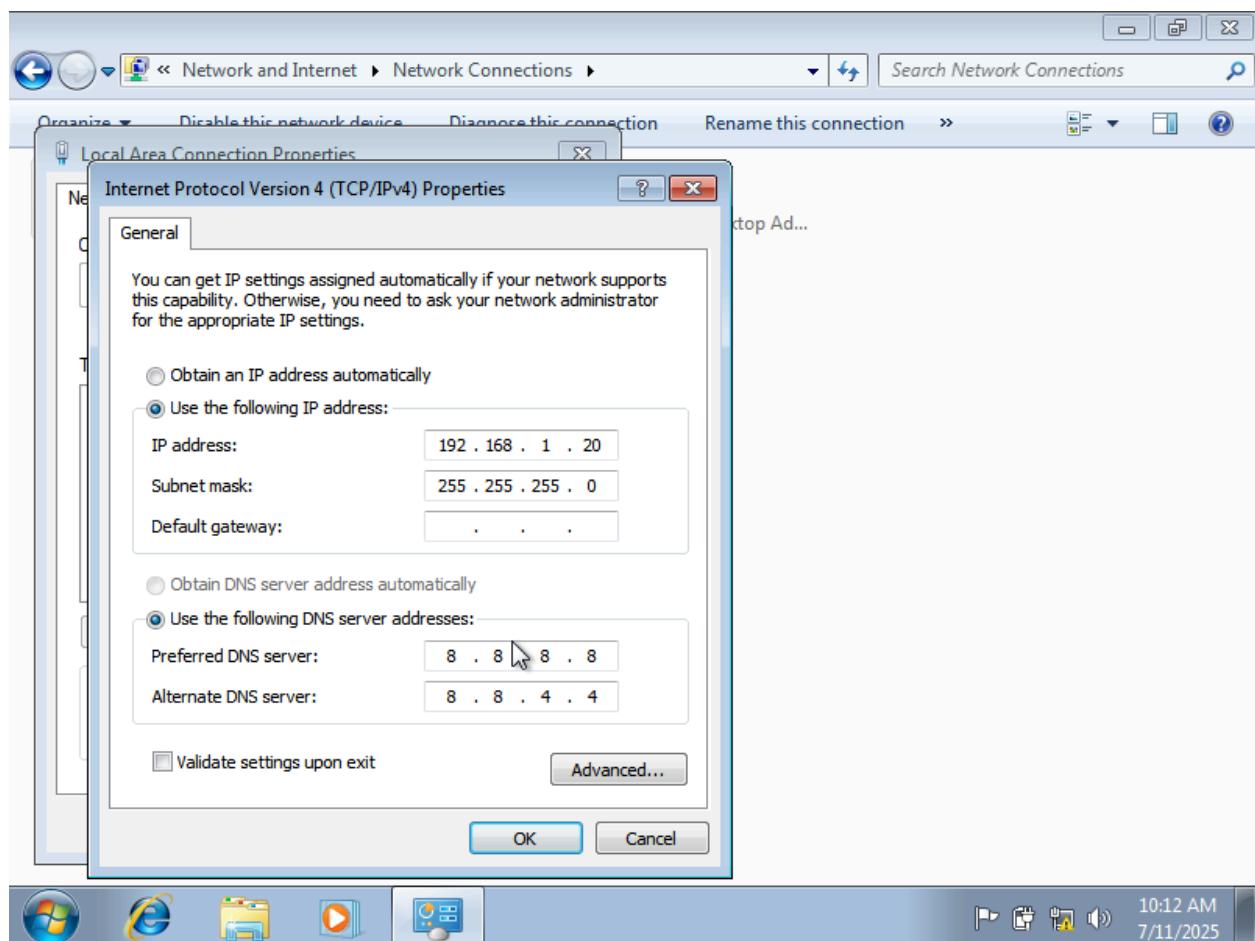
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
                           v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe9e:e1db/
64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

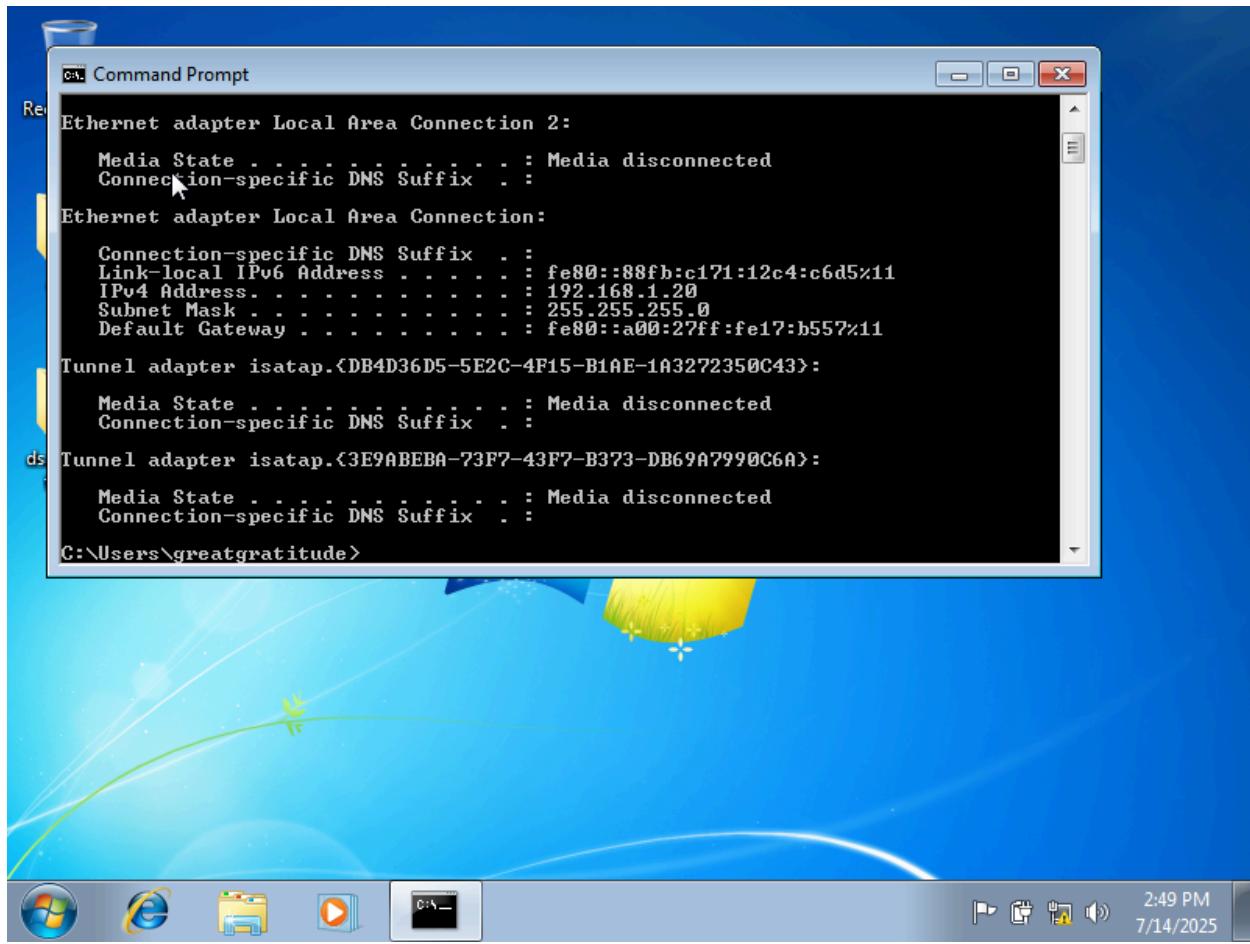
Enter an option: █
```

When I saw the LAN IP Address version 4, I discovered i needed to reset my VMs ip addresses. It is important to state that the above screenshot shows a complete configuration of the pfSense ISO

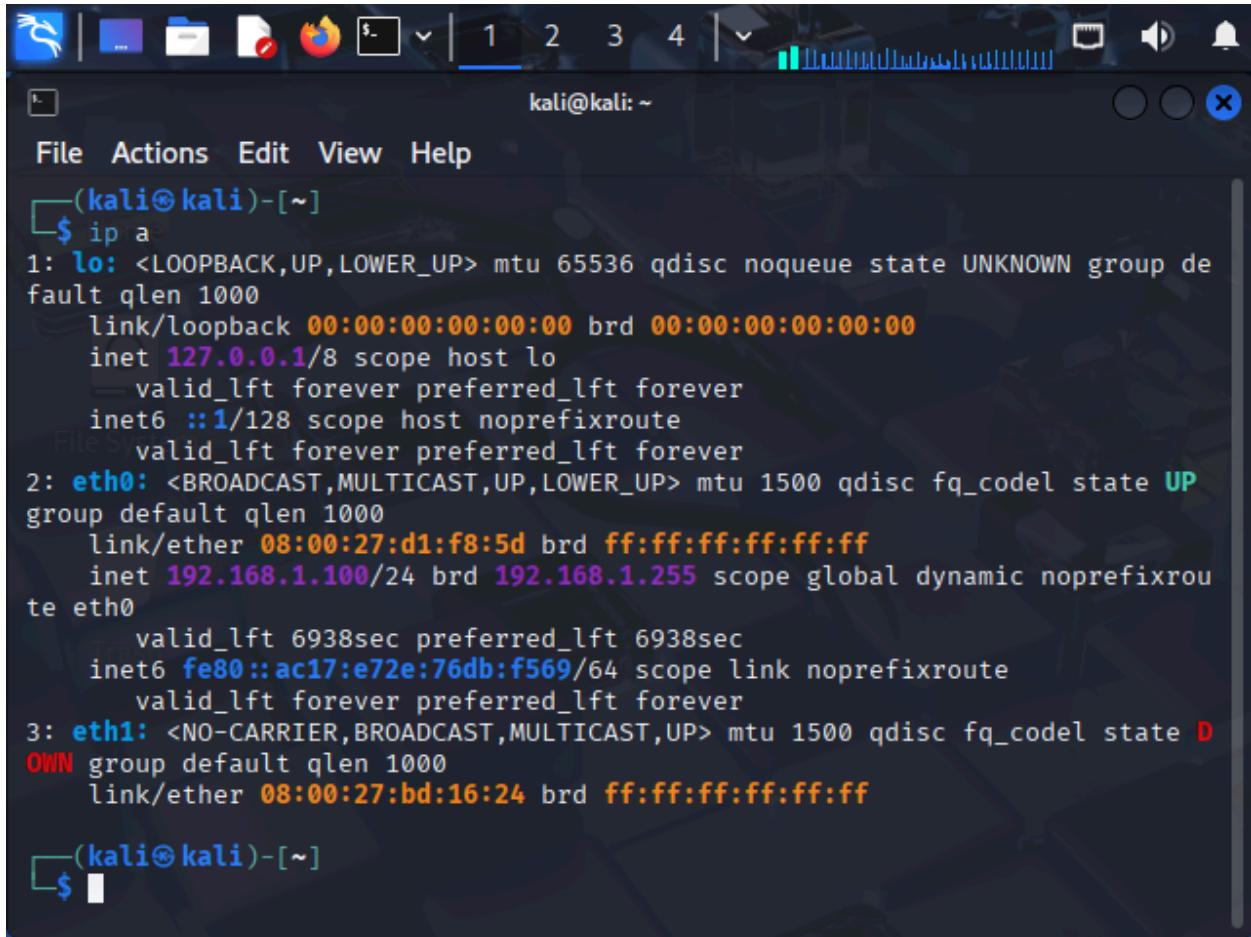
To reset the Windows vm ip address, I went to control panel, then to Network and Sharing, then to LAN. To IPV4 and finally to properties then change the static ip address to 192.168.1.20 and DNS 8.8.8.8 was also set.



After this I did ipconfig and it was



I also confirmed kali linux I discovered its having ip address 192.168.1.100. I decide not to adjust the ip address since it is in the same subnet with the virtual machines.



A screenshot of a Kali Linux terminal window titled "kali@kali: ~". The window shows the output of the command "ip a". The terminal interface includes a header bar with icons for file manager, browser, and terminal, and a menu bar with File, Actions, Edit, View, Help. The main area displays the following network configuration:

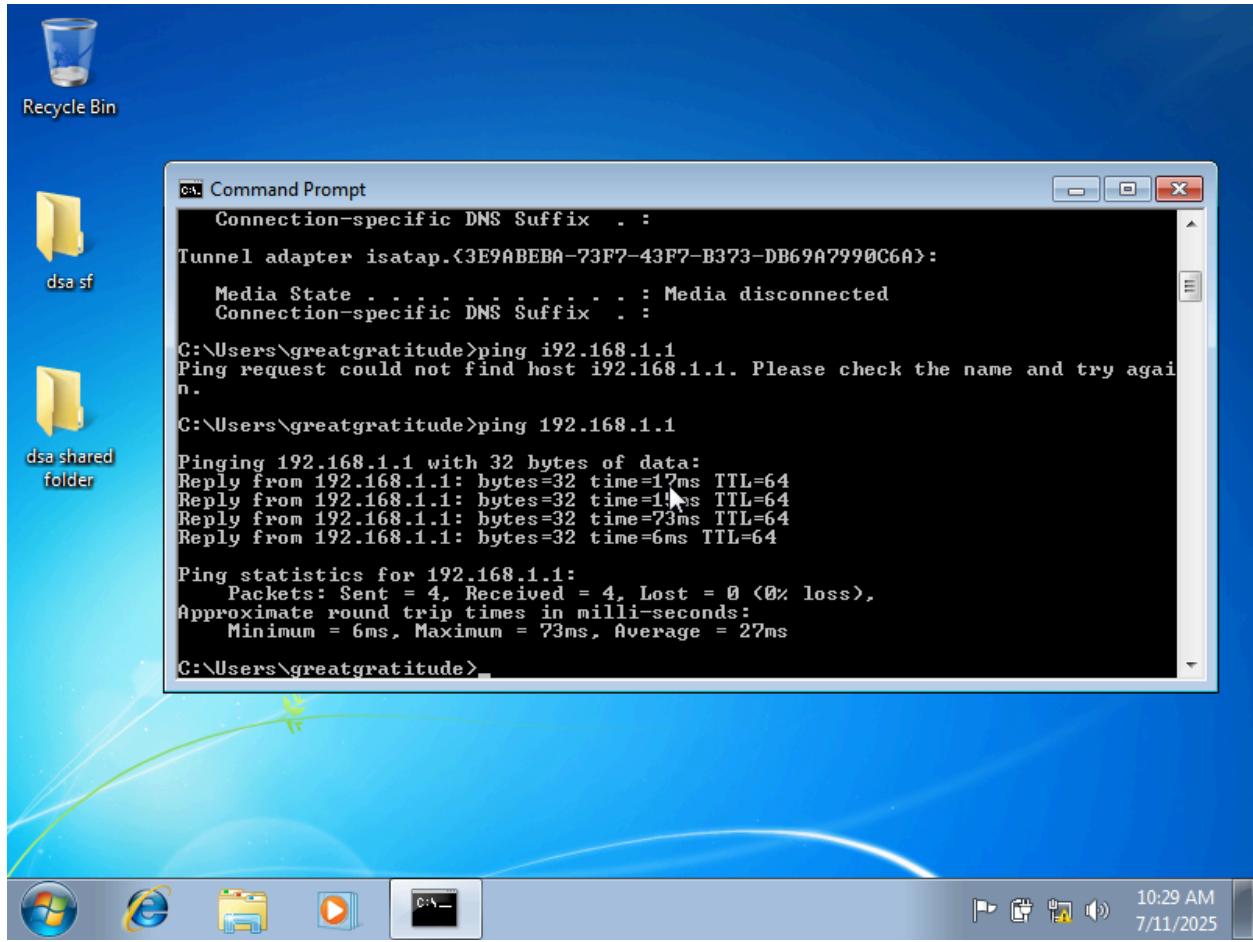
```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        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:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 6938sec preferred_lft 6938sec
    inet6 fe80::ac17:e72e:76db:f569/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:bd:16:24 brd ff:ff:ff:ff:ff:ff
```

Then I started doing service enumeration through ping to know whether the two VMs can actually communicate to one another.

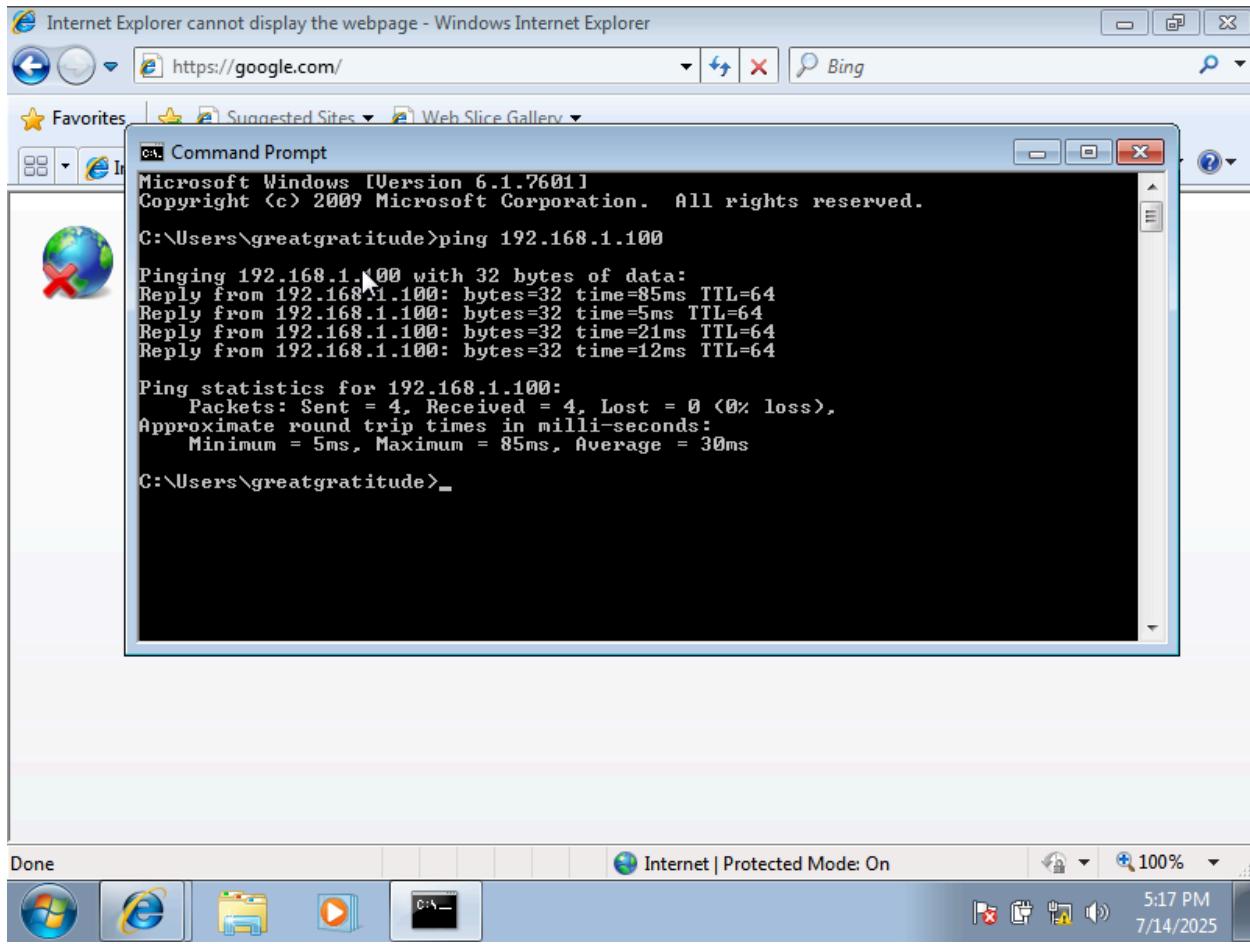
A screenshot of a Kali Linux terminal window. The terminal shows the output of a ping command to the IP address 192.168.1.1. The output includes 14 ICMP echo requests sent, 14 received, with 0% packet loss. The round-trip time (rtt) is listed as 13049ms with a minimum of 12.030ms, average of 125.624ms, maximum of 371.124ms, and standard deviation of 93.052ms. The terminal window has a dark blue background with a green header bar. The title bar says "kali@kali: ~". The menu bar includes "Applications", "File", "Actions", "Edit", "View", and "Help". The bottom of the window shows the command prompt "(kali㉿kali)-[~]" and a blue dollar sign.

```
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=111 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=97.9 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=371 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=182 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=32.2 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=193 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=208 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=102 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=177 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=12.0 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=124 ms
^C
--- 192.168.1.1 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13049ms
rtt min/avg/max/mdev = 12.030/125.624/371.124/93.052 ms
```

That was Kali Linux communicating with the pfSense through pinging.



That was window 7 vm communicating with the pfSense through pinging.



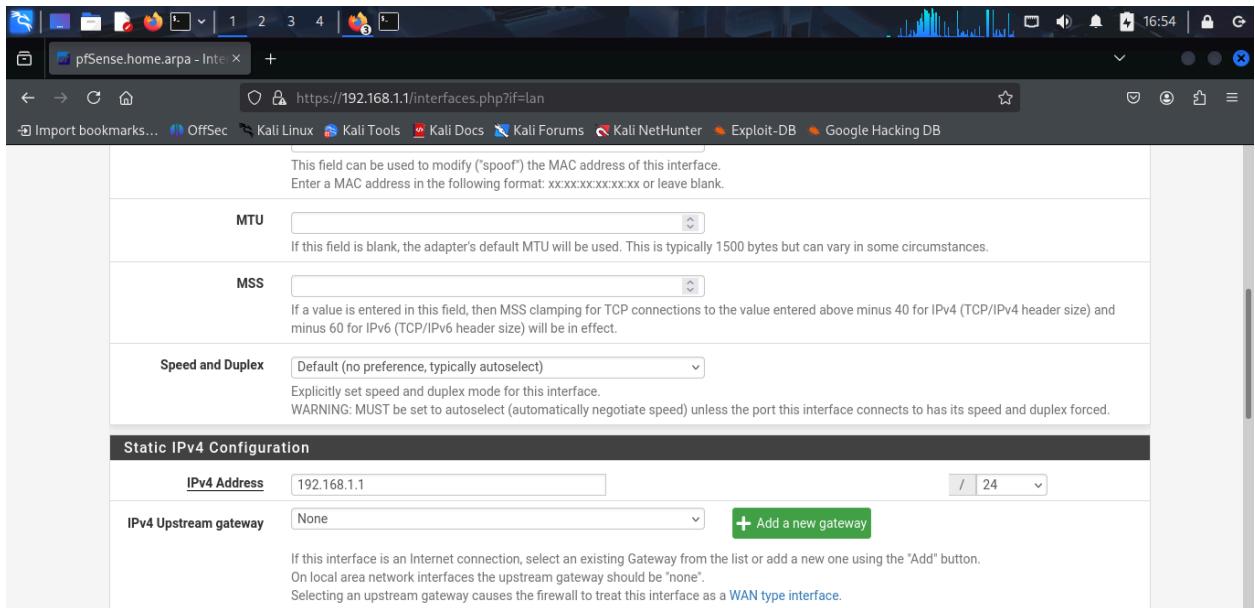
That was window 7 vm communicating with the kali linux through pinging.  
The next thing to do now is to set up firewall rule for the VMs. To achieve this, we need to gain entrance into the pfSense site. I started my kali linux and went to its firefox. On the browser i typed [https://192.168.1.1\(pfSense ip address\)](https://192.168.1.1(pfSense ip address)) and hit enter. It brought me to the pfSense site where i signed in and the firewall environment opened.

The screenshot shows the pfSense Status / Dashboard page. On the left, the System Information panel displays details such as Name (pfSense.home.arpa), User (admin@192.168.1.100), System (VirtualBox Virtual Machine), BIOS (Vendor: innotech GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006), and Version (2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022). On the right, the Netgate Services And Support panel shows a message "Retrieving support information" and the Interfaces panel lists two ports: WAN (10.0.2.15, fd17:625cf037:2:a00:27ff:fe9e:e1db) and LAN (192.168.1.1).

The screenshot shows the pfSense Firewall / Rules / LAN page. The LAN tab is selected. The Rules (Drag to Change Order) table lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 /156 KiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
✓ 0 /117 KiB	IPv4	*	LAN net	*	*	*	*	none	Default allow LAN to any rule	
✓ 0 /0 B	IPv6	*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

At the bottom, there are buttons for Add, Delete, Save, and Separator.



This screenshot shows the pfSense LAN interface configuration page. The URL is <https://192.168.1.1/interfaces.php?if=lan>. The page includes fields for MTU, MSS, Speed and Duplex, and a Static IPv4 Configuration section where the IP address is set to 192.168.1.1.

**MTU:** [Input field]  
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS:** [Input field]  
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

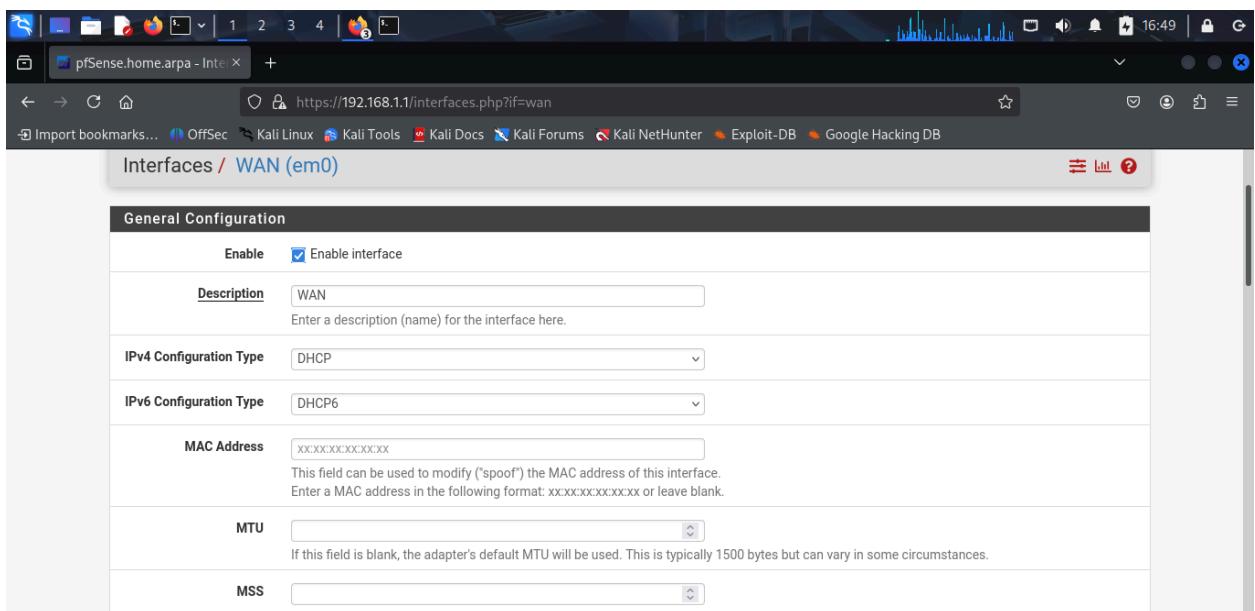
**Speed and Duplex:** [Select dropdown] Default (no preference, typically autoselect)  
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address:** [Input field] 192.168.1.1 / 24  
**IPv4 Upstream gateway:** [Input field] None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be 'none'.  
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.

The last two screenshots are the LAN of the pfSense firewall.



This screenshot shows the pfSense WAN interface configuration page. The URL is <https://192.168.1.1/interfaces.php?if=wlan>. The page includes fields for General Configuration, MAC Address, MTU, and MSS.

**General Configuration**

**Enable:**  Enable interface

**Description:** [Input field] WAN  
Enter a description (name) for the interface here.

**IPv4 Configuration Type:** [Select dropdown] DHCP

**IPv6 Configuration Type:** [Select dropdown] DHCP6

**MAC Address:** [Input field] XX:XX:XX:XX:XX:XX  
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxx:xxxx:xxxx or leave blank.

**MTU:** [Input field]  
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS:** [Input field]  
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and

The above is the WAN interface.

This screenshot shows the 'General DNS Resolver Options' configuration page for the WAN interface. The 'Enable' checkbox is checked, and the 'Listen Port' is set to 53. The 'Network Interfaces' dropdown menu includes options like All, WAN, LAN, WAN IPv6 Link-Local, and LAN IPv6 Link-Local. The 'SSL/TLS Certificate' dropdown is set to 'webConfigurator default (6870cb026aadc)'. The 'SSL/TLS Listen Port' is set to 853.

This screenshot shows the 'General Settings' tab of the 'General DNS Resolver Options' configuration page. It displays the same settings as the previous screenshot, including the 'Enable' checkbox, 'Listen Port' (53), 'Network Interfaces' (All), 'SSL/TLS Certificate' (webConfigurator default), and 'SSL/TLS Listen Port' (853).

The above is the DNS interface on the pfSense firewall

The screenshot shows the pfSense web interface for managing the DHCP LAN service. The URL is https://192.168.1.1/services\_dhcp.php. The page title is "Services / DHCP Server / LAN". The "LAN" tab is selected. Under the "General Options" section, the "Enable" checkbox is checked. The "Deny unknown clients" dropdown is set to "Allow all clients". The "Ignore client identifiers" checkbox is unchecked. Below these settings, there is a note about dual-boot clients. The "Subnet" field is set to 192.168.1.0, "Subnet mask" to 255.255.255.0, and "Available range" to 192.168.1.1 - 192.168.1.254. A "Range" input field shows "192.168.1.100" in the "From" field and "192.168.1.199" in the "To" field.

This screenshot shows the same pfSense DHCP LAN configuration page, but with the "Deny unknown clients" dropdown expanded. It contains three options: "Allow all clients", "Allow known clients from any interface", and "Allow known clients from only this interface". The "Allow all clients" option is selected. The other sections of the page remain the same as in the first screenshot.

The above shows the DHCP LAN interface on the pfSense firewall.

**Edit Redirect Entry**

<b>Disabled</b>	<input type="checkbox"/> Disable this rule
<b>No RDR (NOT)</b>	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
<b>Interface</b>	WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.	
<b>Address Family</b>	IPv4
Select the Internet Protocol version this rule applies to.	
<b>Protocol</b>	TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.	
<b>Source</b>	<a href="#">Display Advanced</a>

<b>Destination</b>	<input type="checkbox"/> Invert match.	WAN address	/
Type Address/mask			
<b>Destination port range</b>	Other	Custom	Other
From port	Custom	To port	Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.			
<b>Redirect target IP</b>	Single host	Address	
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (:1)			
<b>Redirect target port</b>	Other	Custom	
Port	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.		
<b>Description</b>	A description may be entered here for administrative reference (not parsed).		

## The NAT interface.

Now to set a firewall rule for the two VMs(kali and window7), I selected the LAN and blocked the default firewall rule set already

The screenshot shows the pfSense Firewall Rules LAN tab. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The LAN tab is selected, showing three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 /156 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
✓ 0 /117 KIB	IPv4	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚙️
✓ 0 /0 B	IPv6	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚙️

Buttons at the bottom include Add, Save, and Separator.

I had to block the default rules for ipv4 and ipv6. When I did that, I discovered that I could no longer access the DNS server, I could no longer browse again.

The terminal window shows a ping command failing:

```
(kali㉿kali)-[~] $ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

The pfSense LAN configuration screen is visible below, showing a success message:

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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

The above means that I could no longer browse again after blocking the default firewall rule. What I did next was to set another firewall rule that will allow for pinging and for browsing.

The screenshot shows two stacked screenshots of a web browser displaying the pfSense Firewall Rules Edit page. Both screenshots have a dark blue header bar with various icons and a timestamp (19:21 or 19:26). The main content area is titled "Edit Firewall Rule".

**Action:** Pass (selected from a dropdown menu)

**Disabled:**  Disable this rule (unchecked)

**Interface:** LAN (selected from a dropdown menu)

**Address Family:** IPv4 (selected from a dropdown menu)

**Protocol:** ICMP (selected from a dropdown menu)

**ICMP Subtypes:** any (selected from a dropdown menu)

**Source:** Source: LAN net, Invert match: unchecked, Destination Address: /

**Destination:** Destination: any, Invert match: unchecked, Destination Address: /

**Extra Options:**

- Log:**  Log packets that are handled by this rule (unchecked)
- 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 (unchecked)

**Buttons:** Save (blue button)

After setting this rule I could not still ping DNS server nor browse. I then decided to set firewall rule for ports:

The screenshot shows the pfSense Firewall Rules / LAN page. A green message box at the top right indicates that changes have been applied successfully and the filter reload progress is pending. The LAN tab is selected, showing a single rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 /202 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	

The screenshot shows the pfSense Firewall Aliases / Edit page for an alias named "browsing". The "Properties" section includes:

Name	browsing	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	browsing ports	A description may be entered here for administrative reference (not parsed).	
Type	Port(s)		

The "Port(s)" section lists ports 80 and 443 with their respective descriptions and delete buttons.

Hint: Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.		
Port	80	Description
	443	Description

Description: browsing ports  
A description may be entered here for administrative reference (not parsed).

Type: Port(s)

Port	Description	Delete
80		
443		
8080		
53		

Save + Add Port

From the above screenshots, I allow port 80, 443, 8080 and 53 respectively. After setting the rule for port filtering, I went back to adjust the first rule that I made before the ports rule and I the the following adjustment:

Action: Pass  
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: LAN  
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/UDP  
Choose which IP protocol this rule should match.

The screenshot shows the pfSense firewall configuration page for editing rules. The URL is https://192.168.1.1/firewall\_rules\_edit.php?f=lan&after=-1. The page displays a form for defining a new rule. The 'Destination Port Range' section has 'From' set to 'Custom' and 'To' also set to 'Custom'. Below it, a note says 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.' Under 'Extra Options', there is a 'Log' checkbox which is unchecked. A hint below it states: '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).'. There is also a 'Description' field with a placeholder and an 'Advanced Options' section with a 'Display Advanced' button. At the bottom is a 'Save' button.

This time around I adjusted the rule by selected TCP/UDP on the protocol type unlike the ICMP I selected previously. I saved the rule and I tested it again.

The screenshot shows a terminal window titled 'Terminal Emulator' running on a Kali Linux system. The command entered was 'ping www.google.com'. The output shows the ping statistics for the first attempt:

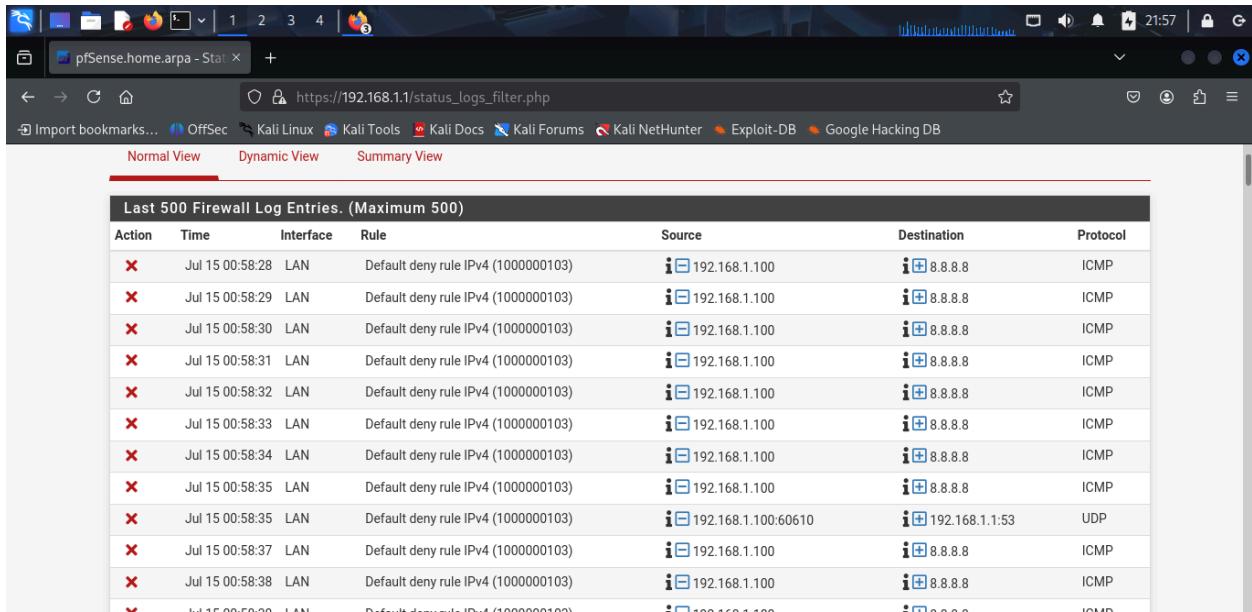
```
ping www.google.com
PING www.google.com (216.58.223.196) 56(84) bytes of data.
64 bytes from los02s03-in-f4.1e100.net (216.58.223.196): icmp_seq=1 ttl=254
time=271 ms
```

After pressing ^C, the terminal shows the statistics for the second attempt:

```
— www.google.com ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 156.026/213.489/270.952/57.463 ms
```

Now it is clear that I can now do pinging communication and browsing as well. I tested the firewall rule on my kali interface by doing, ping 8.8.8.8 and ping [www.google.com](http://www.google.com) and I discovered I could ping and browse again.

Now the two VMs have been connected to route traffic through the firewall.



The screenshot shows a Firefox browser window with the title "pfSense.home.arpa - Stat". The address bar displays "https://192.168.1.1/status\_logs\_filter.php". Below the address bar is a navigation bar with links: "Import bookmarks...", "OffSec", "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", and "Google Hacking DB". Underneath the navigation bar are three tabs: "Normal View" (selected), "Dynamic View", and "Summary View". The main content area is titled "Last 500 Firewall Log Entries. (Maximum 500)". It contains a table with the following columns: Action, Time, Interface, Rule, Source, Destination, and Protocol. The table lists ten entries, all of which are "Default deny rule IPv4 (1000000103)" with a source of 192.168.1.100 and a destination of 8.8.8.8. The protocol for all entries is ICMP. The table has a dark header row and light gray rows for the data.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 15 00:58:28	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:29	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:30	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:31	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:32	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:33	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:34	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:35	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:35	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100:60610	i 192.168.1.1:53	UDP
✗	Jul 15 00:58:37	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP
✗	Jul 15 00:58:38	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.100	i 8.8.8.8	ICMP

The above is the list of the firewall log entries. We can decide to unblock any rule here to make traffic adjustment.