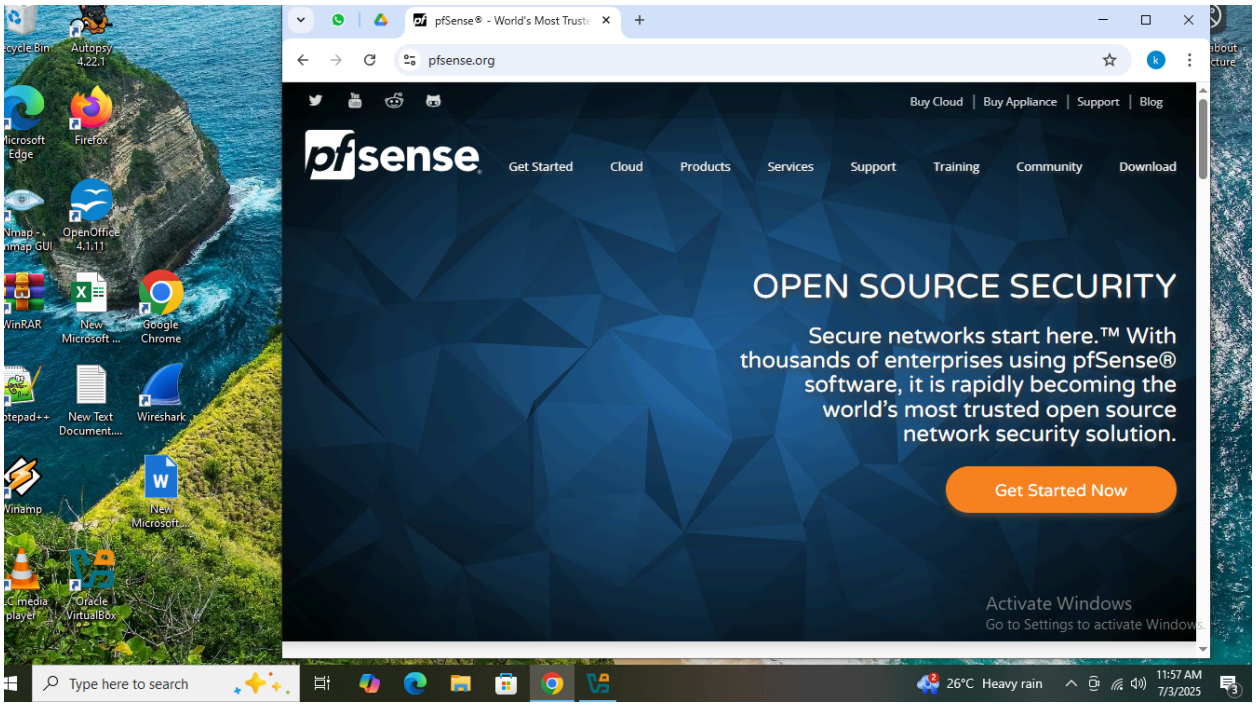
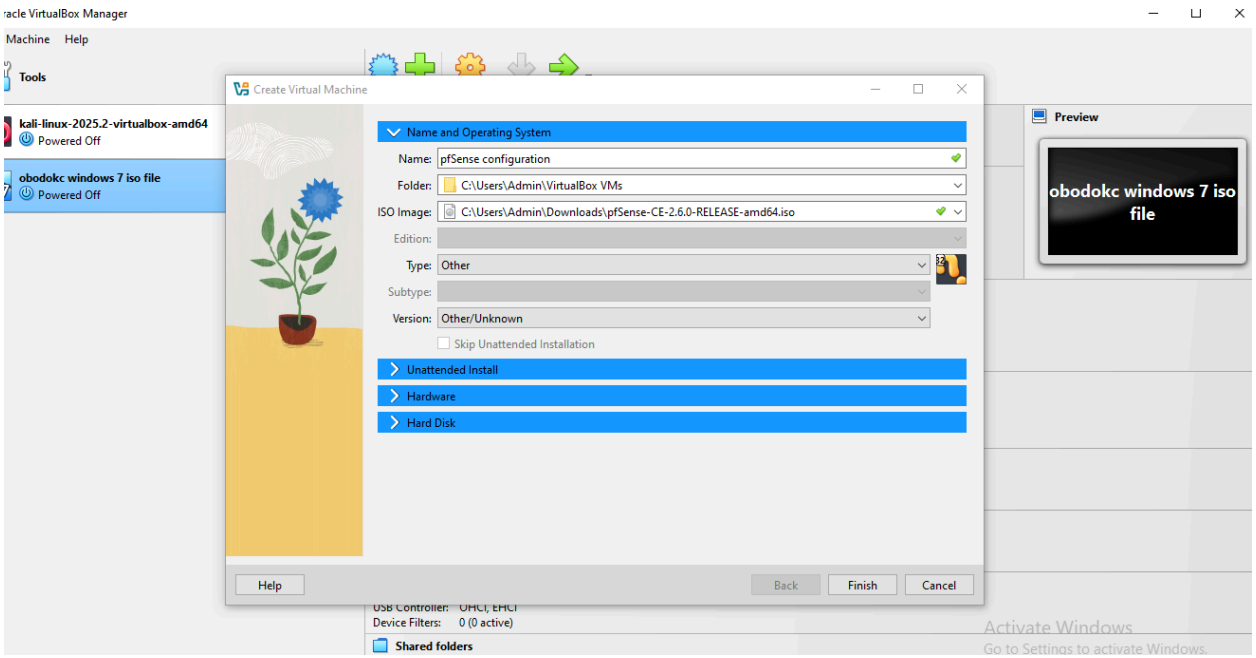
VIRTUAL FIREWALL IMPLEMENTATION USING PFSENSE

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.I

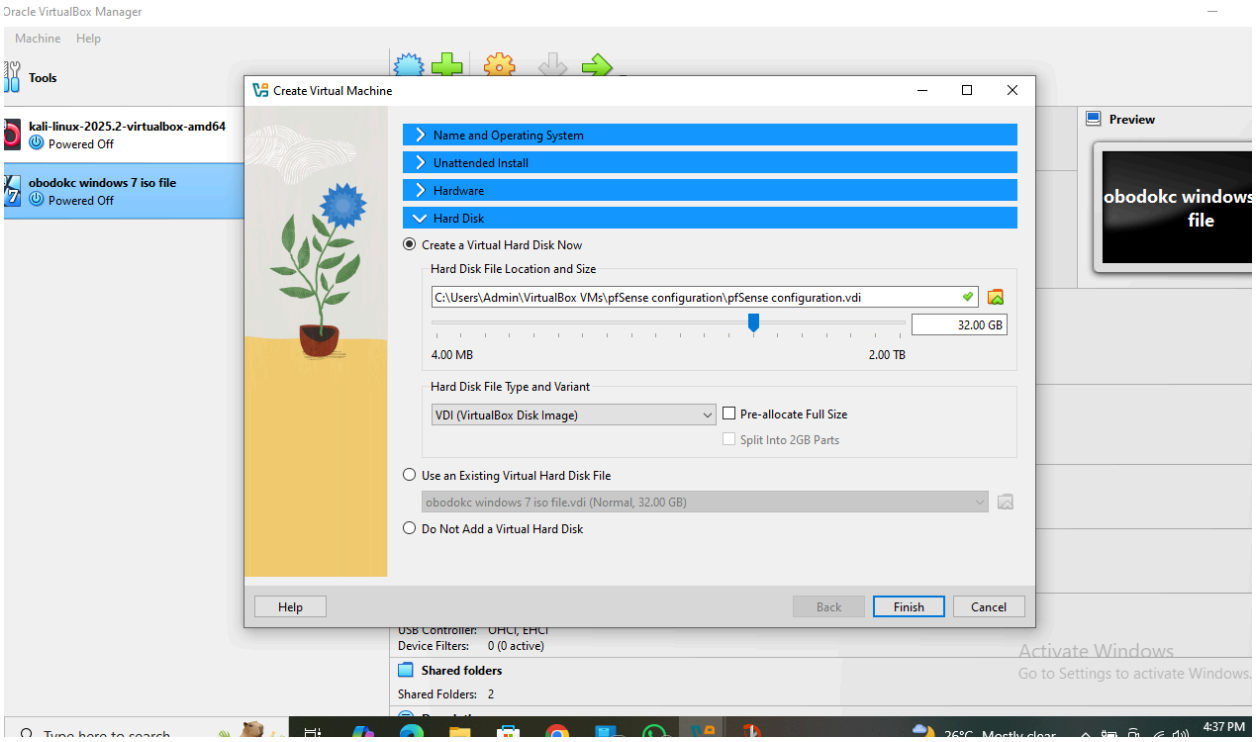
To sart with, I downloaded the pfSense ISO

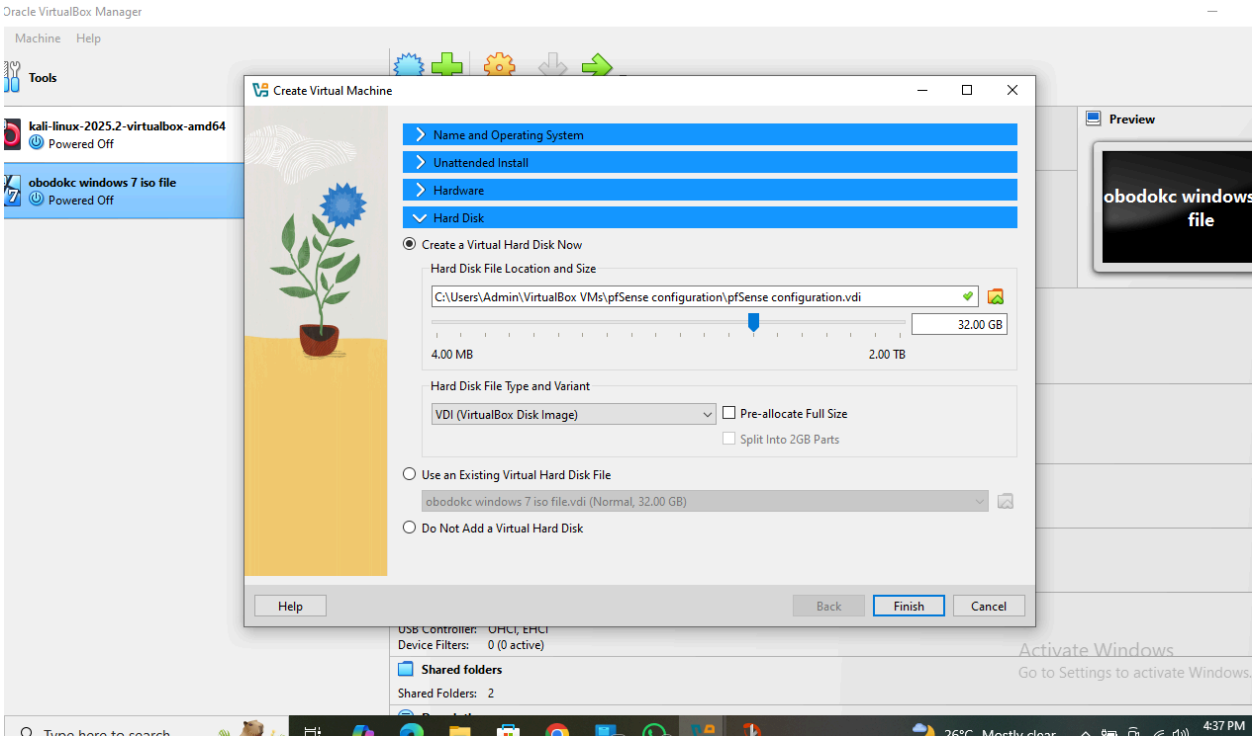


The pfSense was downloaded successfully, and 7zip was used to extract it to the file that will be compatible with the virtualbox. What I did next was to import the extracted ISO file into the virtualbox

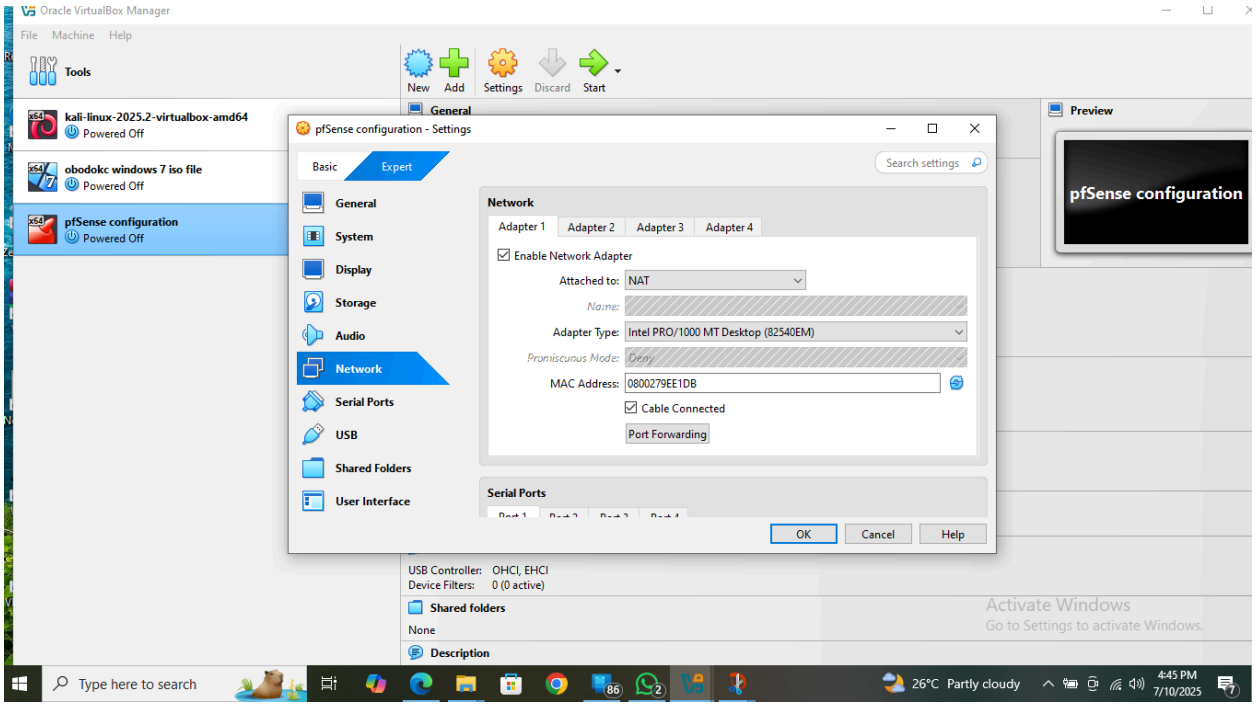


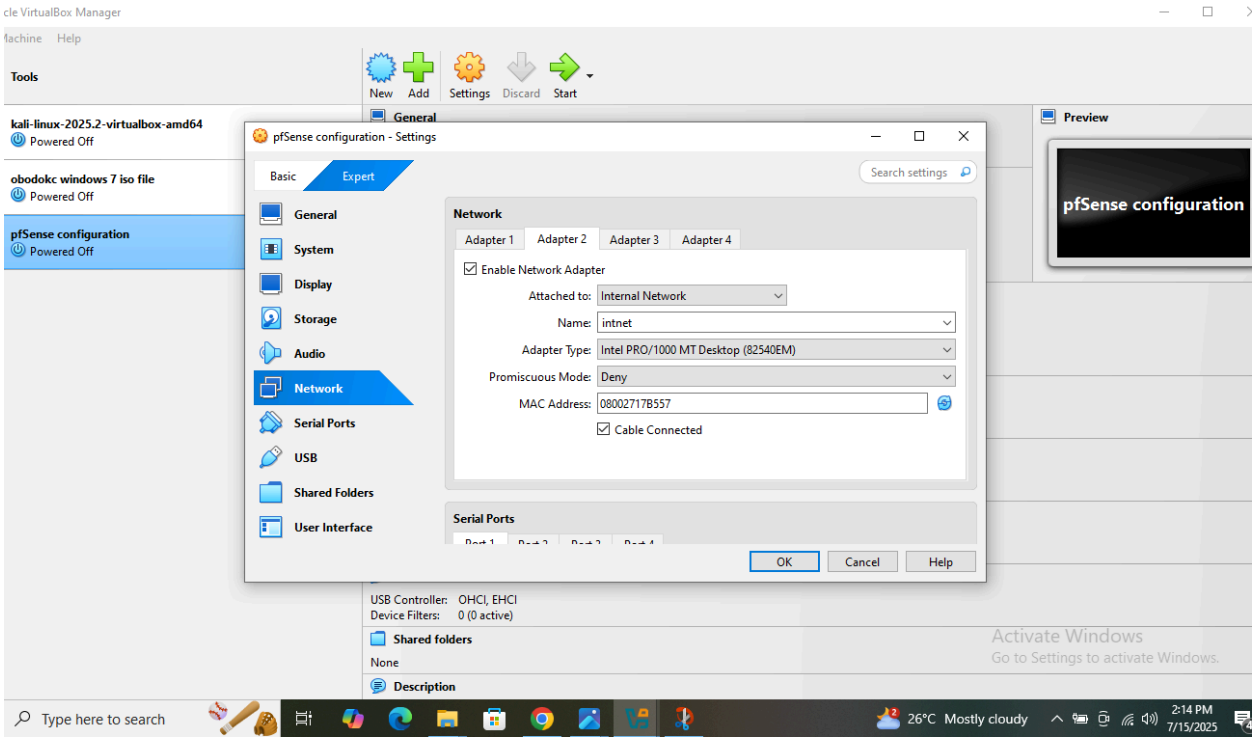
The above screenshot shows the process of importing the pfSense ISO file into the virtualbox. I named the pfSense 'pfSense configuration'. When I clicked on the folder icon, it took me to the location of the extracted ISO file, i selected and imported it and did some settings on the hardware and the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



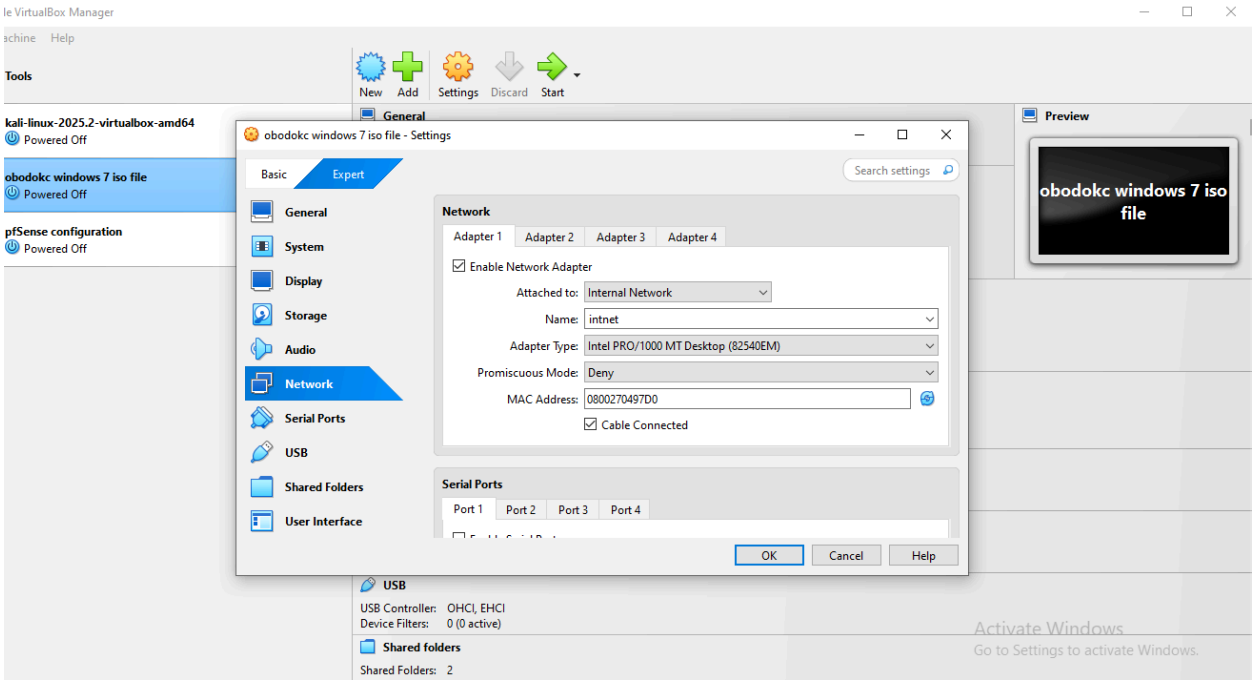


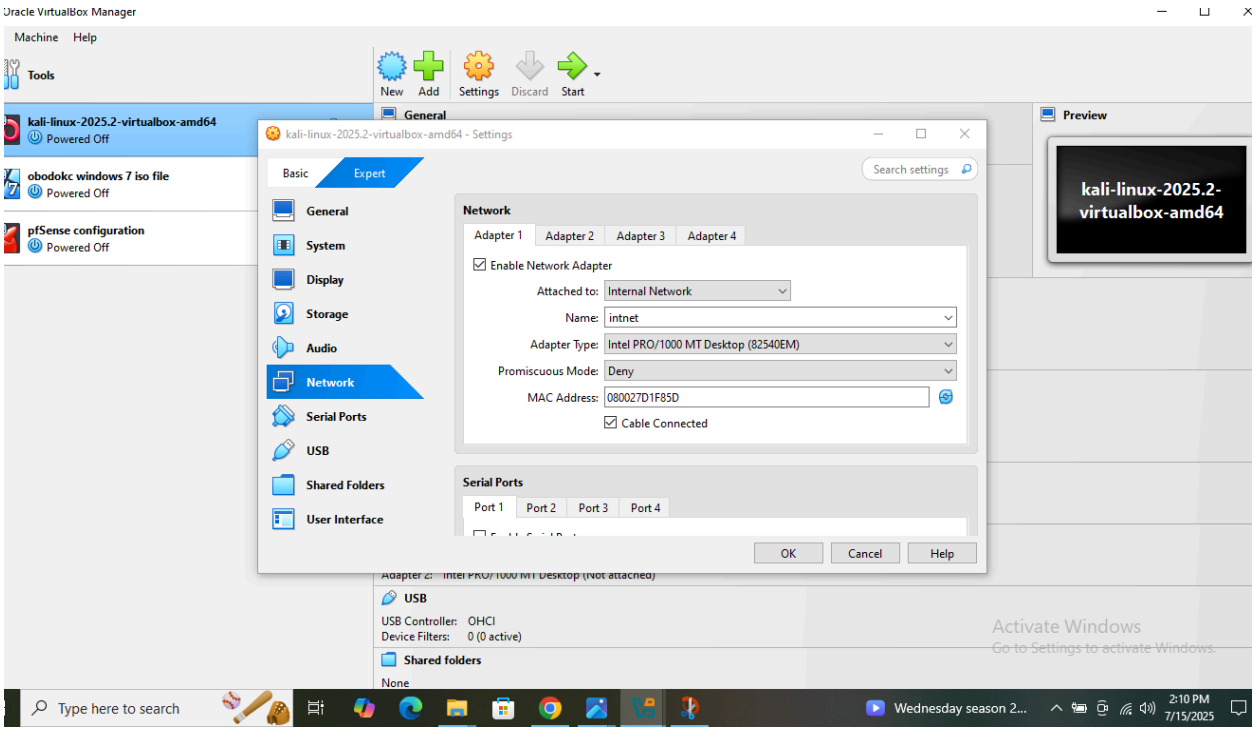
After the hardware and the hard disc settings, I started the configuration process of the pfSense ISO. In the processing of configuration process a prompt will come just select UFS(BIOS) and continue the pfSense configuration. After the installation is completed, the pfSense may start reinstalling itself 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:



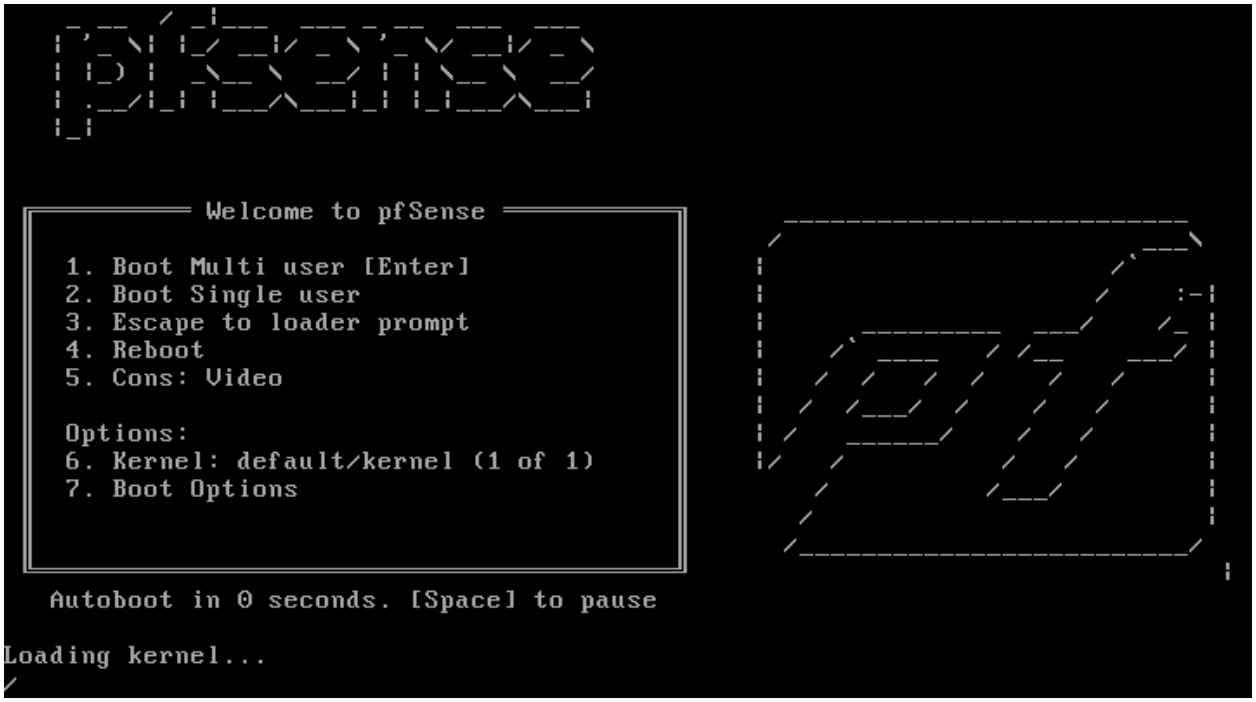


The network adapter that I did for the two VMs (kali and window7) are shown below:

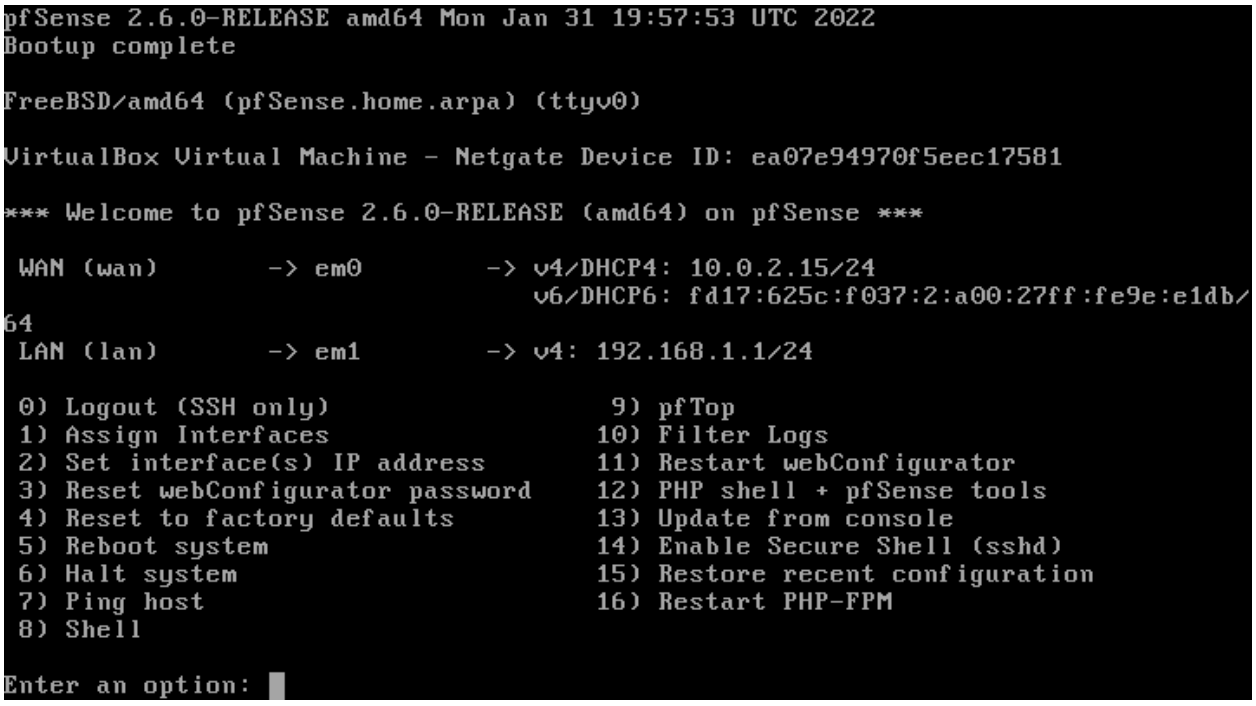




From the above screenshot, I only set network adapter 1 for the VMs on internal network, while for pfSense, adapter 1 was set on NAT. While adapter 2 was set on internal network so it could communicate with the two VMs. Then I restarted the pfSense and it finally came to this;

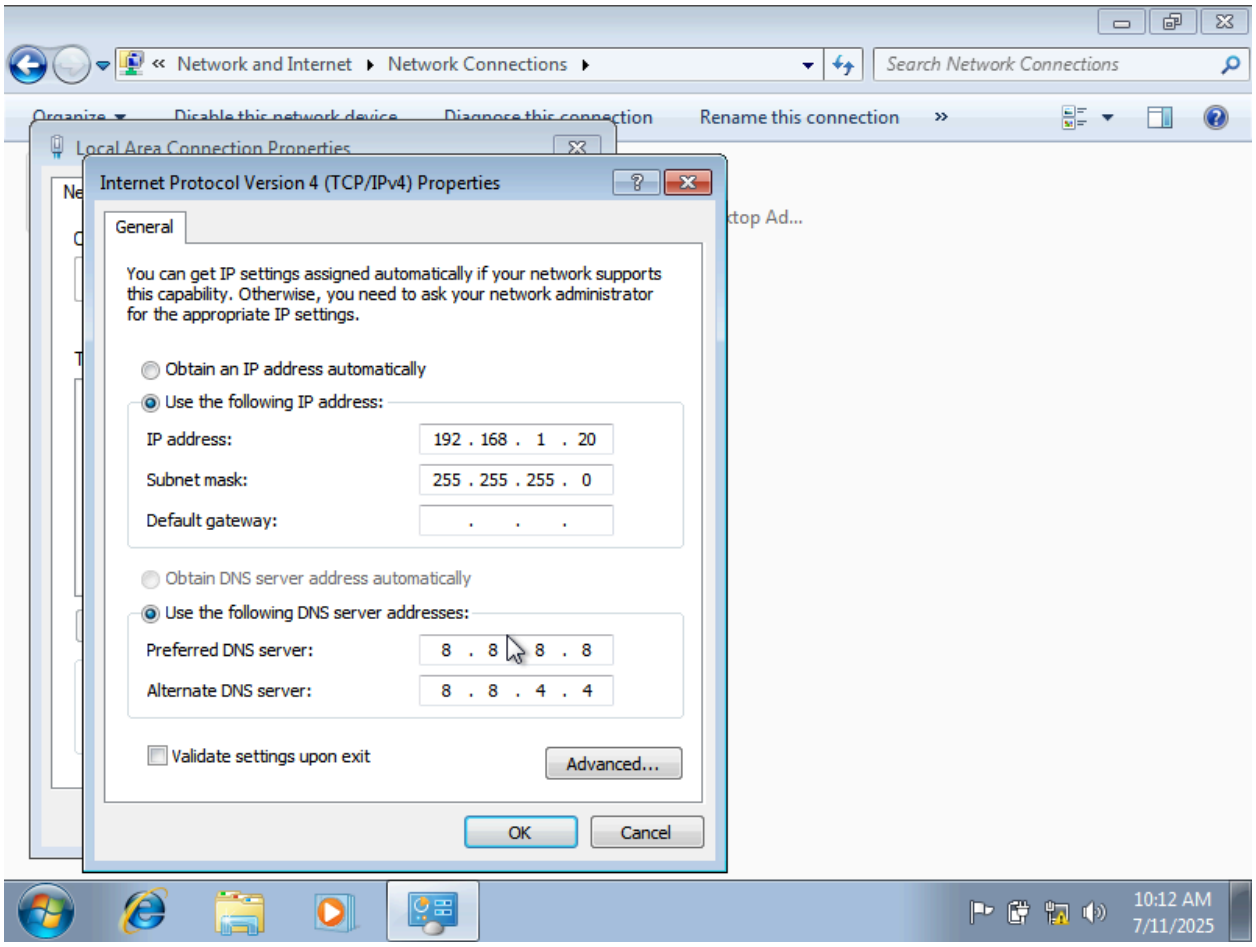


And then to this:

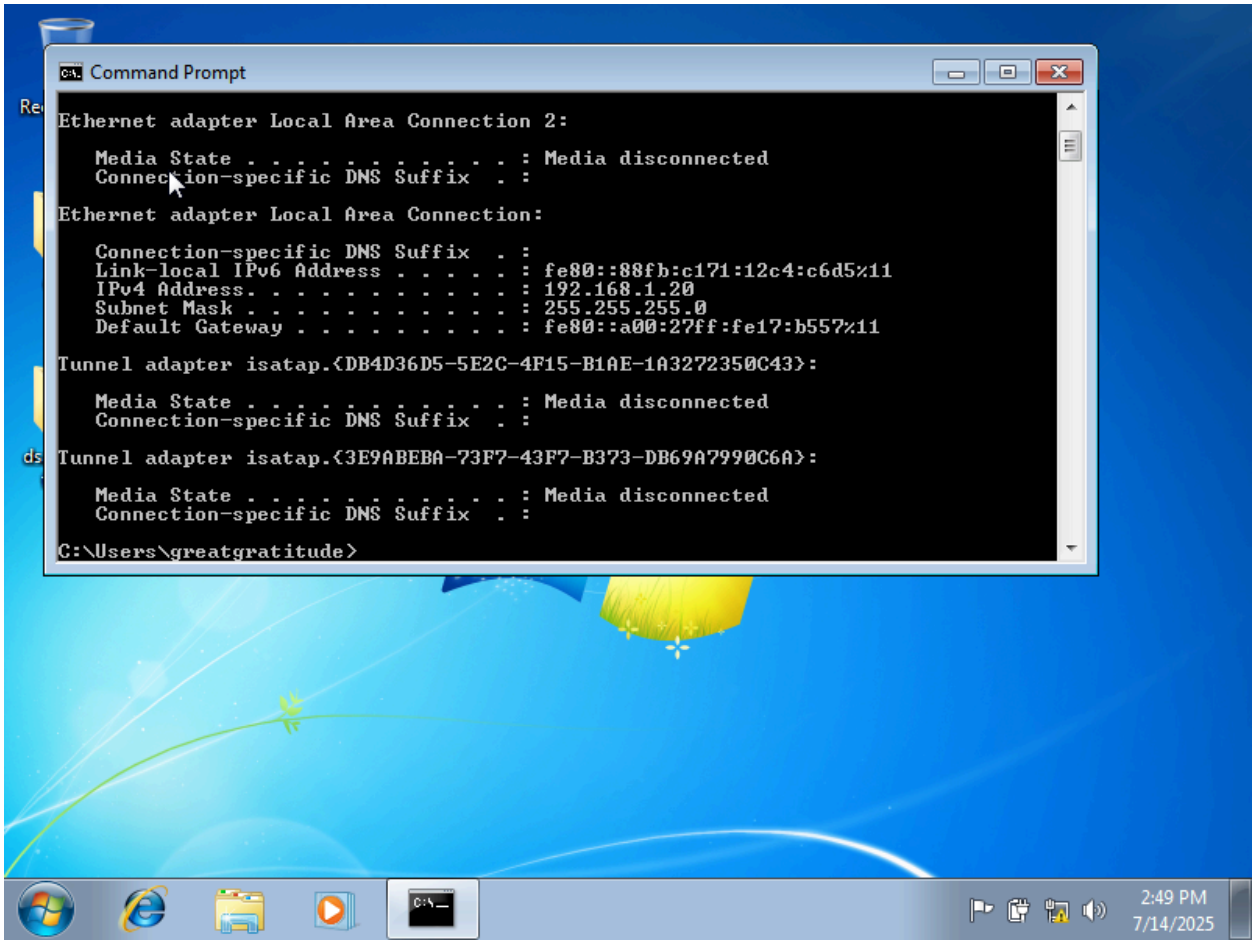


When I saw the LAN IP Address version 4, I discovered i needed to reset my VMs ip addresses. It is important to state that the above screenshot shows a complete configuration of the pfSense ISO

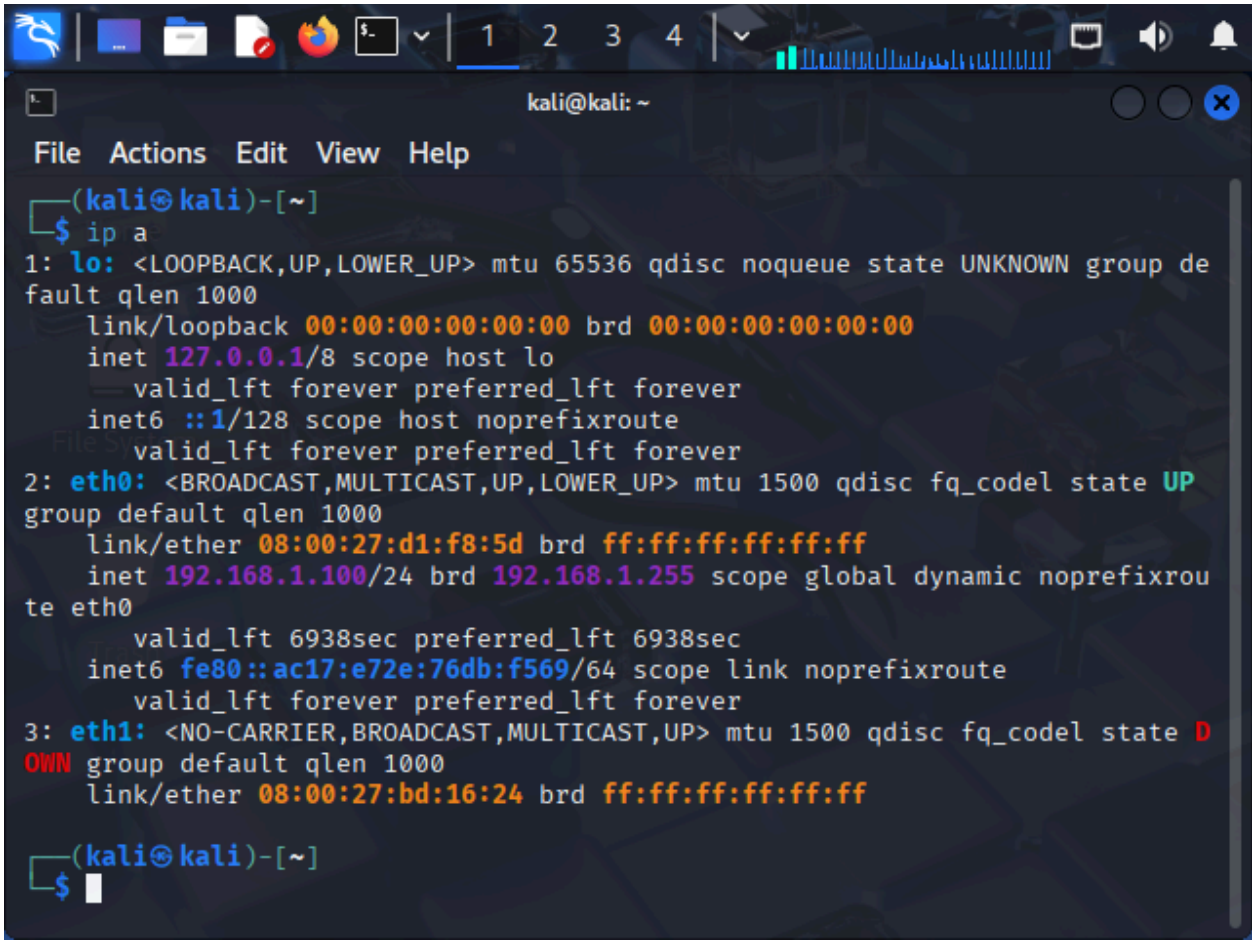
To reset the Windows vm ip address, I went to control panel, then to Network and Sharing, then to LAN. To IPV4 and finally to properties then change the static ip address to 192.168.1.20 and DNS 8.8.8.8 was also set.



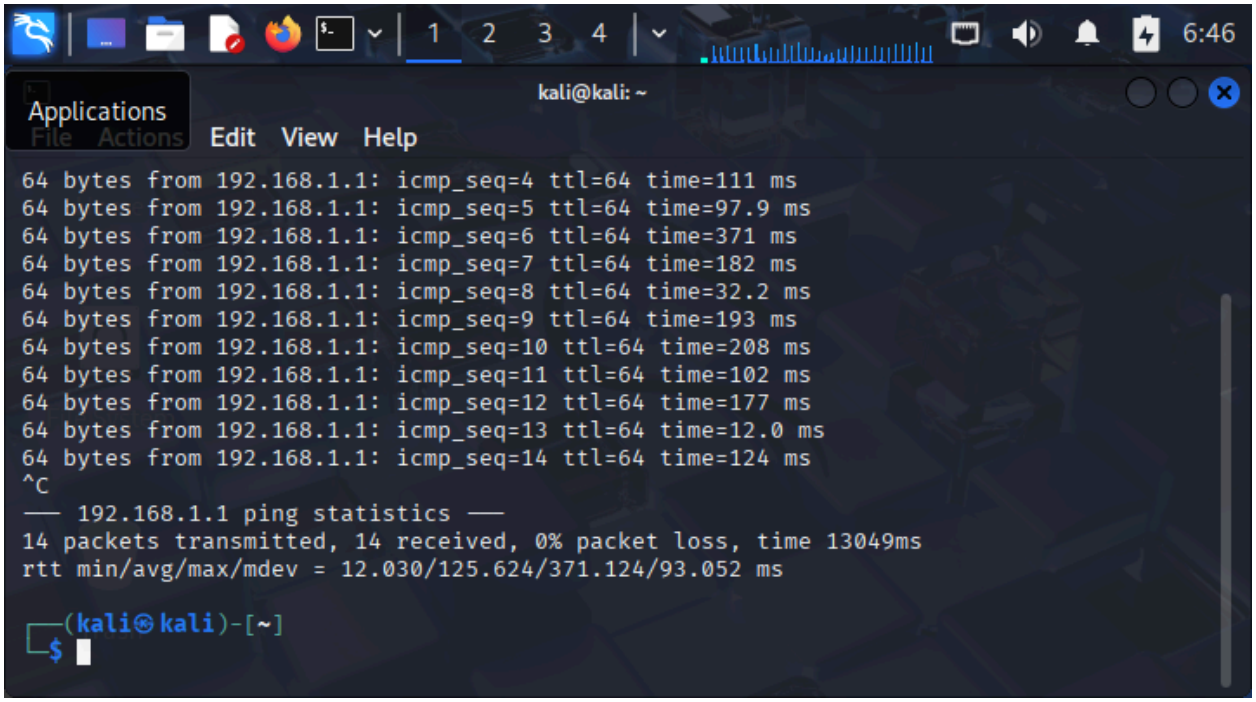
After this I did ipconfig and it was



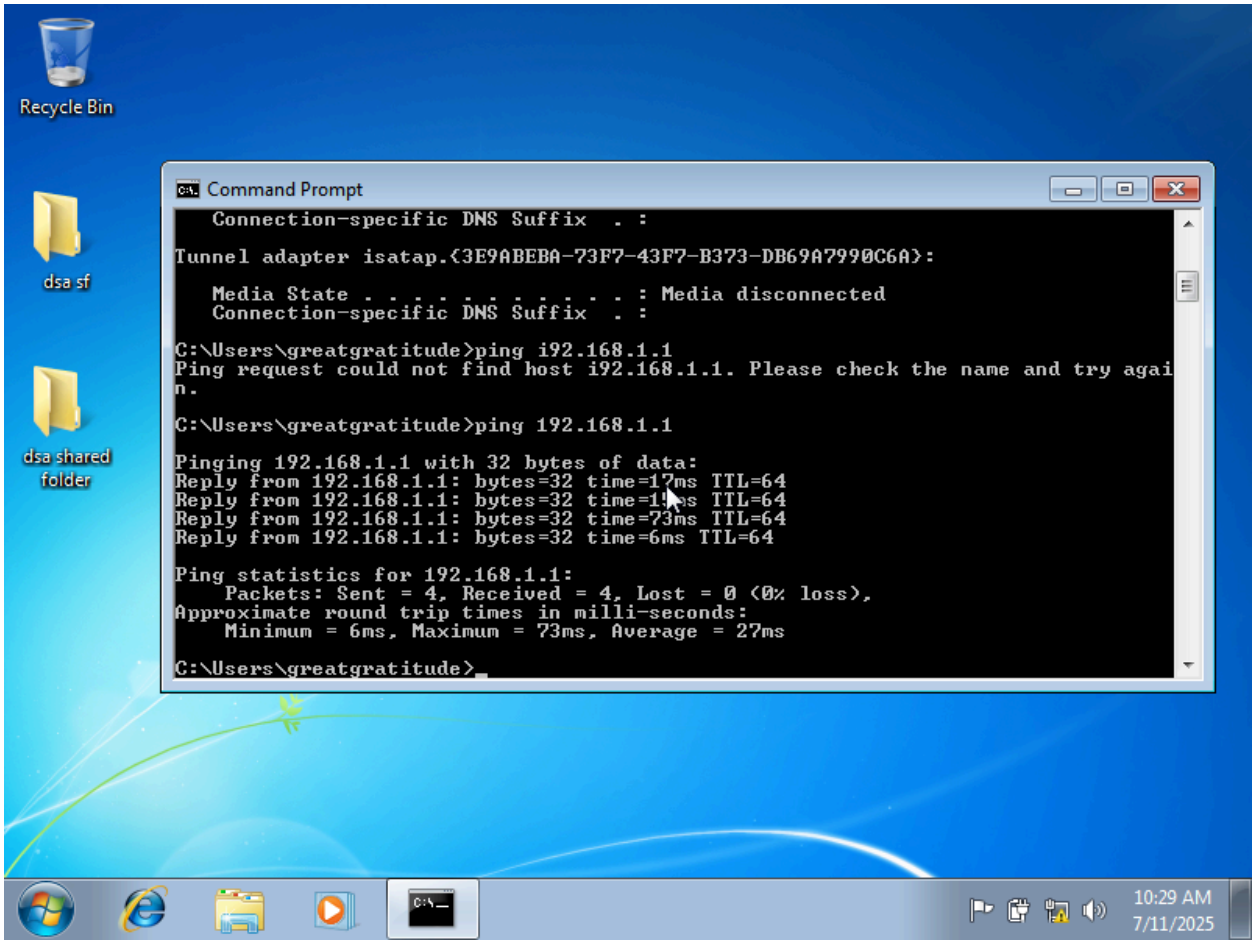
I also confirmed kali linux I discovered its having ip address 192.168.1.100. I decide not to adjust the ip address since it is in the same subnet with the virtual machines.



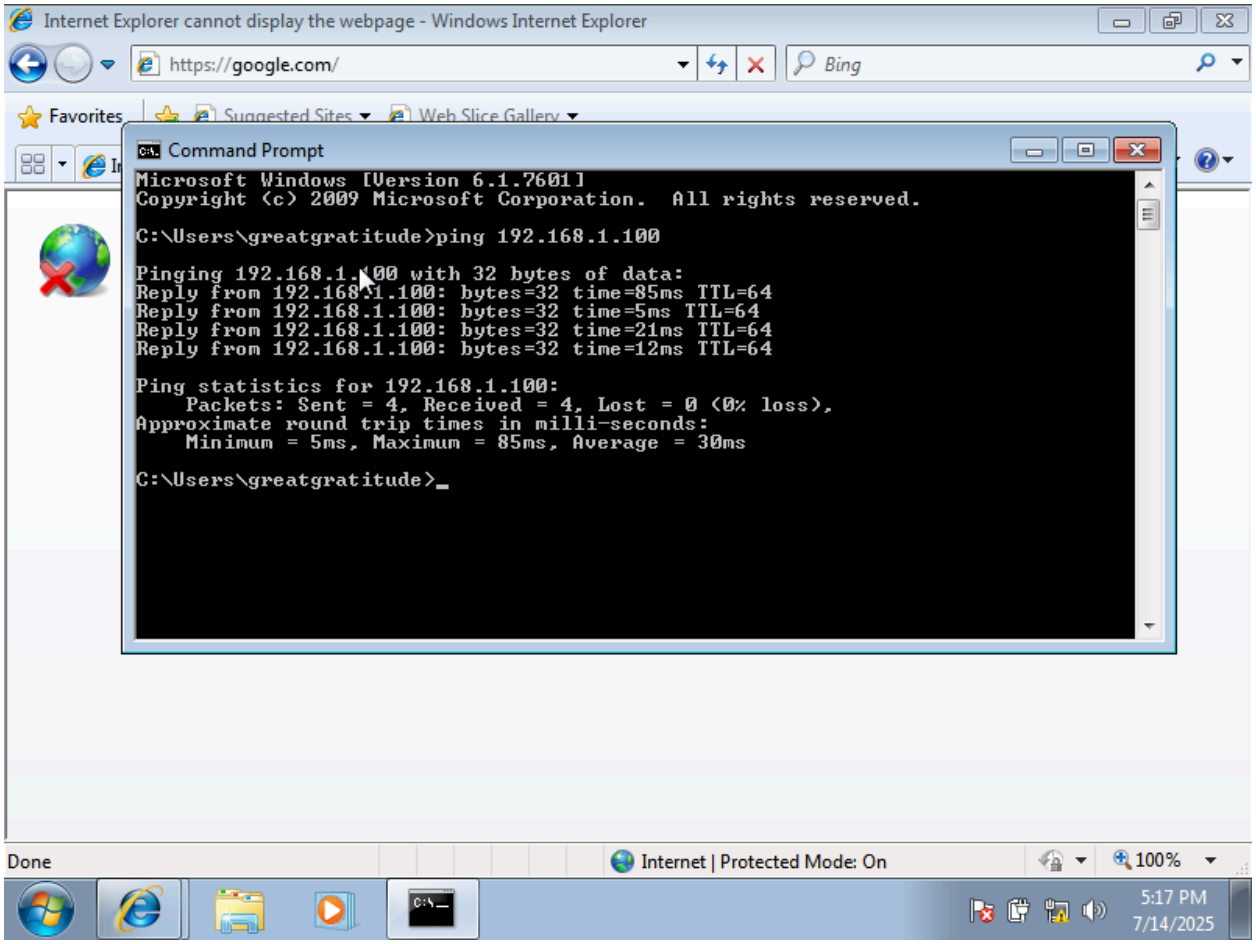
Then I started doing service enumeration through ping to know whether the two VMs can actually communicate to one another.



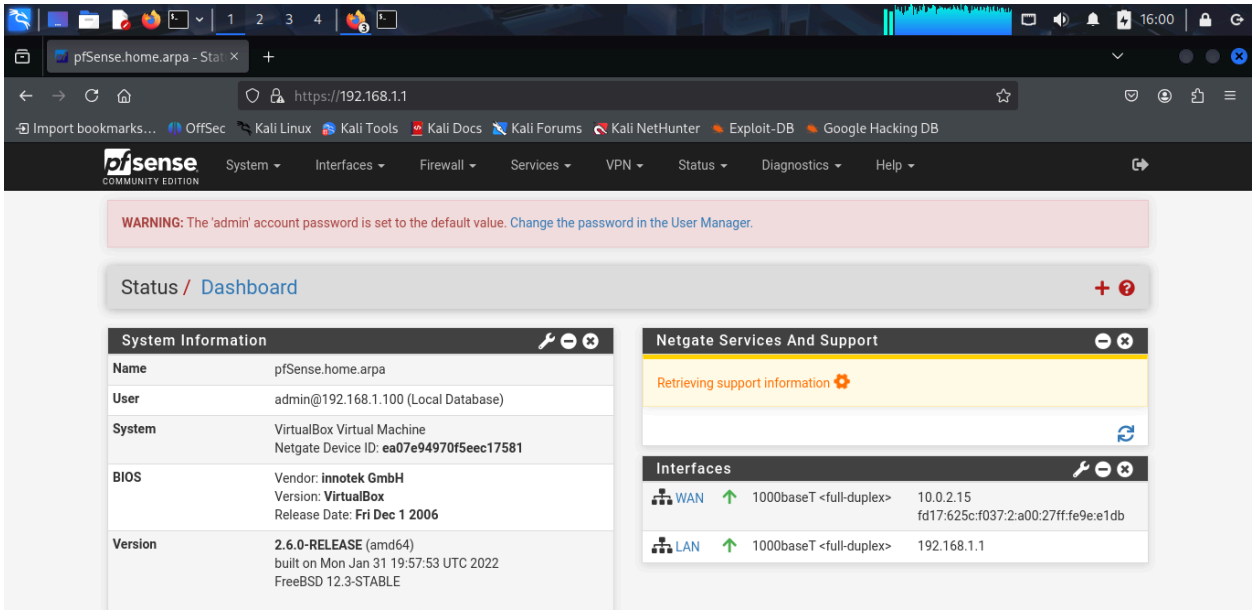
That was Kali Linux communicating with the pfSense through pining.

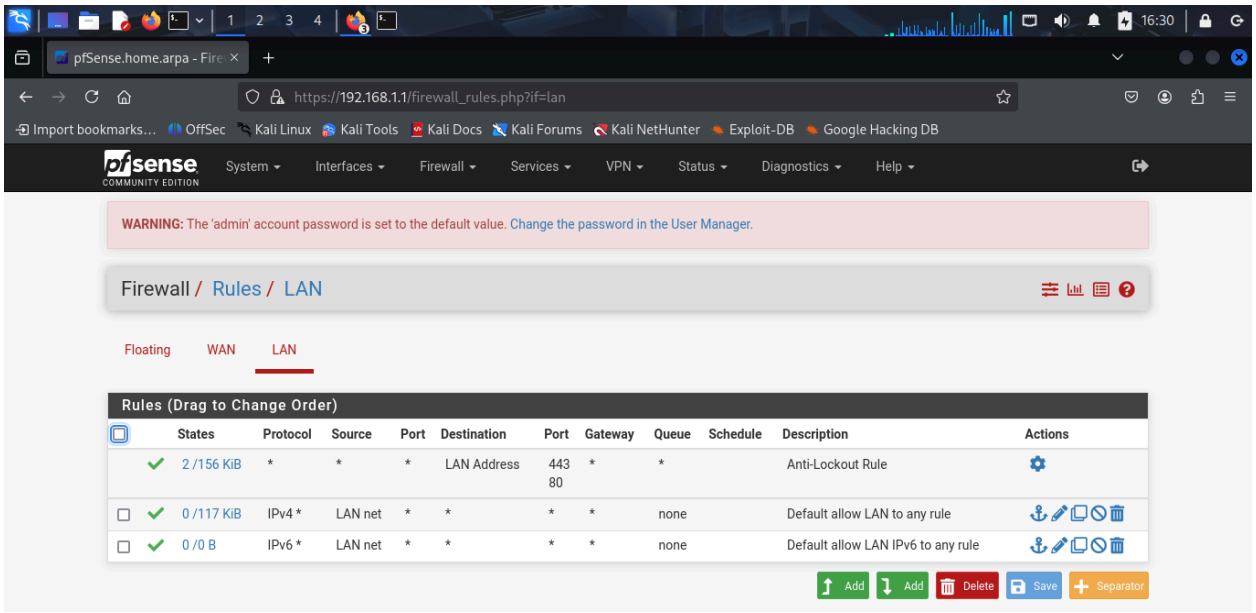


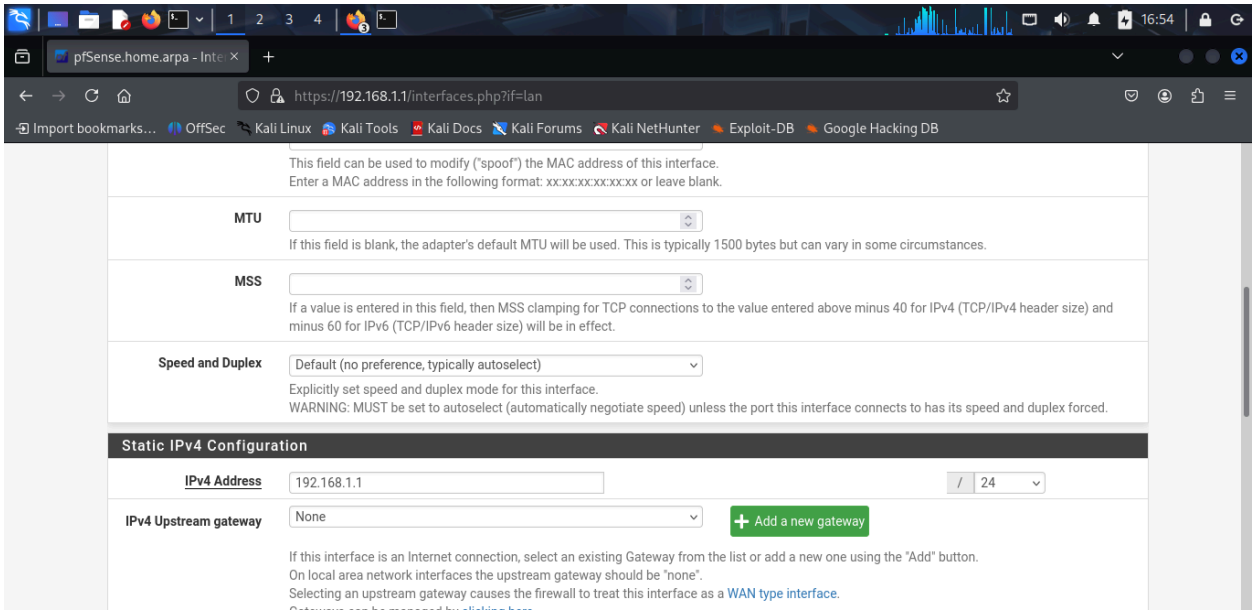
That was window 7 vm communicating with the pfSense through pinging.



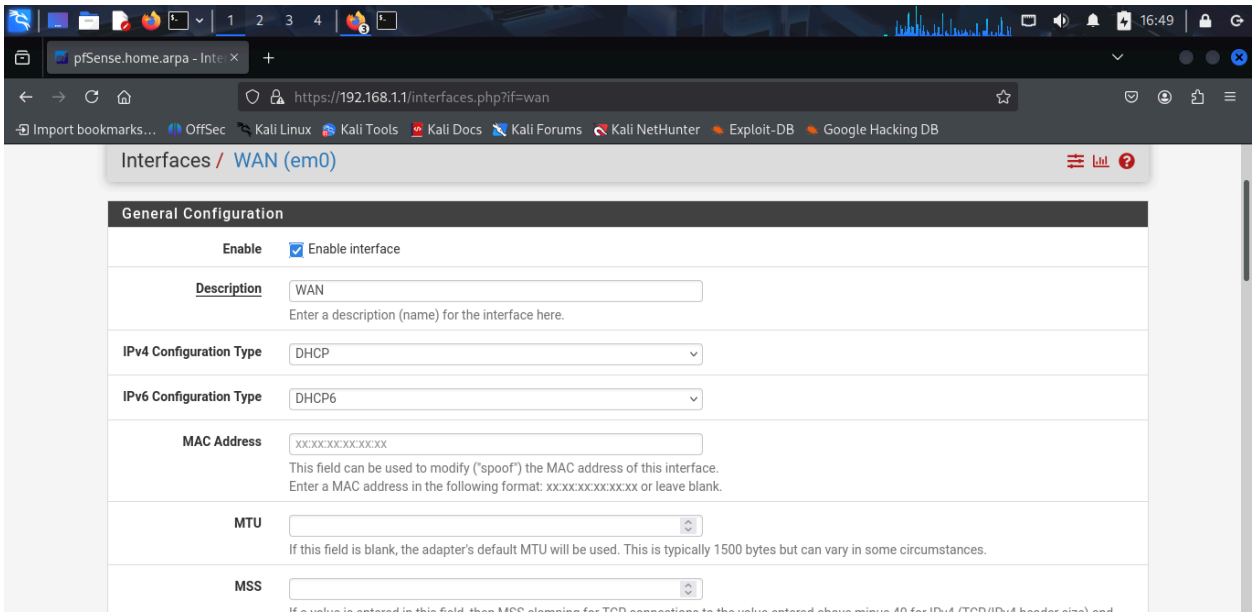
That was window 7 vm communicating with the kali linux through pinging.
The next thing to do now is to set up firewall rule for the VMs. To achieve this, we need to gain entrance into the pfSense site. I started my kali linux and went to its firefox. On the browser i typed https://192.168.1.1(pfSense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


pfSense.home.arpa - Stat
https://192.168.1.1
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Status / Dashboard
System Information
Name pfSense.home.arpa
User admin@192.168.1.100 (Local Database)
System VirtualBox Virtual Machine
Netgate Device ID: ea07e94970f5eec17581
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
Netgate Services And Support
Retrieving support information
Interfaces
WAN 1000baseT <full-duplex> 10.0.2.15
fd17:625c:f037:2:a00:27ff:fe9e:e1db
LAN 1000baseT <full-duplex> 192.168.1.1

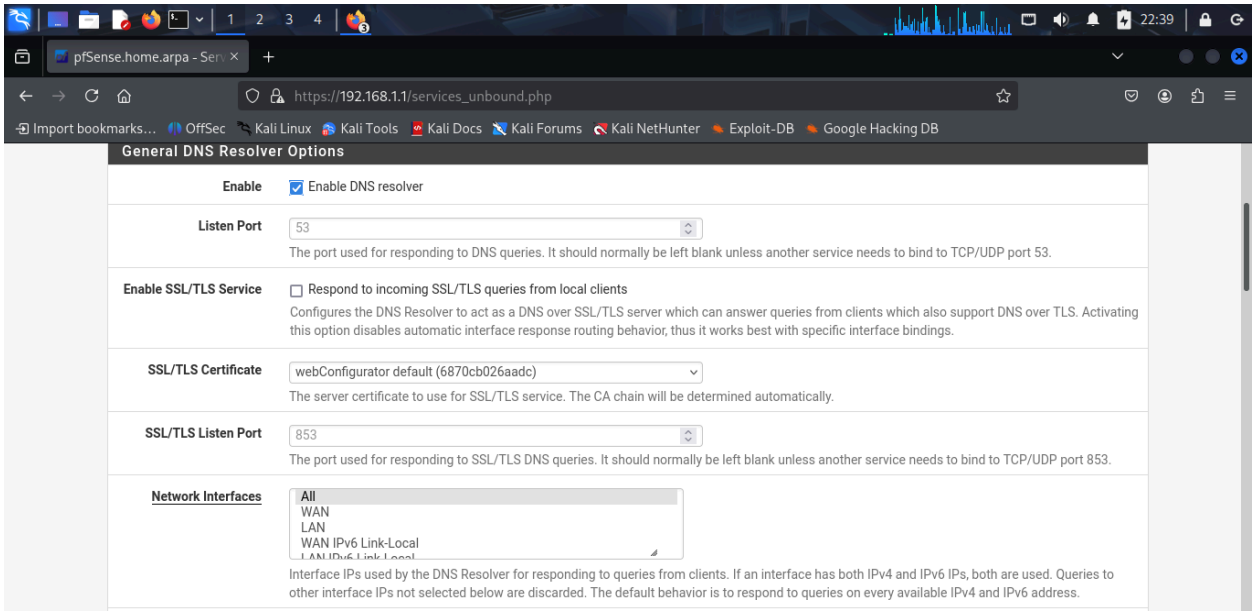

pfSense.home.arpa - Fire
https://192.168.1.1/firewall_rules.php?if=lan
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN
Floating WAN LAN
Rules (Drag to Change Order)
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
Add Add Delete Save Separator

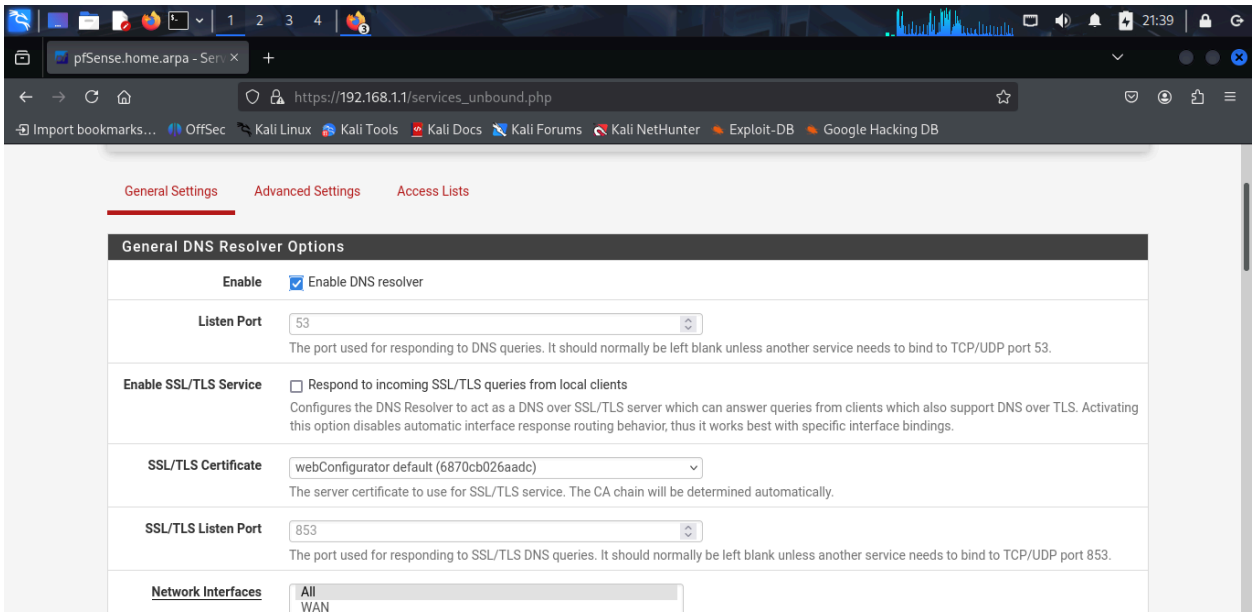


The last two screenshots are the LAN of the pfSense firewall.

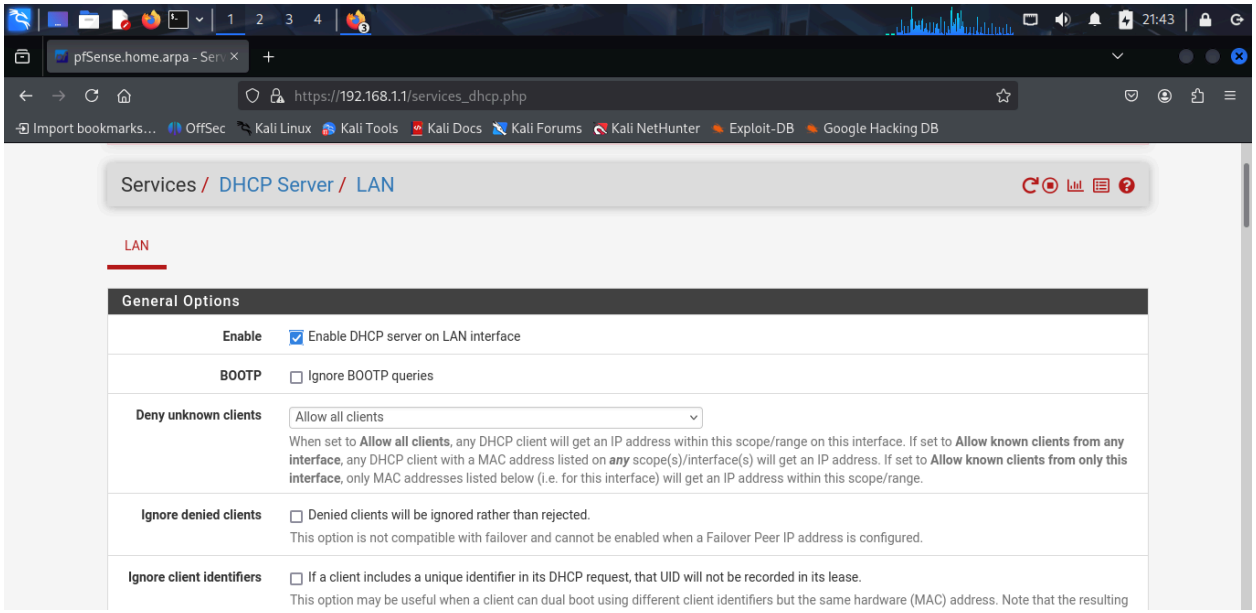


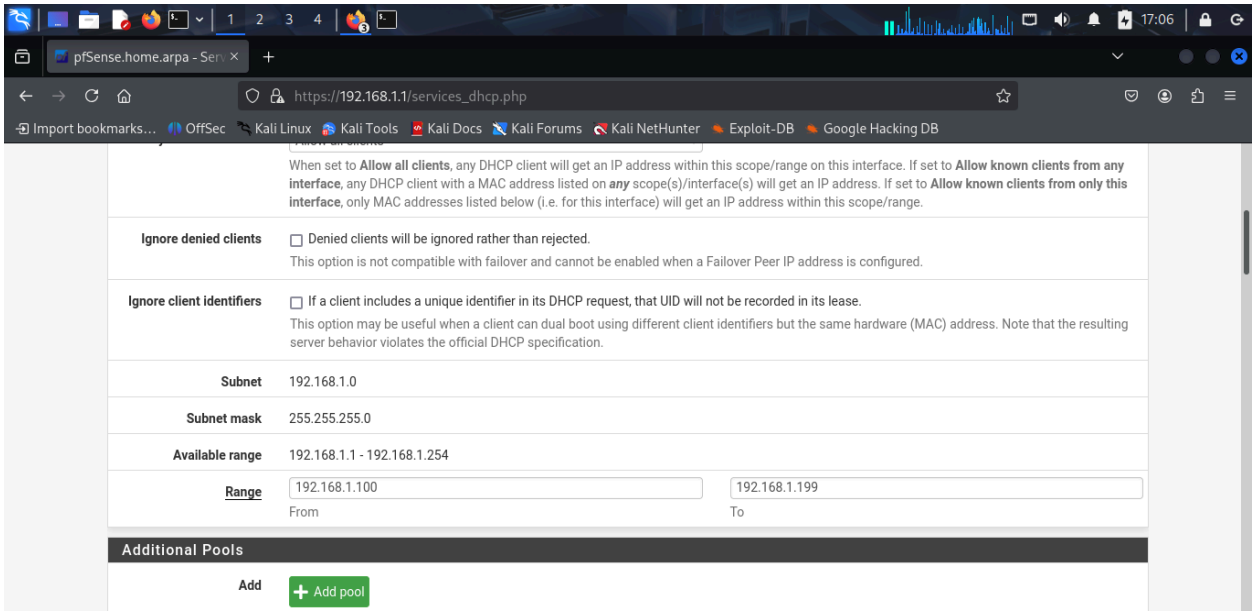
The above is the WAN interface.



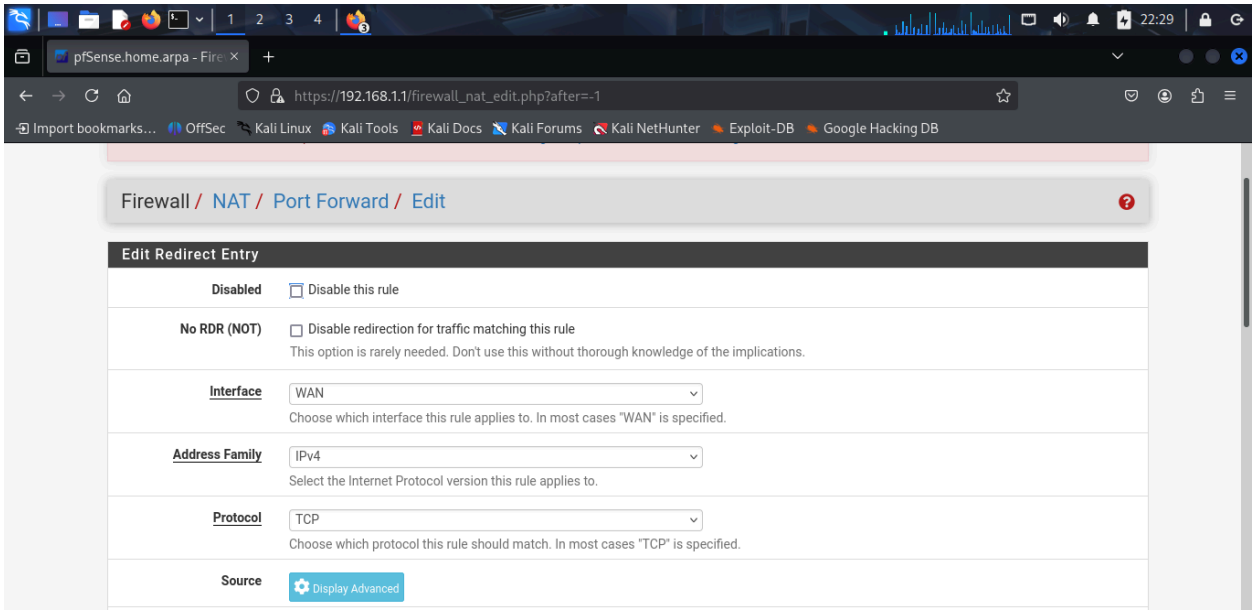


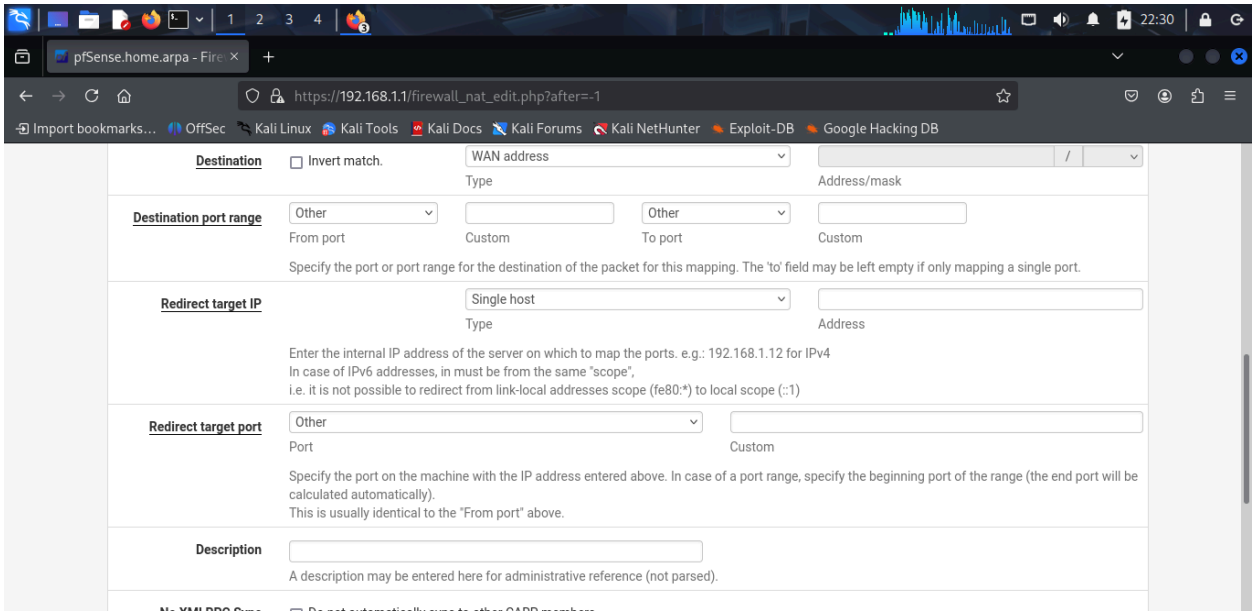
The above is the DNS interface on the pfSense firewall





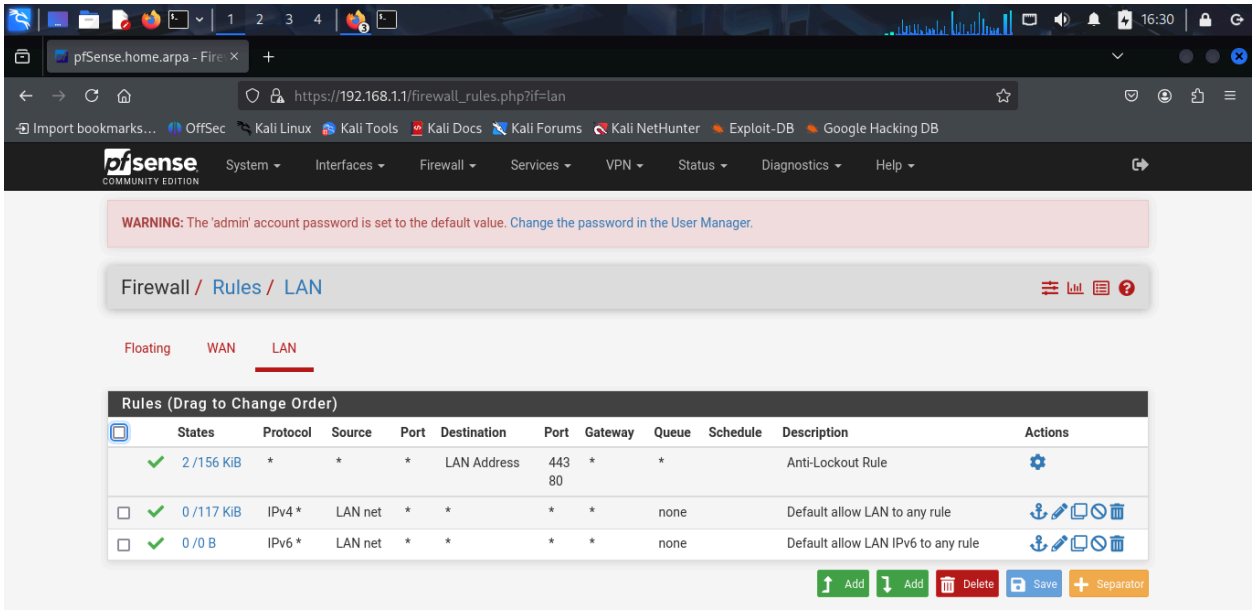
The above shows the DHCP LAN interface on the pfSense firewall.



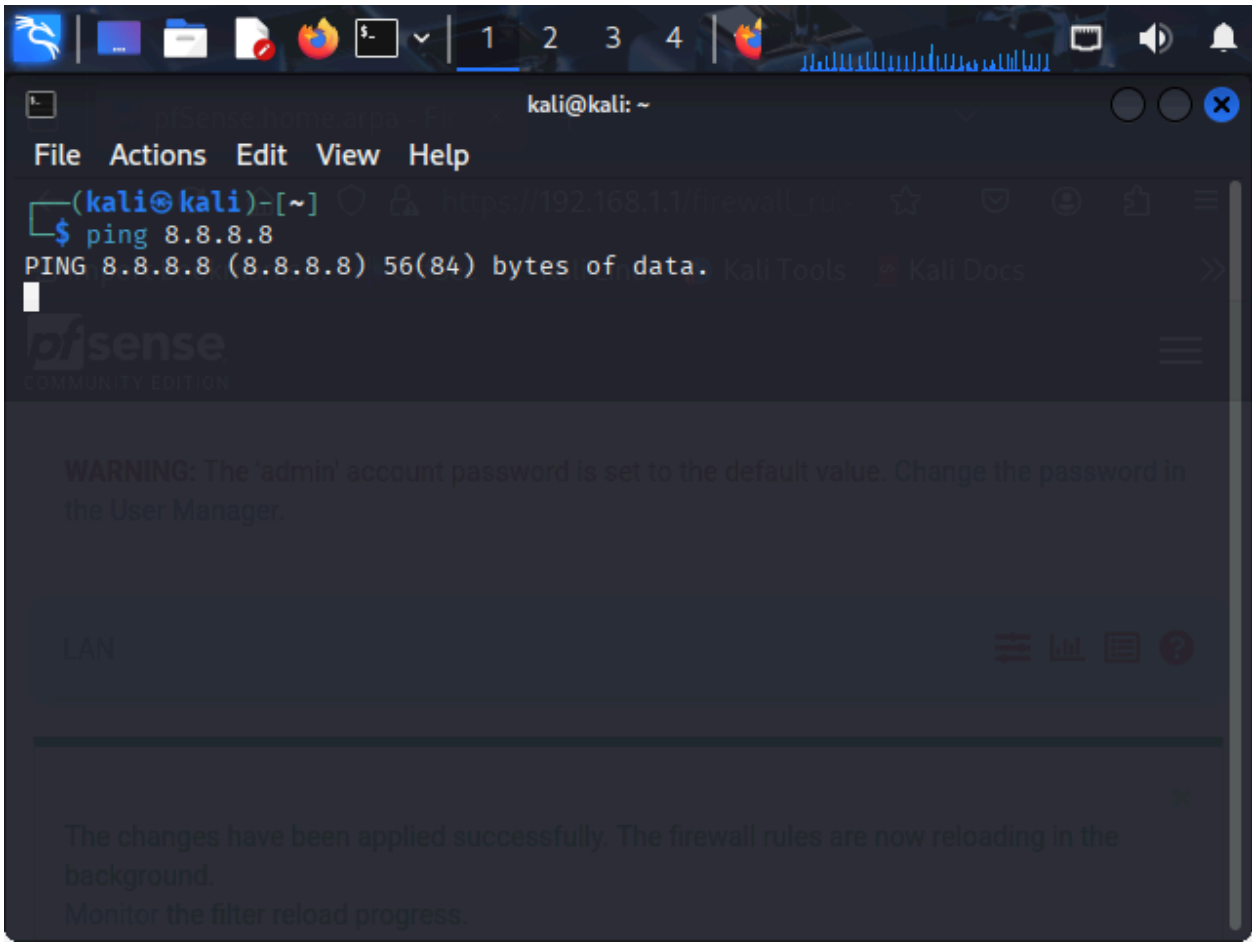


The NAT interface.

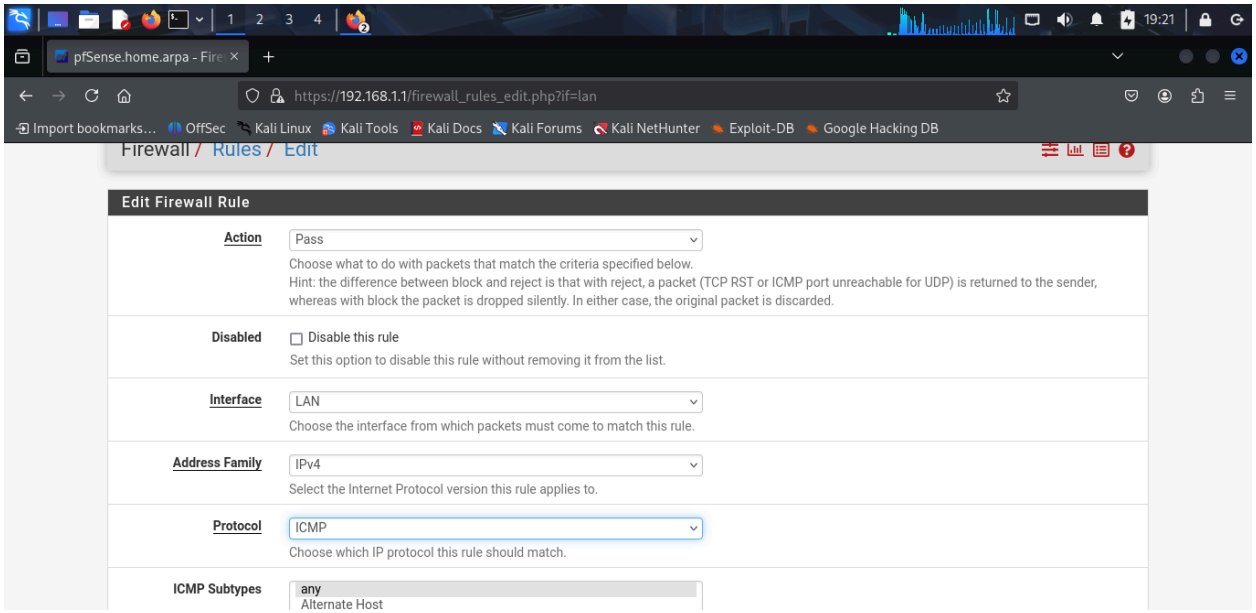
Now to set a firewall rule for the two VMs(kali and window7), I selected the LAN and blocked the default firewall rule set already

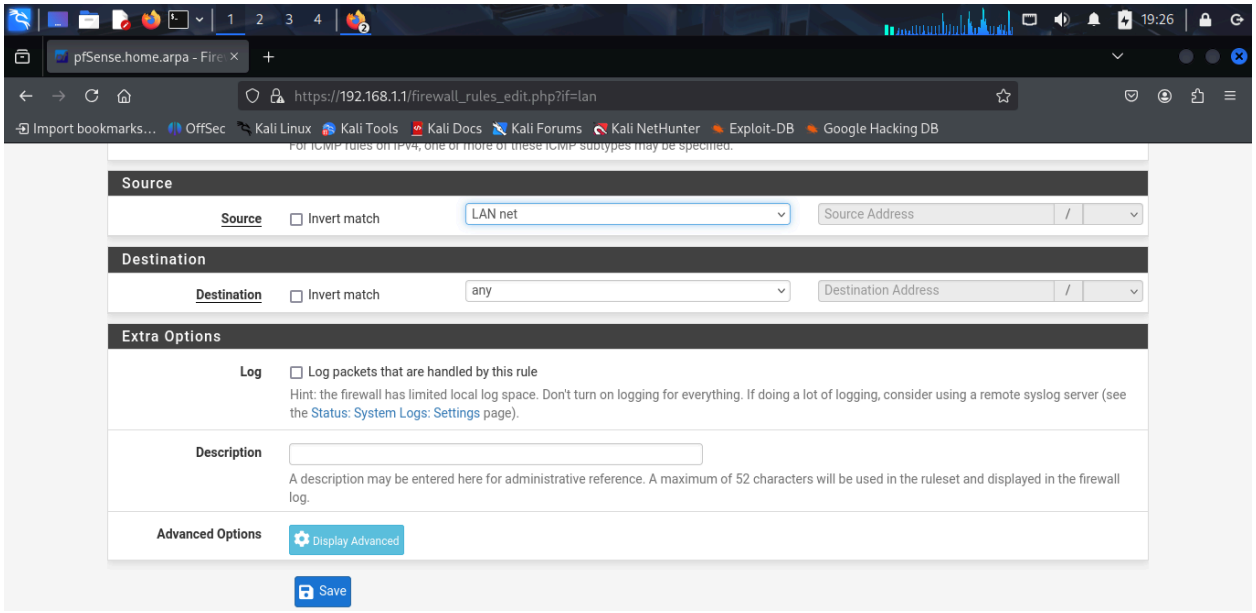


I had to block the default rules for ipv4 and ipv6. When I did that, I discovered that I could no longer access the DNS server, I could no longer browse again.

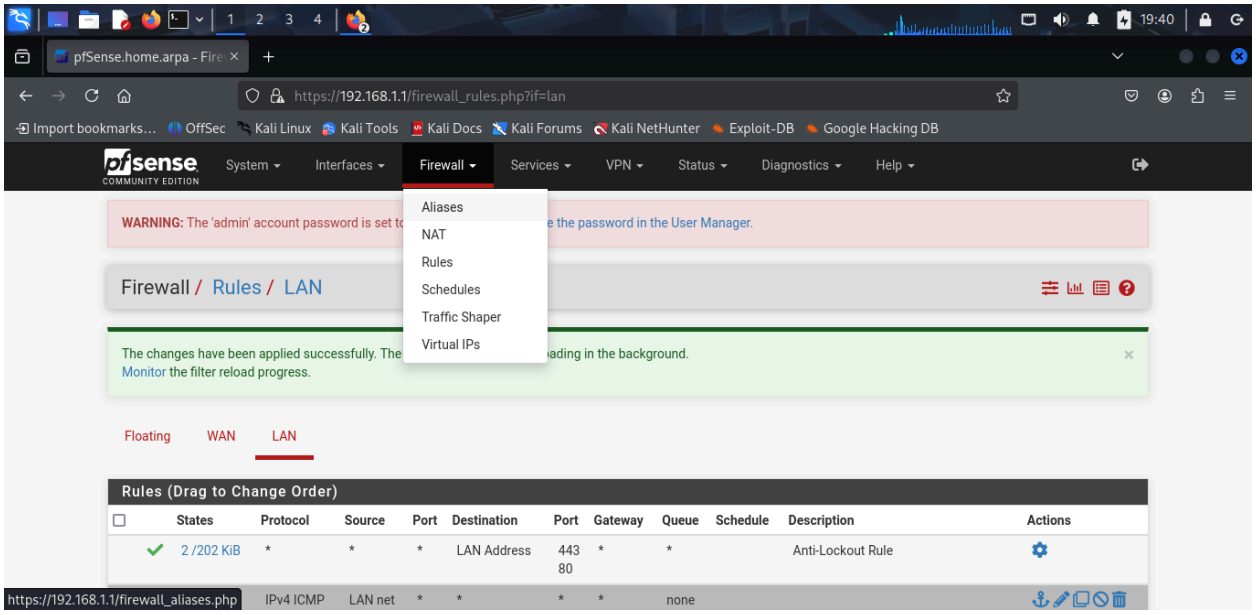


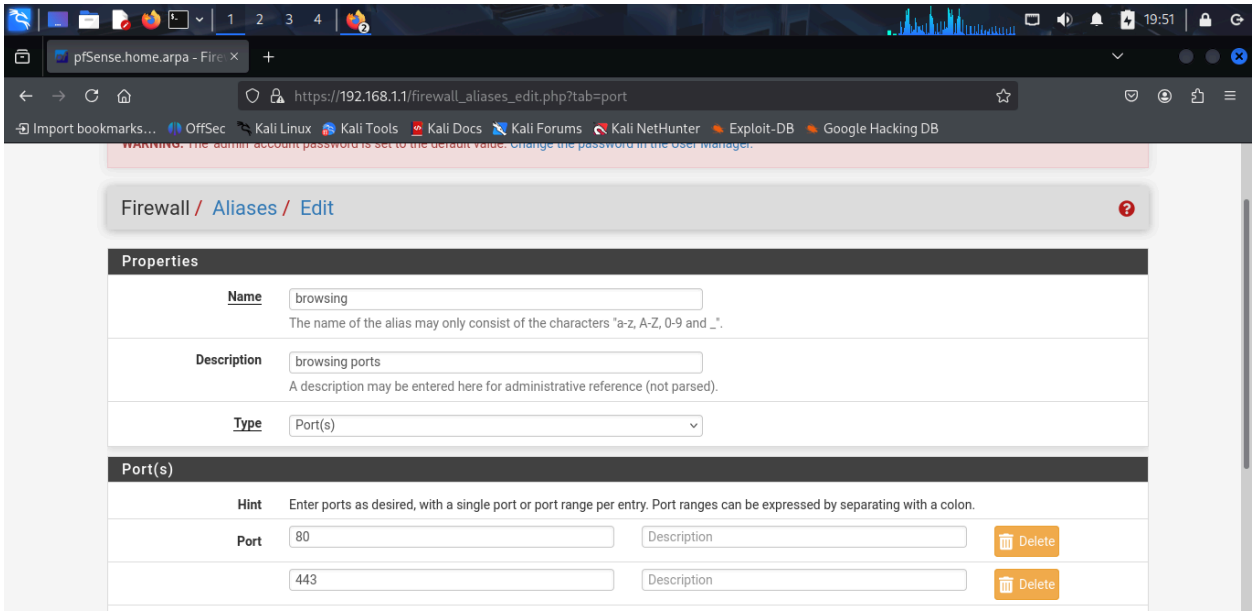
The above means that I could no longer browse again after blocking the default firewall rule. What I did next was to set another firewall rule that will allow for pinging and for browsing.

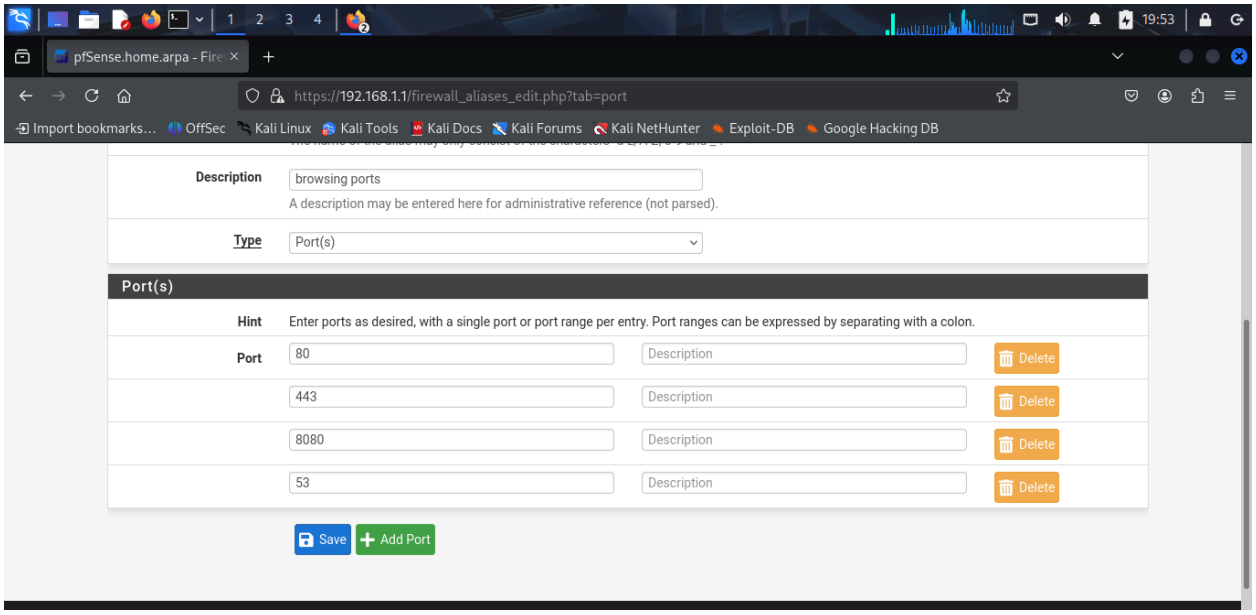




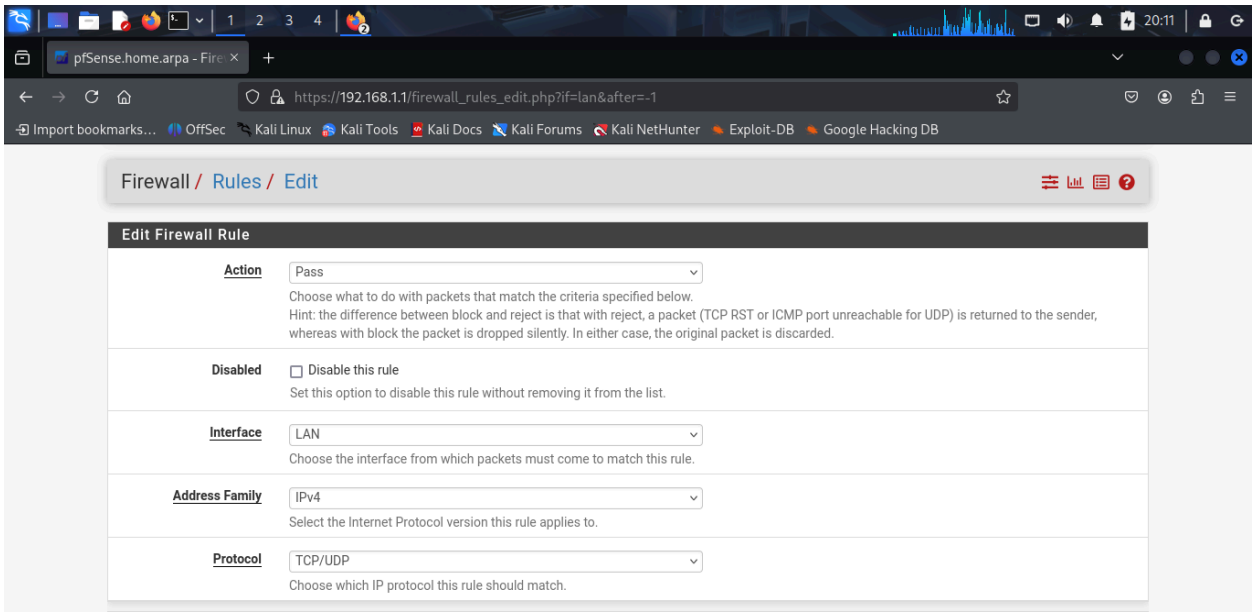
After setting this rule I could not still ping DNS server nor browse. I then decided to set firewall rule for ports:

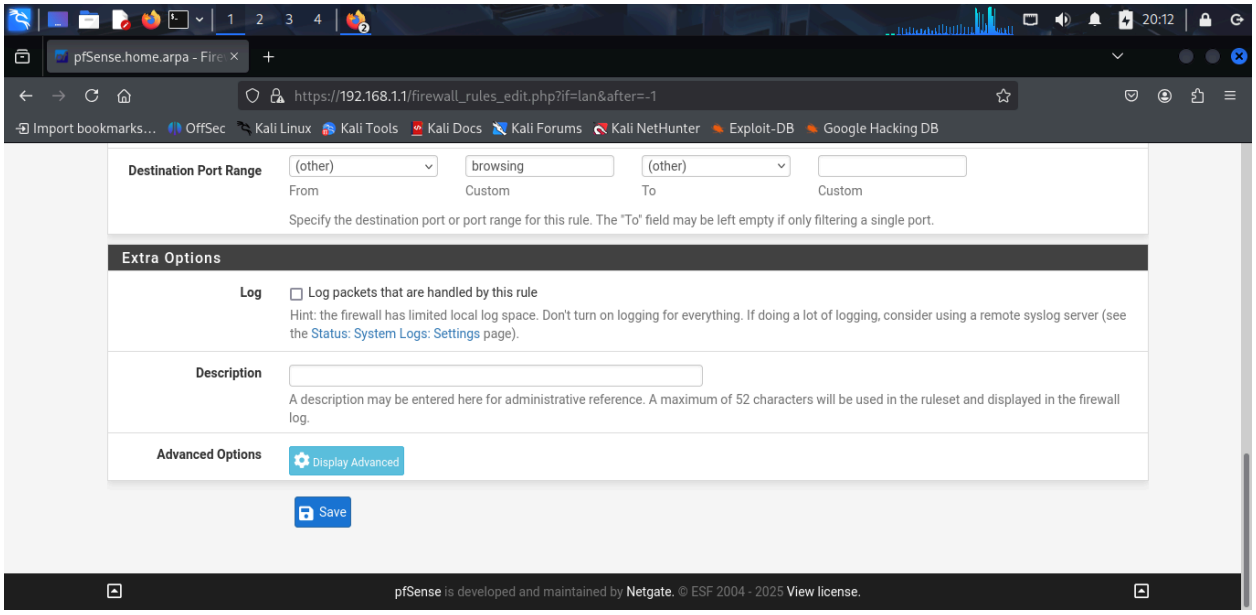

pfSense.home.arpa - Fire
https://192.168.1.1/firewall_rules.php?if=lan
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
WARNING: The 'admin' account password is set to
e the password in the User Manager.
Firewall / Rules / LAN
The changes have been applied successfully. The
ading in the background.
Monitor the filter reload progress.
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
2 /202 KiB * * * LAN Address 443 80 * * Anti-Lockout Rule
https://192.168.1.1/firewall_aliases.php
IPv4 ICMP LAN net * * * * none


pfSense.home.arpa - Fire
https://192.168.1.1/firewall_aliases_edit.php?tab=port
Import bookmarks... OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Firewall / Aliases / Edit
Properties
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)
Port(s)
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
Delete
443
Description
Delete

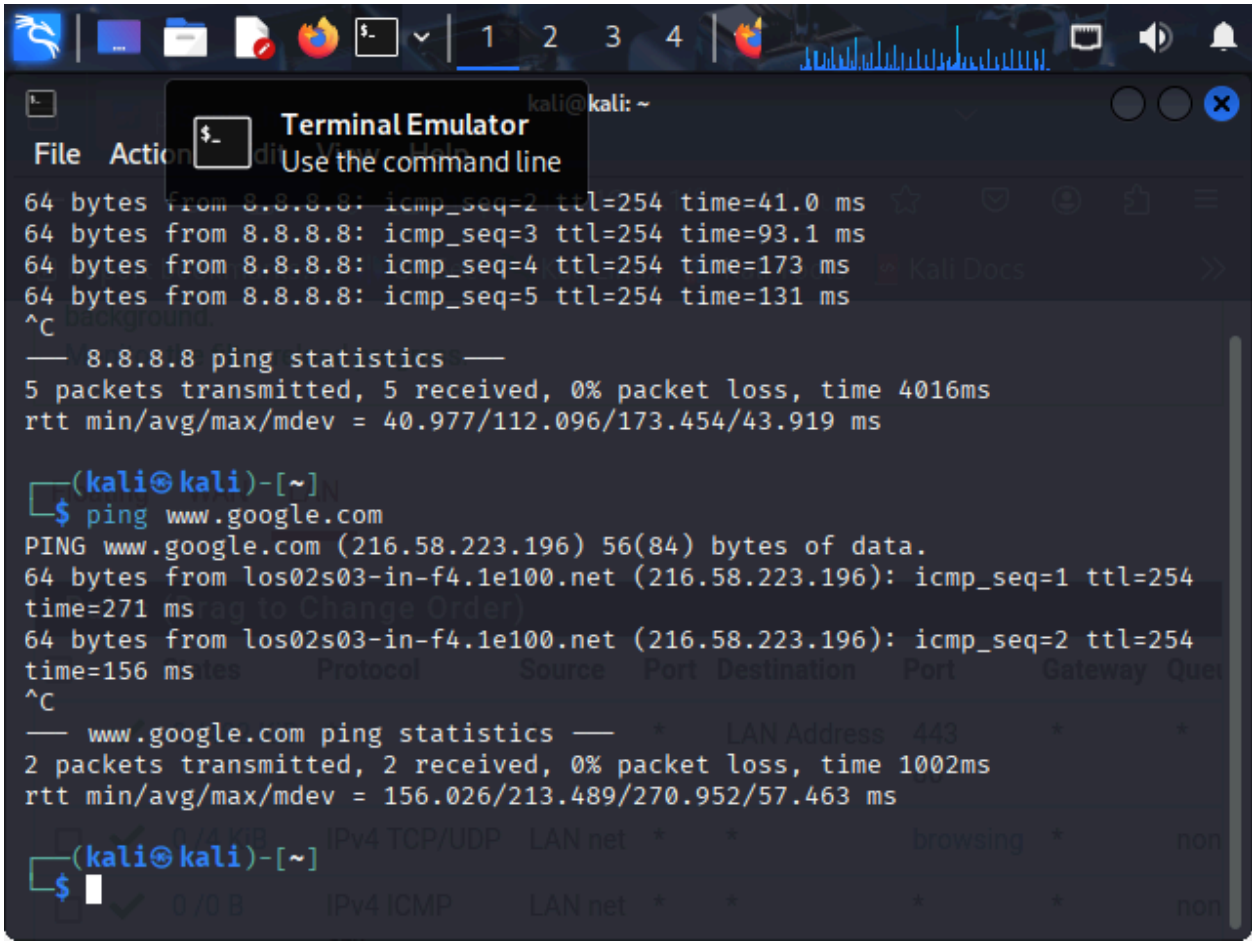


From the above screenshots, I allow port 80, 443, 8080 and 53 respectively. After setting the rule for port filtering, I went back to adjust the first rule that I made before the ports rule and I the the following adjustment:

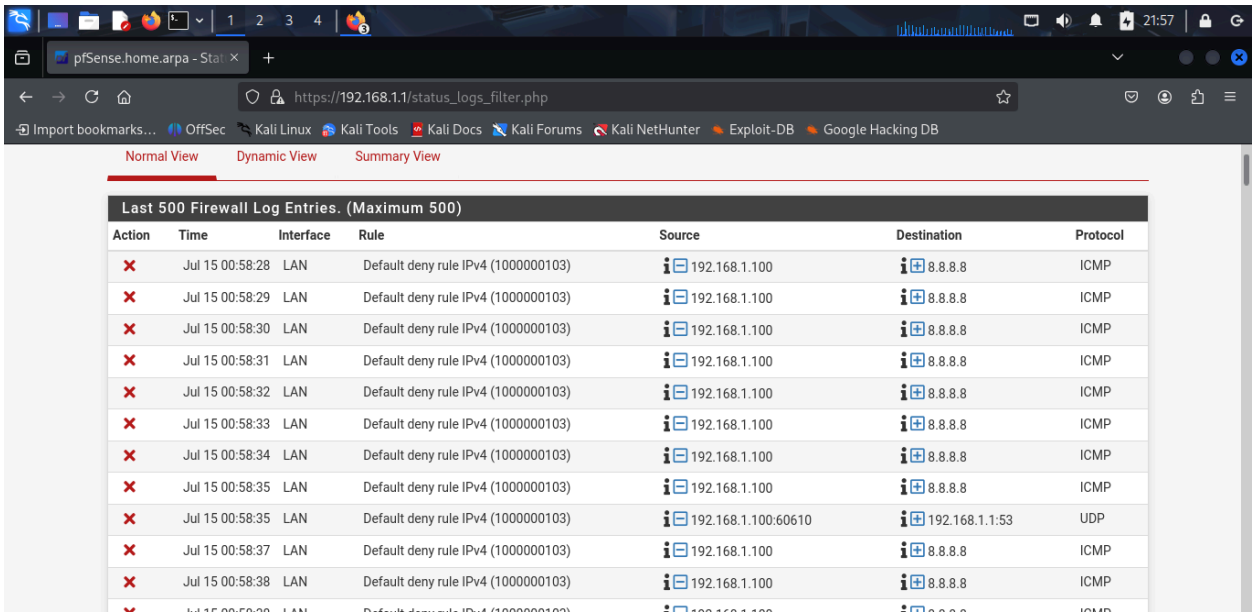




This time around I adjusted the rule by selected TCP/UDP on the protocol type unlike the ICMP I selected previously. I saved the rule and I tested it again.



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 and I discovered I could ping and browse again.
Now the two VMs have been connected to route traffic through the firewall.



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