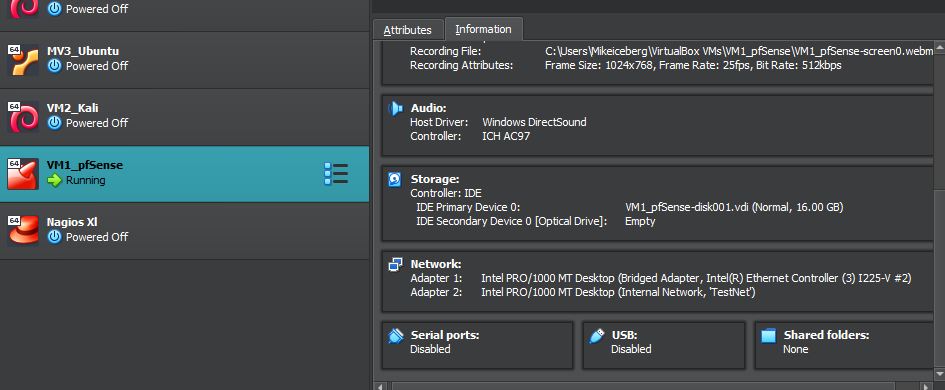
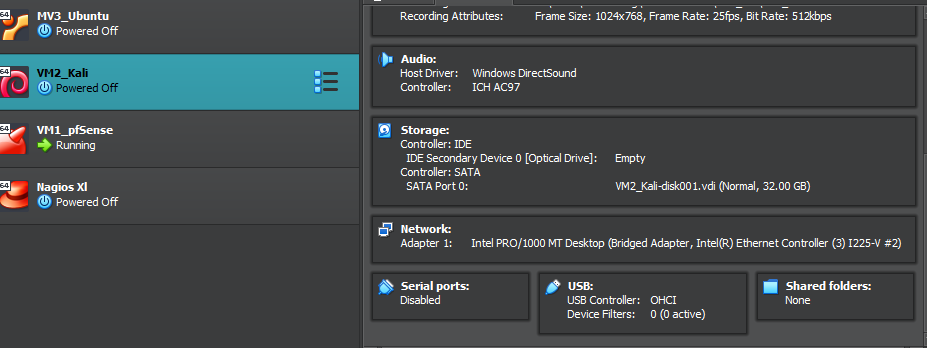
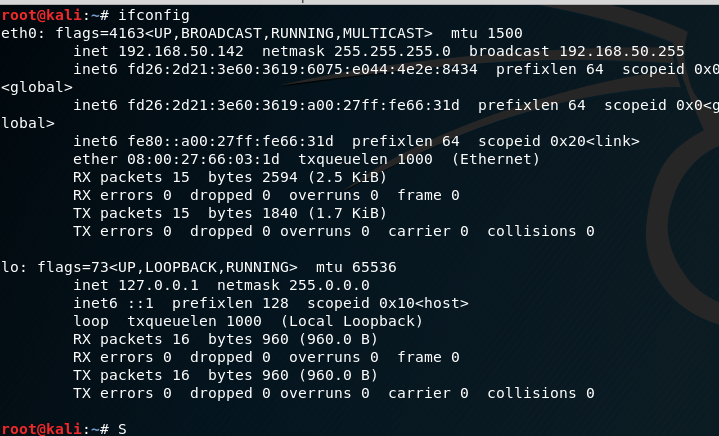
VM 1 PFsense firewall. Separates the Internet from the internal network. Has a WAN address and is from the same subnet as the physical host with a bridge adapter. For the LAN it acts like a DHCP and also runs Suricata In another lab.



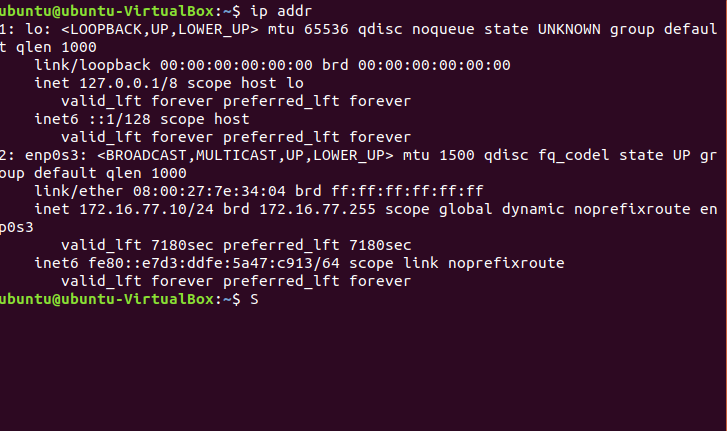
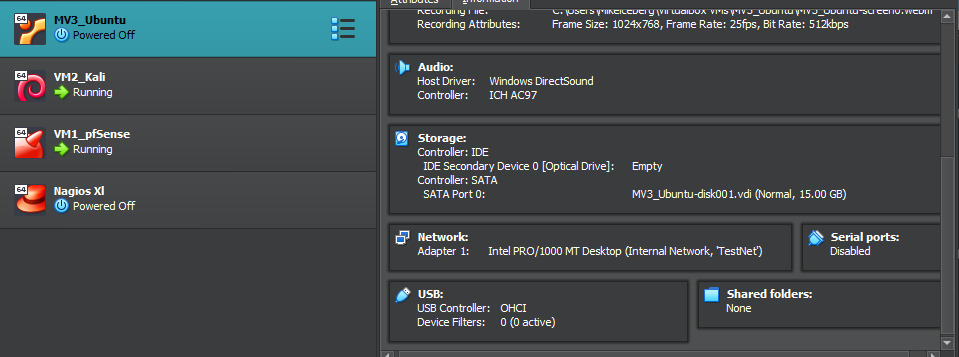


VM2 Kali linux machine to do testing later in the project. Bridged mode ethernet connection.

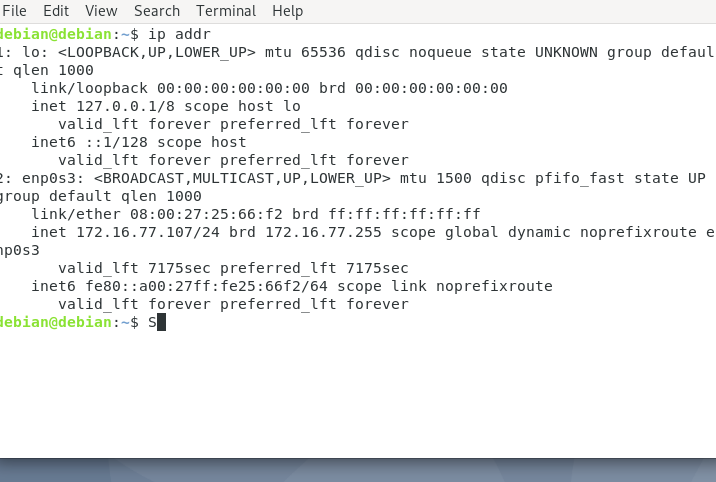
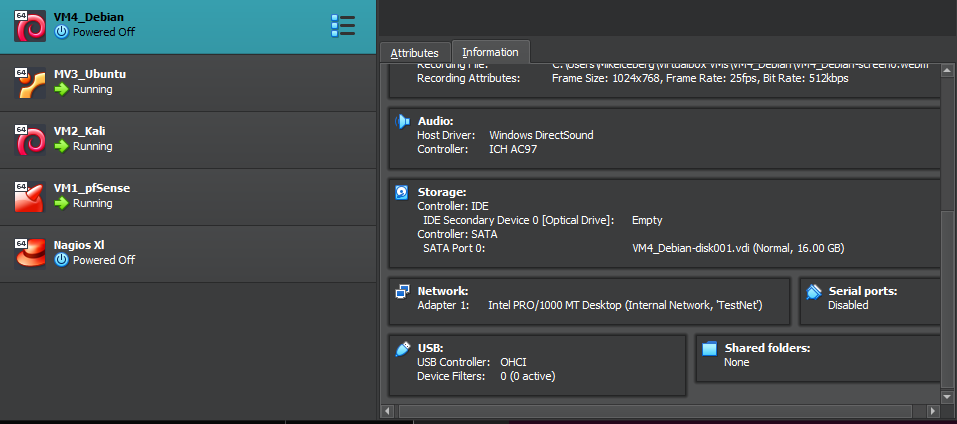




VM3 Ubuntu is representing the we server for the corporation.

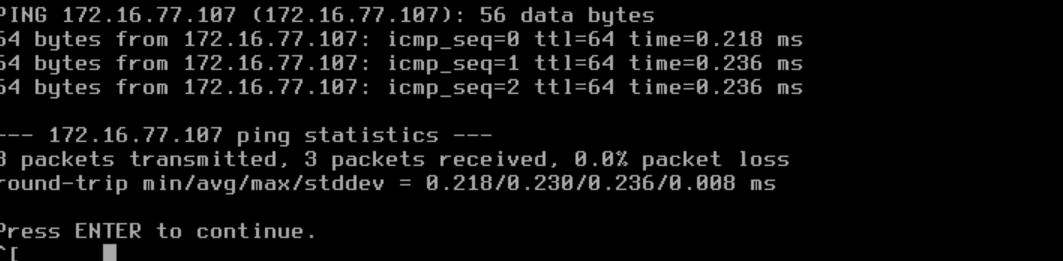


VM4 is the Debian machine and is used for remote access testing and also the DHCP client in the internal network.

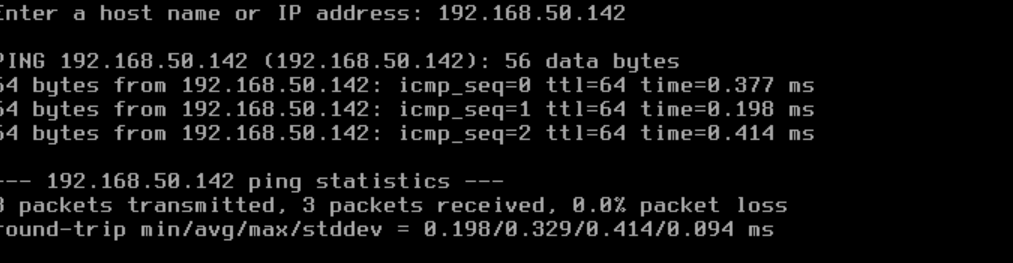


1st scenario.

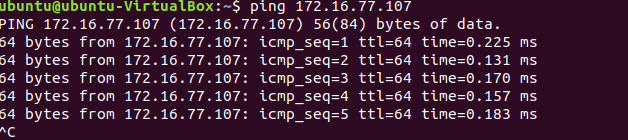
pfSense machine pinging internet subnet and external subnet machines.

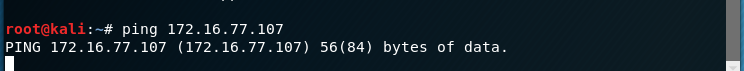
Internal subnet UBUNTU

External subnet KALI

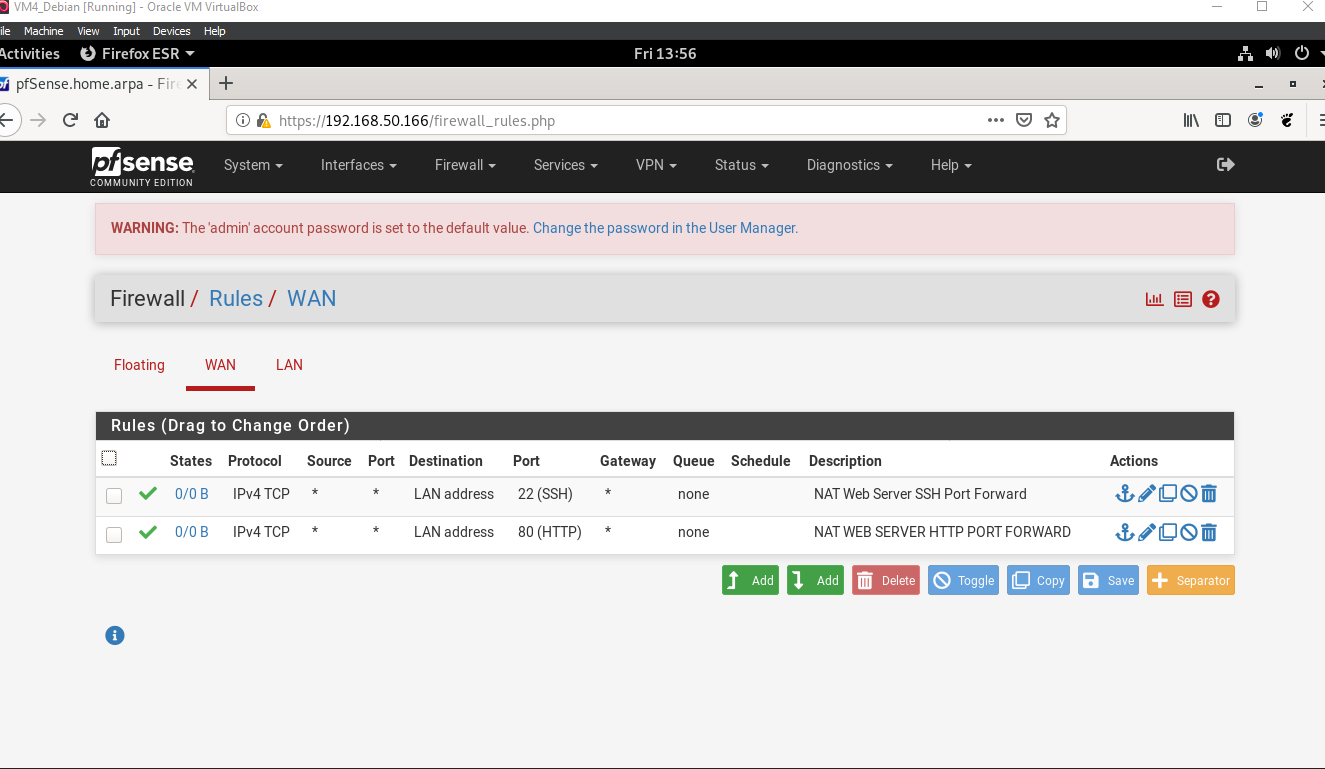
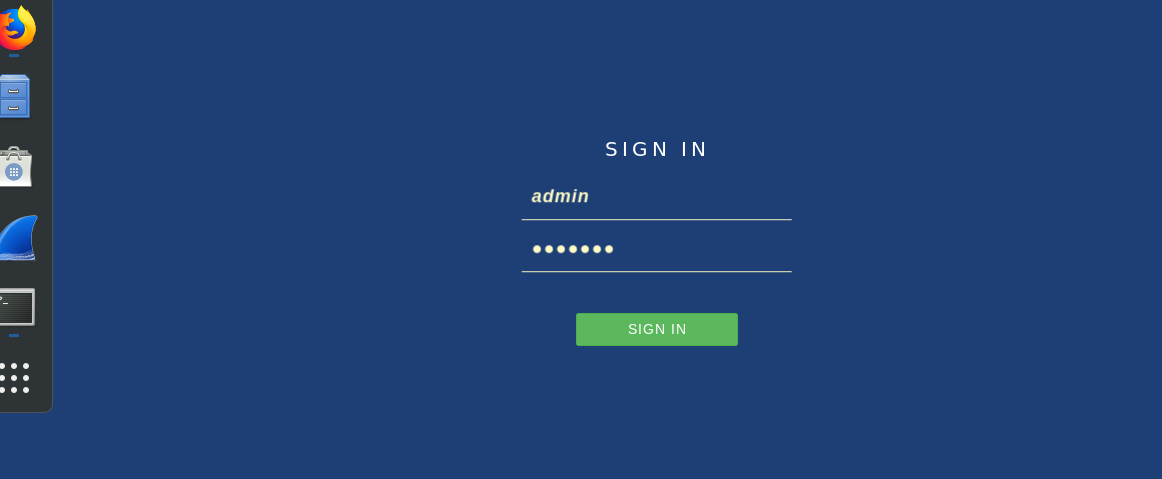


Can ping everything in internal network. Ubuntu to Debian and vice versa

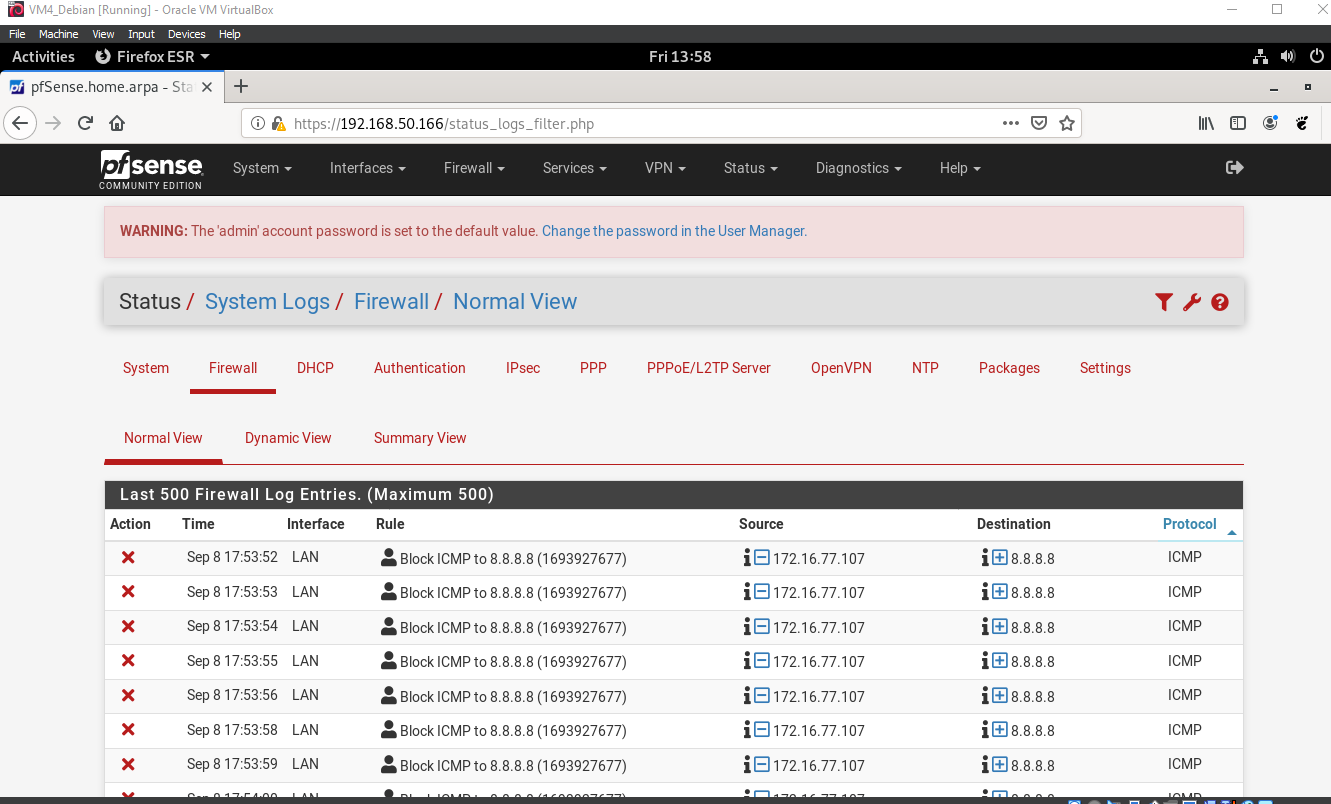
Kali cannot ping anything in the internal subnet but the host



Task 1: Trying to show that ICMP traffic is allowed in the internal network. I don’t have the screen shots because I already completed the project with the pfsense firewall enabled. I do have steps I took to turn on the firewall and implement firewall rules to not ping 8.8.8.8 (outside the network)

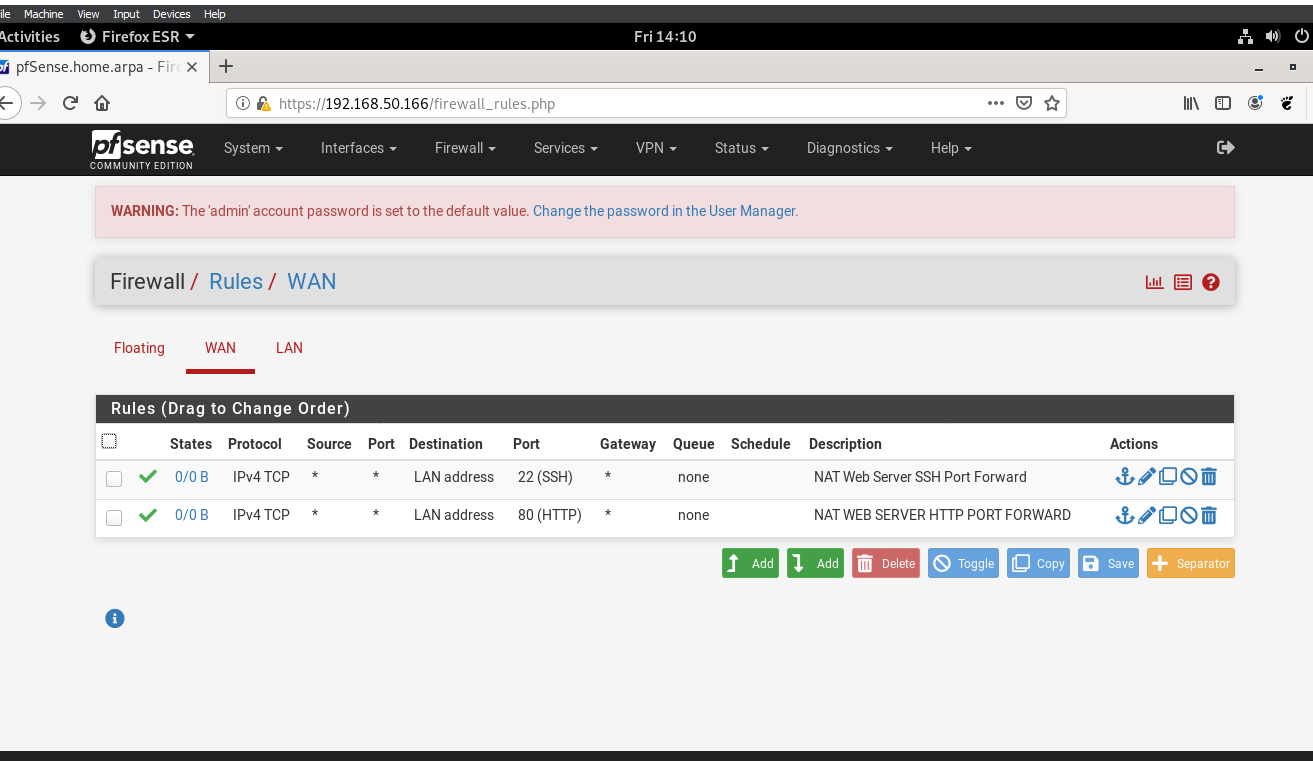
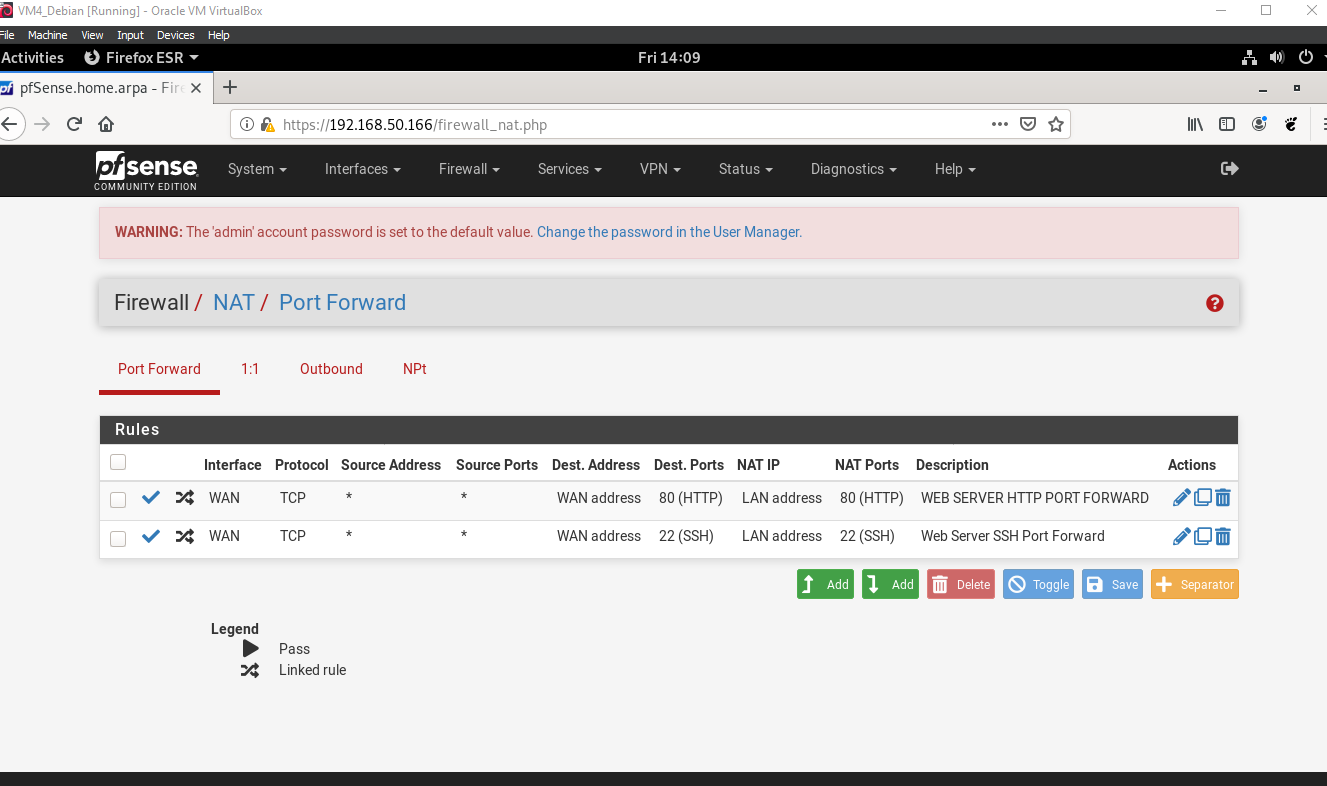


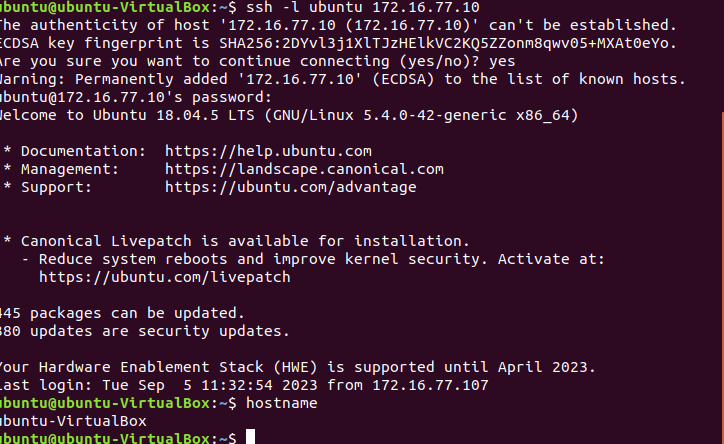
Proof that firewall rules were successful for Project Task 1



Project Task 2 : Setting up remote access

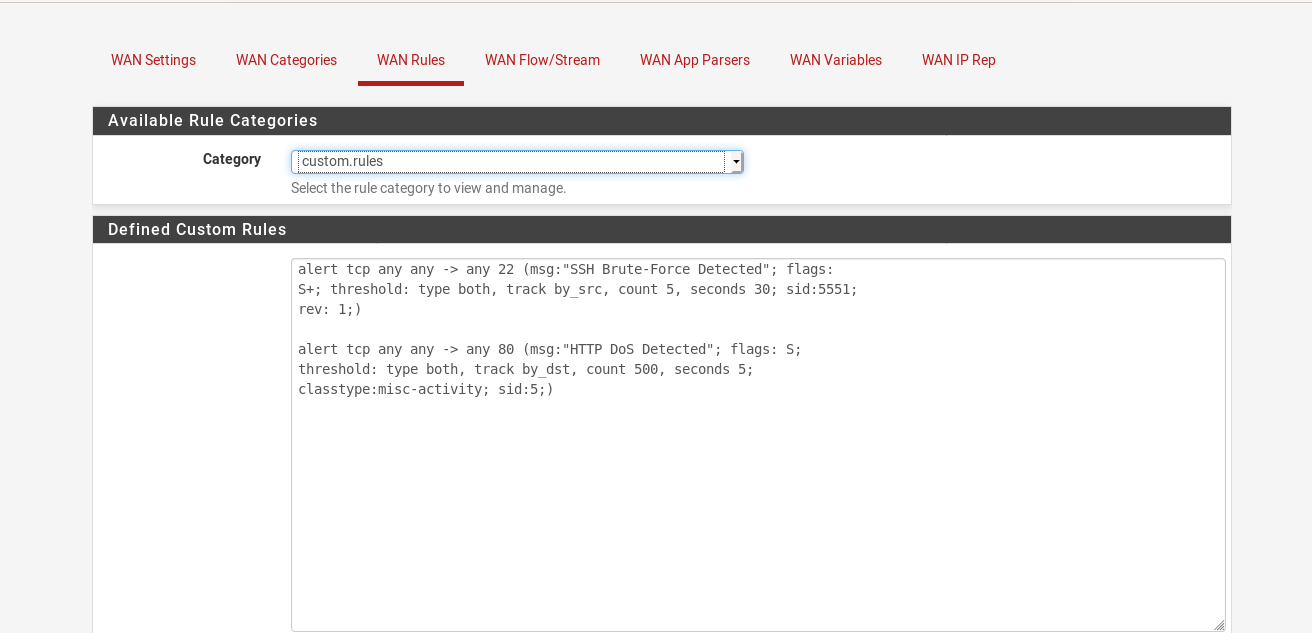
1. Web server can be accessed through Debian VM ( on the same network).
2. I can connect to Ubuntu VM SSH service from Debian VM.
3. 3) Two Nat port forwarding rules were created in pfSense to translate requests to the web server.



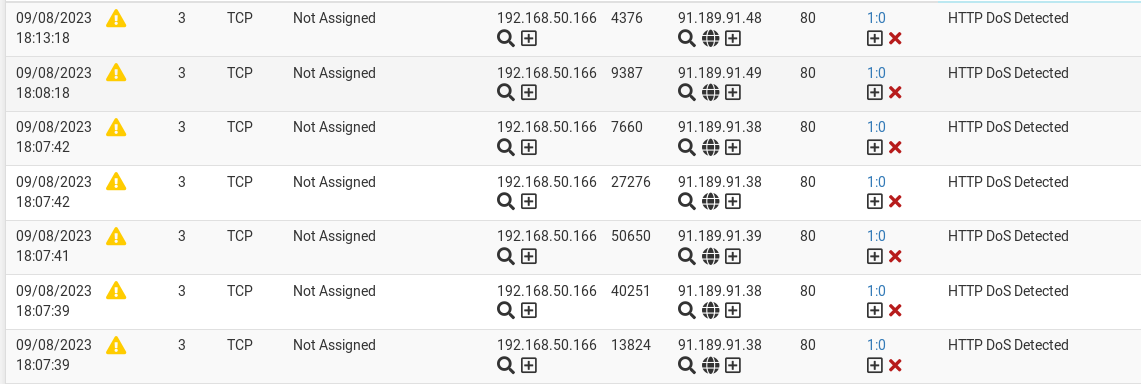
Evidence that multiple systems were able to access both web server and SSH service via pfSense WAN address. 

Task 3: All seeing EYE

1. Added a configuration for Suricata in the pfsense WAN interface with custom rules to detect abnormal traffic.
2. alert tcp any any -> any 22 (msg:"SSH Brute-Force Detected"; flags: S+; threshold: type both, track by\_src, count 5, seconds 30; sid:5551; rev: 1;) alert tcp any any -> any 80 (msg:"HTTP DoS Detected"; flags: S; threshold: type both, track by\_dst, count 500, seconds 5; classtype:misc-activity; sid:5;)



1. Executed the brute force attack and ddos attack. Don’t have the screenshots of the attacks through Kali but have the log evidence.



I couldn’t get the brute force log to show for some reason but this is the result. Im just curious if it was rename differently but I definitely hit the server multiple times like it said in the lab.

