**IT 620 – Wireless Network Security & Administration**

**Mentored by:** Prof. Stanley Senesy

**Project Title: CONFIGURATION OF FIREWALL**

**Submitted by:** VENKATA JAYAPAVAN NARU (vn272)

CLASS: IT 620 001

In this project we will be using virtualization to implement a system that will have an external VM and internal VM connected through a firewall VM that consists of two NICS.

**Requirements:**

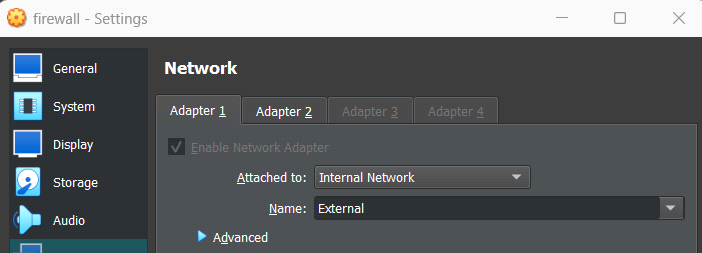
Virtualization hypervisor - Oracle VirtualBox 7.0.4

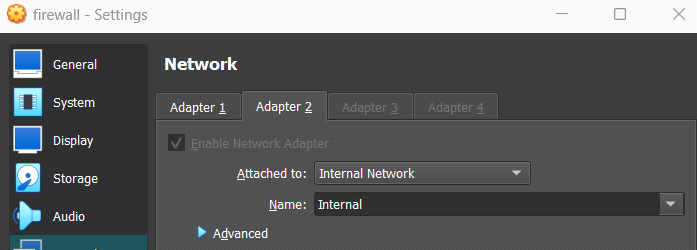
Open-source firewall - pfSense 2.6

Internal and external virtual machines - windows 2016 server.

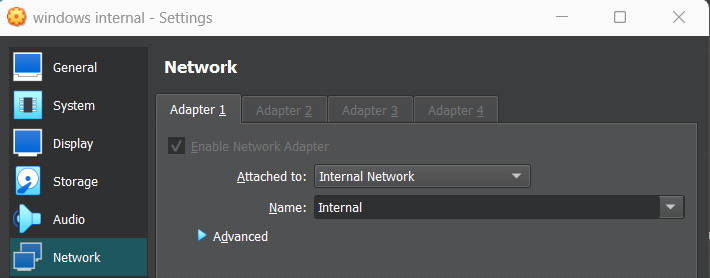
**Construction of machines:**

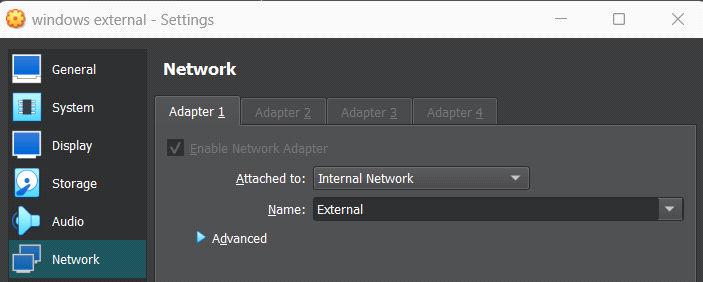
The pfsense firewall has 2 Network adapters that are set to internal network. We will give them 2 different names i.e.; one will be named as ‘Internal’ and the other is named as ‘External’





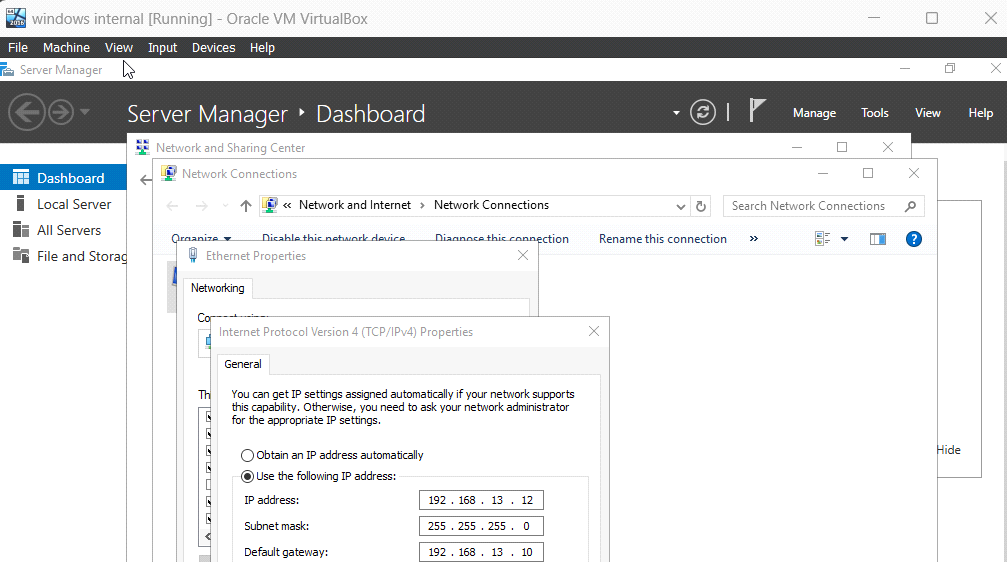
Both the windows server 2016 machines are attached to internal network. Since we have already given 2 names for adapter when we were setting up firewall. We can choose those names for the machines as well. So external machine will be set to ‘External’ and internal machine will be set to ‘Internal’.

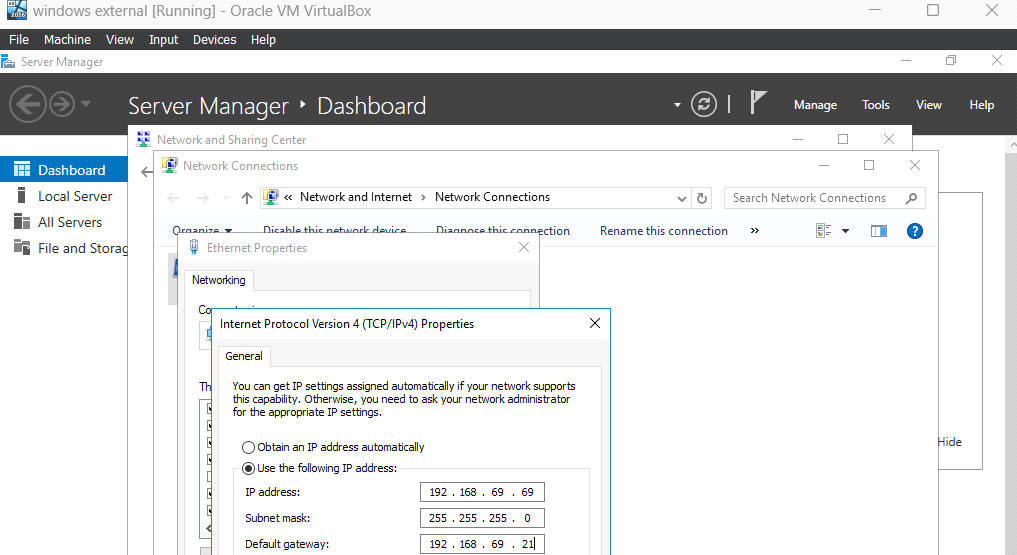




After we customize each virtual machine according to the host system specifications and importing the iso files, we can proceed and install the operating systems in the respective VMs.

In pfsense, since we attached 2 network adapters. we can only see IP address for LAN. We can set interface IP address for WAN and also change for LAN if we want. The addresses of WAN and LAN will be the gateway the IP address of External and Internal machine respectively. Next, we will configure both external and internal machines. By default, both the windows machines will be allocated with random IP and gateway addresses. We will be changing IP and gateway address of both machines to class C address as shown below.





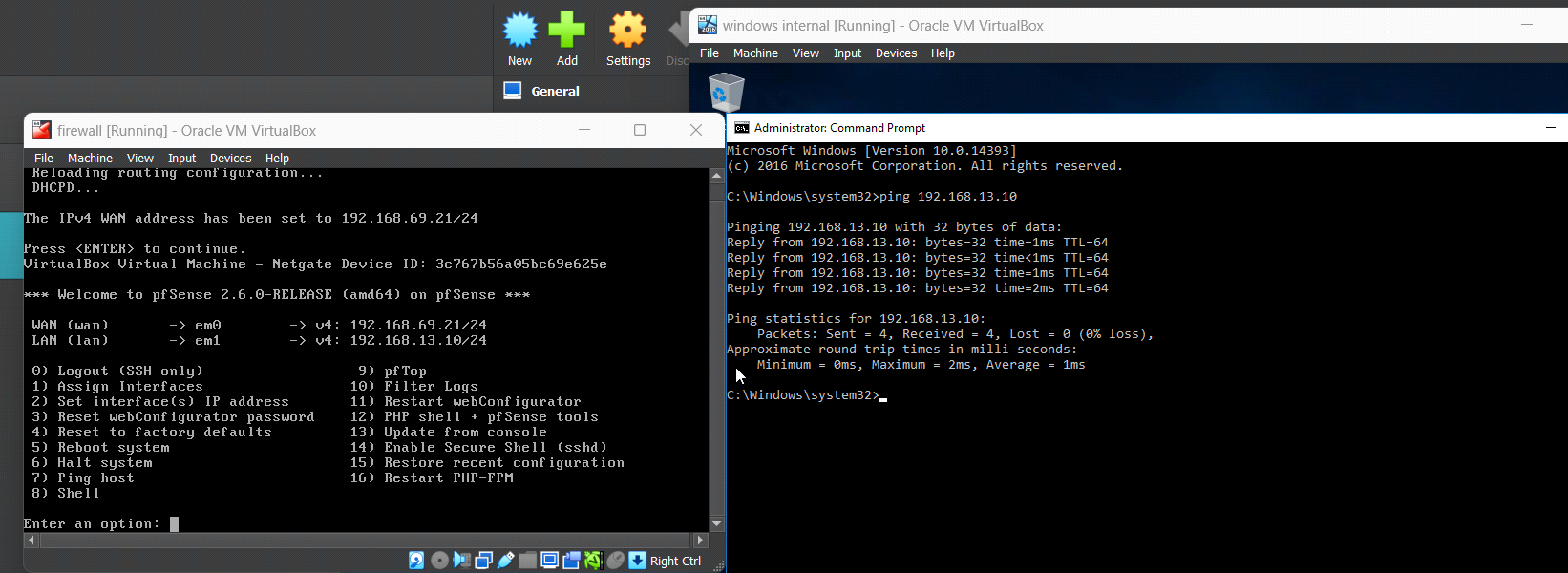
IP address of external machine: **192.168.69.69**

Gateway address of external machine/ WAN address of firewall: **192.168.69.21**

IP address of internal machine: **192.168.13.12**

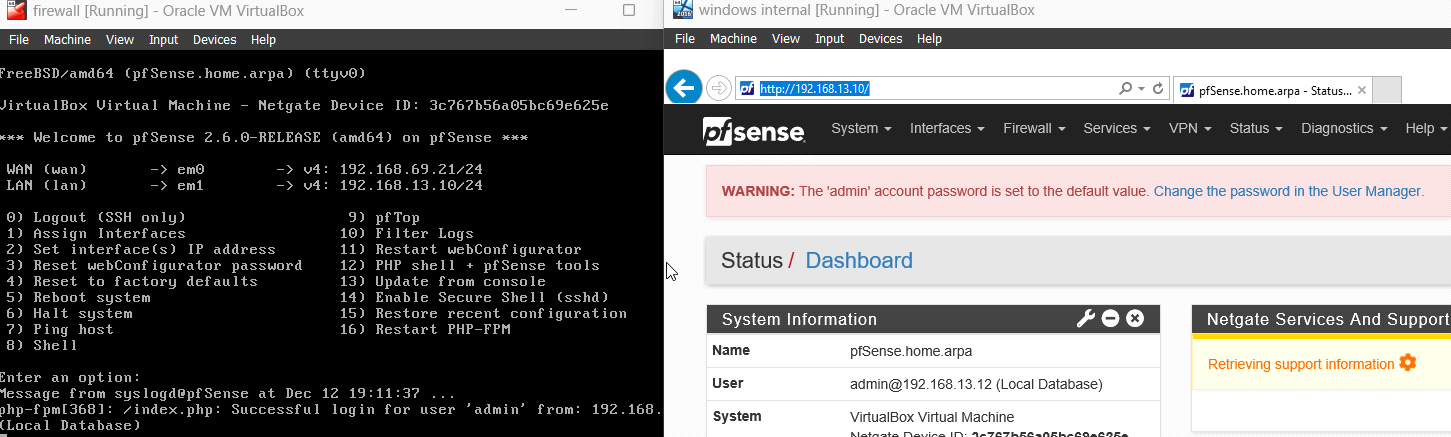
Gateway address of internal machine/LAN address of firewall: **192.168.13.10**

After configuring the networks, we will be able to ping the internal machine to firewall as shown below.

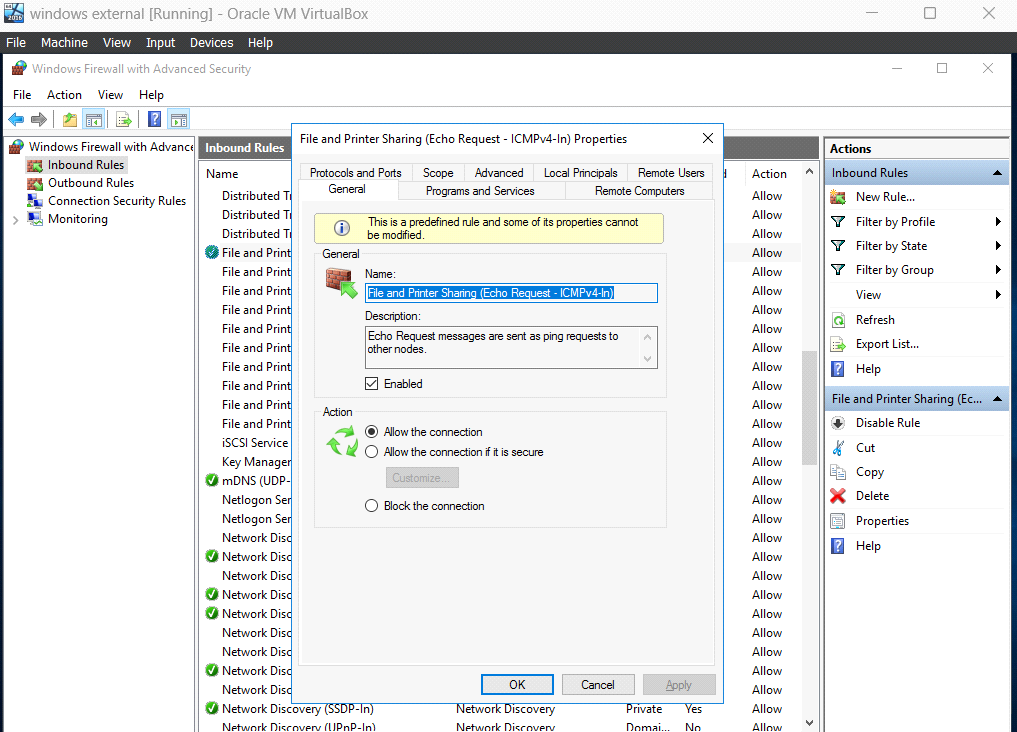


This means we can access pfsense web interface by using gateway address of LAN on internal machine.

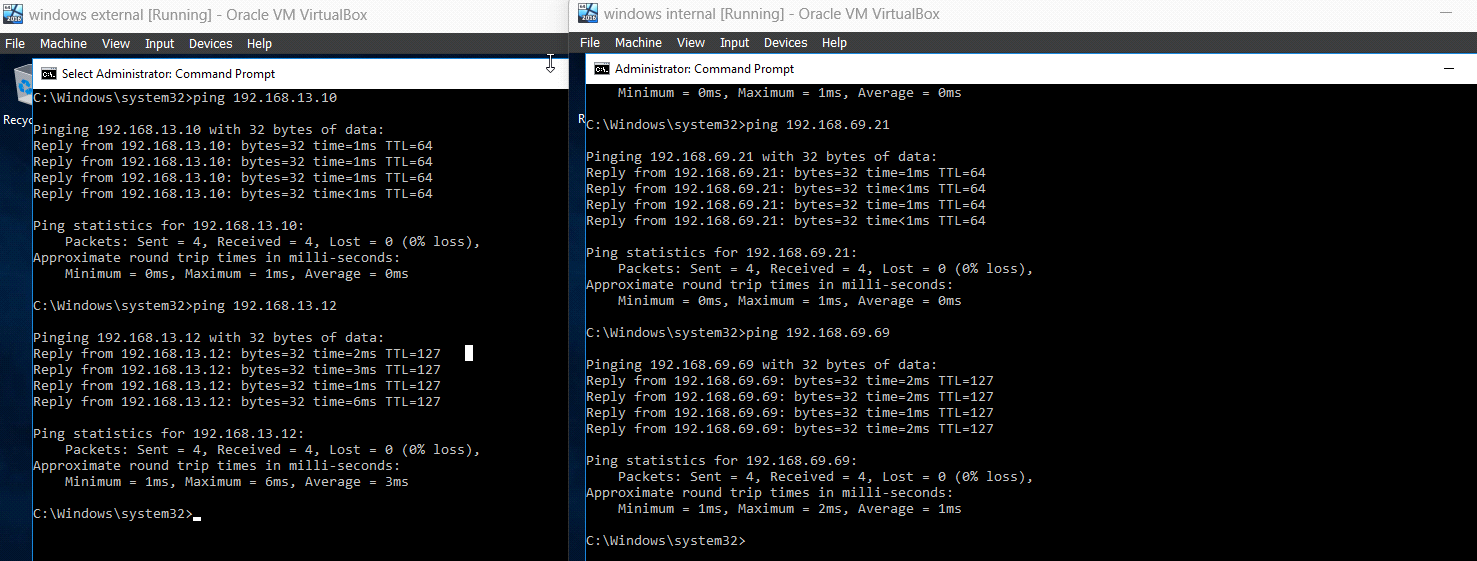
After logging in pfsense we can access all the default rules and components of pfsense.



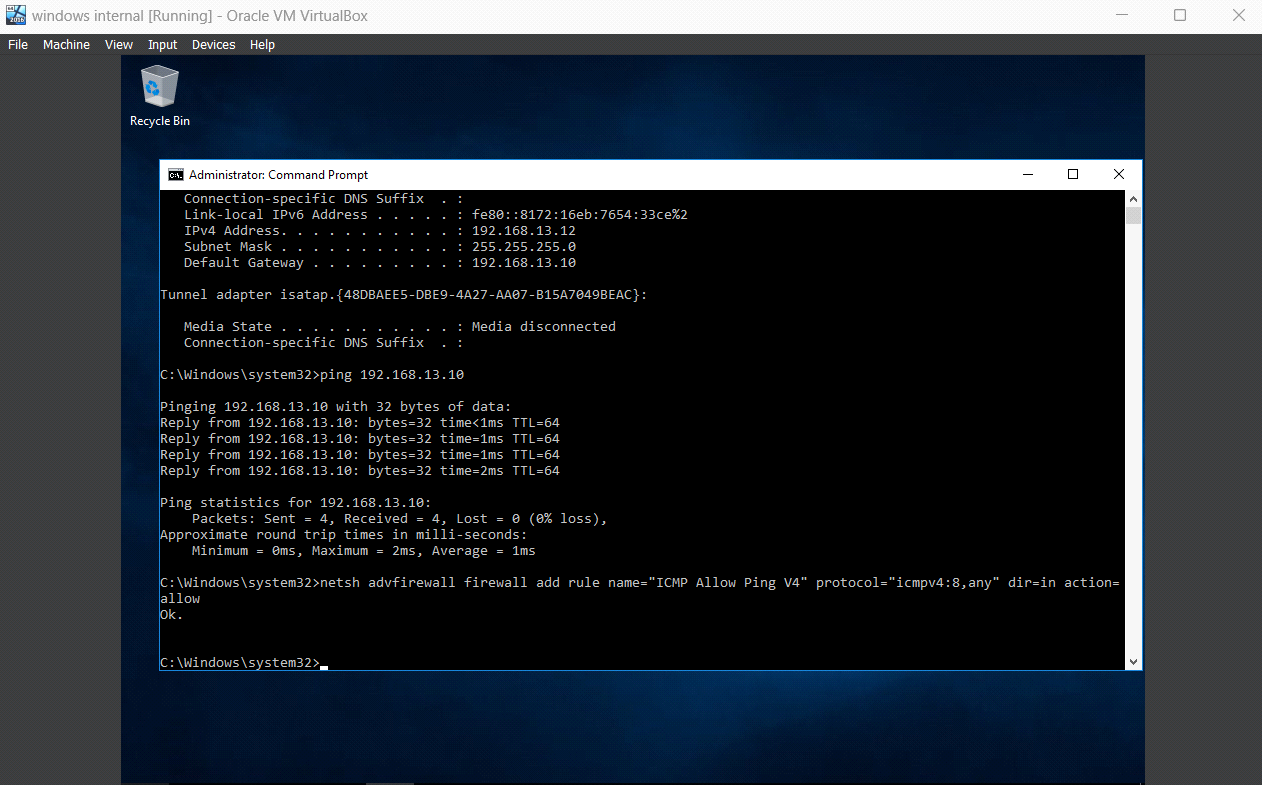
First, we will not be able to ping with external network because of the firewall restrictions in windows.

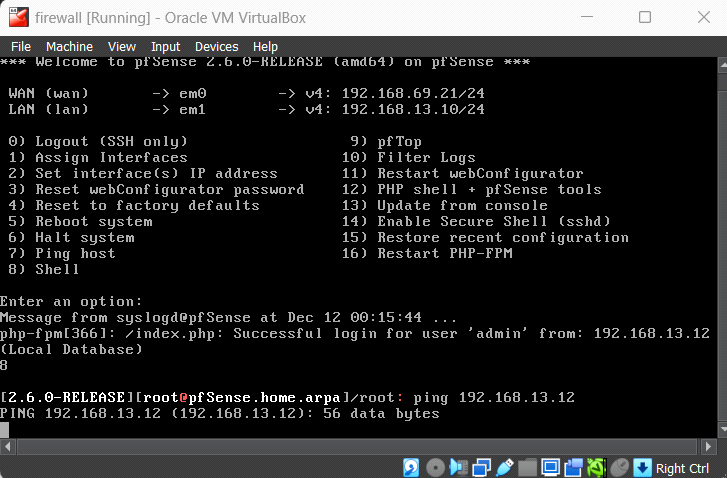


We can change the inbound rules in windows firewall so that we can ping both ip and gateway address from one machine to another.



We can also ping from firewall to both the machines with the following command.

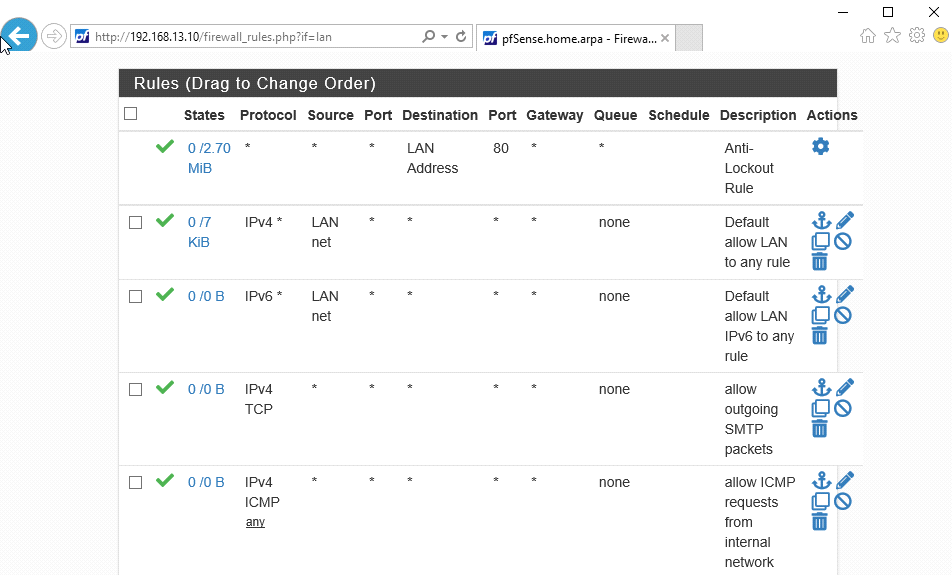


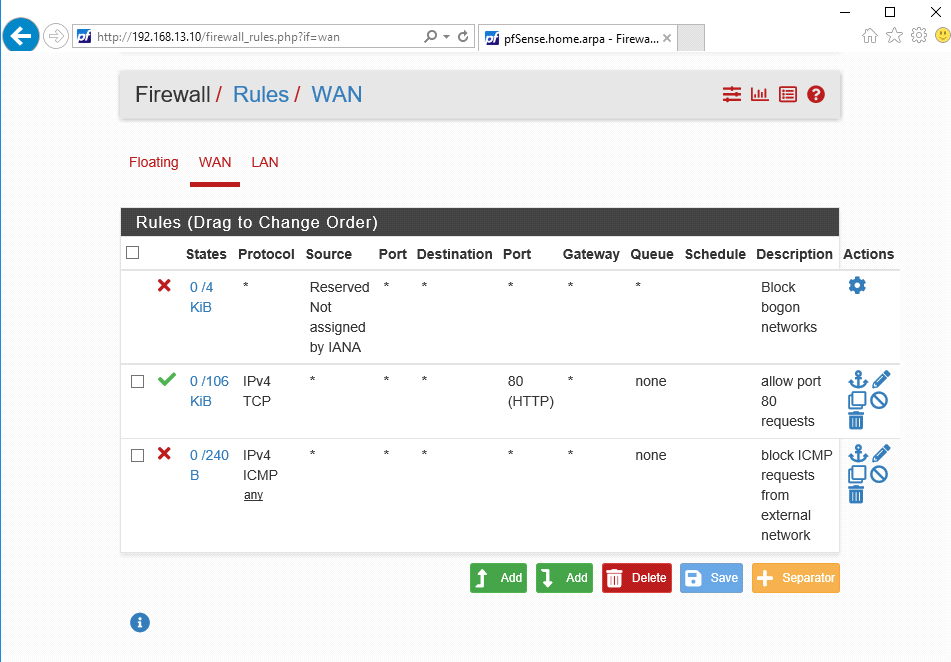


We can now access pfsense and implement rules for firewall.

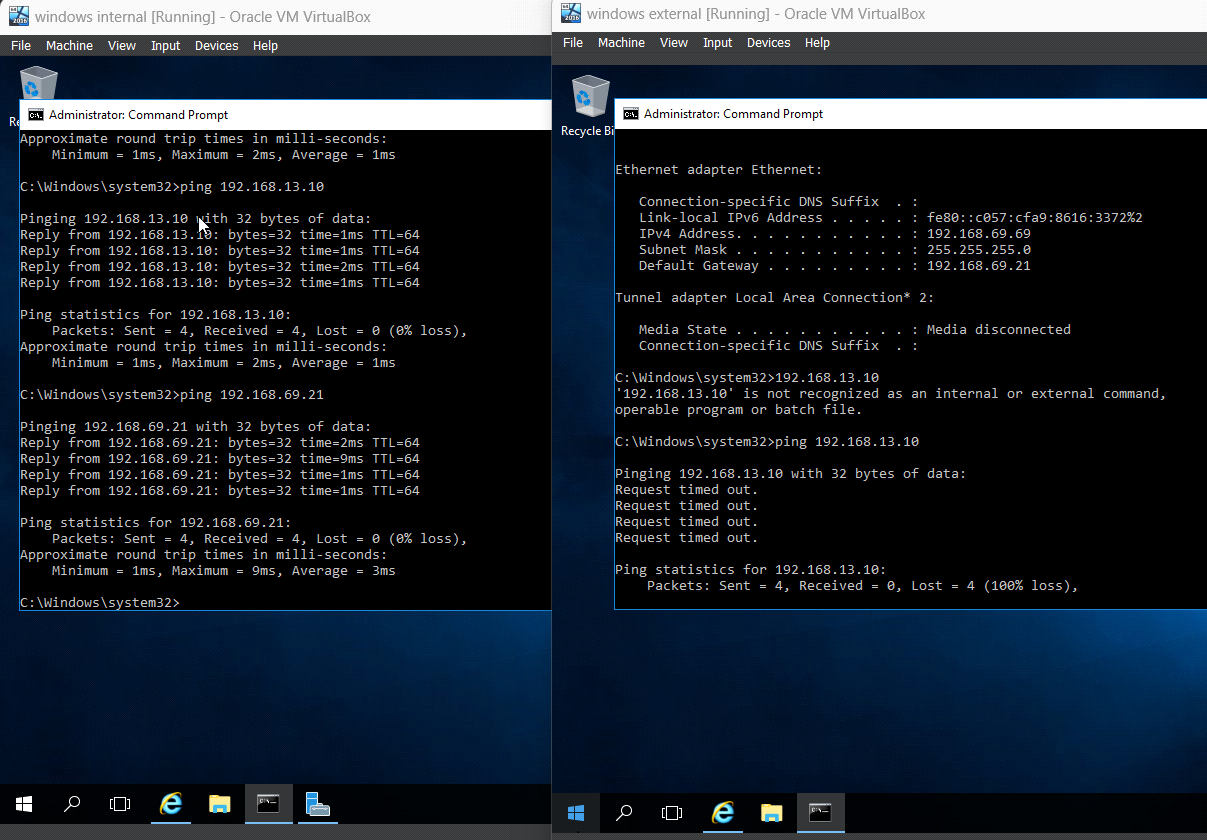
**Firewall configuration:**

* **Block external ICMP messages (ping, traceroute, etc.), but should allow these from interior clients.**

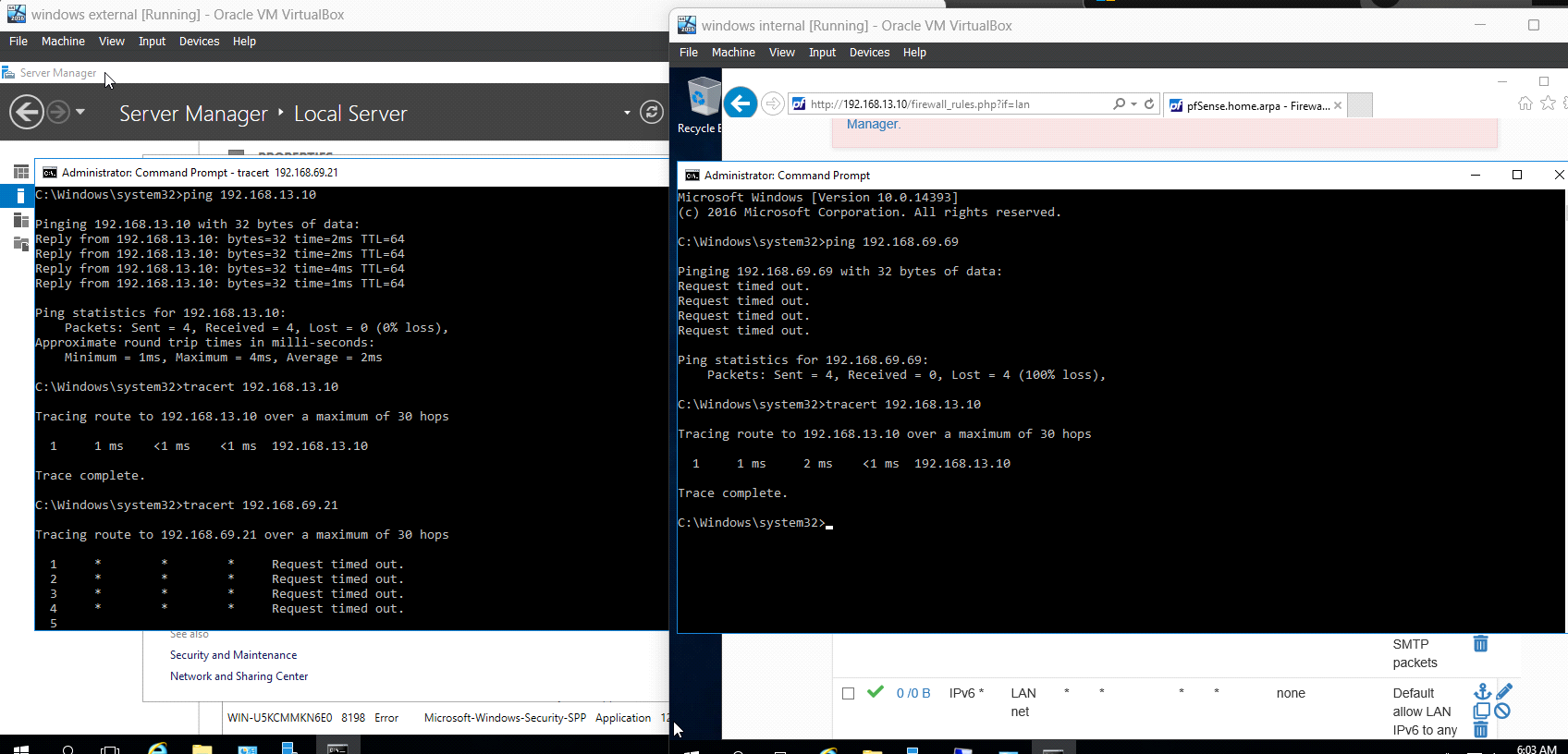




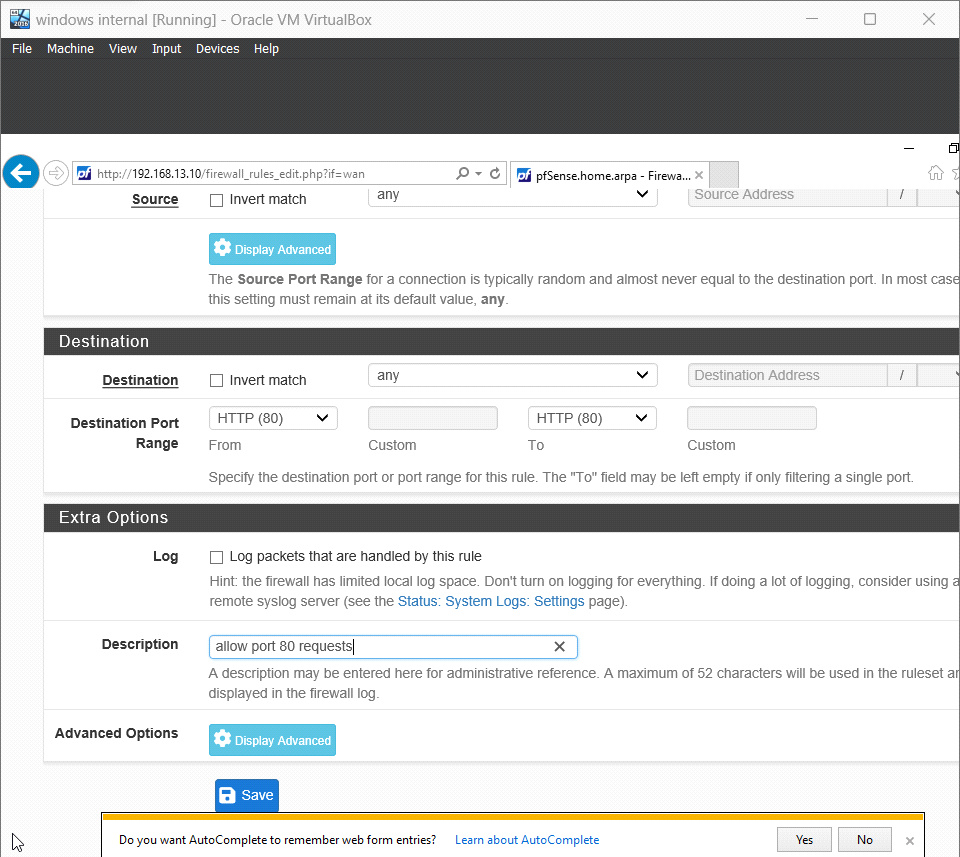
In pfsense web configuration the settings are applied such that firewall blocks ICMP messages from external network but allows when requested by internal network, As shown below.

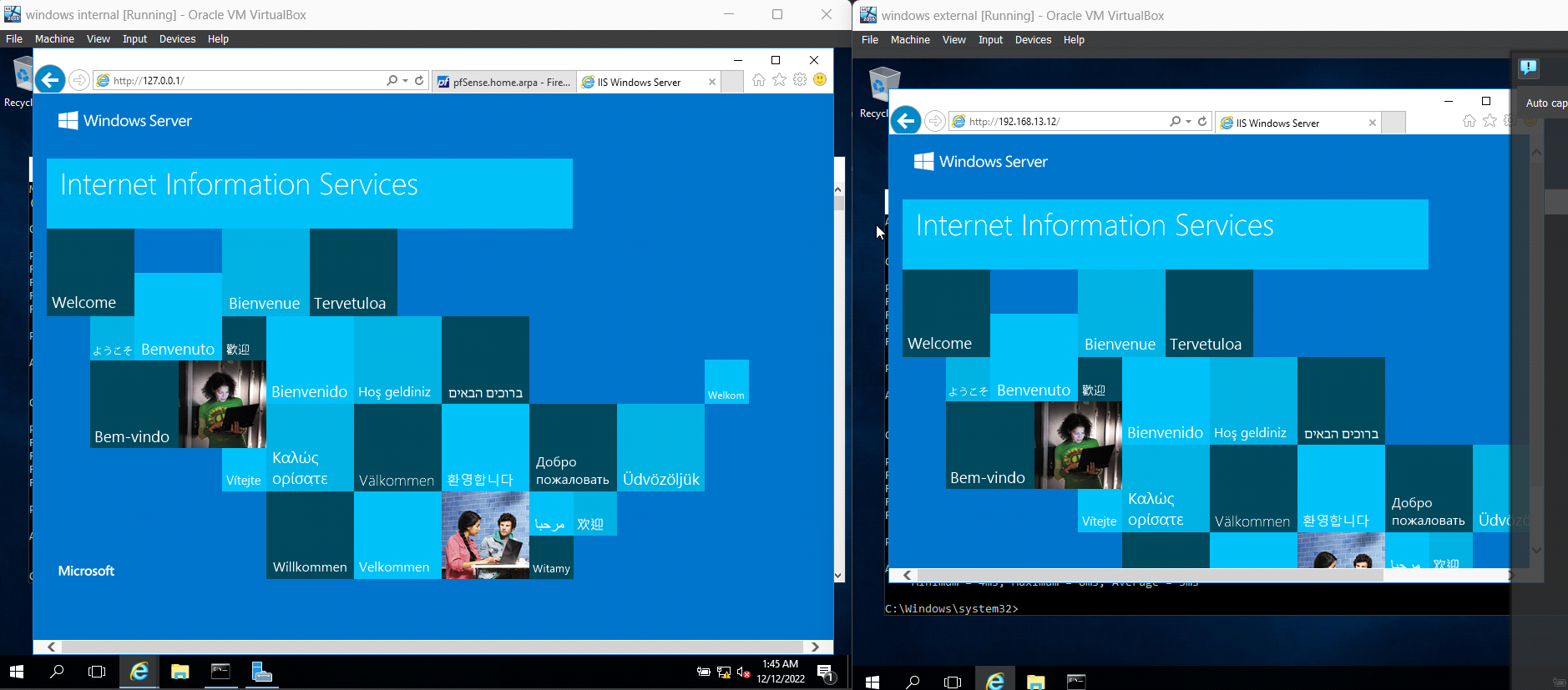


I could ping from internal network to firewall but not from external network. Similarly traceroute also works in internal network but not from external network as shown below



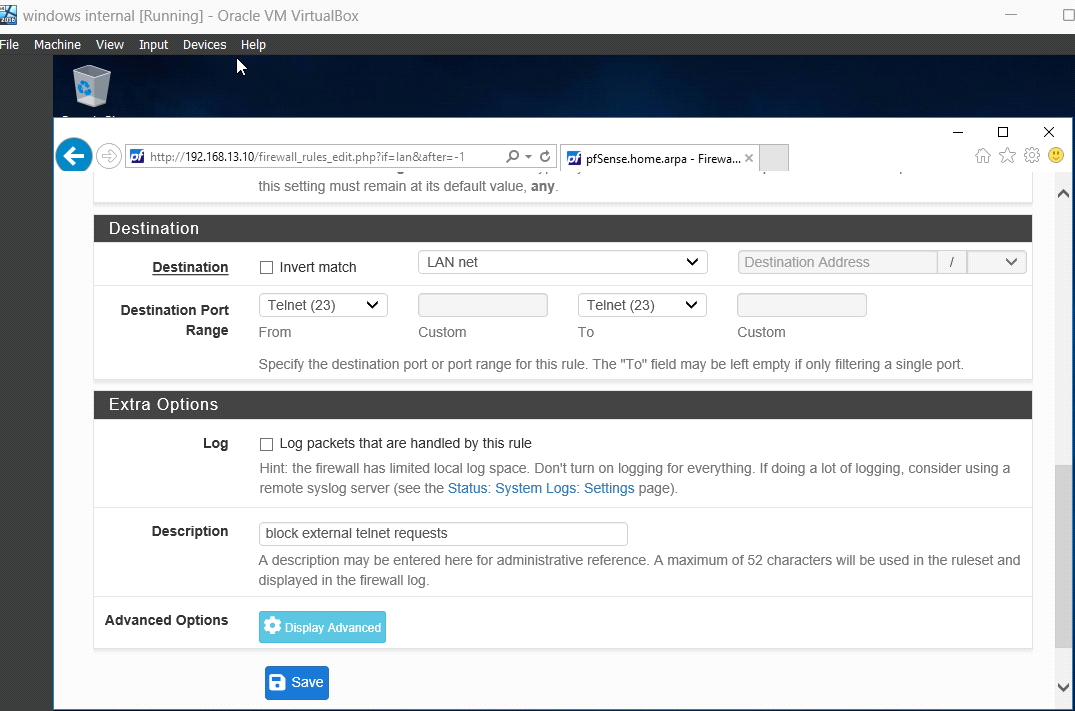
* **Allow port 80 requests to the interior client**



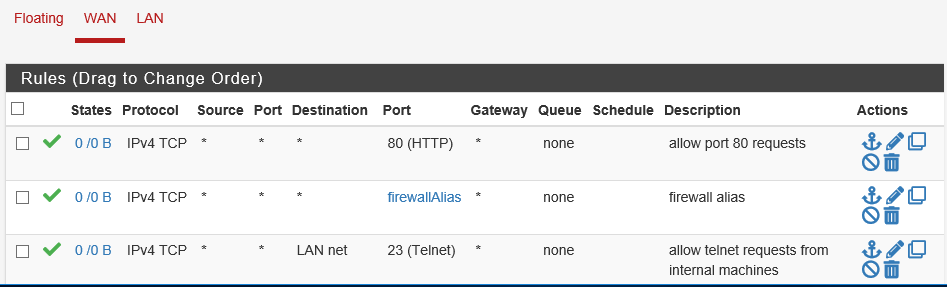


In the above screen we can see that external machine sent http request to internal machine and it was able to access the local server hosted by the internal machine.

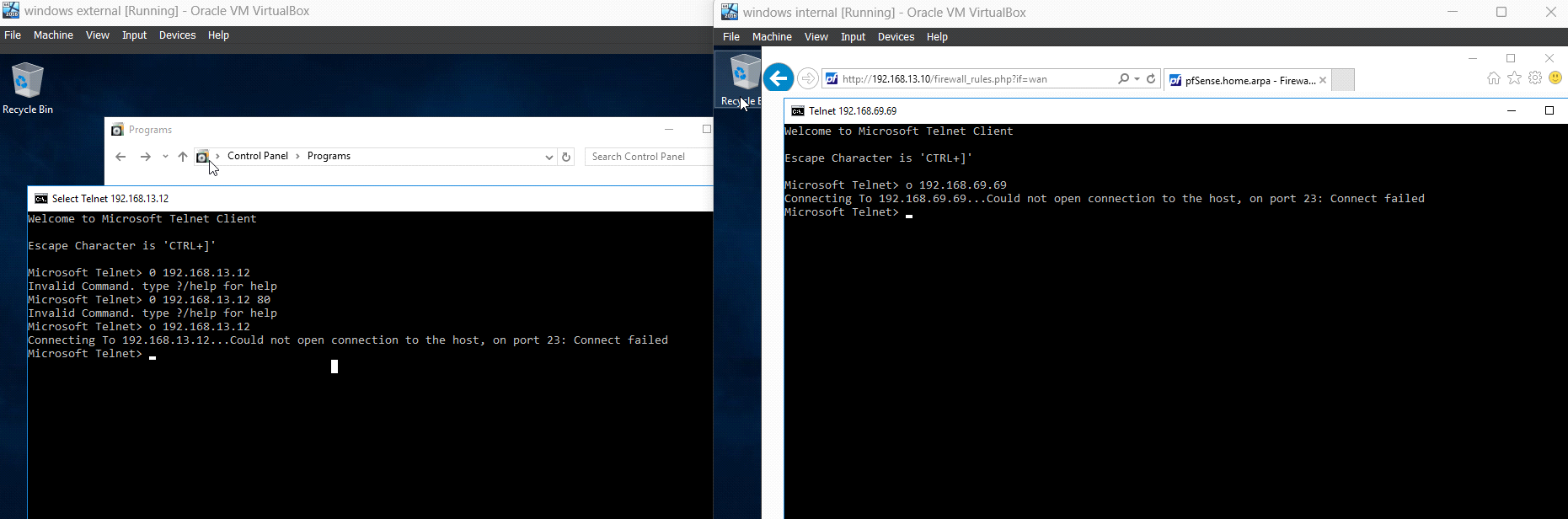
* **Block external telnet, rlogin, and other similar requests**

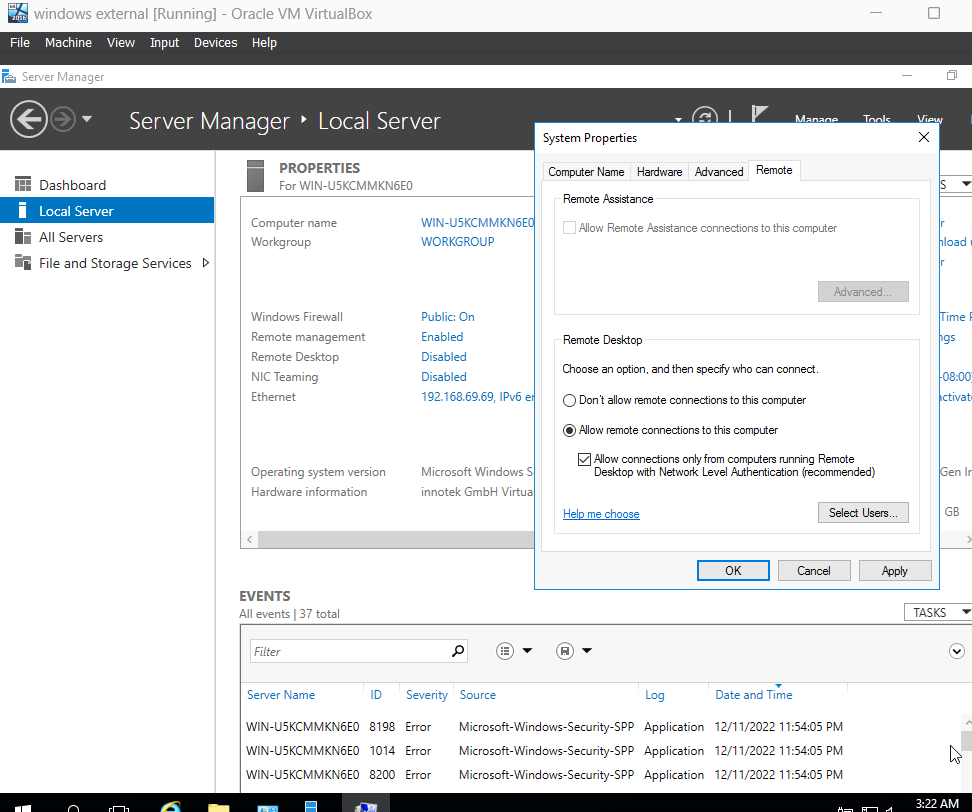


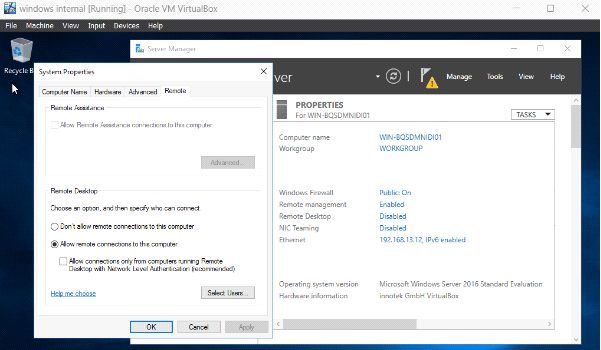




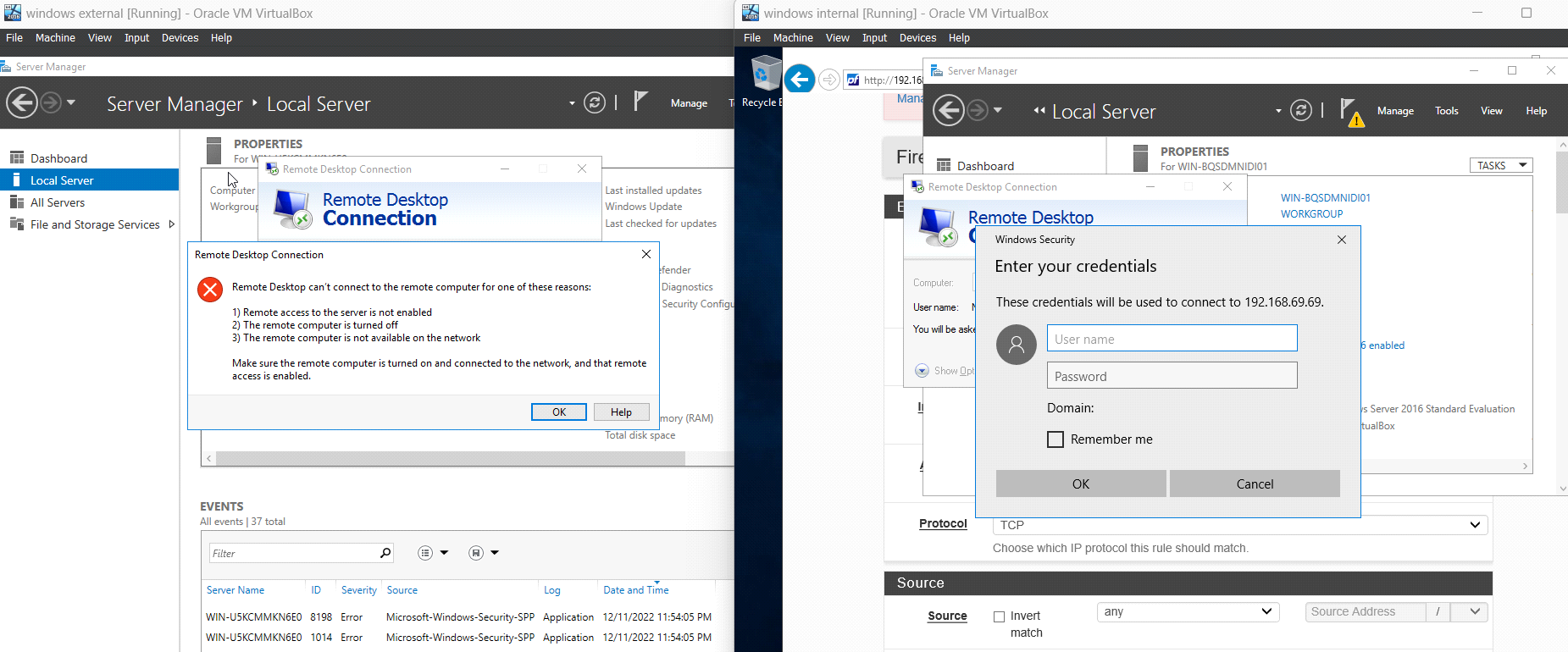
By configuring manually within pfsense firewall. We can block telnet request from external to internal machine via firewall as shown below



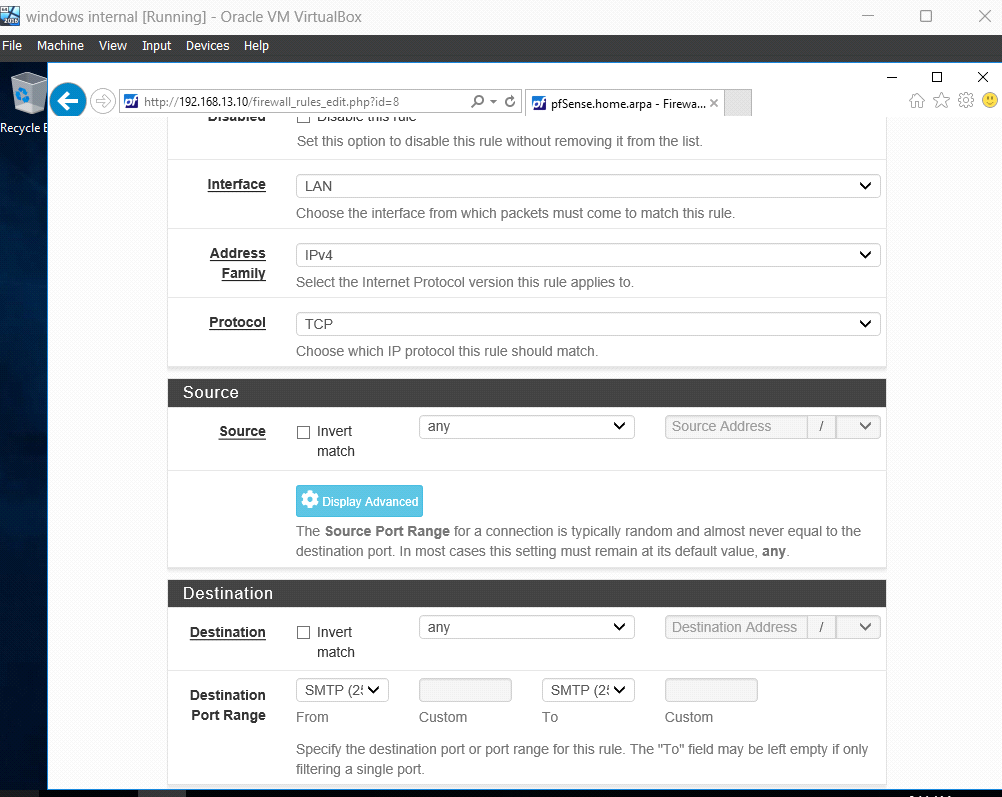


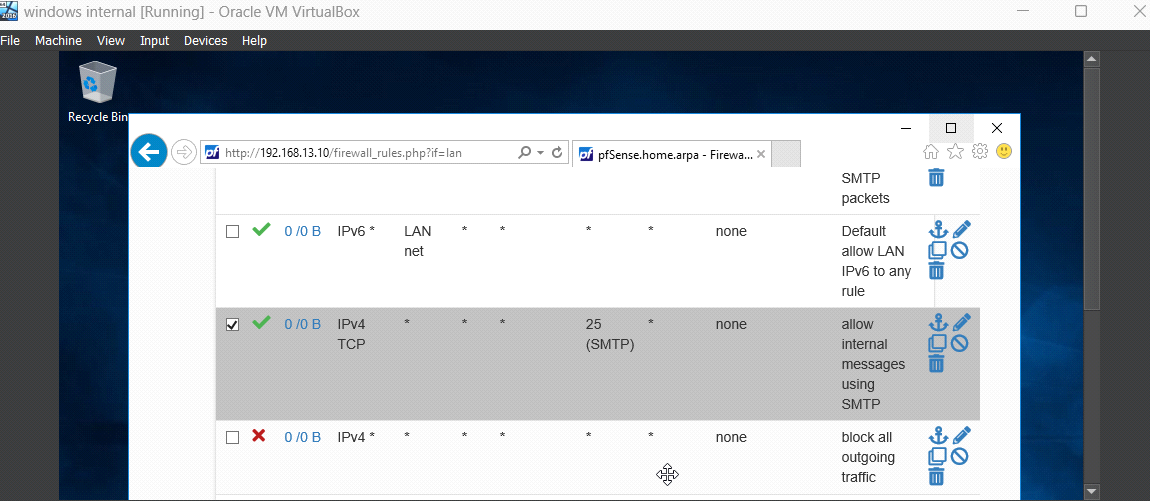


Because the telnet (23) port is blocked in WAN I'm unable to send remote login request from external machine to internal machine but vice versa is possible because I didn’t add a telnet block rule in LAN as shown below.

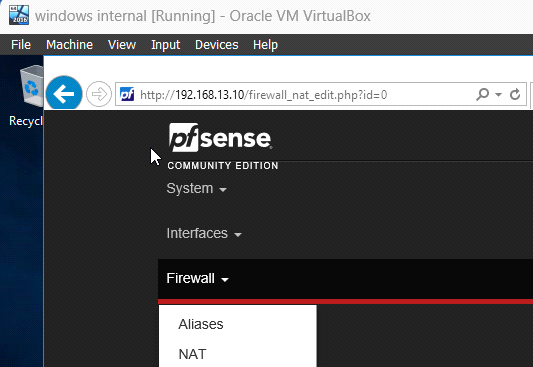


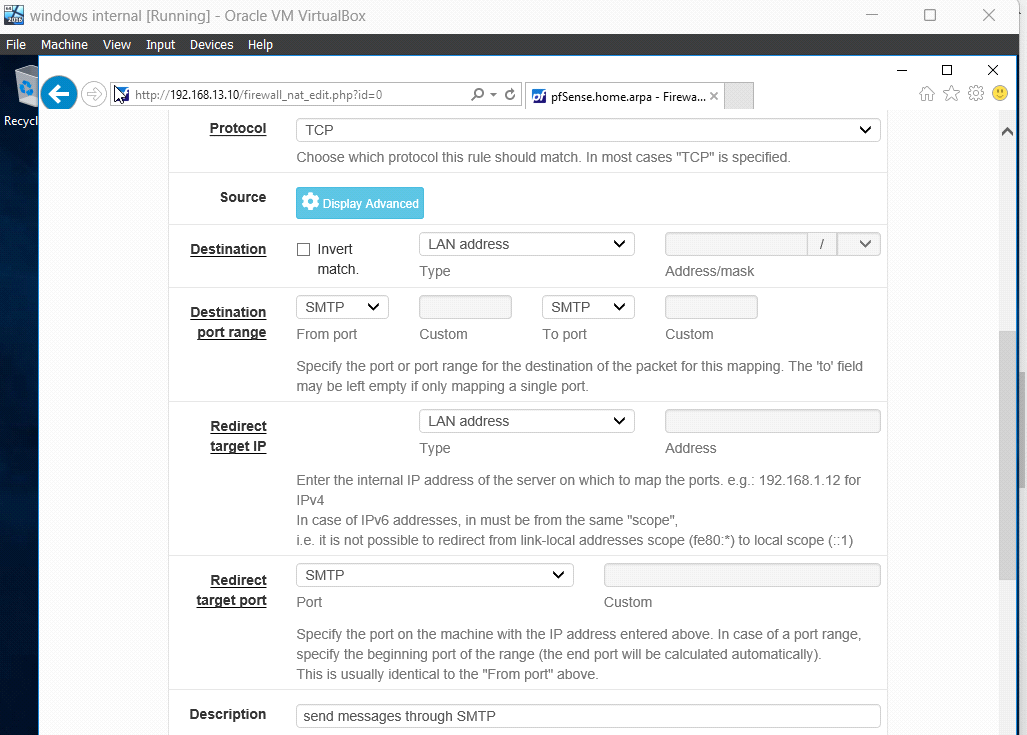
* **Allow internal messages using SMTP to be sent through the firewall**





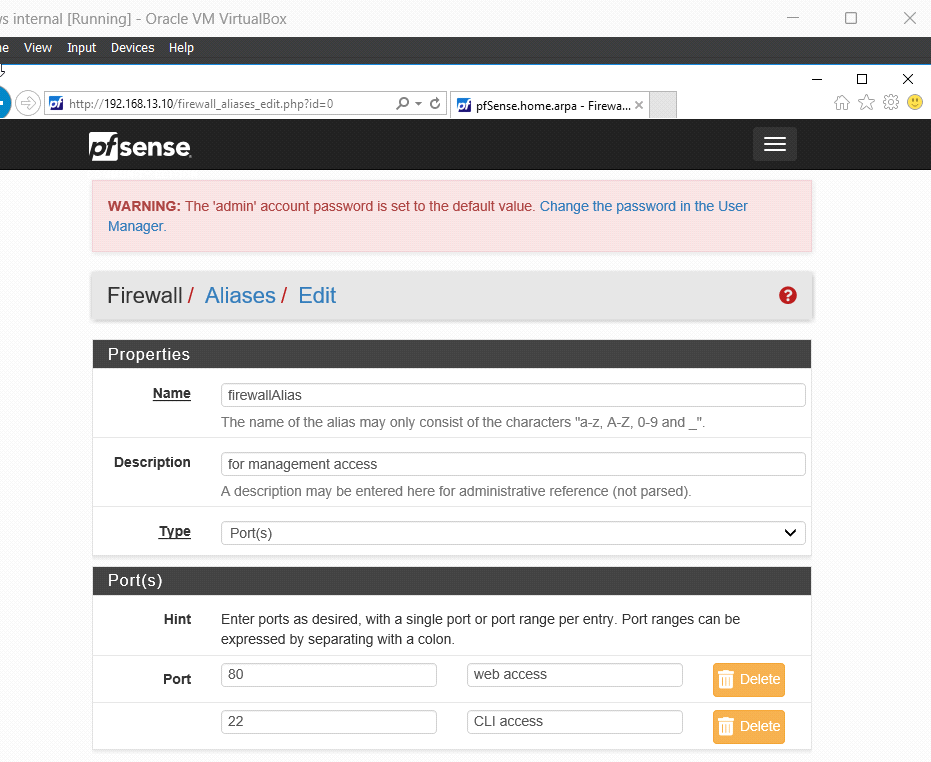
We block default outgoing traffic so that all the internal messages will be sent through SMTP. Another way to forward outgoing traffic using SMTP is by selecting firewall -> NAT -> port forward option.

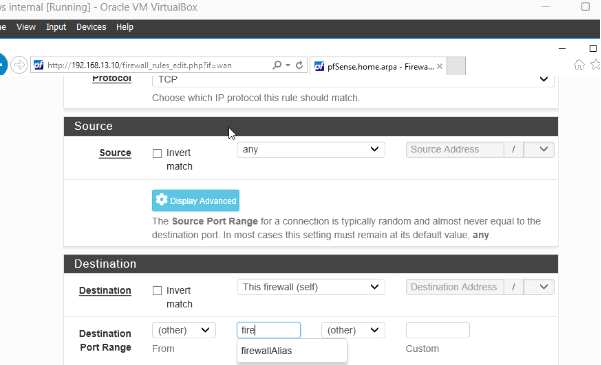




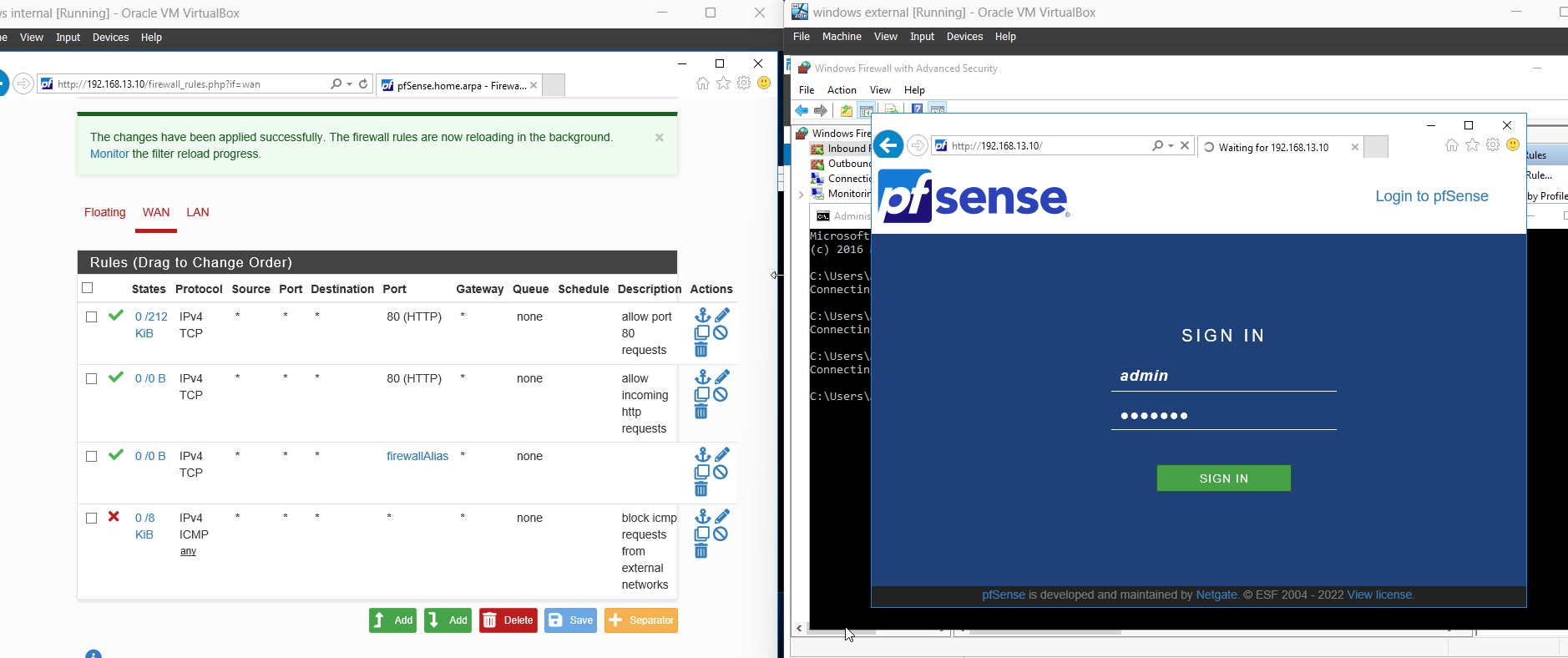
**Additional functionality:**

* Firewall aliases: This is used to add different IPs and ports and reference them in the rules.



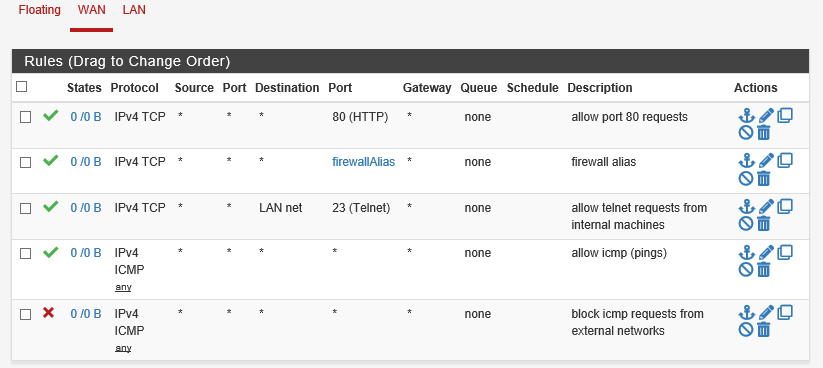


I have added a firewall alias in the rule. This would allow traffic from external to internal machine on port 80 and 22 as shown in below. I was able to access 192.168.13.10 which is my internal network from external machine.

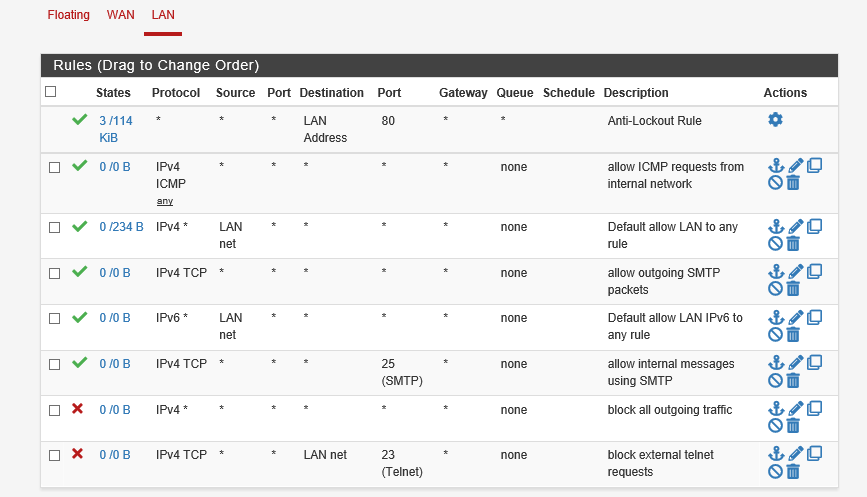


**Final configured firewall:**

**WAN:**



**LAN:**



**Lessons learned:**

* Aside from connecting the 3 virtual machines together, the problems mostly I had was I didn’t have much knowledge how network adapters work before.
* From this project I was able to study how each network adapter work and in which scenario I should use specific network adapter.
* Adding implementing telnet, login functionality was also bit challenging because initially, I was not able implement it properly.
* Initially I didn’t place the firewall rules in order. So, when I placed block outgoing traffic rule above all allow rules. The rules didn’t work so I had to place them in order.