

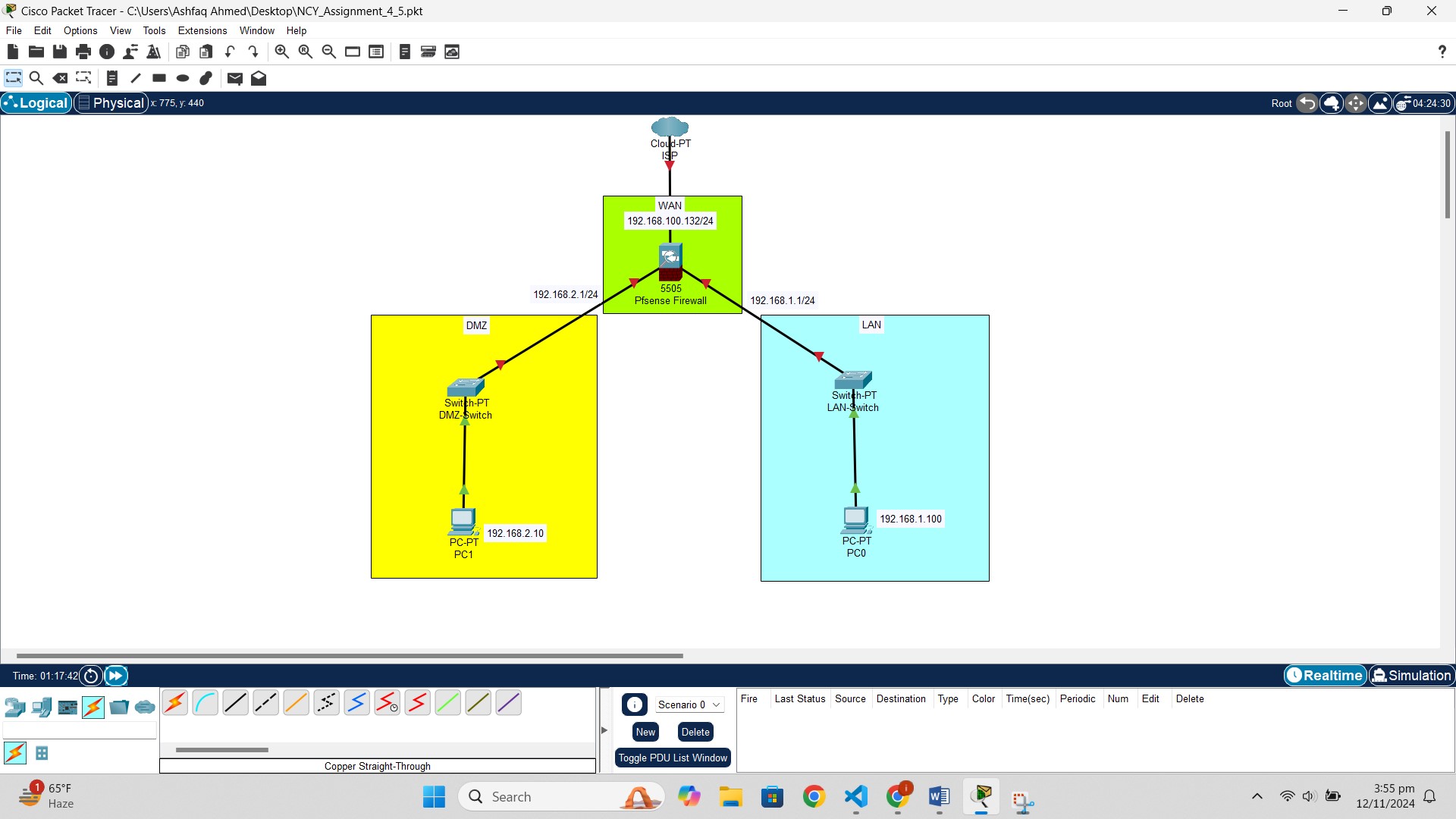
**ASSIGNMENT# 04/05**

**Building a Secure Network with PfSense, Suricata, and DMZ.**

**Name : Sami Ullah, Ashfaq Ahmed**

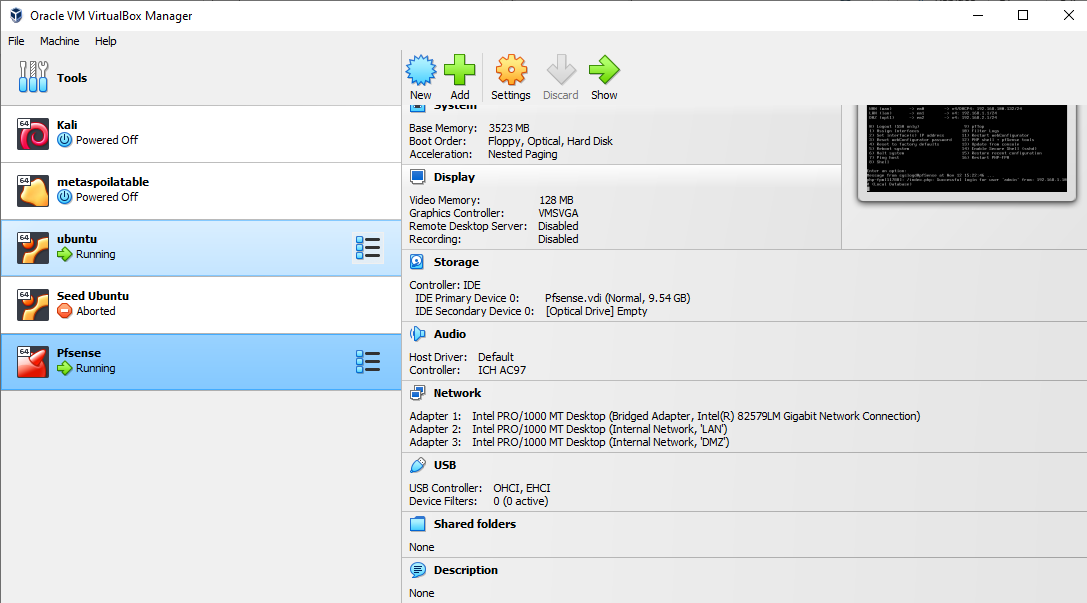
**Roll No: 22i-1663,22i-1616**

**Network Topology Diagram:**

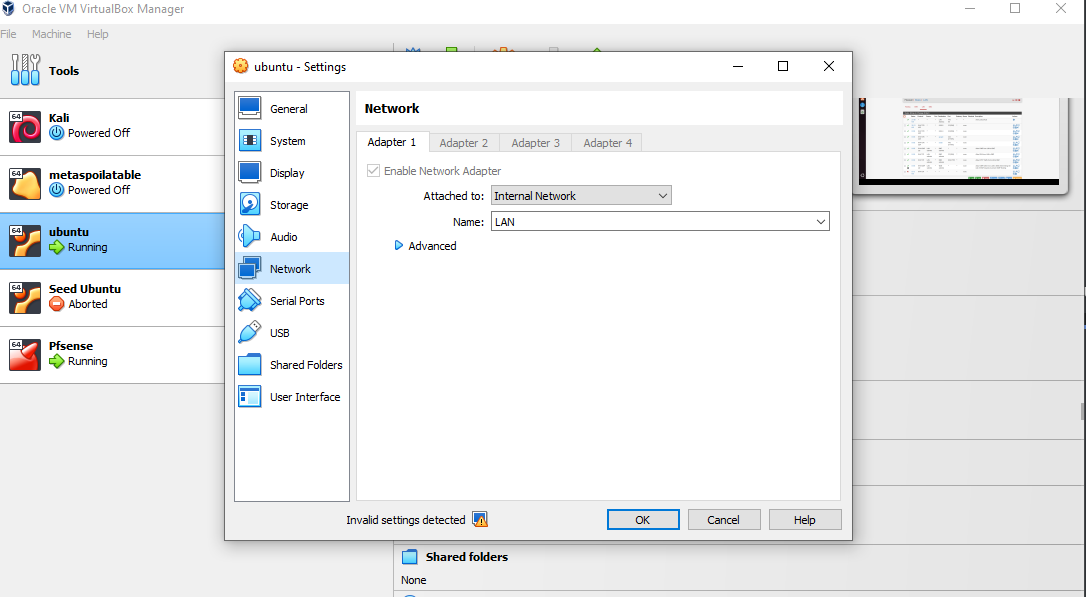


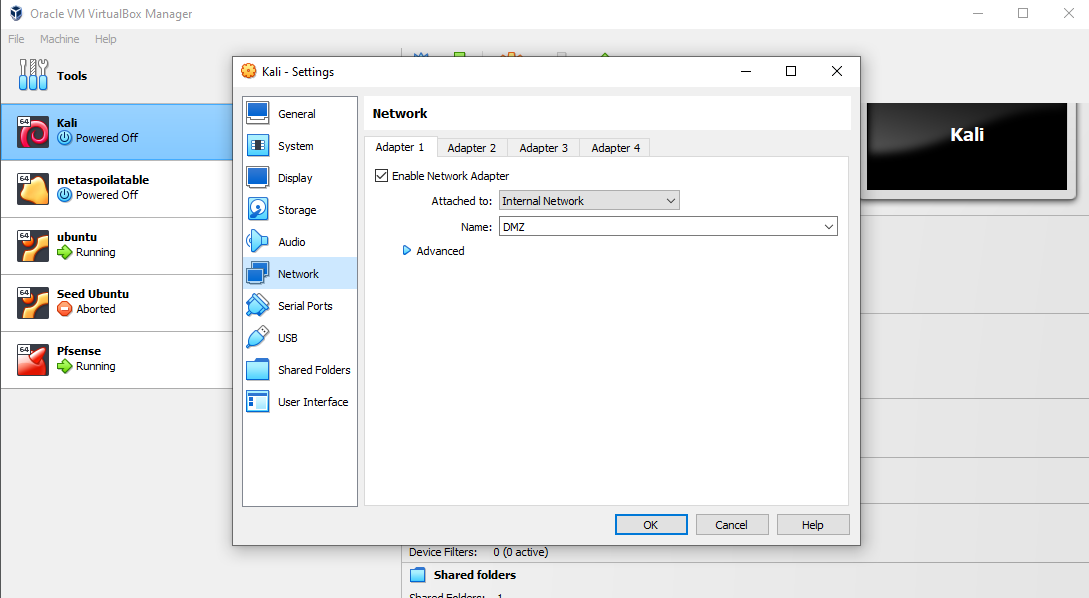
**Configuration Steps for pf Sense, DMZ, Suricata:**

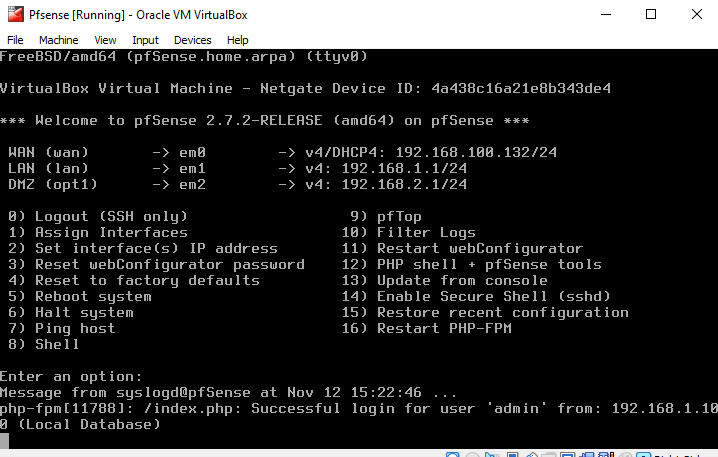
Pfsense is assigned 3 network adpaters. 1 bridge apdater, 1 internal for LAN, 1 internal for DMZ.

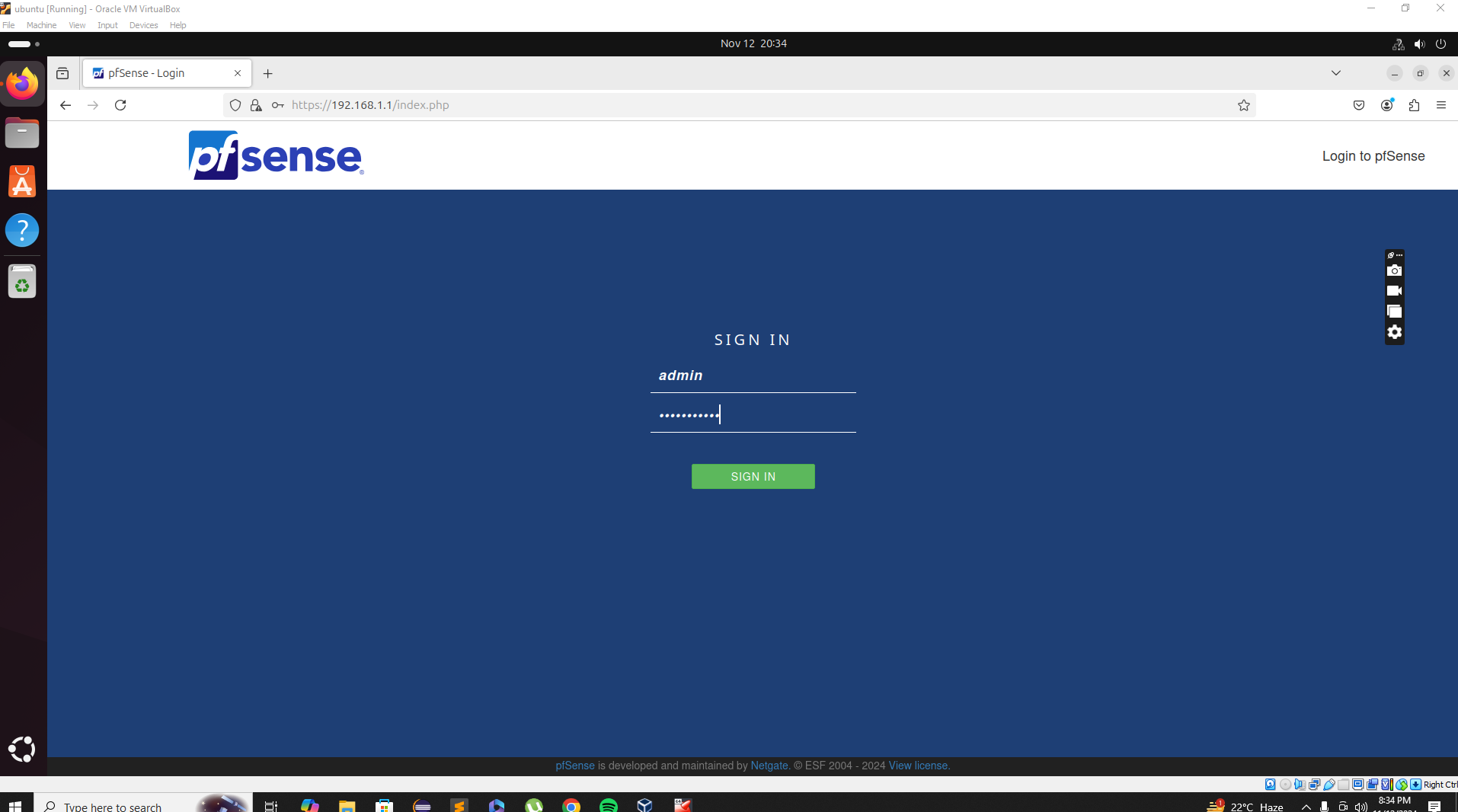


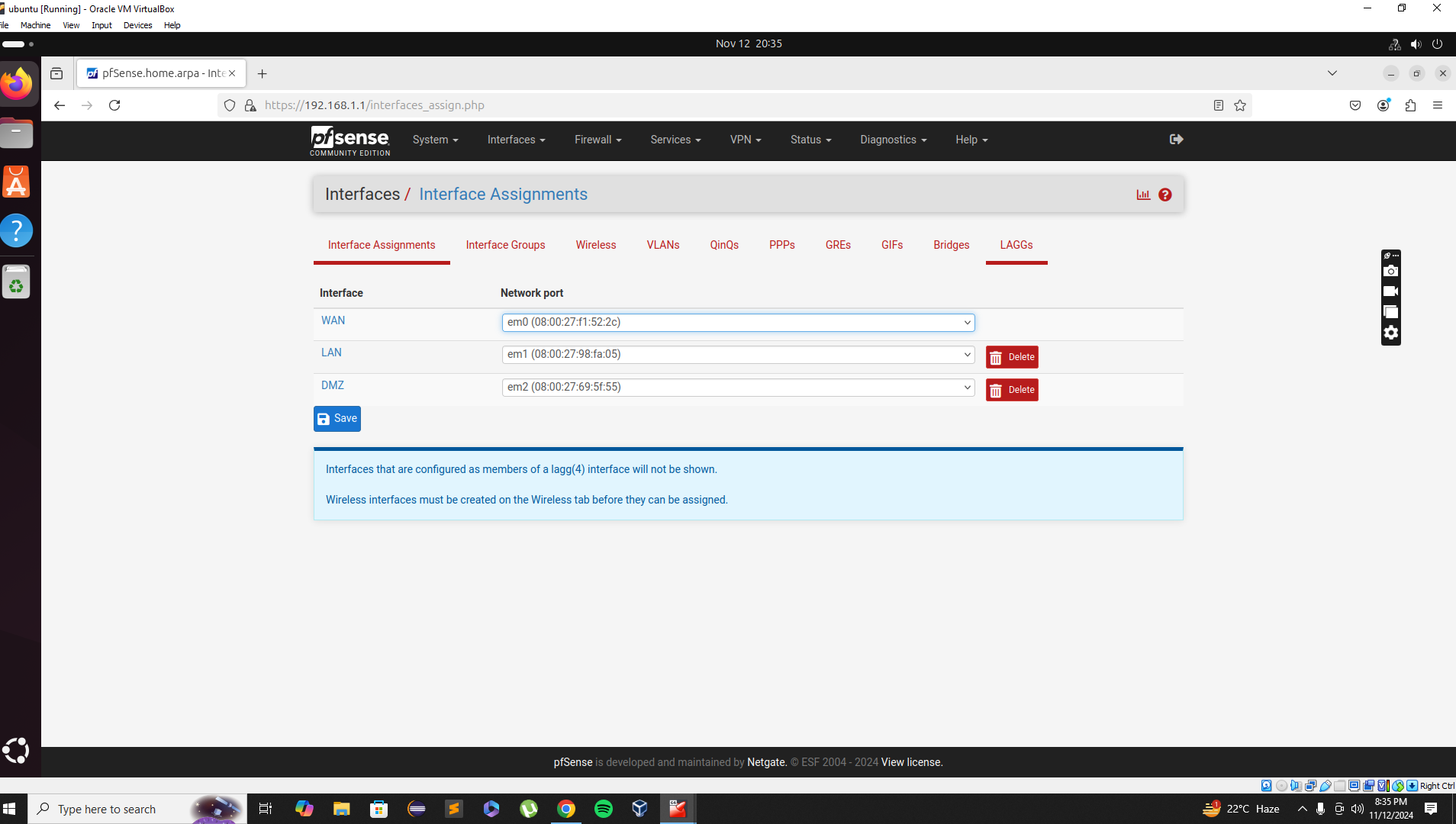
Ubuntu (LAN) machine is connected to pfsense by connecting it to internal network. Similarly for DMZ as well.

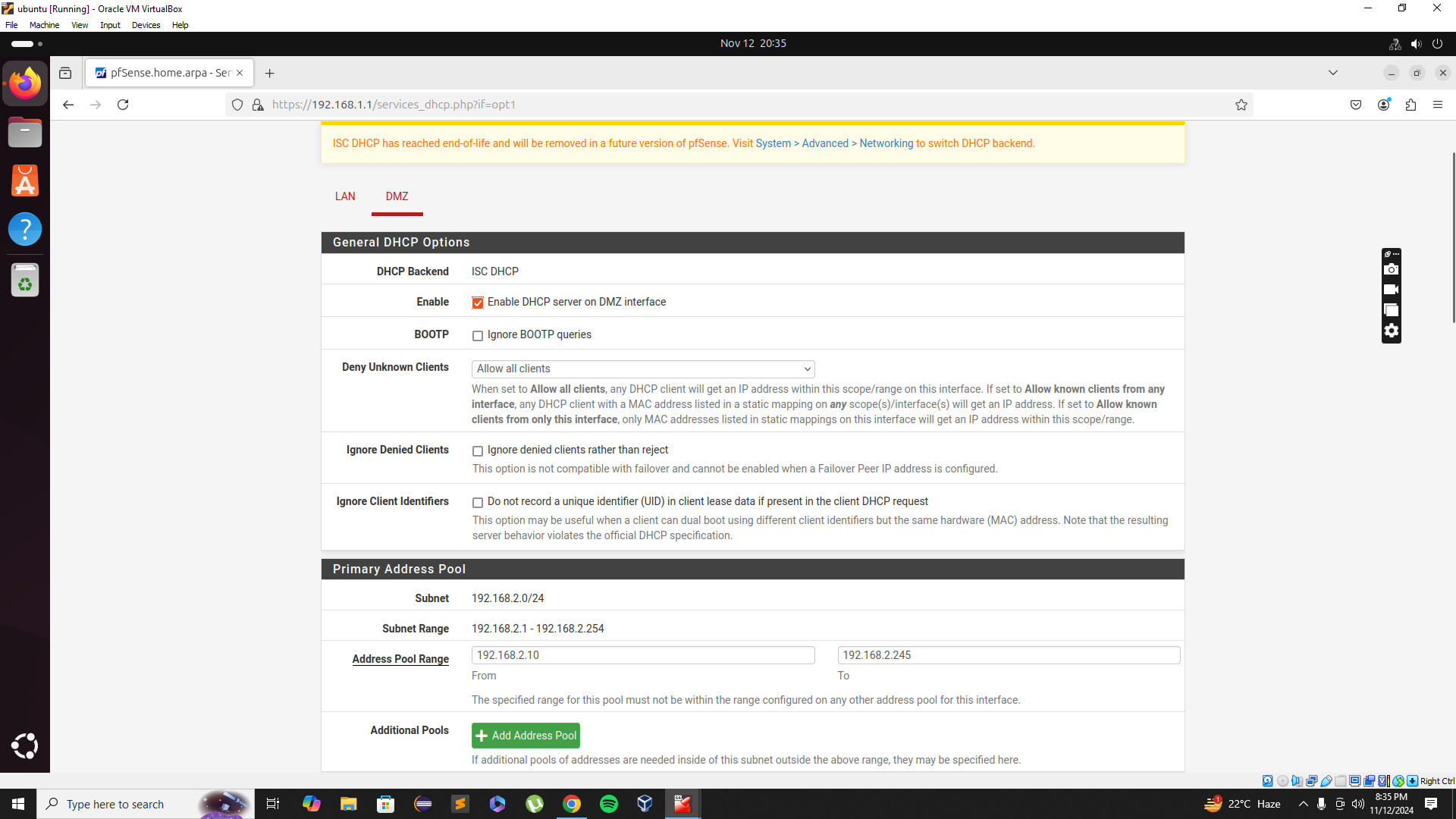


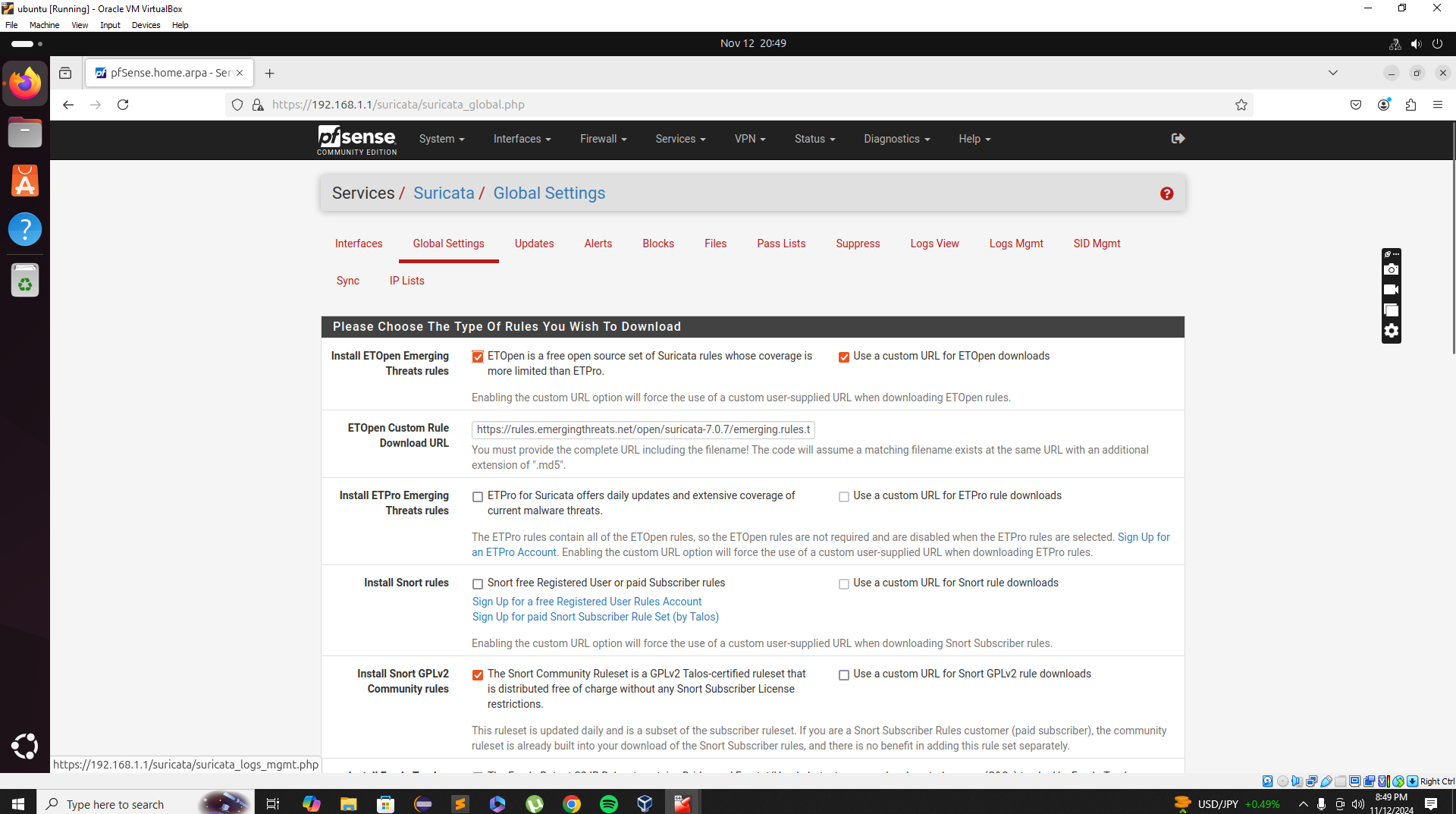


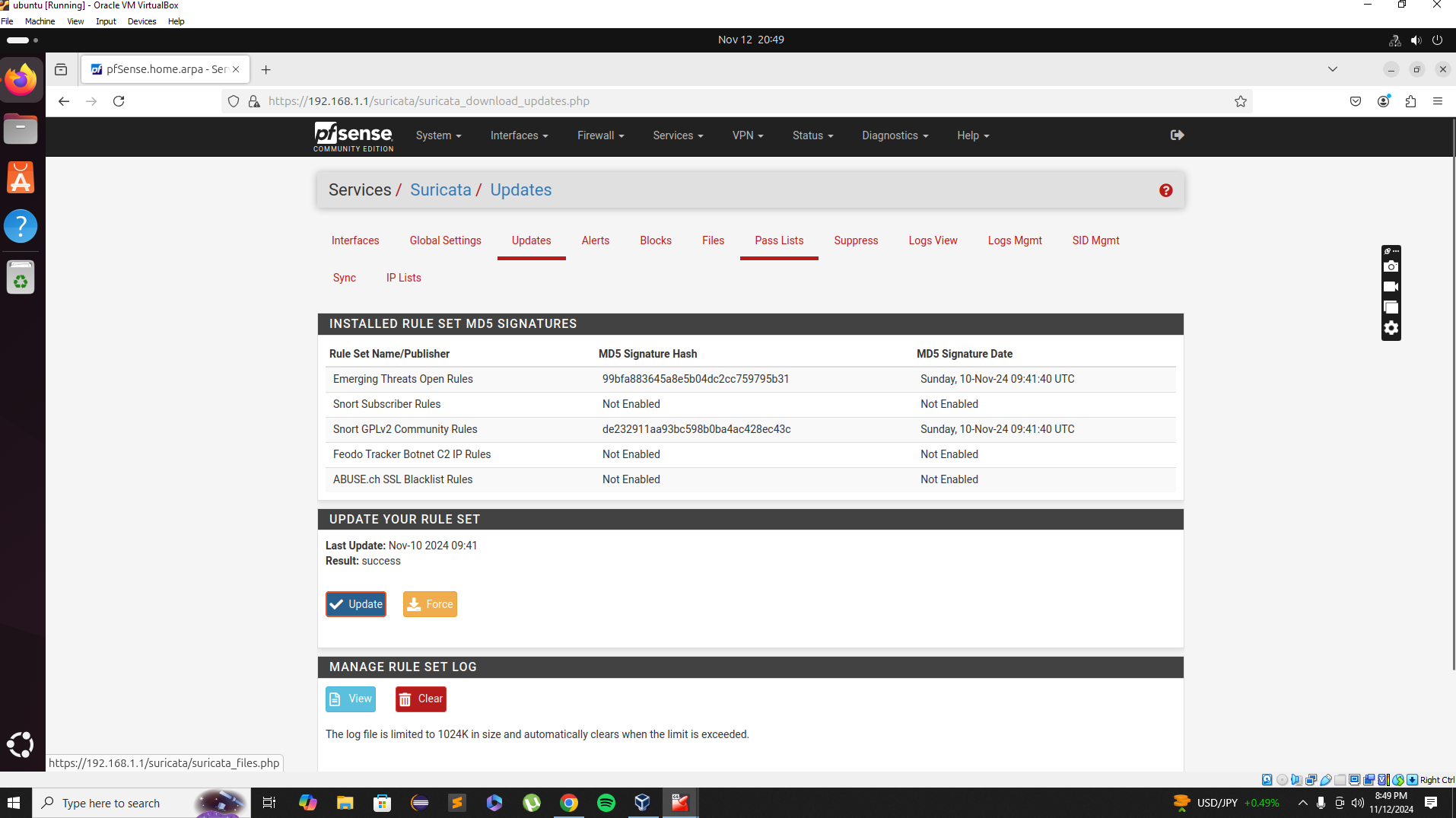


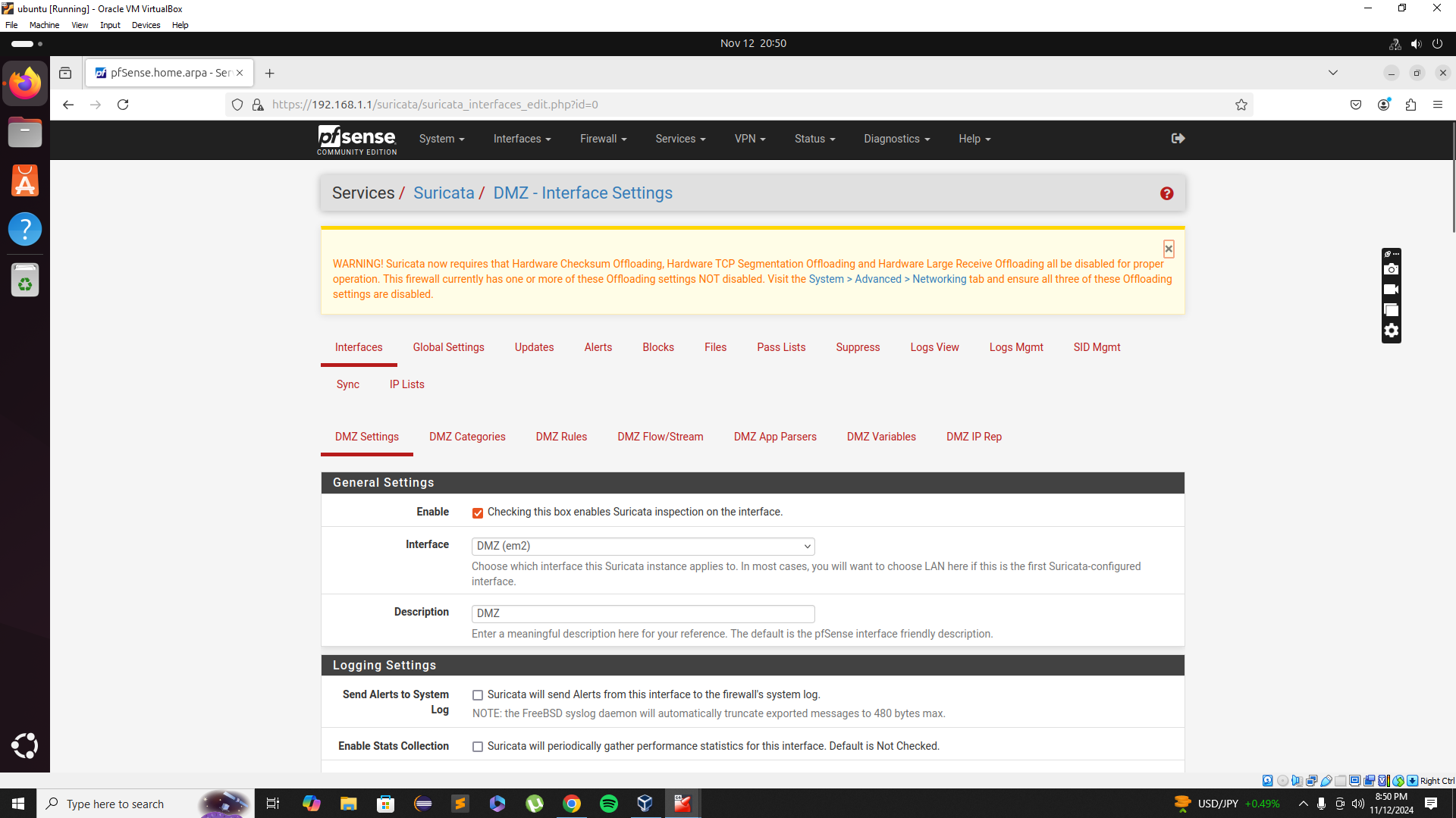








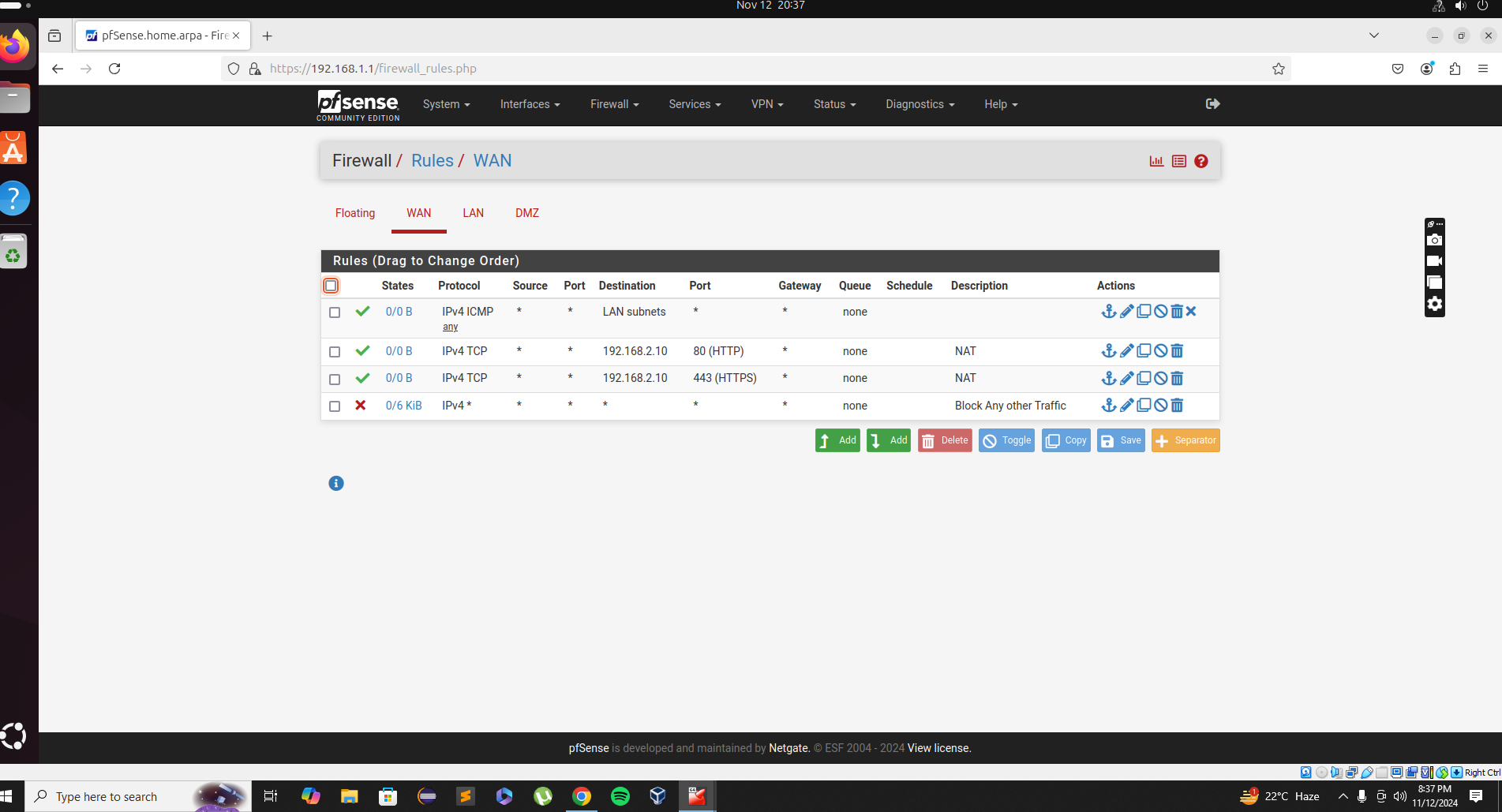


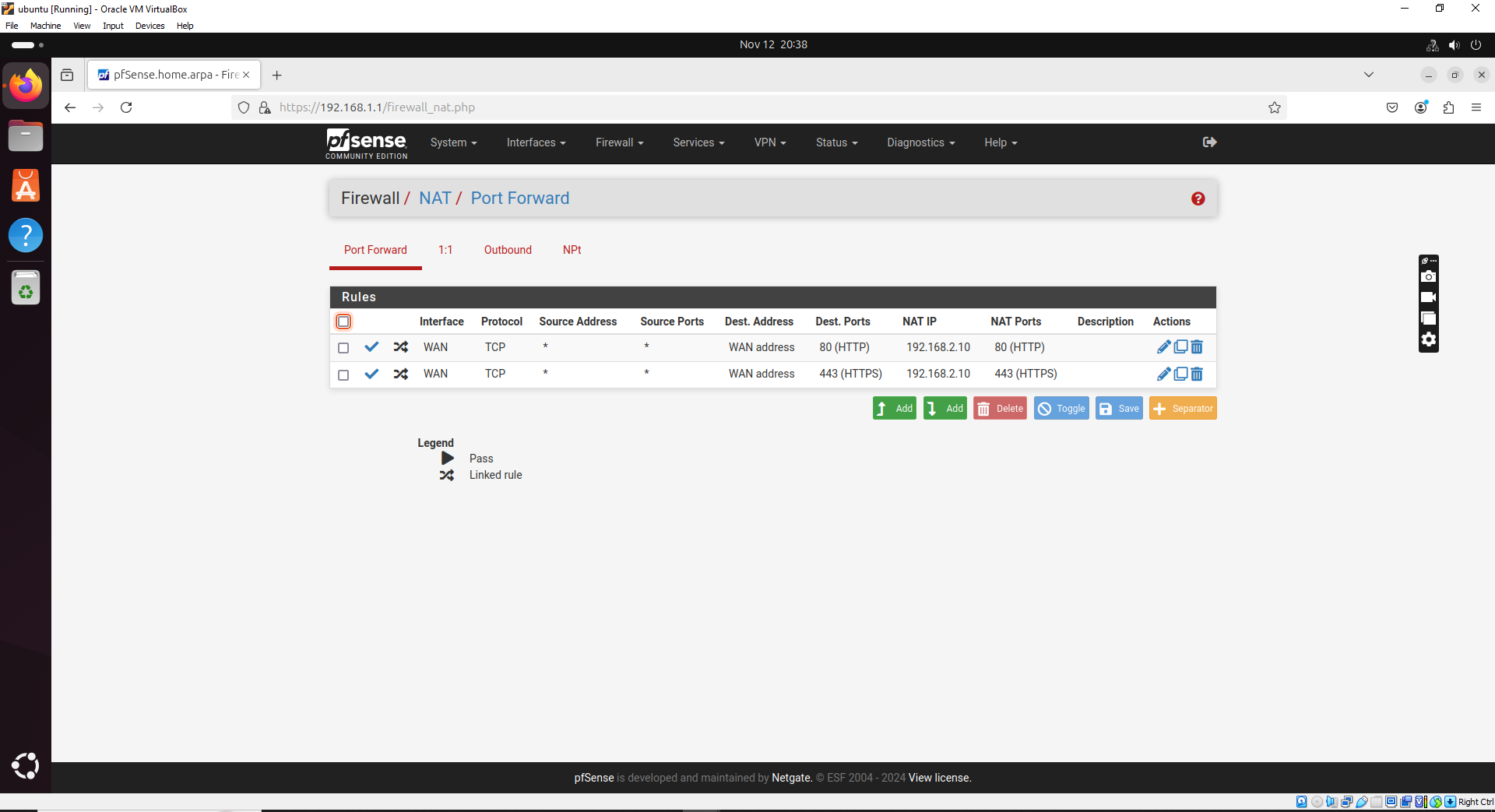


**Firewall rule tables:**

**WAN Side:**

Port Forwarding is used to access the webserver from WAN. It automatically creates the associated rules in the firewall. Any traffic other than that is blocked.





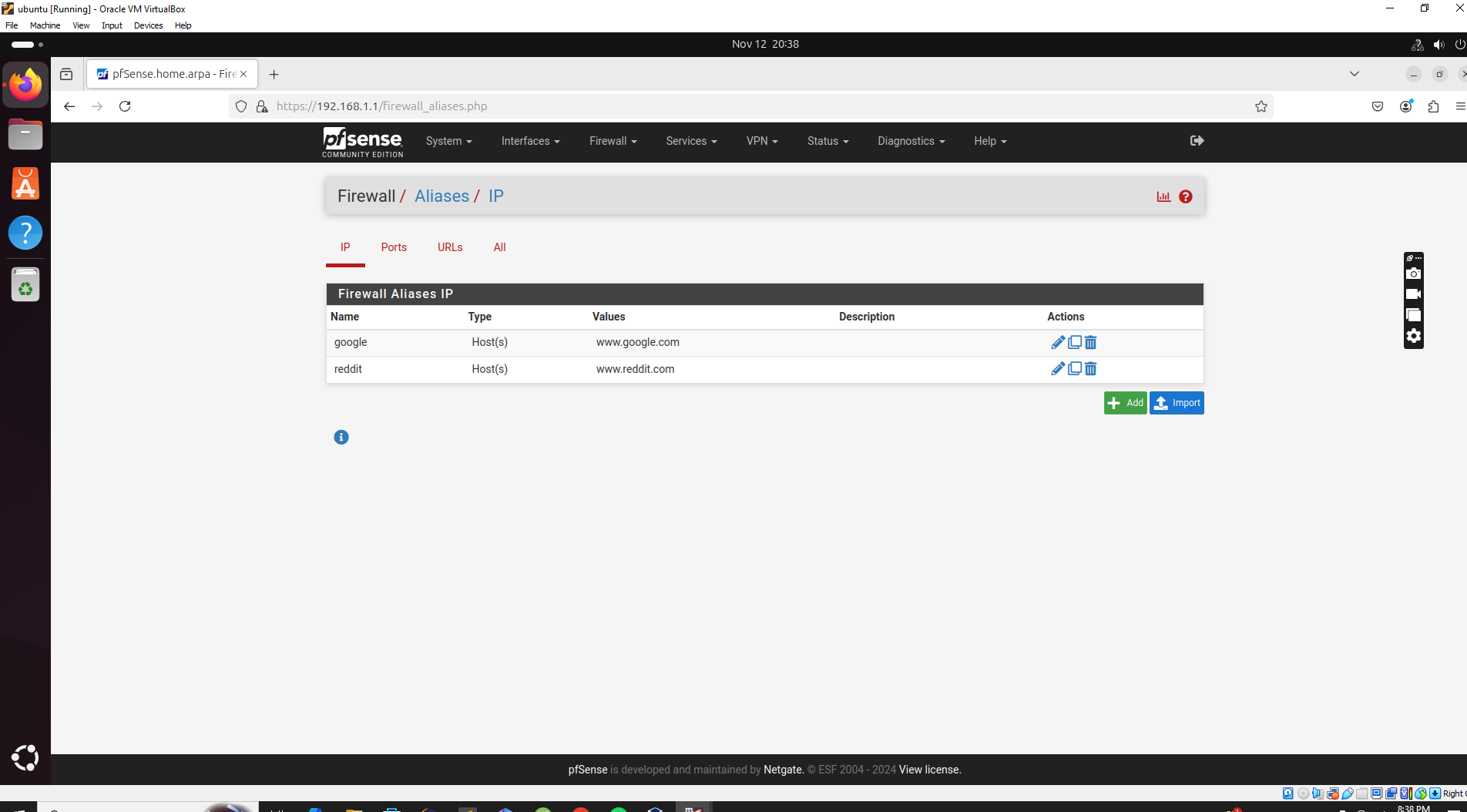
**LAN Side:**

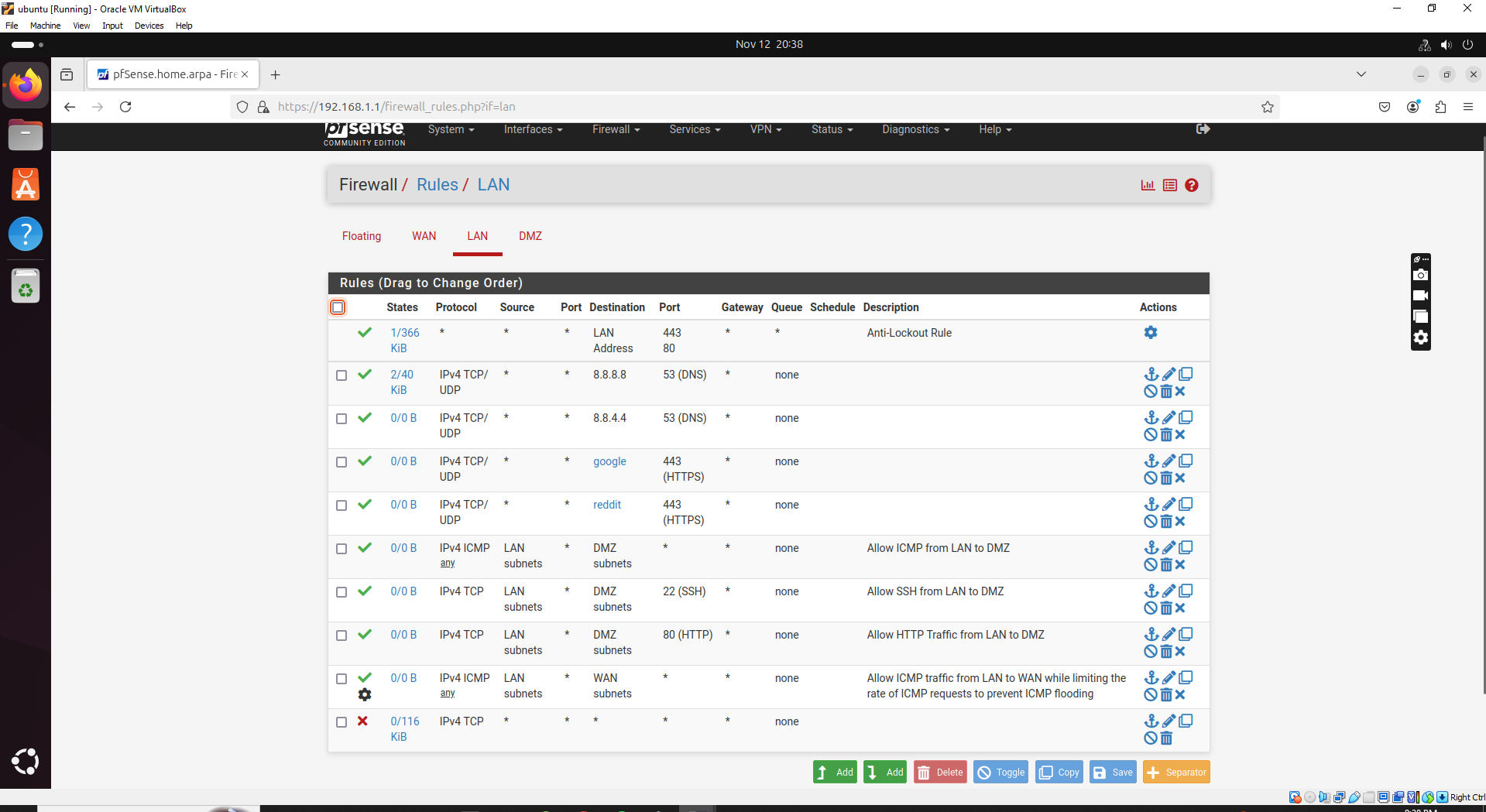
Block traffic from LAN to DMZ except ICMP and SSH for administration purposes. Allow port 80 to access the web server as well.

Allow ICMP (ping) traffic from the LAN network to the WAN network while limiting the rate of ICMP requests to prevent ICMP flooding.

Allow DNS (port 53) traffic from the LAN network to specific DNS servers like 8.8.8.8 and 8.8.4.4 on the Internet.

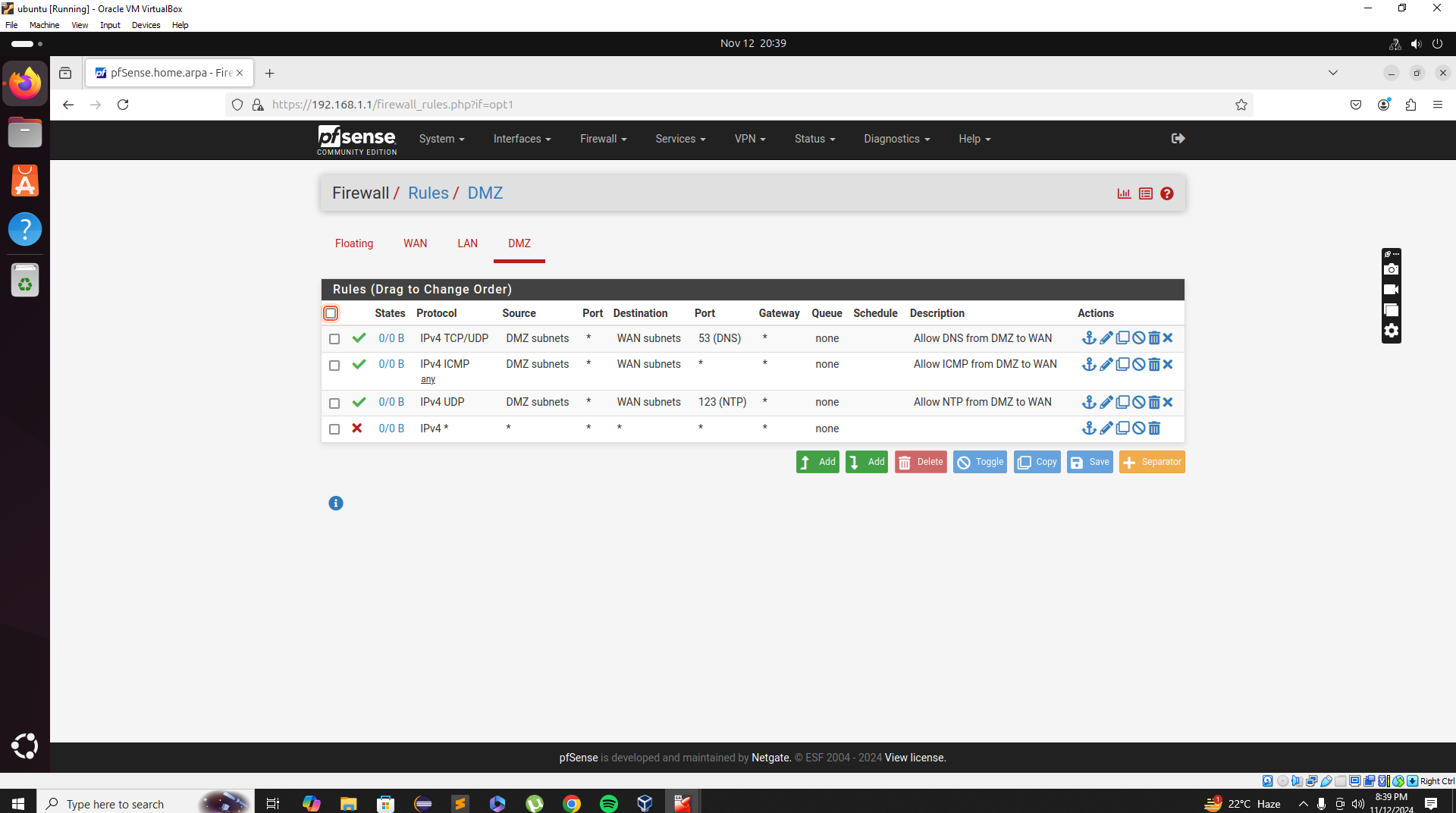
Allow access to limited number of Websites from LAN; Block everything else



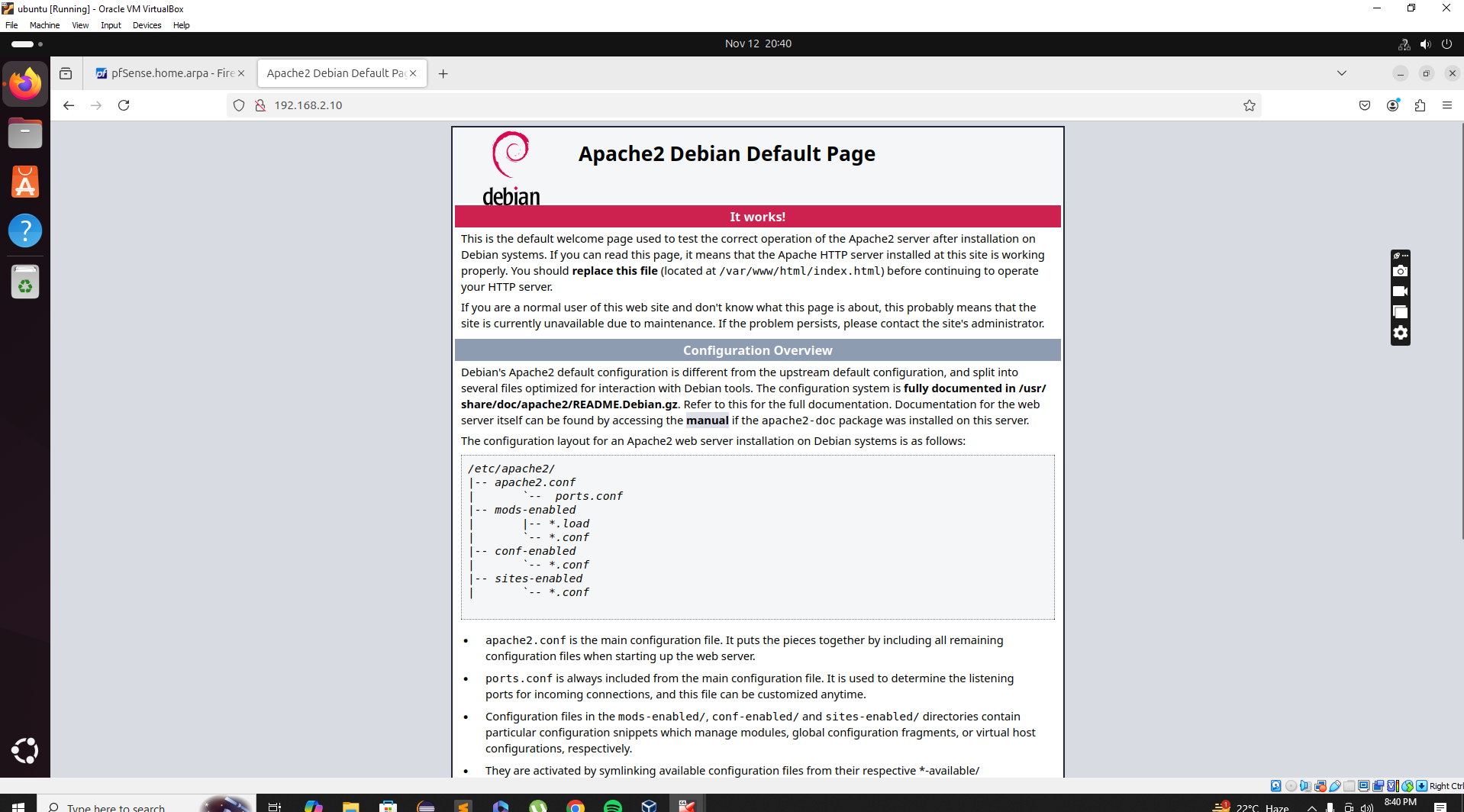


**DMZ Side:**

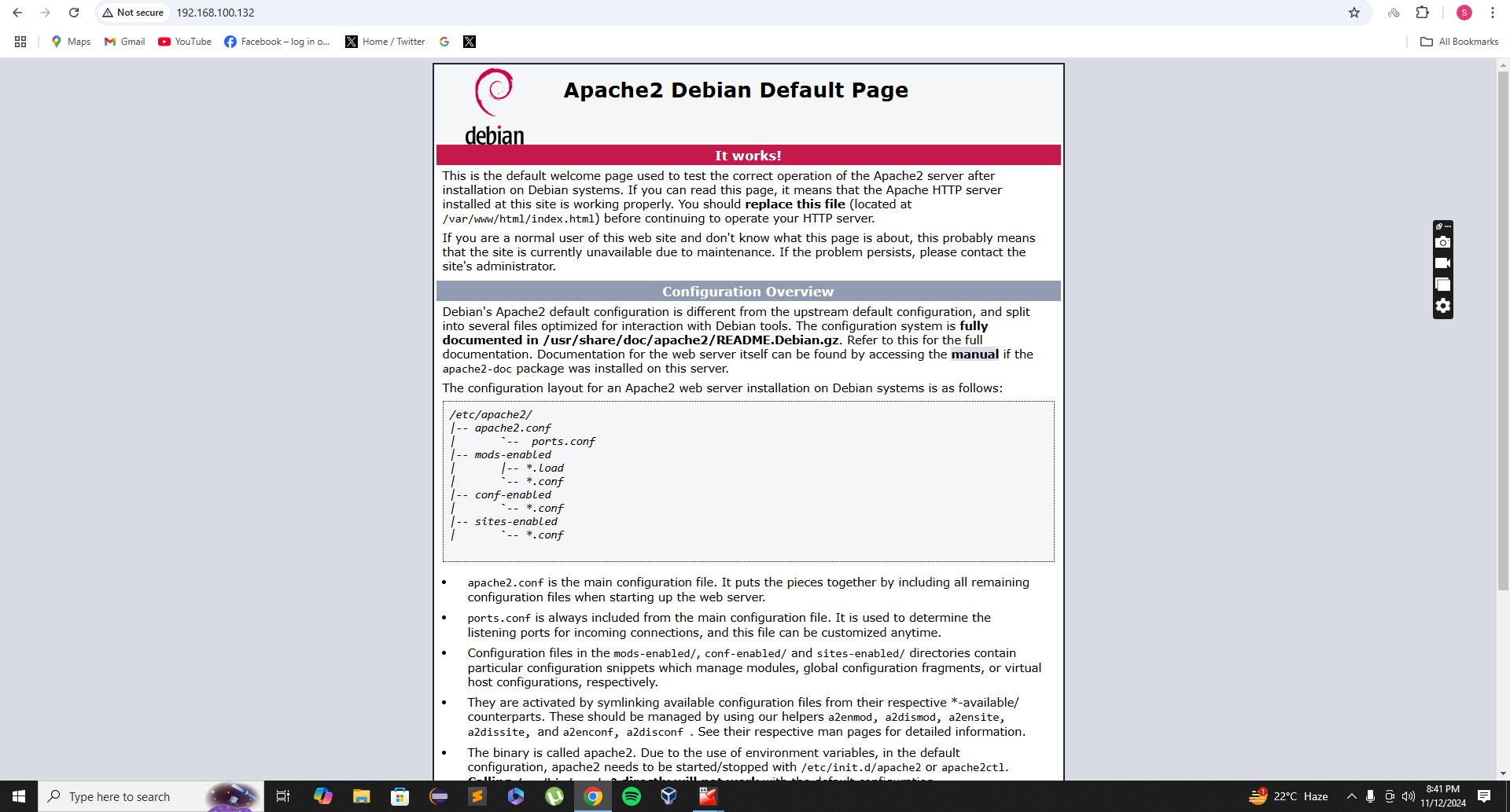
Allow traffic from DMZ to WAN on ports: 53, ICMP and 123 (NTP).



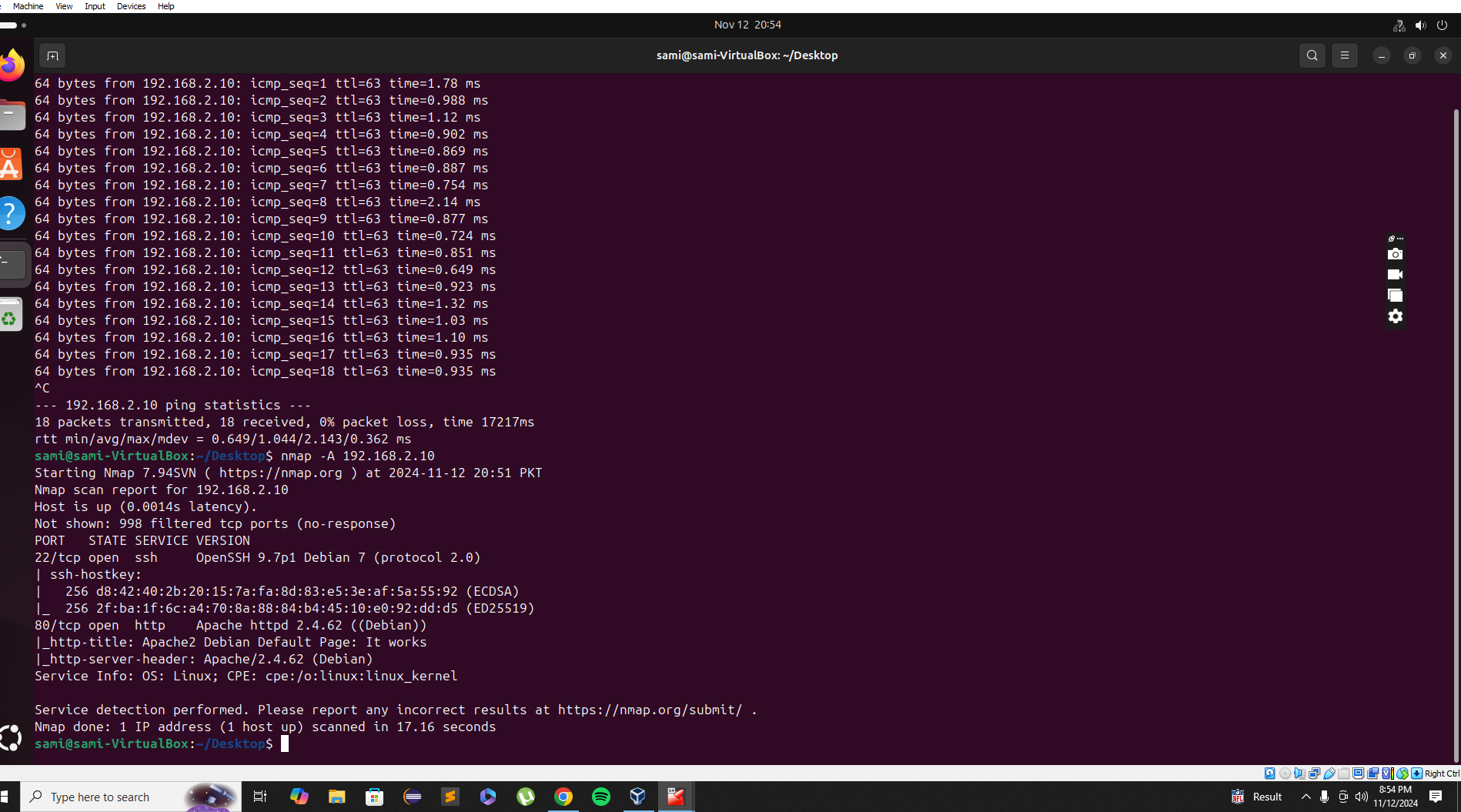
**Access Web Server From LAN:**

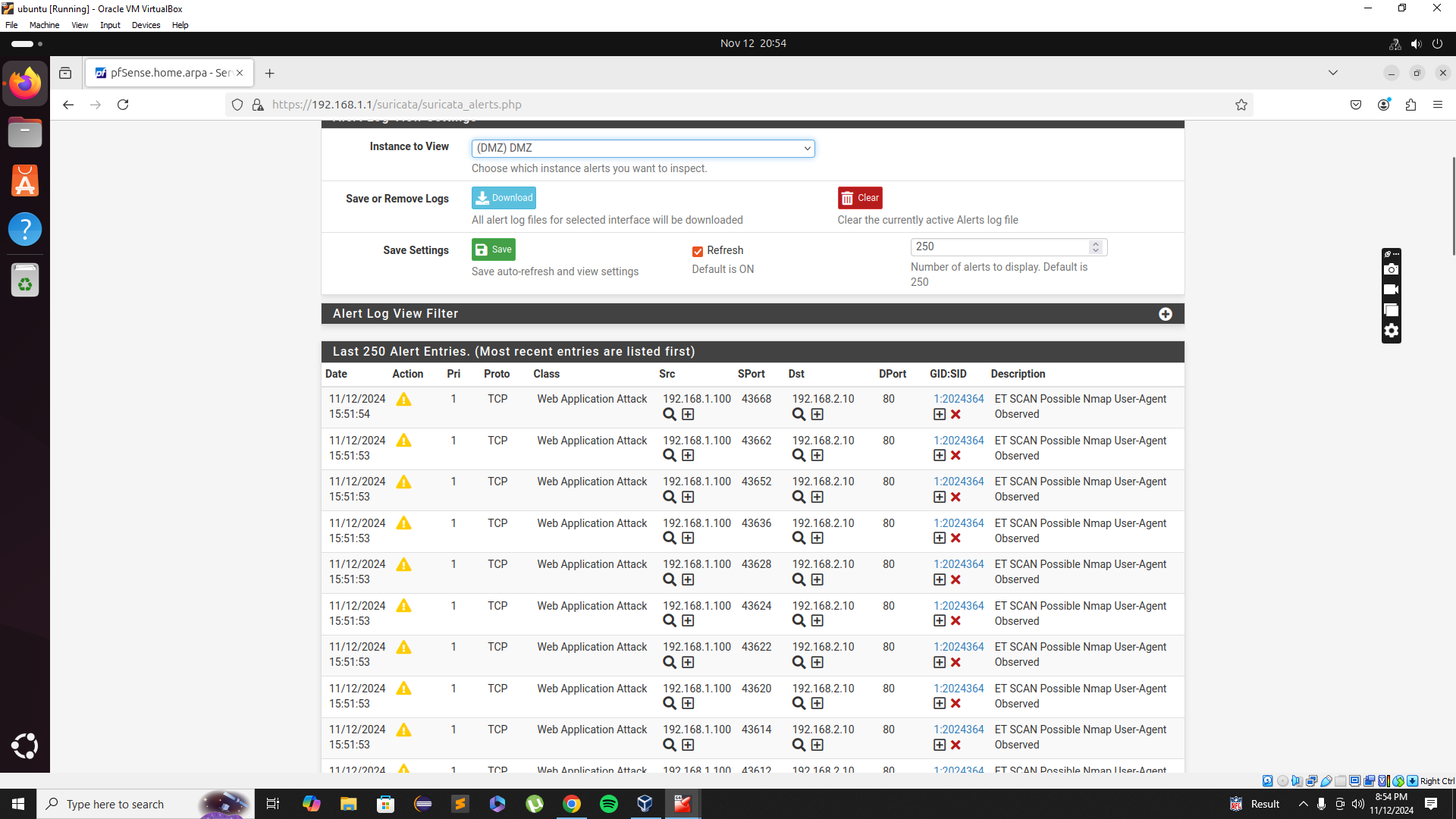


**Access Web Server From Internet:**



**Suricata Alert Logs:**





**Issues Faced:**

Had a lot of difficulties for generating the Suricata alerts.

The only limited websites can be accessed from LAN rule is working sometimes and not working sometimes so that was a headache.

Configuring the Pfsense and DMZ.