Stando al penultimo screen ci sevono 3 macchine
1. DVWA di metasploit
2. Kali per scansioni
3. Pfsense (in mezzo alle due reti) - con 3 interfacce di rete, una connessa a DVWA e una a Kali e l'altra usata come webgateay (NAT)

3 Interfacce
1 em0 - NAT (o bridge) - Da configurare come WAN (con DHCP)
2 em1 - Rete solo host 1 -> 192.168.56.1/24 -> IP pfsense 192.168.56.111 -> verso DVWA 192.168.56.100

3 em2 - Rete solo host 2 -> 192.168.32.1/24 -> IP pfsense 192.168.32.150 -> verso Kali - Scan 192.168.32.120

---

kali

auto eth0
iface eth0 inet static
address 192.168.32.120
gateway (IP di Pfsense) 192.168.32.150
netmask 255.255.255.0

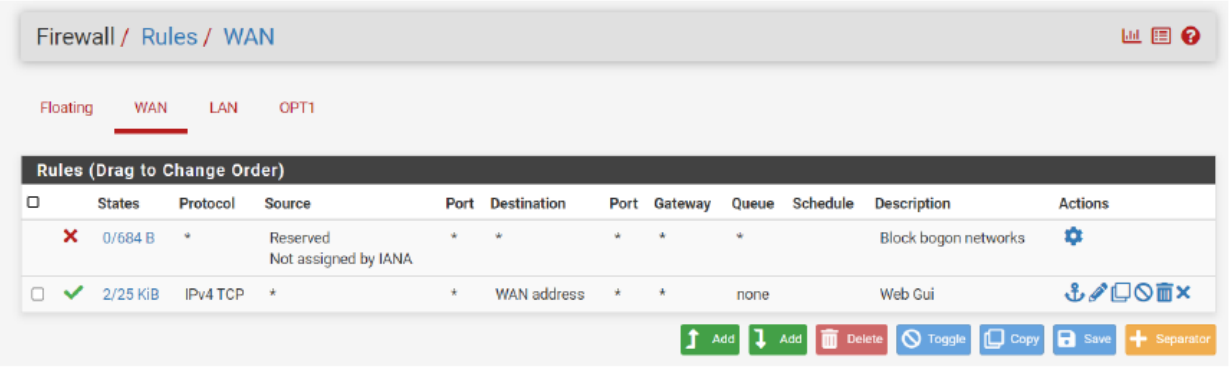
DVWA

auto eth0
iface eth0 inet static
address 192.168.56.100
gateway (IP di Pfsense) 192.168.56.111
netmask 255.255.255.0

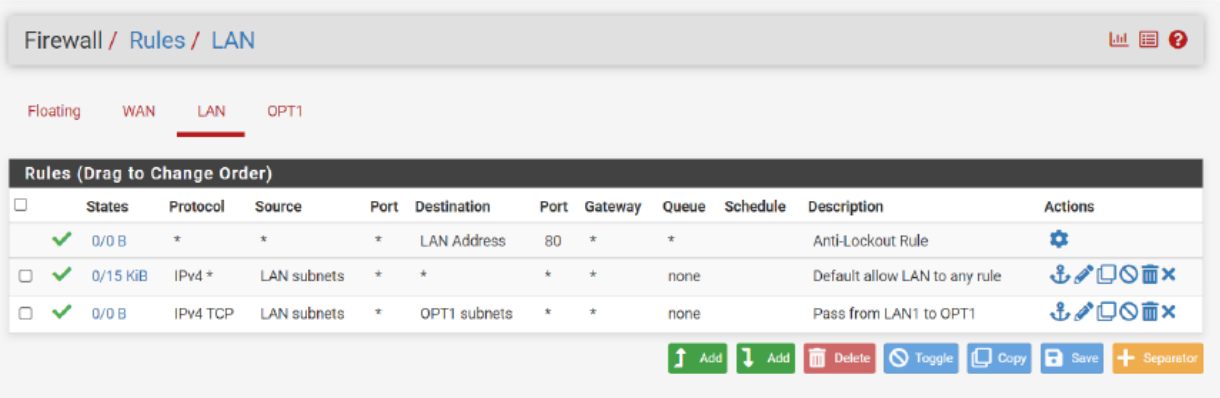
Una volta impostate le interfacce e gli IP statici (ad esclusione della WAN che essendo impostata su una scheda NAT o bridge deve stare sotto al DHCP)
bisogna disabilitare temporaneamente il filtraggio dei pacchetti mediante il comando

pfctl -d

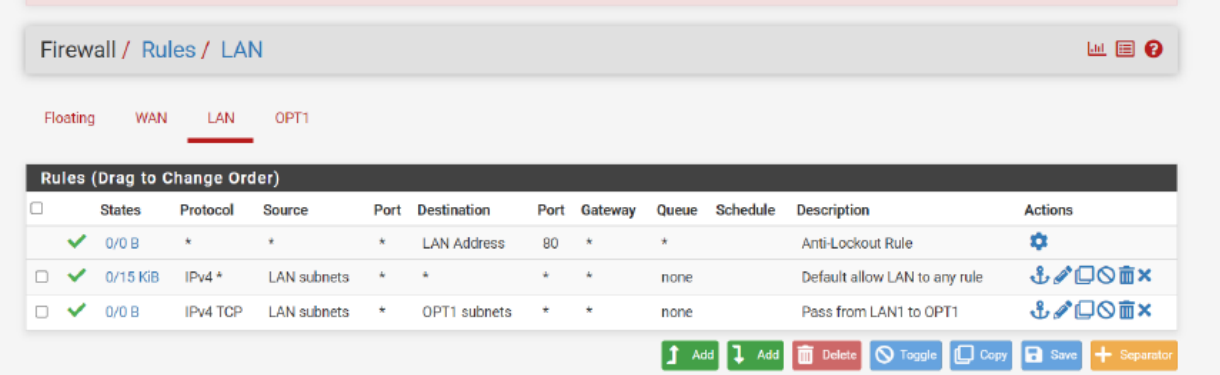
Questa è solo una soluzione temporanea per accedere alla webgui, non è consigliabile mantenere attivo questo parametro,
pertanto è necessario abilitare le connessioni su porta 80 verso gli indirizzi della scheda WAN



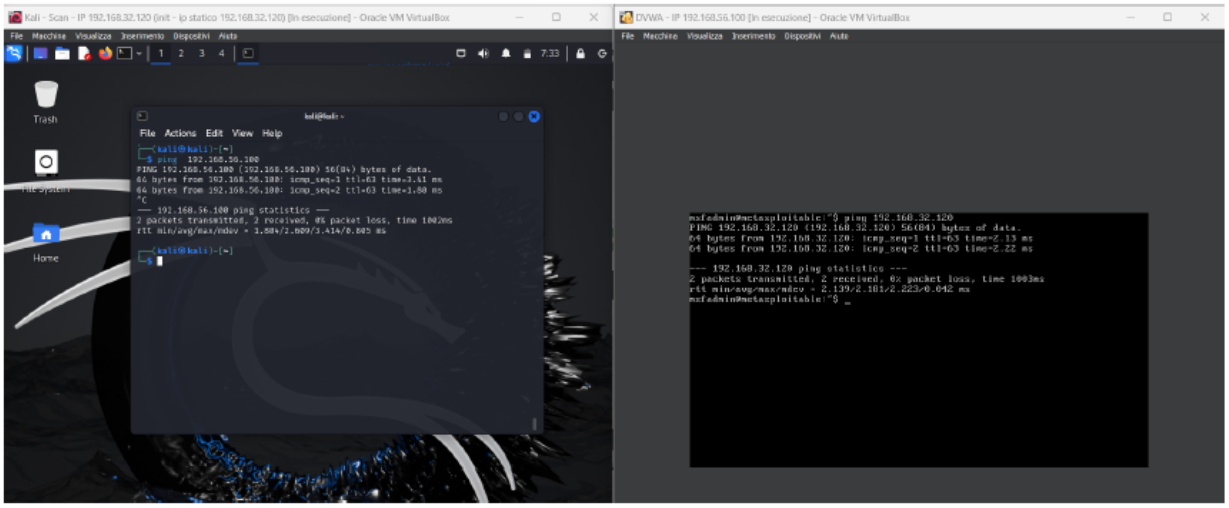
Di seguito lo stato delle regole per l'interfaccia LAN (quella che si collega a DVWA)



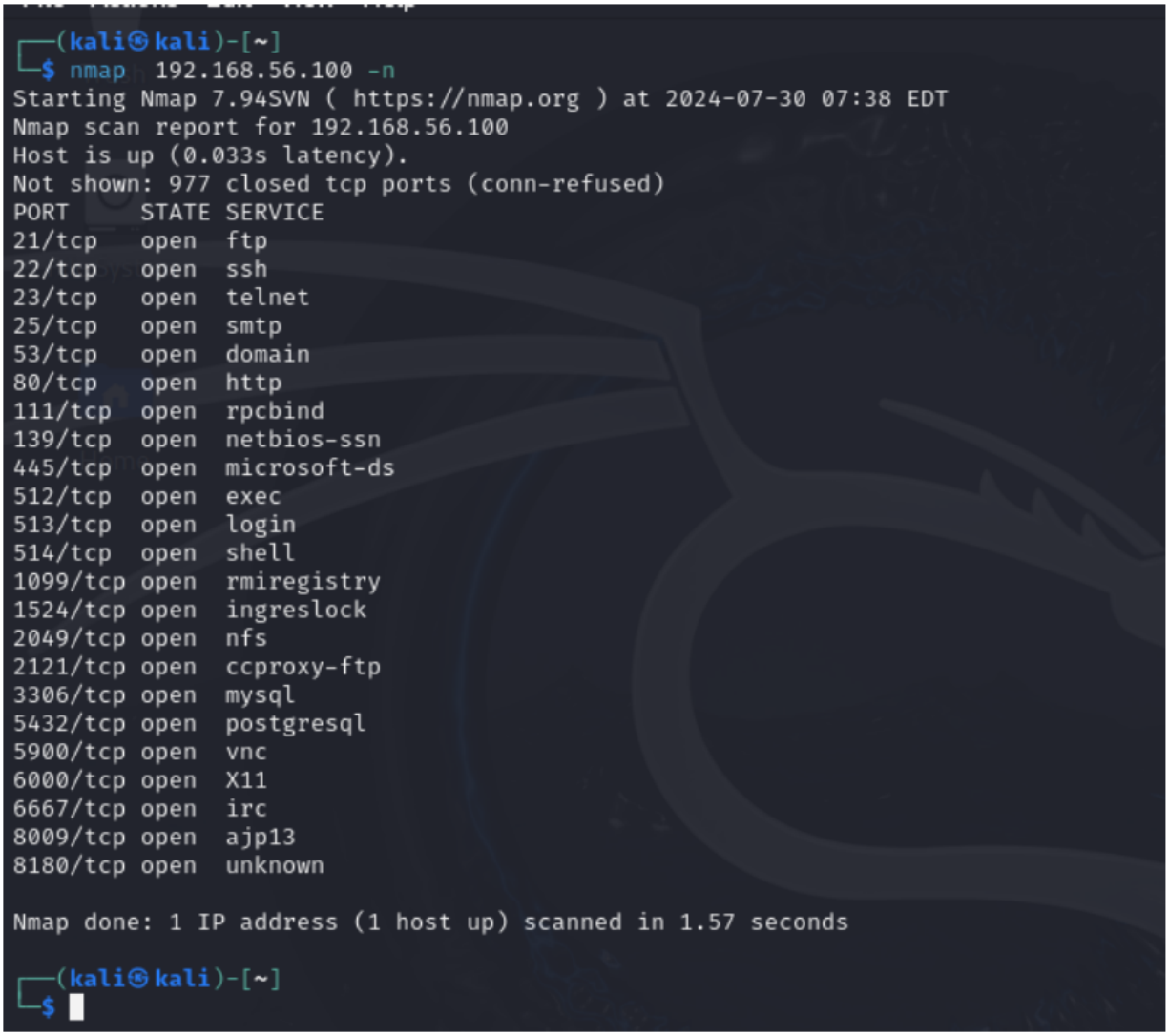
Ora invece quelle sull'interfaccia OPT1 (collegata con la Kali)



Le due macchine di fatto riescono a raggiungersi

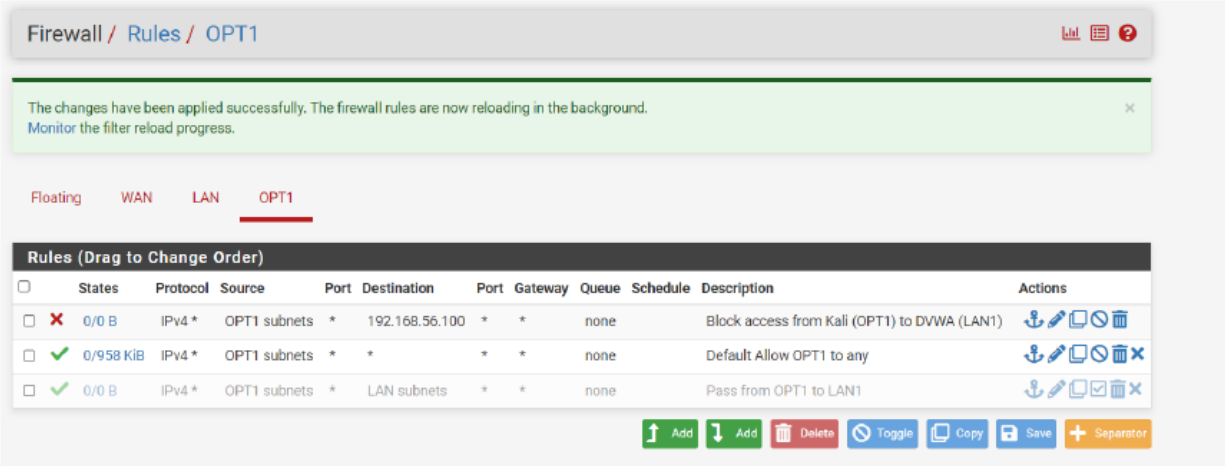


Ora testiamo un Nmap da Kali verso DVWA



Ora modifichiamo le regole in modo da inibire il traffico da Kali a DVWA

Prima disabilito la regola "Pass from OPT1 to LAN"
e poi inserisco una regola in "Block" con Source: OPT1 e Dest: 192.168.56.100
Avrei potuto anche inserire una regola più generica come Dest: LAN, ma in questo caso è giusto per dare un'evidenza maggiore del blocco specifico verso una specifica macchina.



Ricorda che la regola di blocco va inserita per prima, altrimenti il firewall matcha prima quella any to any e non andrebbe a bloccare il traffico

Ora non c'è più connessione