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

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,

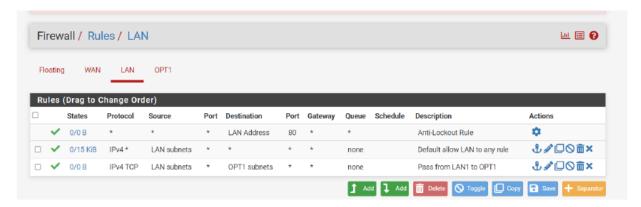
pertanto è necessario abilitare le connessioni su porta 80 verso gli indirizzi della scheda WAN



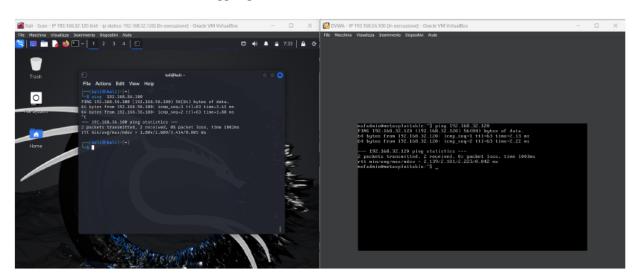
Di seguito lo stato delle regole per l'interfaccia LAN (quella che si collega a DVWA)



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



Le due macchine di fatto riescono a raggiungersi

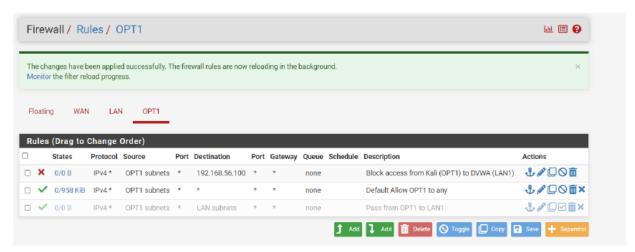


Ora testiamo un Nmap da Kali verso DVWA

```
-(kali⊕kali)-[~]
└$ nmap | 192.168.56.100 -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 07:38 EDT
Nmap scan report for 192.168.56.100
Host is up (0.033s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT
        STATE SERVICE
21/tcp
        open ftp
22/tcp
        open ssh
23/tcp
        open telnet
25/tcp
       open smtp
53/tcp
       open domain
80/tcp
       open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
   (kali⊕kali)-[~]
```

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

```
File Actions Edit View Help

(kali® kali)-[~]

snmap 192.168.56.100 -n

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 07:52 EDT

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds

(kali® kali)-[~]

ping 192.168.56.100

PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.

^C

192.168.56.100 ping statistics —

23 packets transmitted, 0 received, 100% packet loss, time 22513ms

(kali® kali)-[~]

(kali® kali)-[~]
```