CREAZIONE POLICY PFSENSE

1.RICHIESTE

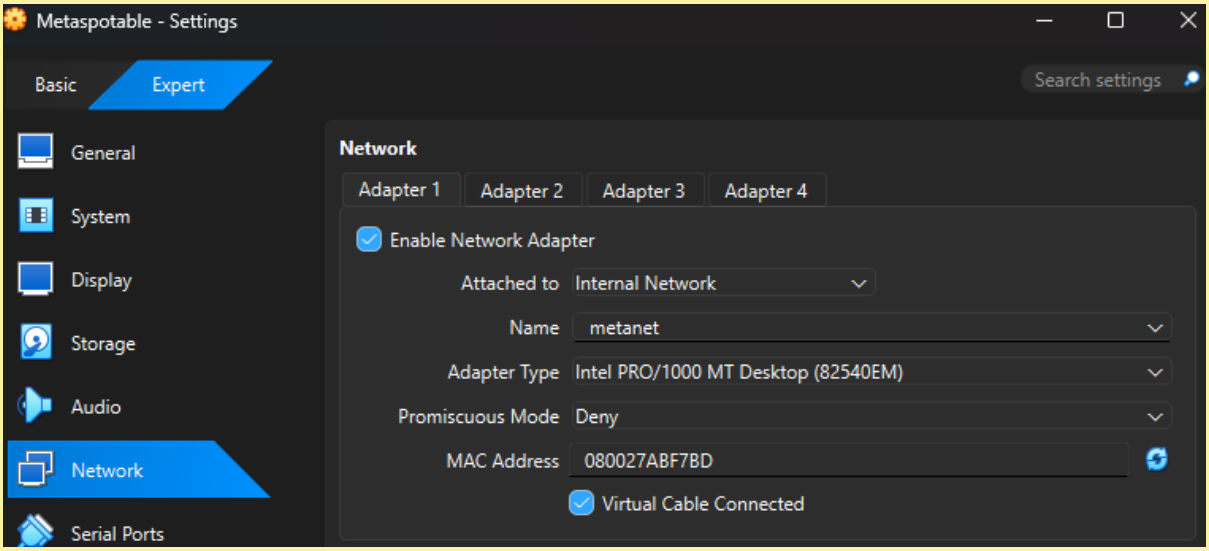
- vm di pfSense dove si vedono le 3 schede di rete e gli ip associati
- 3 screenshot del pannello di pfSense dal browser della kali:
- Firewall rules WAN,
- Firewall rules LAN,
- Firewall rules OPT1,
- browser della Kali che apre la pagina servita della Metasploitable2 (prima dell'applicazione della regola),
- browser della Kali che non riesce più ad aprire la pagina servita della Metasploitable2 (dopo l'applicazione della regola),
- terminale della Kali che riesce a pingare la Metasploitable2 (prima dell'applicazione della regola),
- terminale della Kali che continua a riuscire a pingare la Metasploitable (dopo l'applicazione della regola)

2.SPIEGAZIONE OBBIETTIVO

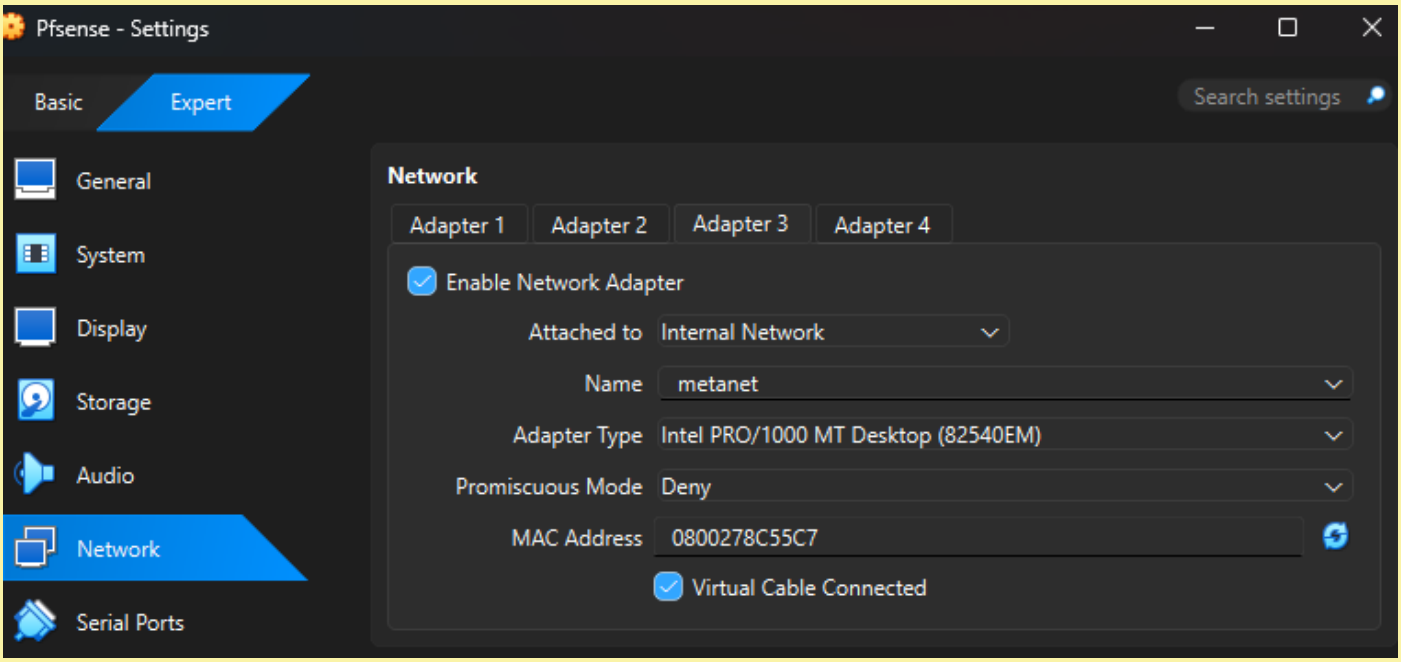
L'obbiettivo è di **bloccare** l'accesso al sito della **Metasploitable** e **DVWA** attraverso una regola **Firewall**(un software o hardware capace di filtrare il traffico dei dati, mantenendo la connessione sicura)ma nello stesso tempo, ricevere risposta dalla macchina attraverso il **ping**

3.PASSAGGI 3.1 CONFIGURAZIONE

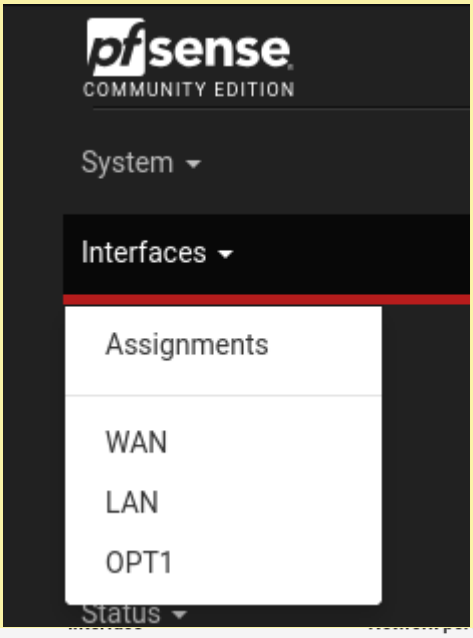
Il primo passaggio è quello di creare una terza interfaccia di rete per la **Metasploitable** , quindi apro le impostazioni Network e seleziono il tipo di rete in *Internal Network e la chiamo "metanet".*

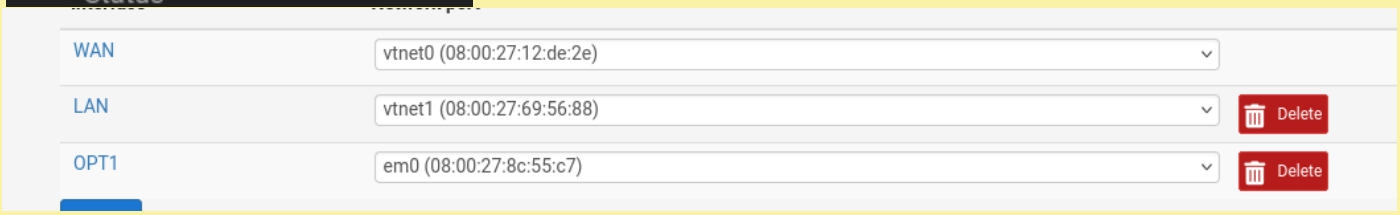


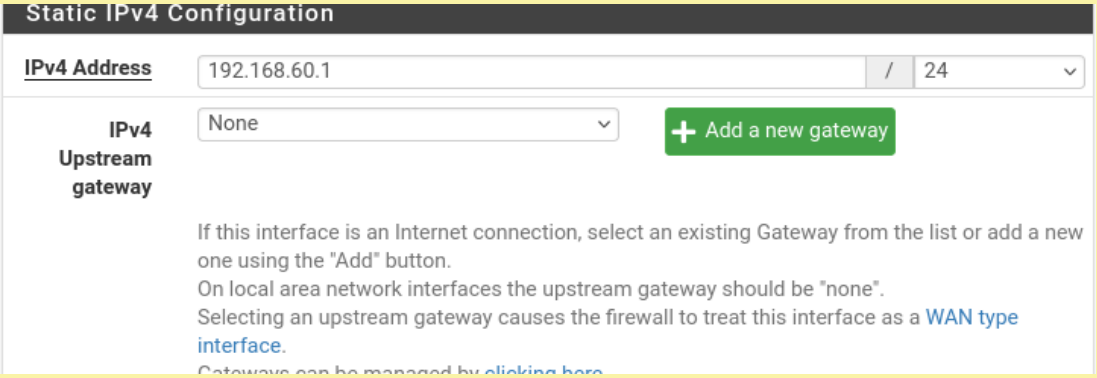
Successivamente apro la sezione *Network della* ***Pfsense****, vado a configurare sull'Adapter 3 la "metanet".*



Una volta fatto,apro la vm di Pfsense e la kali per accedere al sito della Pfsense,dove ho assegnato un'indirizzo IP statico a **OPT1**(Terza Interfaccia).







Una volta assegnato,torno sulla Pfsense e vedo che è stata rilevata.

```
WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.0.28/24
LAN (lan)       -> vtnet1     -> v4: 192.168.50.1/24
OPT1 (opt1)     -> em0        -> v4: 192.168.60.1/24
```

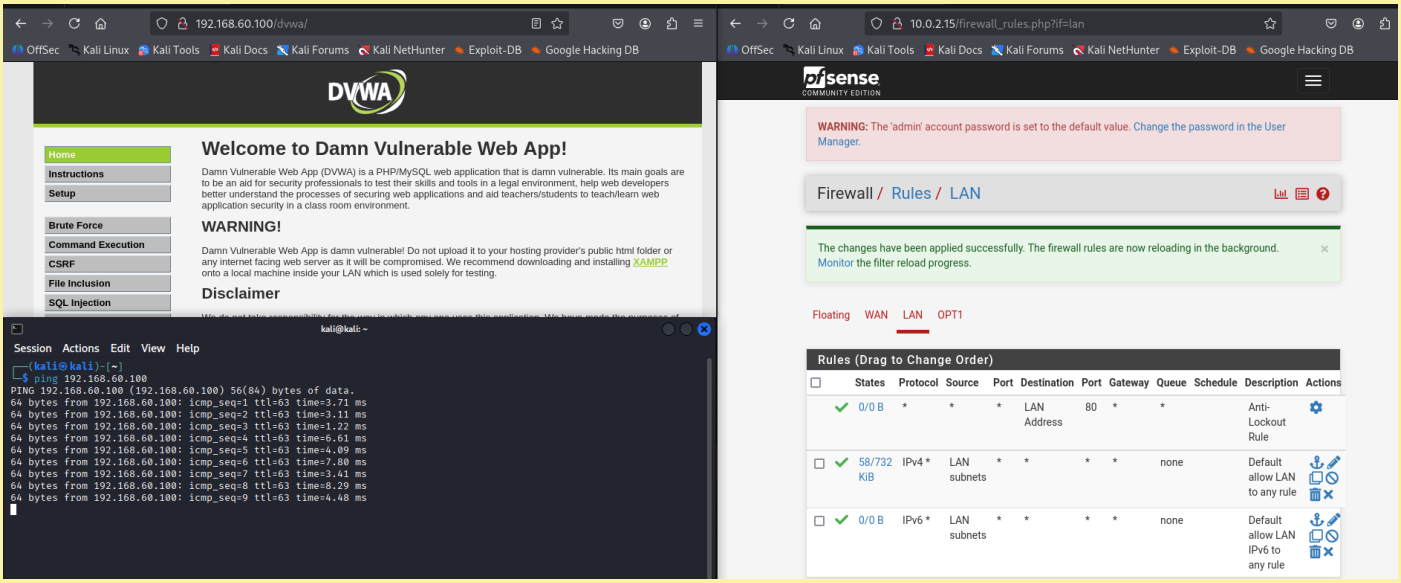
Passo poi alla configurazione della Metasploitable abilitando il servizio di **DHCP.**

```
Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.60.100

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.60.100
Enter the end address of the IPv4 client address range: 192.168.60.200
```

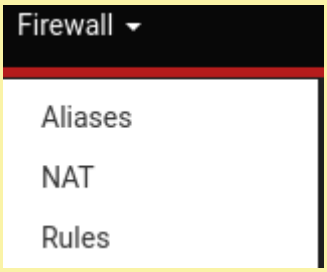
Di seguito apro la Metasploitable per vedere il suo indirizzo IP che consentirà l'accesso al sito Metasploitable2 e di conseguenza al DVWA.

```
eth0: <BROADCAST,MULTICAST,UP
  link/ether 08:00:27:ab:f7:bd
  inet 192.168.60.100/24 brd 1
  inet6 fe80::a00:27ff:feab:f7
```

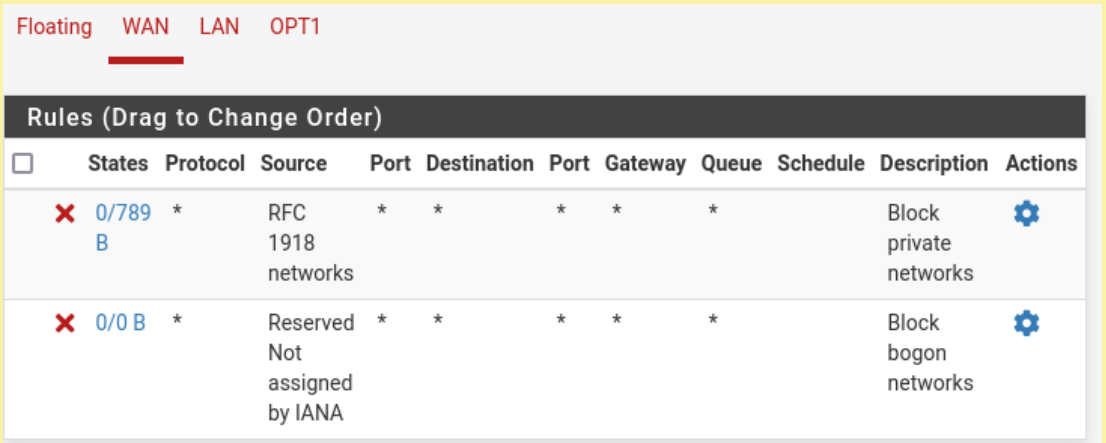
Torno sulla kali e faccio una prova per vedere se senza regola riesco ad accedere al sito e fare il ping.

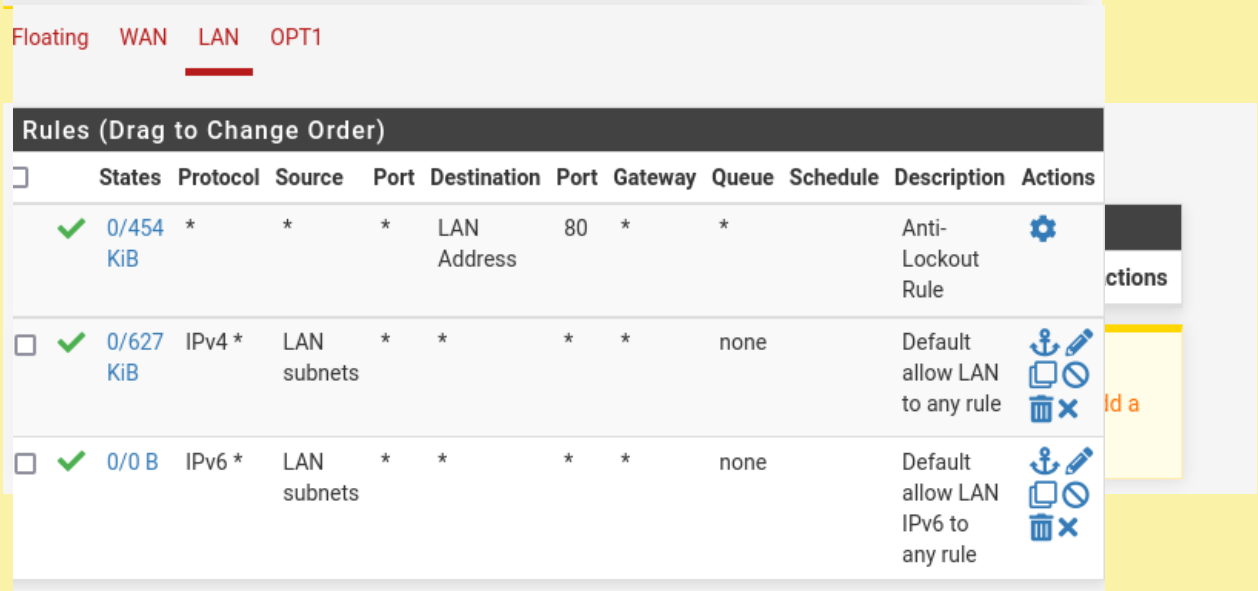


Dato il corretto funzionamento, decido di andare sulla sezione **“Firewall/Rules”** del sito di Pfsense per implementare la regola sul Firewall .



Sono presenti tre sezioni: WAN, LAN, OPT1 .

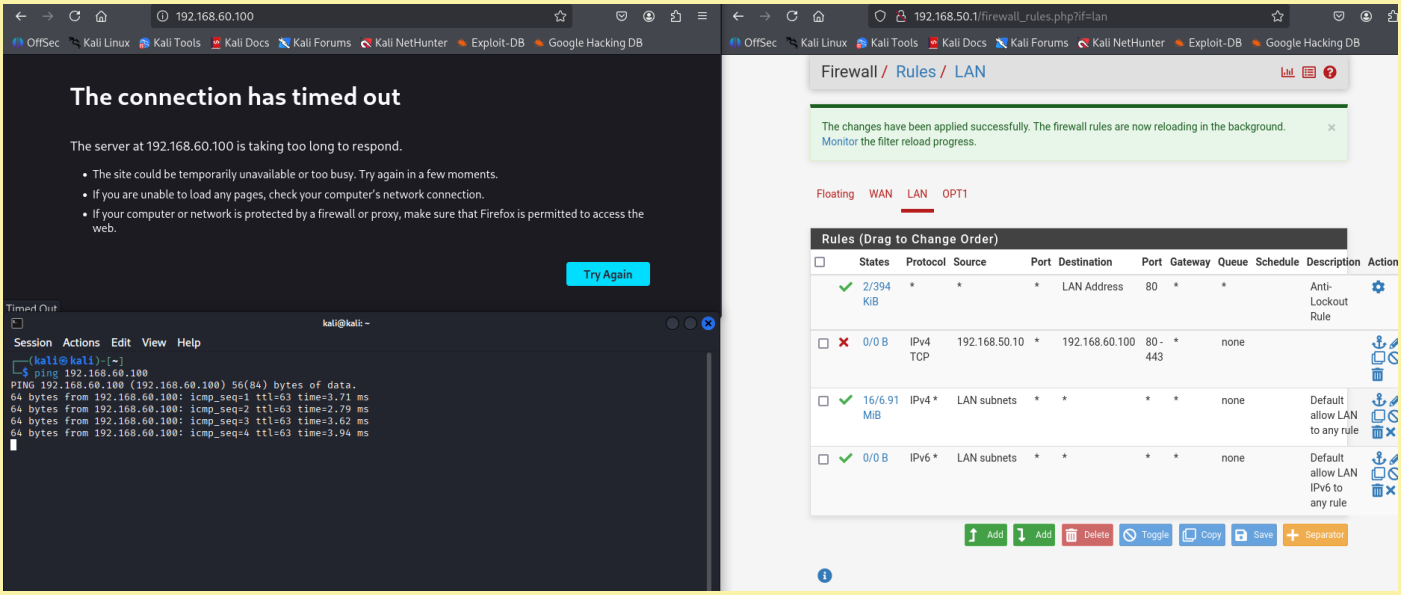




Ho scelto di implementare la regola nella **LAN** perché il pacchetto viene spedito dalla **kali** e all'arrivo nel **punto d'ingresso** del **Firewall,**la regola **negherà** la destinazione(Metasploitable) **e scarterà i pacchetti**.

Quindi dico di bloccare(**Block**) i pacchetti**(TCP)** che partono dalla Kali(**Source Address:192.168.50.10**) la cui destinazione è la Metasploitable(**Destination Address:192.168.60.100**)porta 80(**HTTP**) porta 443(**HTTPS**).

Fatto ciò, sono passato alla prova della regola(bloccare l'accesso al sito ma mantenendo una connessione per il **ping**.)



Mi sono assicurato di aver bloccato solo quel sito aprendo una scheda Amazon con la regola attiva e come mostrato in foto,c'è un corretto funzionamento di quest'ultima.