S3-L5

Creazione reti e regole firewall tramite pf sense

Kevin motti

Overview

Creare 3 reti diverse(LAN, WAN, OPT) utilizzando **pf sense** come router-firewall per collegare **2** LAN in reti diverse e **1** WAN.

Successivamente creare una regola che impedisca alla kali di accedere alla pagina DVWA di meta.

Obbiettivo 1 WAN:

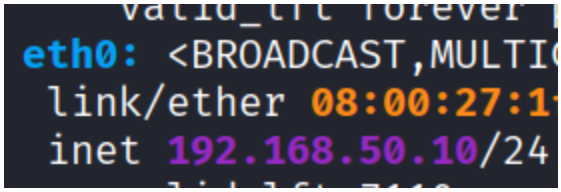
Dentro il terminale di pf sense ho creato una rete WAN utilizzando il servizio DHCP del mio router, che ha assegnato automaticamente l'indirizzo IP.

Obbiettivo 2 kalinet (LAN):

Terminale pf sense:

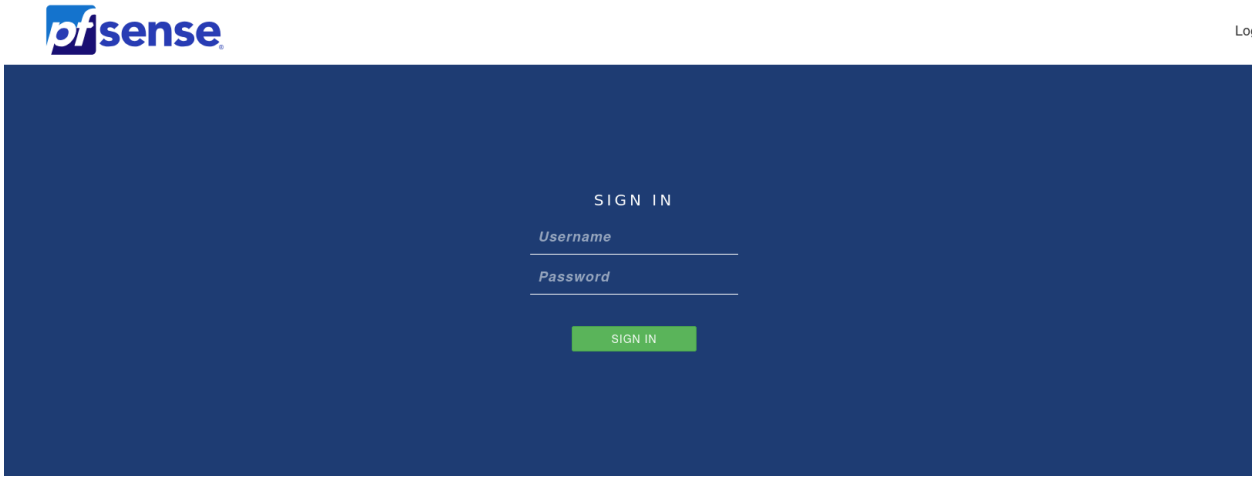
Da terminale ho settato manualmente l'indirizzo IP di pf sense e l'ho impostato come gateway con il seguente indirizzo: 192.168.50.1

Successivamente ho attivato il servizio DHCP per poter assegnare automaticamente l'indirizzo IP privato alla kali. L'indirizzo che è stato assegnato è il seguente:



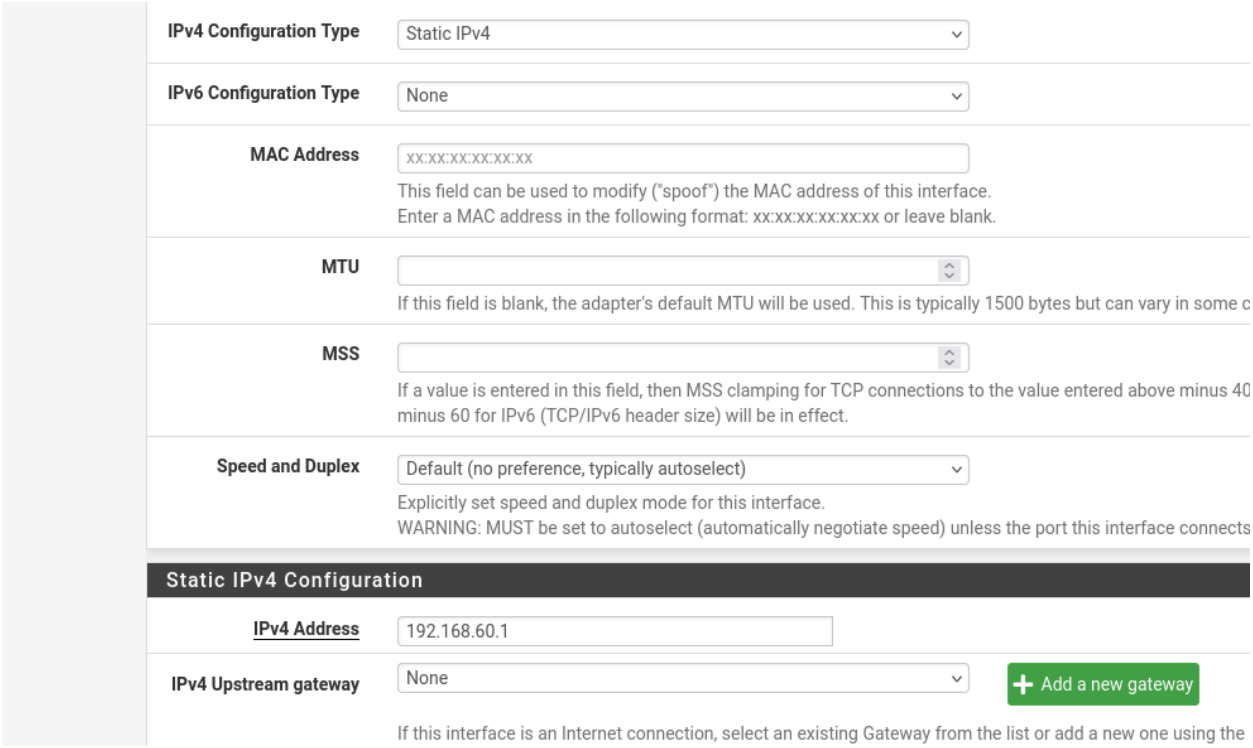
Obbiettivo 3 Creazione della terza rete per la meta:

Aprendo il browser dalla kali inserisco l'IP gateway di pfsense (192.168.50.1) che abbiamo impostato prima, così accedendo alla GUI di setup.



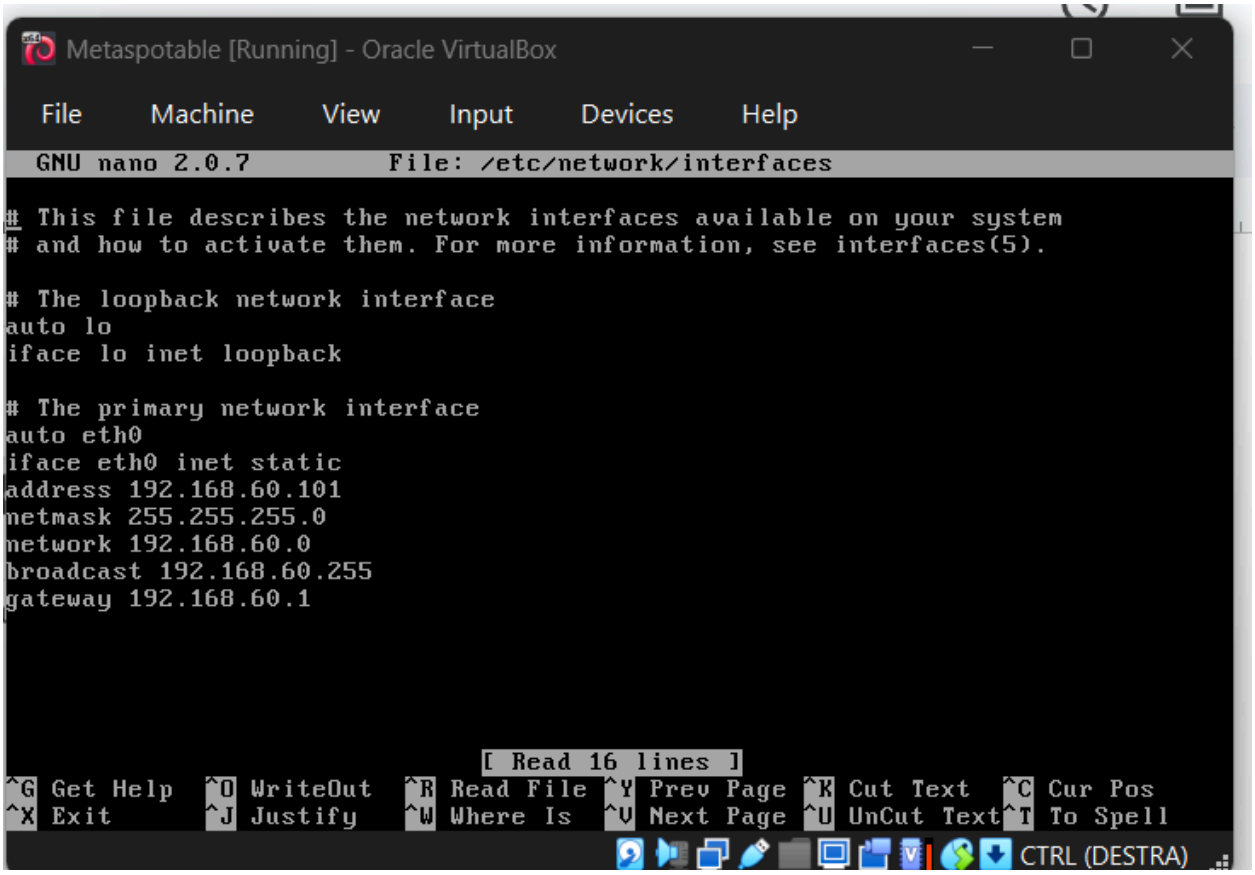
3

Dentro la pagina “interfaces” ho impostato l’indirizzo IP di gateway per questa rete (OPT): 192.168.60.1



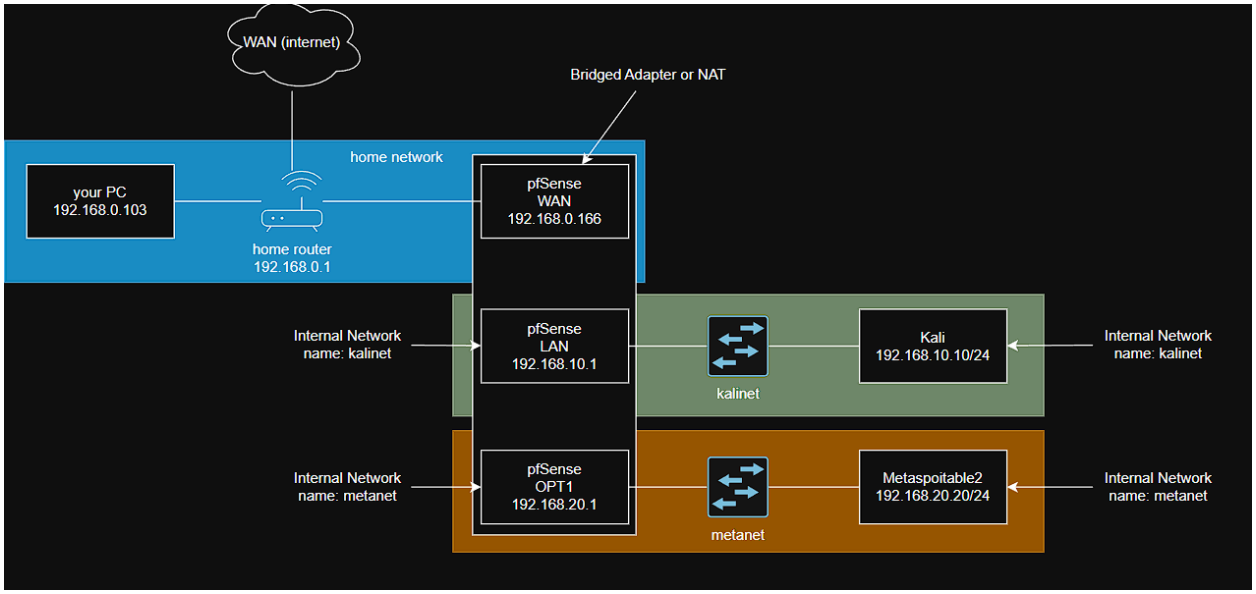
Meta:

Dentro il “pannello” per la configurazione degli IP di meta che ho aperto tramite comando: sudo nano /etc/network/interfaces



Ho impostato l’IP (192.168.60.101), il gateway corretto e il network (192.168.60.0)

Ora che tutte le impostazioni sono state salvate abbiamo 3 reti impostate in questo modo

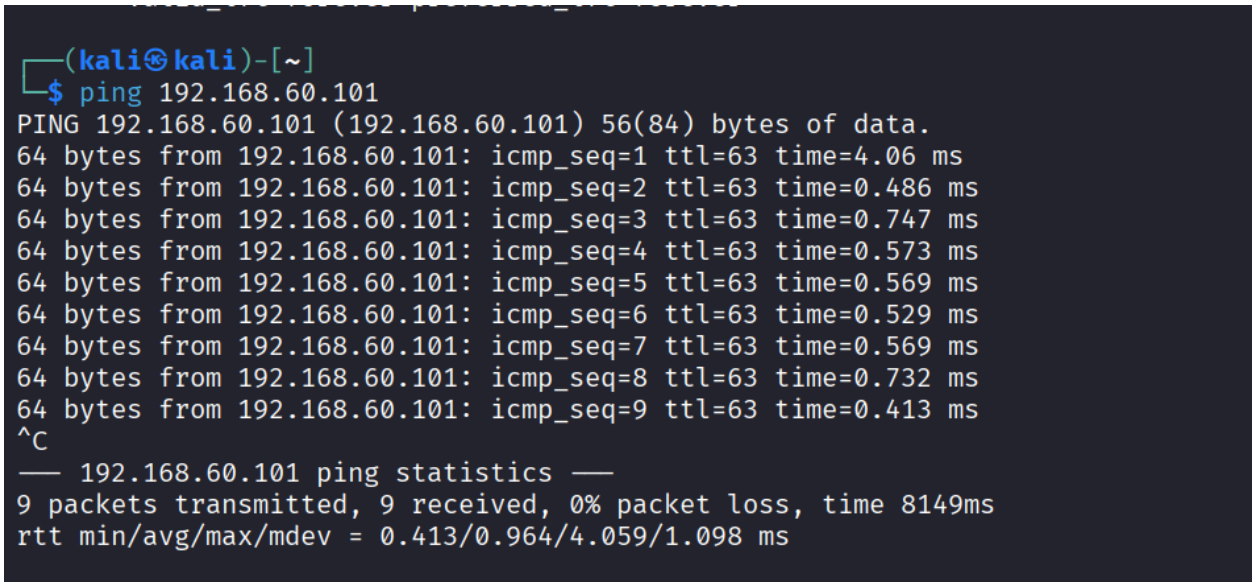


RETE PRIVATA METANET: metasploitable (192.168.60.101) metanet (witch, rete) pf sense “192.168.60.1” (router, firewall)

RETE PRIVATA KALINET: kali (192.168.50.10) kalinet (switch, rete) pf sense “192.168.50.1” (router firewall)

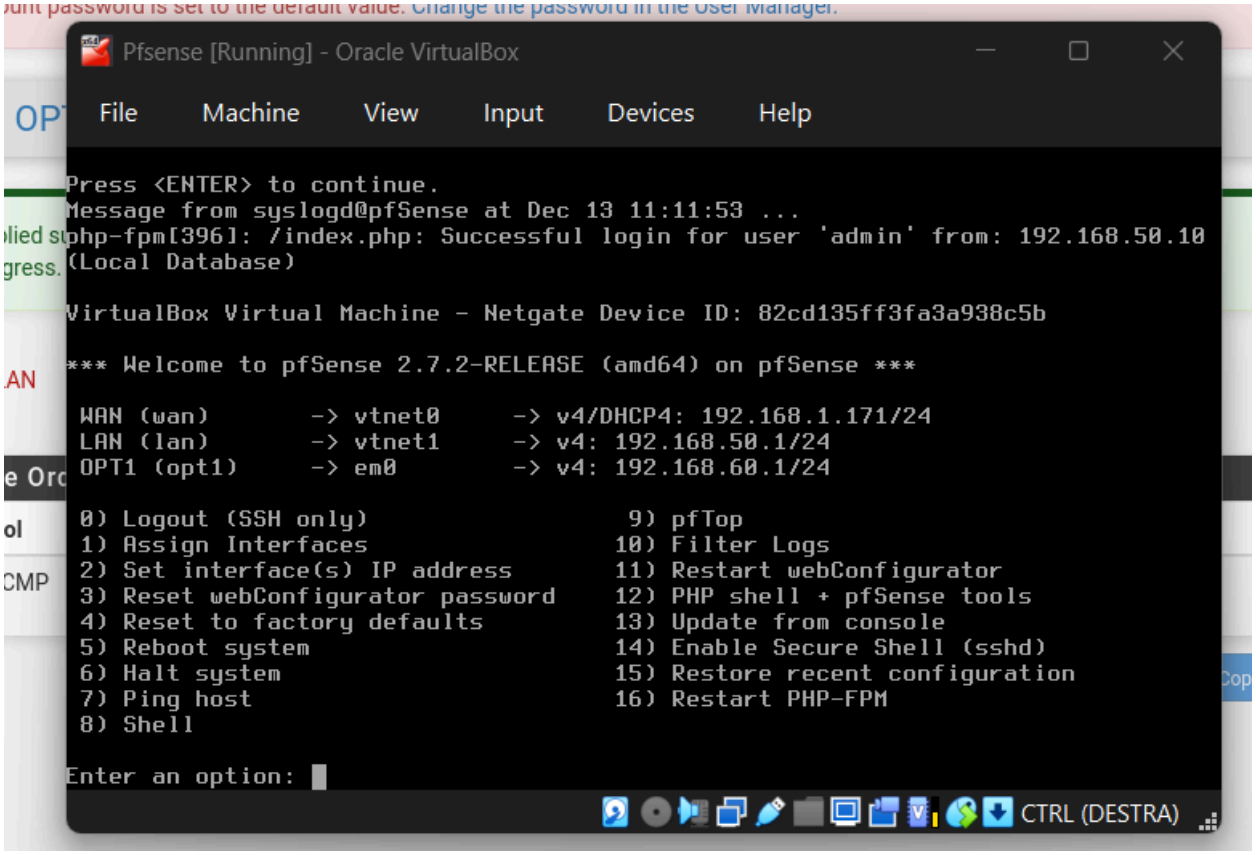
PF SENSE WAN: 192.168.1.171/24 (via DHCP)

Se facciamo una prova di ping dalla kali alla meta:

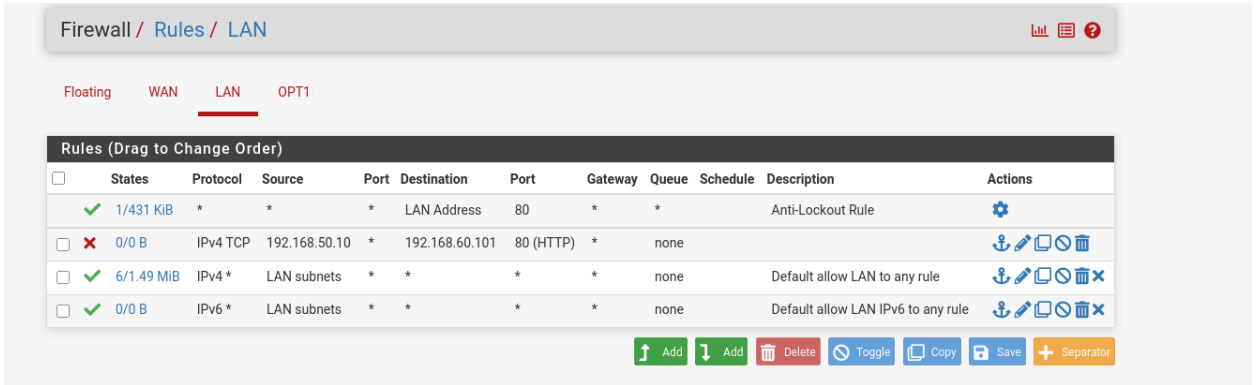


Tutto funziona correttamente.

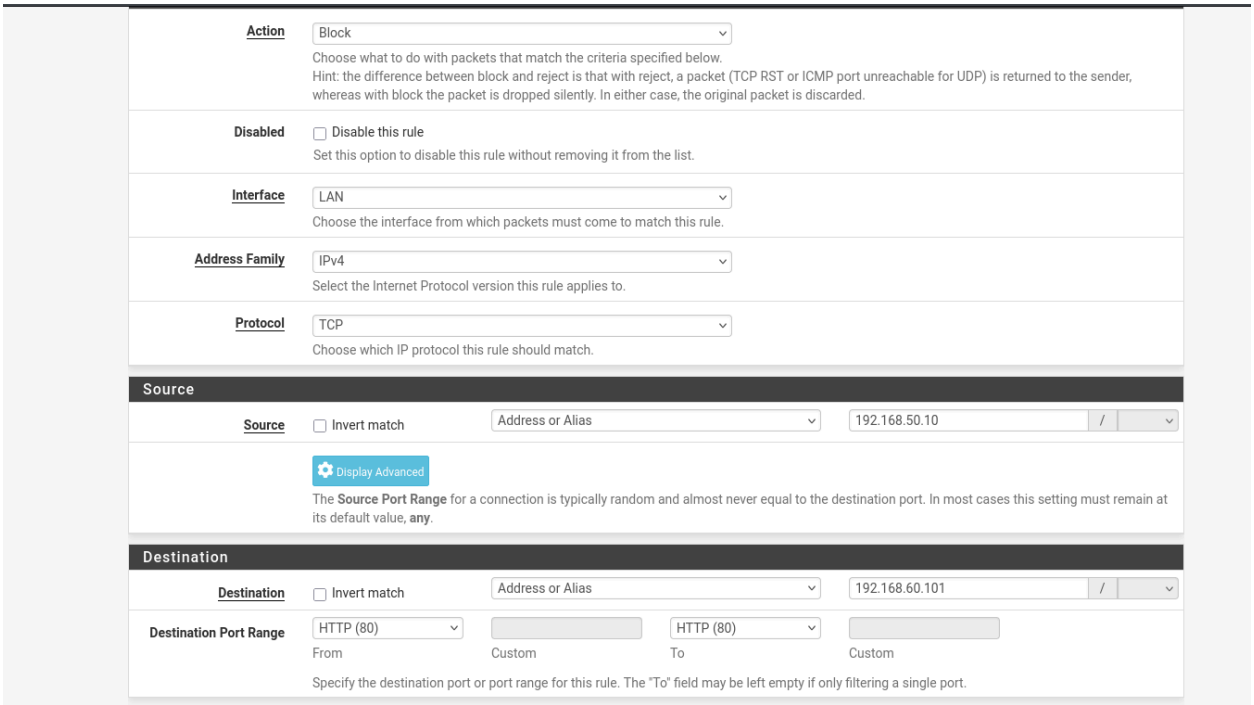
Questa è la visuale da terminale pf sense:



Obbiettivo 4 creazione regola firewall:



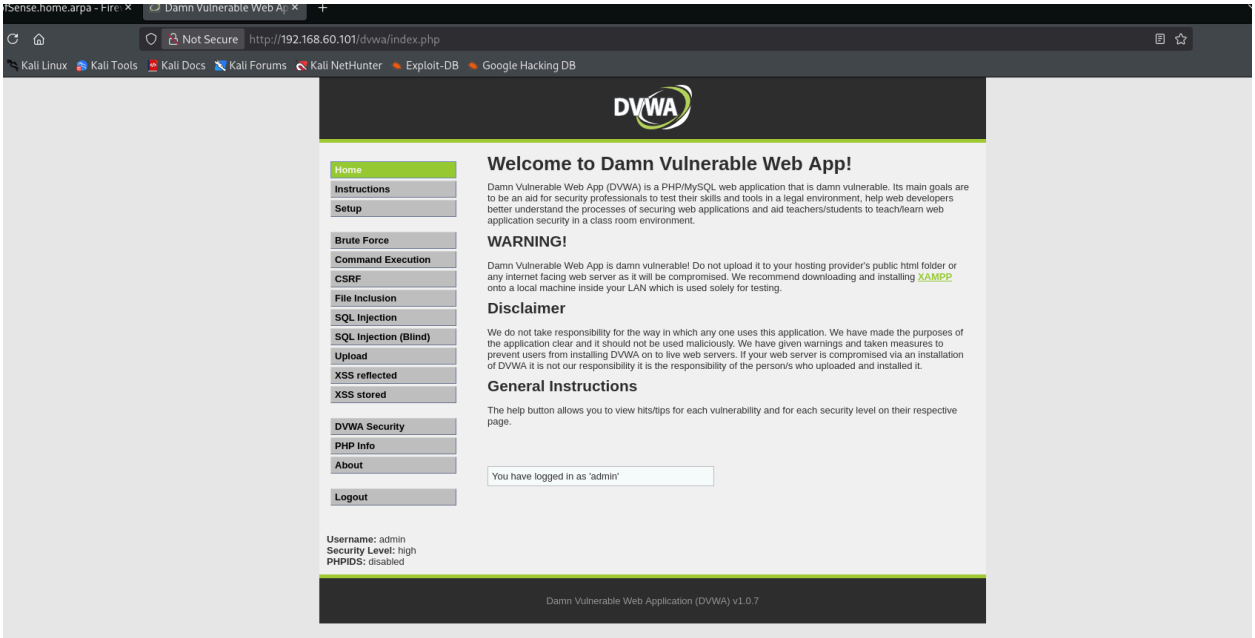
Dentro il pannello delle configurazioni del firewall scelgo di modificare le regole **LAN** (essendo una regola di blocco per la kali) e aggiungo **in cima alla lista** una regola che impedisca alla kali di scambiare protocolli TCP con l'IP di destinazione 192.168.60.101 (meta) alla **porta 80.**



(la posizione delle regole è di fondamentale importanza dato che il firewall le legge dall'alto verso il basso, per questo motivo se la regola di blocco è inferiore nella lista rispetto a una regola che permette il passaggio, la regola di blocco non avrà effetto.)

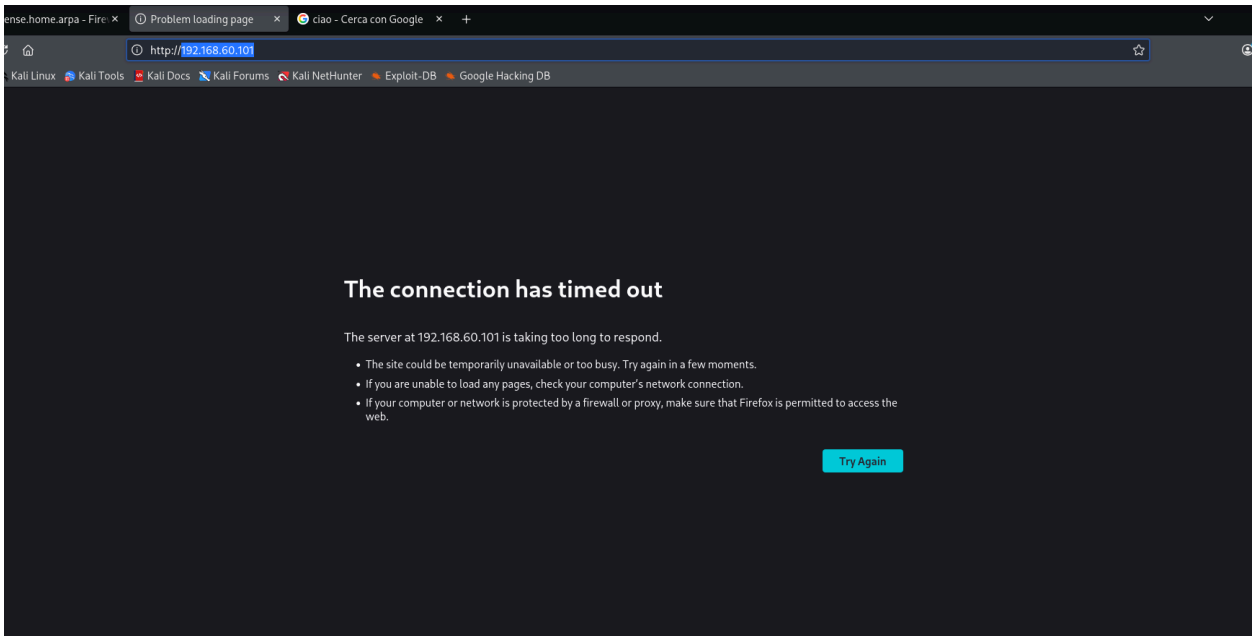
CONCLUSIONE:

Questa è una visuale del **prima** e del **dopo** la regola:



prima si può notare che inserendo nella barra di ricerca del browser di kali l'indirizzo IP della meta (192.168.60.101) arriviamo alla pagina della DVWA che è la pagina a cui vogliamo impedire l'accesso alla kali.

Dopo l'applicazione della regola possiamo vedere come l'accesso a quella pagina ora ci è stato negato.

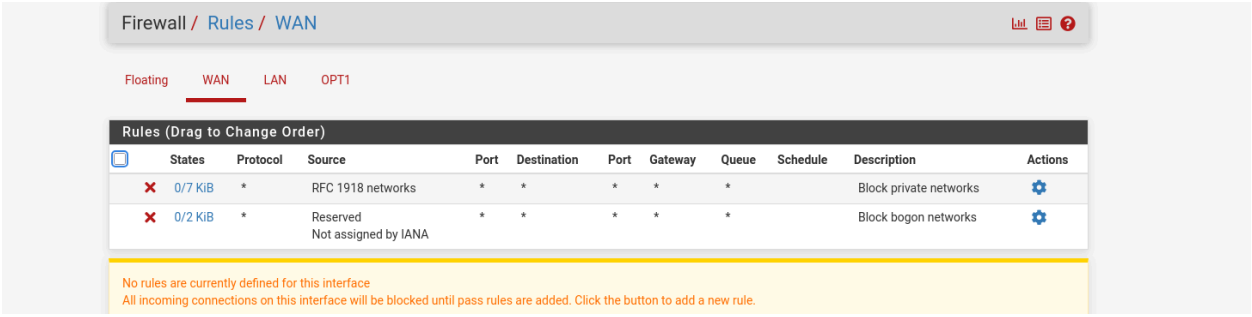


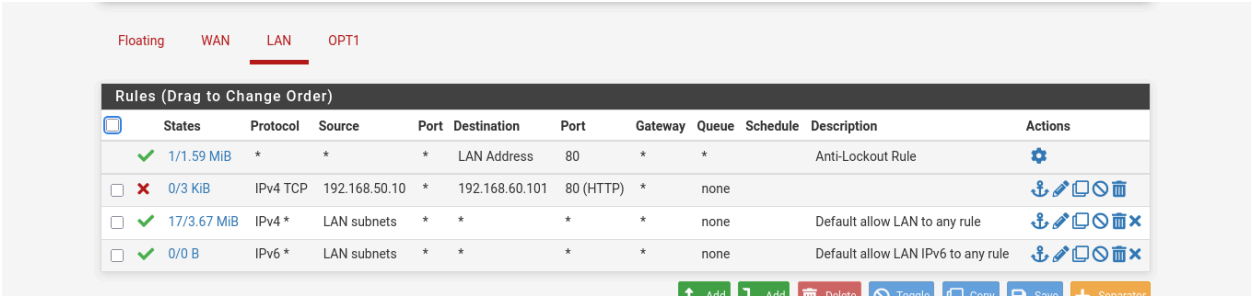
Un ultima prova di ping per confermare che ci sia ancora comunicazione tra le due macchine anche dopo l'applicazione della regola del firewall:

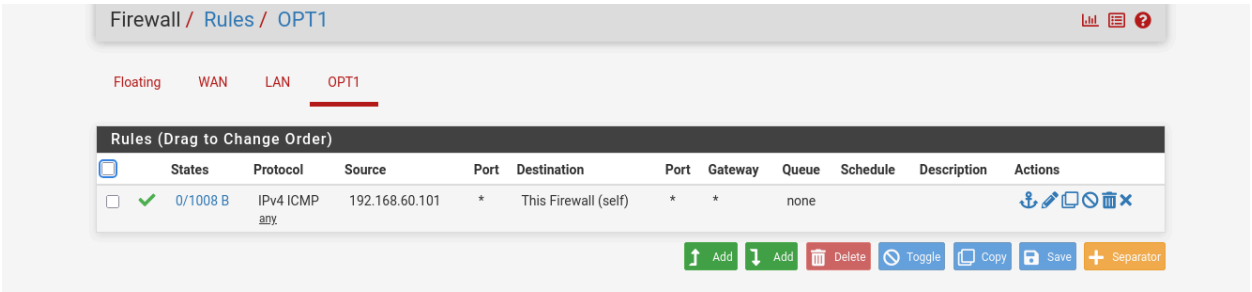
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=0.585 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=0.679 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=0.820 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=0.681 ms
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=0.774 ms
64 bytes from 192.168.60.101: icmp_seq=6 ttl=63 time=0.737 ms
64 bytes from 192.168.60.101: icmp_seq=7 ttl=63 time=0.520 ms
64 bytes from 192.168.60.101: icmp_seq=8 ttl=63 time=0.915 ms
64 bytes from 192.168.60.101: icmp_seq=9 ttl=63 time=0.809 ms
^C
── 192.168.60.101 ping statistics ──
9 packets transmitted, 9 received, 0% packet loss, time 8163ms
rtt min/avg/max/mdev = 0.520/0.724/0.915/0.115 ms
```

Tutto funziona correttamente.

Note aggiuntive:







Queste sono le regole firewall per ogni rete.

Ho aggiunto una regola a OPT1 per permettere al protocollo ICMP di comunicare, in modo da poter testare la comunicazione tra la meta e pf sense.