

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)

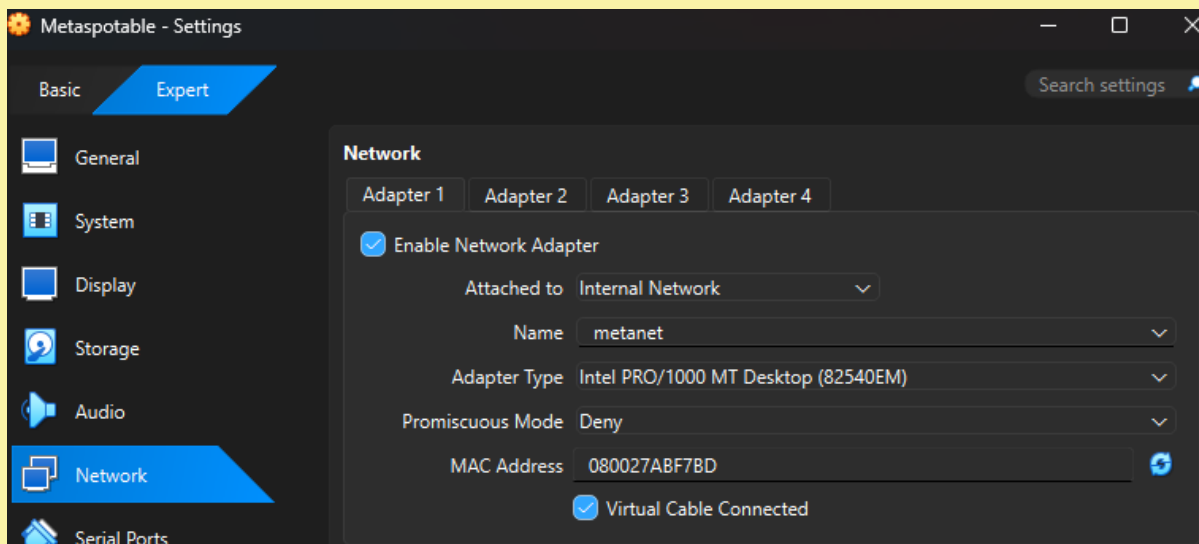
2.SPIEGAZIONE OBIETTIVO

L'obiettivo 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**

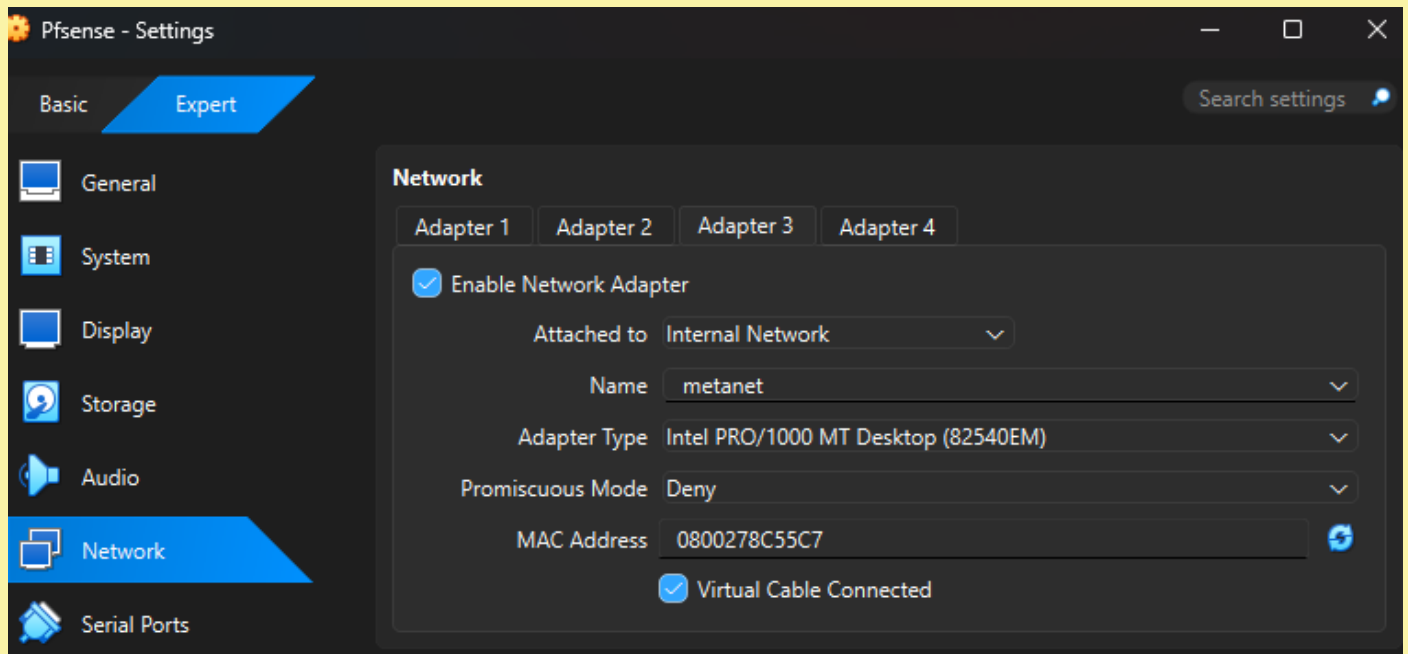
3.PASSAGGI

3.1 CONFIGURAZIONE

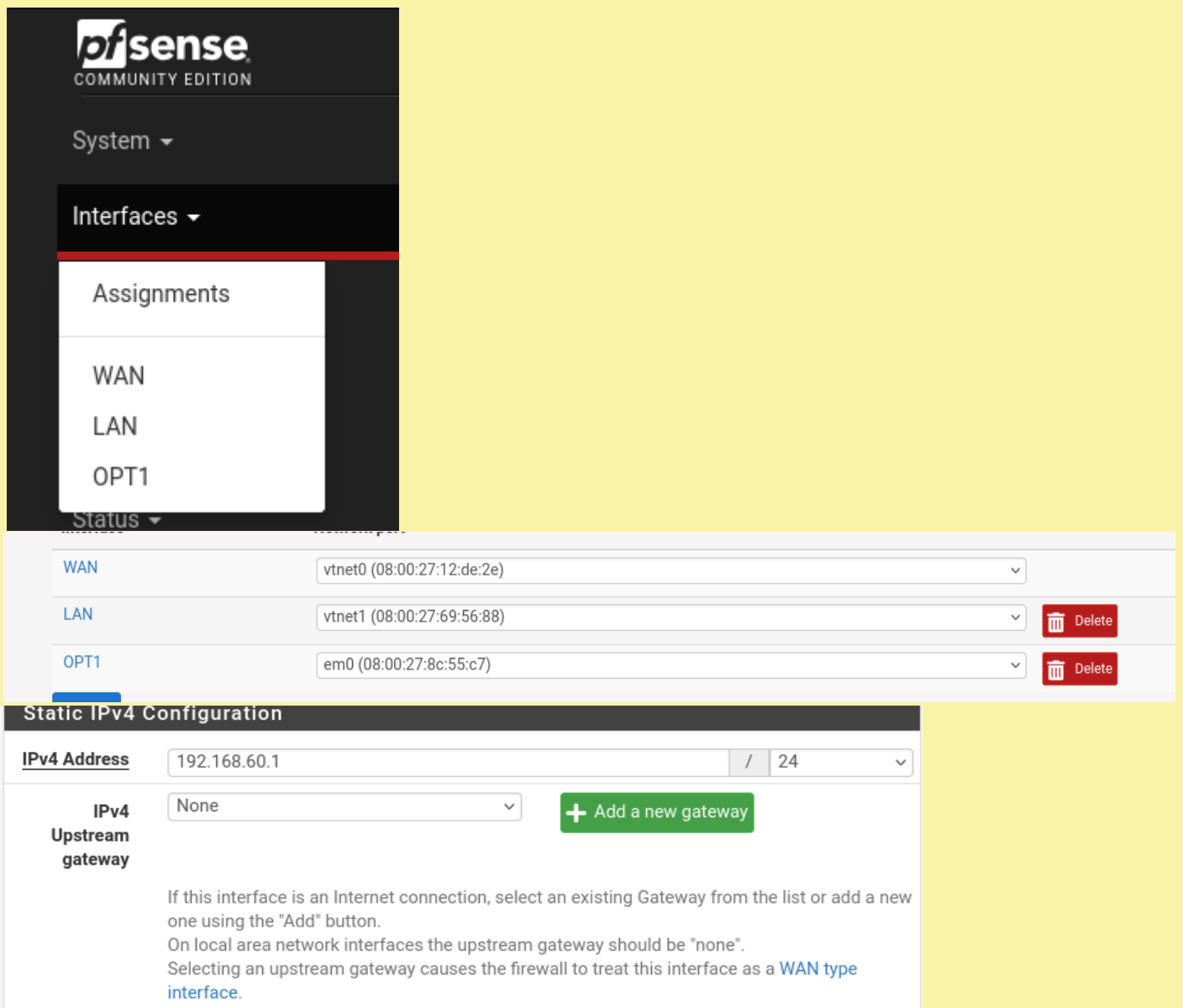
Il primo passaggio è quello di creare una terza interfaccia di rete per la **Metasploitable** , quindi apro le impostazioni Network e seleziono il tipo di rete in *Internal Network* e la chiamo "metanet".



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, (“metanet”), 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:
>

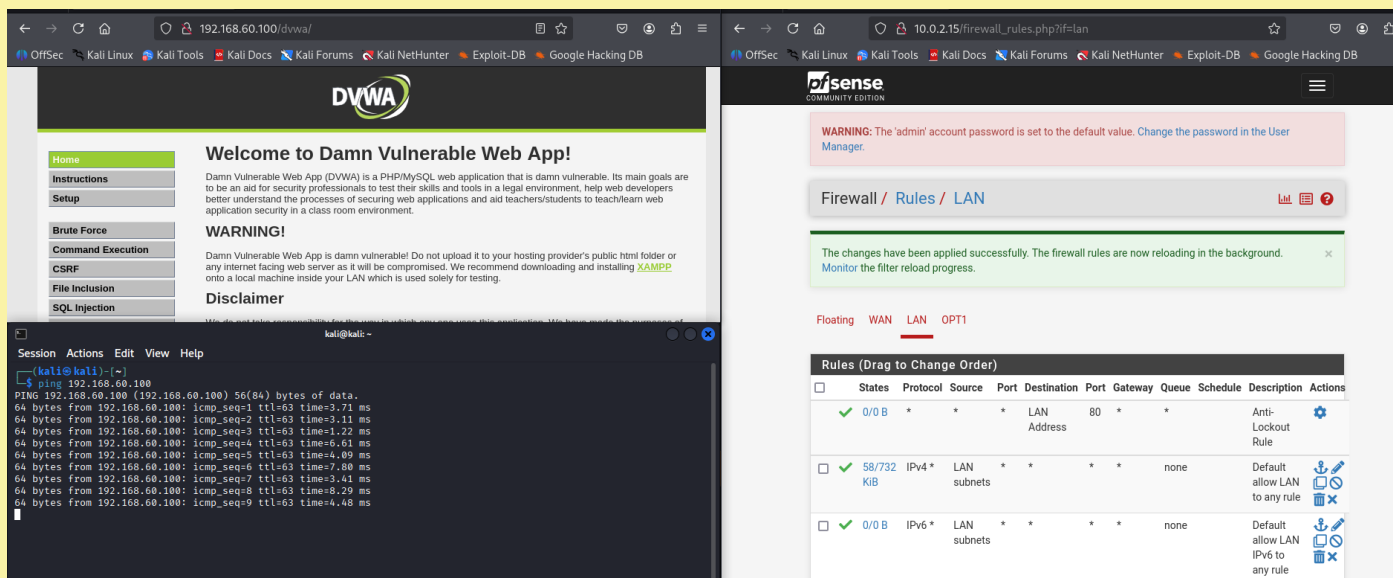
Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

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
```

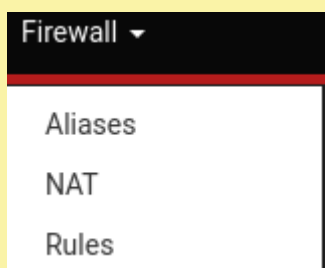
Di seguito apro la Metasploitable per vedere il suo indirizzo IP che consentirà di l’accesso al sito Metasploitable2 e di conseguenza al DVWA.

```
eth0: <BROADCAST,MULTICAST,UP>
    link/ether 08:00:27:ab:f7:bd
    inet 192.168.60.100/24 brd 192.168.60.255
    inet6 fe80::a00:27ff:feab:f7
```

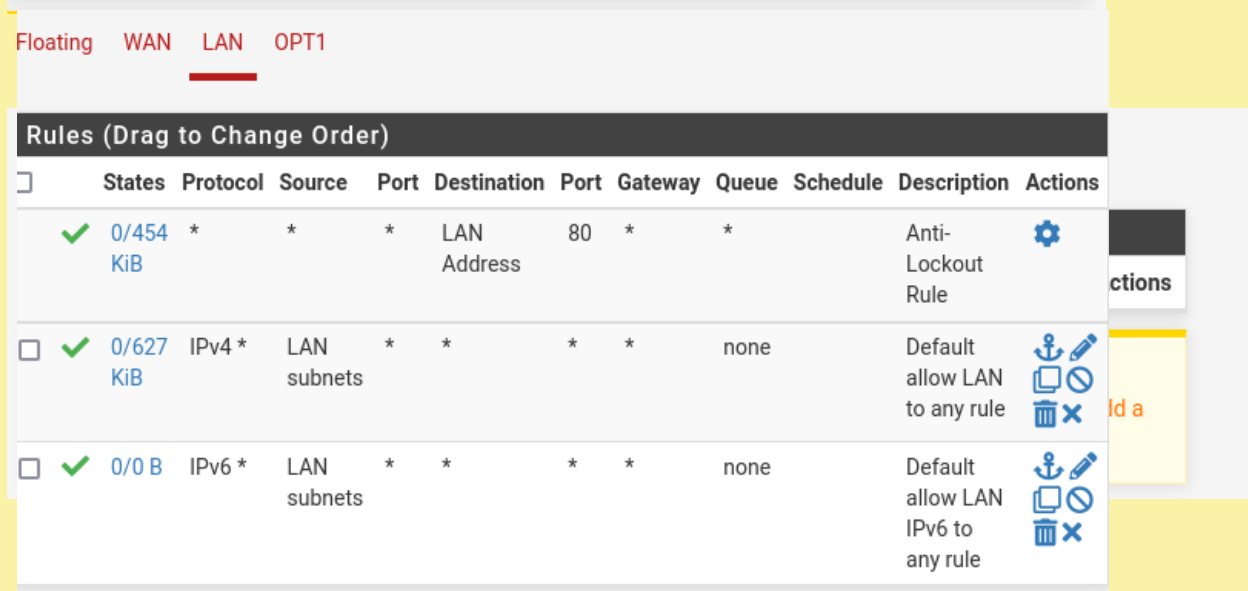
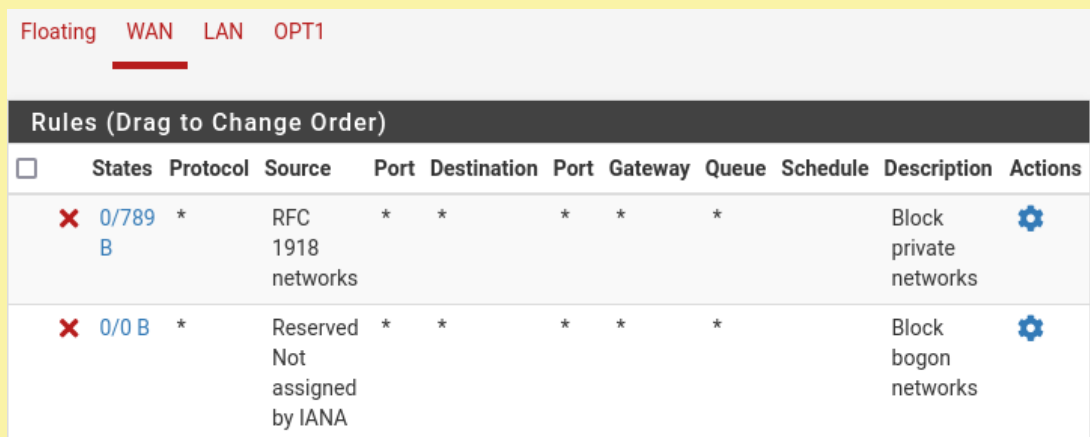
Torno sulla kali e faccio una prova per vedere se senza regola riesco ad accedere al sito e fare il ping.



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



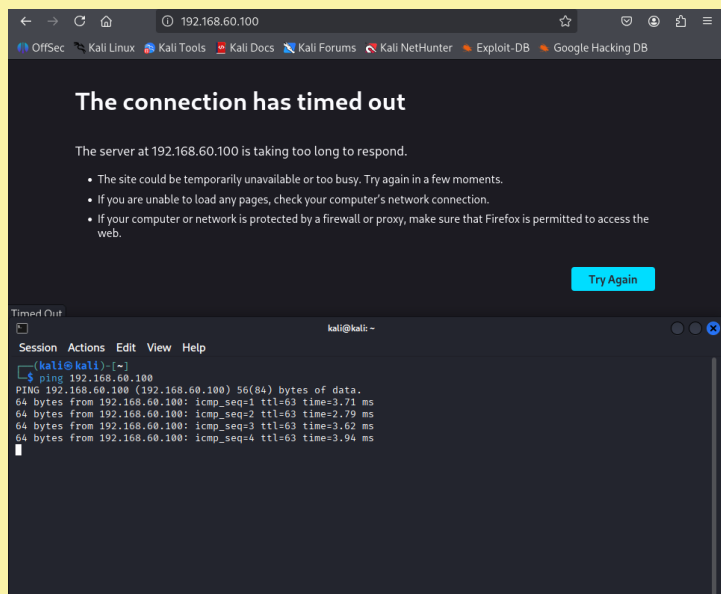
Sono presenti tre sezioni: WAN, LAN, OPT1 .



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**) dalla porta 80 (**HTTP**) alla 443 (**HTTPS**).

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



The connection has timed out

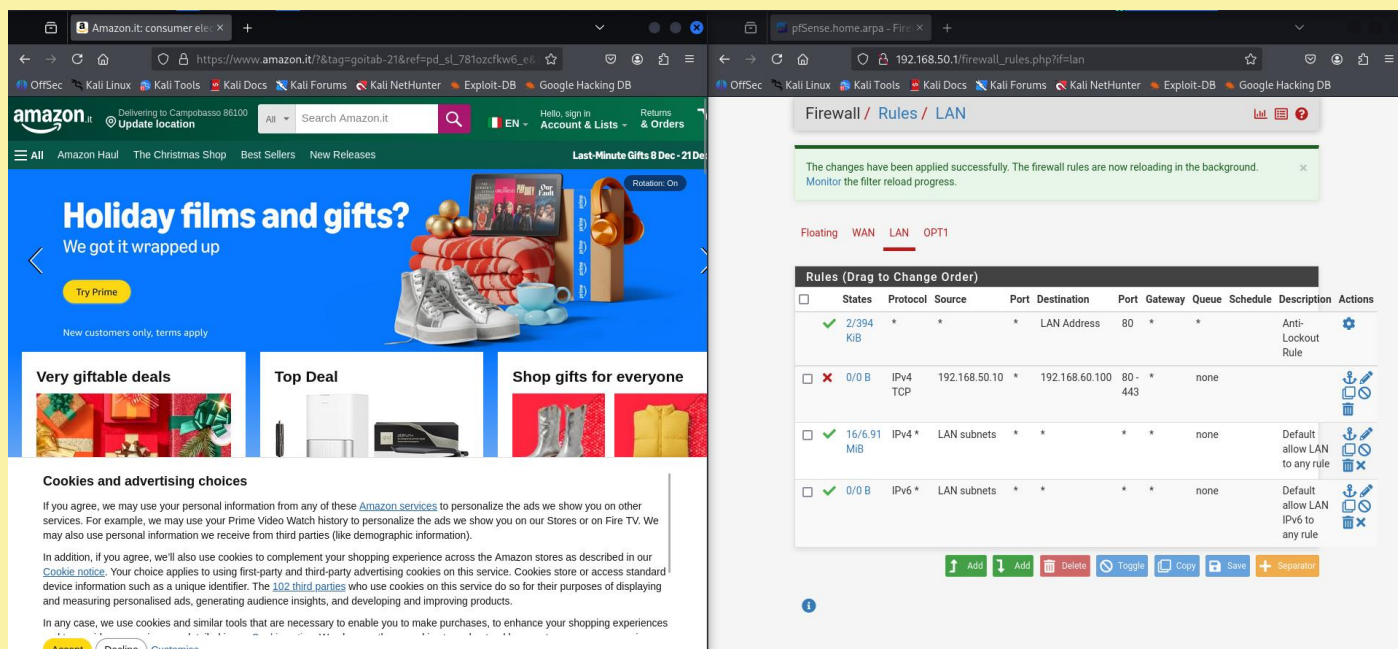
The server at 192.168.60.100 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

```
kali@kali: ~  
$ ping 192.168.60.100  
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data:  
64 bytes from 192.168.60.100: icmp_seq=1 ttl=63 time=3.71 ms  
64 bytes from 192.168.60.100: icmp_seq=2 ttl=63 time=2.79 ms  
64 bytes from 192.168.60.100: icmp_seq=3 ttl=63 time=3.62 ms  
64 bytes from 192.168.60.100: icmp_seq=4 ttl=63 time=3.94 ms
```

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.



Amazon.it: consumer ele... x

https://www.amazon.it/?tag=goitab-21&ref=pd_sl_781ozcfkw6_e... x

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN OPT1

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	2/394 KIB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.50.10	*	192.168.60.100	80 - 443	*	none		
<input type="checkbox"/>	16/6.91 MIB	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator