

ESAME S3

Creazione policy PfSense

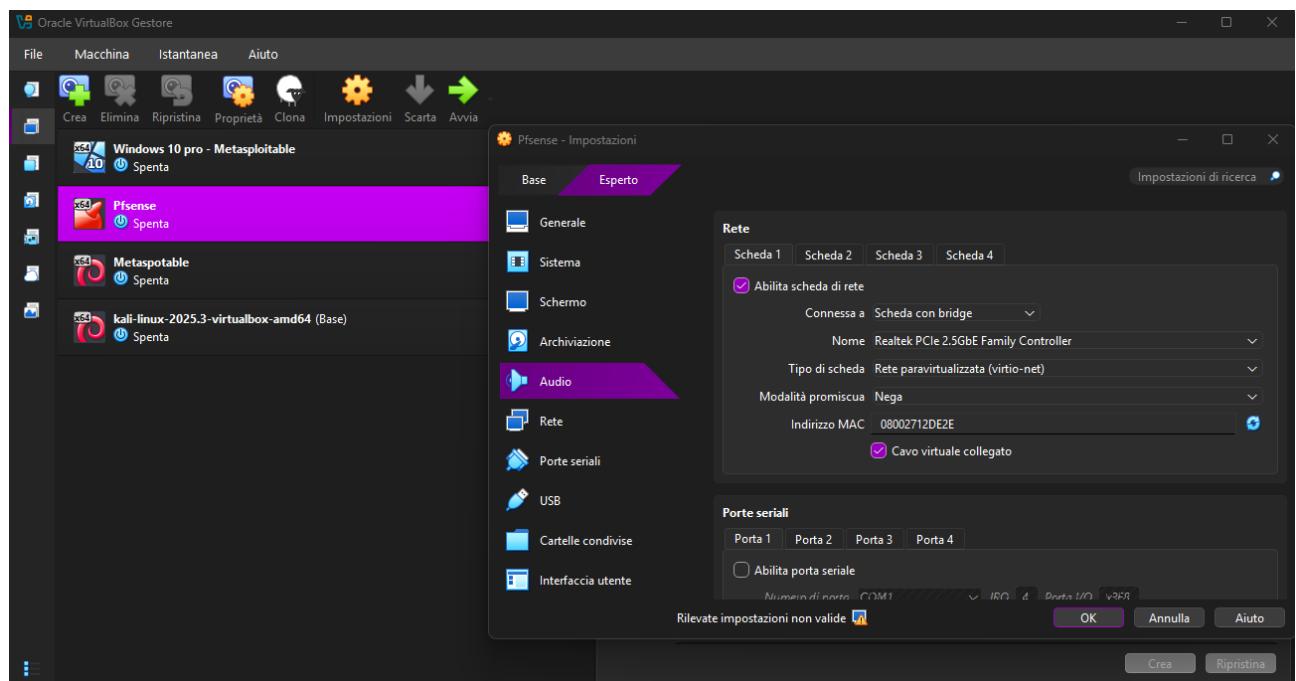
- CONFIGURAZIONE HARDWARE -

Per prima cosa configuro, all'interno di **Virtualbox**, l'hardware relativo alle schede di rete relative alle macchine che utilizzerò per l'esercitazione di oggi.

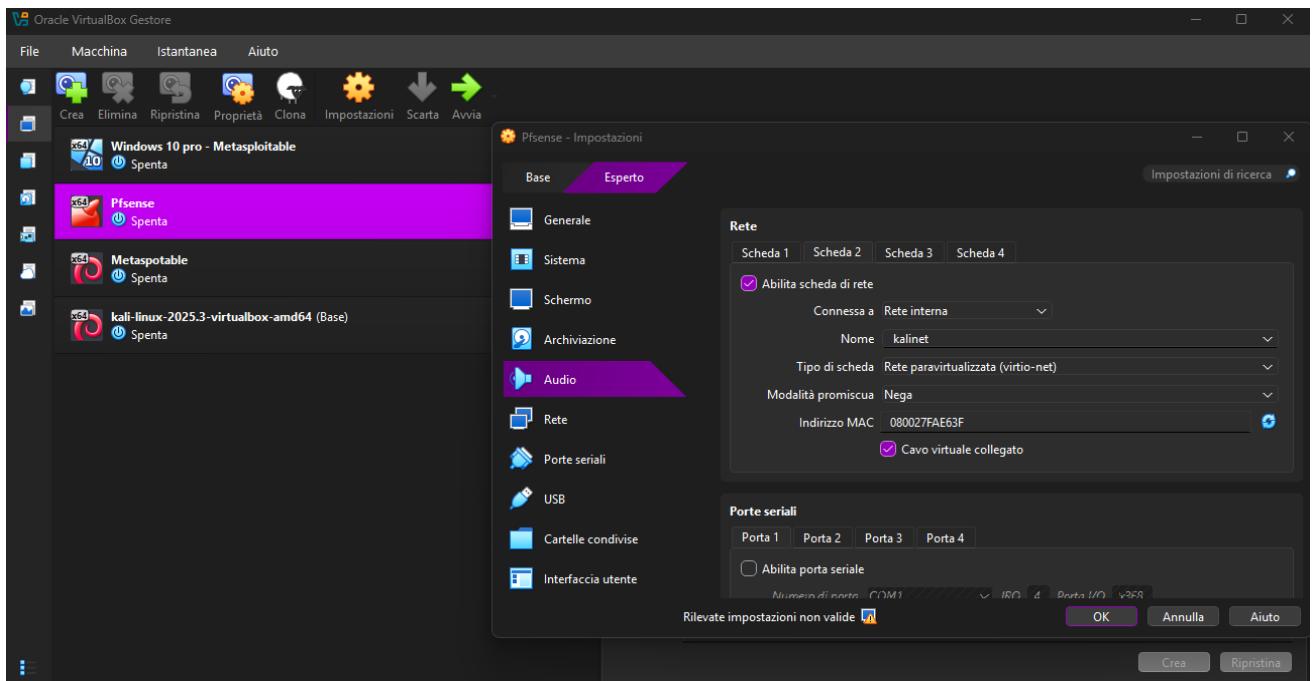
PfSense

Qui dovrò creare tre diverse interfacce di rete perché questa macchina fungerà da intermediario tra le altre due macchine appartenenti a reti diverse, pfSense sarà il nostro **firewall**.

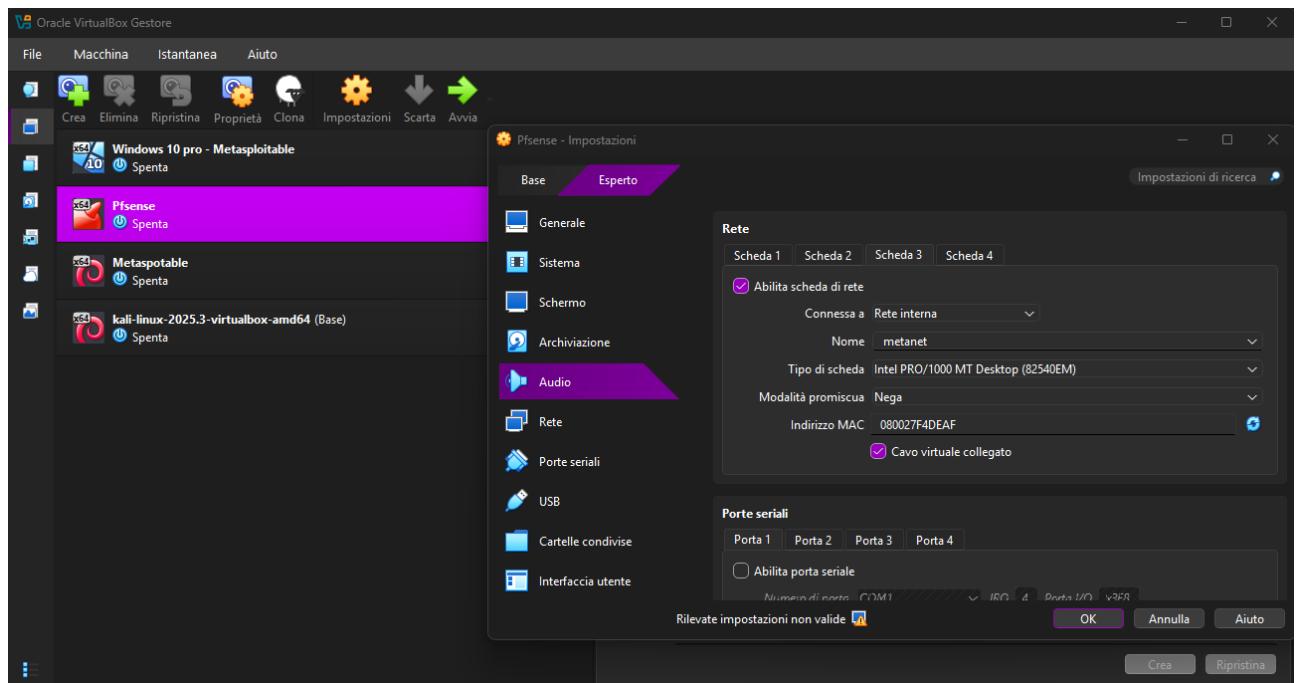
Setto la Scheda 1 in Bridge, connessa cioè alla **WAN** (Internet):



Collego la Scheda 2 alla LAN di Kali Linux e la chiamo “kalinet”

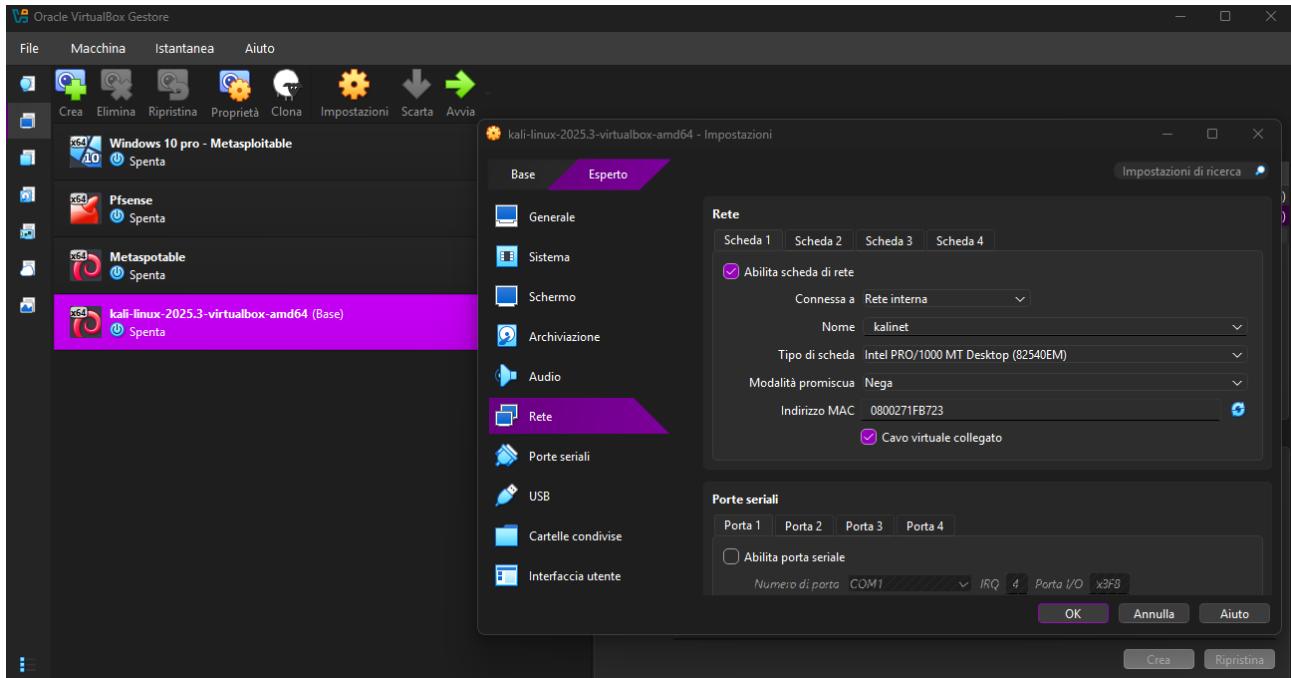


Collego la Scheda 2 alla LAN di Metasploitable e la chiamo “metanet”



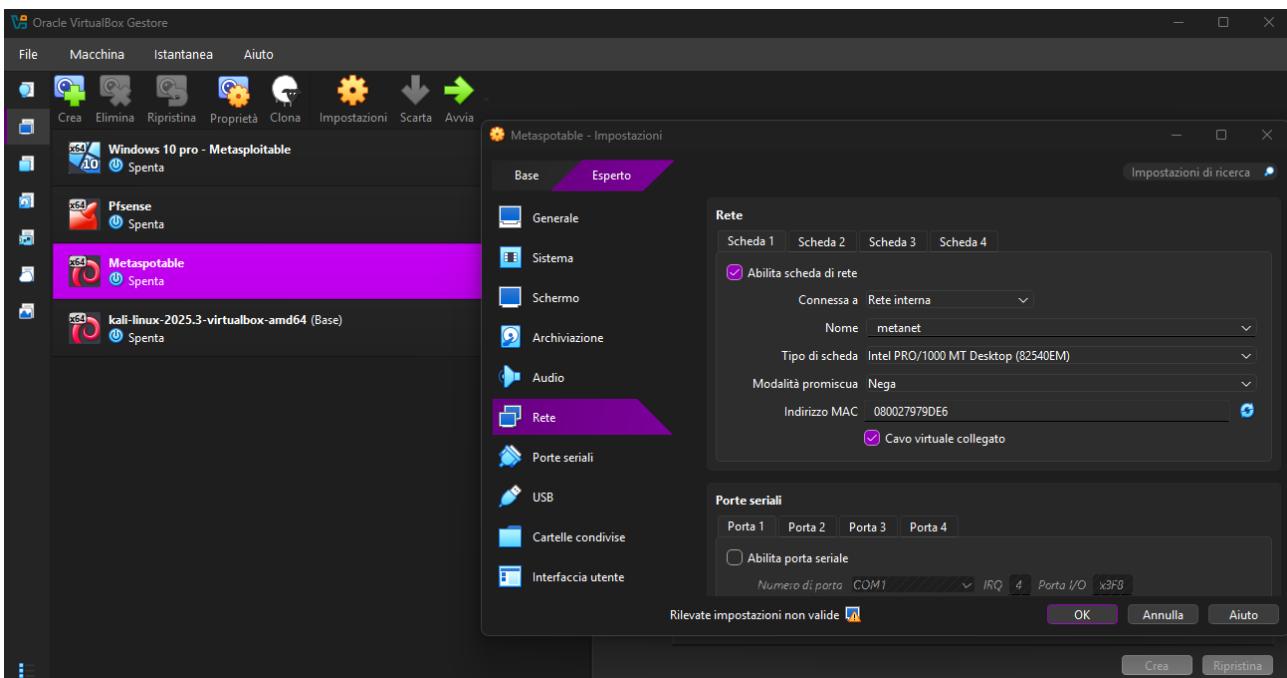
Kali

Per Kali andrò ad impostare la scheda 1 in locale e mi accerto di dare lo stesso nome a questa scheda di rete per simulare una connessione con la macchina pfSense (in questo caso “**kalinet**”)



Metasploitable

Per Metasploitable andrò ad eseguire lo stesso procedimento ma stando attento questa volta ad inserire il nome che ho assegnato a questa Lan (in questo caso “**metanet**”)



- CONFIGURAZIONE SOFTWARE -

Possiamo adesso accendere la macchina **pfSense** e configurare le nostre reti.

La configurazione è molto semplice in quanto consiste in una serie di domande guidate per poter settare al meglio le nostre LAN.

Nella schermata iniziale vedremo una serie di opzioni che potremo selezionare digitando il numero corrispondente:

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 9) pfTop |
| 1) Assign Interfaces | 10) Filter Logs |
| 2) Set interface(s) IP address | 11) Restart webConfigurator |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools |
| 4) Reset to factory defaults | 13) Update from console |
| 5) Reboot system | 14) Enable Secure Shell (sshd) |
| 6) Halt system | 15) Restore recent configuration |
| 7) Ping host | 16) Restart PHP-FPM |
| 8) Shell | |

A noi interessano le opzioni 1 e 2:

- in “**Assign Interfaces**” andremo ad assegnare le interfacce che noi utilizzeremo; nel nostro caso dovremo creare una interfaccia **WAN** (pfSense), una interfaccia **LAN** (Kali) e una **OPT1** (Metasploitable).
- In “**Set interfaces**” invece configureremo singolarmente le nostre interfacce assegnando gli indirizzi IP che andremo ad utilizzare:
WAN → 192.168.1.140/24
LAN → Con DHCP attivo con IPv4 che va da 192.168.50.10 a 192.168.50.100 (Kali)
OPT1 → Con DHCP attivo con IPv4 che va da 192.168.60.10 a 192.168.60.100 (Metasploitable)

Quando assegniamo le interfacce di rete ci verrà chiesto se impostare o meno le VLAN, non servono per il completamento del nostro test quindi risponderemo /n.

Alla fine della configurazione avremo schermata simile a questa:

```
The IPv4 OPT1 address has been set to 192.168.60.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.60.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 9f95701a52536b2e37b9

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtne0       -> v4/DHCP4: 192.168.1.140/24
LAN (lan)      -> vtne1       -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.60.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

- Kali linux -

Una volta avviata Kali entriamo nel nostro browser ed accediamo al sito di gestione di pfSense immettendo come URL l'indirizzo IPv4 che abbiamo impostato poco fa per WAN:

http://192.168.1.140

Dopo aver eseguito l'accesso possiamo andare alla pagina in cui potremo andare a gestire le regole sulle quali si baserà il nostro firewall:

Firewall → Rules → LAN

Da questa schermata clicchiamo su **Add** per aggiungere una nuova regola al firewall.

Adesso possiamo compilare un form in cui specifichiamo vari dettagli sulla regola che stiamo impostando:

- Action: Block, perchè vogliamo bloccare (silenziosamente) ogni tentativo di comunicazione di Kali alla Metasploitable.
- Protocol: lasciamo solo il TCP (Così da non bloccare anche il ping ICMP).
- Source: seleziona “Address or Alias” ed inserirò l’IP del mio Kali 192.168.50.10

- Destination: seleziono anche qui “Address or Alias” ed inserirò l’IP del mio Metasploitable 192.168.60.11, infine blocchiamo solo la porta 80 (HTTP)

Firewall / Rules / Edit

Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source

Source: Invert match Address or Alias 192.168.50.10 /
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination: Invert match Address or Alias 192.168.60.11 /
Destination Port Range: HTTP (80) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Cliccando su “**Save**” e successivamente su “**Apply changes**” abbiamo confermato la regola che impedisce a Kali di comunicare alla porta 80 con Metasploitable.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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
✓ 0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/1 KiB	IPv4 TCP	192.168.50.10	*	192.168.60.11	80 (HTTP)	*		none		
✓ 1/533 KiB	IPv4 *	LAN subnets	*	*	*	*		none	Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*		none	Default allow LAN IPv6 to any rule	

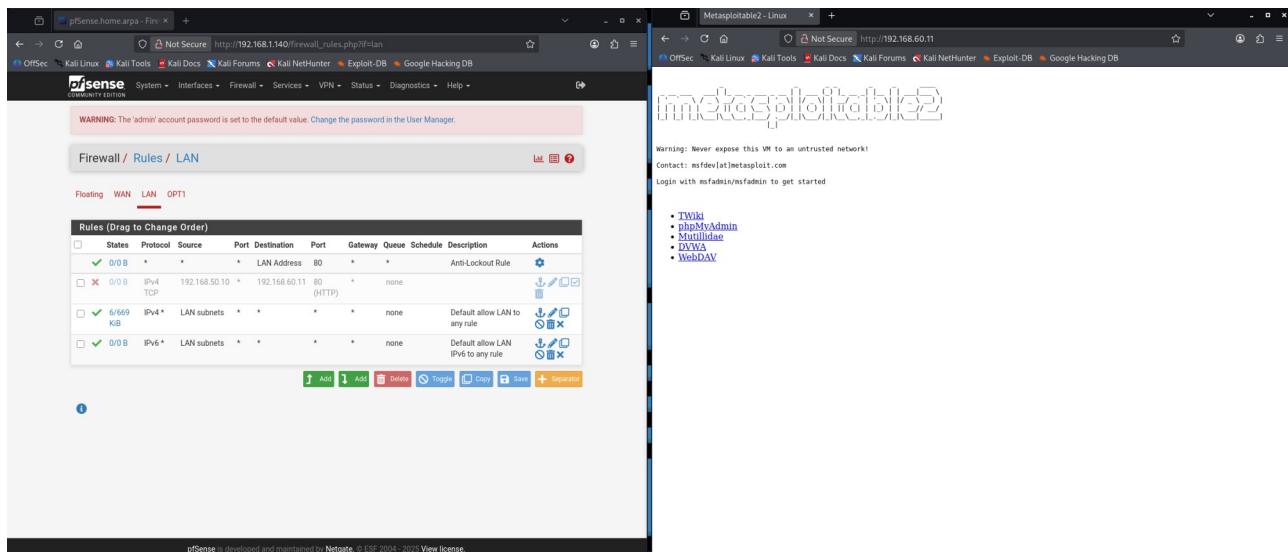
Add **Up** **Down** **Delete** **Toggle** **Copy** **Save** **Separator**

- Testing -

Adesso non ci resta altro che tentare di accedere alla macchina Metasploitable da Linux tramite browser per verificare che il nostro firewall è stato configurato correttamente.

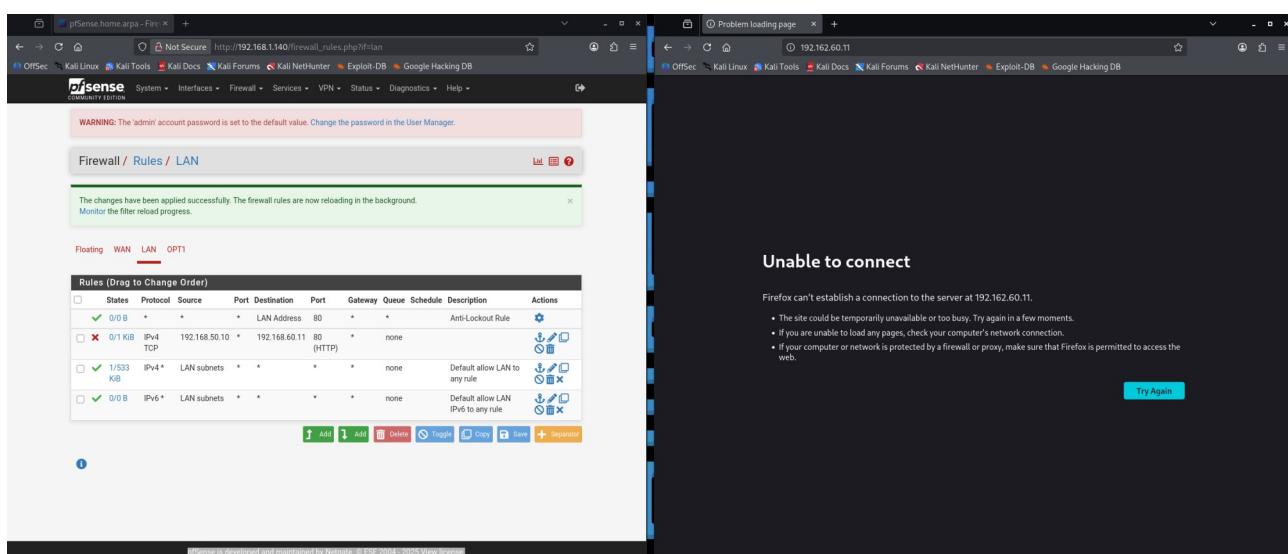
Disattivo temporaneamente la regola di blocco su pfSense e provo ad accedere alla macchina Metasploitable tramite il suo indirizzo:

<http://192.168.60.5>.



Riusciamo a connetterci tranquillamente.

Riattivo la regola di blocco e riprovo ad accedere a <http://192.168.60.5>.



Non riusciamo a connetterci, la connessione va in Time Out.

Se effettuiamo il ping da Kali a Metasploitable otteniamo risposta poiché noi abbiamo bloccato solo il **TCP** della porta 80 e non l'**ICMP**

```
(kali㉿kali)-[~]
$ ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=63 time=0.981 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=63 time=0.857 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=63 time=0.847 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=63 time=0.750 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=63 time=0.592 ms
64 bytes from 192.168.60.11: icmp_seq=6 ttl=63 time=0.612 ms
64 bytes from 192.168.60.11: icmp_seq=7 ttl=63 time=0.939 ms
64 bytes from 192.168.60.11: icmp_seq=8 ttl=63 time=0.527 ms
64 bytes from 192.168.60.11: icmp_seq=9 ttl=63 time=0.533 ms
64 bytes from 192.168.60.11: icmp_seq=10 ttl=63 time=0.482 ms
64 bytes from 192.168.60.11: icmp_seq=11 ttl=63 time=0.646 ms
64 bytes from 192.168.60.11: icmp_seq=12 ttl=63 time=0.693 ms
64 bytes from 192.168.60.11: icmp_seq=13 ttl=63 time=0.582 ms
64 bytes from 192.168.60.11: icmp_seq=14 ttl=63 time=0.547 ms
64 bytes from 192.168.60.11: icmp_seq=15 ttl=63 time=0.692 ms
■
```