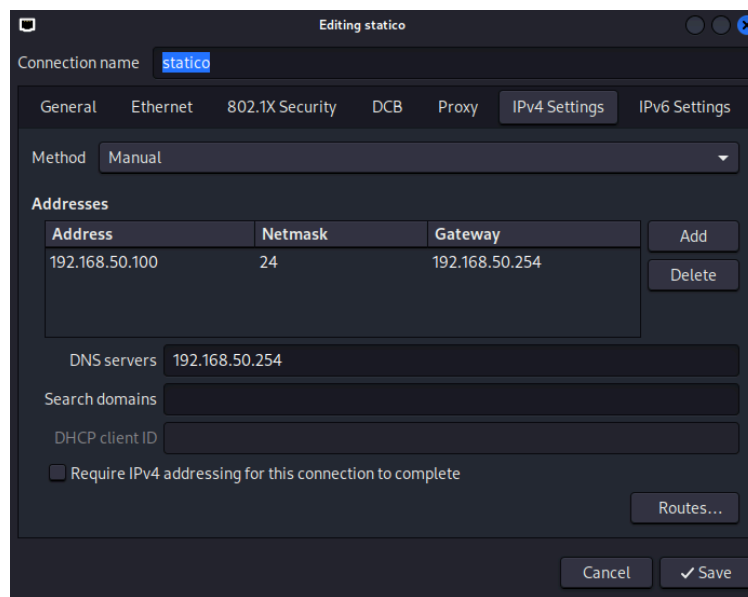


Esercizio per il progetto settimanale Unit 1 - S3 - L5

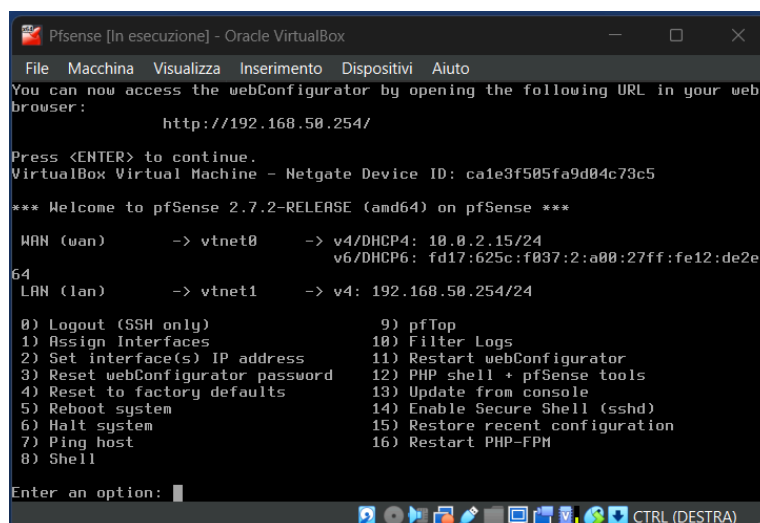
Svolto da Gioele Parla

Esercizio: Creazione di una regola Firewall.

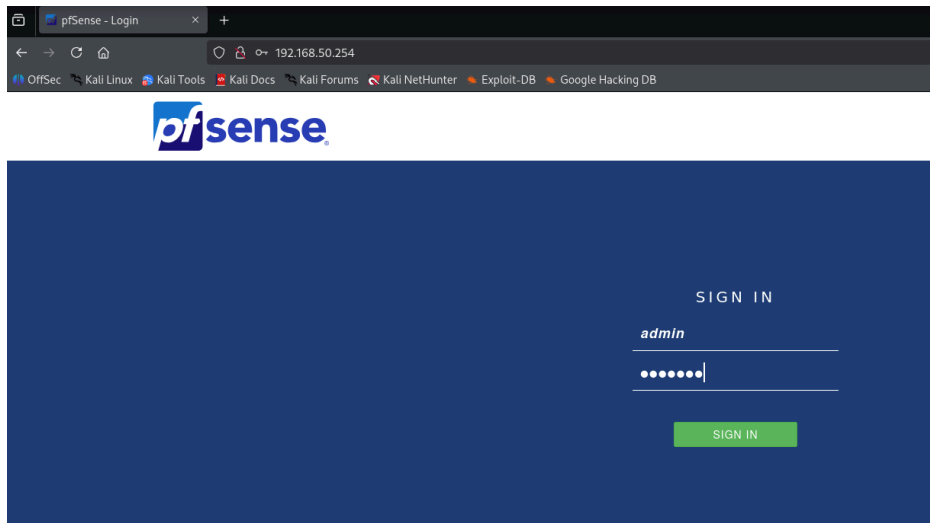
Per prima cosa giusto per impostare correttamente tutto l'ambiente di rete configuriamo la nostra rete di KALI in **statica** e andando su edit connections per comodità impostiamo gateway e DNS servers su 192.168.50.254 poicè la pfsense ogni tanto cambia il suo DHCP prendendo spunto da uno statico della macchina e si mette come gateway sull'1 quindi preferiamo mettere la pfsense sulla 254.



Andando sull'interfaccia di pfsense da VirtualBox dovremo impostare la LAN su **192.168.50.254** e per impostarla ci basterà seguire i comandi andando prima su 2, dichiarare di non voler attivare il DHCP e poi impostare manualmente

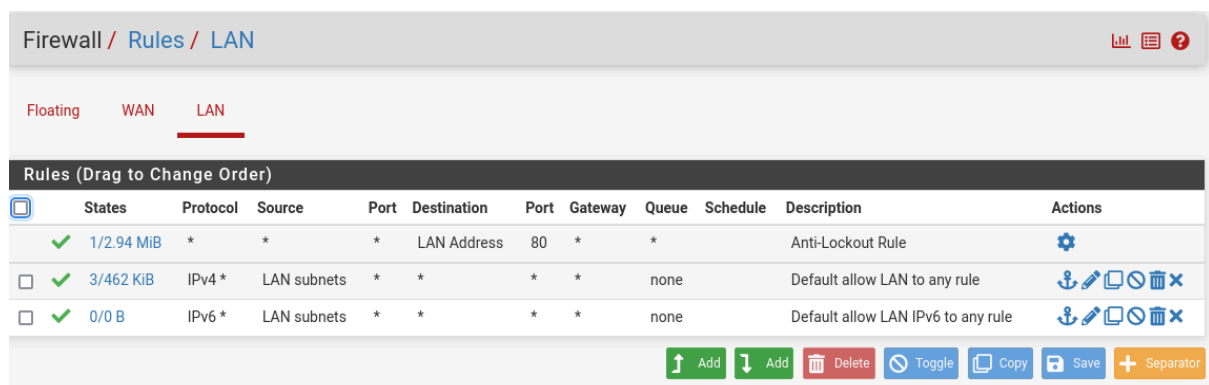


Una volta configurato andando sul browser di kali accediamo sull'UTM 192.168.50.254 e funzionerà già da firewall



Una volta entrati nel nostro firewall possiamo procedere con il nostro esercizio che chiede:

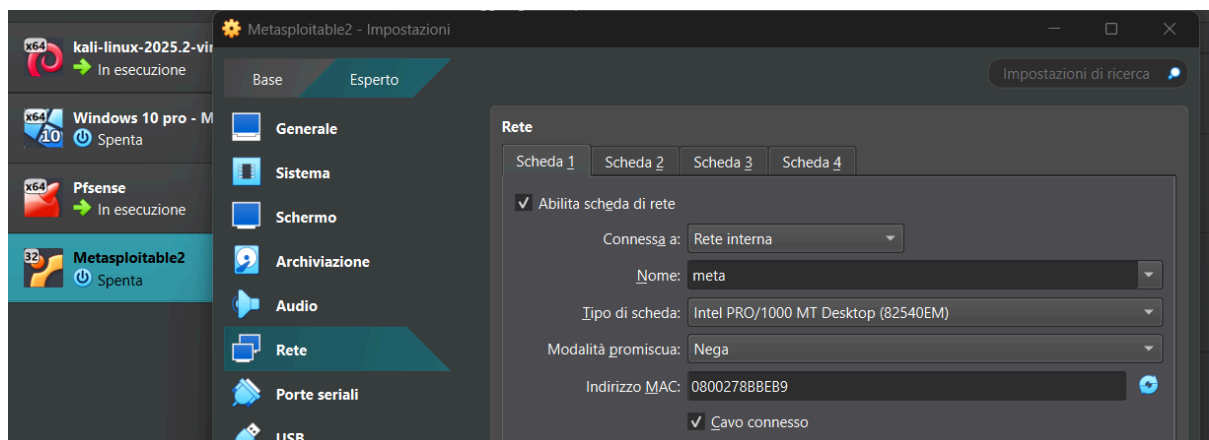
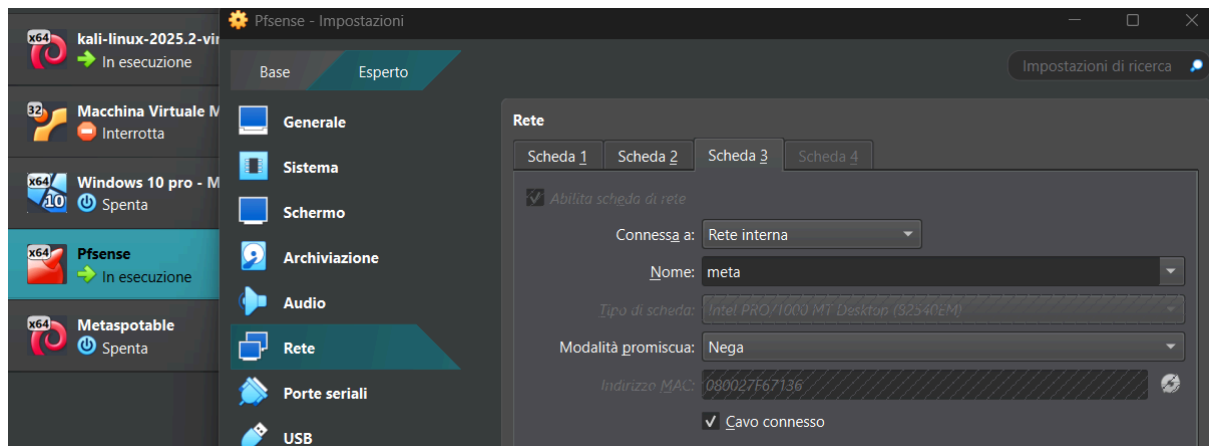
Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.



Quindi il nostro esercizio chiede di aggiungere una nuova regola rispetto a quelle già presenti, le rules sono importanti perchè tramite le rules è possibile configurare come deve comportarsi il nostro firewall col traffico di input per ognuna di queste wal/lan, le regole floating sono regole che valgono per tutti, in LAN la prima regola non posso modificarla e riguarda l'accesso a questa interfaccia web, potremo al massimo portarla in HTTPS invece le altre due regole LAN consentono la navigazione in internet separata in ipv4 e ipv6.

Dopo una breve panoramica configuriamo le reti delle nostre macchine kali e metasploitable così da poter successivamente creare una regola firewall da applicare a queste 2 reti.

L'esercizio ci consiglia di impostare le macchine Kali e Metasploitable su **reti diverse**, quindi per prima cosa andiamo nelle impostazioni di rete di Pfense su VirtualBox e aggiungiamo una nuova interfaccia di rete(scheda 3) che chiameremo "**meta**" così potremo gestire una ulteriore rete e successivamente andando in impostazioni di rete della macchina virtuale metasploitable 2 dovremo impostare la rete interna su "meta".



Una volta configurato VirtualBox con le corrette impostazioni di rete di pfense e Metasploitable2 il passaggio successivo sarà quello di configurare la nuova rete meta all'interno di pfense avviandola.

All'interno di PfSense dobbiamo gestire la nuova rete **meta**, dalle impostazioni dovremo quindi aggiungere una nuova interfaccia di rete **vtnet2** e assegnare a questa interfaccia l'indirizzo IP ad esempio 192.168.60.1 così che questa interfaccia si occuperà della rete meta dove si trova metasploitable

```
Pfsense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Do you want to proceed [y/n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: d6d4bdae76ece3640ca0

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
                                     v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe12:de2e/
64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.254/24
OPT1 (opt1)    -> vtnet2      ->

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: 2
```

```
Pfsense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Enter an option: 2

Available interfaces:

0 - WAN (vtnet0 - dhcp, dhcp6)
1 - LAN (vtnet1 - static)
2 - OPT1 (vtnet2)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) 192.168.60.1
Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.60.1

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
```

```
Pfsense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

router: http://192.168.60.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: d6d4bdae76ece3640ca0

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
                                     v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe12:de2e/
64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.254/24
OPT1 (opt1)    -> vtnet2      -> 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:
```

Adesso andiamo sulla Web Gui per attivare e configurare la nuova interfaccia come suggerisce l'esercizio e clicchiamo sulla OPT1

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:74:87:53)
OPT1	vtnet2 (08:00:27:f6:71:36)

All'interno delle impostazioni di OP1 dovremo rinominare l'interfaccia in meta assicurandoci che abbia l'IPv4 corrispondente e salviamo le modifiche.

Interfaces / OPT1 (vtnet2)

General Configuration

Enable

☒ Enable interface

Description

meta

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx.

MTU

If this field is blank, the adapter's default MTU will be used. This value can be set to a maximum of 65535.

MSS

If a value is entered in this field, then MSS clamping for TCP connections will be in effect.
The value must be in the range of 0 to 65535, minus 60 for IPv6 (TCP/IPv6 header size).

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate) to avoid a performance penalty.

Static IPv4 Configuration

IPv4 Address

192.168.60.1

Una volta configurata l'interfaccia di rete possiamo proseguire alla creazione della nostra regola, andiamo in Firewall / rules e creiamo la nostra regola, su action impostiamo **BLOCK** poichè ci serve che blocchi l'accesso al DVWA e mettiamo come sorgente la macchina kali con l'indirizzo IP corrispondente e come destinazione la rete meta che abbiamo creato

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	<input type="checkbox"/> 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	Any	Choose which IP protocol this rule should match.

Source		
Source	<input type="checkbox"/> Invert match	Address or Alias
		192.168.50.100 /

Destination		
Destination	<input type="checkbox"/> Invert match	Address or Alias
		192.168.60.100 /

una volta salvata la regola la troveremo all'interno della lista delle regole presenti sul nostro firewall, possiamo notare la **X** che rappresenta come sia una regola di blocco, come ultima azione dovremmo assicurarci che la regola sia posta in cima (quando l'ho creata ho usato la freccia su quindi si troverà già posizionata in cima)

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 2/215 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.50.100	*	192.168.60.100	*	*	none			
<input type="checkbox"/>	✓ 2/275 KIB	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

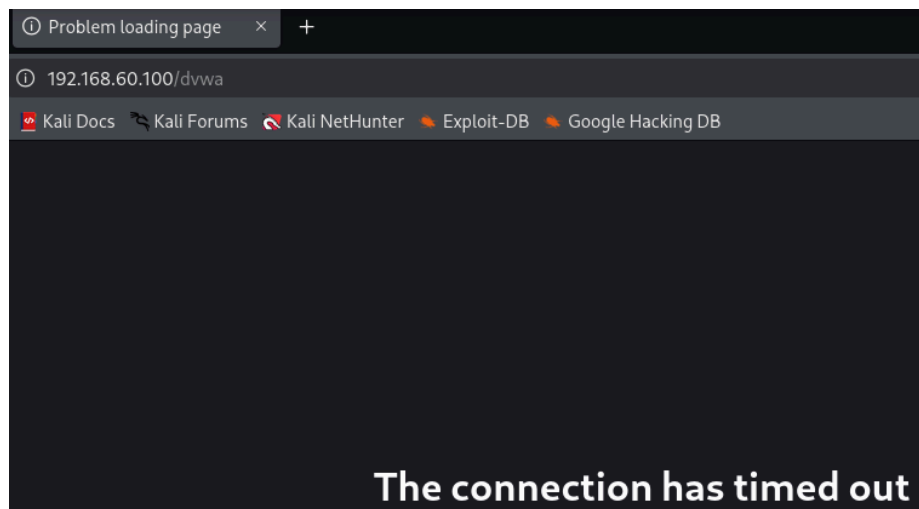
Toggle

Copy

Save

Separator

Una volta applicata la nostra regola sulla rete meta provando ad accedere alla DVWA di 192.168.60.100 ci darà **errore**.



Provando a fare delle ultime prove sul terminale di kali noteremo come riesce a comunicare con i gateway delle reti ma non con la nostra rete meta poichè abbiamo **bloccato** il traffico solamente tra la macchina kali e la macchina metasploitable tramite la nostra regola.

```
(kali@kali)-[~]  
$ ping 192.168.60.100  
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data.  
|
```

```
$ ping 192.168.50.254  
PING 192.168.50.254 (192.168.50.254) 56(84) bytes of data  
64 bytes from 192.168.50.254: icmp_seq=1 ttl=64 time=0.27  
64 bytes from 192.168.50.254: icmp_seq=2 ttl=64 time=0.27  
64 bytes from 192.168.50.254: icmp_seq=3 ttl=64 time=0.24  
64 bytes from 192.168.50.254: icmp_seq=4 ttl=64 time=0.25  
64 bytes from 192.168.50.254: icmp_seq=5 ttl=64 time=0.28  
64 bytes from 192.168.50.254: icmp_seq=6 ttl=64 time=0.26  
64 bytes from 192.168.50.254: icmp_seq=7 ttl=64 time=0.24  
64 bytes from 192.168.50.254: icmp_seq=8 ttl=64 time=0.26
```

```
(kali@kali)-[~]  
$ ping 192.168.60.1  
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.  
64 bytes from 192.168.60.1: icmp_seq=1 ttl=64 time=0.312 ms  
64 bytes from 192.168.60.1: icmp_seq=2 ttl=64 time=0.246 ms  
64 bytes from 192.168.60.1: icmp_seq=3 ttl=64 time=0.236 ms  
64 bytes from 192.168.60.1: icmp_seq=4 ttl=64 time=0.268 ms  
64 bytes from 192.168.60.1: icmp_seq=5 ttl=64 time=0.330 ms  
64 bytes from 192.168.60.1: icmp_seq=6 ttl=64 time=0.230 ms
```