

# Report Esercizio 13/12/2024

## Progetto Firewall Leonardo Catalano

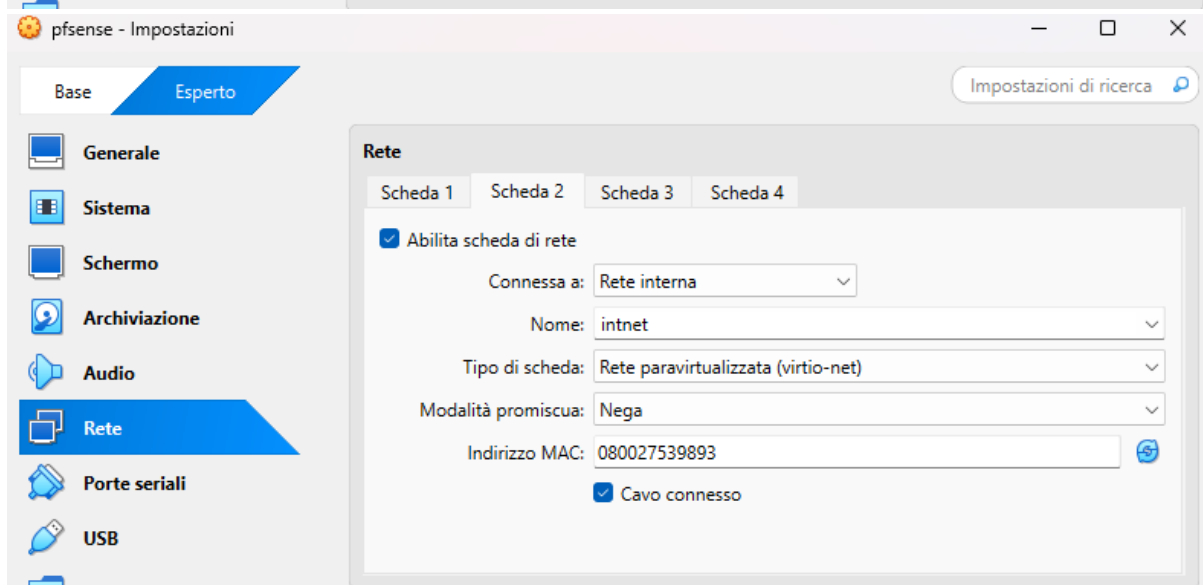
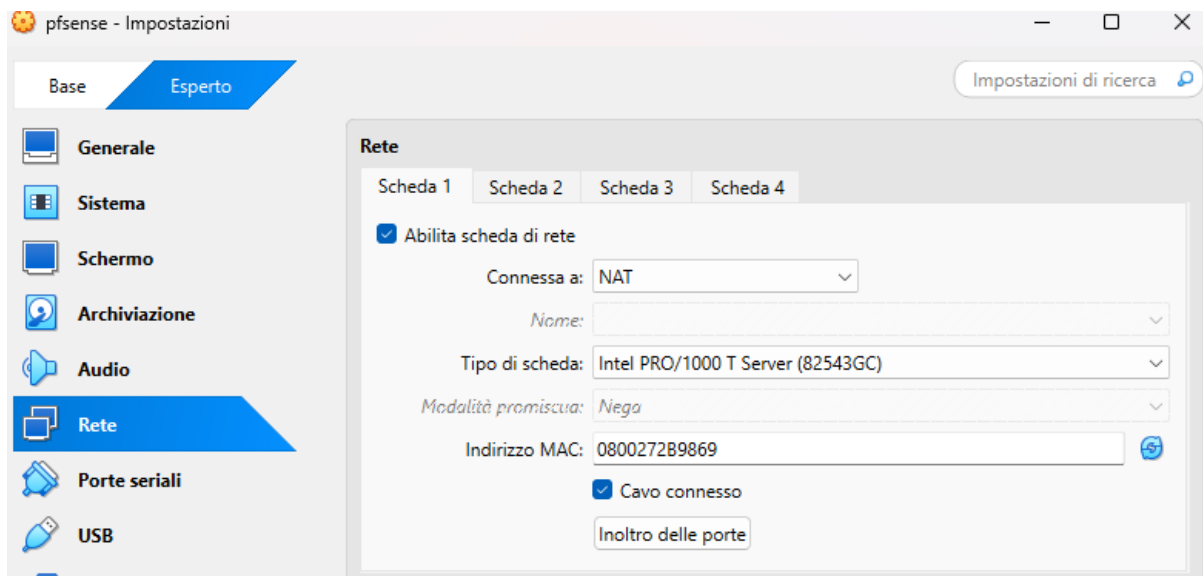
“La traccia di oggi ci chiede di creare una policy su pfsense facendo una nuova regola firewall, che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina kali linux e ne impedisca lo scan.”

Bonus: “Creare una regola che impedisca da kali l’accesso a metasploitable tramite il protocollo telnet (porta 23)”.

Le reti kali e Metasploitable devono essere su reti diverse.

Allora prima di iniziare accendiamo le macchine.

Pfsense: (Scheda 1 Nat – Scheda 2 Rete interna)



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

The IPv4 LAN address has been set to 192.168.10.7/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.10.7/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: e0409f52302cc03b88f1

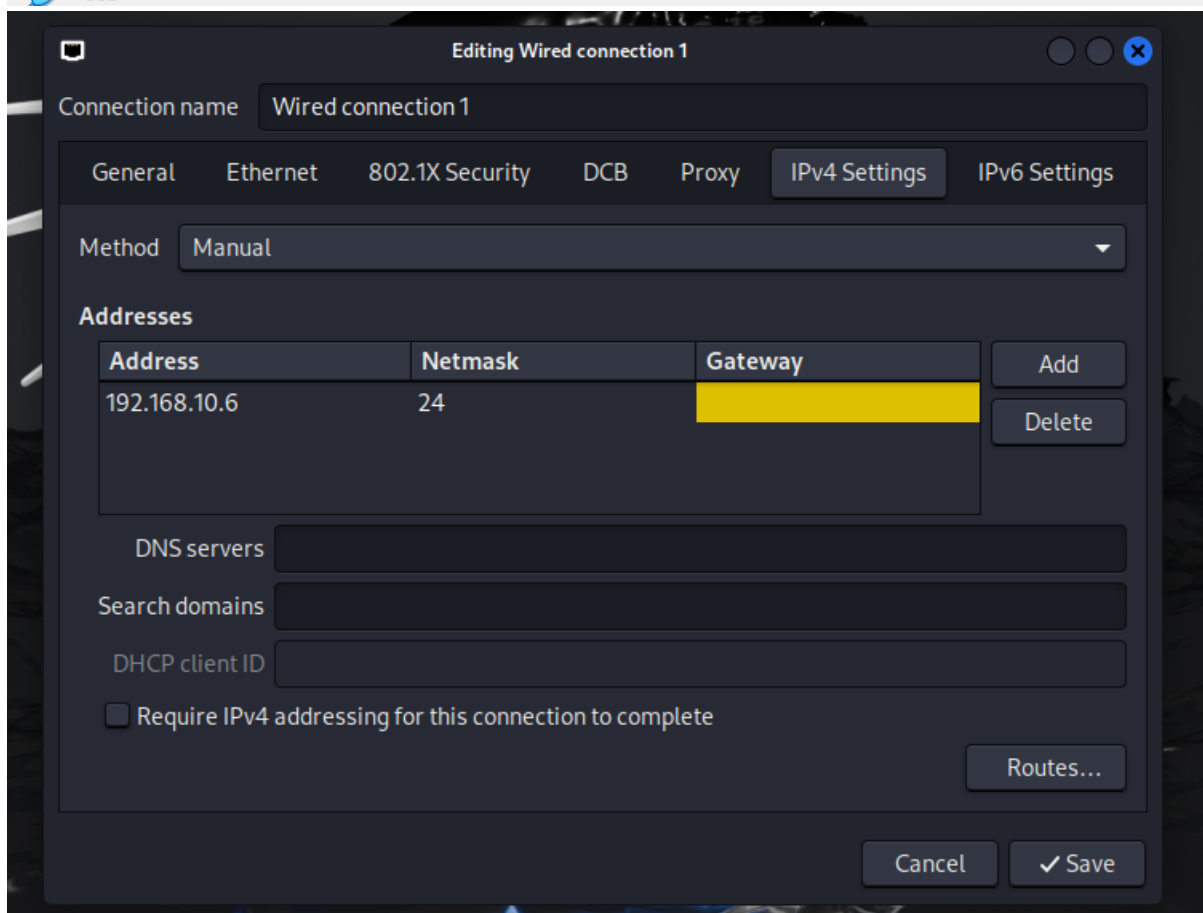
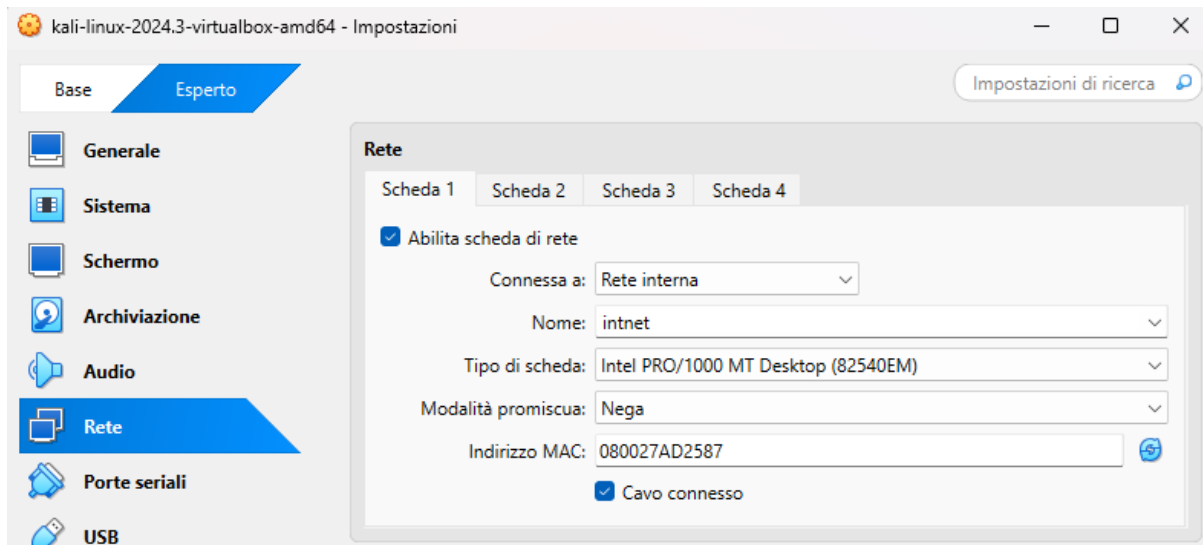
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0   -> v4: 192.168.10.7/24

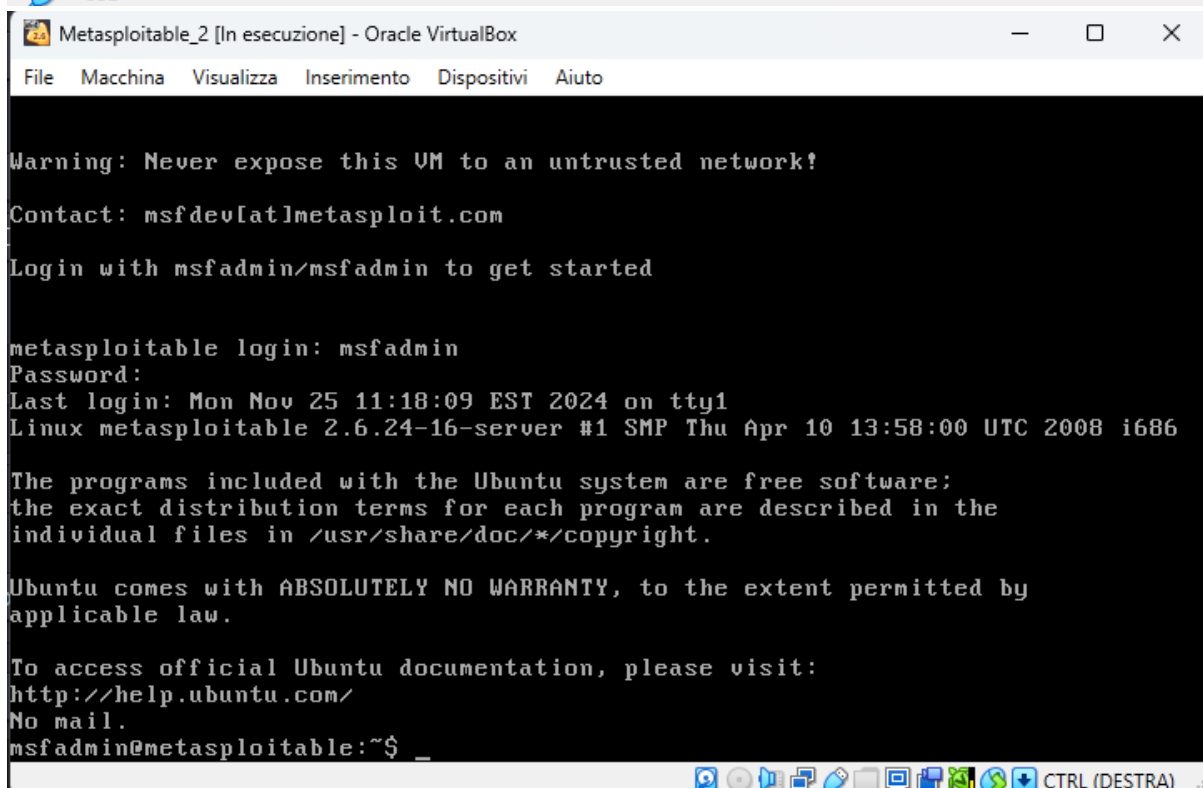
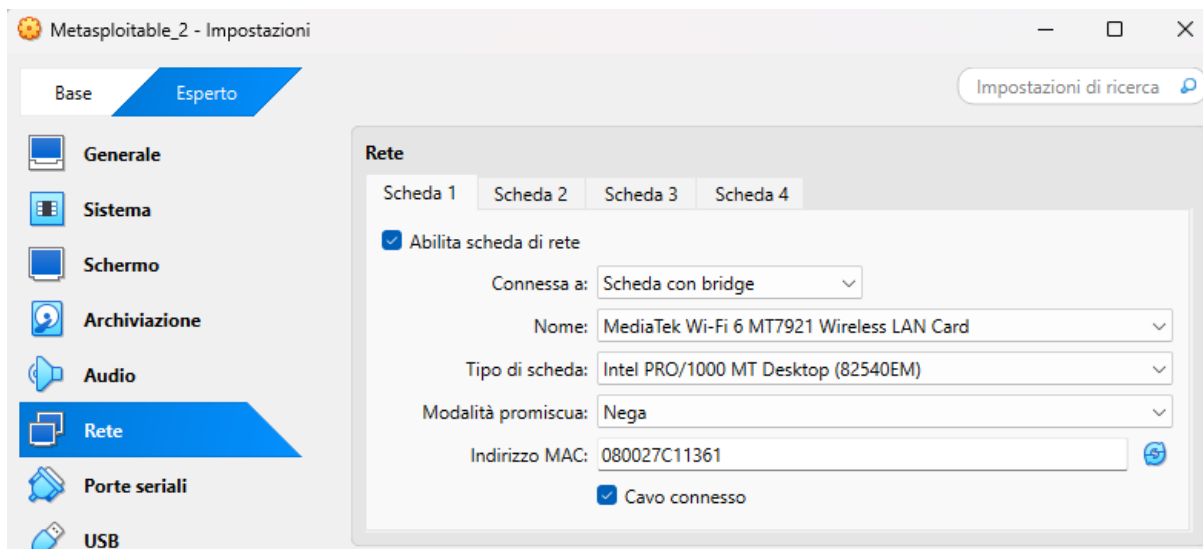
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: 
```

Kali: (Scheda 1 Rete locale)



Metasploitable 2: (Scheda 1 Scheda con bridge)



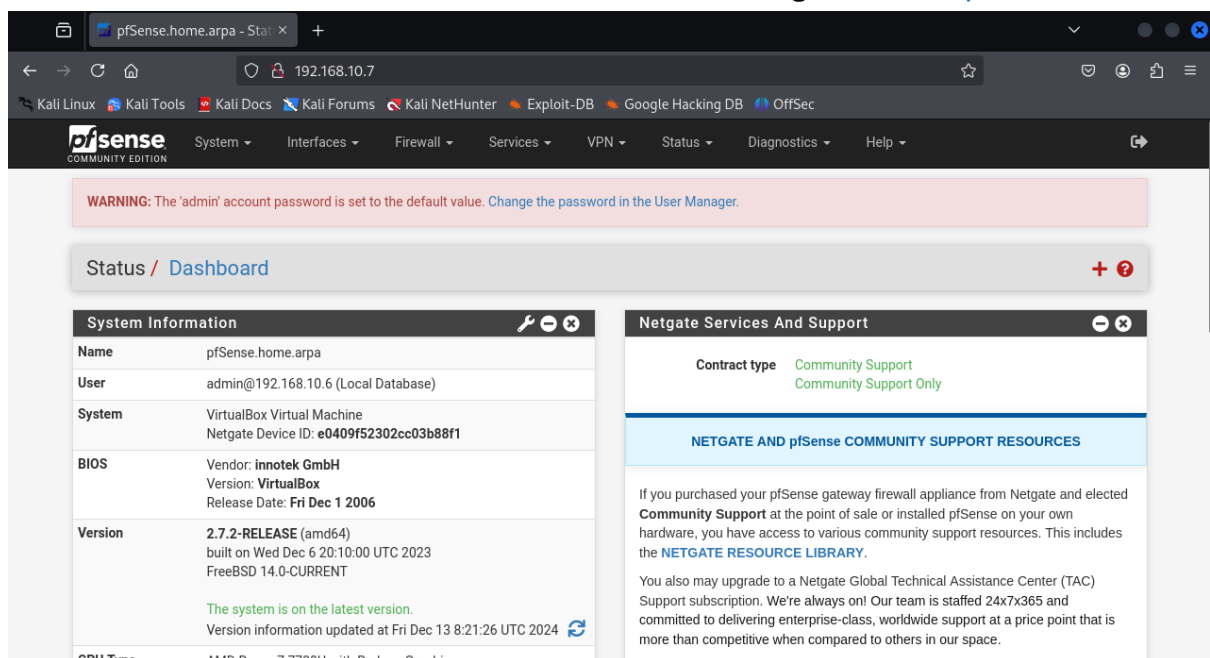
```
Metasploitable_2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:13:61
          inet addr:192.168.1.63  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd3:8753:8e68:10:a00:27ff:fec1:1361/64 Scope:Global
          inet6 addr: 2a0d:3344:3288:a110:a00:27ff:fec1:1361/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fec1:1361/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5401 (5.2 KB)  TX bytes:7140 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

(Ho messo la scheda in bridge perchè senò se mettevo in rete locale mi dava l'indirizzo con ipv6.)

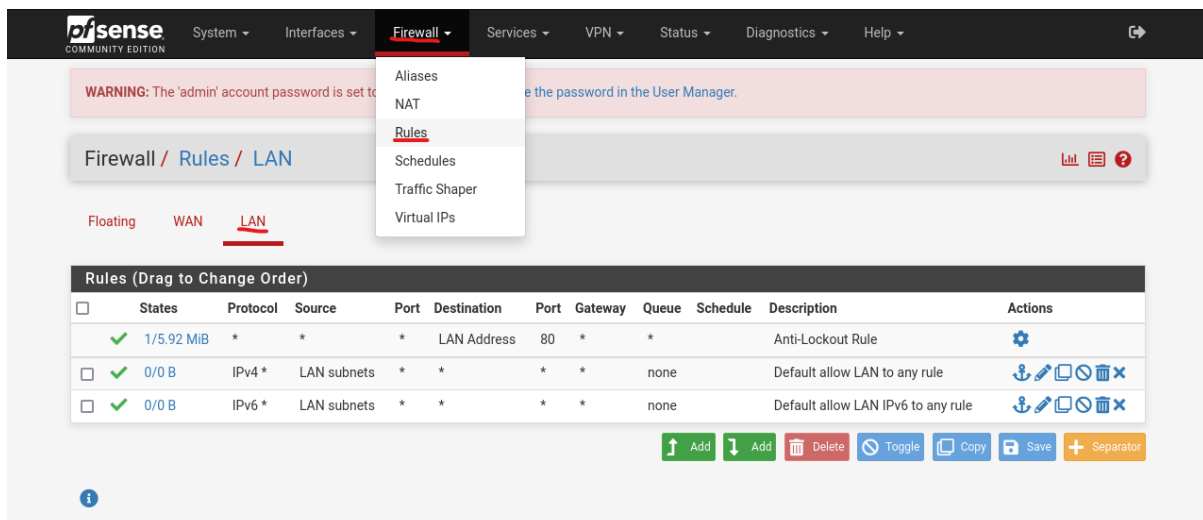
Poi si accede con il browser su **kali** all'interfaccia di configurazione di **pfSense**.



E si comincia la **procedura di policy**.

Per creare una nuova regola **firewall** bisogna andare su :

Firewall->Rules-> Sezione Lan e clicchiamo su Add.



Successivamente avremo un'interfaccia dove avremo dei settaggi da effettuare:

**Action:** in questa sezione si può scegliere come gestire il traffico se farlo passare o bloccarlo. (In questo caso scegliamo Block per impedire il passaggio del traffico)

**Interface:** L'interfaccia da dove arrivano i pacchetti

**Address family:** La versione del protocollo Ipv4 o Ipv6 a quale applicare la policy.

**Protocol:** Si sceglie il protocollo (tcp, udp ...)

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/UDP

Choose which IP protocol this rule should match.

**Source:** In questa sezione si può scegliere che tipo di sorgente inserire, come un indirizzo ipv4/6 network ... , in questo caso si inserisce l'ipv4 della macchina kali (192.168.10.6).

**Destination:** In questa sezione si può scegliere che tipo di sorgente inserire, come un indirizzo ipv4/6 network..., in questo caso si inserisce l'ipv4 della macchina metasploitable (192.168.1.63)

**Destination port range:** In questa sezione si specificano le porte destinazione. (In questo caso si inserisce la porta di default per le richieste [http](#) (80)).

**Source**

Source ☐ Invert match Address or Alias 192.168.10.6 /

[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 192.168.1.63 /

**Destination Port Range** HTTP (80) From Custom To HTTP (80) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Si clicca infine su Save e la regola Firewall verrà creata:

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/6.17 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	<a href="#">Settings</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	192.168.10.6	*	192.168.1.63	*	*	none		Firewall Test	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">X</a>
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">X</a>

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Ora bisogna creare l'interfaccia per l'altra rete (192.168.1.0) ossia quella di **metasploitable** senò **pfsense** non la conosce.

Si va su Interfaces --> Interface Assignments

**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.](#)

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:2b:98:69)
LAN	vtnet0 (08:00:27:53:98:93) <a href="#">Delete</a>

[Save](#)

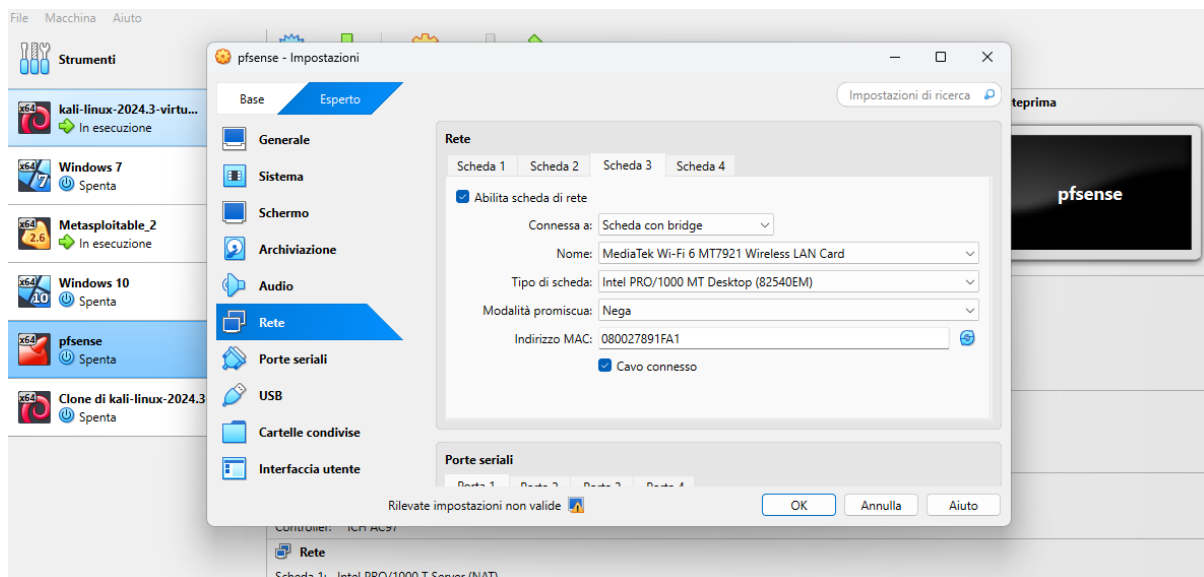
Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

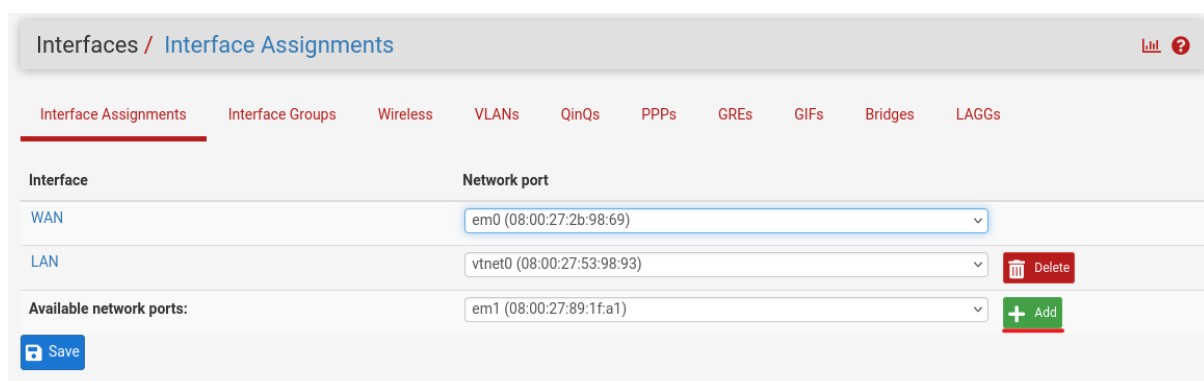
Come vediamo però abbiamo solamente **2 interfacce** una per la wan e una per la lan, quindi bisogna aggiungerne una **3\*** per l'altra rete.

Si torna quindi in questo caso su VirtualBox, **pfsense** e si aggiunge una **3\* scheda di rete**.





Così facendo dopo che si è riavviata la macchina **pfSense**, se si torna sull'interfaccia gui nella sezione Interface, possiamo configurare la **3\* interfaccia**.



Ora andiamo a crearla e a settarla:

Interfaces / LAN2 (em1)

### General Configuration

**Enable** ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
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 or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

### Static IPv4 Configuration

**IPv4 Address**  /

**IPv4 Upstream gateway**  [+ Add a new gateway](#)  
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

Gli assegniamo il nome (Lan2), tipo ip Static IPV4, e gli configuriamo l'ipv4 della macchina metasploitable (192.168.1.63 /24).

Si clicca su save e controlliamo se l'interfaccia è stata creata.

**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.](#)

Interfaces / Interface Assignments

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#) [LAGGs](#)

Interface	Network port	
WAN	em0 (08:00:27:2b:98:69)	
LAN	vtnet0 (08:00:27:53:98:93)	<a href="#">Delete</a>
<b>LAN2</b>	em1 (08:00:27:89:1f:a1)	<a href="#">Delete</a>

[Save](#)

Infine andiamo ad effettuare la prova di **scansione** delle porte e dei servizi sulla macchina Metasploitable, da kali utilizziamo il comando:

"nmap -v -A -sV 192.168.1.63"

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -v -A -sV 192.168.1.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 06:21 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
setup_target: failed to determine route to 192.168.1.63
NSE: Script Post-scanning.
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.51 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

(kali㉿kali)-[~]
$
```

Avendo aggiunto la regola nel **firewall** lo **scan** da **kali** a **metasploit** non funziona, non riuscendo ad accedere a metasploitable, essendo che la regola è stata impostata su "Block", il firewall impedirà il traffico che proviene dalla macchina kali (192.168.10.6) alla macchina Metasploitable (192.168.1.63) .

Per l'esercizio **Bonus** bisogna creare una regola su **pfsense** per bloccare da **kali** il **telnet** verso **metasploitable**, quindi bisogna creare una medesima regola soltanto cambiando la porta invece della **porta 80**, http di base, si mette la **porta 23** standard del **telnet**. Si va nella sezione Rules--> Lan e si crea una medesima regola cambiando soltanto la sezione Destination Port range, mettendo la **porta 23** (predefinita del **Telnet**).

**Source**

Source ☐ Invert match Address or Alias 192.168.10.6 /

[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 192.168.1.63 /

**Destination Port Range** Telnet (23) 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.

Infine avremo una situazione di questo tipo:

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/257 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	<a href="#">Settings</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	192.168.10.6	*	192.168.1.63	80 (HTTP)	*	none		Firewall Test	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	192.168.10.6	*	192.168.1.63	23 (Telnet)	*	none		Firewall Test2	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">X</a>
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">X</a>

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Ora per testare se il blocco funziona bisogna usare il comando: telnet + ip + porta dalla shell di kali:

“telnet 192.168.1.63 23” (indirizzo ip + porta)

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ telnet 192.168.1.63 23
Trying 192.168.1.63 ...
telnet: Unable to connect to remote host: Network is unreachable

(kali@kali)-[~]
$

```

Come da Output anche qui la 2<sup>a</sup> regola del firewall ha bloccato l'accesso al servizio Telnet da Kali verso Metasploitable.