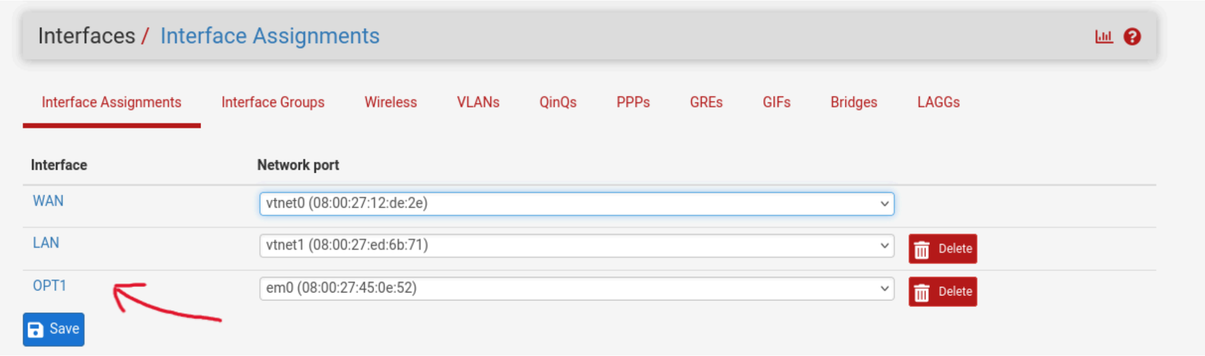
RELAZIONE S3/L5

OBIETTIVO

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

1.Creazione delle interfacce

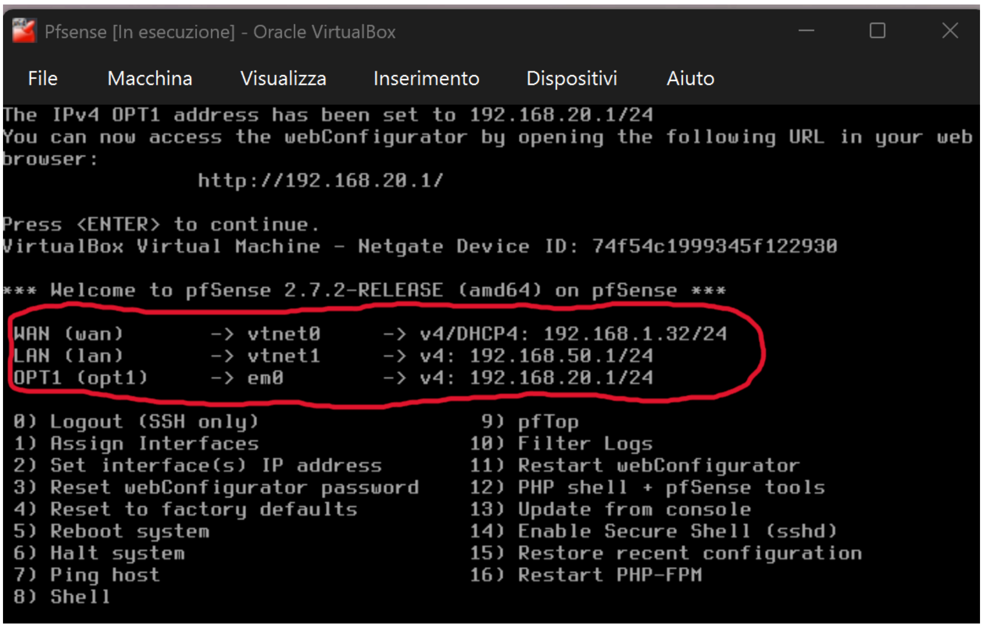
Per prima cosa rechiamoci nella **Web Gui di Pfsense** (bisogna inserire l'IP della WAN) e creiamo una nuova interfaccia di rete:



Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:ed:6b:71)
OPT1	em0 (08:00:27:45:0e:52)

Come si può vedere nell'immagine, abbiamo 3 interfacce:

- **WAN:** collega la rete locale a internet
- **LAN:** l'interfaccia dove è collegata la Kali
- **OPT1:** l'interfaccia dove è collegata Metasploitable

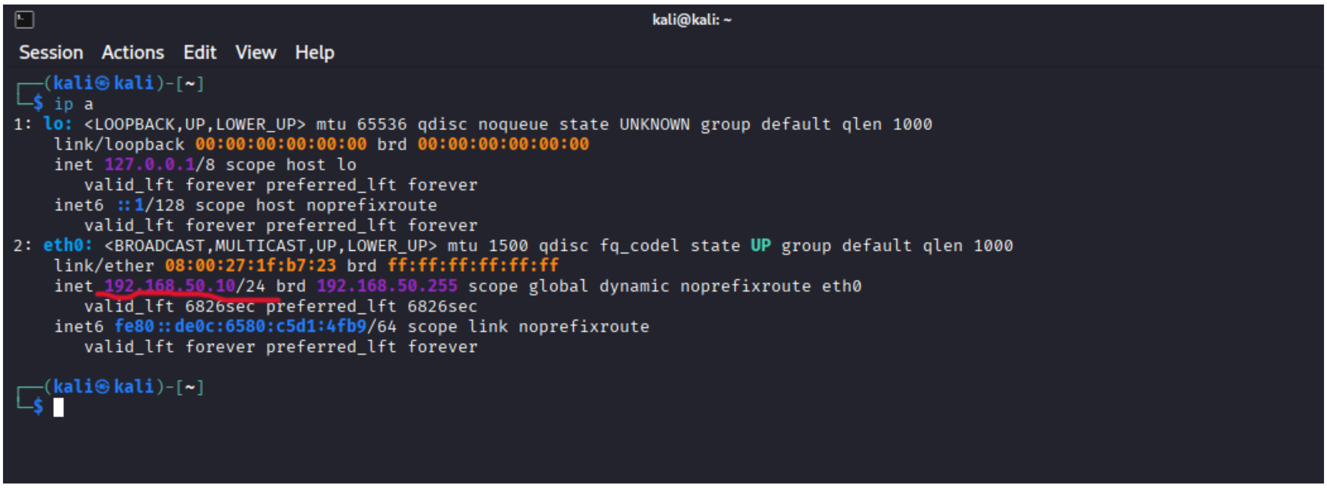


```
The IPv4 OPT1 address has been set to 192.168.20.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.20.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 74f54c1999345f122930

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.1.32/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.50.1/24
 OPT1 (opt1)     -> em0        -> v4: 192.168.20.1/24

 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
```

2.Verifica IP delle macchine virtuali

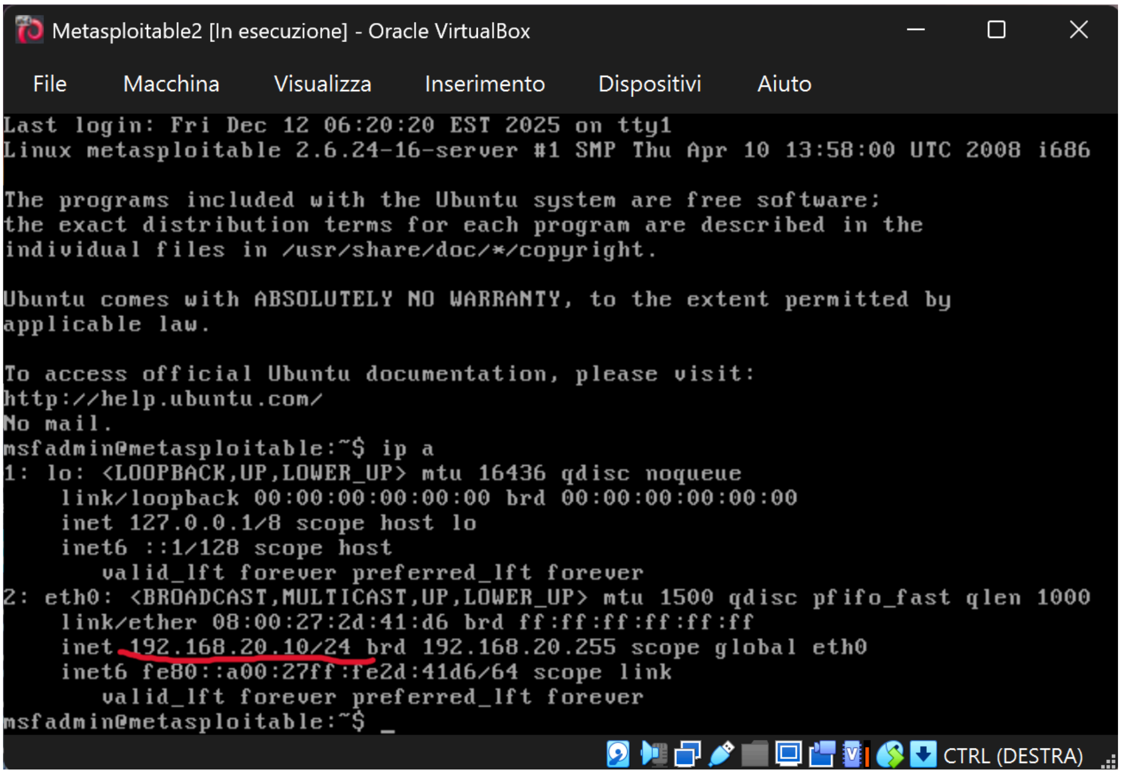
Dopo aver creato e configurato le interfacce, effettuiamo un **test** sulle macchine virtuali per accertarci che entrambe abbiano ricevuto un **IP** dalle rispettive interfacce tramite **DHCP:**

KALI



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.10/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 6826sec preferred_lft 6826sec
    inet6 fe80::de0c:6580:c5d1:4fb9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

META



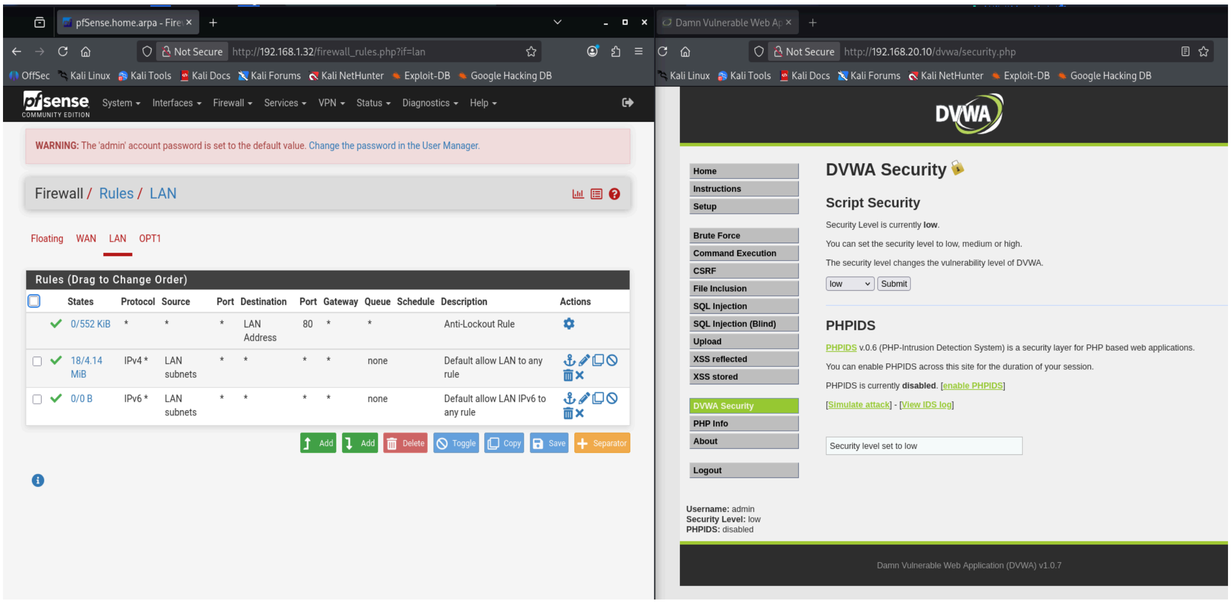
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

```
Last login: Fri Dec 12 06:20:20 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:2d:41:d6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.10/24 brd 192.168.20.255 scope global eth0
    inet6 fe80::a00:27ff:fe2d:41d6/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

3.Creazione regola Firewall

Ora non ci resta che creare una regola **Firewall** per bloccare **SOLO** la navigazione di **Kali** verso **Metasploitable**.

Attualmente se proviamo a navigare verso Metasploitable, possiamo tranquillamente farlo:



pfSense.home.arpa - Fire

Not Secure http://192.168.1.32/firewall_rules.php?if=lan

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

Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/552 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□ ✓	18/4.14 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□ ✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Damn Vulnerable Web Ap

Not Secure http://192.168.20.10/dvwa/security.php

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

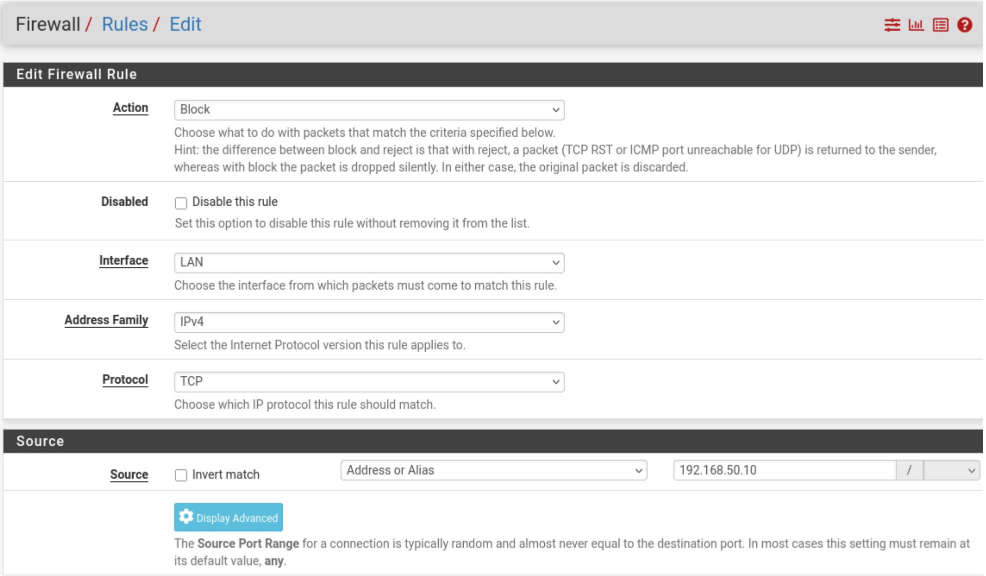
[Simulate attack] - [View IDS log]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Ora rechiamoci in **Firewall > Rules > LAN** e creiamo una nuova regola



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.

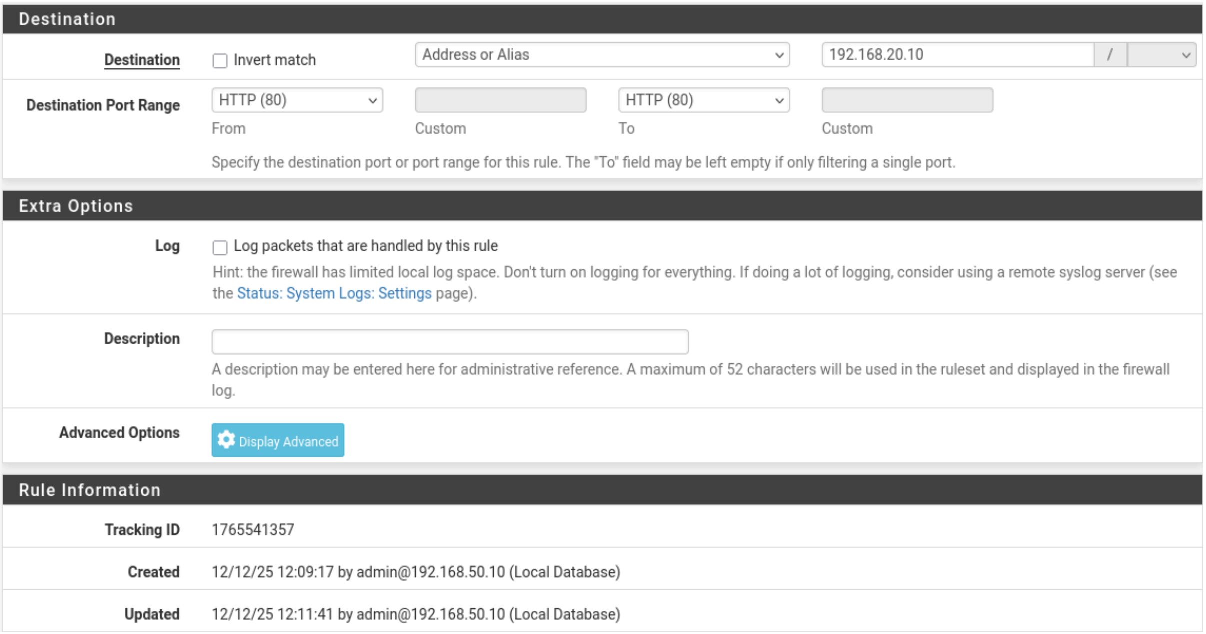
Address Family: IPv4
Select the Internet Protocol version this rule applies to.

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

Source

Source: □ Invert match Address or Alias 192.168.50.10 /

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 · 192.168.20.10 /
Destination Port Range	HTTP (80) From · Custom · HTTP (80) 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.

Extra Options

Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Display Advanced

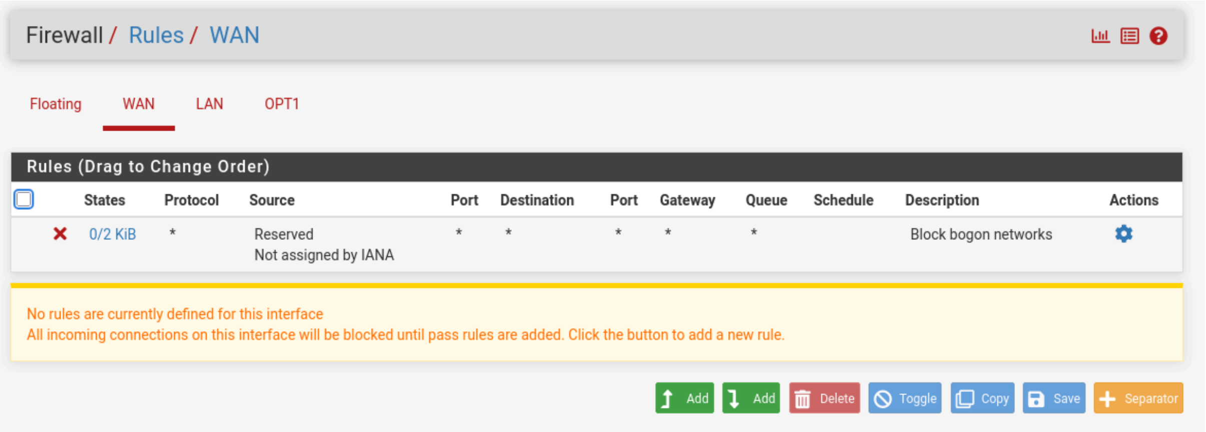
Rule Information

Tracking ID	1765541357
Created	12/12/25 12:09:17 by admin@192.168.50.10 (Local Database)
Updated	12/12/25 12:11:41 by admin@192.168.50.10 (Local Database)

Ho impostato:

- **Action:** block
- **Protocol:** TCP
- **Source Address(IP Kali):** 192.168.50.10
- **Destination Address(Metaspoitable):** 192.168.20.10
- **Destination Port Range:** HTTP(80)

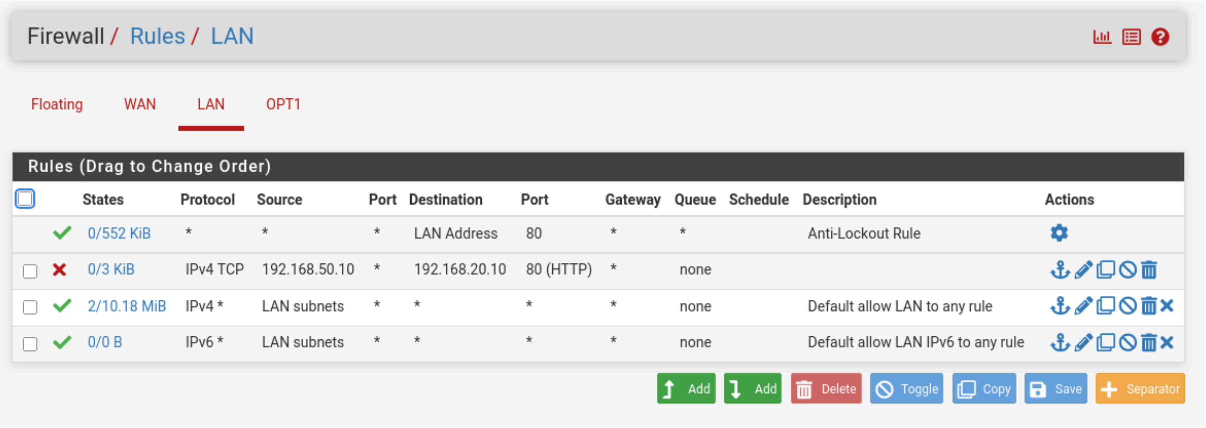
Prima di fare il test, vi mostro una panoramica di tutte le **regole** presenti nelle varie **interfacce**:



Rules (Drag to Change Order)

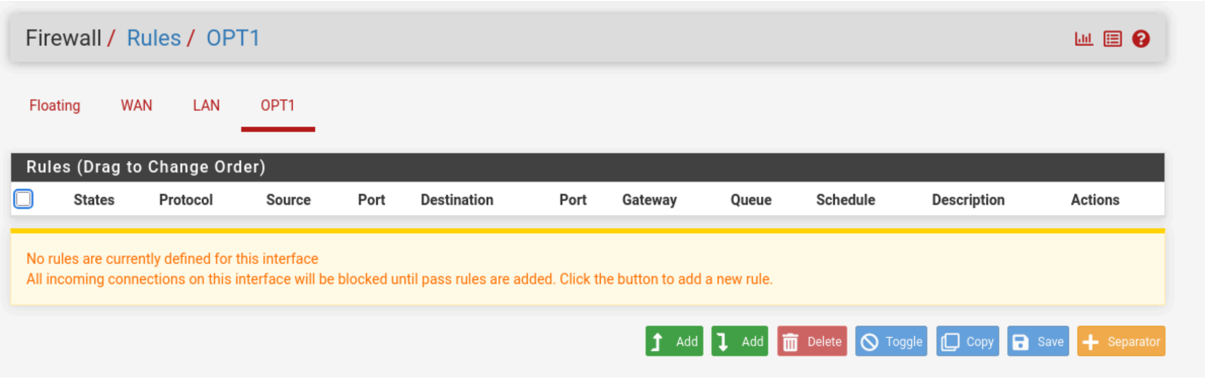
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/552 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐	✗	0/3 KiB	IPv4 TCP	192.168.50.10	*	192.168.20.10	80 (HTTP)	*	none			⚓ ✎ ❐ ⊘ 🗑
☐	✓	2/10.18 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ❐ ⊘ 🗑 ✗
☐	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ❐ ⊘ 🗑 ✗



Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

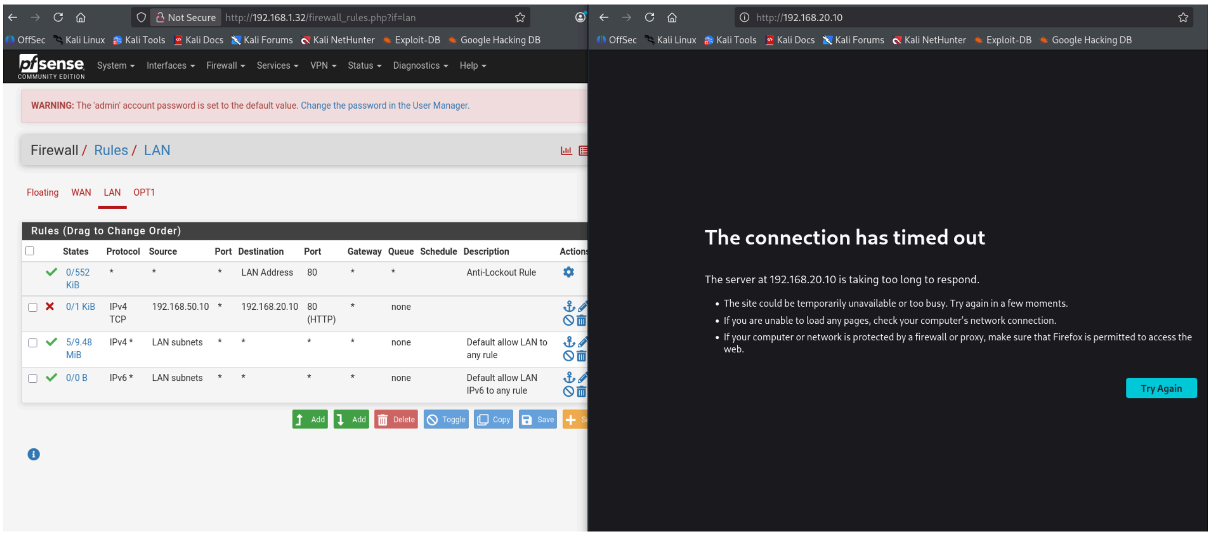
4.Test finale

Per essere sicuri che tutto funzioni **correttamente**, devono succedere 2 cose:

- Quando proviamo a **navigare** dalla **Kali** verso **Metasploitable**, la navigazione deve essere **bloccata**

- Se effettuiamo un **ping** dalla **Kali** verso **Metasploitable**, i pacchetti devono essere consegnati senza problemi

N.B. La regola che abbiamo impostato, blocca solo la navigazione. Non blocca lo scambio di pacchetti.



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

Firewall / Rules / LAN

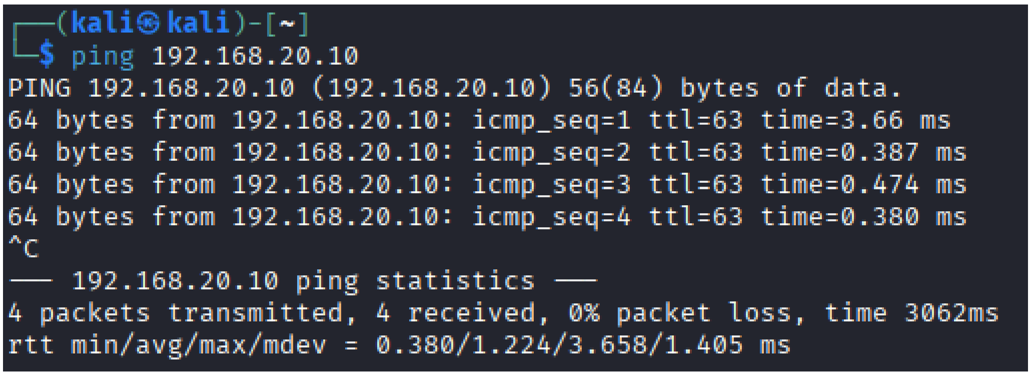
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/552 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✗	0/1 KiB	IPv4 TCP	192.168.50.10	*	192.168.20.10	80 (HTTP)	*	none			
□	✓	5/9.48 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

The connection has timed out

The server at 192.168.20.10 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.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=3.66 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=0.387 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=0.474 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=0.380 ms
^C
--- 192.168.20.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3062ms
rtt min/avg/max/mdev = 0.380/1.224/3.658/1.405 ms
```