

PROGETTO S3/L5

CREAZIONE PRATICA DI UNA REGOLA FIREWALL

Al fine di creare una regola che vada a bloccare il traffico da un'altra rete si utilizza pfsense.  
Per questo esercizio si utilizzerà Kali come macchina bloccante (a cui è già stato assegnato l'indirizzo IP statico 192.168.50.100) e metasploitable come macchina bloccata (a cui è stato assegnato l'indirizzo IP statico 192.168.40.101)

Il primo passaggio è creare un profilo, in questo caso sarà nominato OPT1 e verrà indicata come indirizzo del gateway 192.168.40.1

Enable☒ Enable interface

Description

OPT1

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

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

Default (no preference, typically autoselect)

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

192.168.40.1

/24

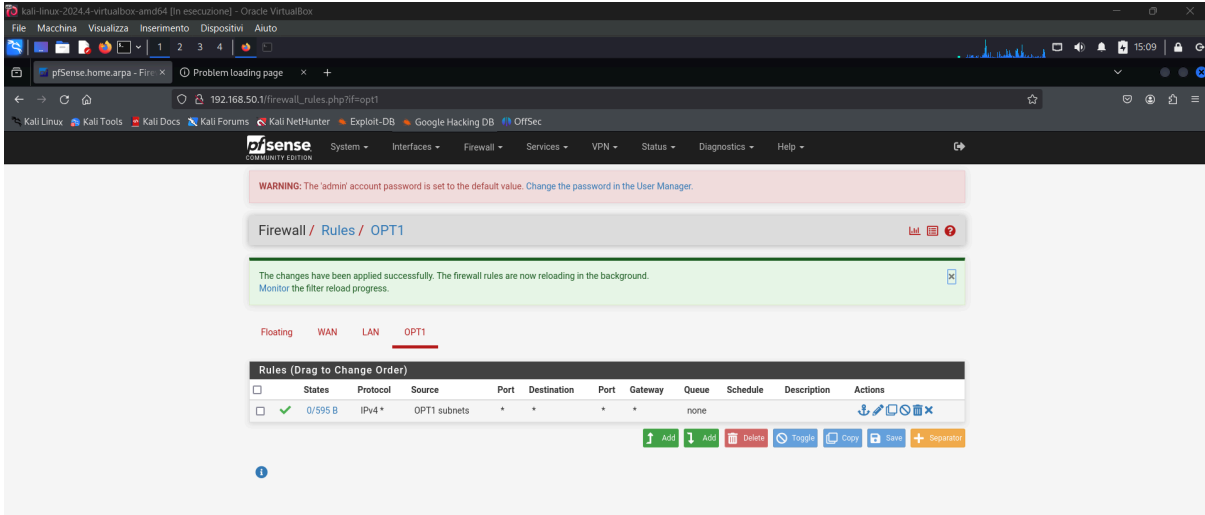
IPv4 Upstream gateway

None

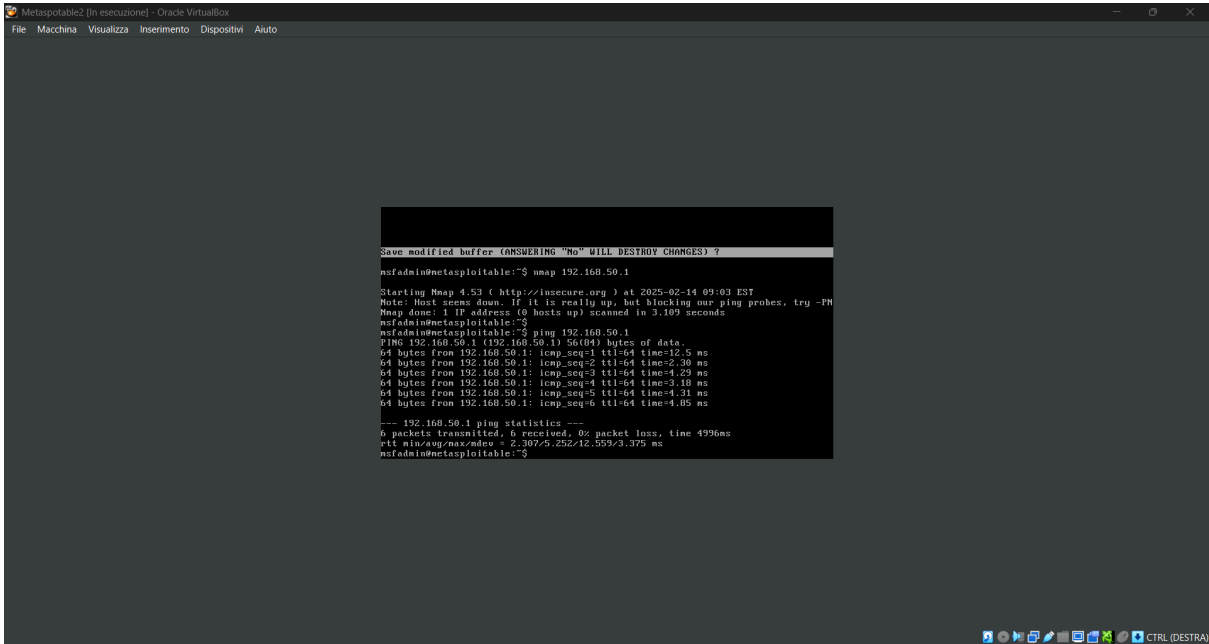
+ Add a new gateway

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](#).

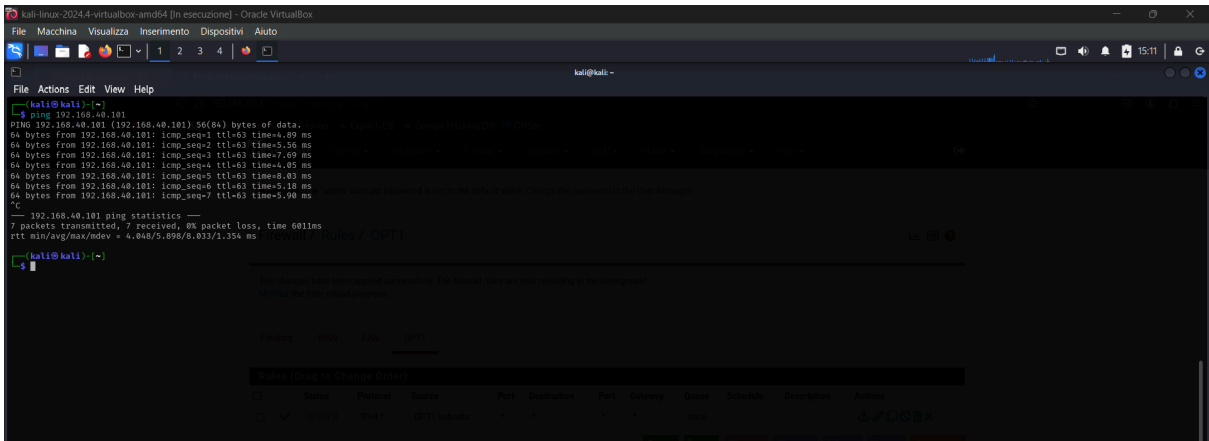
Le rules iniziali per OPT1 prevedono la possibilità di contattare e di essere contattati



Ping dalla macchina 192.168.40.101 al gateway 192.168.50.1



Ping dalla 192.168.50.100 al gateway 192.168.40.1



Successivamente si aggiunge una rule su pfsense che vada a bloccare tutti gli indirizzi della rete 192.168.40.XXX

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

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

OPT1

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

☐ Invert match

OPT1 subnets

Source Address

/

Destination

Destination

☒ Invert match

Any

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

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 / OPT1

Floating
WAN
LAN
OPT1

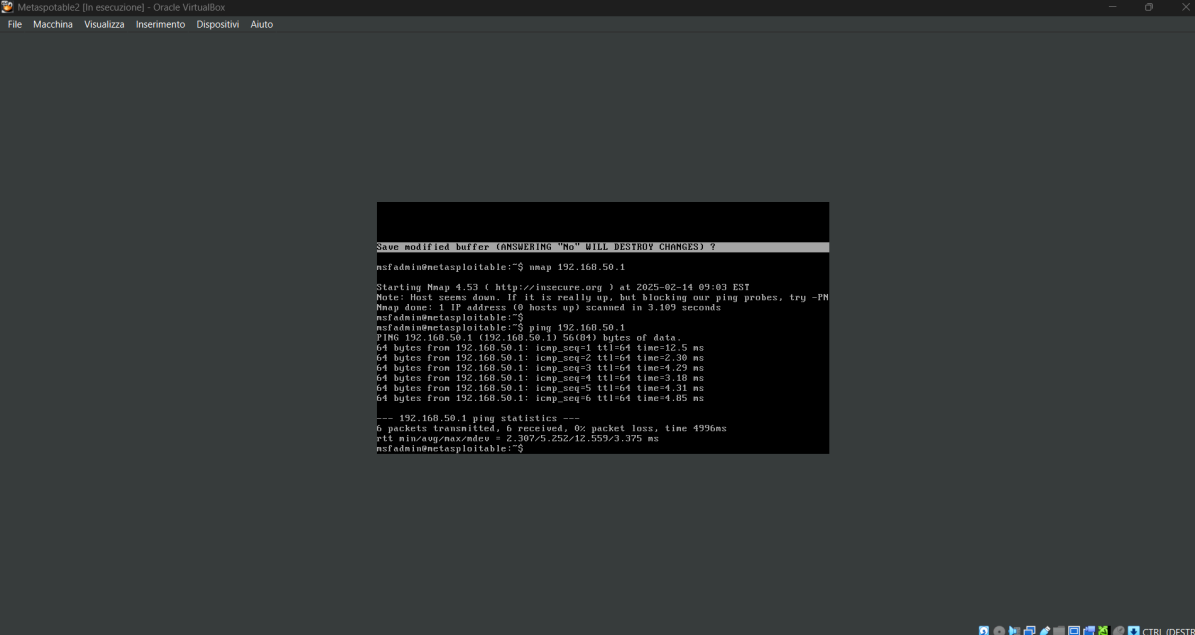
Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/3 KIB	IPv4 *	OPT1 subnets	*	*	*	*	none			

Add
 Add

Delete
 Toggle
 Copy
 Save
 Separator

Si noterà che dalla macchina con indirizzo 192.168.40.101 non sarà possibile contattare la rete con gateway 192.168.50.1, cioè quella su cui è stata inserita la regola firewall.



```
Metasploit> [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

nsfadmin@metasploit> $ nmap 192.168.50.1

Starting Nmap 4.53 ( http://nmap.org ) at 2025-02-14 09:03 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 3.109 seconds
nsfadmin@metasploit> $
nsfadmin@metasploit> $ ping 192.168.50.1
Png 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=12.5 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=2.30 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=4.29 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=3.18 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=4.31 ms
64 bytes from 192.168.50.1: icmp_seq=6 ttl=64 time=4.05 ms

--- 192.168.50.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4996ms
rtt min/avg/max/mdev = 2.307/5.252/12.553/3.375 ms
nsfadmin@metasploit> $
```