

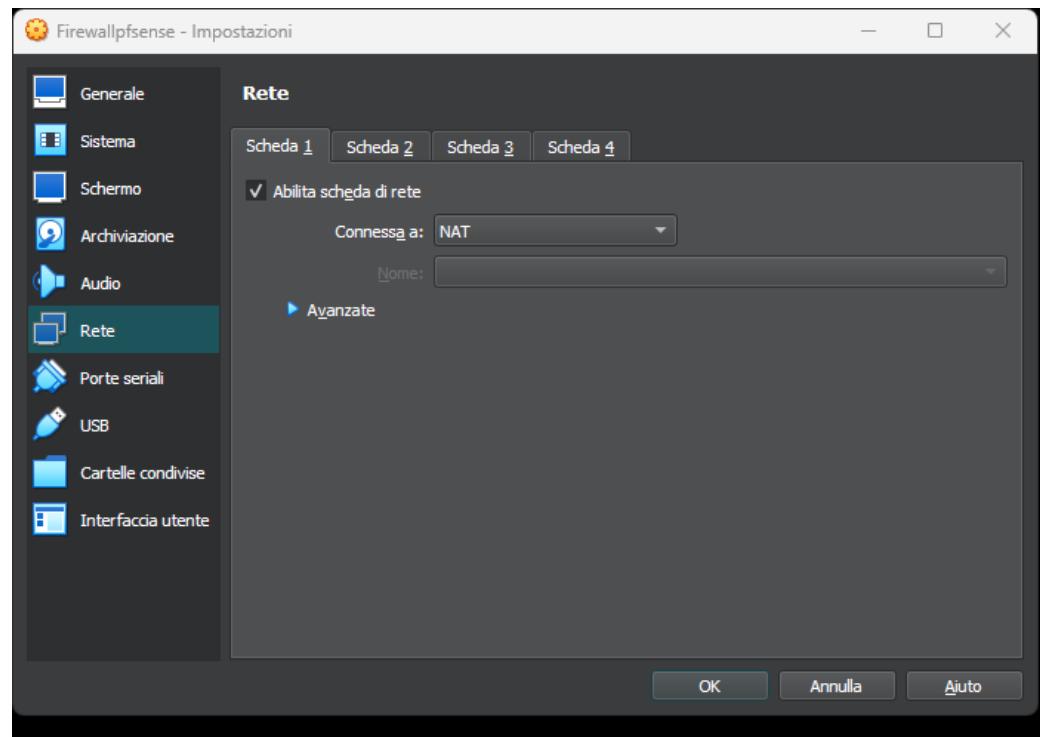
S5 L1

Imposto le 3 schede di rete di pfsense.

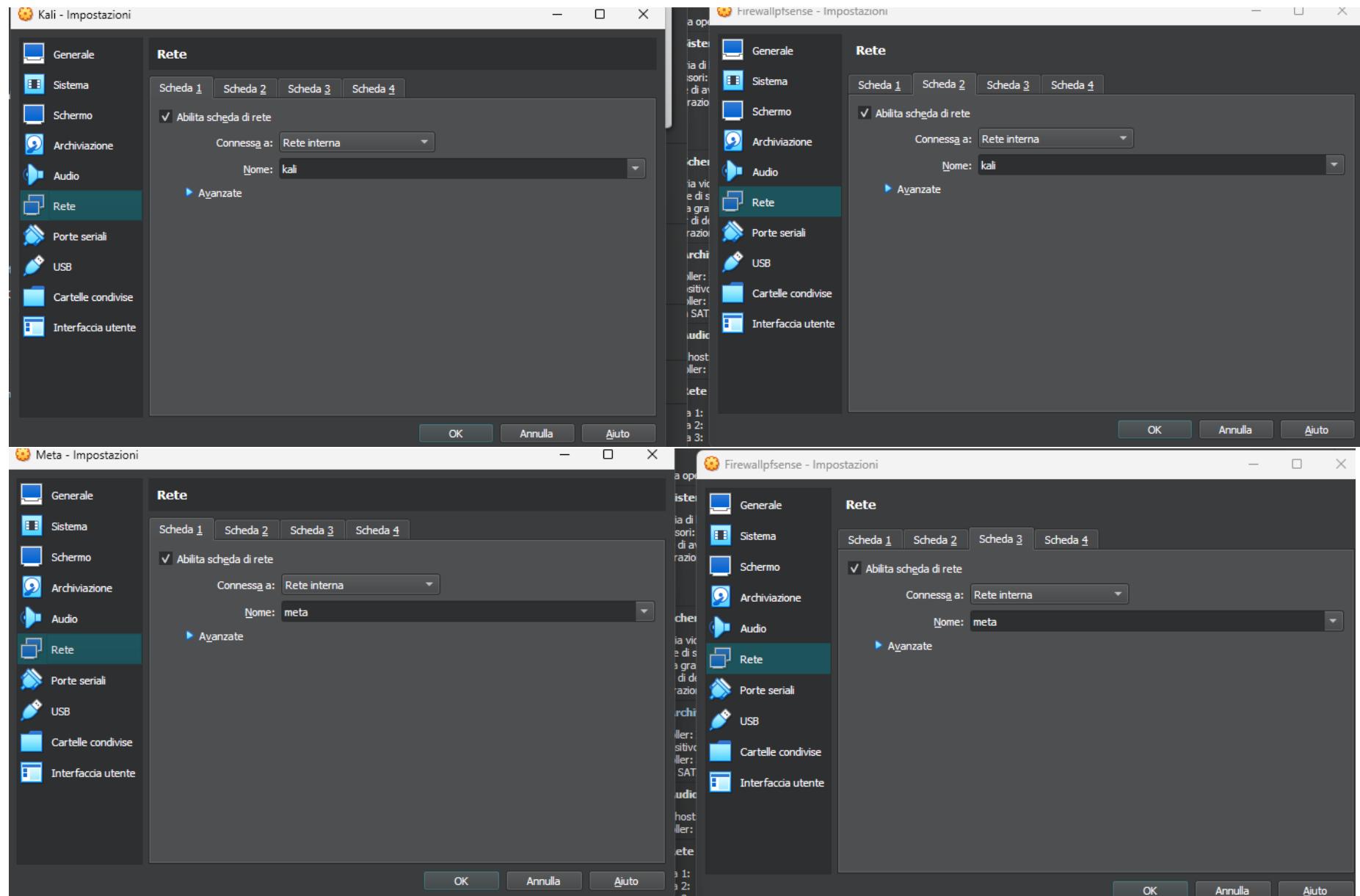
La prima su NAT

La seconda col nome kali, sarà la rete dov'è presente la vm kali

La terza dove sarà presente la vm metà



Configuro le macchine, affinchè siano sotto la rete giusta



Configuro la macchina kali, dove imposto come default gateway, l'ip di pfsense. E configuro l'interfaccia relativa alla scheda di rete.

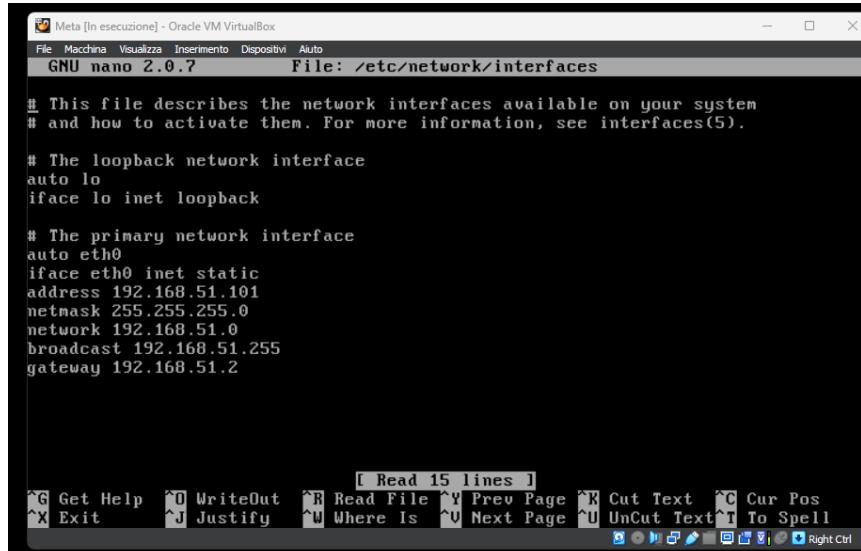
The image shows two windows from a Kali Linux desktop environment. The left window is a configuration interface for a network interface named 'kali'. It includes sections for General Configuration (with 'Enable interface' checked), IPv4 Configuration (set to Static IPv4 with address 192.168.50.2), and Static IPv4 Configuration (specifying the upstream gateway as 'None'). The right window is a terminal session showing the contents of the /etc/network/interfaces file. The file defines the loopback interface (auto lo) and the eth0 interface (inet static with address 192.168.50.100, netmask 255.255.255.0, broadcast 192.168.50.255, and gateway 192.168.50.2). The terminal also displays nano editor status bar information and various command-line navigation keys.

```
GNU nano 7.2 /etc/network/interfaces
This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.2
```

Faccio lo stesso per metasploit e relativa scheda di rete pfSense



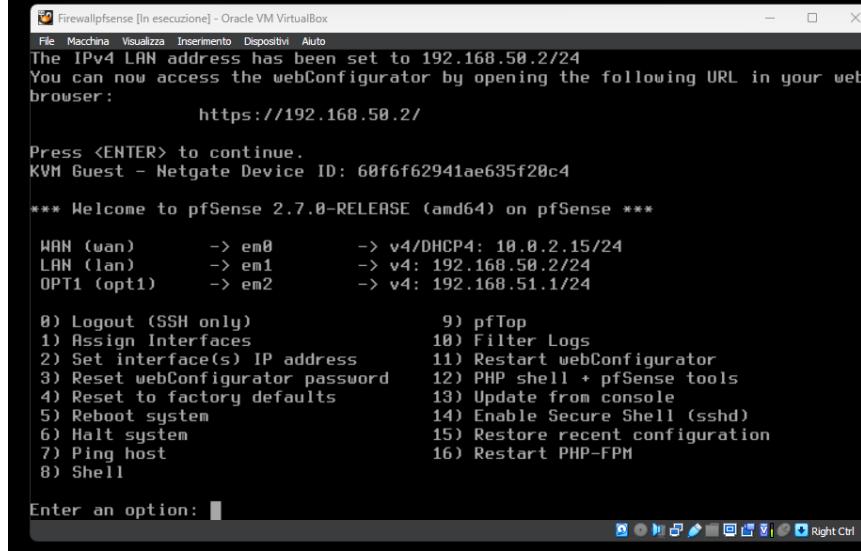
```
File Macchina Visualizza Inserimento Dispositivi Auto
GNU nano 2.0.7  File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.51.101
    netmask 255.255.255.0
    network 192.168.51.0
    broadcast 192.168.51.255
    gateway 192.168.51.2

[ Read 15 lines ]
^C Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
^W Right Ctrl
```



```
File Macchina Visualizza Inserimento Dispositivi Auto
The IPv4 LAN address has been set to 192.168.50.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.50.2/

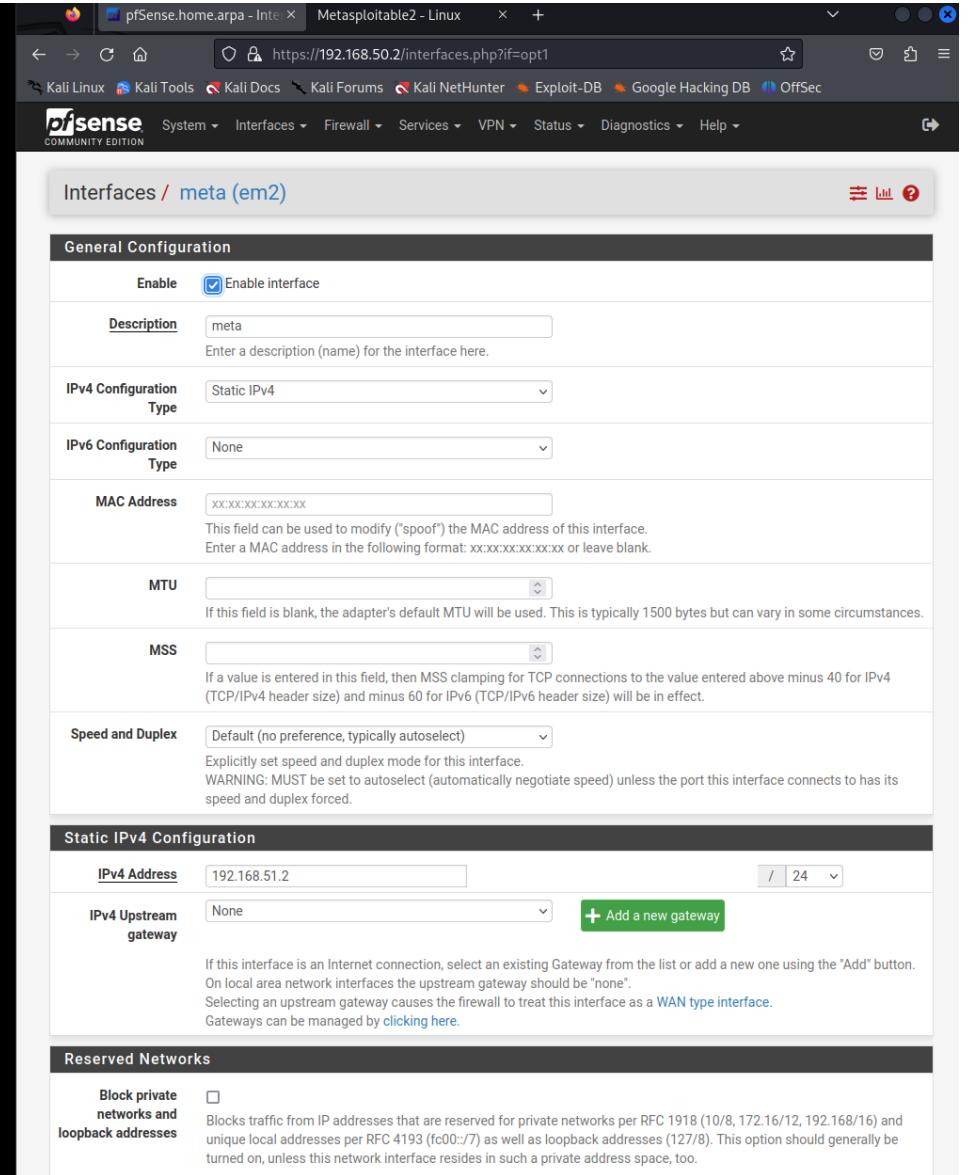
Press <ENTER> to continue.
KVM Guest - Netgate Device ID: 60f6f62941ae635f20c4

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.2/24
OPT1 (opt1)    -> em2      -> v4: 192.168.51.1/24

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: [
```



pfSense - pfSense Community Edition

Interfaces / meta (em2)

General Configuration

Enable Enable interface

Description meta

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address XX:XX:XX:XX:XX:XX

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)

Static IPv4 Configuration

IPv4 Address 192.168.51.2 / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)

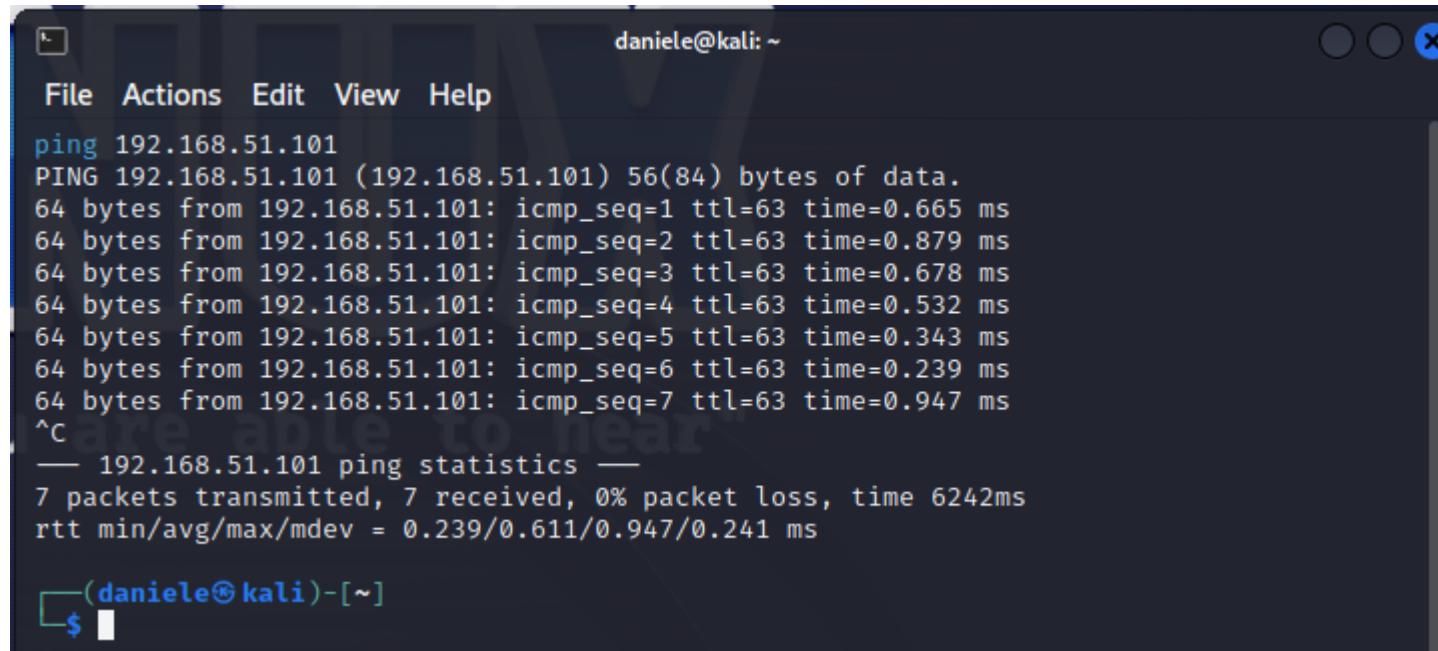
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a **WAN** type interface.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

Reserved Networks

Block private networks and loopback addresses

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Possiamo notare che da kali avviene il ping verso metà, pur essendo su di una rete diversa.



A screenshot of a terminal window titled "daniele@kali: ~". The window contains the output of a "ping" command. The output shows several ICMP echo requests being sent to the IP address 192.168.51.101. The responses show varying round-trip times (rtt) and sequence numbers (icmp_seq). The terminal window has a dark background with light-colored text. The title bar and menu bar are visible at the top. The prompt "(daniele@kali)-[~]" is at the bottom left, and a small dollar sign (\$) is at the bottom right.

```
ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.665 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=0.879 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.678 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.343 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.239 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.947 ms
^C
--- 192.168.51.101 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6242ms
rtt min/avg/max/mdev = 0.239/0.611/0.947/0.241 ms
```

Imposto una regola firewall per blocca pacchetti di tipo icmp da kali verso meta.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/111 Kib	*	*	*	KALI Address	443 *	*			Anti-Lockout Rule	
✗ 0/0 B	IPv4 ICMP any	192.168.50.100	*	192.168.51.101	*	*	none		block icmp	
✓ 1/26 Kib	IPv4 *	KALI net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	KALI net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

The terminal window shows a ping command being run:

```
daniele@kali:~$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
--- 192.168.51.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3083ms
```

The terminal also displays a banner at the bottom: "Welcome, the more you type, the more you are able to hear".

Ho impostato una regola per bloccare le richieste sulla porta 80 da kali verso metasploit. Utilizzando reject, avremo subito risposta dal browser con unable to connect. Con la regola block, invece ci sarà un lungo caricamento della pagina, finchè la connessione non va in timeout.

The screenshot illustrates a network setup where traffic from Kali Linux (IP 192.168.51.101) is being blocked by a pfSense firewall rule. The browser on Kali shows an 'unable to connect' error, while the terminal session shows successful ping tests to the target host.

pfSense Firewall Rules (KALI Tab):

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/170 Kib	*	*	*	KALI Address	443 80	*	*		Anti-Lockout Rule	
0/672 B	IPv4 ICMP any	192.168.50.100	*	192.168.51.101	*	*	none		block icmp	
0/180 B	IPv4 TCP	192.168.50.100	*	192.168.51.101	80 (HTTP)	*	none		reject http	
0/33 Kib	IPv4 *	KALI net	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	KALI net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Firefox Browser Error:

Unable to connect
An error occurred during a connection to 192.168.51.101.
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.
[Try Again](#)

Terminal Session (daniele@kali: ~)

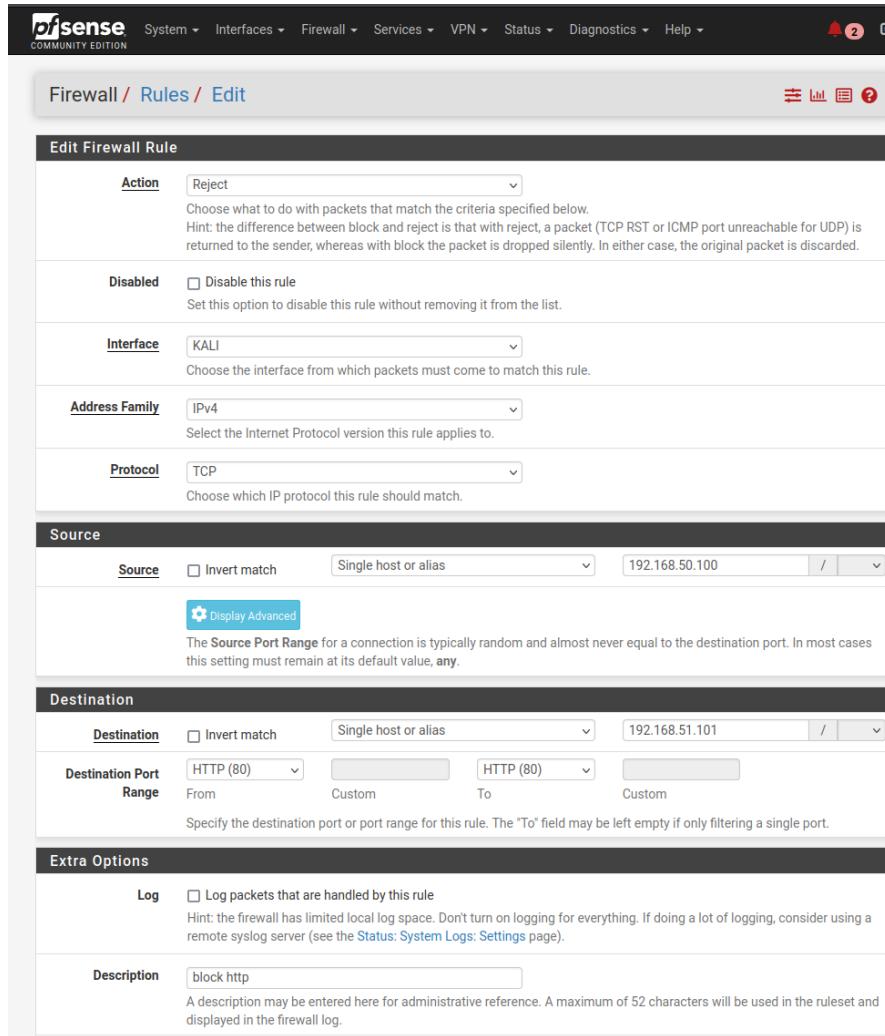
```

(daniele@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.336 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.652 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.353 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.520 ms
^C
--- 192.168.51.101 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6075ms
rtt min/avg/max/mdev = 0.336/0.623/1.290/0.298 ms

(daniele@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
--- 192.168.51.101 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7163ms

(daniele@kali)-[~]
$ 

```



Unable to connect

An error occurred during a connection to 192.168.51.101.

- 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.

[Try Again](#)

File Actions Edit View Help

```
ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
--- 192.168.51.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3083ms

(daniele@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.336 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.652 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.353 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.520 ms
^C
--- 192.168.51.101 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6075ms
rtt min/avg/max/mdev = 0.336/0.623/1.290/0.298 ms
```

(daniele@kali)-[~]

\$

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: KALI
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 Single host or alias 192.168.50.100 / [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 Single host or alias 192.168.51.101 / [Display Advanced](#)
Destination Port Range: 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.

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: block http
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: 1698055777

The connection has timed out

The server at 192.168.51.101 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.

[Try Again](#)

Timed Out

Welcome, the more you

```
daniele@kali: ~
File Actions Edit View Help
ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
--- 192.168.51.101 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3083ms

(daniele@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.336 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.652 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.353 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.520 ms
^C
--- 192.168.51.101 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6075ms
rtt min/avg/max/mdev = 0.336/0.623/1.290/0.298 ms

(daniele@kali)-[~]
$
```