

# Consegna S3L5

## Traccia

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

## Introduzione

Nella consegna ci viene chiesto di configurare un firewall con pfsense in modo da gestire il traffico fra le due reti e bloccare l'accesso alla DVWA da Kali Linux per impedire lo scan. Quindi andiamo prima a verificare il traffico fra le due macchine virtuali e successivamente lo andremo a bloccare tramite un firewall pfsense.

## Svolgimento

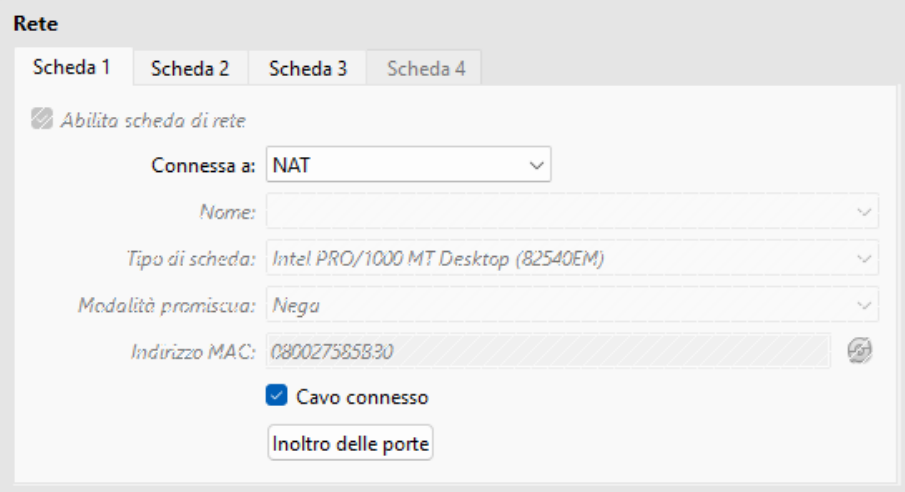
Andiamo a configurare le schede di rete in pfsense

Wan > en0

Lan 1 > vetnet0 (intnet)

Lan 2 > vetnet 1 (meta)

### Pfsense:



The screenshot shows the 'Rete' (Network) configuration page in pfSense, specifically the 'Scheda 1' (NIC 1) tab. The interface is in Italian. The 'Abilita scheda di rete' (Enable network card) checkbox is checked. The 'Connessa a:' (Connected to) dropdown is set to 'NAT'. The 'Nome:' (Name) field is empty. The 'Tipo di scheda:' (Card type) dropdown is set to 'Intel PRO/1000 MT Desktop (82540EM)'. The 'Modalità promiscua:' (Promiscuous mode) dropdown is set to 'Nega'. The 'Indirizzo MAC:' (MAC address) field is set to '080027585B30'. The 'Cavo connesso' (Cable connected) checkbox is checked. There is a button labeled 'Inoltro delle porte' (Port forwarding) at the bottom.

**Rete**

Scheda 1   Scheda 2   Scheda 3   Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: intnet

Tipo di scheda: Rete paravirtualizzata (virtio-net)

Modalità promiscua: Nega

Indirizzo MAC: 080027657608

☒ Cavo connesso

**Rete**

Scheda 1   Scheda 2   Scheda 3   Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: meta

Tipo di scheda: Rete paravirtualizzata (virtio-net)

Modalità promiscua: Nega

Indirizzo MAC: 080027D02774

☒ Cavo connesso

E configuriamo le schede di rete delle nostre Virtual Machine nel seguente modo:

### Kali Linux:

**Rete**

Scheda 1   Scheda 2   Scheda 3   Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: intnet

Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)

Modalità promiscua: Nega

Indirizzo MAC: 080027135CF8

☒ Cavo connesso

## Metasploitable:

**Rete**

Scheda 1   Scheda 2   Scheda 3   Scheda 4

☒ Abilita scheda di rete

Connessa a: Rete interna

Nome: meta

Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)

Modalità promiscua: Nega

Indirizzo MAC: 080027EA8A42

☒ Cavo connesso

Ora configuriamo manualmente le interfacce in Kali e in Metasploitable.

## Kali linux:

Editing Static 50

Connection name: Static 50

General   Ethernet   802.1X Security   DCB   Proxy   **IPv4 Settings**   IPv6 Settings

Method: Manual

**Addresses**

Address	Netmask	Gateway
192.168.50.100	24	192.168.50.1

DNS servers: 192.168.50.1

Search domains:

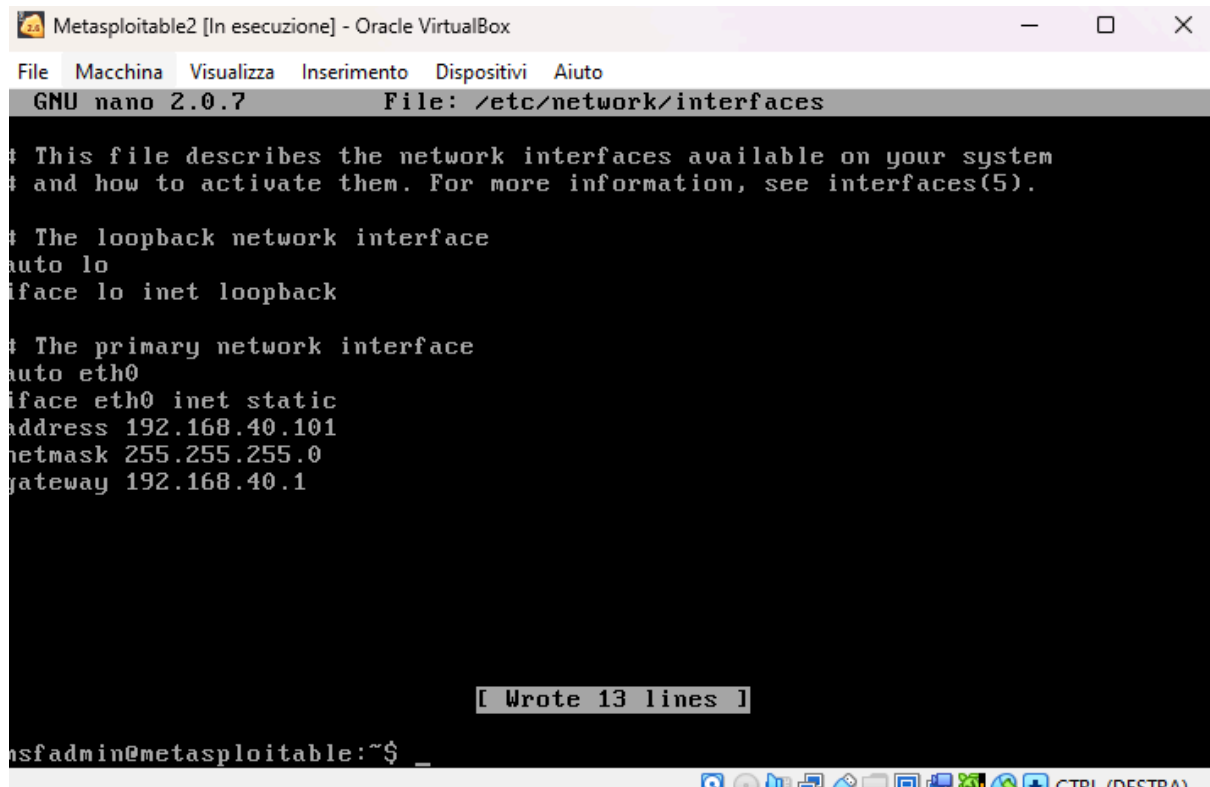
DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel   Save

## Metasploitable:



```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
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).

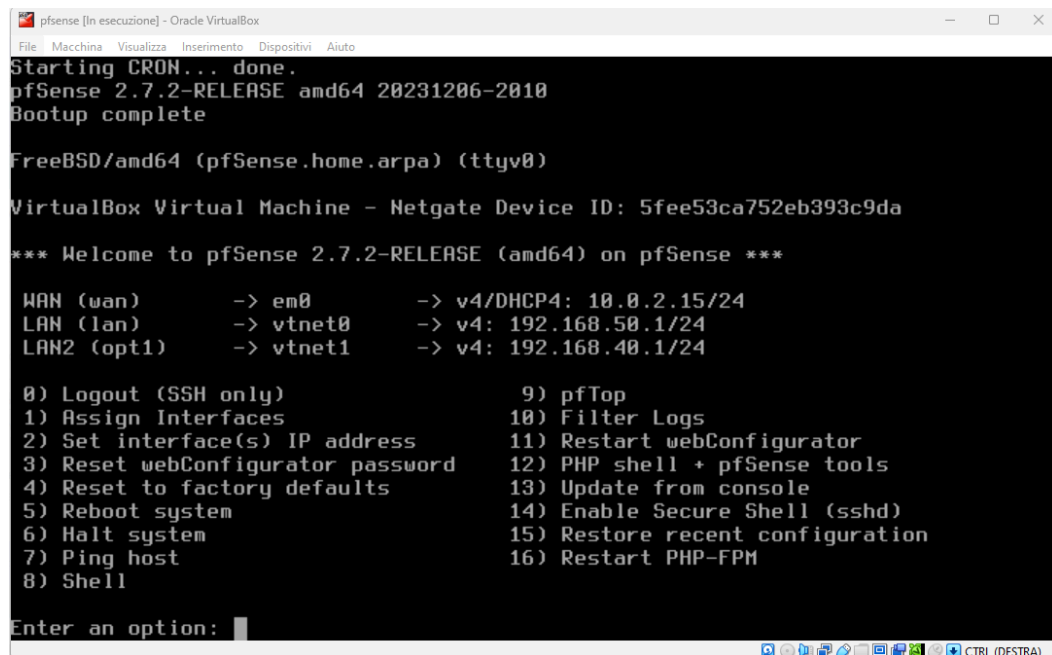
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.40.101
netmask 255.255.255.0
gateway 192.168.40.1

[ Wrote 13 lines ]

msfadmin@metasploitable:~$ _
```

Quindi controlliamo tramite pfsense che sia tutto settato in modo corretto:



```
pfSense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 5fee53ca752eb393c9da

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0    -> v4: 192.168.50.1/24
LAN2 (opt1)    -> vtnet1    -> v4: 192.168.40.1/24

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: 
```

Wan > en0 > 10.0.2.15

Lan 1 > vtnet0 (intnet) > 192.168.50.1

Lan 2 > vtnet 1 (meta) > 192.168.40.1

Ora procediamo con la configurazione del Firewall con pfsense nel seguente modo.

Abilitiamo la Lan2

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	em0 (08:00:27:58:5b:30)
LAN	vtnet0 (08:00:27:65:76:0b)
Lan2	vtnet1 (08:00:27:d0:27:74)

Save

Settiamo le regole della Lan2 nel firewall pfsense

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

LAN2

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

LAN2 subnets

Source Address

/

Destination

Destination

☐ Invert match

Any

Destination Address

/

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

1739528582

Created

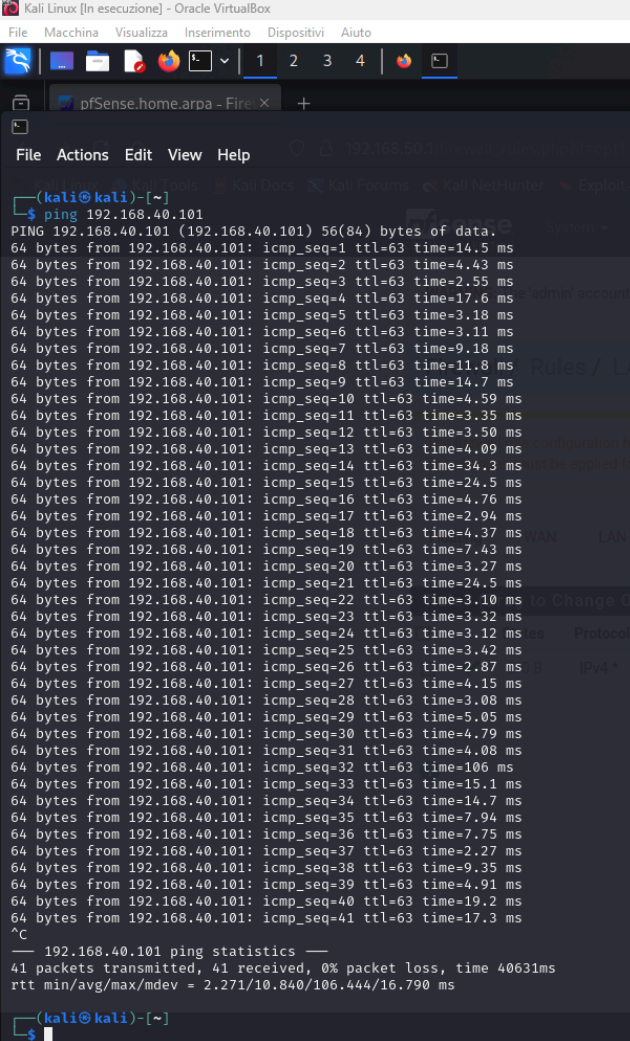
2/14/25 10:23:02 by admin@192.168.50.100 (Local Database)

Updated

2/14/25 10:23:02 by admin@192.168.50.100 (Local Database)

Save

Ora che tutto è stato impostato le VM possono comunicare tra di loro:



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

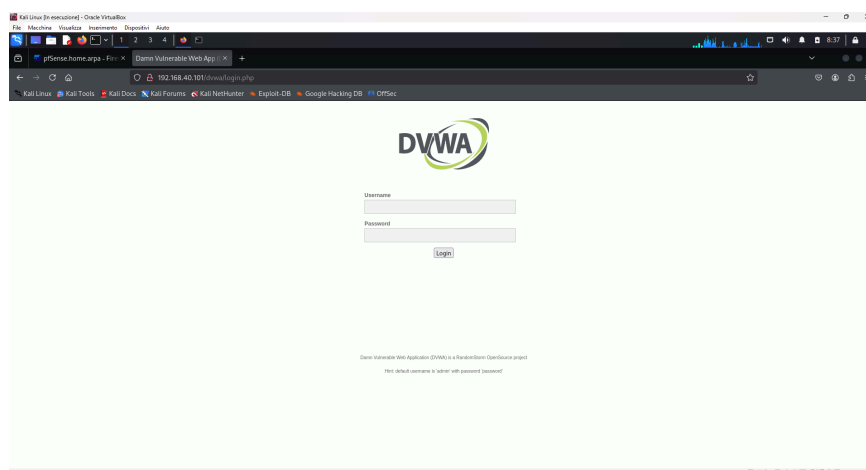
pfSense.home.arpa - Fire X +

File Actions Edit View Help

(kali@kali)-[~]
$ ping 192.168.40.101
PING 192.168.40.101 (192.168.40.101) 56(84) bytes of data:
64 bytes from 192.168.40.101: icmp_seq=1 ttl=63 time=14.5 ms
64 bytes from 192.168.40.101: icmp_seq=2 ttl=63 time=4.43 ms
64 bytes from 192.168.40.101: icmp_seq=3 ttl=63 time=2.55 ms
64 bytes from 192.168.40.101: icmp_seq=4 ttl=63 time=17.6 ms
64 bytes from 192.168.40.101: icmp_seq=5 ttl=63 time=3.18 ms
64 bytes from 192.168.40.101: icmp_seq=6 ttl=63 time=3.11 ms
64 bytes from 192.168.40.101: icmp_seq=7 ttl=63 time=9.18 ms
64 bytes from 192.168.40.101: icmp_seq=8 ttl=63 time=11.8 ms
64 bytes from 192.168.40.101: icmp_seq=9 ttl=63 time=14.7 ms
64 bytes from 192.168.40.101: icmp_seq=10 ttl=63 time=4.59 ms
64 bytes from 192.168.40.101: icmp_seq=11 ttl=63 time=3.35 ms
64 bytes from 192.168.40.101: icmp_seq=12 ttl=63 time=3.50 ms
64 bytes from 192.168.40.101: icmp_seq=13 ttl=63 time=4.09 ms
64 bytes from 192.168.40.101: icmp_seq=14 ttl=63 time=34.3 ms
64 bytes from 192.168.40.101: icmp_seq=15 ttl=63 time=24.5 ms
64 bytes from 192.168.40.101: icmp_seq=16 ttl=63 time=4.76 ms
64 bytes from 192.168.40.101: icmp_seq=17 ttl=63 time=2.94 ms
64 bytes from 192.168.40.101: icmp_seq=18 ttl=63 time=4.37 ms
64 bytes from 192.168.40.101: icmp_seq=19 ttl=63 time=7.43 ms
64 bytes from 192.168.40.101: icmp_seq=20 ttl=63 time=3.27 ms
64 bytes from 192.168.40.101: icmp_seq=21 ttl=63 time=24.5 ms
64 bytes from 192.168.40.101: icmp_seq=22 ttl=63 time=3.10 ms
64 bytes from 192.168.40.101: icmp_seq=23 ttl=63 time=3.32 ms
64 bytes from 192.168.40.101: icmp_seq=24 ttl=63 time=3.12 ms
64 bytes from 192.168.40.101: icmp_seq=25 ttl=63 time=3.42 ms
64 bytes from 192.168.40.101: icmp_seq=26 ttl=63 time=2.87 ms
64 bytes from 192.168.40.101: icmp_seq=27 ttl=63 time=4.15 ms
64 bytes from 192.168.40.101: icmp_seq=28 ttl=63 time=3.08 ms
64 bytes from 192.168.40.101: icmp_seq=29 ttl=63 time=5.05 ms
64 bytes from 192.168.40.101: icmp_seq=30 ttl=63 time=4.79 ms
64 bytes from 192.168.40.101: icmp_seq=31 ttl=63 time=4.08 ms
64 bytes from 192.168.40.101: icmp_seq=32 ttl=63 time=106 ms
64 bytes from 192.168.40.101: icmp_seq=33 ttl=63 time=15.1 ms
64 bytes from 192.168.40.101: icmp_seq=34 ttl=63 time=14.7 ms
64 bytes from 192.168.40.101: icmp_seq=35 ttl=63 time=7.94 ms
64 bytes from 192.168.40.101: icmp_seq=36 ttl=63 time=7.75 ms
64 bytes from 192.168.40.101: icmp_seq=37 ttl=63 time=2.27 ms
64 bytes from 192.168.40.101: icmp_seq=38 ttl=63 time=9.35 ms
64 bytes from 192.168.40.101: icmp_seq=39 ttl=63 time=4.91 ms
64 bytes from 192.168.40.101: icmp_seq=40 ttl=63 time=19.2 ms
64 bytes from 192.168.40.101: icmp_seq=41 ttl=63 time=17.3 ms
^C
— 192.168.40.101 ping statistics —
41 packets transmitted, 41 received, 0% packet loss, time 40631ms
rtt min/avg/max/mdev = 2.271/10.840/106.444/16.790 ms

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

Ora dobbiamo creare una regola firewall che blocca l'accesso alla DVWA. Accediamo all'interfaccia di DVWA inserendo l'ip della metasploitable e vediamo che l'accesso ci viene consentito.



Ora andiamo a creare la nostra regola per impedire a kali di aver accesso a DVWA:

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/579 KIB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.40.101	80 (HTTP)	*	none		

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

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

192.168.50.100

/

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

Address or Alias

192.168.40.101

/

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

1739540059

Created

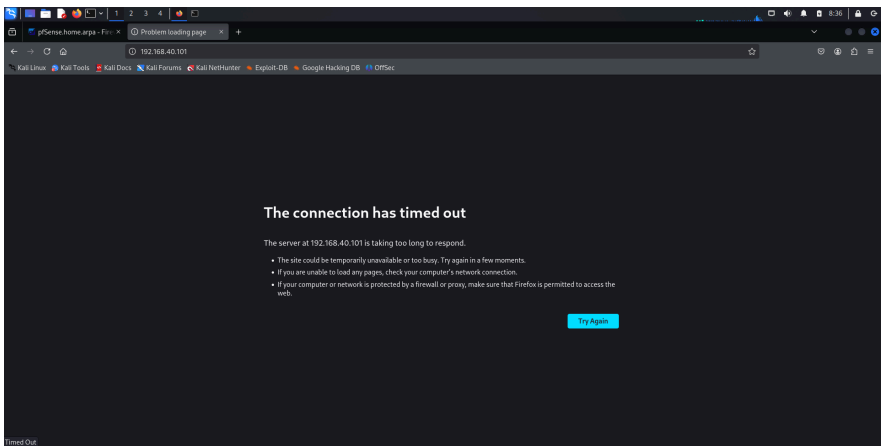
2/14/25 13:34:19 by admin@192.168.50.100 (Local Database)

Updated

2/14/25 13:34:19 by admin@192.168.50.100 (Local Database)

Save

Grazie a questa regola sarà impossibile raggiungere la pagina a causa del firewall.



Grazie al comando nmap possiamo andare a verificare lo stato della porta 80 prima con il blocco attivo e poi con il blocco disattivato:

```
(kali㉿kali)-[~]
└─$ nmap -p80 -A 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-14 09:36 EST
Nmap scan report for 192.168.40.101
Host is up (0.010s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   3.32 ms  pfSense.home.arpa (192.168.50.1)
2   5.61 ms  192.168.40.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds

(kali㉿kali)-[~]
└─$ nmap -p80 -A 192.168.40.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-14 09:37 EST
Nmap scan report for 192.168.40.101
Host is up (0.014s latency).

PORT      STATE      SERVICE VERSION
80/tcp    open      http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.29 (Gentoo)
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   3.18 ms  pfSense.home.arpa (192.168.50.1)
2  10.26 ms  192.168.40.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

## Conclusione

Nell'esercizio di oggi siamo andati a configurare un firewall pfsense, le macchine virtuali con le rispettive schede di rete e con indirizzi statici, e verificato la loro connettività tramite il comando ping.

Successivamente abbiamo creato delle regole firewall per fare in modo che la macchina kali non potesse effettuare traffico sulla porta 80 in modo da bloccare un eventuale scansione di vulnerabilità.