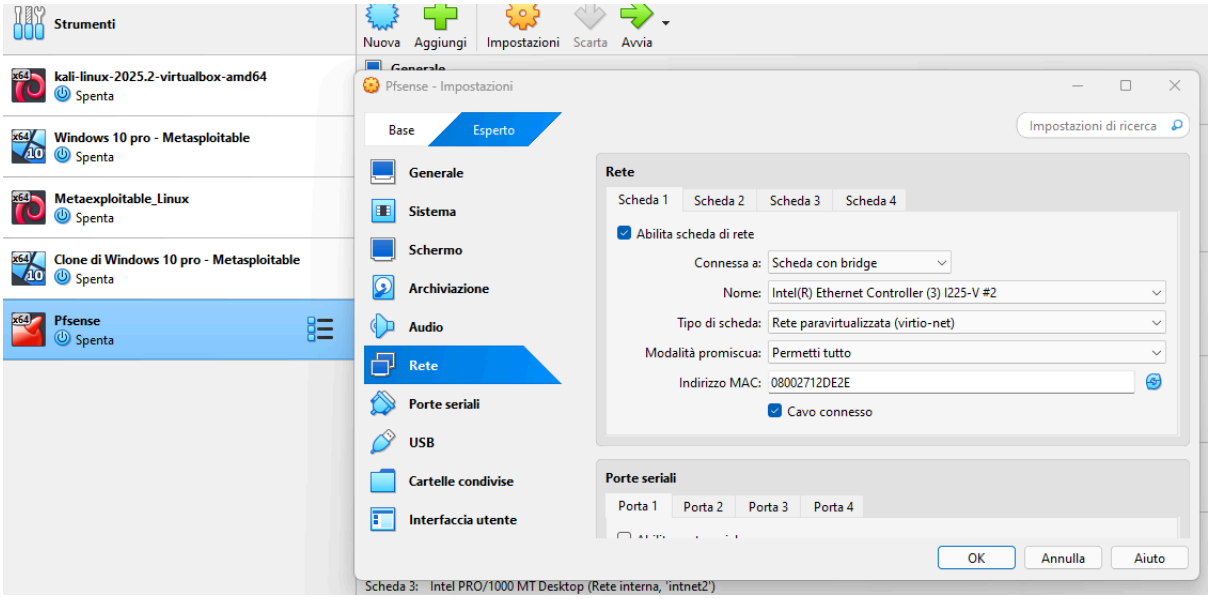
TRACCIA:

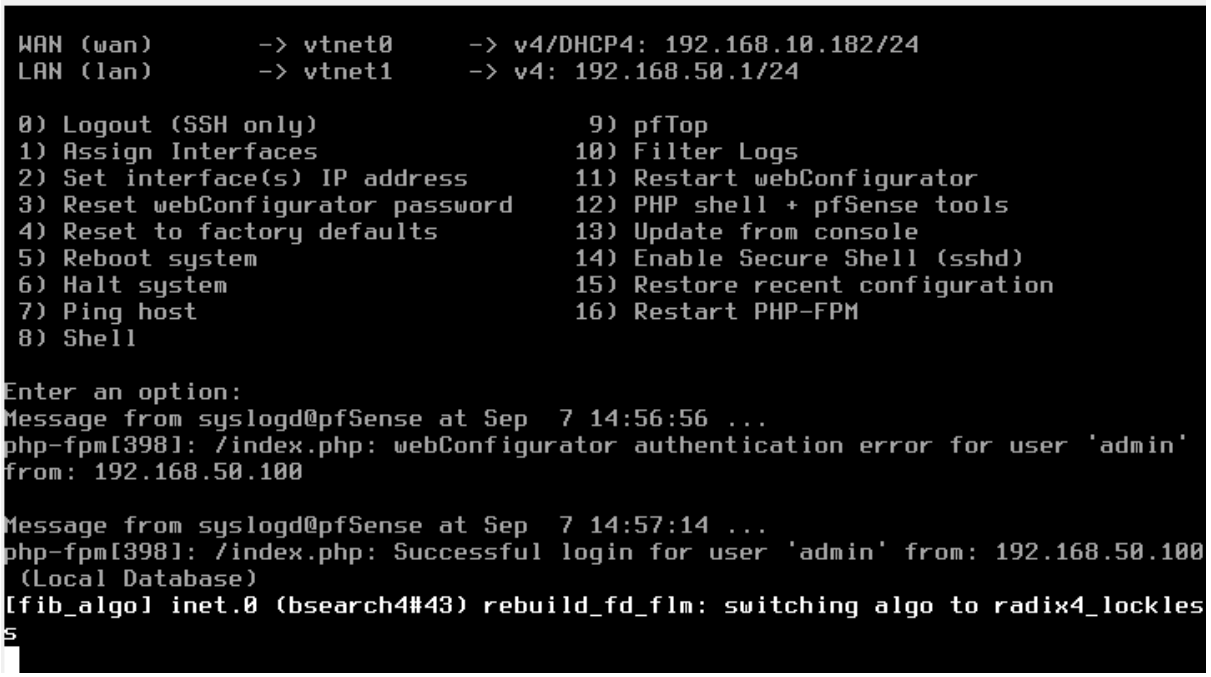
Questa esercitazione è divisa in due fasi preliminari (1 e 2) e una terza che sarà l'esercizio da svolgere autonomamente (3):

1. Installazione di Pfsense e configurazione architettura di rete di partenza (aka architettura target);
2. Creazione guidata di una policy firewall generica;
3. Esercizio che prevede la creazione di un'ulteriore rete e l'applicazione di una policy firewall tra le due reti;
    a. Facoltativo: approfondimenti sulla gestione dei log e del troubleshooting di rete

1. INSTALLAZIONE PFSENSE E CONFIGURAZIONE ARCHITETTURA DI RETE DI PARTENZA.

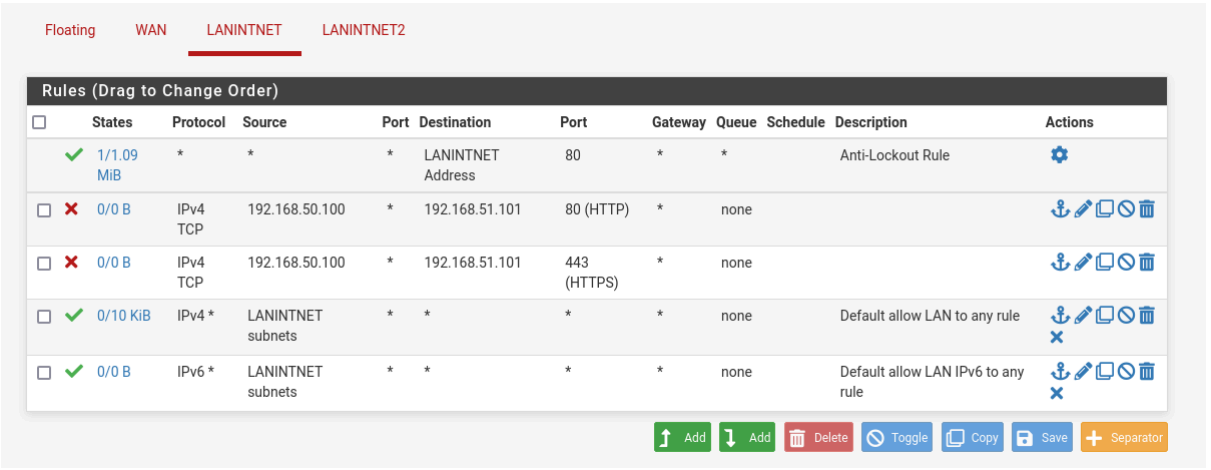


ho installato la macchina pfsense ho impostato le schede di rete come da esercizio a macchina spenta.



ho acceso la macchina pfsense ho cambiato l'ip lan, poi su kali sono andata su firefox con l'ip della macchina pfsense per configurare le regole del firewall.

2. CREAZIONE GUIDATA DI UNA POLICY FIREWALL



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 LANINTNET

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

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 | 192.168.51.101 /

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 1757260870

Created 9/7/25 18:01:10 by admin@192.168.50.100 (Local Database)

Updated 9/7/25 18:01:10 by admin@192.168.50.100 (Local Database)

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
LANINTNET
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**.

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
192.168.51.101 /

Destination Port Range
HTTPS (443) — From
Custom
HTTPS (443) — 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

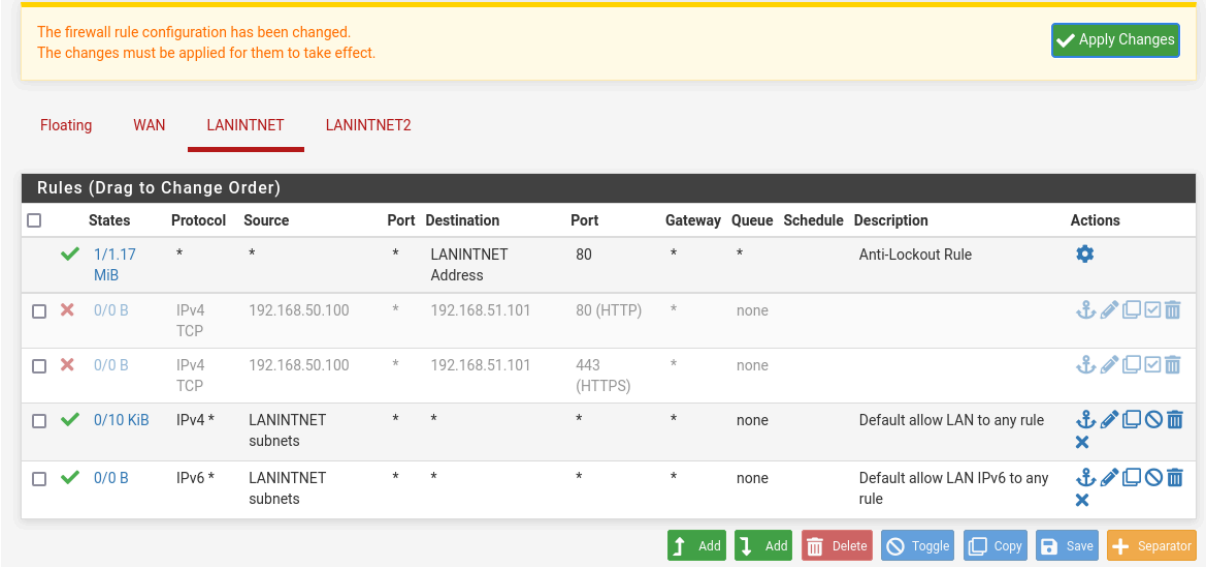
Tracking ID 1757260922

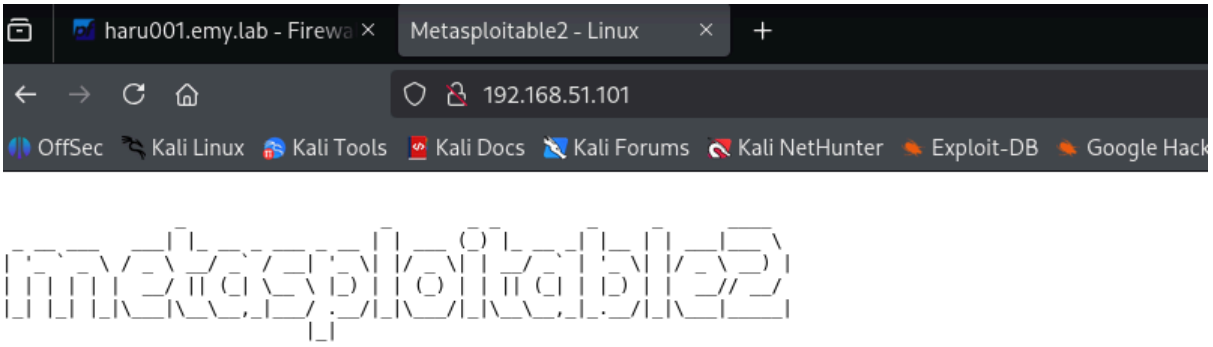
Created 9/7/25 18:02:02 by admin@192.168.50.100 (Local Database)

Updated 9/7/25 18:02:02 by admin@192.168.50.100 (Local Database)

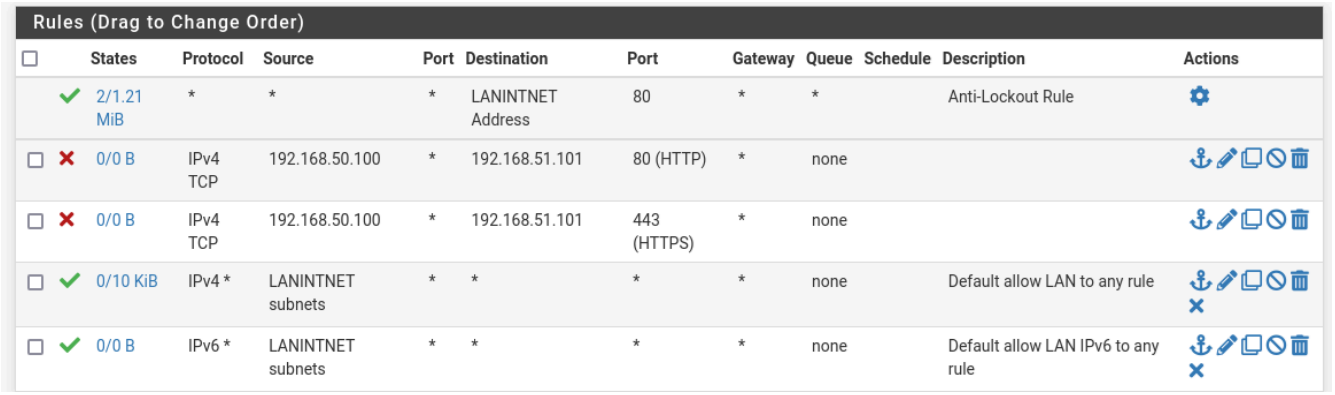
```
        sysctl [-n] [-e] -A
root@metasploitable:/home/msfadmin# /etc/init.d/restart networking
bash: /etc/init.d/restart: No such file or directory
root@metasploitable:/home/msfadmin# /etc/init.d/restart network
bash: /etc/init.d/restart: No such file or directory
root@metasploitable:/home/msfadmin# /etc/init.d/reboot
.bash_history               .rhosts
.distcc/                    .ssh/
.mysql_history              .sudo_as_admin_successful
.profile                    vulnerable/
root@metasploitable:/home/msfadmin# /etc/init.d/networking restart
 * Reconfiguring network interfaces...                                  [ OK ]
root@metasploitable:/home/msfadmin# 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 08:00:27:9a:8b:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
    inet6 fe80::a00:27ff:fe9a:8b1e/64 scope link
       valid_lft forever preferred_lft forever
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
```

ho creato le regole del firewall ho selezionato block perché l'esercizio ci dice di bloccare da kali l'accesso alla DVWA di meta ho selezionato l'interfaccia di rete poi ipv4 il tipo di protocollo TCP ho selezionato con l'opzione address o alias l'indirizzo ip di kali nella voce sorgente e nella voce destinazione quello di meta (cambiato l'ultimo screenshot) ho salvato e applicato le regole per completezza per bloccare tutto il traffico anche se l'esercizio non lo chiedeva perchè DVWA utilizza il protocollo in chiaro HTTP sulla porta 80 ho creato un altra regola con le stesse caratteristiche bloccando anche il protocollo HTTPS cifrato sulla porta 443.



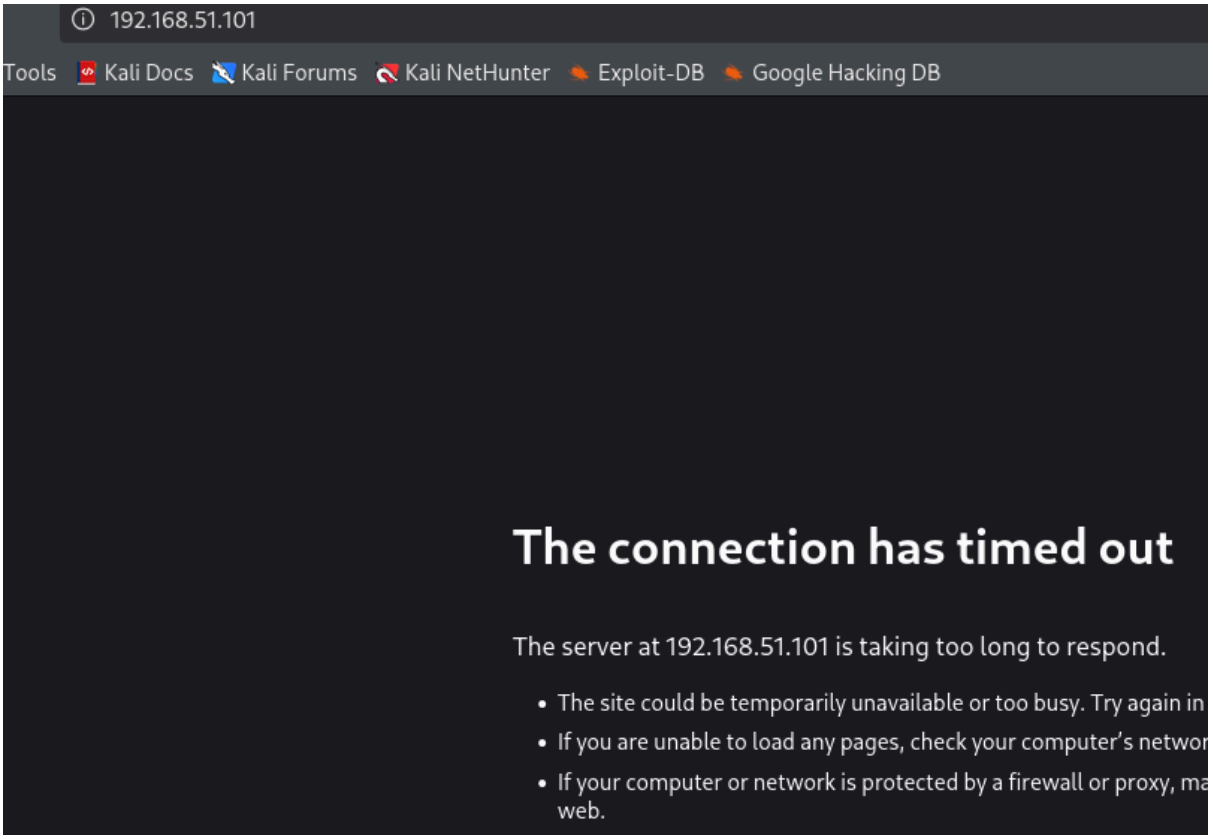


come si vede dagli screenshot se disabilito le regole appena create da kali posso raggiungere DVWA di meta.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2/1.21 MiB	*	*	*	LANINTNET Address	80	*	*		Anti-Lockout Rule	
✗	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.51.101	80 (HTTP)	*	none			
✗	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.51.101	443 (HTTPS)	*	none			
✓	0/10 KiB	IPv4 *	LANINTNET subnets	*	*	*	*	none		Default allow LAN to any rule	
✓	0/0 B	IPv6 *	LANINTNET subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	



se le regole firewall sono abilitate non riesco a connettermi a DVWA di meta, cercando su internet ho constatato sarebbe più corretto mettere la regola reject per avere una risposta di refused piuttosto che un time out come nel caso del block.