

## PROGETTO S3 L5



### Obiettivo :

Implementare una soluzione di sicurezza di rete attraverso pfSense per controllare il traffico tra due macchine virtuali posizionate su segmenti di rete differenti.

In particolare, impedire alla macchina Kali Linux di accedere al servizio DVWA (Damn Vulnerable Web Application) presente su Metasploitable2.7

### RISPOSTA

Comincio con il Setup delle Macchine Virtuali

Per rispettare i requisiti dell'esercizio, ho configurato le due macchine su reti completamente separate:

```

(kali㉿kali)-[~]
$ ip a
: 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
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever

```

## Macchina Kali Linux:

Indirizzo IP: 192.168.50.100/24

```

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK> mtu 16436 qdisc noop
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:72:ce:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.100/24 brd 192.168.70.255 scope global eth0
    inet6 fe80::a00:27ff:fe72:ce0f/64 scope link
        valid_lft forever preferred_lft forever

msfadmin@metasploitable:~$ root add default gw 192.168.70.1

```

## Macchina Metasploitable2:

Indirizzo IP: 192.168.70.100/24

Gateway: 192.168.70.1

## Configurazione di pfSense

Procedo con la configurazione pfSense per gestire entrambe le reti. Ho dovuto aggiungere una nuova interfaccia e configurarla:

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="meta"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> 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	<input type="text"/> 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	<input type="text"/> 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	<input type="text" value="192.168.70.1"/> / 24
IPv4 Upstream gateway	<input type="text" value="metaGW - 192.168.70.100"/> <a href="#">+ Add a new gateway</a> If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.


## Parametri della nuova interfaccia

Nome: "meta"

Tipo: Static IPv4

Indirizzo: 192.168.70.1/24

# CREAZIONE DELLA REGOLA

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 / 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

Destination

Destination

☐ Invert match

Address or Alias

192.168.70.100

/

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

Blocco Accesso da Kali a DVWA

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

1752835700

Created

7/18/25 10:48:20 by admin@192.168.50.100 (Local Database)

Updated

7/18/25 13:06:01 by admin@192.168.50.100 (Local Database)

Save

Attraverso la sezione Firewall >>> Rules >>> LAN e ho creato una nuova regola con le seguenti caratteristiche:

## Parametri

**Azione:** Block (scarta i pacchetti senza notificare il mittente)

**Interfaccia:** LAN (da dove proviene il traffico di Kali)

**Address Family:** IPv4

**Protocollo:** TCP

**Sorgente:** 192.168.50.100 (indirizzo di Kali Linux)

**Destinazione:** 192.168.70.100 (indirizzo di Metasploitable2)

**Porta di Destinazione:** HTTP (80)

**Descrizione:** "Blocco accesso Kali a DVWA"

## Posizionamento della Regola

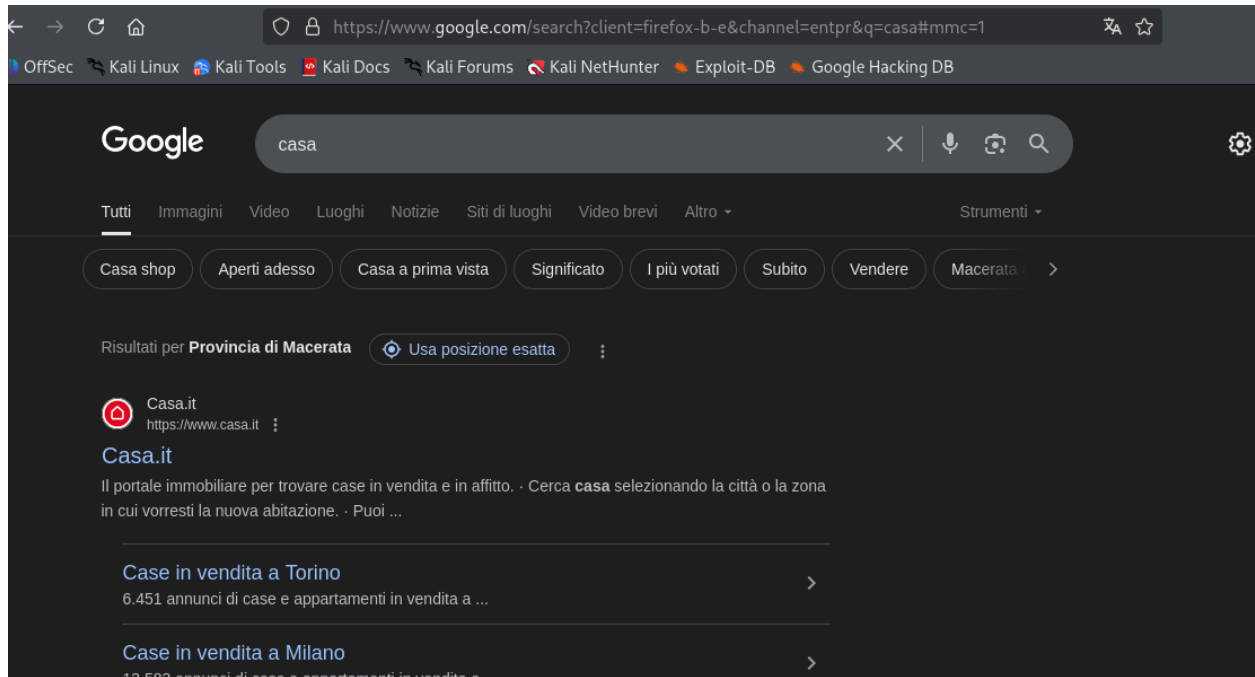
Ho posizionato questa regola **in cima** alla lista delle regole dell'interfaccia LAN per assicurarmi che avesse la priorità più alta e venisse applicata prima di eventuali regole di permesso generale.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/218 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.50.100	*	192.168.70.100	80 (HTTP)	*	none		Blocco Accesso da Kali a DVWA	
<input type="checkbox"/>	✓ 2/1.69 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

## Test di Verifica

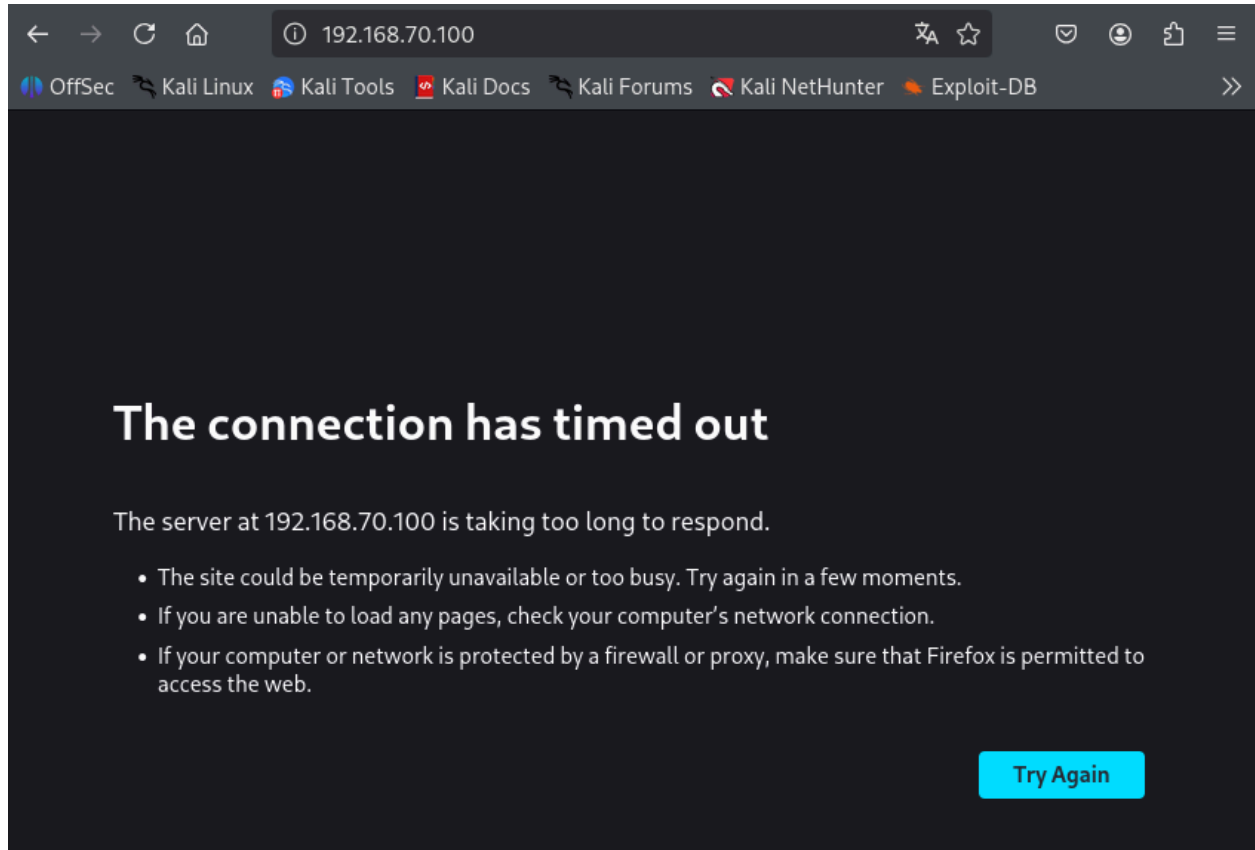
Per verificare che la regola non compromettesse la connettività generale, ho testato la navigazione verso Google e altri siti HTTPS



**Risultato: Funzionamento corretto**

## Test di Blocco Specifico

Tentativo di accesso a DVWA:



Risultato: **Timeout della connessione**

Dunque, la regola **blocca correttamente** il traffico dato che "The connection has timed out" da conferma che Il blocco è efficace.

Successivamente proseguo con la scansione delle porte **prima** dell'attivazione delle regole:

```

(kali㉿kali)-[~]
$ nmap -n 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:32 EDT
Nmap scan report for 192.168.70.100
Host is up (0.0043s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

```

Eseguito scan completo con **nmap**

**Risultato:** Tutte le porte dei servizi risultavano aperte “open”



Dopo l'attivazione delle regole:

Ripeto lo stesso scan che vediamo in basso :

```
(kali㉿kali)-[~]
$ nmap -n 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:30 EDT
Nmap scan report for 192.168.70.100
Host is up (0.0093s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
80/tcp    filtered  http
111/tcp   open      rpcbind
512/tcp   open      exec
513/tcp   open      login
514/tcp   open      shell
1099/tcp  open      rmiregistry
1524/tcp  open      ingreslock
2121/tcp  open      ccproxy-ftp
3306/tcp  open      mysql
5432/tcp  open      postgresql
5900/tcp  open      vnc
6000/tcp  open      X11
6667/tcp  open      irc
8009/tcp  open      ajp13
8180/tcp  open      unknown

Nmap done: 1 IP address (1 host up) scanned in 2.96 seconds
```

**Risultato:** Porta 80 risulta **"filtered"**

**Conferma:** Il firewall sta **bloccando** correttamente!

## CONSIDERAZIONI FINALI

L'obiettivo dell'esercitazione è stato completamente raggiunto. La regola firewall implementata su pfSense **blocca efficacemente** il traffico HTTP dalla macchina Kali Linux verso il servizio DVWA su Metasploitable2, mantenendo inalterata la connettività per tutti gli altri servizi di rete.

La configurazione dimostra come sia possibile implementare controlli di sicurezza **senza compromettere** la funzionalità generale del sistema.

Questo esercizio mi ha fatto capire quanto sia importante la **pianificazione** nella configurazione di sistemi di sicurezza e viste le difficoltà incontrate che ogni **piccolo dettaglio** può fare la differenza tra una configurazione funzionante e una che non lo è.