

# Esercizio S3\_L5

## Obiettivo:

In questo esercizio è stato richiesto di configurare un ambiente virtuale con pfSense per separare due macchine (Kali Linux e Metasploitable2) su sottoreti differenti e bloccare l'accesso all'applicazione DVWA, installata su Metasploitable2, da parte della macchina Kali.

## Preparazione dell'ambiente

Come prima cosa, ho lavorato sulla configurazione di pfSense e Kali, che inizialmente si trovavano nella rete [192.168.50.0/24](#). Ho preferito cambiare gli ip per cimentarmi nel processo di configurazione come se partissi da un ambiente totalmente nuovo.

```
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: 09818f70e30de7a0a28d
** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
                -> v6/DHCP6: fd00::a00:27ff:fe12:de2e/64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24

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: 
```

## Reimpostazione IP di pfSense

Dalla console di pfSense ho selezionato l'opzione **2) Set interface(s) IP address** e ho assegnato un nuovo indirizzo IP alla LAN:

[192.168.1.1/24](#)

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 
```

```

The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:

    http://192.168.1.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 09818f70e30de7a0a28d

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

WAN (wan)          -> vtnet0          -> v4/DHCP4: 10.0.2.15/24
                                   v6/DHCP6: fd00::a00:27ff:fe12:de2e/64
LAN (lan)          -> vtnet1          -> v4: 192.168.1.1/24

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:

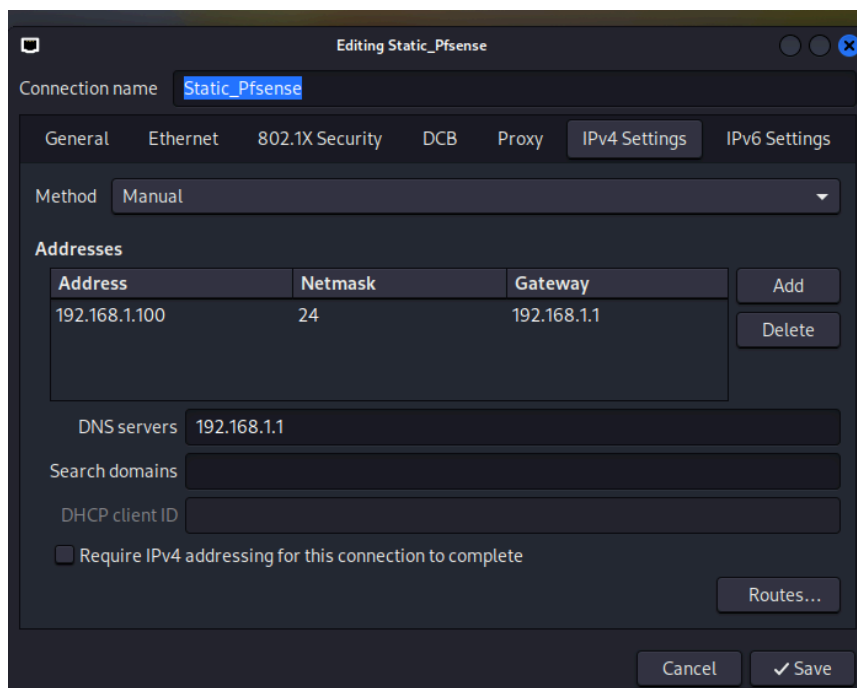
```

Non ho impostato gateway, né IPv6, e ho lasciato disabilitato il DHCP poiché preferivo assegnare IP statici.

## Configurazione IP statico su Kali Linux

Essendo Kali già collegata alla rete interna (VirtualBox [intnet](#)), ho aggiornato la configurazione della rete tramite l'interfaccia grafica impostando:

- IP: [192.168.1.100](#)
- Netmask: [255.255.255.0](#)
- Gateway: [192.168.1.1](#)
- DNS: [192.168.1.1](#)
- il metodo IPv4 su **manual**.



Dopo queste modifiche, Kali ha riconosciuto correttamente la rete, ed era possibile pingare pfSense ([192.168.1.1](#)) e accedere alla sua GUI via browser.

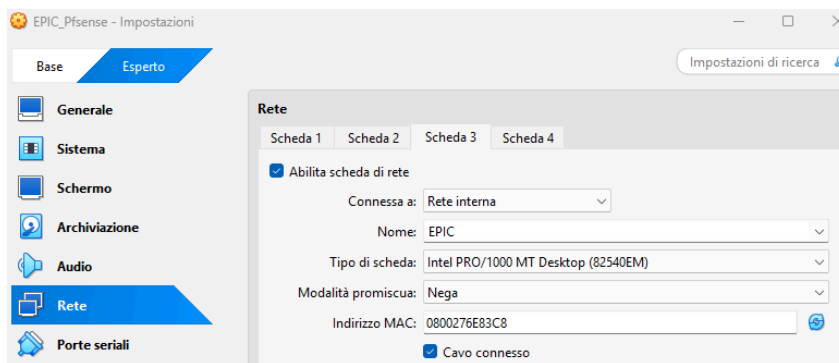
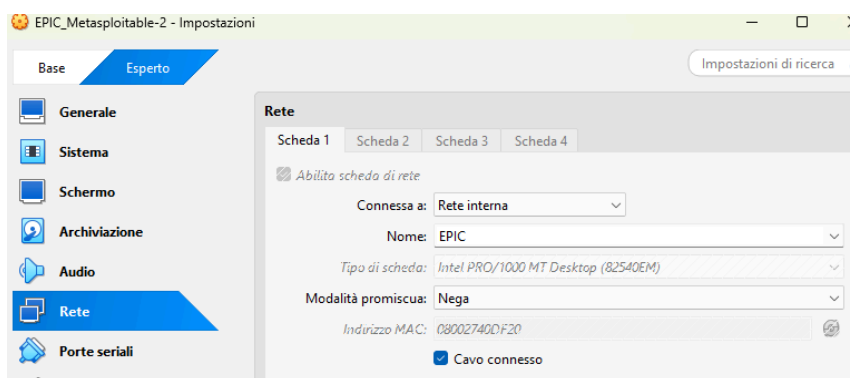
## Aggiunta e configurazione di Metasploitable2 in una rete separata

Per isolare Metasploitable2 da Kali, ho deciso di collocarla in una subnet diversa.

### Configurazione rete interna "EPIC"

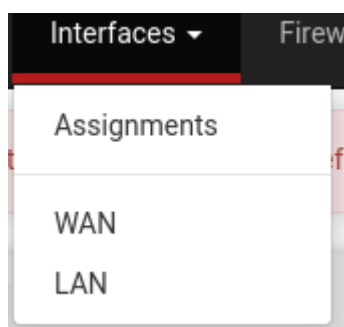
Ho creato una nuova rete interna in VirtualBox, chiamata EPIC, e l'ho assegnata:

- Alla Scheda 1 di Metasploitable2
- Alla Scheda 3 di pfSense




### Configurazione interfaccia OPT1 su pfSense


Avviato pfSense, ho assegnato la nuova interfaccia dalla GUI in Interfaces > Assignments.




La nuova interfaccia appare dunque disponibile ad essere aggiunta; ho premuto dunque su “add”.

Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:d4:41:3a)
Available network ports:	em0 (08:00:27:6e:83:c8)

 Save


 Add


 Delete


Ho dunque aperto la scheda di configurazione della nuova interfaccia, chiamata di default OPT1, l'ho rinominata in **METASPLOIT\_NET** e le ho assegnato il relativo ip di gateway: **192.168.2.1/24**.

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#) [LAGGs](#)

Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:d4:41:3a)
<b>OPT1</b>	em0 (08:00:27:6e:83:c8)

 Save

 Delete

 Delete

Interfaces / **OPT1 (em0)**

**General Configuration**

Enable ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx 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) or minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex**   
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**  /

**IPv4 Upstream 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 RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in a private address space, too.

**Block bogon networks** ☐  
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.  
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.  
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Una volta effettuato il salvataggio delle impostazioni, un avviso ci comunica che le modifiche all'interfaccia sono avvenute ma è necessario applicarle. Procediamo dunque a cliccare su "Apply changes".

The METASPLOIT\_NET configuration has been changed.  
The changes must be applied to take effect.  
Don't forget to adjust the DHCP Server range if needed after applying.

✓ Apply Changes

## Configurazione IP statico su Metasploitable2

Nel file `/etc/network/interfaces` ho impostato:

```
auto eth0
iface eth0 inet static
    address 192.168.2.100
    netmask 255.255.255.0
    gateway 192.168.2.1
```

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# 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 192.168.2.100
netmask 255.255.255.0
gateway 192.168.2.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
```

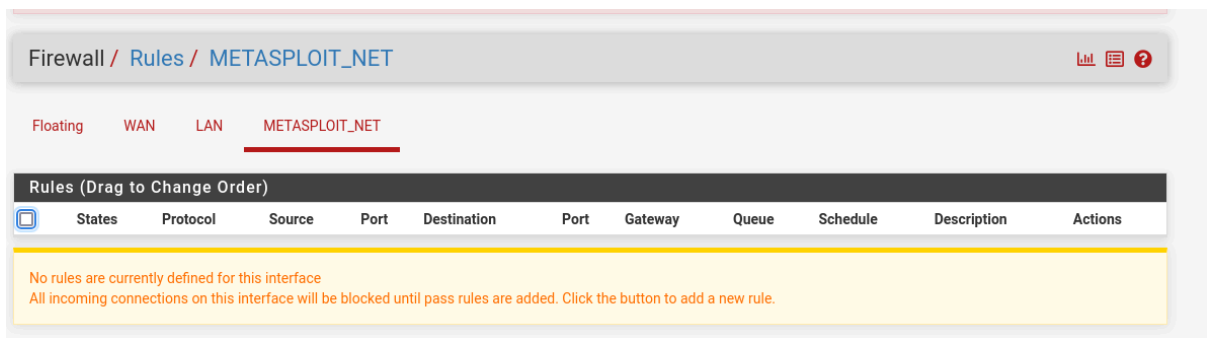
```
Last login: Fri Jul 18 03:28:07 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 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 08:00:27:40:df:20 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.100/24 brd 192.168.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe40:df20/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

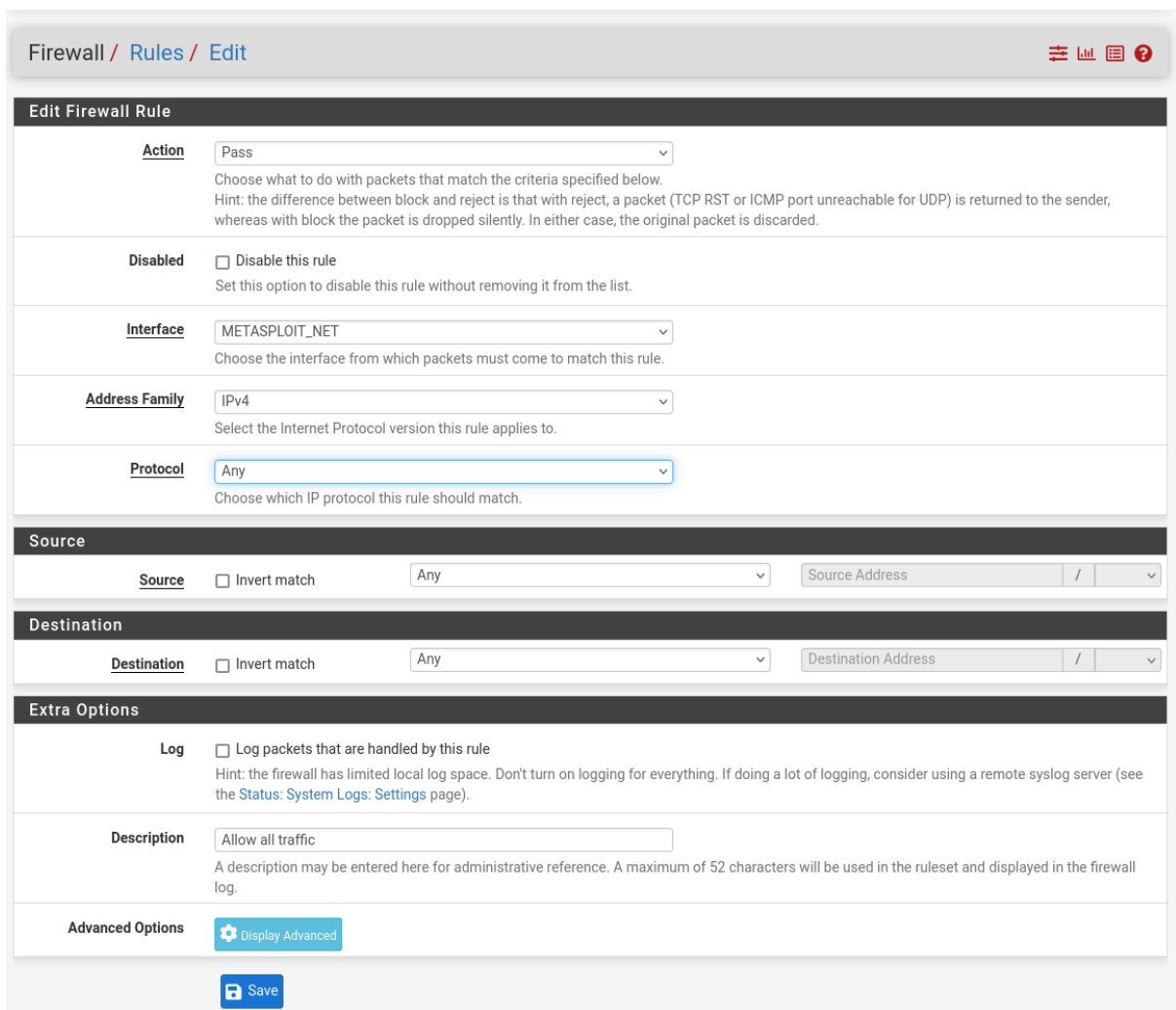
Dopo il riavvio della rete, Metasploitable riusciva a pingare pfSense. Tuttavia, non riusciva a pingare Kali inizialmente, poiché pfSense blocca di default il traffico in entrata su nuove interfacce.



## Sblocco Traffico da METASPLOITABLE\_NET

Per consentire la connettività, ho creato una regola temporanea “PASS” chiamata “Allow all traffic” sull’interfaccia [METASPLOIT\\_NET](#) in Firewall > Rules > METASPLOIT\_NET.

Tramite questa regola ho permesso a qualunque tipo di traffico proveniente dall’interfaccia METAPLOIT\_NET di transitare senza problemi.



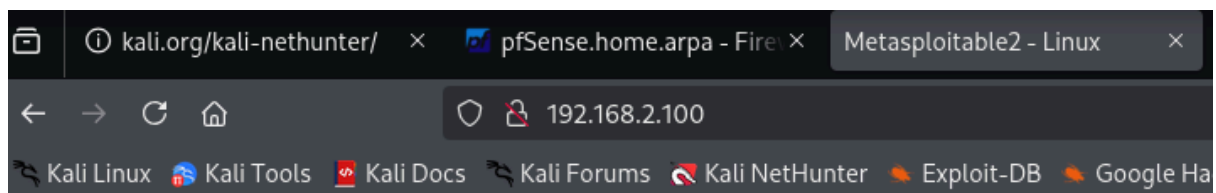
Dopo averla applicata Metasploitable riusciva a pingare Kali ([192.168.1.100](https://192.168.1.100)).

```
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.  
  
[21]+  Stopped                  ping 192.168.1.100  
msfadmin@metasploitable:~$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=0.571 ms  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=63 time=0.786 ms  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=63 time=0.660 ms  
64 bytes from 192.168.1.100: icmp_seq=4 ttl=63 time=0.566 ms  
  
[31]+  Stopped                  ping 192.168.1.100  
msfadmin@metasploitable:~$
```

---

## Verifica dell'accesso a DVWA da Kali

Per dimostrare che l'accesso a DVWA fosse inizialmente **funzionante**, ho inserito l'ip della metasploitable sulla barra di ricerca del browser.



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

La ricerca ha restituito la pagina DVWA, confermando che:

- Kali riusciva a raggiungere il web server su Metasploitable.
  - La porta 80 era aperta.
-

# Blocco dell'accesso a DVWA tramite pfSense

Per impedire a Kali di connettersi a DVWA, ho creato due regole firewall sulla LAN, in Firewall > Rules > LAN, entrambe con **Action: Block**.

## Regola 1 – Blocca HTTP:

- Source: 192.168.1.100
- Destination: 192.168.2.100
- Destination port: 80

Firewall / Rules / Edit

### Edit Firewall Rule

**Action:** Block

**Disabled:** ☐ Disable this rule

**Interface:** LAN

**Address Family:** IPv4

**Protocol:** TCP

**Source:** 192.168.1.100

**Destination:** 192.168.2.100

**Destination Port Range:** HTTP (80) to HTTP (80)

**Log:** ☐ Log packets that are handled by this rule

**Description:** HTTP BLOCK FROM KALI

**Advanced Options:** [Display Advanced](#)

## Regola 2 – Blocca HTTPS:

- Source: 192.168.1.100
- Destination: 192.168.2.100
- Destination port: 443



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 192.168.1.100 /

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 192.168.2.100 /

**Destination Port Range** HTTPS (443) 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).

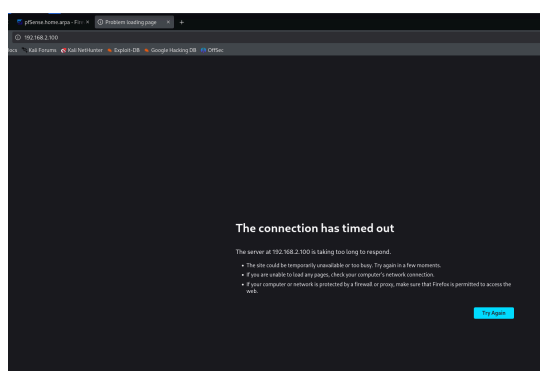
**Description** HTTPS BLOCK KALI  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Ho creato la regola 2 per impedire anche la connessione https qualora si fosse voluto abilitare tale protocollo nelle impostazioni della Metasploitable2.

Entrambe le regole sono state inserite sopra eventuali regole "Allow all" per essere sicuro che venissero applicate per prime.

## Verifica del blocco

Dopo l'applicazione delle regole la connessione a DVWA risultava, come ci si aspetterebbe, impossibile in quanto bloccata dal firewall.



```
(kali㉿kali)-[~]
$ nmap -p 80 192.168.2.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:43 EDT
Nmap scan report for 192.168.2.100
Host is up (0.00051s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

---

## Conclusione

Al termine di questo esercizio sono riuscito a:

- Ripristinare e configurare correttamente gli IP statici per pfSense, Kali e Metasploitable2.
- Creare due sottoreti isolate, collegate tramite pfSense.
- Dimostrare il funzionamento iniziale dell'accesso a DVWA.
- Implementare un blocco mirato, tramite firewall rules, per impedire che Kali possa interagire con DVWA.

Questo approccio ha permesso di simulare un contesto realistico di segmentazione di rete e controllo degli accessi, utile per esercitazioni di cybersecurity in ambienti virtuali controllati.

## Considerazioni aggiuntive:

*In questa configurazione, l'accesso alla DVWA è stato bloccato esclusivamente per la macchina con IP **192.168.1.100**, ovvero Kali Linux. È importante però sottolineare che qualsiasi altra macchina presente su una delle due reti (LAN o METASPLOIT\_NET) avrebbe comunque la possibilità di connettersi a DVWA senza alcuna restrizione.*

*Inoltre, la regola firewall così impostata è **facilmente aggirabile**: sarebbe sufficiente per l'attaccante modificare il proprio indirizzo IP (es. da 192.168.1.100 a 192.168.1.101) per bypassare completamente il blocco e accedere nuovamente all'applicazione. Questo rende il meccanismo efficace solo a scopo dimostrativo o in ambienti strettamente controllati.*

*Per una gestione **più sicura**, sarebbe preferibile adottare un approccio **deny-by-default**, ovvero:*

*Impostare una regola di blocco generica per tutto il traffico (es. dalla subnet **192.168.1.0/24**)*

*E successivamente **definire in modo esplicito le eccezioni**, autorizzando solo determinati dispositivi*

*Una possibile estensione potrebbe includere l'uso di **filtri basati su indirizzo MAC**, che, pur essendo meno sicuri di una segmentazione logica, rendono più difficile l'elusione semplice via **IP spoofing** o **cambio IP manuale**.*

*Infine, è buona pratica in scenari reali utilizzare anche strumenti come:*

- **VLAN** per separare fisicamente il traffico.
- **IPS/IDS** per rilevare, e bloccare nel caso IPS, comportamenti anomali.
- **Regole specifiche per intere sottoreti**, ad esempio bloccare la 192.168.1.0/24 e autorizzare solo indirizzi specifici sulla 192.168.2.0/24.