

## Progetto S3L5.

### Creazione policy Pfsense

*“Crea una regola firewall che blocchi l’accesso alla DVWA (su Metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.”*

### Configurazione delle reti:

- **Meta (Metasploitable)** ha IP: 192.168.70.100 con gateway 192.168.70.1.
- **Kali Linux (intnet)** ha IP: 192.168.50.100 con gateway 192.168.50.1.
- Come possiamo notare, le due macchine sono su reti separate.

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:57:52:fb 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:fe57:52fb/64 scope link
            valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~$
```

(Meta)

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    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 eth
        valid_lft forever preferred_lft forever
```

(Kali)

### Aggiunta di una nuova interfaccia su pfSense:

Successivamente, è stata configurata una terza rete per pfSense, che funge da gateway tra le due macchine.

Per farlo, è stato avviato pfSense, e tramite il browser di Kali Linux è stata aggiunta l'interfaccia OPT1Meta.

Dopo aver aggiunto questa interfaccia, è stato necessario configurare il gateway appropriato.

## 1. Aggiunta dell'interfaccia OPT1Meta a pfSense per gestire la rete Meta.

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** 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** OPT1META  
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 Address or Alias 192.168.70.100 /

**Destination**

**Destination** ☐ Invert match Any Destination Address /

## 2. Configurazione del gateway per l'interfaccia Meta.

### Static IPv4 Configuration

**IPv4 Address** 192.168.70.1 / 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](#).

### Impostazione delle Regole su pfSense:

Dopo aver configurato la rete Meta su pfSense, abbiamo creato un set di regole firewall attraverso la tab "Rules" di pfSense.

Le regole sono state configurate come segue:

- **Azione: Bloccare (Block)** – La regola blocca i pacchetti che corrispondono ai criteri definiti.
- **Interfaccia: LAN** – La regola si applica ai pacchetti in arrivo sulla rete locale (LAN).
- **Indirizzo di Origine (Source):** L'indirizzo IP **192.168.50.100** (Kali) è stato selezionato come sorgente da bloccare.

- **Indirizzo di Destinazione (Destination):** L'indirizzo IP **192.168.70.100** (Metasploitable2) è stato selezionato come destinazione da bloccare.
- **Protocollo: TCP** – La regola è applicata ai pacchetti TCP.
- **Porta di Destinazione: HTTP (porta 80)** – La regola impedisce il traffico verso il servizio HTTP sulla macchina Metasploitable.

Questa configurazione blocca l'accesso della macchina Kali al servizio HTTP sulla macchina Metasploitable, impedendo così eventuali scansioni.

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 /

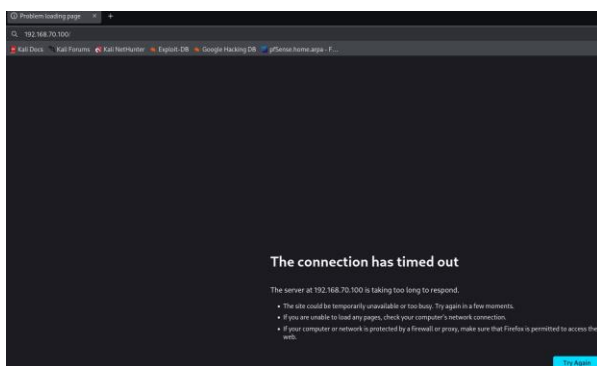
**Destination**

**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.

Fatto questo il nostro obiettivo è stato raggiunto, non ci resta che testarne l'efficienza.

***N.B. Qualsiasi tipo di modifica viene apportata su PfSense va salvata, altrimenti l'impostazione andrà persa una volta lasciata la pagina.***



Una volta configurato il firewall con le regole appropriate, l'obiettivo è stato raggiunto, e l'accesso a DVWA su Metasploitable è stato correttamente bloccato da Kali.

Ora, per testare l'efficacia della regola, sarà necessario eseguire una scansione con **Nmap** sul terminale di Kali per verificare se il traffico viene effettivamente bloccato.

```
(kali@kali)-[~]
$ nmap -p 80 192.168.70.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:59 EDT
Nmap scan report for 192.168.70.100
Host is up (0.00032s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Nmap indica che la porta **80/tcp**, utilizzata dal servizio HTTP su Metasploitable, è "**filtered**". Questo significa che il traffico diretto alla porta HTTP è stato bloccato, senza che Nmap ricevesse una risposta chiara. Questo è coerente con l'obiettivo della regola firewall che abbiamo creato precedentemente.

Quindi, la regola firewall che abbiamo creato sta funzionando correttamente, bloccando l'accesso alla DVWA su Metasploitable da Kali Linux, come richiesto dall'esercizio.

Conclusioni personali:

Oggi l'esercizio ha messo alla prova le conoscenze che ho acquisito finora, e inizialmente non nego di essermi sentito sopraffatto. Tuttavia, ho cercato di mantenere la calma, affrontando ogni fase con logica e pazienza, questo mi ha permesso di visualizzare i passaggi necessari per arrivare alla soluzione. So che il mio report possa essere migliorato, ma ho preferito focalizzarmi prima sulla risoluzione della traccia, per poi dedicarmi con alla documentazione finale. Sono consapevole che questa scelta influirà sul livello del mio documento, ma credo che l'approccio che ho adottato mi abbia permesso di arrivare alla soluzione.