Gabriele Di giampietro **Data 21/11/2022**

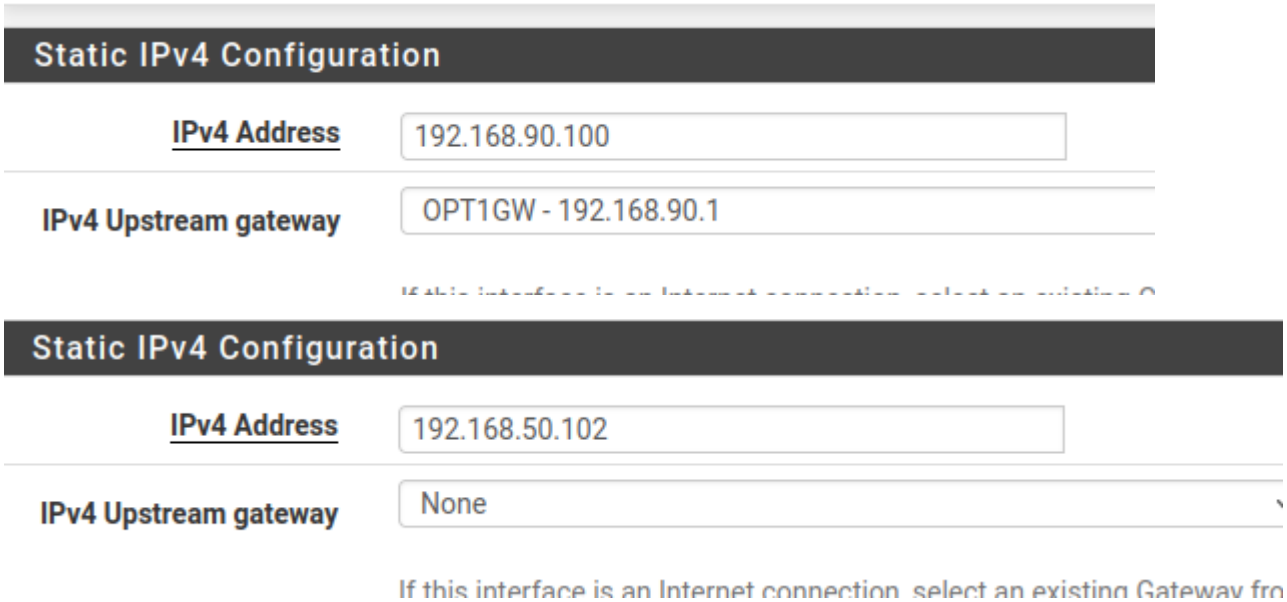
Obbiettivo: Configurare il firewall psfsense in VM, per la comunicazione di due VM su reti diverse (Kali 192.168.50.100 – Metasploitable 192.168.90.100)

Nell'esercitazione di oggi siamo andati a settare come firewall pfsense, per prima cosa abbiamo impostato le reti sia su metasploitable sia su kali con reti differenti e su quest'ultimo il gateway su 192.168.50.102 dove pfsense fungerà da router come vediamo nelle immagini seguenti:

```
# and how to activate them. For m

source /etc/network/interfaces.d/

# The loopback network interface
auto lo
iface lo inet loopback


auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.102
```

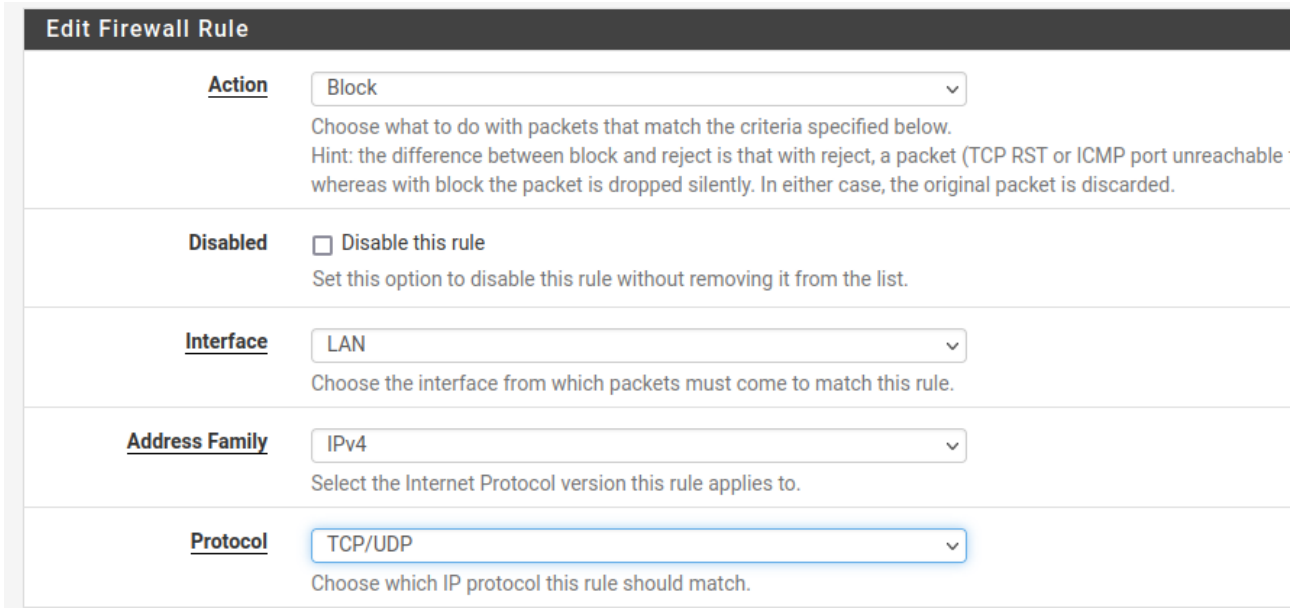
```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.90.100
netmask 255.255.255.0
network 192.168.90.0
broadcast 192.168.90.255
gateway 192.168.90.1
```

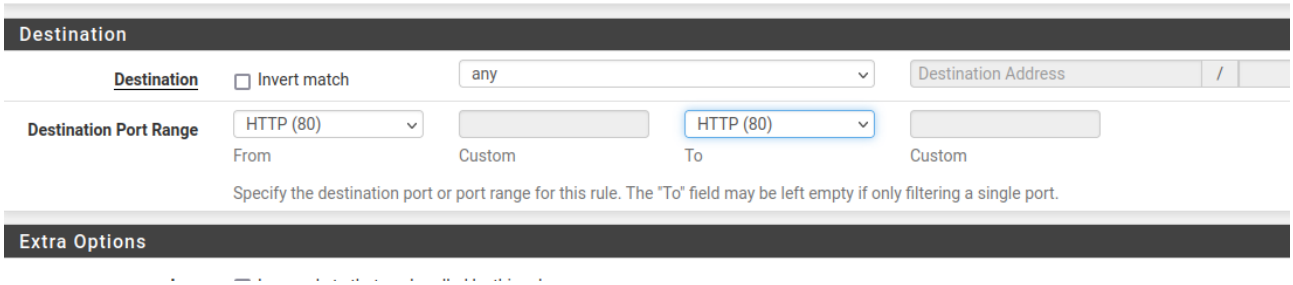
Dopo di che da browser siamo entrati nel settagio di pfsense, da li abbiamo inserito una seconda lan per collegare metasploitable (LAN2) e settato l'altra LAN con i relativi indirizzi ip.



Dopodiche abbiamo impostato le nostre rules per la funzione firewall, per impedire l'ingresso sulla nostra DVWA di metasploitable e quindi impostiamo l'action in block e indichiamo la porta 80 con

servizi http.





Infine effettuiamo una scansione nmap prima con il nostro firewall disattivato e poi attivo, possiamo notare come nella prima scansione ci trova le relative porte aperte. Con il nostro firewall attivo invece troviamo la dicitura filtred sulla porta 80 che ci indica l'impedimento nel raggiungerla e anche da browser la pagina non viene caricata.

```
└─$ sudo nmap -sS 192.168.90.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 10:47 EST
Nmap scan report for 192.168.90.100
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p80 192.168.90.100
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 12:11 EST
Nmap scan report for 192.168.90.100
Host is up (0.0024s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```