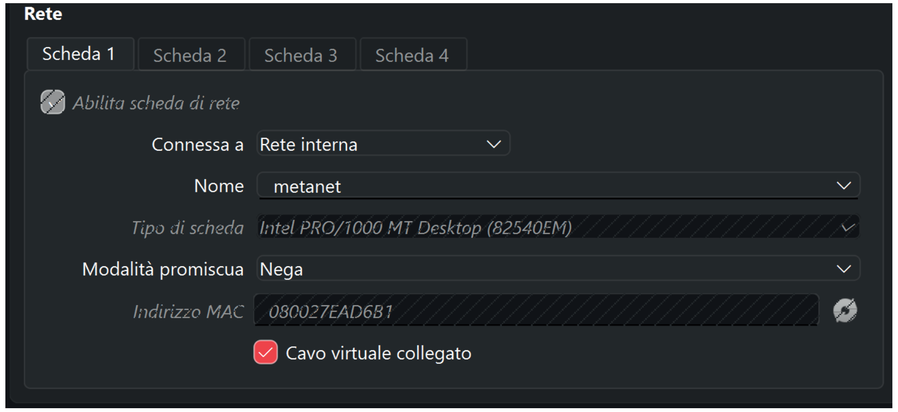
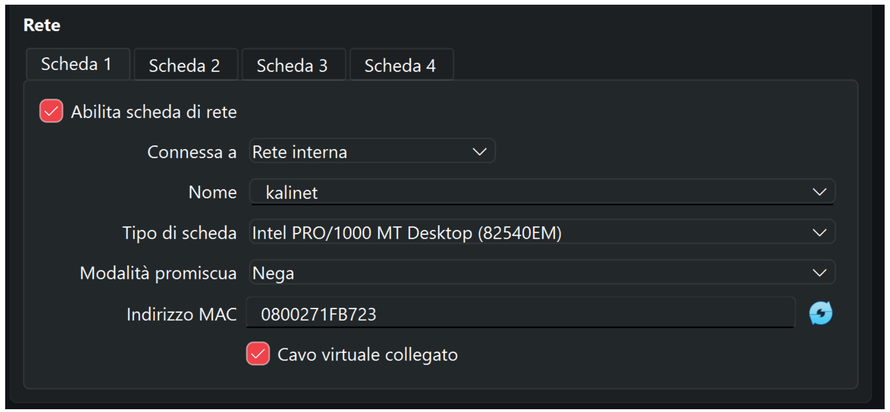
Richiesta

Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Preparazione ambiente: Metanet & Kalinet

Inanzitutto serve creare 2 reti separate per le 2 macchine come da richiesta. Quindi dalle impostazioni di rete delle macchine virtuali imposto "rete interna", simulando così 2 switch virtuali chiamati rispettivamente Metanet e Kalinet.

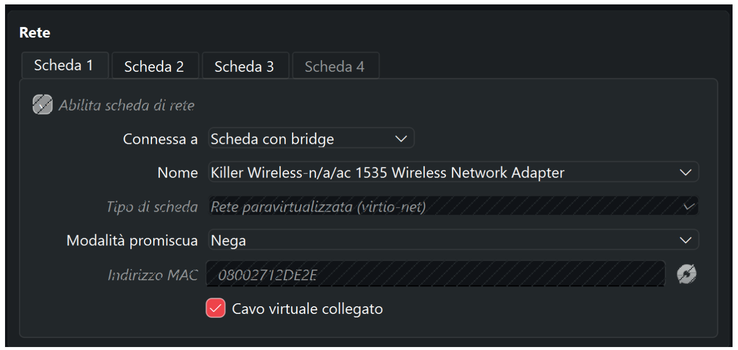


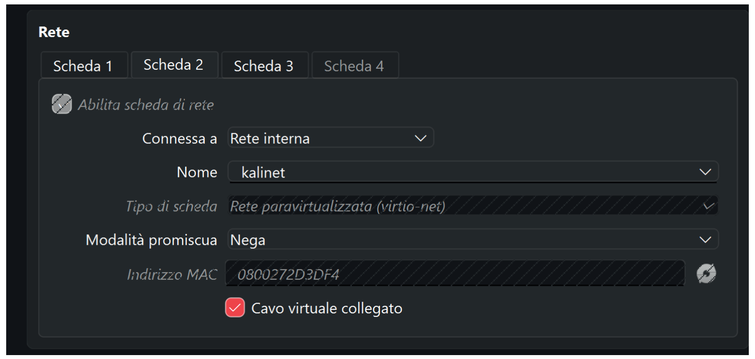


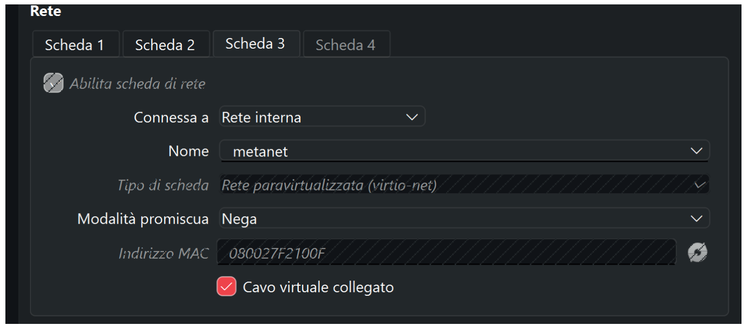
Ora le 2 macchine sono collegate "virtualmente" al loro rispettivo swicth e a nient'altro, quindi non hanno alcuna connessione ad internet e non c'è comunicazione nemmeno tra di loro.

Configurazione Pfsense

A questo punto configuro l'ambiente Pfsense dalle impostazioni della macchina.
Fungendo anche da router posso impostare le interfacce di rete necessarie alla comunicazione delle macchine.
La scheda 1 la tengo in bridge, ed è la scheda connessa al router di casa e di conseguenza ad internet.
La scheda 2 è collegata alla rete interna (LAN) kalinet, è quindi collegata virtualmente allo switch a cui è collegata la Kali.
Stesso discorso per la scheda 3 che è connessa a Metanet (metaspoatable).







Lo step successivo è avviare la macchina Pfsense e, se tutto è configurato correttamente, visualizzare le 3 interfacce di rete direttamente nel terminale. Qui assegno gli indirizzi IP alle mie 2 LAN:
- Kalinet 192.168.10.0
- Metanet 192.168.20.0

Impostando il DHCP vengono assegnati automaticamente degli IP alle macchine connesse alle rispettive reti.v

Test

Se l'ambiente è stato configurato correttamente, chiudendo e riaprendo la Pfsense si vedono le 3 reti (WAN, LAN1, LAN2) e i loro rispettivi indirizzi IP configurati.

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.1.171/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.10.1/24
 OPT1 (opt1)     -> vtnet2     -> v4: 192.168.20.1/24
```

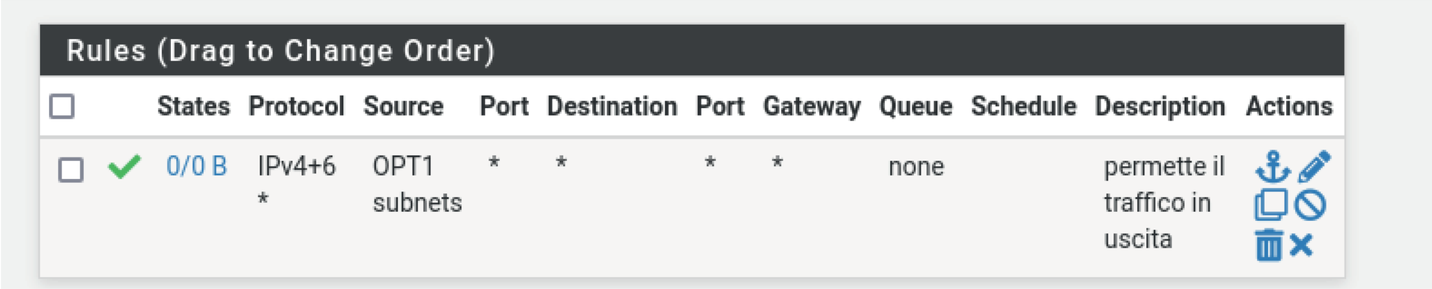
Procedo a fare dei test per confermare le connessioni. Dalla kali riesco a fare i ping su ogni macchina, mentre dalla meta-spoatable ancora no, perchè non ci sono regole nel firewall che permettono comunicazioni di nessun tipo.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=1.54 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=1.01 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=0.916 ms
^X64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=1.36 ms
^C
── 192.168.20.10 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.916/1.208/1.544/0.254 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.587 ms
^C
── 192.168.10.1 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.483/0.535/0.587/0.052 ms
```

Configurazione regole

A questo punto entro nel pannello di gestione di Pfsense dal browser della Kali all'IP 192.168.10.1 (gateway della Kalinet). *Firewall -> Rules* ed inserisco la regola nella rete della META che permette alla meta di comunicare traffico in uscita.




```
--- 192.168.20.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms
```

Prima della regola

```
--- 192.168.20.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.480/1.867/4.143/1.622 ms
msfadmin@metasploitable:~$ _
```

Dopo la regola

Configurazione regole

Procedo con l'obiettivo del progetto, inserisco una regola nella LAN (kalinet) che blocchi l'accesso alla DVWA da Kali.

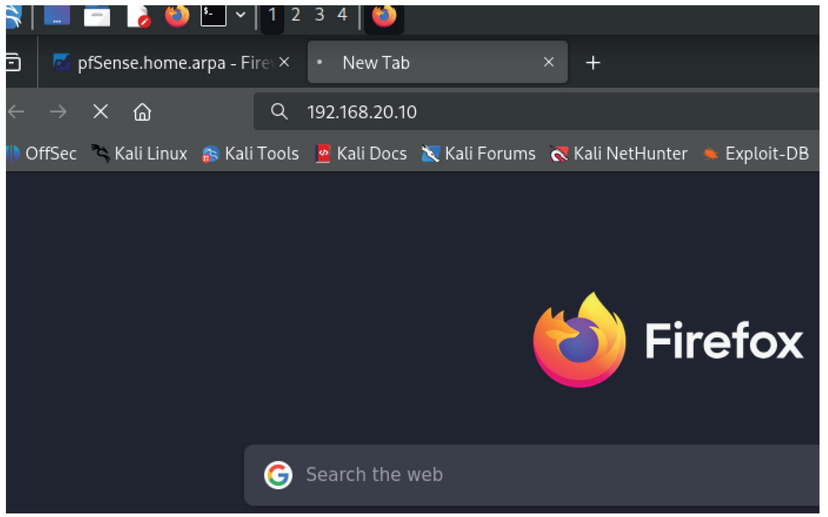
Floating | WAN | LAN | OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	3/1.44 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
	0/5 KiB	IPv4 TCP	192.168.10.100	*	192.168.20.10	80 (HTTP)	*	none		blocca accesso dvwa da kali	
	4/107 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Prima

Dopo



Conclusione

Nella regola ho specificato protocollo TCP e gli indirizzi IP destinatario e sorgente in questo modo non ho bloccato l'intero traffico della rete ma solo verso quella specifica pagina.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=0.467 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=0.831 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=0.542 ms
^X64 bytes from 192.168.20.1: icmp_seq=4 ttl=64 time=0.520 ms
64 bytes from 192.168.20.1: icmp_seq=5 ttl=64 time=0.475 ms
^C
── 192.168.20.1 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4282ms
rtt min/avg/max/mdev = 0.467/0.567/0.831/0.134 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=9.30 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=1.04 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=1.01 ms
^X64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=1.30 ms
^C
── 192.168.20.10 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.011/3.162/9.302/3.546 ms
```

La kali continua a inviare con successo ping verso la Metanet