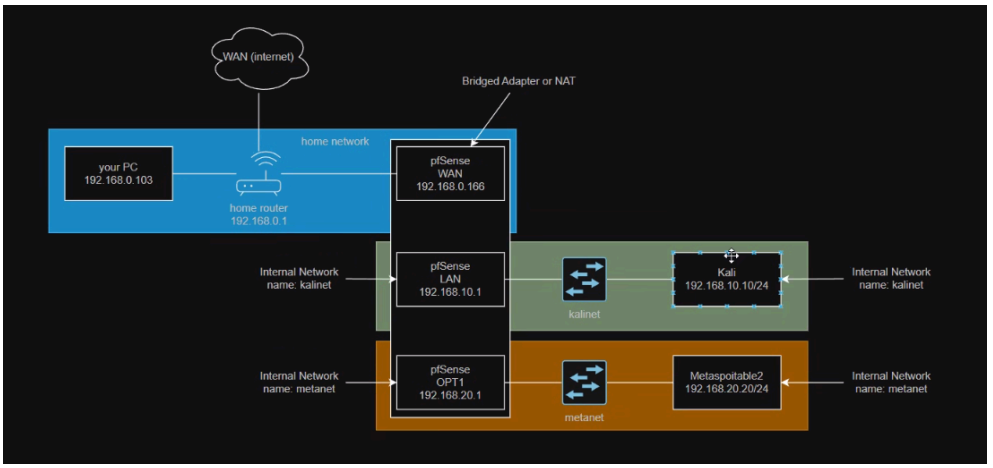
Informazioni Generali

L’esercizio consiste nella creazione pratica di una regola Firewall.
Per svolgere l’esercizio sono state utilizzate tre macchine virtuali (**KaliLinux**, **Metasploitable 2** e **pfSense**) gestite tramite Oracle VirtualBox. Queste macchine virtuali costituiscono i **dispositivi (host)** all'interno delle diverse reti necessarie a simulare l'architettura di rete.



Obiettivo dell’esercizio

L'obiettivo dell'esercizio è **bloccare il traffico HTTP (TCP 80)** originato dalla rete **kalinet** (dove risiede Kali Linux) e diretto all'applicazione web **DVWA** (su Metasploitable 2).

L'architettura di rete è gestita da pfSense, che instrada e filtra tra le seguenti interfacce:

- **LAN:** Corrisponde alla rete **kalinet**.
- **OPT1:** Corrisponde alla rete **metanet** (target).
- **WAN:** Rappresenta la connettività esterna.

Queste reti comunicheranno tra loro grazie alla MV **pfSense**, che funge da firewall e router.

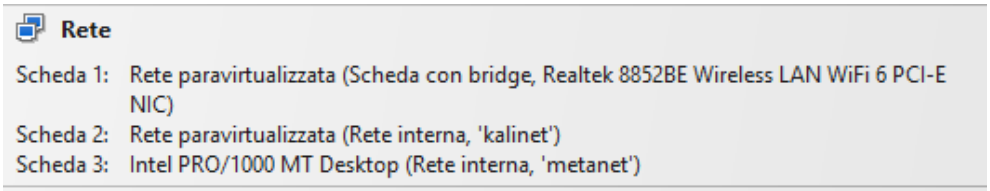
Il traffico può essere bloccato sull'interfaccia di origine (**LAN**) o su quella di destinazione (**OPT1**).

Ai fini di questo esercizio, si è scelto di applicare la regola di blocco all'interfaccia **LAN**.

Bloccare il traffico **in uscita** dalla LAN impedisce immediatamente l'inoltro dei pacchetti indesiderati all'interno di pfSense, ottimizzando l'uso delle risorse prima che il traffico tenti di raggiungere l'interfaccia **OPT1**.

Impostazioni di Rete

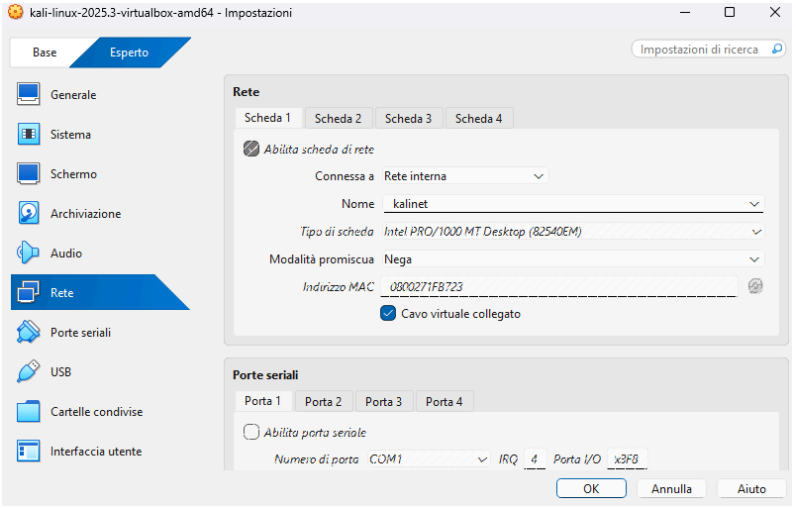
Impostazione pfSense



Sulla macchina pfSense sono montate 3 schede di rete:

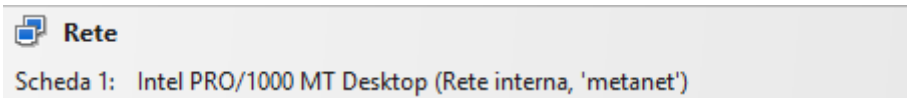
- La prima connessa in Bridge (**WAN**);
- La seconda connessa a Rete Interna (**LAN**, kalinet);
- La terza connessa a Rete Interna (**OPT1**, metanet).

Impostazioni Kali Linux



La kali è connessa ad una rete interna (**kalinet**) che sarà la nostra rete “**LAN**” con IP **192.168.10.10/24**

Impostazioni Metasploitable2



La Metasploitable2 è connessa ad una rete interna (**metanet**) che sarà la nostra rete “**OPT1**” con IP **192.168.20.20/24.**
L’**OPT1** viene configurato all’interno del Browser della Kali collegato all’interfaccia di pfSense.
Su Interfaces > Assignments è possibile aggiungere una nuova interfaccia, ovvero l’**OPT1.**

Fase 1: Verifica della connettività

Il primo passo fondamentale, prima di toccare qualsiasi regola del Firewall, è verificare che le nostre macchine siano effettivamente connesse alle reti stabilite e che il traffico possa fluire liberamente tra di esse. Dobbiamo assicurarci che la Kali possa raggiungere l'applicazione web DVWA sulla Metasploitable 2.

Controllo della Connettività di Rete

Per prima cosa, eseguiamo un test base per confermare che il routing attraverso pfSense stia funzionando. Dalla macchina Kali, apriamo il terminale e inviamo un semplice `ping` all'indirizzo IP della Metasploitable 2:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=0.508 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=0.412 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=0.429 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=0.389 ms
^C
── 192.168.20.20 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.389/0.434/0.508/0.044 ms
```

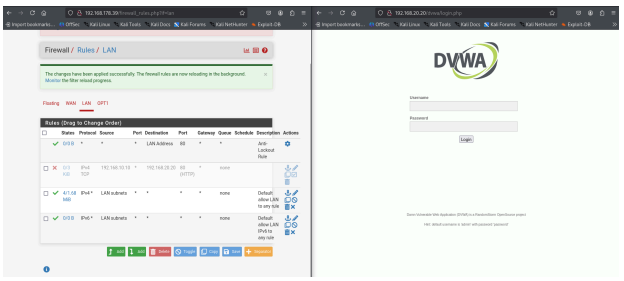
Una volta ricevute le risposte, sappiamo che la connettività a livello di rete (protocollo **ICMP**) è attiva, e **pfSense** sta correttamente instradando il traffico tra la nostra **kalinet** e la **metanet**.

Controllo Servizio Web (DVWA)

Verificata la connettività di rete, procediamo con il test del servizio web **(protocollo HTTP sulla porta 80/TCP)**.

Dal browser della Kali, inserisco l'indirizzo IP della Metasploitable (http://192.168.20.20/dvwa).

La visualizzazione della pagina di login di **DVWA** conferma che il traffico **HTTP** (che sarà l'oggetto della nostra regola di blocco) fluisce liberamente attraverso il firewall.



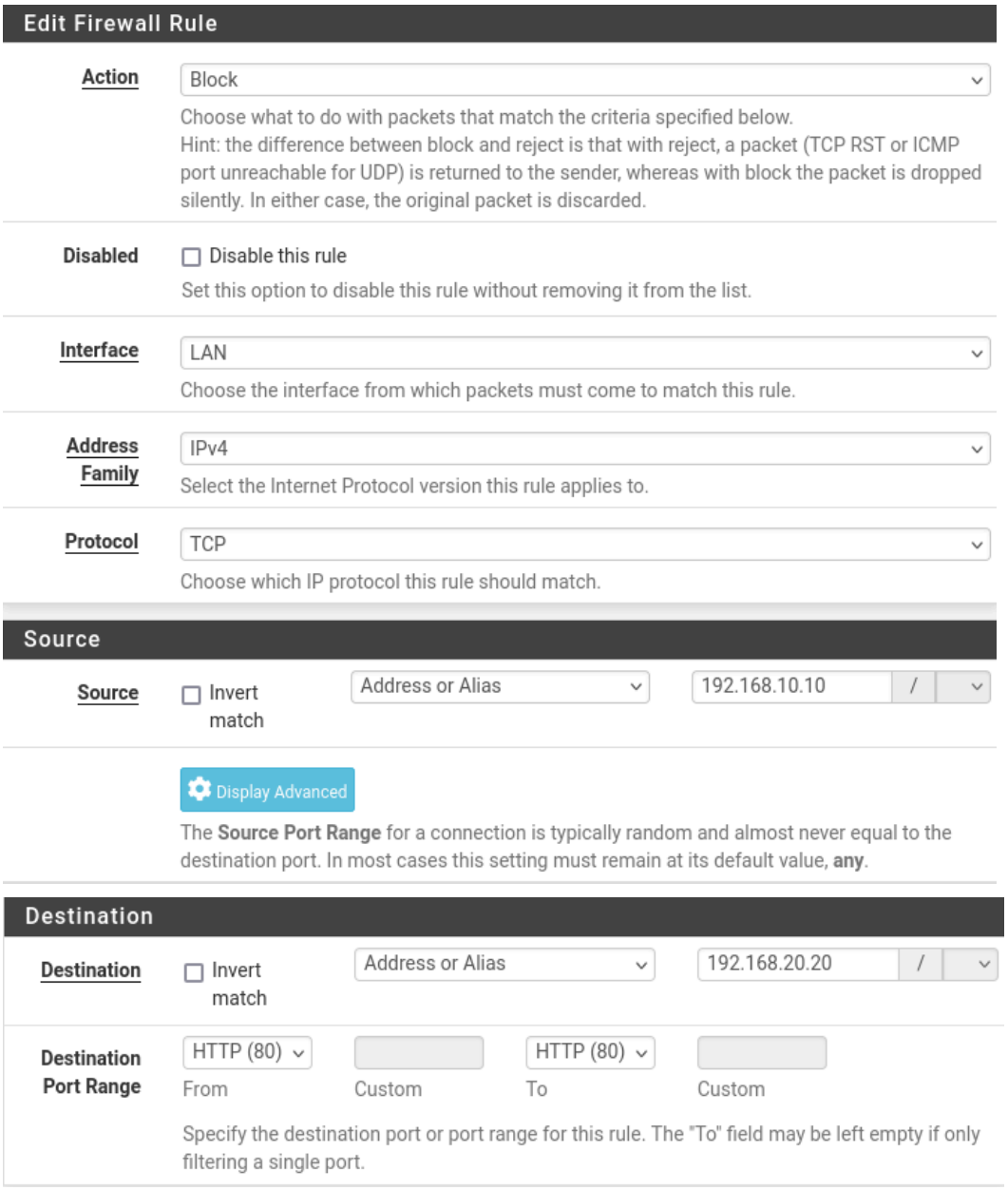
Fase 2: Creazione della regola Firewall su pfSense

Dopo aver verificato la connettività di base, l'obiettivo è implementare la regola che blocchi specificamente il traffico della Kali verso l'applicazione web DVWA. Ai fini dell'esercizio, si agirà a livello della rete sorgente, cioè **kalinet**.

Quando una macchina sulla **kalinet** (la Kali Linux) tenta di raggiungere un indirizzo sulla **metanet** (la Metasploitable), il traffico **esce** dalla scheda **LAN (kalinet)** del nostro pfSense. Applicando la regola di blocco su questa interfaccia, il traffico viene intercettato il prima possibile, così che non venga instradato verso la Metasploitable.

Dall'interfaccia web di pfSense, spostarsi in **Firewall > Rules**. Qui, selezionare la scheda relativa all'interfaccia **LAN (kalinet)** per creare la nuova regola.

La regola è stata creata con i seguenti parametri:

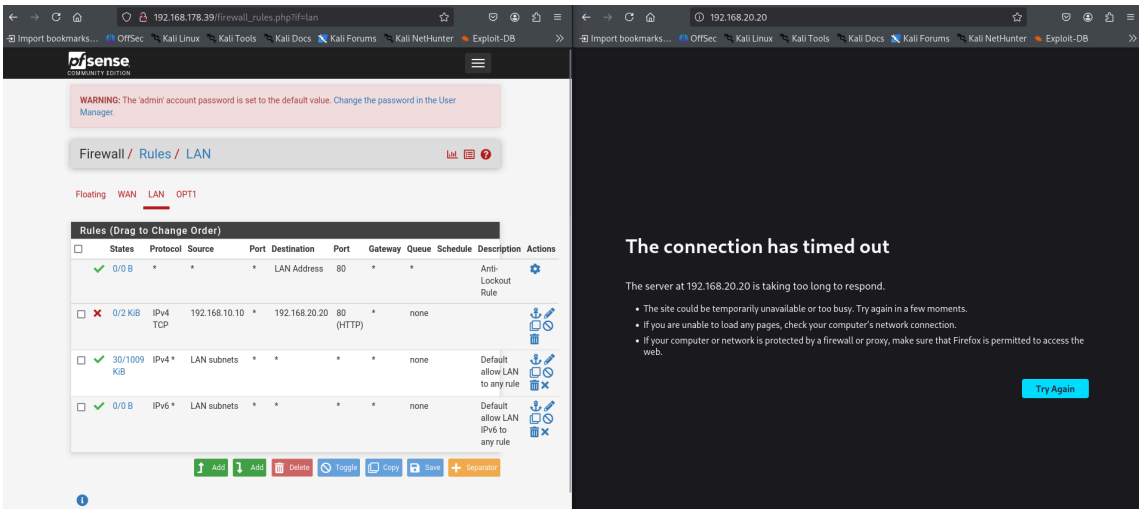


La regola blocca il traffico **TCP sulla porta 80 (HTTP)** in uscita dalla rete **kalinet** e destinato all'indirizzo IP della Metasploitable 2 (**192.168.20.20**).

Fase 3: Verifica del funzionamento della regola

Dopo aver implementato e applicato la regola di **Block** sull'interfaccia **LAN (kalinet)** del Firewall pfSense, si procede immediatamente alla verifica dell'efficacia.

Viene innanzitutto rieseguito il test di accesso all'applicazione web. Dalla macchina Kali, si tenta nuovamente di raggiungere l'indirizzo della Metasploitable 2 tramite il browser. Il browser, anziché visualizzare DVWA, deve restituire un errore di connessione o un **"Connection timed out"**. Questo risultato conferma che la regola di **Block** sta intercettando e negando il traffico applicativo in uscita dalla rete **kalinet**.



Per dimostrare la precisione del blocco, è essenziale verificare che altre comunicazioni di rete non siano state interrotte. Per questo, si ripete il comando **ping** dalla macchina Kali verso la Metasploitable 2. Poiché la regola è stata configurata per bloccare esclusivamente il traffico **TCP sulla porta 80** e non il protocollo ICMP utilizzato dal ping, i pacchetti **devono continuare a raggiungere la destinazione**, fornendo risposte regolari.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=0.744 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=0.408 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=0.434 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=0.463 ms
^C
── 192.168.20.20 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.408/0.512/0.744/0.135 ms
```

Il blocco selettivo del traffico HTTP/TCP e il mantenimento della connettività ICMP conferma la corretta implementazione e la granularità della regola Firewall.