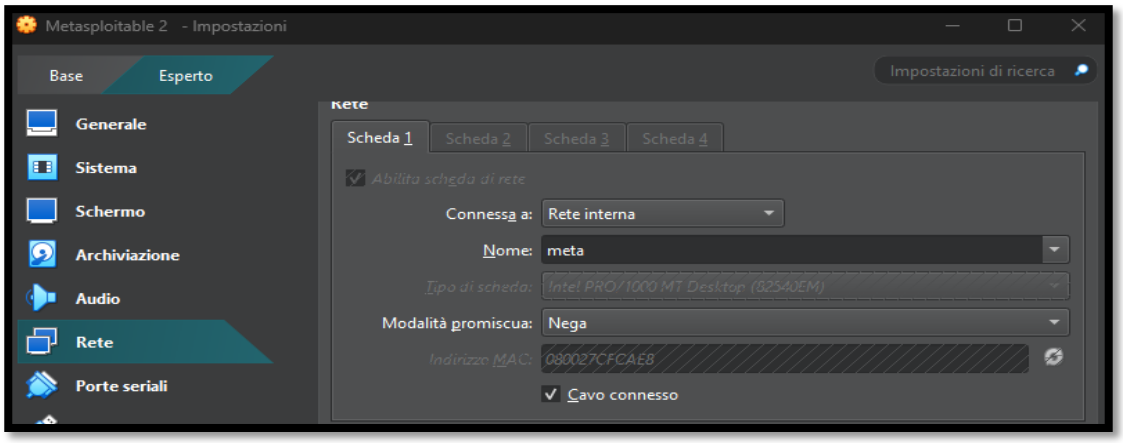
Creazione policy Pfsense

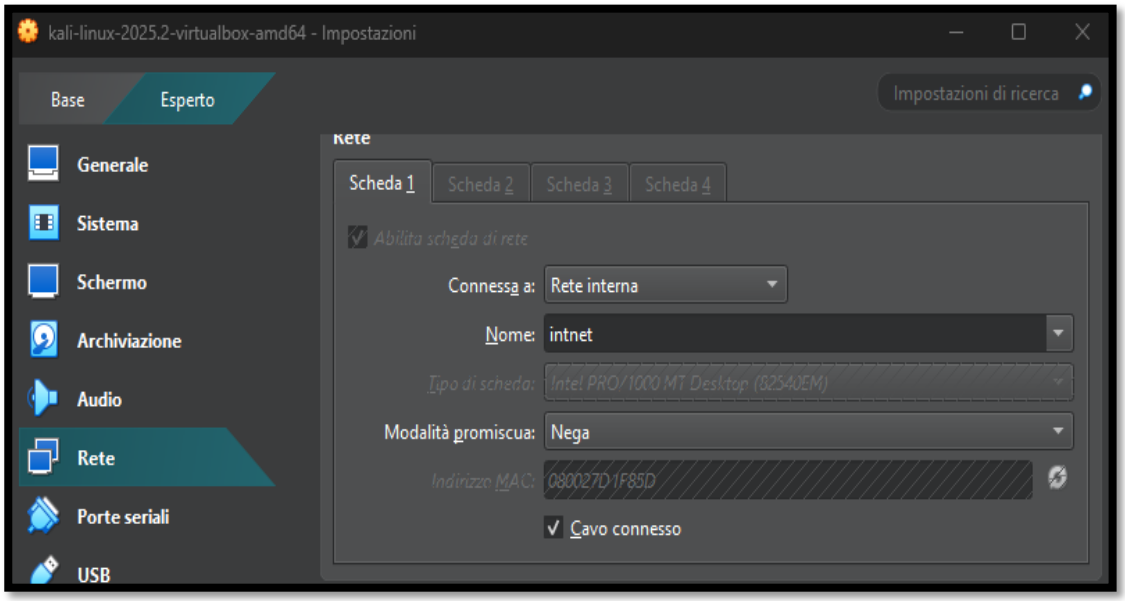
L’esercizio di oggi prevedeva l’uso del nostro laboratorio virtuale, con particolare attenzione al firewall Pfsense, la macchina con Kali Linux e la Metasploitable2.

Come prima cosa ho configurato le schede di rete delle varie macchine virtuali.

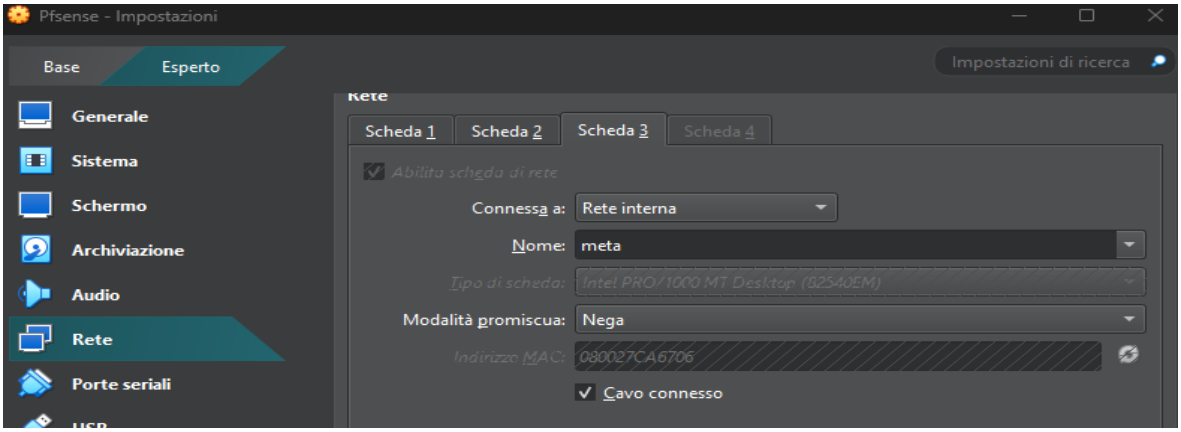
- Metasploitable2



- Kali



- Firewall Pfsense:

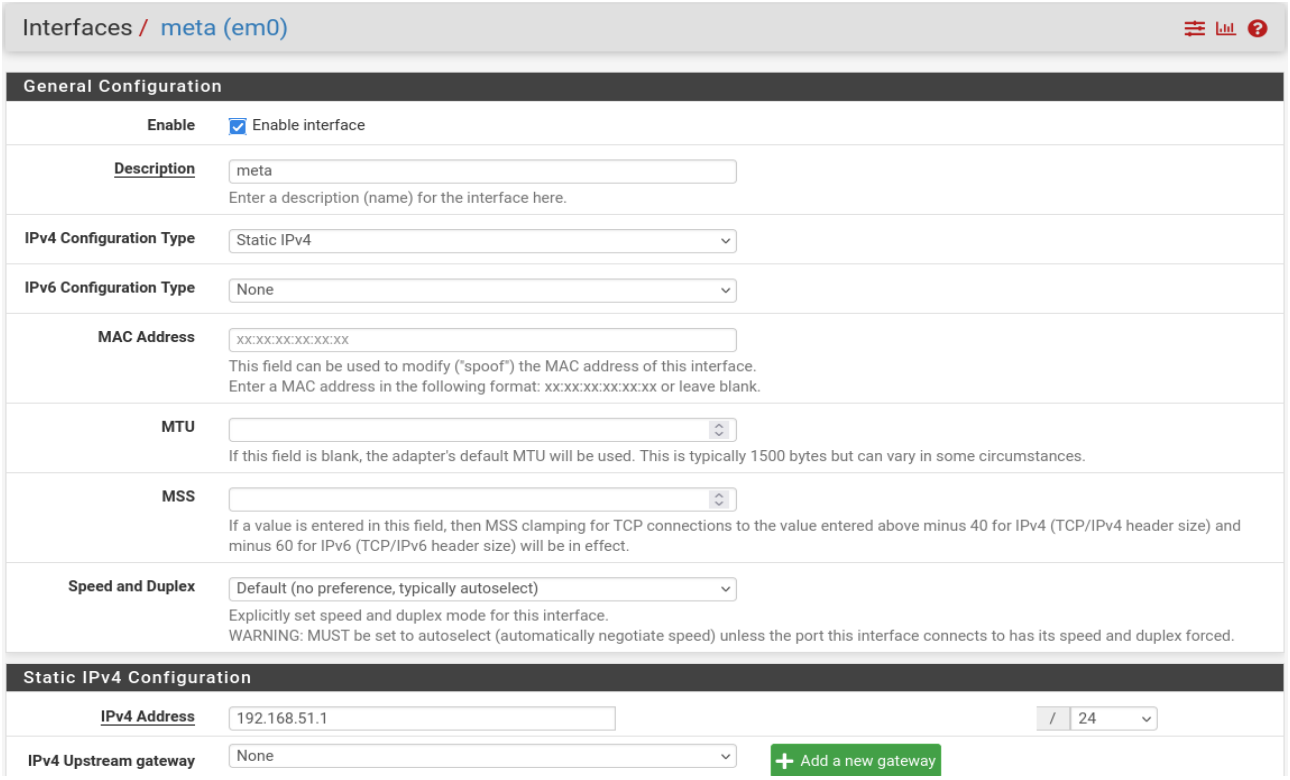


La traccia richiedeva anche che la Kali e la Metasploitable fossero in due reti diverse; perciò, ho settato la Kali con indirizzo IP **192.168.50.100** e la Metasploitable con indirizzo IP **192.168.51.100.**

Obiettivo

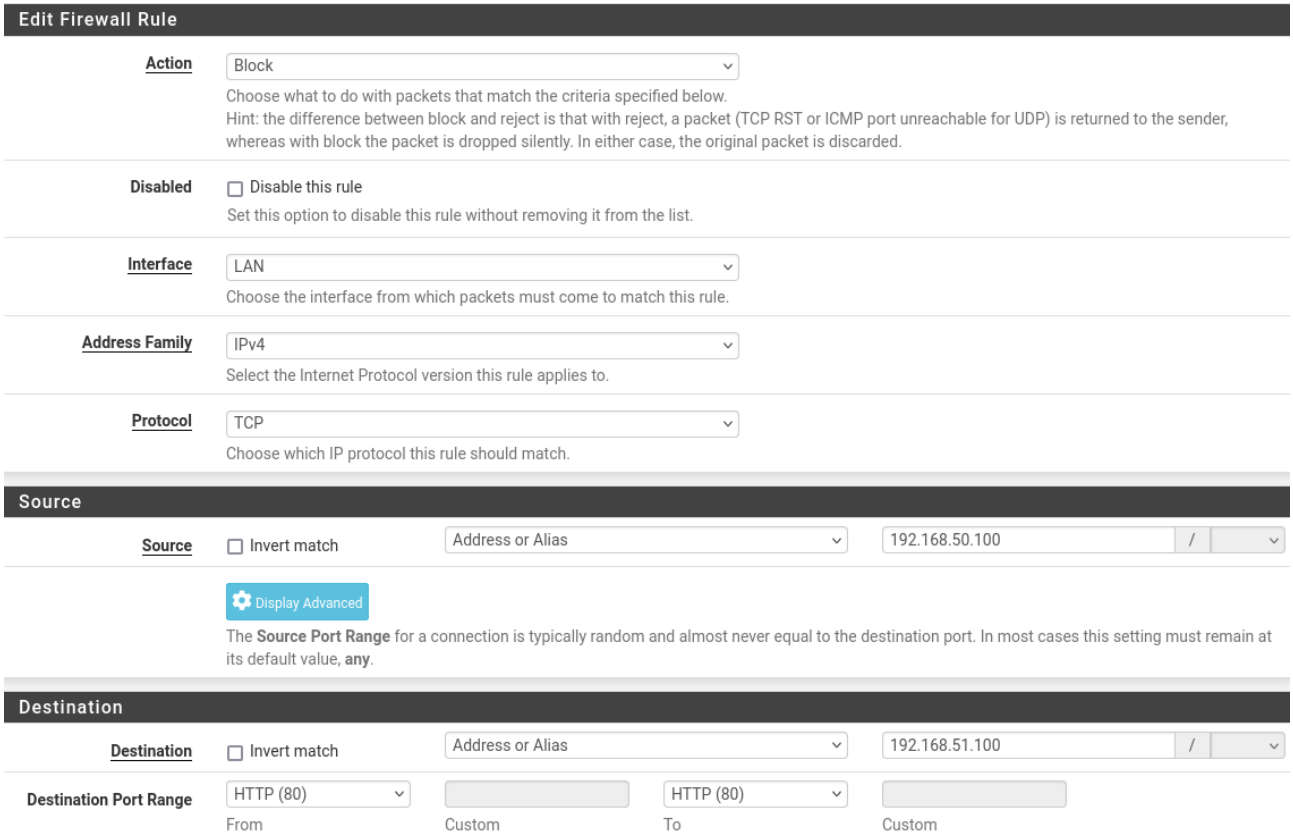
Creare una regola firewall che blocchi l'accesso alla DVWA su Metasploitable dalla macchina Kali Linux

1. Come primo step ho aggiunto la nuova interfaccia Meta



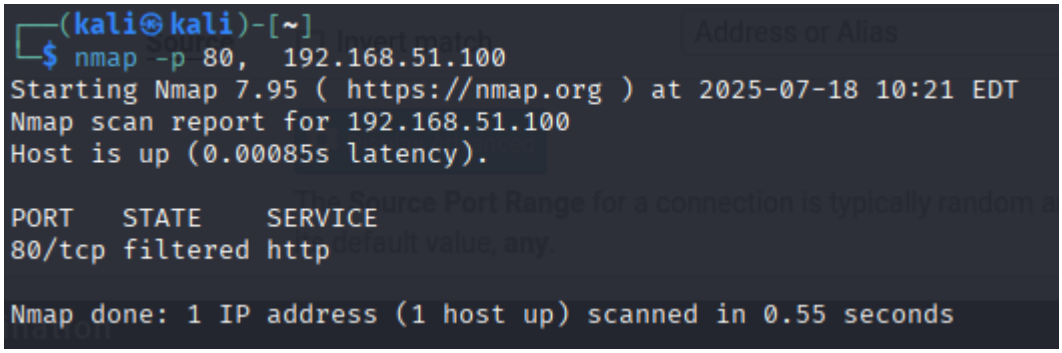
Ho settato l'IPv4 statico e come indirizzo ho messo il gateway 192.168.51.1 in modo che le macchine che usano la scheda di rete chiamata meta usino 192.168.51.1 come punto di uscita per quella rete.

2. Poi ho creato le regole firewall in modo da impedire la comunicazione http tra Kali e Metasploitable



Ho impostato come azione quella di bloccare il traffico, scelto LAN come interfaccia da cui arrivano i pacchetti e imposto il protocollo su TCP perché blocca specificatamente l'accesso web alla DVWA mantenendo altri servizi funzionanti; infatti, se facessi una prova di ping tra Kali e Metasploitable risulterebbe eseguito con successo. Infine, imposto come IP sorgente l'IP della Kali, come IP destinazione quello di Metasploitable e il range delle porte su 80(porta http).

3. Come prova dell'effettivo funzionamento della regola, ho eseguito uno scan Nmap su porta 80 verso l'indirizzo IP 192.168.51.100(Metasploitable2).



La risposta allo scan risulta corretta perché lo stato della porta 80 è filtrata, il che vuol dire che la regola impostata nel firewall funziona.