Traccia:

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

Introduzione

Si precisa in via preliminare che per lo svolgimento della traccia in oggetto si renderà necessario l'utilizzo simultaneo di tre macchine virtuali (da qui a seguire v.m.):

- una v.m. con un sistema operativo "Kali Linux";
- una v.m. con installata la distribuzione "Pfsense";
- una v.m. con installato il software "Metasploitable".

Sempre a livello didascalico, si specifica che il software Metasploitable consiste in una piattaforma che consente di eseguire dei *"penetration test"* in totale sicurezza.

Nella consegna odierna si procederà dunque alla realizzazione di una prima – sebbene molto semplice – difesa contro tentativi di accesso alla DVWA dalla v.m. con Kali Linux.

A tale scopo si renderà necessario impostare specifiche regole nel *Firewall* [1]attraverso la Web Gui di Pfsense.

Passo 1 – azioni preliminari

Prima di procedere con lo svolgimento della traccia risulta di fondamentale importanza verificare le impostazioni di rete di tutte e tre le v.m.

Per eseguire la verifica occorre accedere alla propria piattaforma ospitante le v.m., preselezionare la v.m. interessata, quindi cliccare su "impostazioni".

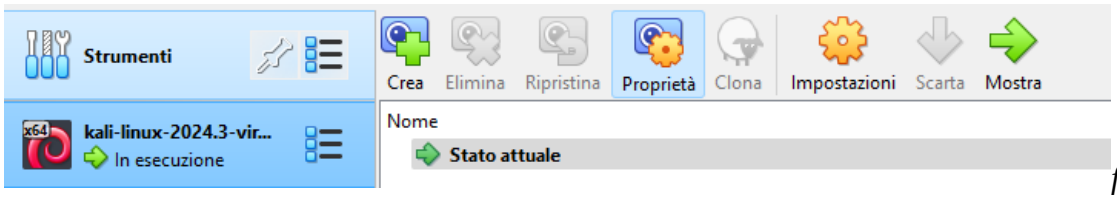

fig.1

Una volta entrati nelle impostazioni, selezionare "rete" sul menù a tendina e verificare che la scheda di rete sia abilitata e:

- nel caso della v.m. con Kali Linux, impostata su rete interna

[1] *"Dispositivo hardware o software di difesa, utilizzato durante la navigazione in rete contro eventuali attacchi di cracker o altri tentativi di intrusione; funziona come un filtro dei dati in entrata e in uscita dal computer collegato a Internet, dei quali controlla l'affidabilità innalzando il livello di sicurezza del sistema sul quale è installato".* https://www.treccani.it/vocabolario/firewall/

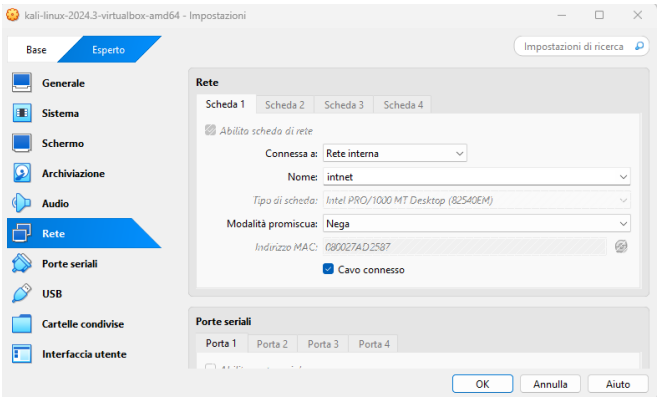

fig.2

- nel caso della v.m. con Pfsense siano abilitate tre schede di rete, rispettivamente la prima con una rete NAT, la seconda con una rete Interna e la terza con una rete bridge

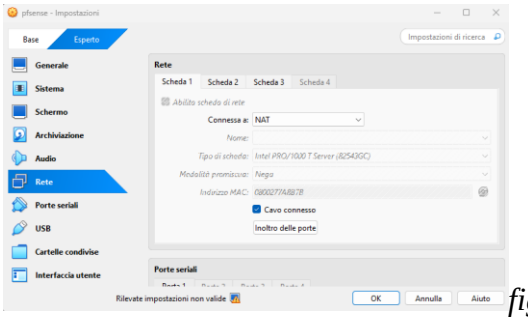

fig.3

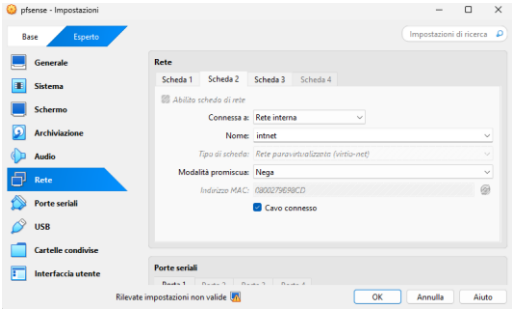

fig.4

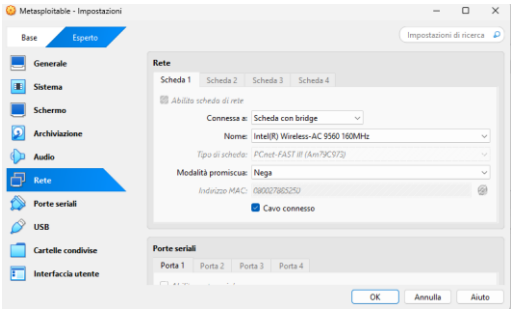

fig.5

- nel caso invece di Metasploitable, vi deve essere una sola scheda di rete attiva, con una rete bridge.

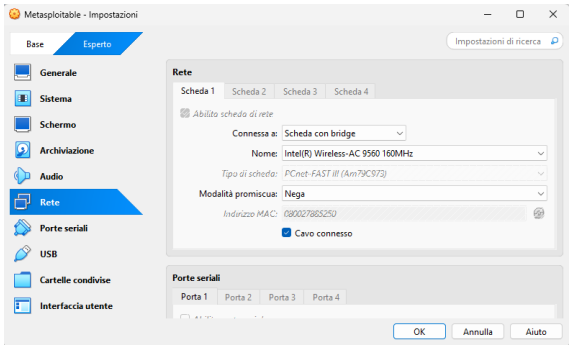

fig.6

Passo 2 – configurazione IP

Una volta verificate che le schede di reti siano correttamente impostate, occorre ora sincerarsi che:

- Kali e Pfsense insistano sulla medesima rete;
- Metasploitable sia collocato in una rete diversa.

Per procedere in tal senso è necessario agire a livello IP: sostanzialmente gli IP di Kali e Pfsense dovranno condividere il terzo ottetto dell'indirizzo.

Nel caso di specie si è imposto manualmente un nuovo indirizzo IP su Kali, seguendo il procedimento di cui alle seguenti figure.

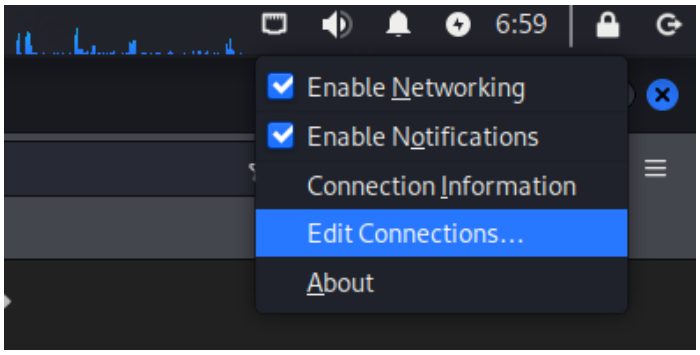

fig.7

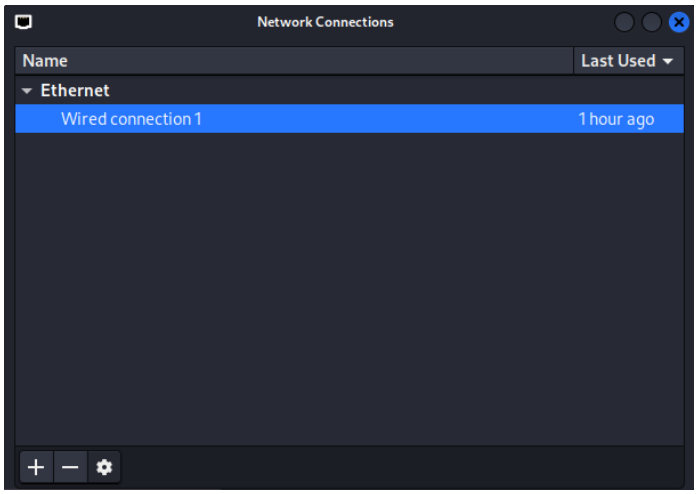

fig.8

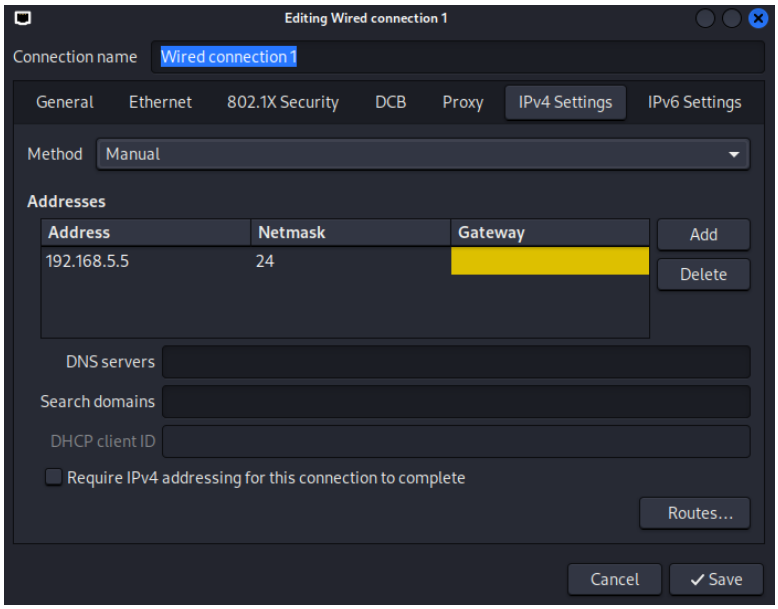

fig.9

Impostare Manual su "Method", quindi aggiungere l'indirizzo IP di nostro interesse con "**add**", congiuntamente con una Netmask (24 nel caso di specie) e infine cliccare su salva. A questo punto per una maggiore sicurezza si può procedere con l'esecuzione di una prova.

Su Terminal Emulator dare il comando "**ip a**".

L'output dovrebbe dare riscontro col medesimo indirizzo IP impostato manualmente.

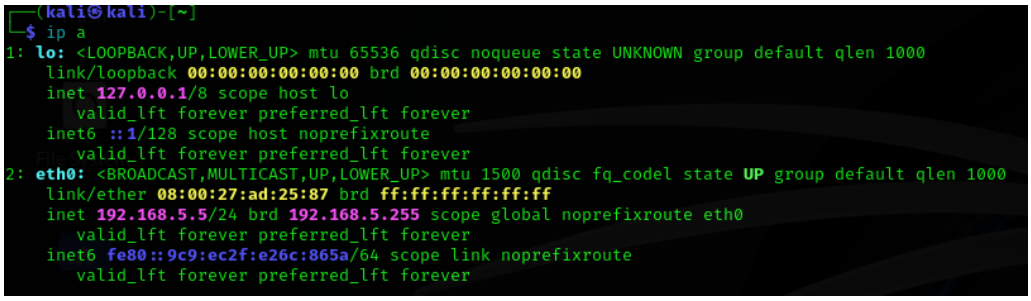

fig.10

Ora procedere con il verificare e (se necessario) modificare l'indirizzo IP su Pfsense.

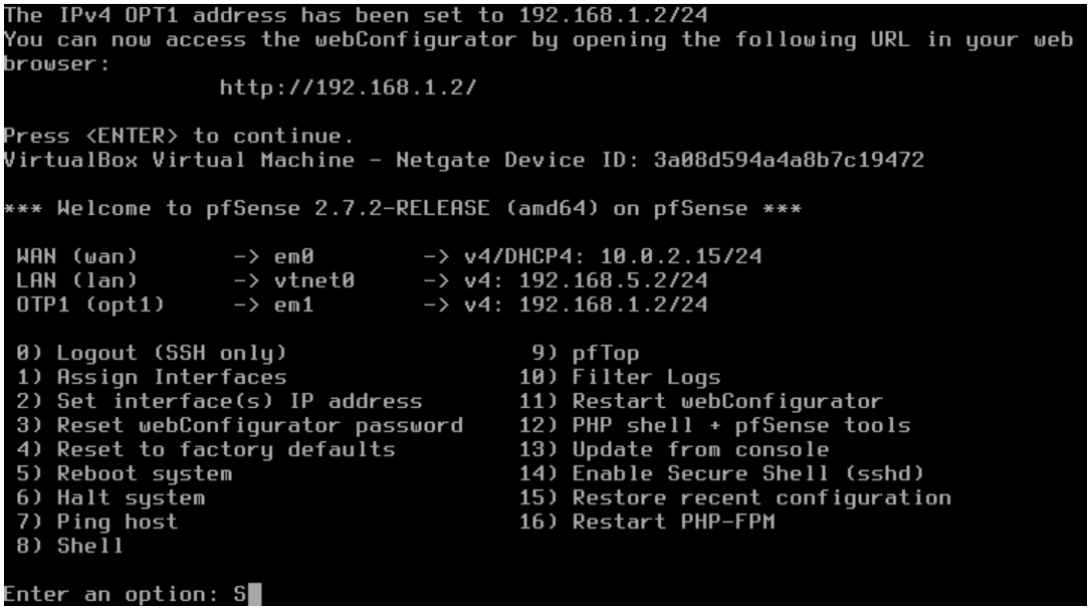

fig.11

Nel caso che ci interessa l'indirizzo IP di Pfsense si trova già impostato sulla medesima rete di Kali Linux, ma nel caso in cui così non fosse si dovrebbe digitare "2" e seguire la procedura guidata del programma, inserendo solamente l'IP desiderato quando richiesto.

A questo punto, per scrupolo, verificare l'IP di Metasploitable, dandogli il comando "**ifconfig**".

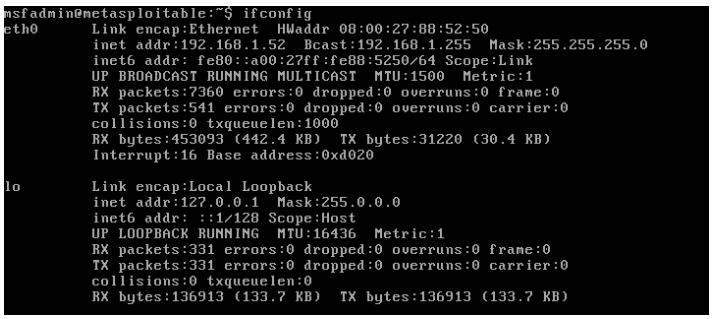

fig.12

L'IP di *default* di Metasploitable provvede già a collocarlo su una rete differente.

Passo 3 – il Firewall

A questo punto si apra il *browser* di Kali Linux e digitare nella barra di ricerca l'indirizzo IP di Pfsense.

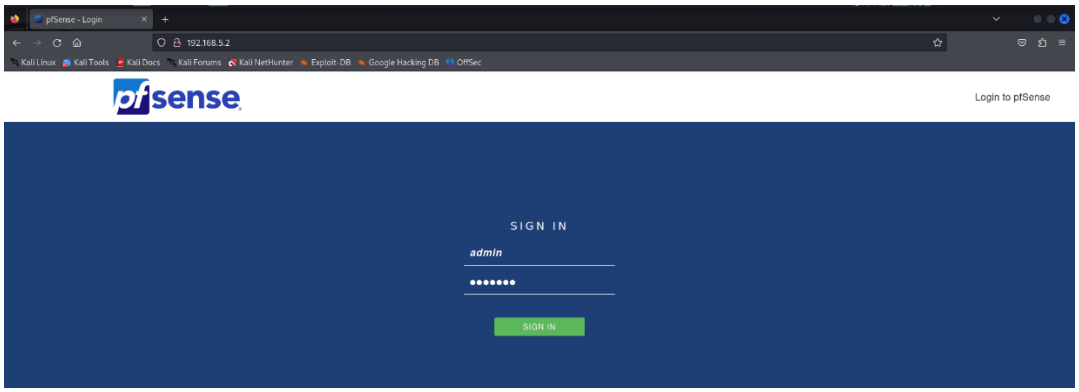

fig. 13

Procedere, qualora richiesto, ad eseguire il "*log in"* sul Web Gui con le credenziali di *default* (user: "admin"; password: "pfsense") oppure con quelle personalizzate se precedentemente alterate.

Dalla barra degli strumenti quindi selezionare Firewall e quindi "*rules*".

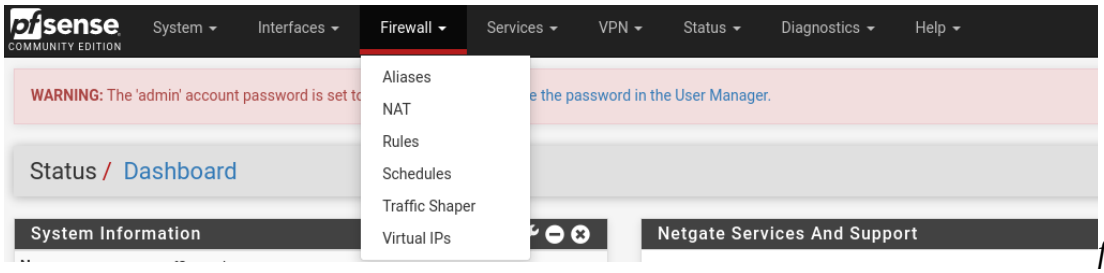

fig.14

A questo punto è possibile procedere con la creazione di una regola su una o più delle reti di Pfsense.

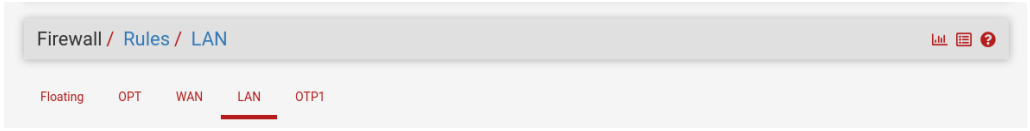

fig.15

Si proceda dunque a imporre una regola di blocco sulla rete LAN, premendo sul tasto "**add**".

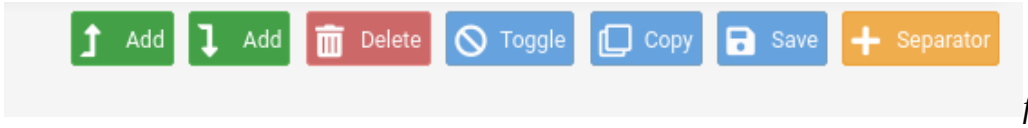

fig.16

Completare i riquadri con le informazioni richieste come nella figura a seguire.

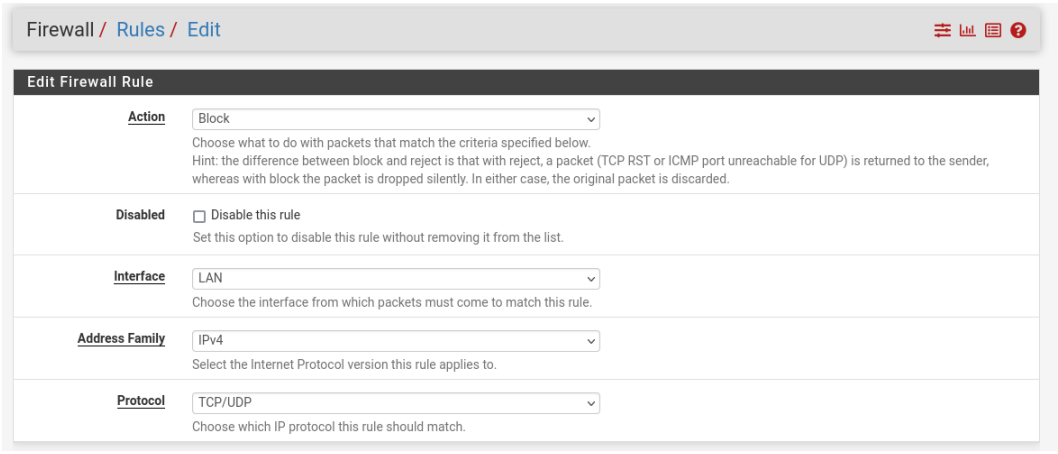

fig. 17

Ora, inserire l'IP sorgente e l'IP destinazione, allo scopo di imporre correttamente il senso di marcia del traffico dati che si intende bloccare con la regola di blocco.

Un elemento particolarmente importante del passaggio in questione è la parte relativa all'indicazione delle porte. Nel caso che interessa si è proceduto ad impostare "**any**", allo scopo di impedire che il flusso di dati passi attraverso "qualunque" porta.

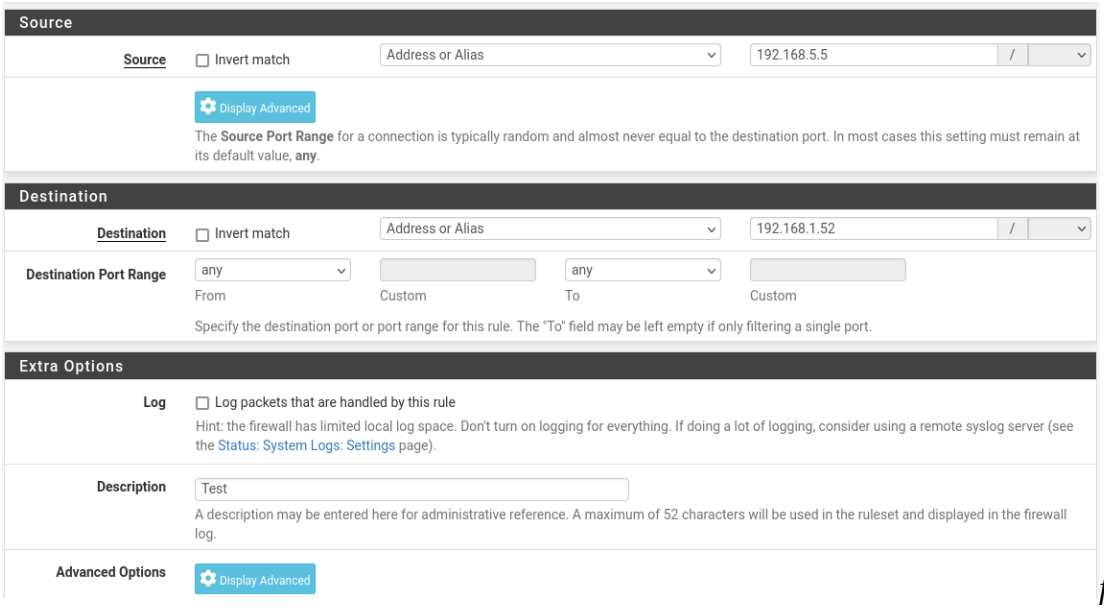

fig.18

A questo punto cliccare "**salva**" e successivamente su "***apply changes***".

Seguendo il medesimo procedimento è possibile creare anche diverse altre tipologie di regole o ripetere la medesima regola anche su altre reti di Pfsense, come nella figura a seguire.

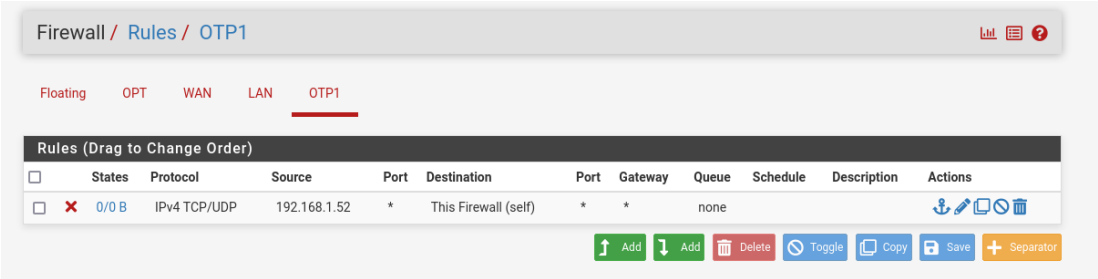

fig.19

Ulteriore passaggio significativo è anche la configurazione dell'interfaccia che si è andata a creare nel momento in cui si sia dovuto procedere con l'abilitazione *ex novo* della terza scheda di rete sulla v.m. di Pfsense.

A tale scopo si torni alla barra strumenti della Web di Pfsense, si selezioni "**Interfaces**" e dunque "**Assignments**".

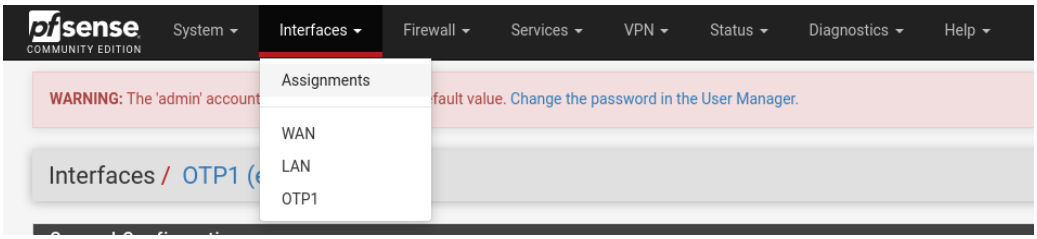

fig.20

Ora si prema sulla rete OTP1

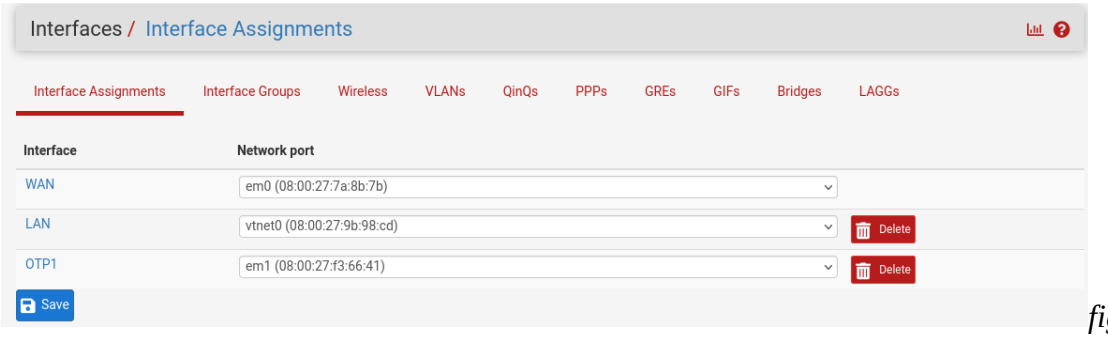

fig. 21

Dunque, si proceda al relativo settaggio come in figura a seguire. Nel caso di interesse si è proceduto ad inserire l'IP di Metasploitable.

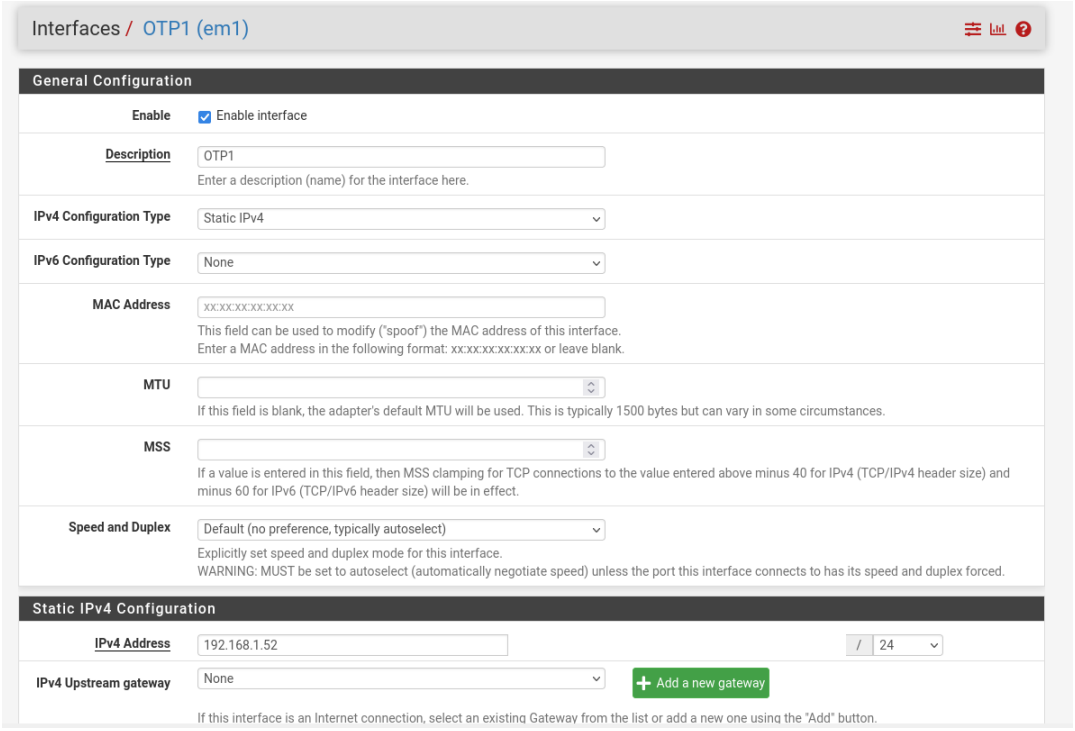

fig.22

Passo 4 – verifica

Con la configurazione del Firewall così come precedentemente descritta nei passaggi precedenti, né Kali Linux né Metasploitable sono in grado di comunicare.

Si è infatti provato sia ad eseguire il comando **ping** da Kali verso Metasploitable e l'output ha dato riscontro negativo;

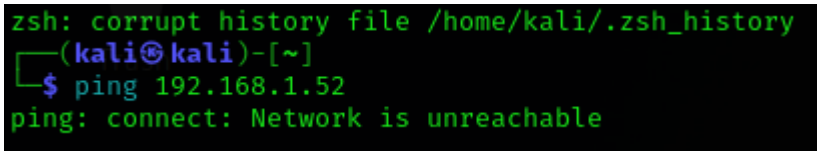

fig. 23

Si è provato altresì a dare il comando di scansione a Metasploitable, ricevendo esito sempre negativo.

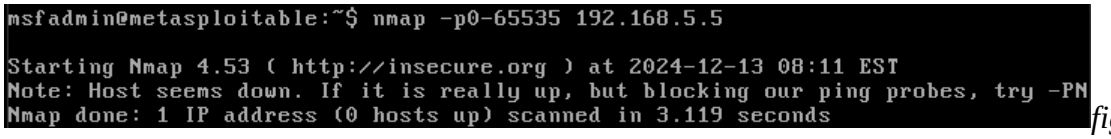

fig. 24