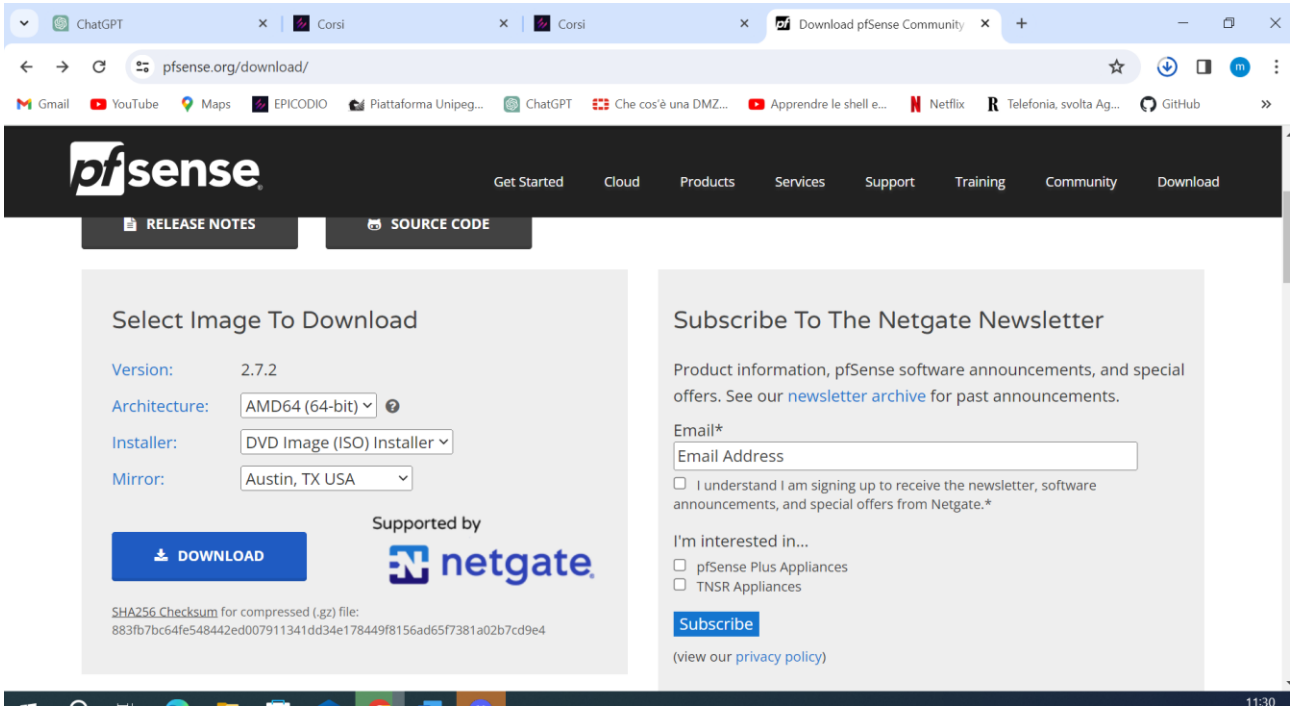
Pratica S5 – L1 FIREWALL VIRTUALE PFSENSE

Per consolidare le conoscenze a livello network, e vedere in pratica come funziona un firewall e come impatta eventualmente i test (ad esempio gli scan) ne vedremo uno virtuale: pfsense.

Pfsense è una distribuzione basata su FreeBSD ottimizzata per essere utilizzata come firewall. Può essere utilizzata sia su macchina virtuale (scaricando l'immagine dal sito ufficiale) oppure può essere installato su Hardware fisico.

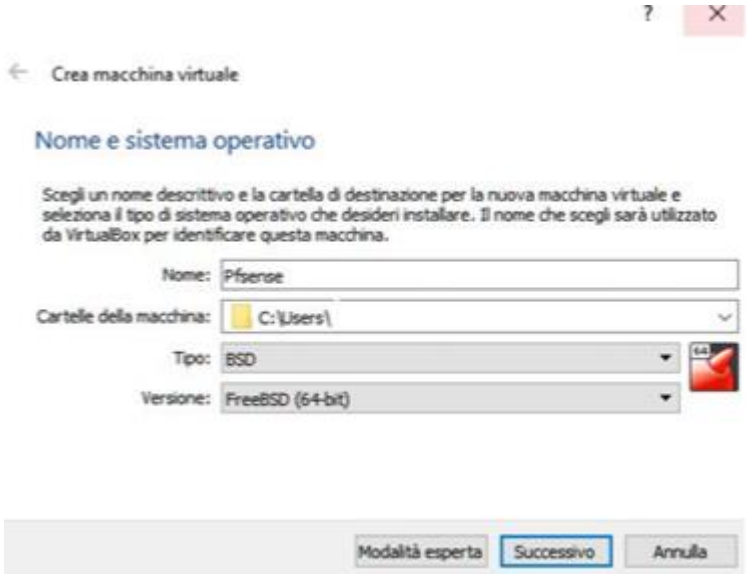
INSTALLAZIONE, ESTRAZIONE E CONFIGURAZIONE VM PFSENSE.

L'immagine da installare in virtualbox può essere scaricata da **https://www.pfsense.org/download/** scegliendo, come di consueto, la piattaforma consona in base alla nostra macchina.



Dopo aver scaricato Pfsense, procediamo ad **estrarre il file .iso** dall'archivio.
Per questo scopo utilizziamo winrar (o altra) per estrarre il file andando sul download scaricato di Pfsense e cliccando "estrai qui". Appare l'icona sul desktop dell'iso di Pfsense.

Poi su virtual box creiamo una **nuova VM**, **Pfsense**, (nuova) selezionando FreeBSD nel campo versione (32 o 64 bit in base all'immagine che avete scaricato), assegnando CPU e spazio disco come consigliato. **N.B**. Fare attenzione a rimuovere (tramite le impostazioni cliccando sulla macchina appena creata) la 2° opzione che rappresenta Il pacchetto di installazione e che, se non rimosso, fa l'installazione all'infinito (grafico 1).



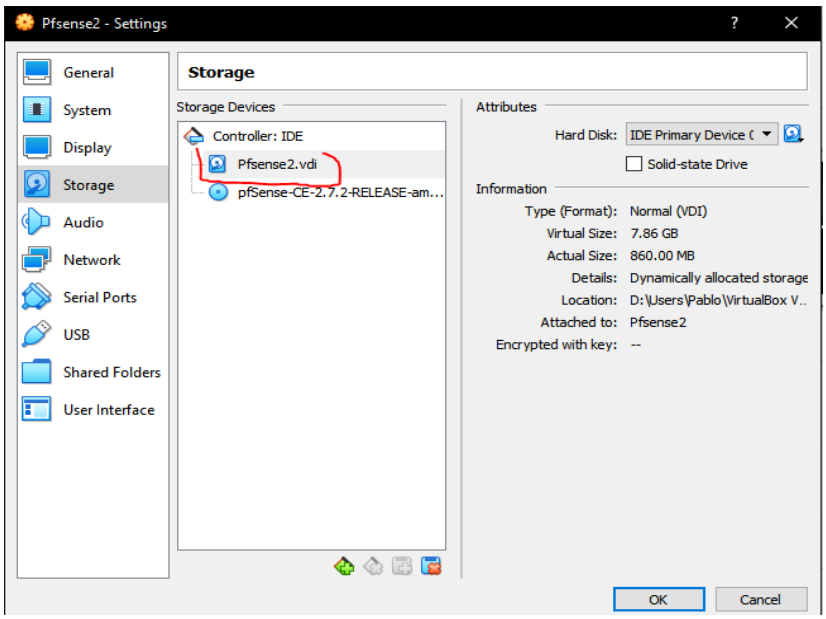
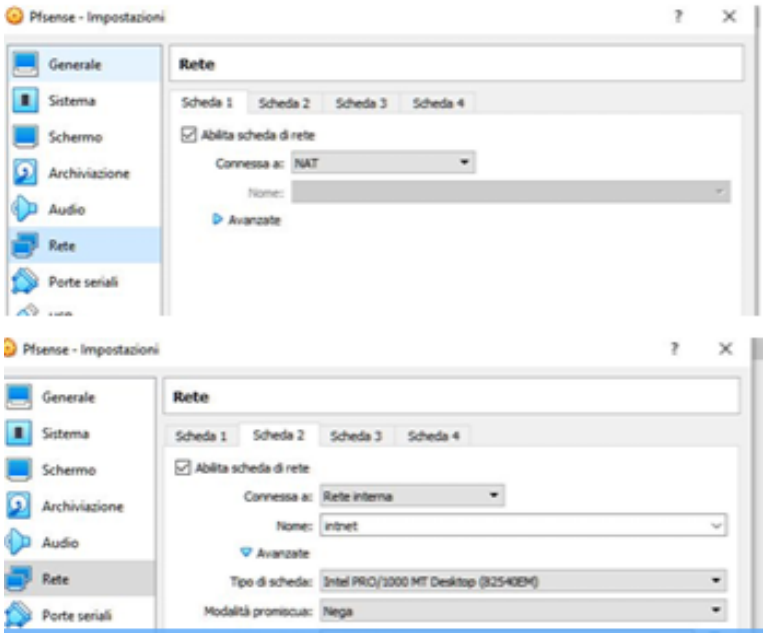


grafico 1

Poi andiamo sulle impostazioni della nuova macchina Pfsense e **creiamo 2 NIC** (interfacce di rete):

1° con NAT = interfaccia WAN

2°con INTERN = interfaccia LAN



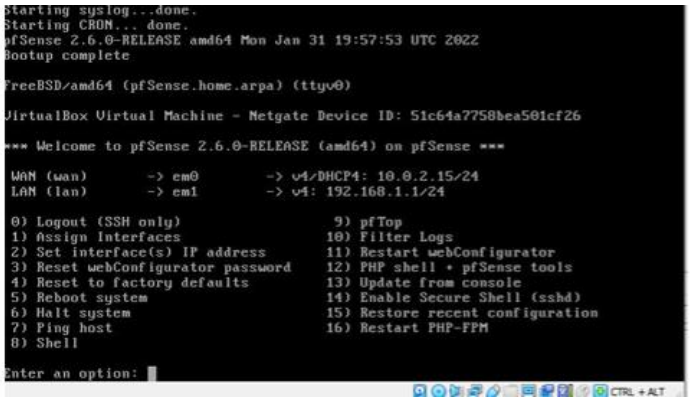
Una volta completata l'installazione di base, la macchina si riavvierà (accertatevi che nella lista dei boot ci sia il disco rigido come prima scelta) e si possono vedere le **configurazioni di rete sulla Shell**.

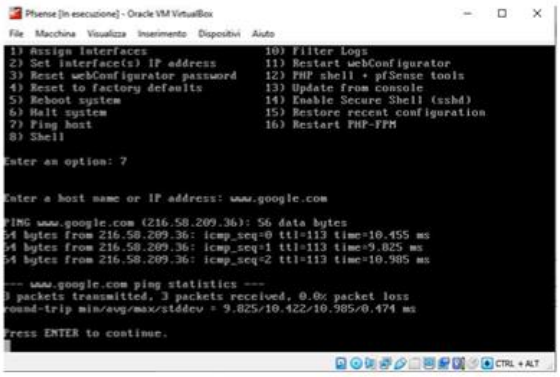
La macchina ha quindi 2 interfacce di rete, una WAN e due LAN.

Proviamo ad inviare un ping a www.google.com per accertarci che le configurazioni dell'interfaccia WAN sia ok e che ci sia connettività verso Internet.

Selezioniamo Ping host con il numero 7, poi scriviamo l'host da pingare.

Ps. In caso sia necessario cambiare la configurazioni di rete, per tornare alle configurazioni originarie è sufficiente scegliere l'opzione 4) Reset to factory default.



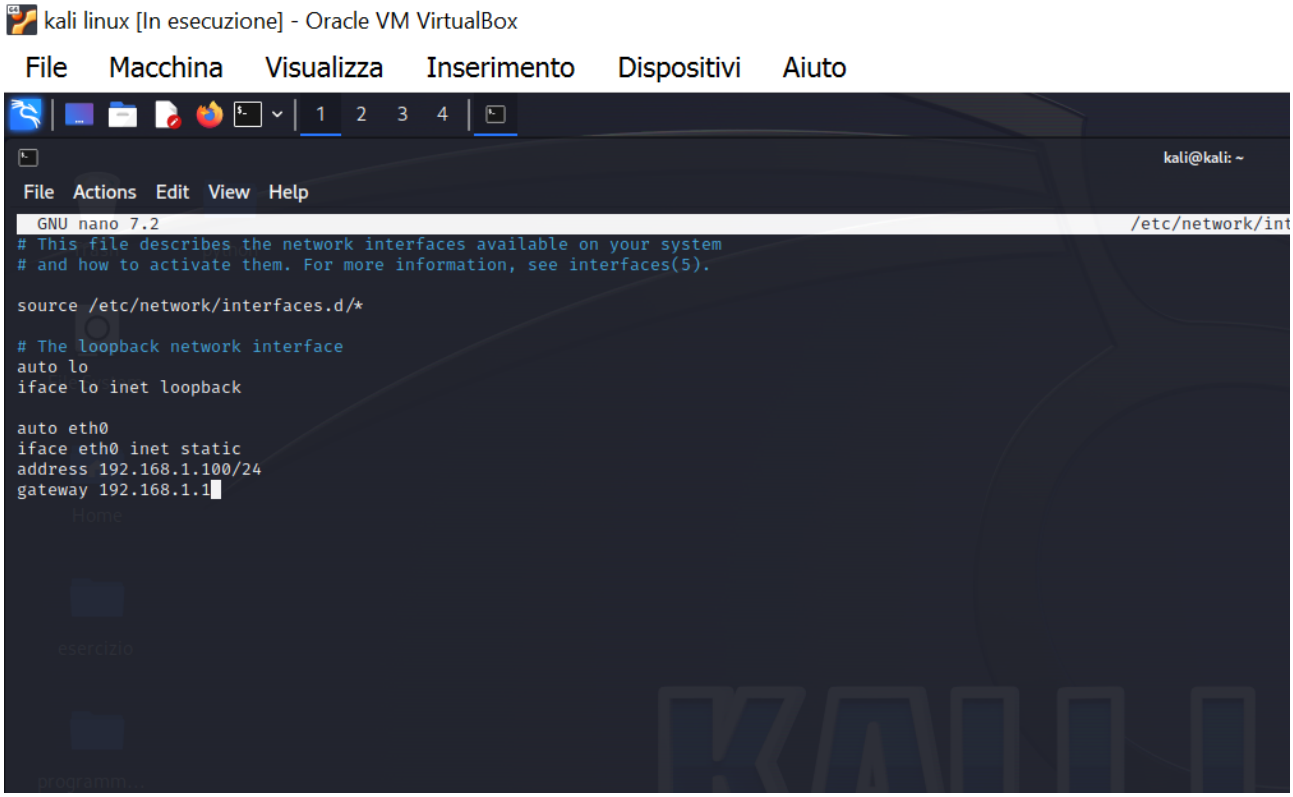


Creazione pratica di una regola Firewall (CON PRECEDENTE CREAZIONE DI ALTRA INTERFACCIA "LAN2"

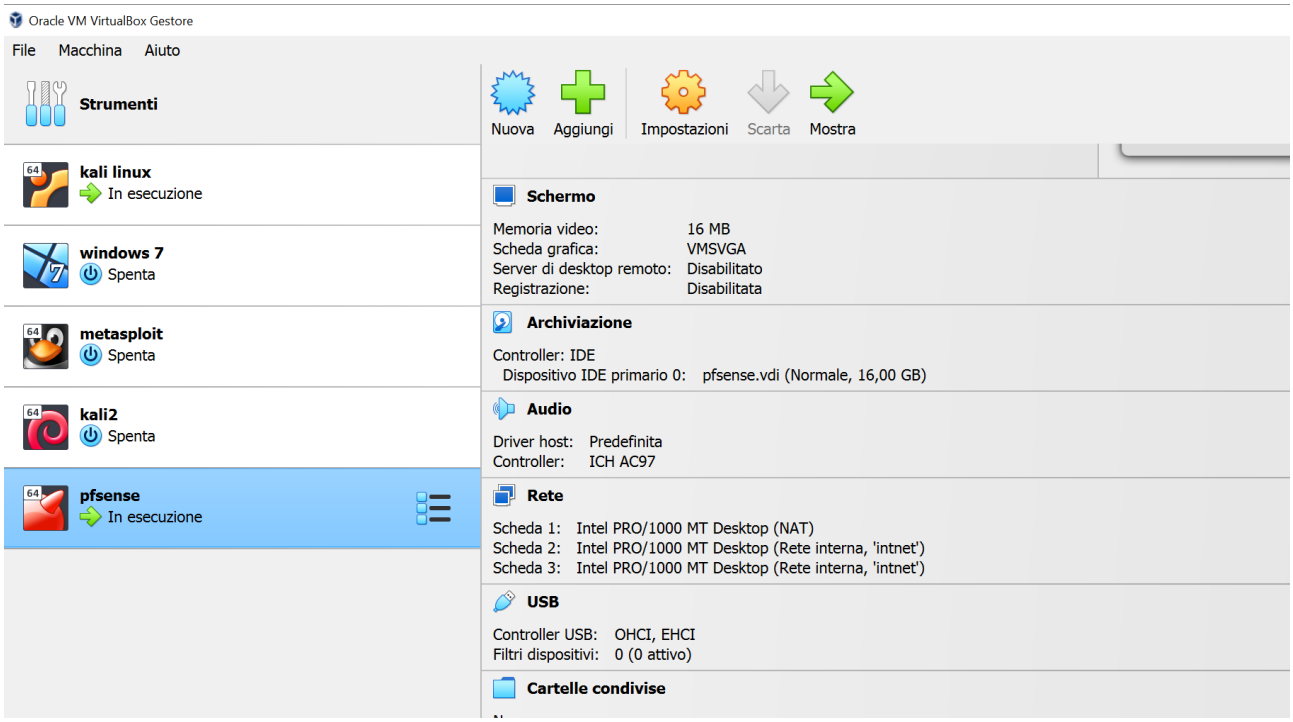
La pratica di oggi consiste nel **creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.**

Un **requisito** fondamentale dell'esercizio è che le **macchine Kali e Metasploitable siano su reti diverse**, potete aggiungere una **nuova interfaccia di rete a Pfsense** in modo tale da gestire una ulteriore rete.

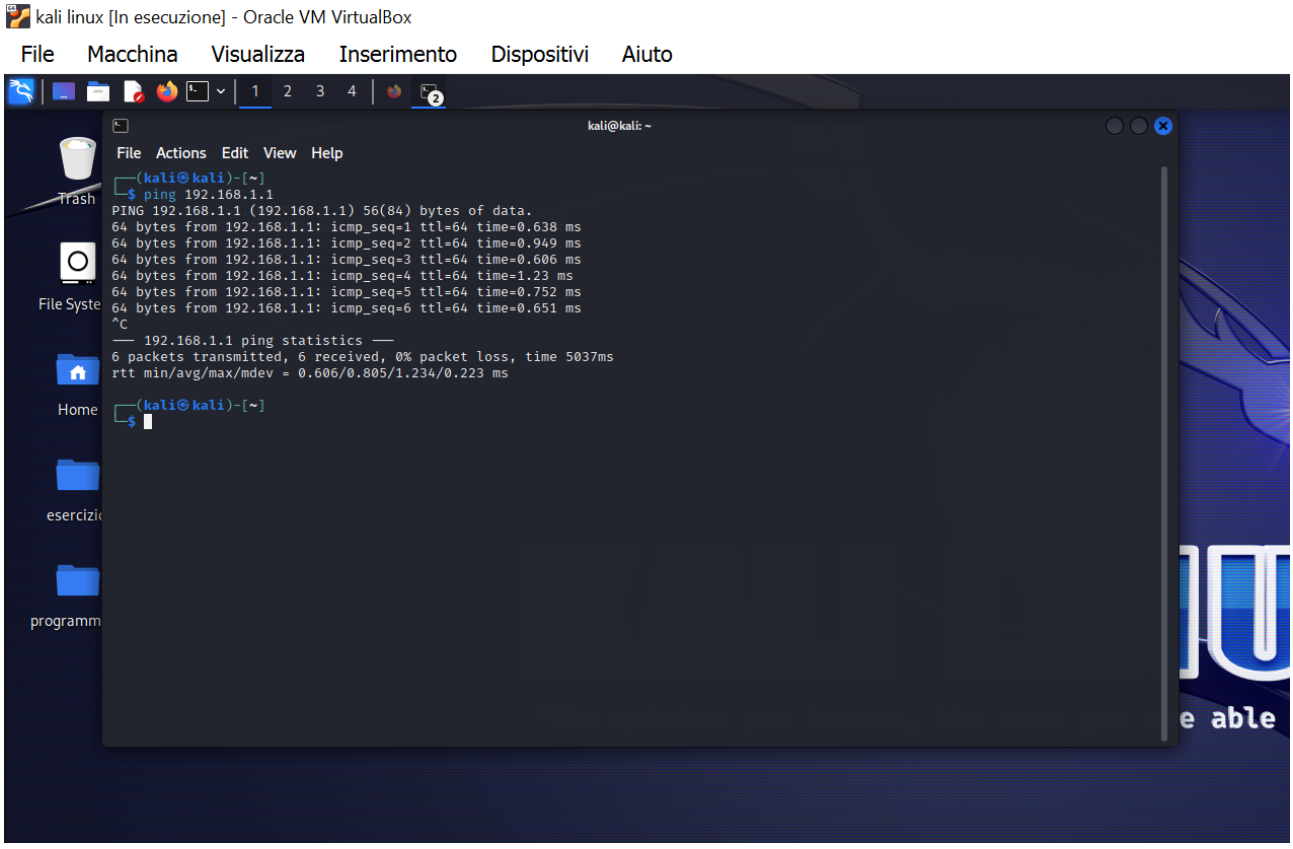
- Quindi prima di tutto sono andata nella configurazione di rete di **Kali linux** in INTERN (non è necessario sia connessa a Internet) e, con il comando sudo nano /etc/network/interfaces ho **modificato address e gateway**, inserendo come **subnet** quella **di Pfsense** (.1.), come in figura sotto. In tal modo, senza toccare la configurazione di Meta, Kali e Meta risulteranno avere due reti diverse.



- Poi ho creato la **terza scheda di rete** sulla macchina **Pfsense**, che corrisponde ad un'altra **LAN**, sempre **INTERN.**

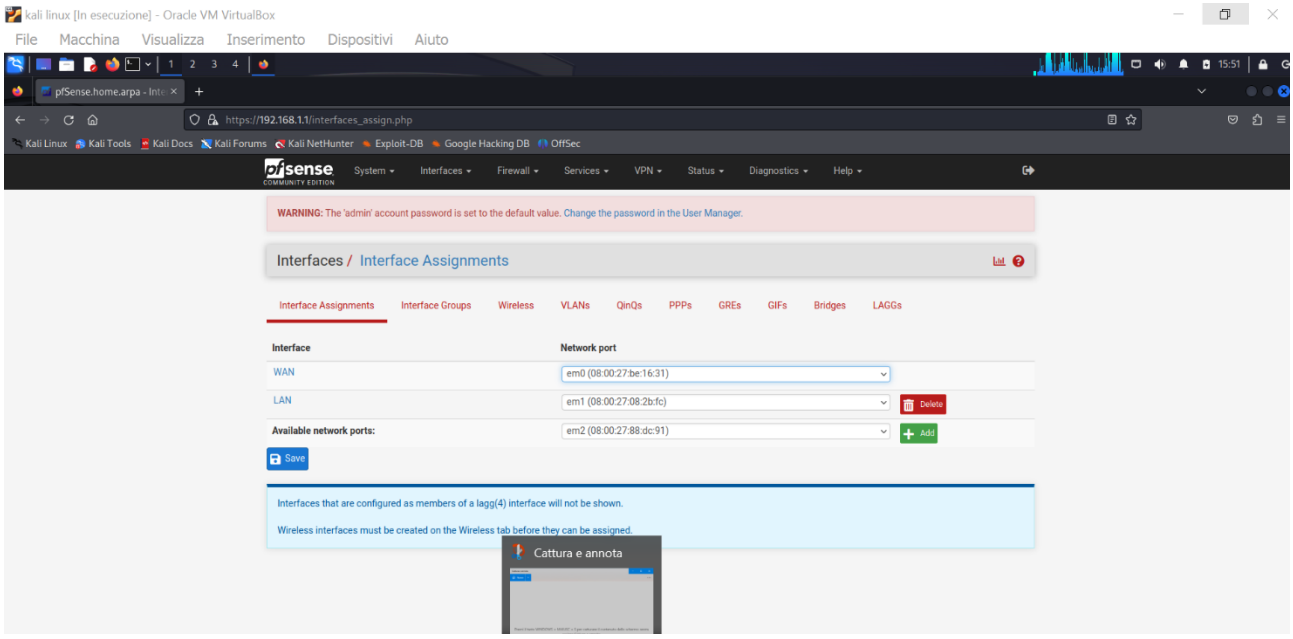


Per vedere se Kali e Pfsense comunicano, sono andata a fare il **ping da Kali con l'IP di Pfsense**.



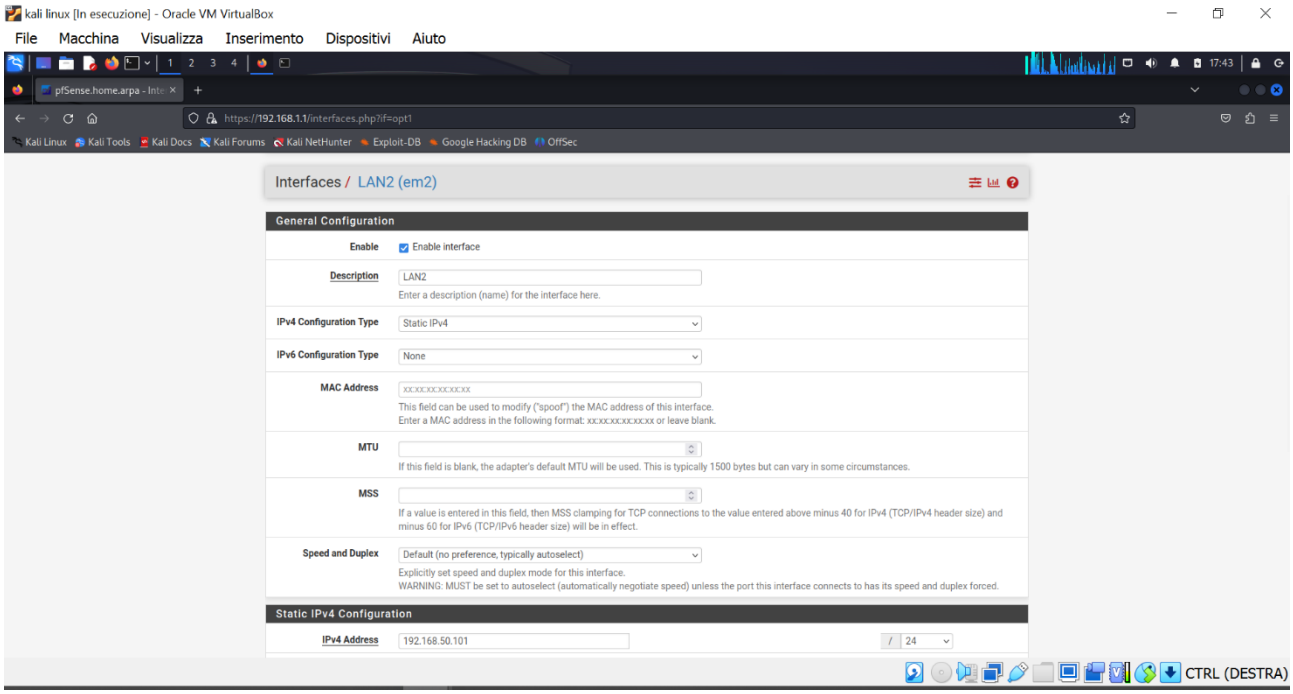
Per la creazione della regola Firewall che blocchi l'accesso alla DVWA (di Meta) sono andata ad **inserire l'IP (LAN) di Pfsense nel browser di Kali**.

- Prima di tutto, ho **creato l'interfaccia della 2° rete LAN Intern** andando su Interfaces, Assignments e cliccando su Add e poi su OPT1.

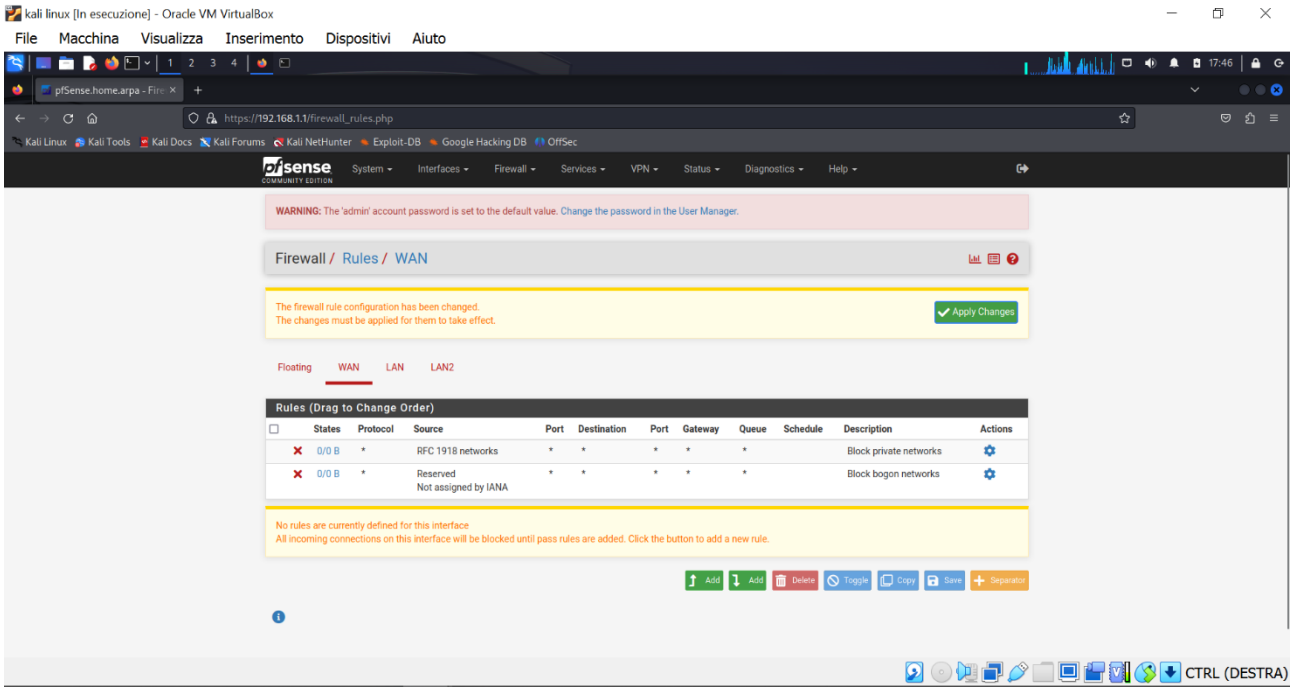


Ho poi **inserito i dati necessari**:

✓ Enable interfaces, LAN2, Static IPv4 e In "IPv4 Address" l'IP di Meta/24. Infine ho **salvato** (Save, che in figura era in basso anche se non visibile). Infine ho cliccato su "**Apply changes**".

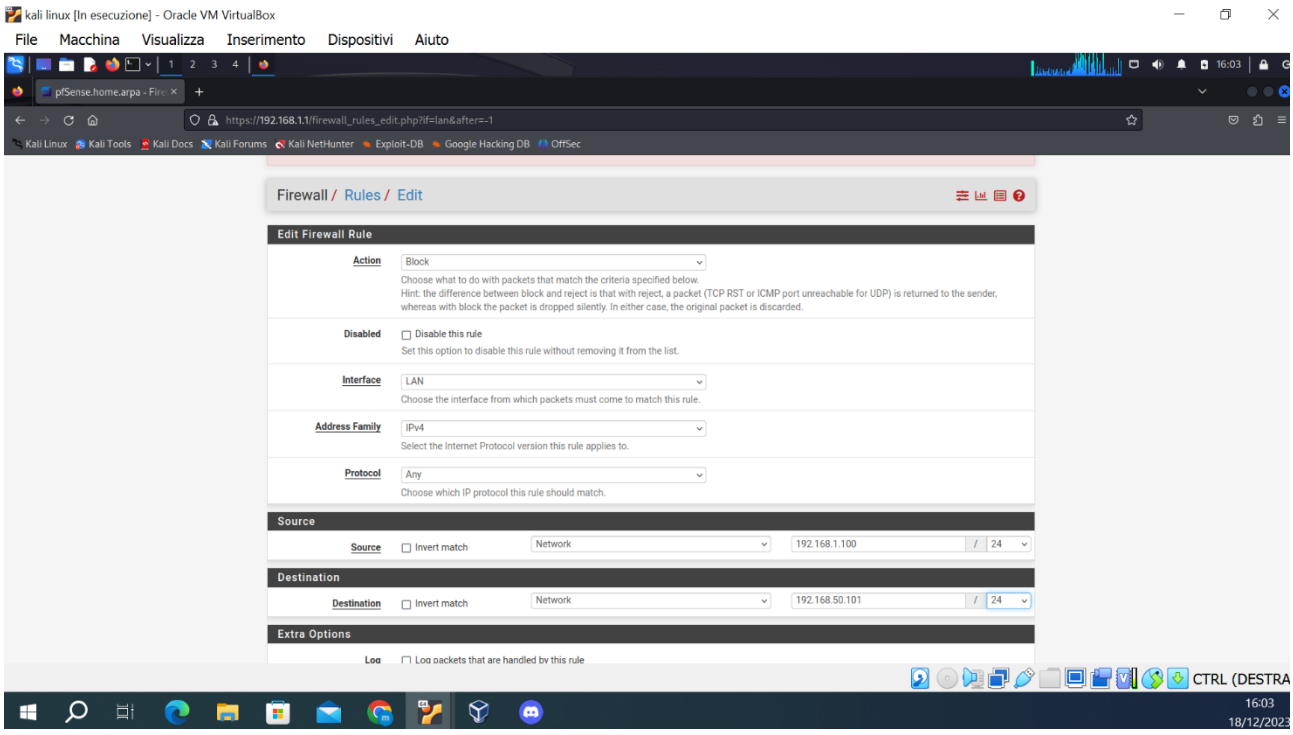


Poi sono andata su Firewall/Rules/LAN2 per **creare la nuova regola,** cliccando su **LAN2**.

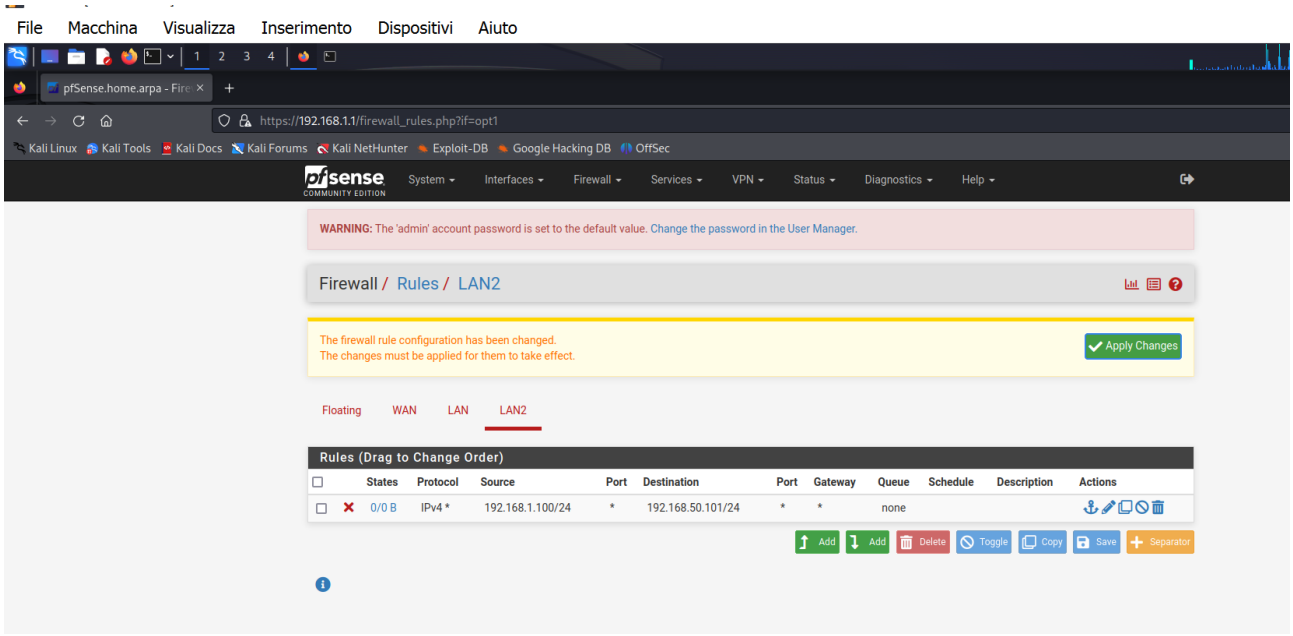


In LAN2, ho premuto **Add** e ho inserito i seguenti dati:

- in “Action”: Block
- in “Protocol”: Any
- nei campi di Source prima Network, poi IP di Kali/24
- nei campi di Destination: prima Network, poi IP di Meta/24.



Infine ho cliccato su Save e Apply changes, ottenendo il risultato grafico della nuova regola impostata, come si vede in figura.



- Infine ho **tentato** il **ping da kali all'indirizzo IP di Meta**, per testare l'efficacia della regola settata nel Virtual Firewall.
  Come si vede dall' immagine successiva, la comunicazione fra le due macchina potrebbe effettivamente avvenire perché, nonostante siano su due reti diverse, Pfsense fa da tramite. La connessione però viene bloccata proprio dal Firewall stesso.
  Qualora, invece, tentando il ping, la risposta fosse stata "Host unreachable", allora le due macchine non avrebbero avuto alcun tipo di comunicazione.