Che cos’è un Firewall?

Un firewall è uno dei componenti fondamentali nella sicurezza informatica. Si tratta di un dispositivo o di un **software** progettato per proteggere una rete informatica o un sistema da minacce esterne, regolando il traffico di rete in entrata e in uscita. Un **firewall** funge da guardiano tra una rete interna e il mondo esterno. Esamina il traffico di rete e decide se consentire o bloccare il passaggio dei dati in base a regole predefinite.

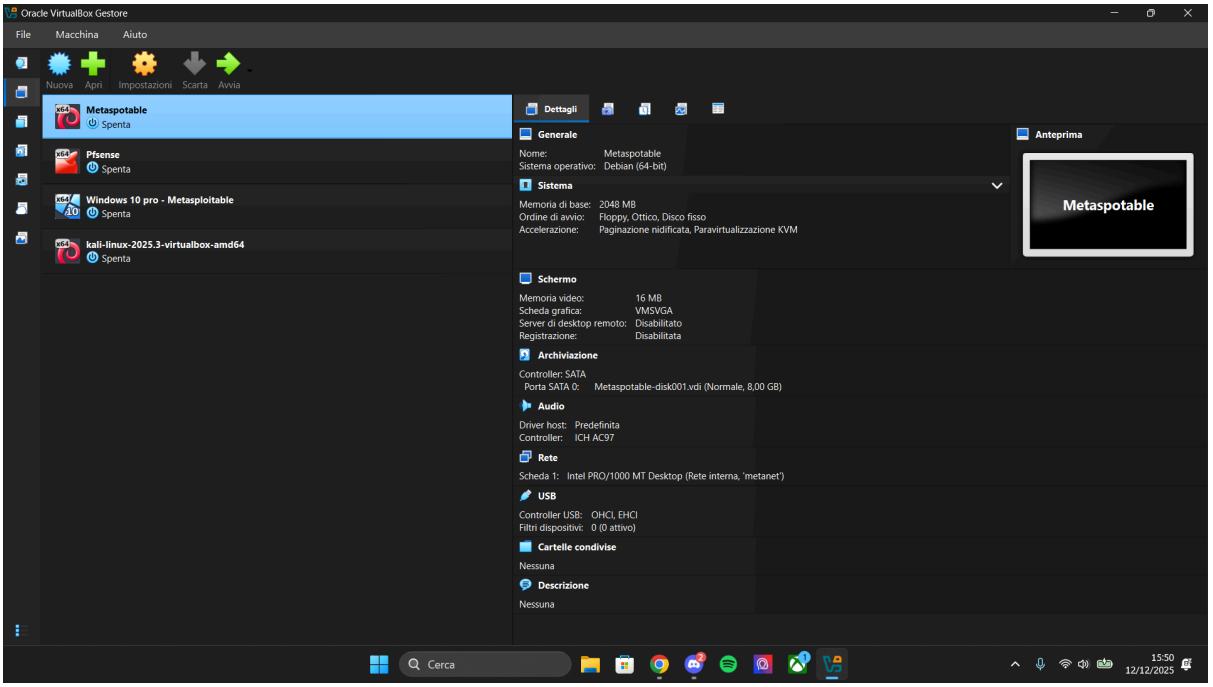
Componenti del Firewall:

I firewall possono essere costituiti da **software**, **hardware** o una combinazione di entrambi. I componenti principali includono:

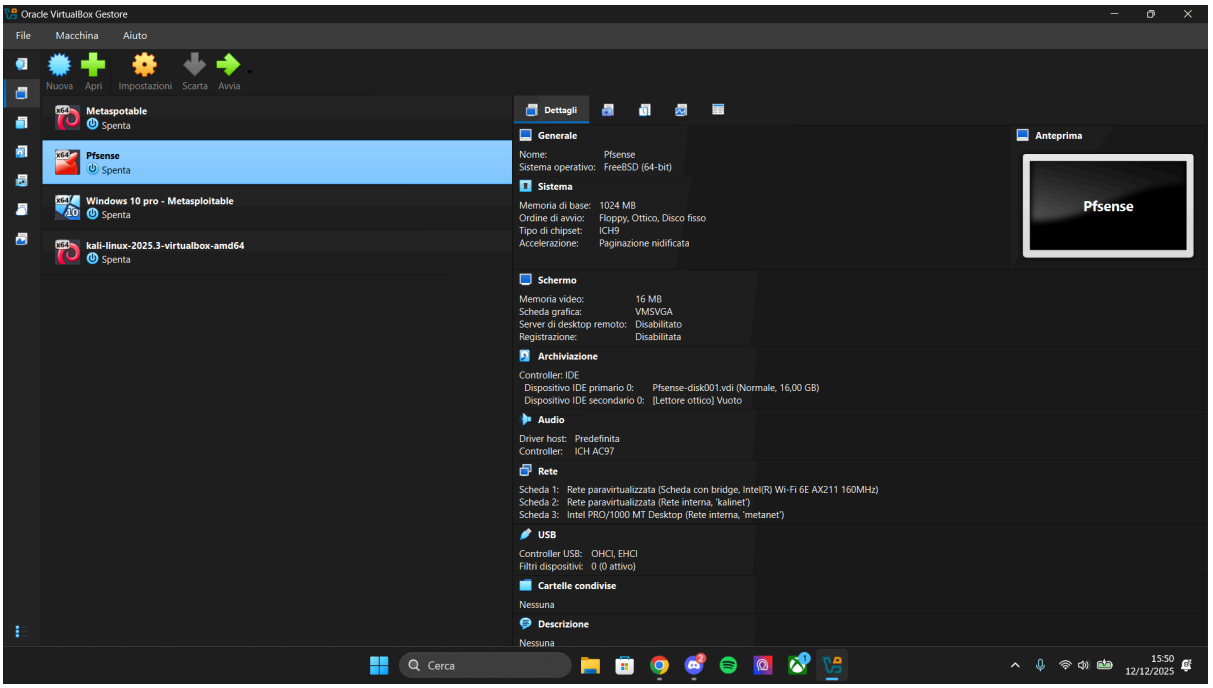
1. **Motore di ispezione del traffico:** Il motore di ispezione del traffico è il cuore di un **firewall**. Questo componente analizza il traffico di rete che attraversa il **firewall** per determinare se deve essere permesso o bloccato, basandosi su regole di sicurezza preconfigurate.
2. **Interfaccia di gestione:** L'interfaccia di gestione è lo strumento attraverso il quale gli amministratori configurano e monitorano il **firewall**. Una buona interfaccia di gestione è essenziale per una gestione efficace e intuitiva del **firewall**.
3. **Database delle regole:** Il database delle regole è dove sono memorizzate tutte le politiche di sicurezza e le regole di filtraggio del **firewall**. È il componente che il motore di ispezione del traffico consulta per determinare l'azione da intraprendere per ciascun pacchetto di dati.

Configurazione delle schede di rete su Virtual Box

Sulla **metasploitable,** creiamo una scheda di rete numero 1 e la settiamo su **rete interna.** Questa suddetta rete la chiamiamo **metanet.**



Sulla **pfsense** facciamo la stessa cosa, creiamo la nostra scheda di rete numero 3 e anche questa la settiamo su **rete interna** e la chiamiamo **metanet** così che la **pfsense** e la **metasploitable** possono comunicare.
Il **pfsense** farà da **firewall** tra le reti che abbiamo:
Scheda di rete 1: La **WAN** settata in **scheda con bridge** che comunica con la **rete esterna**.
Scheda di rete 2: E' configurata in **"rete interna"** che comunica con la **Virtual machine kali linux** e l'abbiamo chiamata **kalinet.**
Scheda di rete 3: E' configurata in **rete interna** con la **metasploitable** ed è chiamata **metanet.**

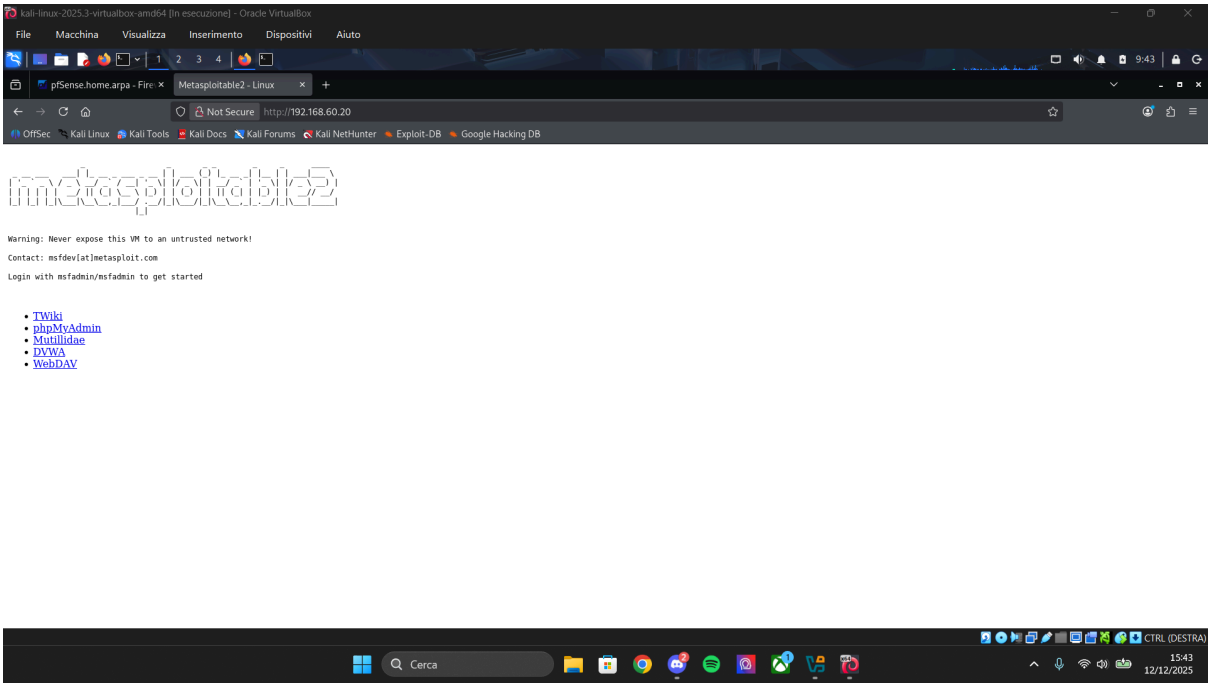


Configurazione della opt1

Sulla **pfsense** creiamo la rete **opt1** con indirizzo ip **192.168.60.0/24** e gli settiamo il **192.168.60.1/24** come **default gateway**, gli abbilitiamo il servizio di **DHCP** e gli diamo un range da **20-100 indirizzi** che lui può prendere per dividerli sui vari dispositivi.

```
The IPv4 OPT1 address has been set to 192.168.60.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.60.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 5edbc57bb83ebcf97efd

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.68.105/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.40.1/24
 OPT1 (opt1)     -> em0        -> v4: 192.168.60.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Fatto le configurazioni proviamo da browser della **kali** a raggiungere il sito della **metasploitable** usando l'indirizzo ip **192.168.60.20** perchè il **20** finale? il **20** finale sta per il primo indirizzo disponibile nel **pool** di indirizzi che gli abbiamo dato nella configurazione.
Il sito è raggiungibile.

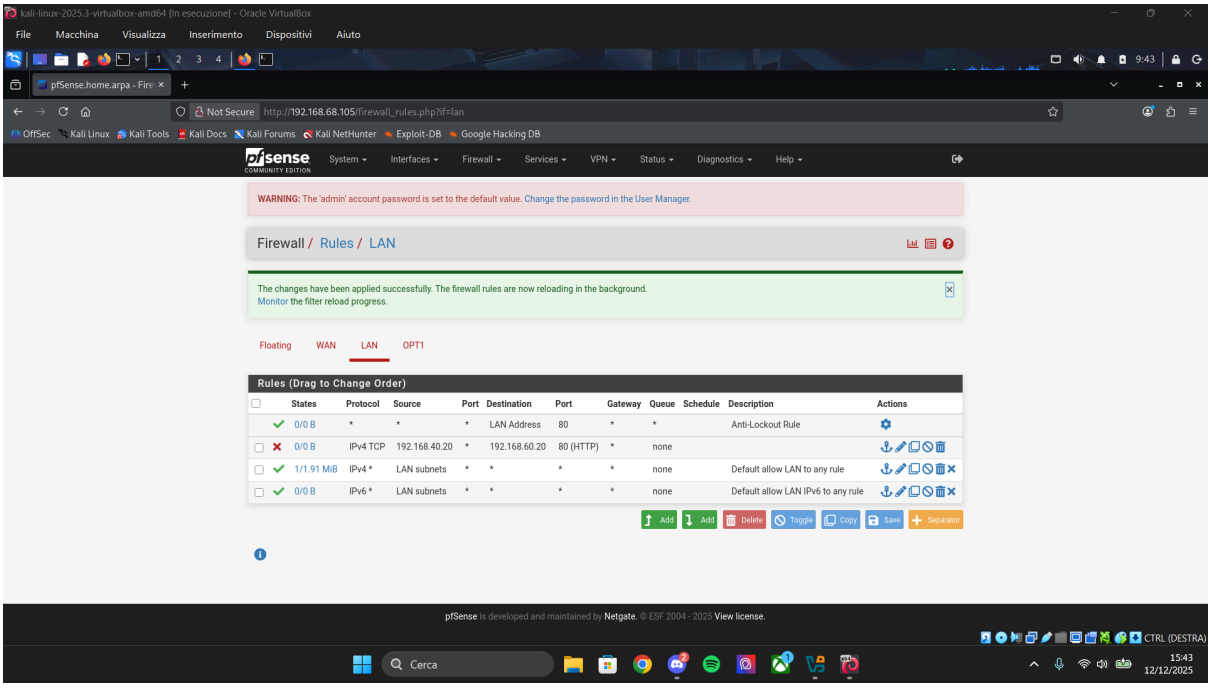


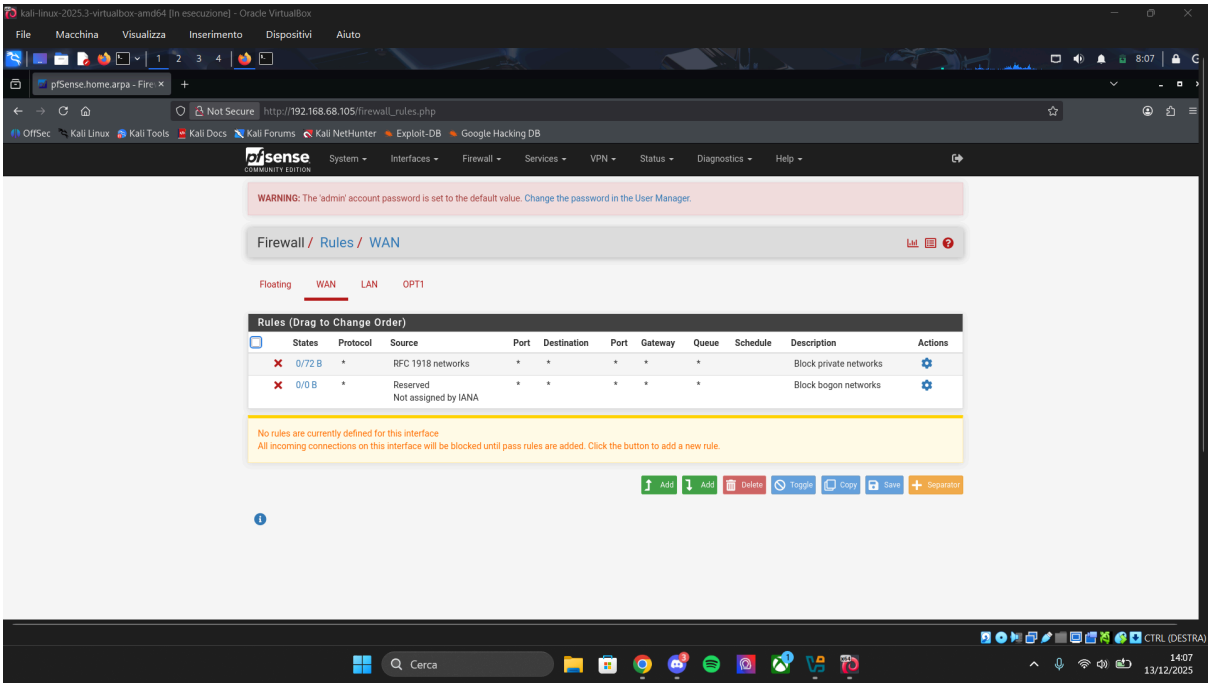
Regole sul Firewall

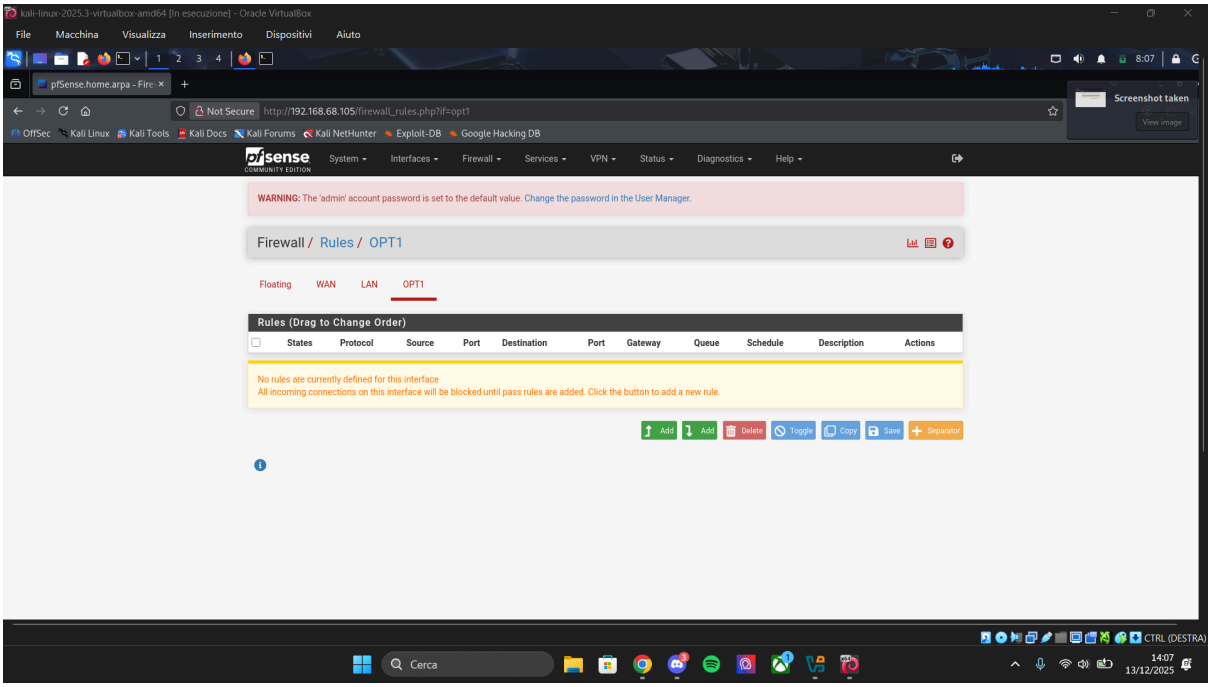
Per raggiungere il **firewall** andiamo sul indirizzo ip **192.168.68.105/24** una volta entrati ci dirigiamo sul **Rules** e aggiungiamo la regola che blocca il traffico dalla **kali** alla **metasploitable.**

Gli diciamo che dal indirizzo ip **192.168.60.20** il traffico verrà bloccato e la sorgente è **192.168.40.20** ovvero la **kali.**

Applicate le regole e salvate, se proviamo ad andare sul sito della **metasploitable** non riusciremo a raggiungerlo perché la regola precedentemente creata sta funzionando correttamente e blocca il traffico.







Ping

Vediamo se il ping funziona con il comando **ping 192.168.60.20** la connessione viene avviata con successo.