# Open Source Security

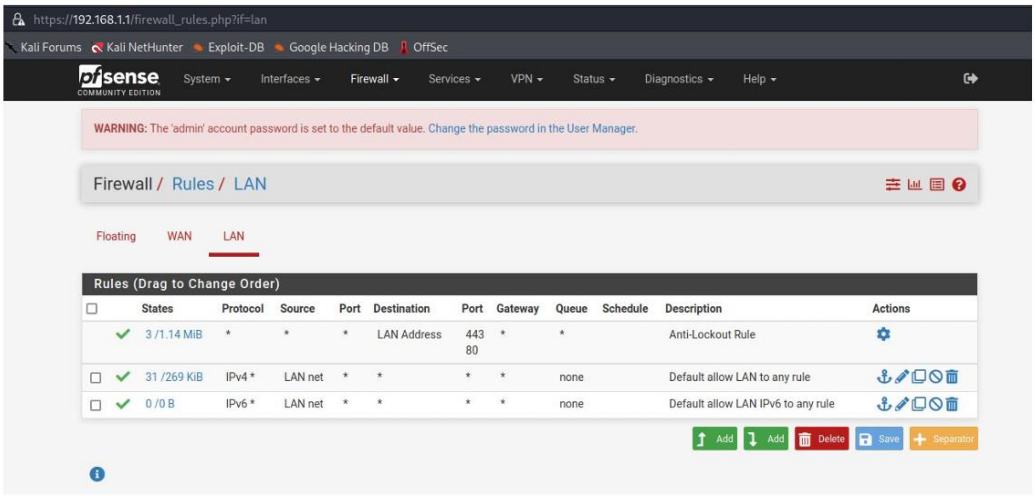
Secure networks start here.™ With thousands of enterprises using pfSense® software, it is rapidly becoming the world's most trusted open source network security solution.

## Sommario

# Traccia esercizio

Creazione pratica di una regola Firewall

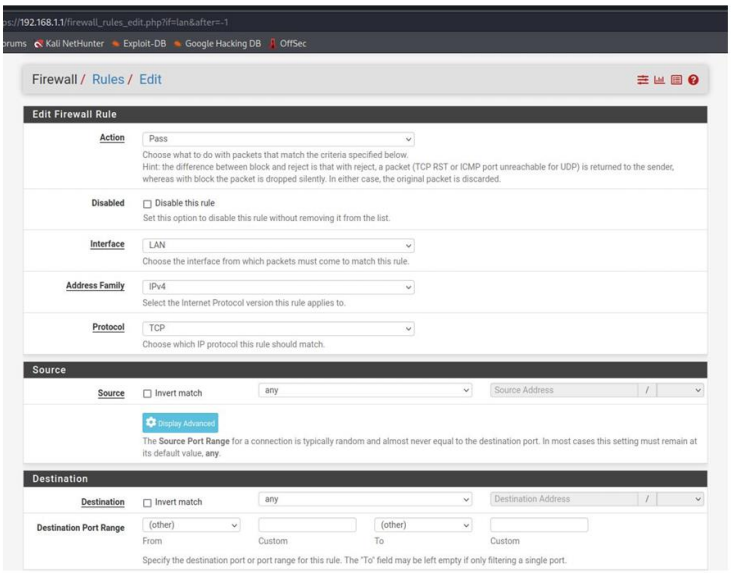
Per la creazione di una regola firewall, andare su **Firewall** > **Rules**. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su **Add** (come vedete ci sono 2 Add, il primo crea la regola in cima al policy set, la seconda in basso)




Cliccando su Add, possiamo aggiungere:

Informazioni generiche:

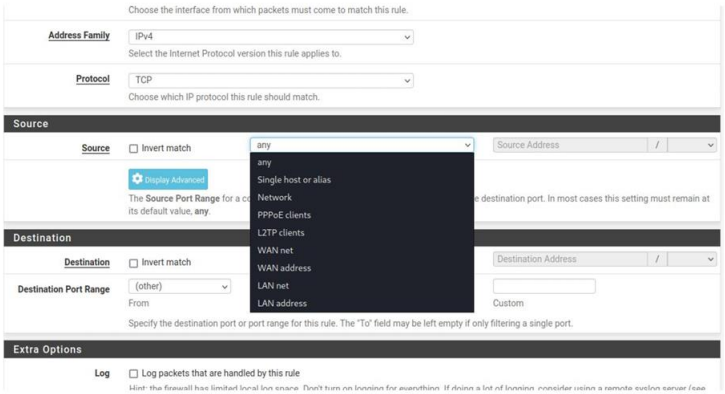
- **Action**: in questa sezione si può scegliere come gestire il traffico analizzato
- **Interface**: l'interfaccia da dove arrivano i pacchetti (es. LAN)
- **Address family**: IPv4 oppure IPv6, si sceglie la versione di protocolli IP ai quali applicare la policy
- **Protocol**: si sceglie il protocollo (es., TCP, UDP, ICMP)




Cliccando su Add, possiamo aggiungere:

Informazioni sulla sorgente:

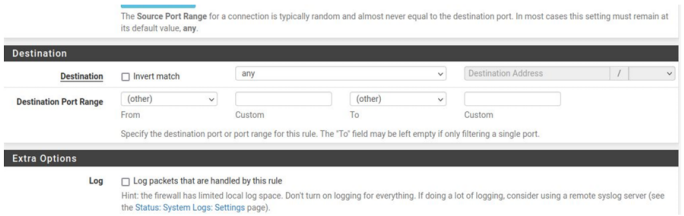
- **Source**: in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera.
  Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.



Cliccando su Add, possiamo aggiungere:

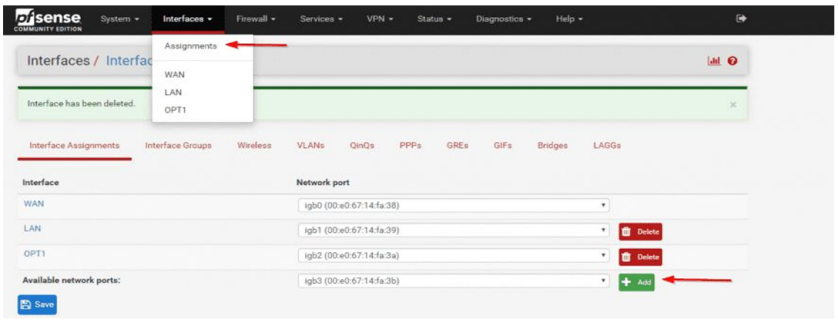
Informazioni sulla destinazione:

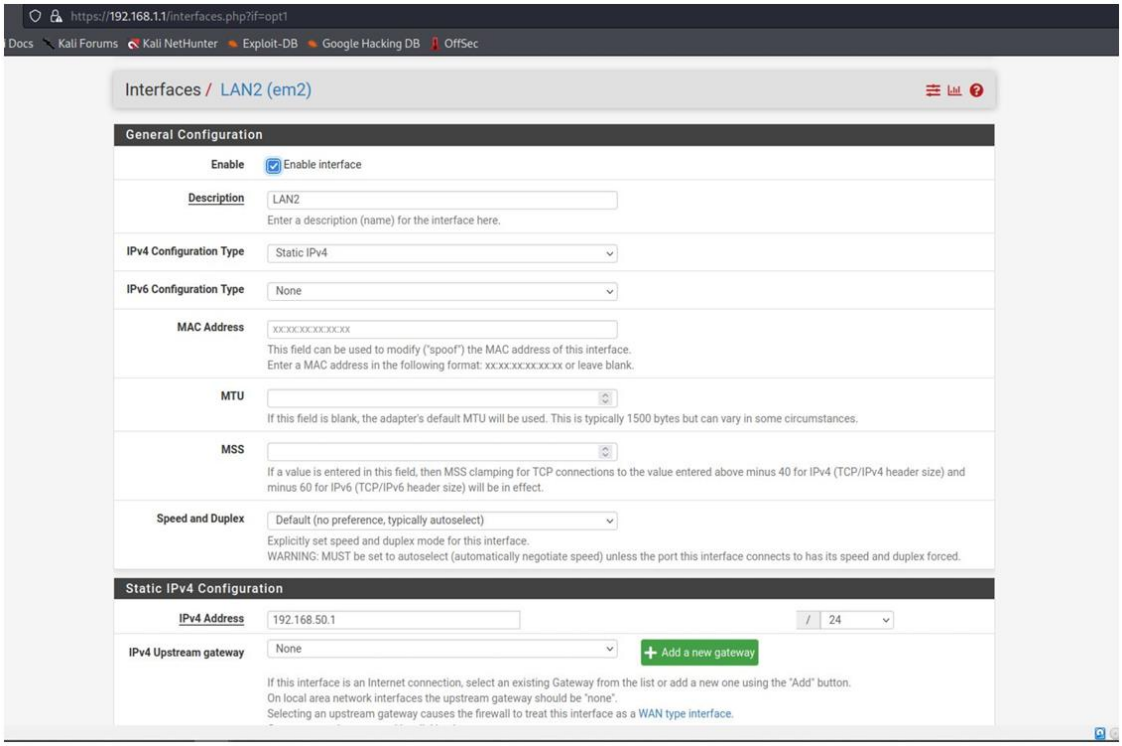
- **Destination**: in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.
- **Destination port range:** in questa sezione si specificano le porte destinazione. Si possono specificare: singole porte, intervalli, aliases (oggetti di porte custom)




Sulla base di quanto visto, creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). 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.

Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.






## Traccia esercizio facoltativo

- Ispezionare i log del Firewall
  https://docs.netgate.com/pfsense/en/latest/monitoring/logs/firewall.html
- Fare pratica con la procedura di troubleshooting delle regole firewall
  https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html

# Requisiti

## Premessa: cos'è pfSense

pfSense è un sistema operativo basato su FreeBSD progettato per essere utilizzato come firewall e router. È una soluzione open source e offre una vasta gamma di funzionalità per la gestione della rete. Ecco alcune delle sue caratteristiche principali:

1. **Firewall e Router**: pfSense è principalmente usato per proteggere le reti gestendo il traffico in entrata e in uscita, configurando regole di filtraggio avanzate.
2. **Interfaccia web**: La configurazione e la gestione di pfSense avviene tramite un'interfaccia web intuitiva, rendendolo accessibile anche a utenti non esperti.
3. **VPN (Virtual Private Network)**: pfSense supporta diversi tipi di VPN come IPsec, OpenVPN e PPTP, consentendo la connessione sicura tra reti remote.
4. **Traffic Shaping**: Offre funzionalità di "traffic shaping", che permette di prioritizzare determinati tipi di traffico, ad esempio limitando la banda per il download e assicurando che le applicazioni critiche abbiano una connettività ottimale.
5. **Monitoraggio e reportistica**: pfSense fornisce strumenti di monitoraggio del traffico e può generare report dettagliati per analizzare l'attività della rete.
6. **Gestione degli accessi**: Può essere configurato per gestire l'accesso a internet per gli utenti della rete, con funzioni come il blocco di siti specifici o la limitazione della larghezza di banda.
7. **Ridondanza e Failover**: Supporta funzionalità avanzate come la ridondanza e il failover per garantire l'affidabilità e la continuità del servizio.

In sintesi, pfSense è un sistema versatile, utilizzato in contesti aziendali e domestici per la gestione di firewall e rete con elevate prestazioni e flessibilità.

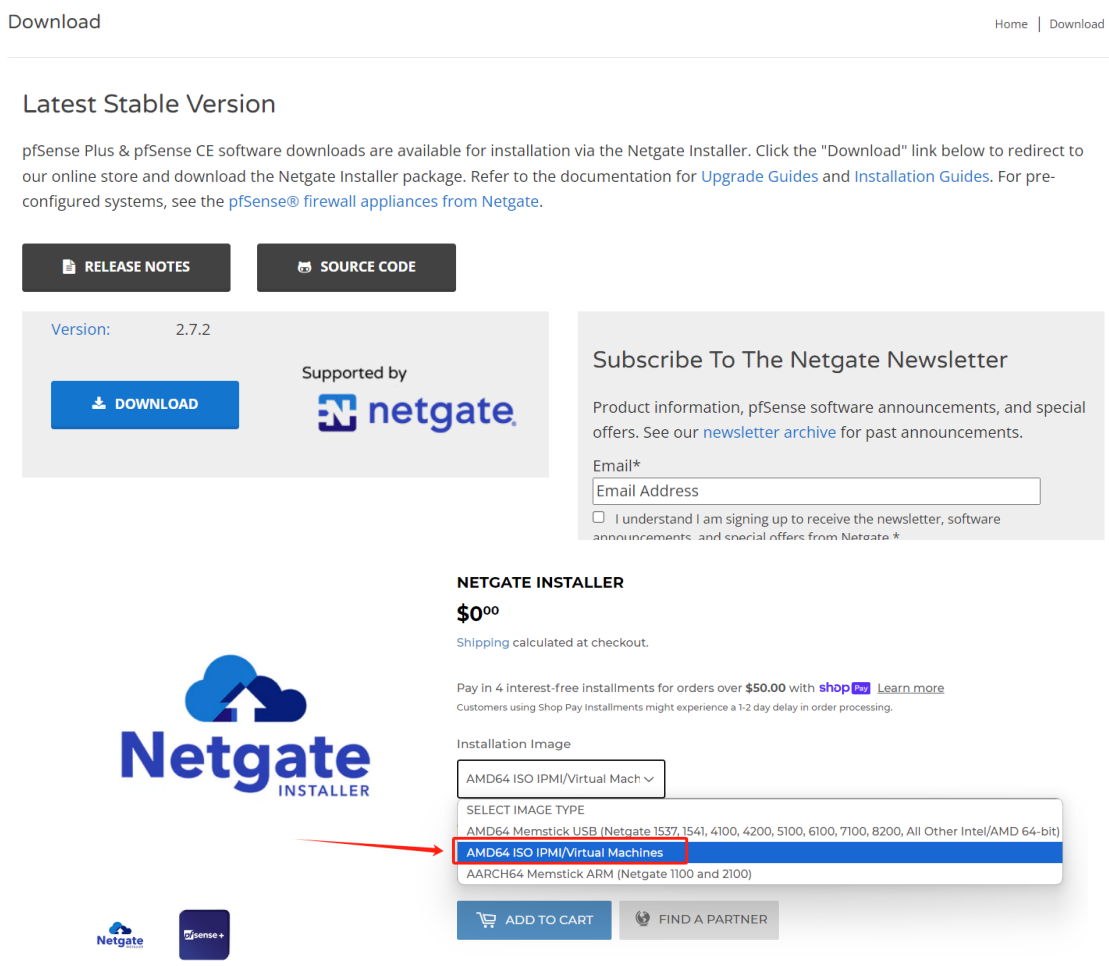
*La licenza FreeBSD consente di modificare e utilizzare il codice in progetti chiusi o commerciali, richiedendo solo di dare credito agli autori originali.*

Ai fini del corso, pfSense sarà utilizzato e configurato nel laboratorio virtuale, quindi installato come sistema operativo, nel presente report, con VirtualBox.

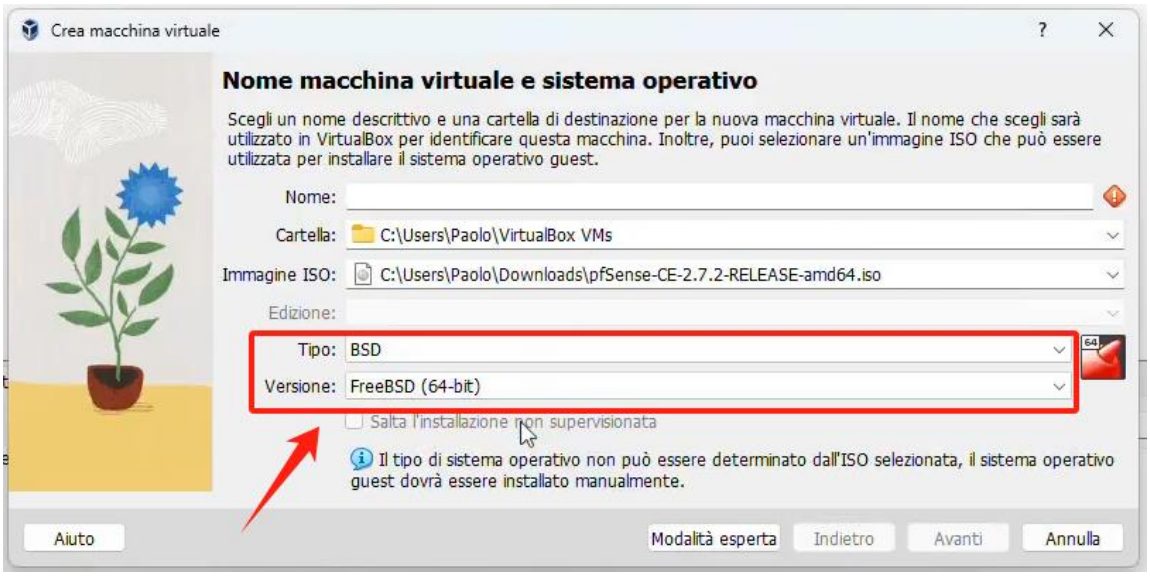
Per una migliore comprensione, il ruolo di pfSense in questo laboratorio virtuale può essere paragonato, per analogia, a quello di un modem/router in una rete domestica, svolgendo funzioni di firewall e gestione del traffico tra le macchine collegate alla rete.

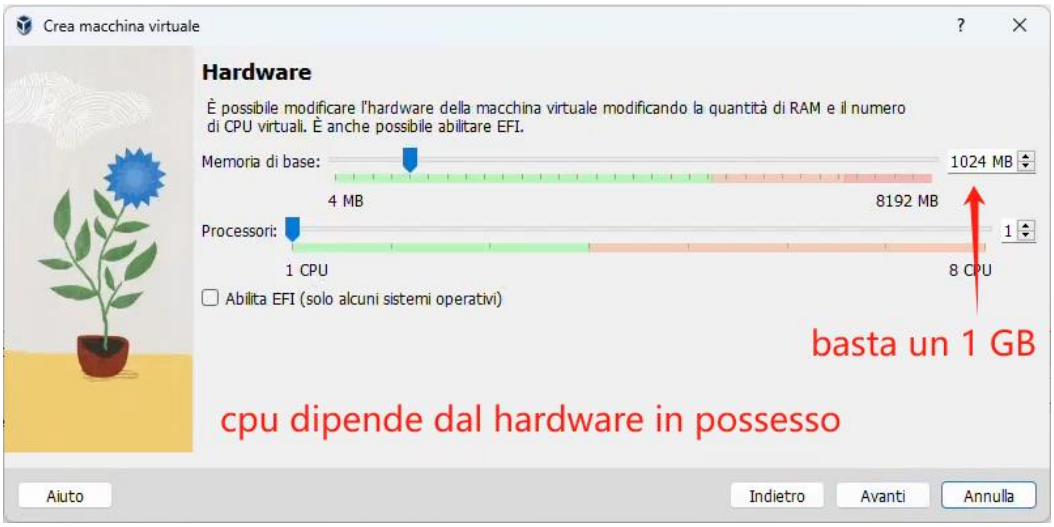
## Installazione di pfSense

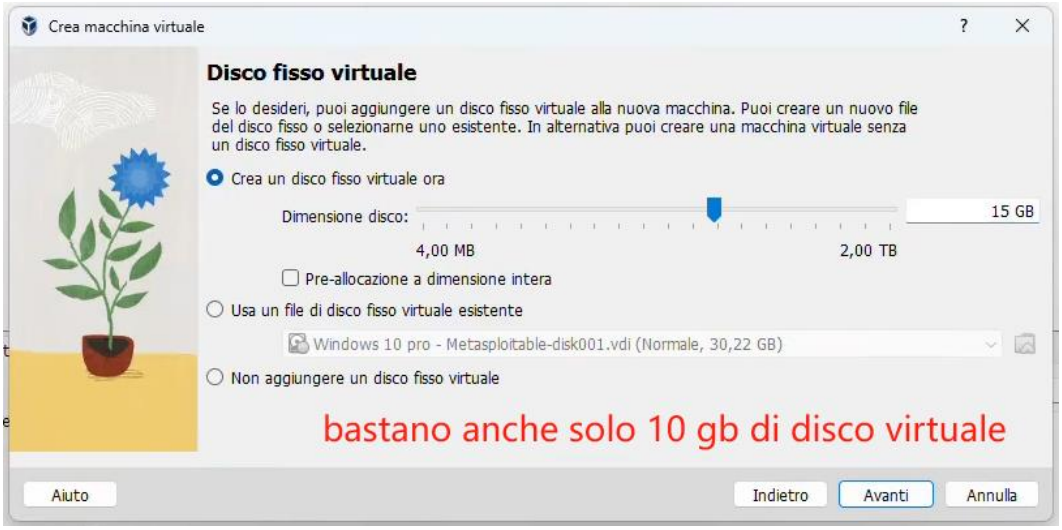
Scaricare l'immagine .ISO scegliendo la versione per Virtual Machine dal sito ufficiale https://www.pfsense.org/download/ e seguire le istruzioni per il download.



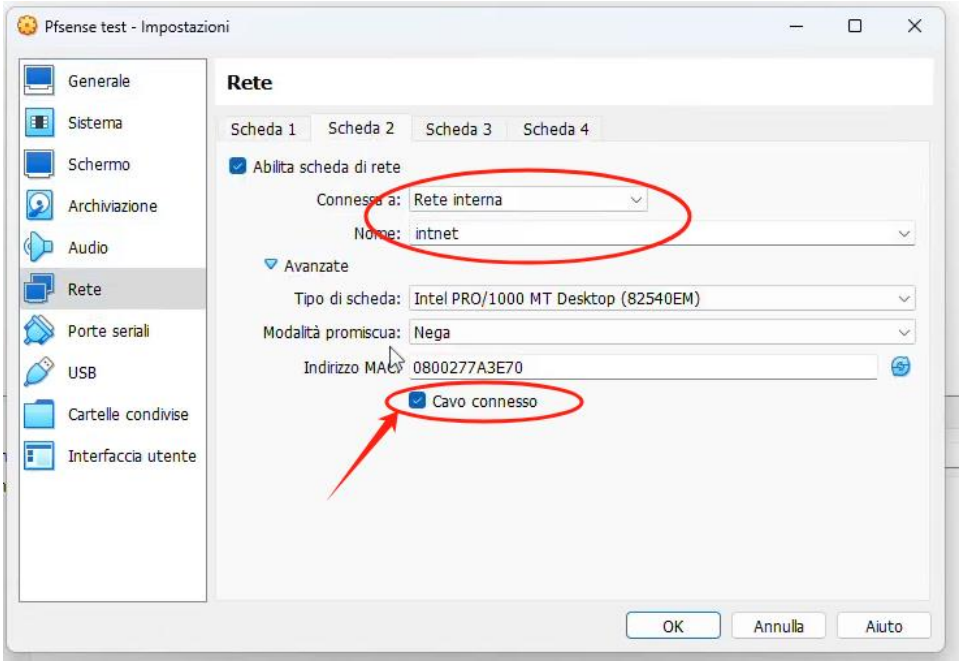

Seguire le istruzioni del report M1\W1\D3 su come installare un OS con VirtualBox con la seguente configurazione.



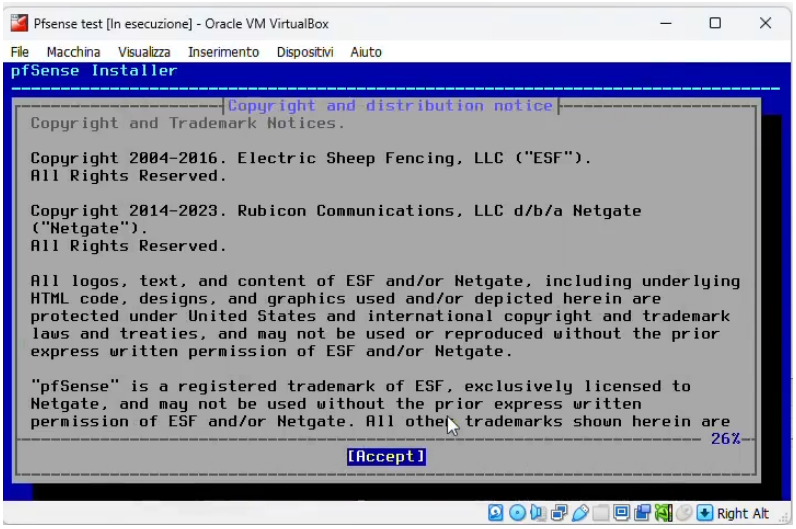


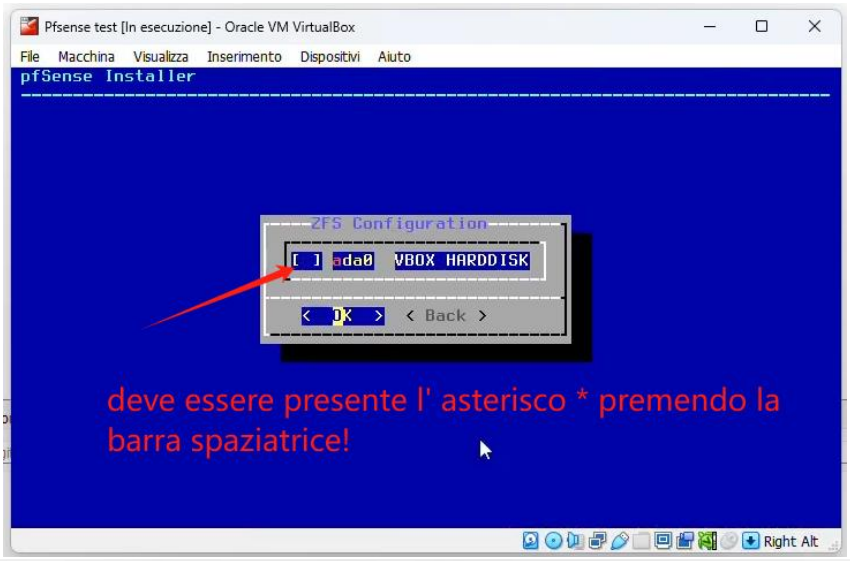

Prima di avviare la VM, molto importante è la configurazione delle schede di rete 1 e 2, abilitate, rispettivamente in **NAT** e **Rete Interna**, entrambi con **Cavo connesso**.

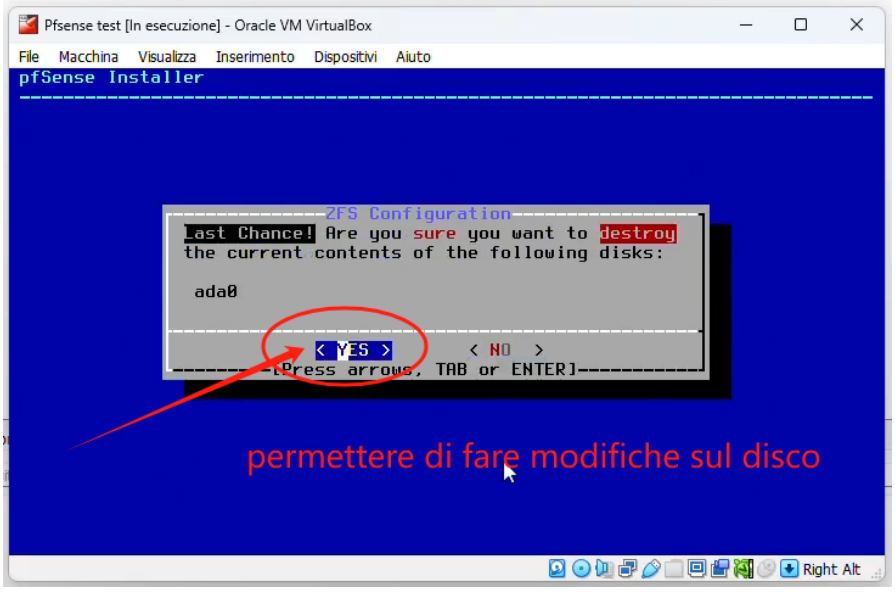


Avviare la macchina virtuale di pfSense e seguire le istruzioni intuitive per l'installazione, procedendo sempre con il tasto Invio.

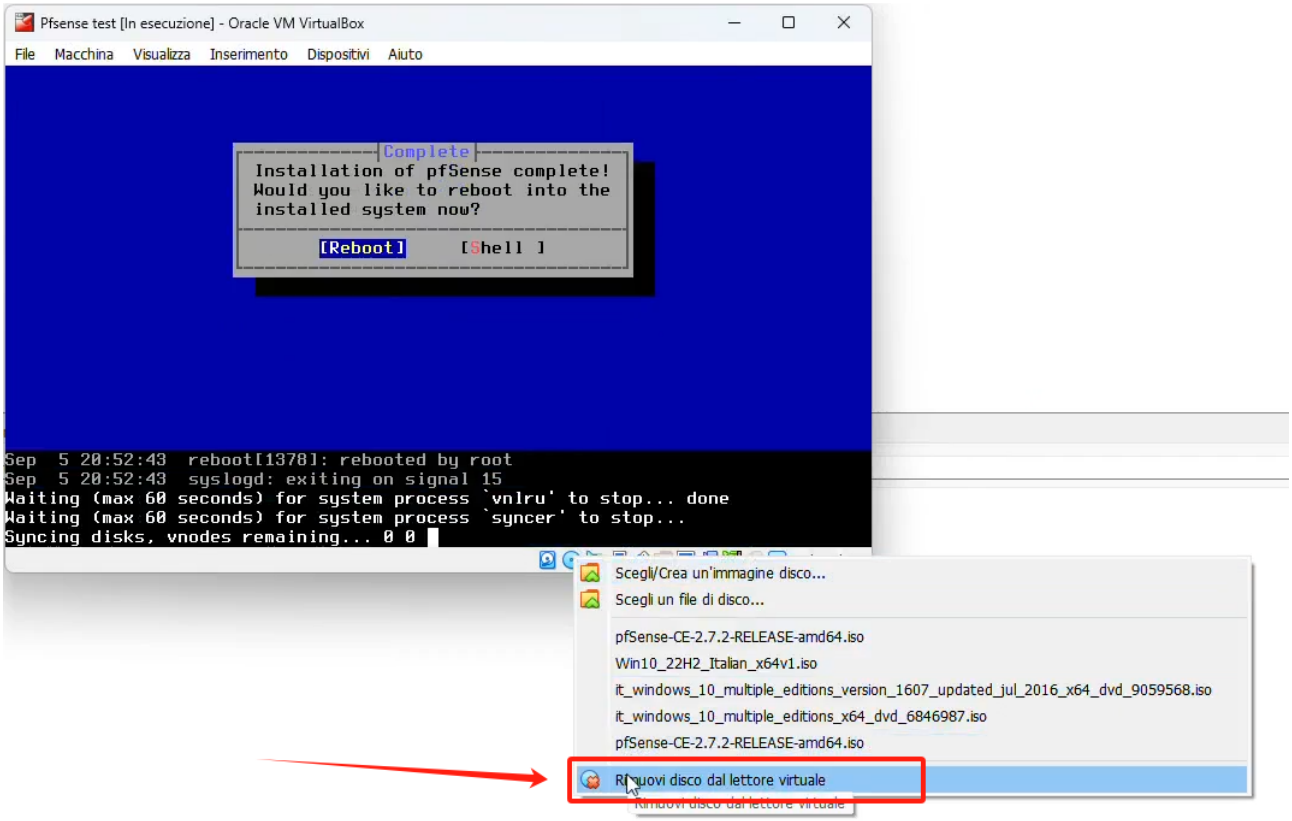



**Attenzione all'unico passaggio da prestare la massima attenzione per selezionare il disco e dare il permesso alla modifica dello stesso.**



Alla fine del procedimento, riavviare la VM e durante il processo di riavvio, rimuovere il disco virtuale dalla VM per evitare che la macchina avvii il sistema operativo dal disco di installazione (l'ISO scaricata), invece di avviarlo dal disco virtuale.



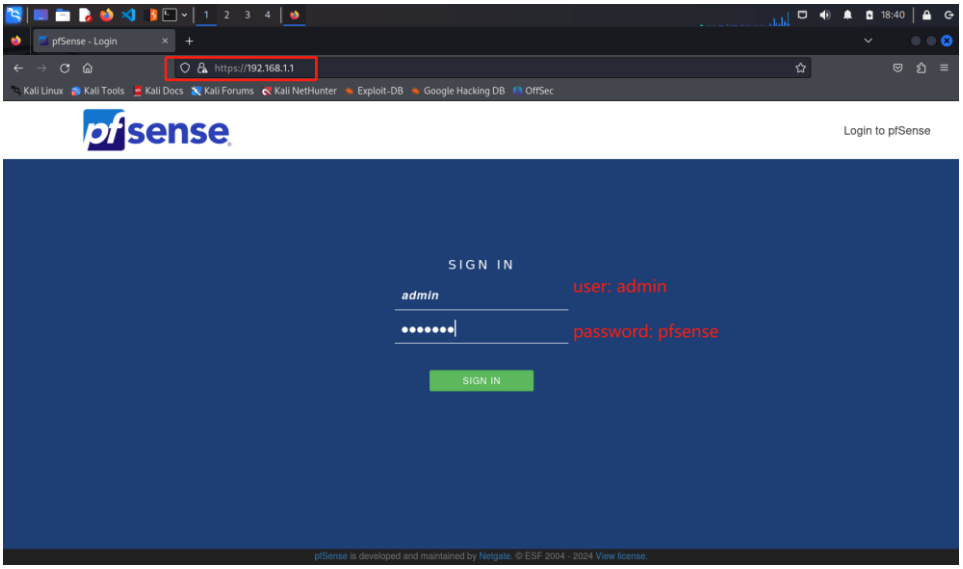

Una volta completato l'operazione, tenere acceso pfSense.

## Collegamento tra pfSense, Kali Linux ed eventuali altre VM

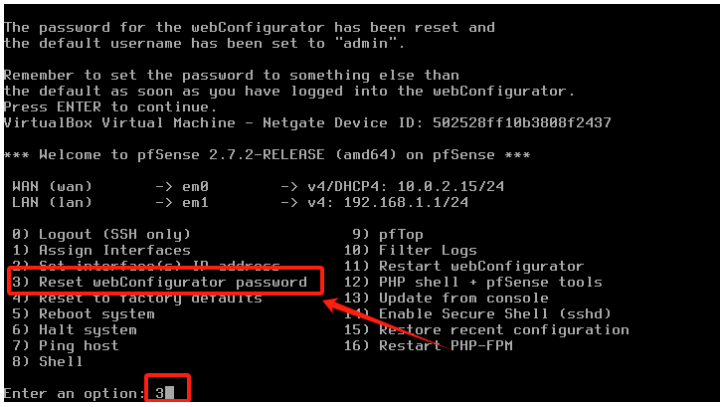
Kali Linux deve avere la scheda di rete in rete interna con cavo connesso e deve essere in DHCP. Verificare con il comando **ip a** su terminale Kali che sia connessa correttamente alla rete di pfSense.


In questo caso 192.168.**1**.100 indica perfettamente che si è connessa correttamente, pertanto per entrare nella pagina di configurazione, aprire il browser e digitare l'indirizzo di gateway, in questo caso **192.168.1.1**, bypassare eventuali avvisi di sicurezza del browser.

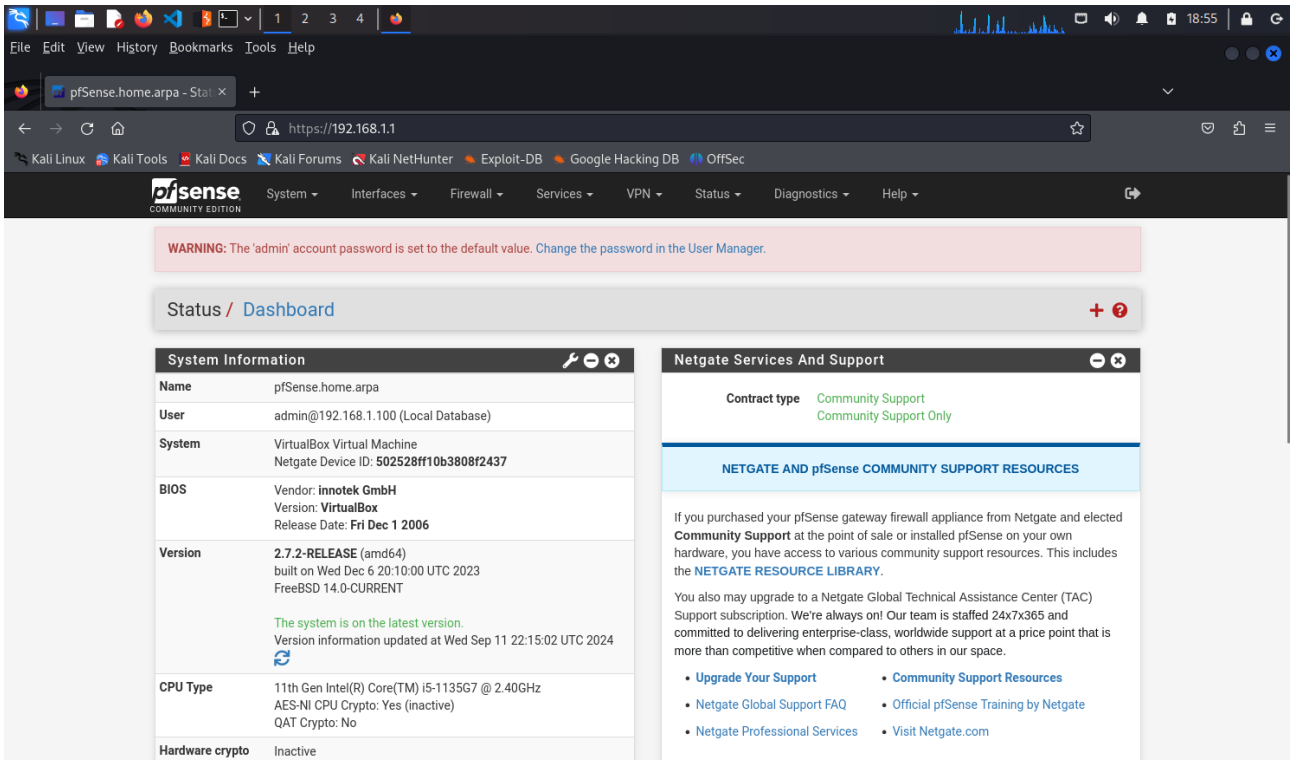
Credenziali di default: user **admin** password **pfsense**




Per ripristinare la password di default usare le opzioni su pfSense. In questo caso col numero 3.

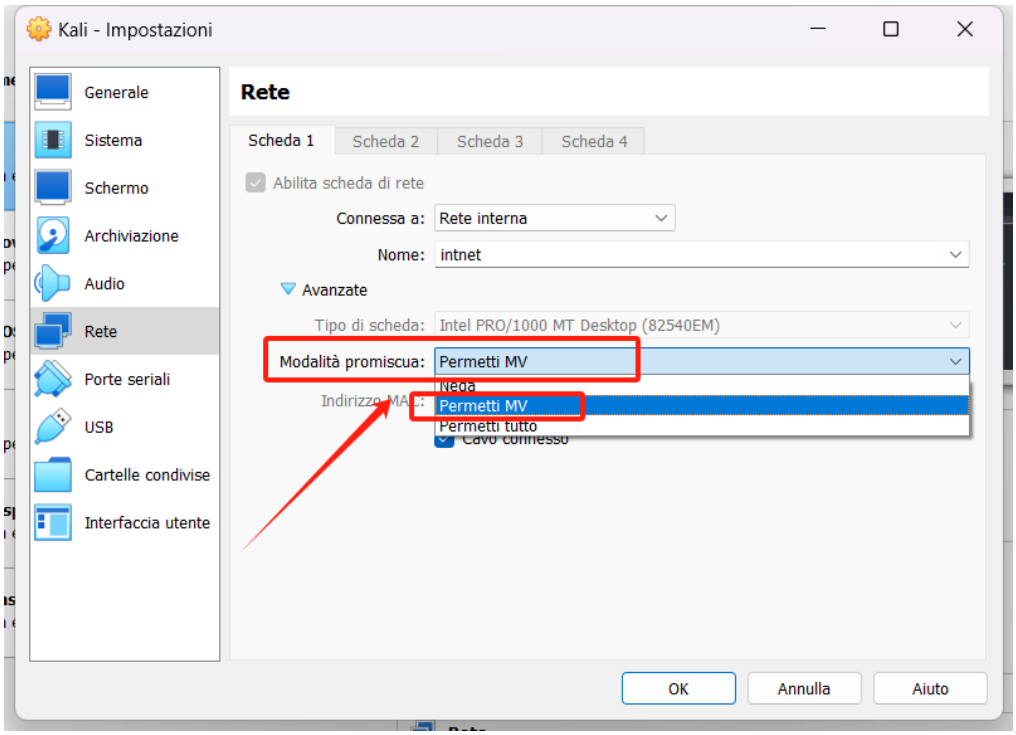


Seguire passo passo la configurazione intuitiva di benvenuto.




Da questa schermata, la Dashboard si possono effettuare tutte le configurazioni e impostazioni desiderate.

Per mantenere attivo la connessione a internet, rete esterna, sulla macchina Kali Linux attivare la modalità promiscua. Questa modalità consente alla VM di vedere tutto il traffico sulla rete a cui è connessa, permettendo a pfSense di funzionare correttamente come router. **Attivarla anche su pfSense.**

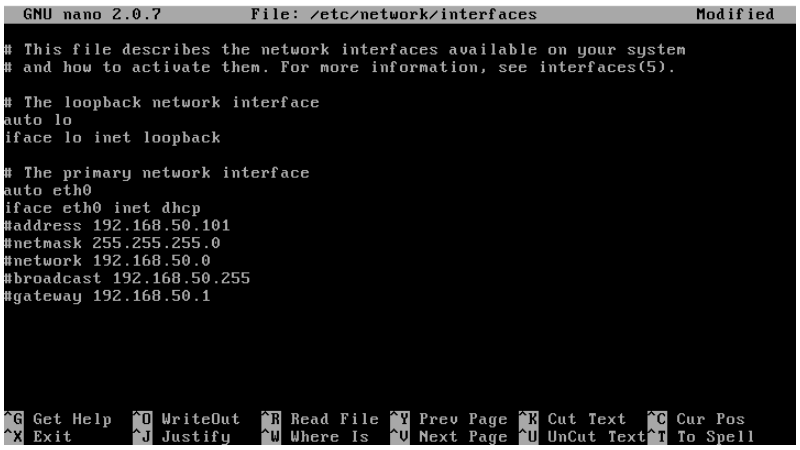



La motivazione è che pfSense, nella rete del laboratorio virtuale, ha il ruolo di Server DHCP e pertanto le macchine virtuali connesse non riescono a vedere tutto il traffico di rete per configurazioni di sicurezza di default.

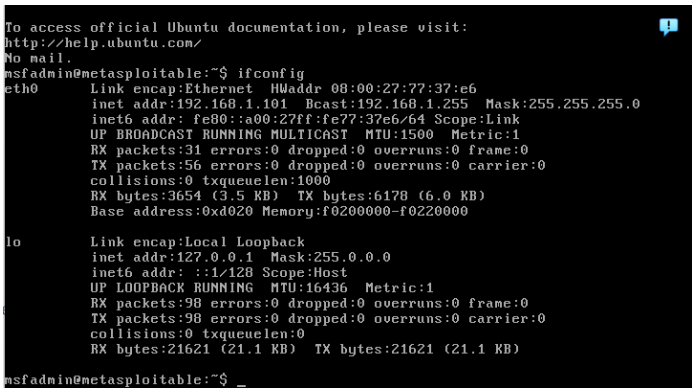
# Svolgimento della traccia principale

## Impostare le VM in DHCP

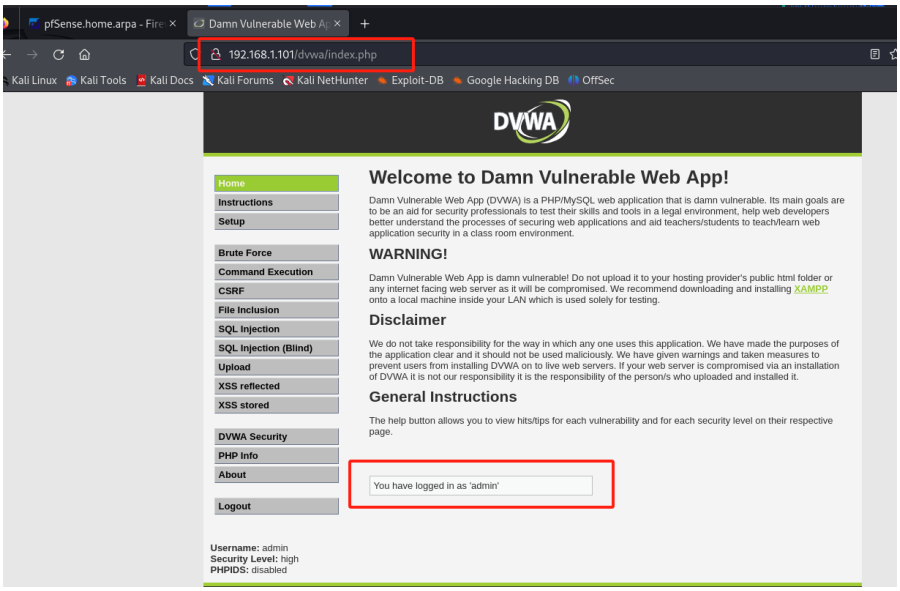
Dato che pfSense fa da server DHCP, ha il ruolo di assegnare gli indirizzi IP, pertanto è essenziale che le macchine del laboratorio virtuale siano in DHCP e rete interna. Seguire il report del M1\W1\D5 per impostare Metasploitable2 in DHCP.




## Verifica connessione con DVWA (Metasploitable2)

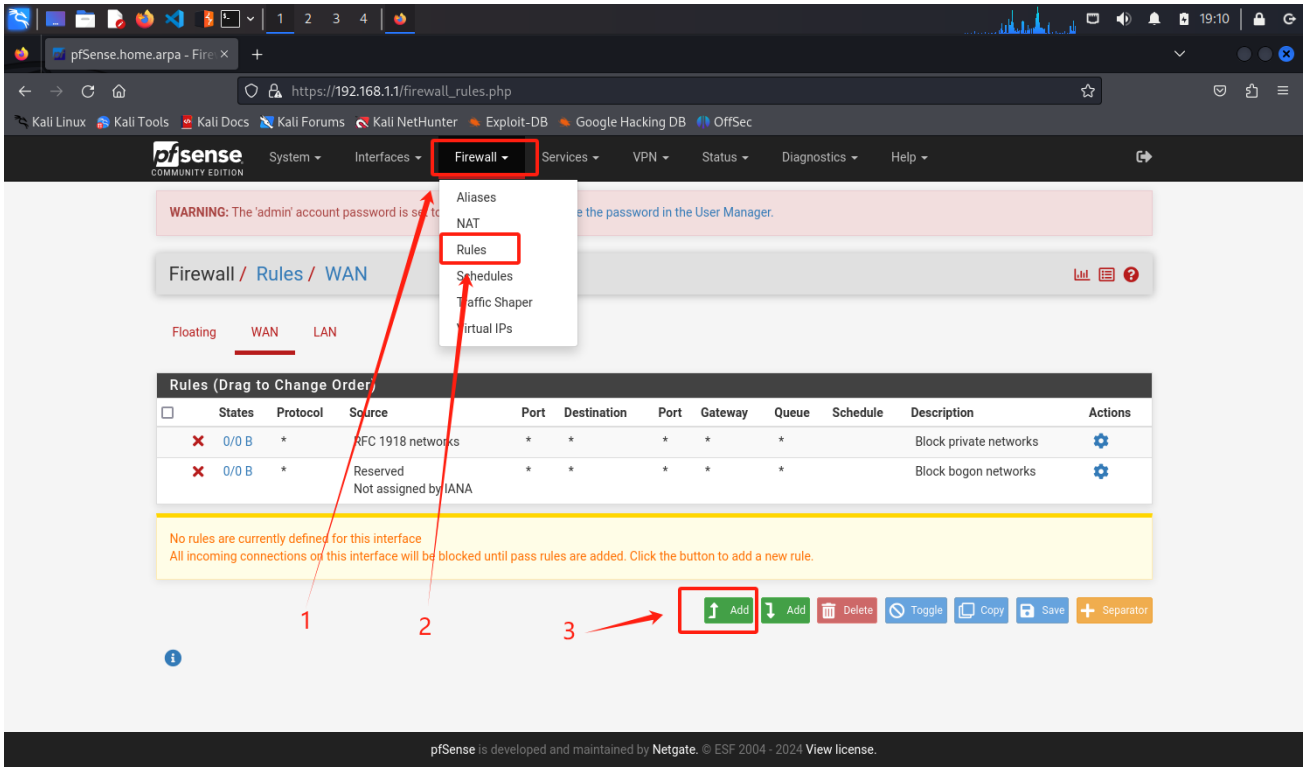


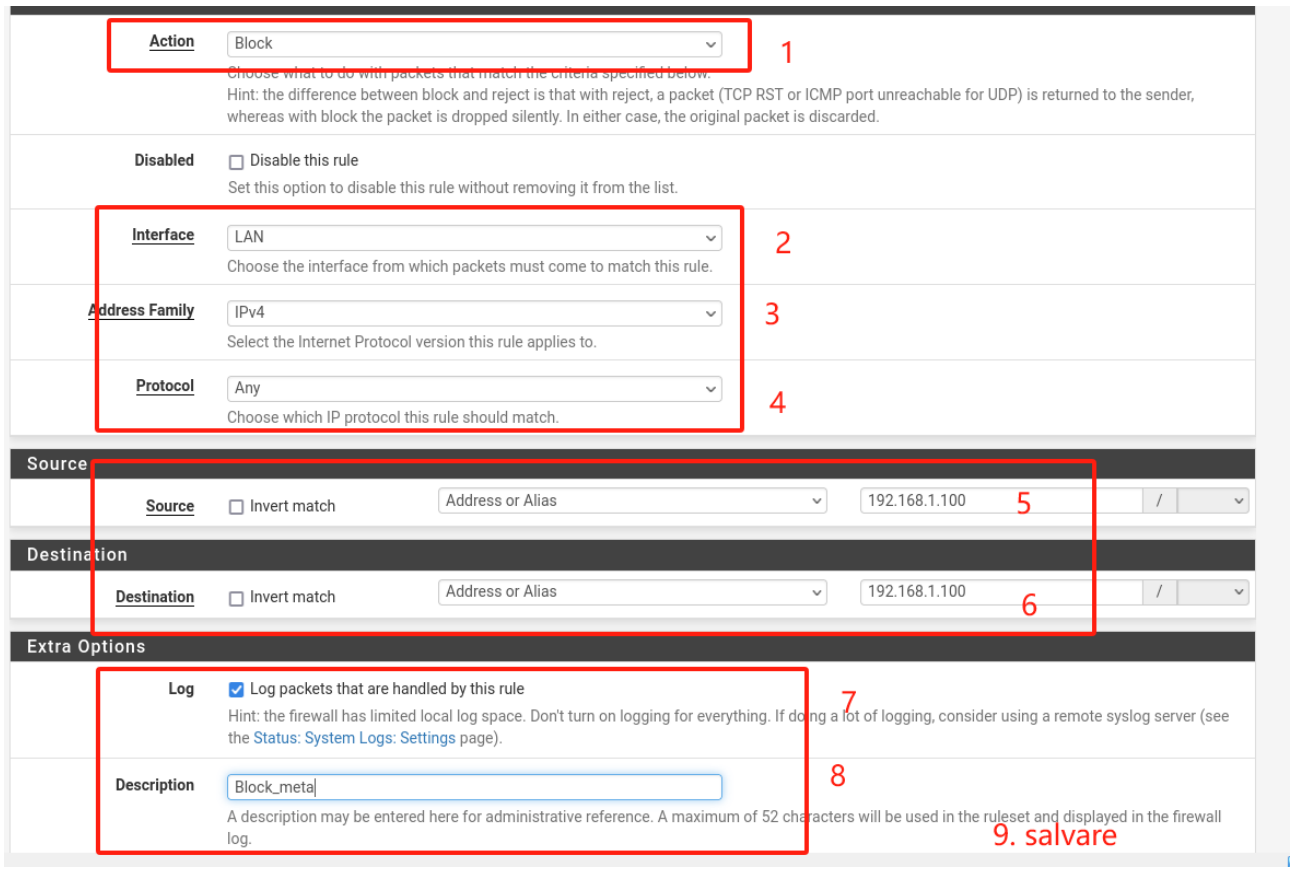

Con il comando su Metasploitable2 **ifconfig** si ottiene l'indirizzo IP del server DVWA, in questo caso **192.168.1.101**. Pertanto tramite il browser si verifica subito la connessione al link http://192.168.1.101/dvwa/login.php con le credenziali **admin** e **password**.



## Creazione regola su pfSense per bloccare l'accesso a DVWA

Tornare all'interfaccia di configurazione di pfSense da browser, quindi **192.168.1.1** con le credenziali note e aggiungere una nuova regola firewall come da immagine sottostante: Firewall > Rules > Add Aggiungere una nuova regola, in questo caso è indifferente se in cima o in basso per l'ordine di priorità.



1. Azione di blocco
2. Interfaccia Lan
3. Ipv4
4. Tutti i protocolli
5. L'indirizzo di origine da bloccare
6. L'indirizzo di destinazione da bloccare
7. Opzionale: i log
8. Dare una descrizione alla regola
9. Salvare la configurazione

Dopo aver configurato, nella schermata precedente, applicare i cambiamenti. p.s. in questo tentativo, si sono riavviati le macchine e pertanto il server DHCP pfSense ha assegnato 192.168.1.100 a Meta e 192.168.1.101 a Kali.

## La regola di blocco non funziona nella stessa rete

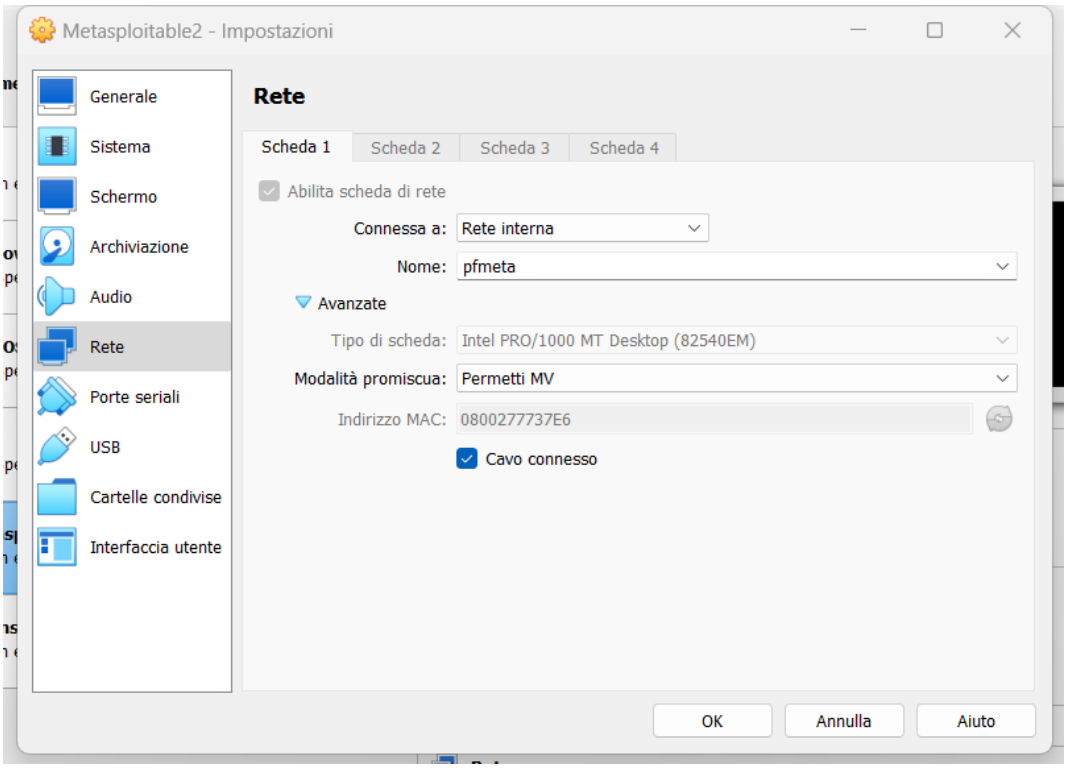
Dai test effettuati, si conclude che il blocco impostato correttamente su pfSense non funziona, né può funzionare, perché pfSense agisce come firewall tra Kali e Meta. Tuttavia, in questo caso, poiché Kali e Meta si trovano nella stessa rete interna, il loro traffico non passa attraverso il router/modem virtuale pfSense, e di conseguenza non viene filtrato da quest'ultimo.

Quindi testare il blocco correttamente e obbligare il traffico tra Meta e Kali attraverso pfSense, si può configurare con due reti diverse: Kali nel gateway 192.168.1.1 & Meta nel gateway 192.168.50.1

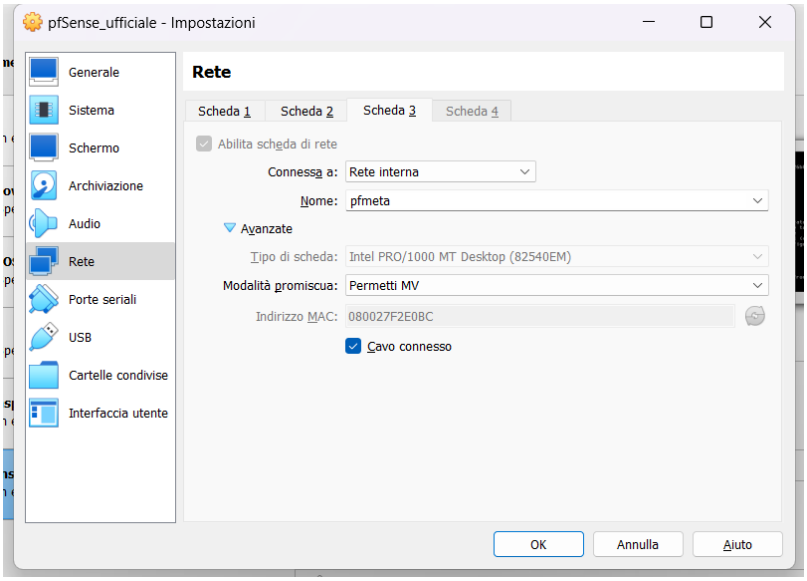
## Configurazione in reti diverse

Configurare su Virtual Box, un'altra rete interna.

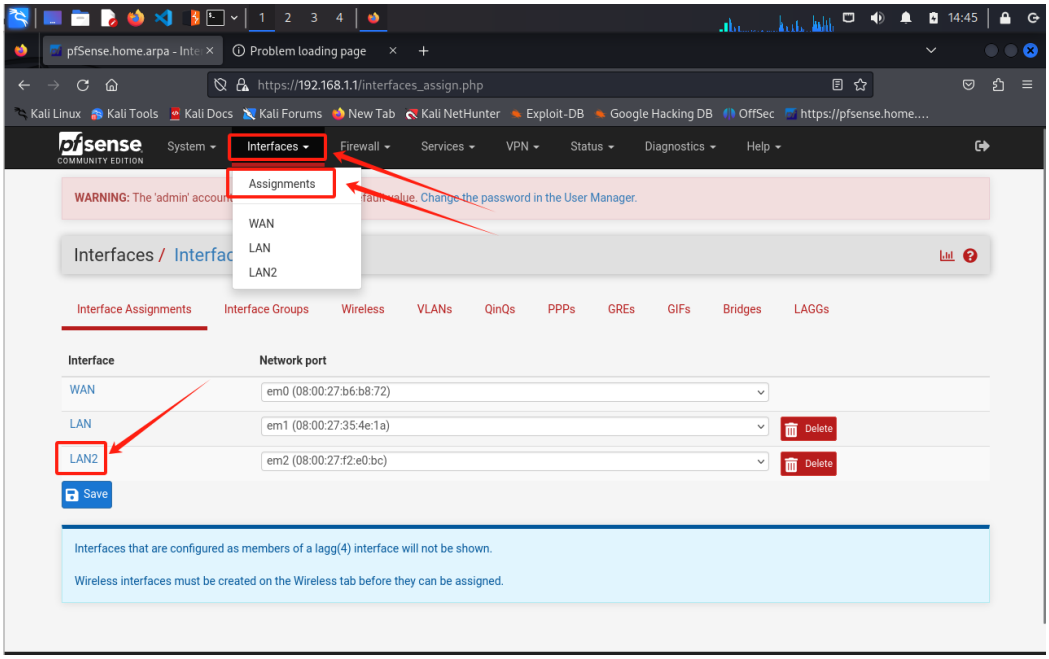
Metasploitable2 cambiare con un nome a piacere la rete interna, in questo caso **pfmeta**

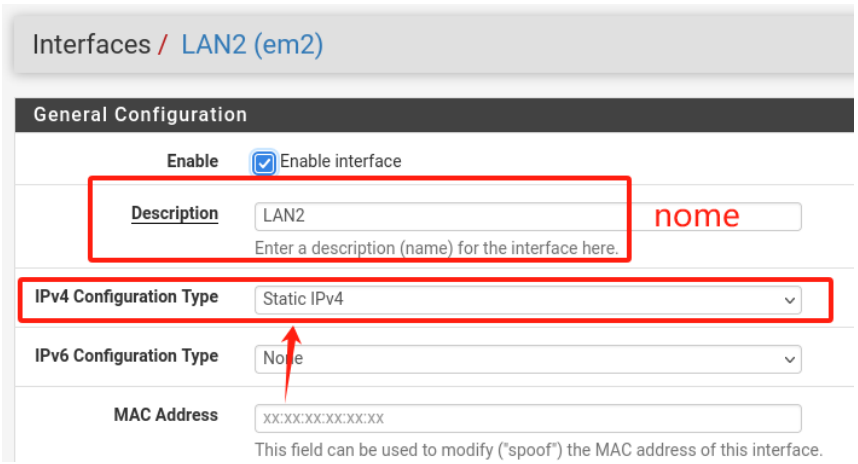


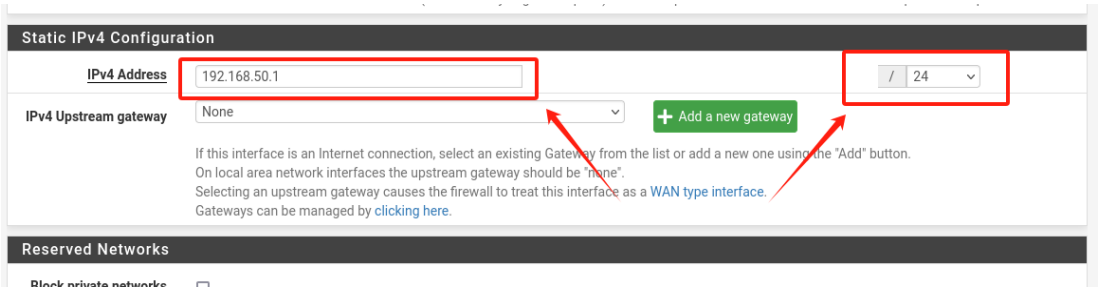
Invece su pfSense aggiungere una nuova scheda di rete chiamandola con lo stesso nome di Meta.




Da Kali andare nella pagina di configurazione di pfSense andare su **Interfaces > Assigments** e cliccare su **opt1** (quest'ultimo si potrà modificarlo con un nome personalizzato, LAN2 in questo caso).

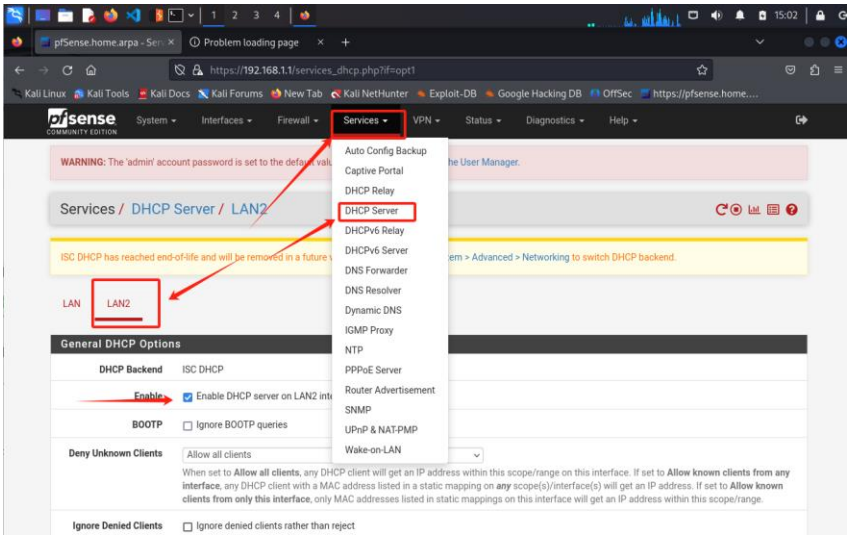


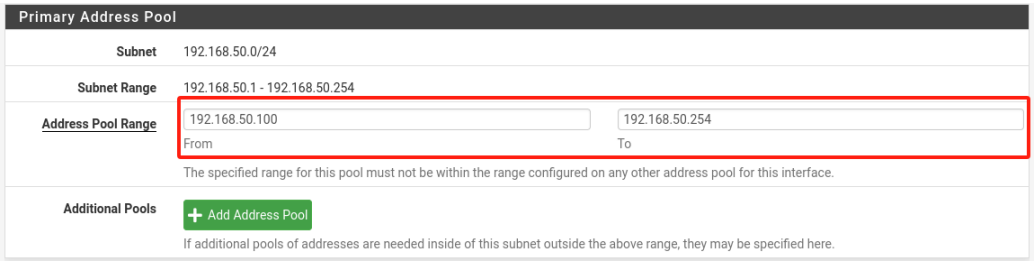






Inserire l'indirizzo di gateway, in questo caso il 192.168.50.1 in subnet 24 e salvare.

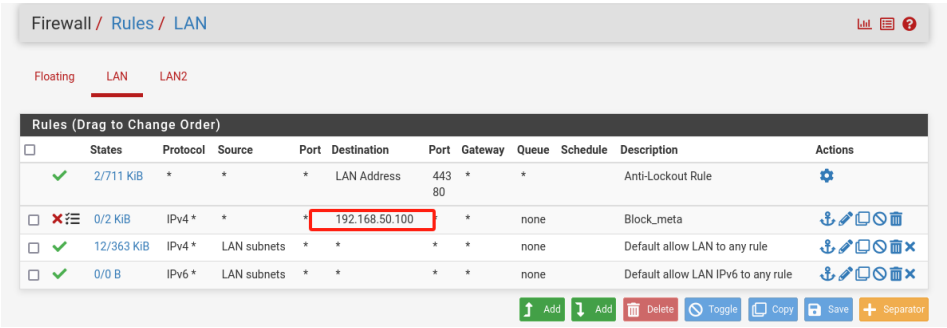
Attivare il servizio del DHCP Server in **Services > DHCP Server**




Impostare il range di indirizzi IP che il server DHCP potrà assegnare e salvare.

Con questa configurazione Metasploitable2, una volta riavviato, si connetterà alla rete 192.168.50.1 e lanciare il comando **ip a** o **ifconfig** per ottenere l'indirizzo IP.

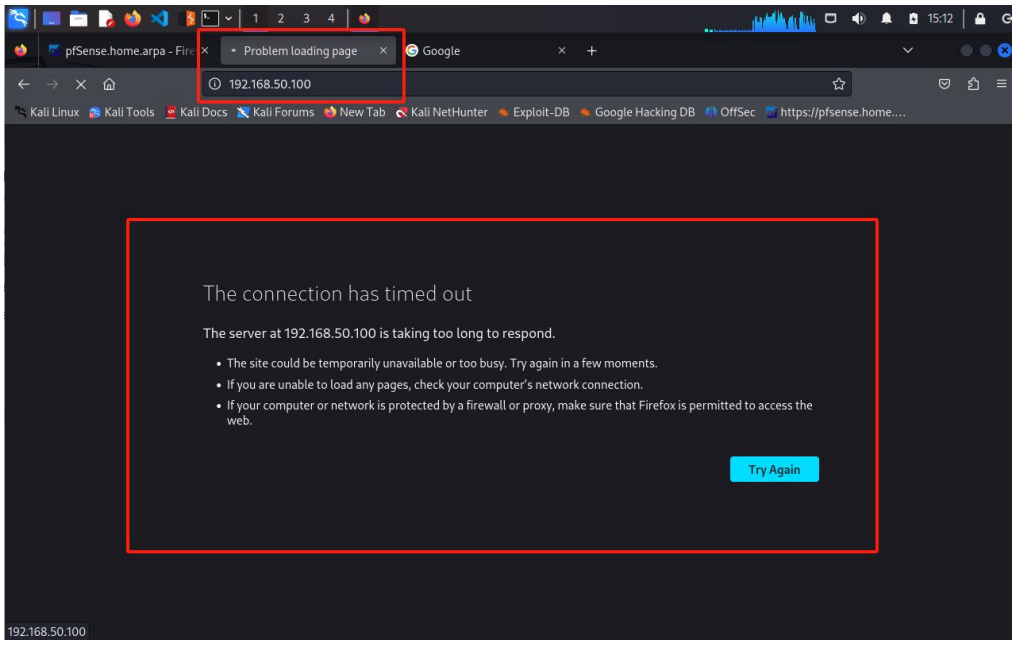



Su **Firewall > Rules** LAN impostare nuovamente la regola bloccando l'indirizzo IP di Metasploitable2.

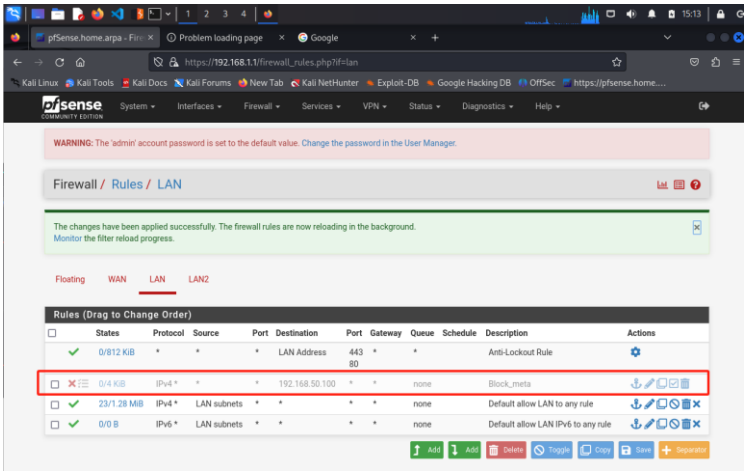
In questo caso è 192.168.50.100 per Metasploitable2 e 192.168.1.100 per Kali Linux.

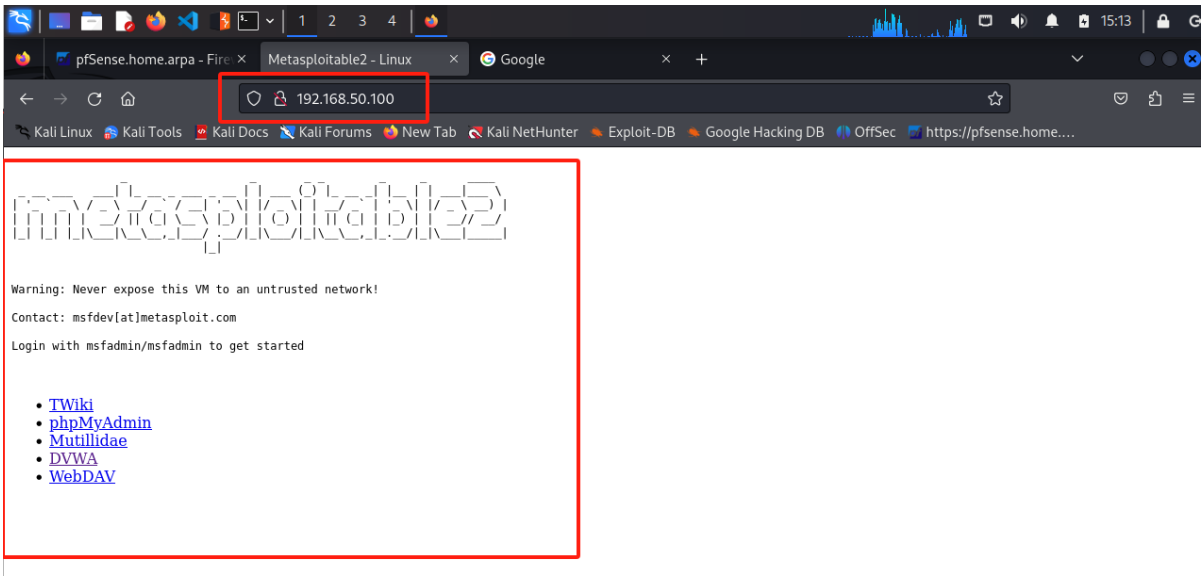
## Test regola di firewall

La regola di firewall su LAN funziona correttamente.



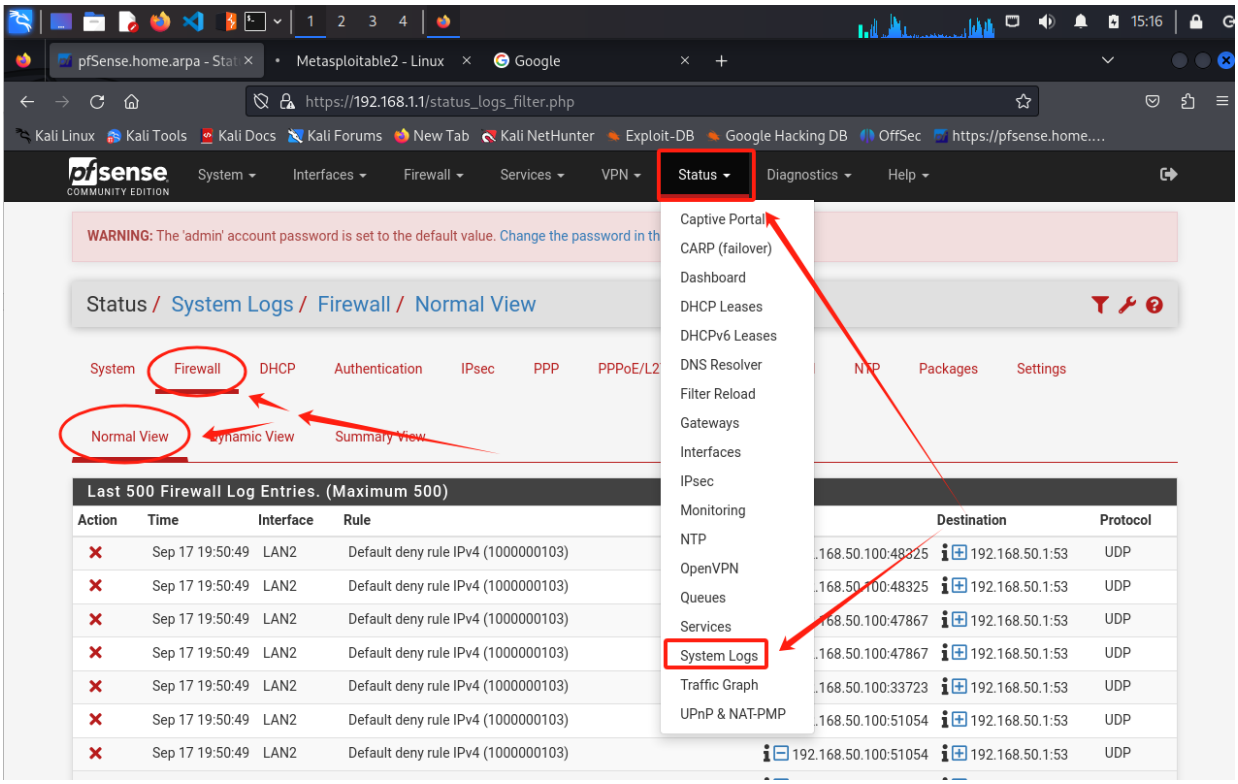

Se si disattiva la regola, il server DVWA di Meta ricomincia a funzionare.



# Svolgimento esercizio facoltativo

## Analisi dei log




Recandosi nella sezione come da figura, si notano tutti i tentativi di connessione all'indirizzo IP bloccato da pfSense 192.168.50.100 in qualsiasi protocollo (era stato impostato ANY).

## Troubleshooting delle regole firewall

Visitare la pagina web https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html ed esplorare le impostazioni di pfSense raggiungibile anche dal dominio https://pfsense.home.arpa/