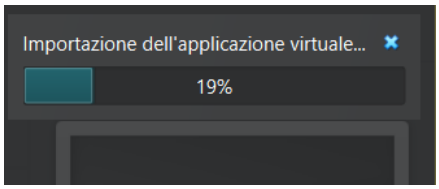
W9D4

INSTALLAZIONE E CONFIGURAZIONE INIZIALE pfSense

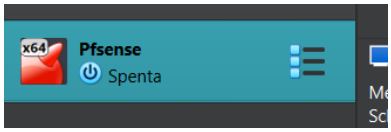
Importazione della VM pfSense

Carico l'immagine OVA in VirtualBox/VMware cliccando due volte sul file

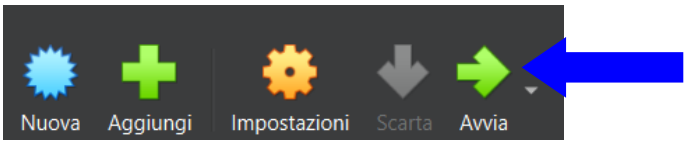
Comparirà questa schermata dopo aver confermato:



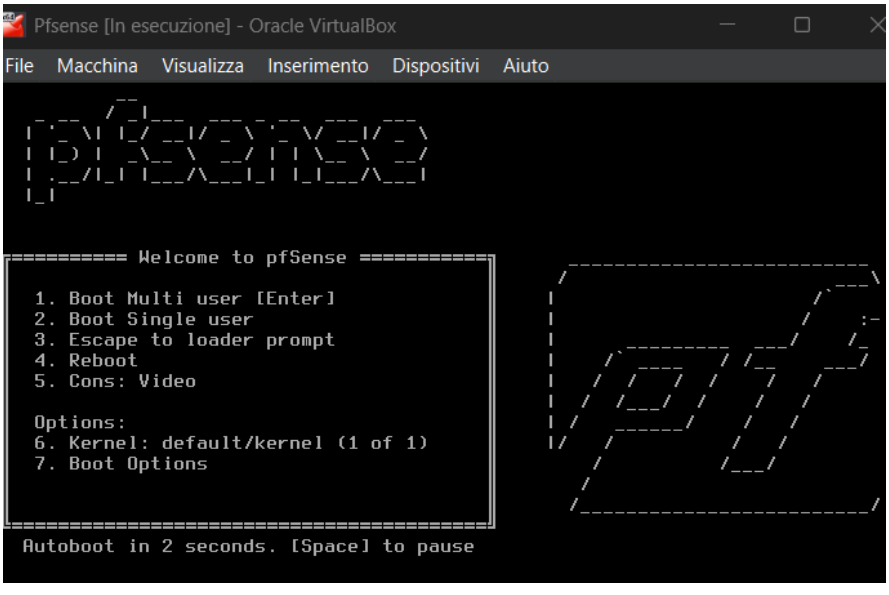
Ora controllo su VirtualBox che l'immagine OVA e stata caricata correttamente



Avvio Pfsense



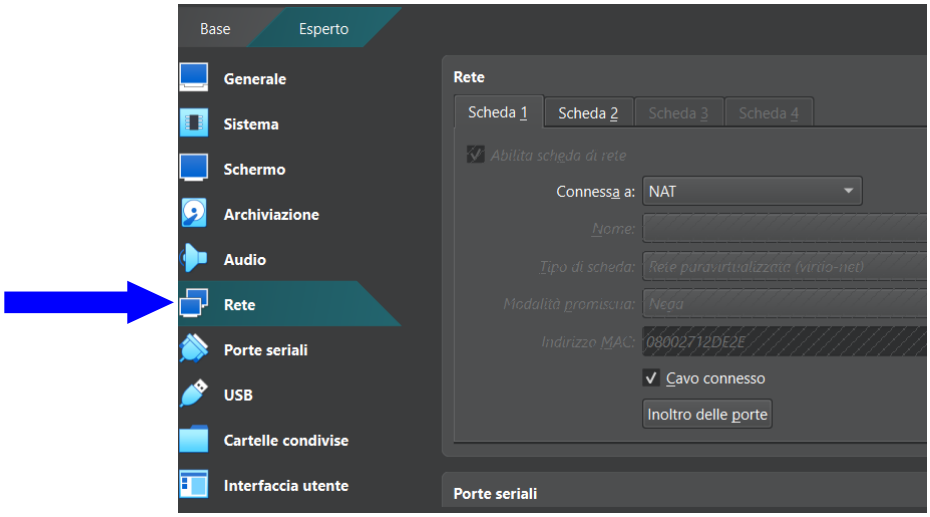
Schermata di apertura pfSense



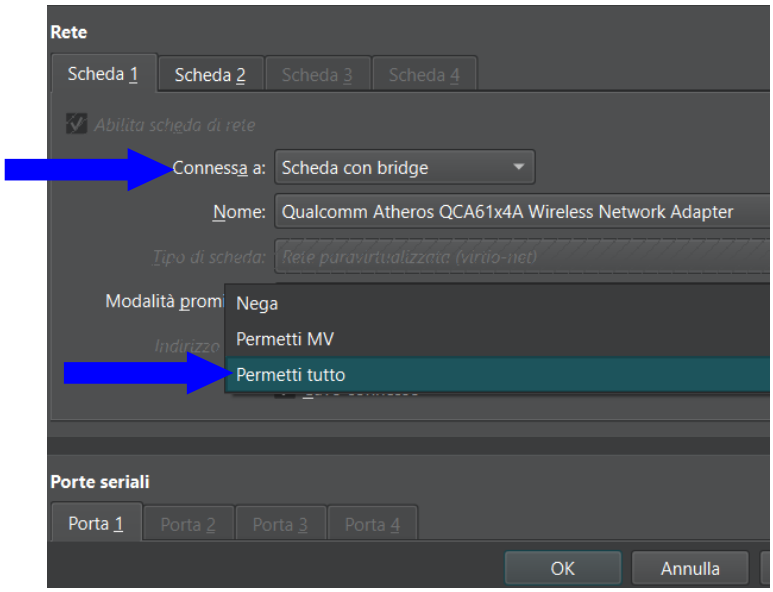
Configuro le schedi di reti

Apro impostazioni è trovo due interfacce preconfigurate

⇒ 1) Interna
⇒ 2) Nat



Procedo con la modifica della rete da Nat a Bridge selezionando nella modalità promisqua Permetti tutti

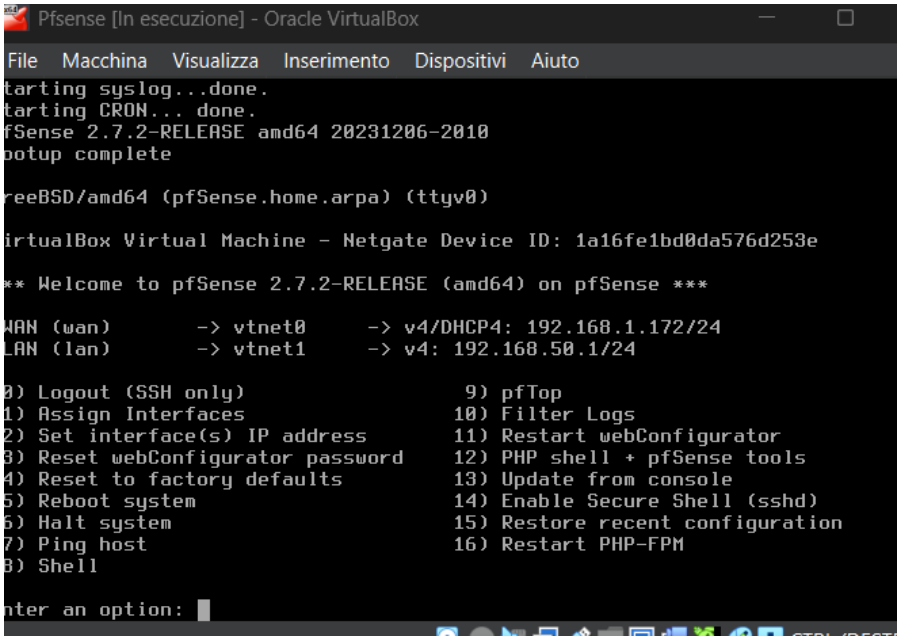


Ho selezionato permetti tutti perche in VirtualBox il firewall non fa parlare nessuno con pfSense

Quindi ora le schede di rete saranno :

⇒ Adapter 1 Briddge si trova direttamente sulla mia rete (prende IP dal mio router)
⇒ Adapter 2 NAT parla con Kali Metasploitable2 e Windows

Salvo e riavvio pfSense scrivendo il numero 5 per il reboot system poi digito Y per il riavvio normale, il riavvio parte con successo e alla fine comparirà questa schermata



WAN vtnet0

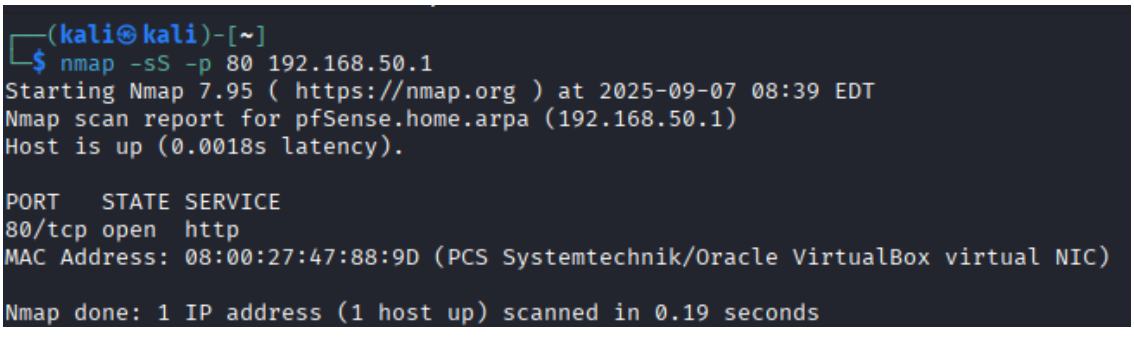
- **IP** 192.168.1.172 (assegnato dinamicamente via DHCP dal router/host).
- **Scopo** Collega pfSense alla ret esterna (in questo caso la mia rete domestica)

LAN vtnet1

- **IP** 192.168.50.1 (assegnato staticamente durante la configurazione).
- **Scopo**: Rete interna isolata, a cui sono connesse le VM client (Kali, Metasploitable2 e Windows)
- **Subnet Mask**: /24 (equivalente a 255.255.255.0), che definisce la rete 192.168.50.0/24

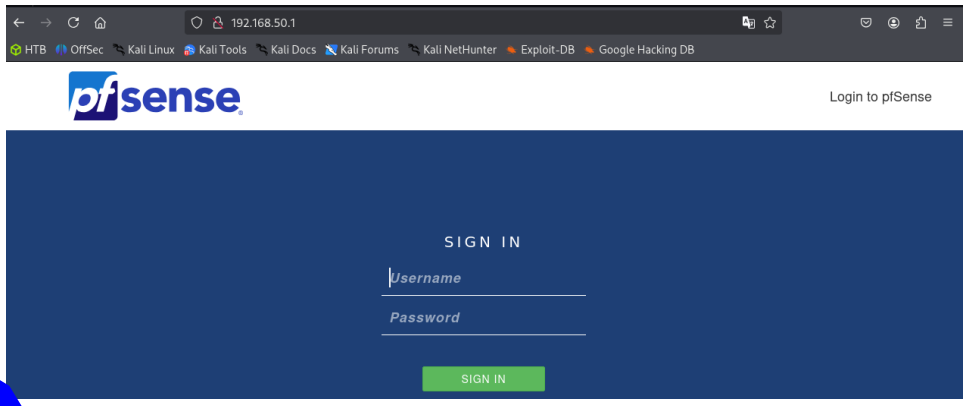
Verifico IP pfSense dove se troverò una porta aperta verifichero l'interfaccia di pfSense, procedendo col comando

Nmap -sS -p 80 192.168.50.1



La porta è aperta e verifico sul browers con http perchè coma abbiamo valutao in call la OVA attuale non ha https

http://192.168.50.1

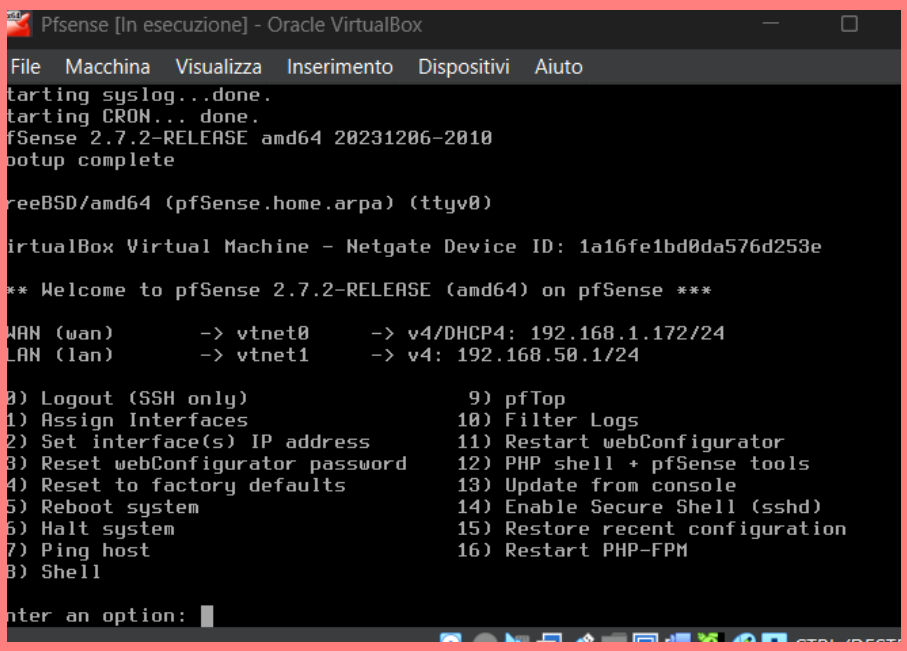


Ok ho conferma della presenza di pfSense

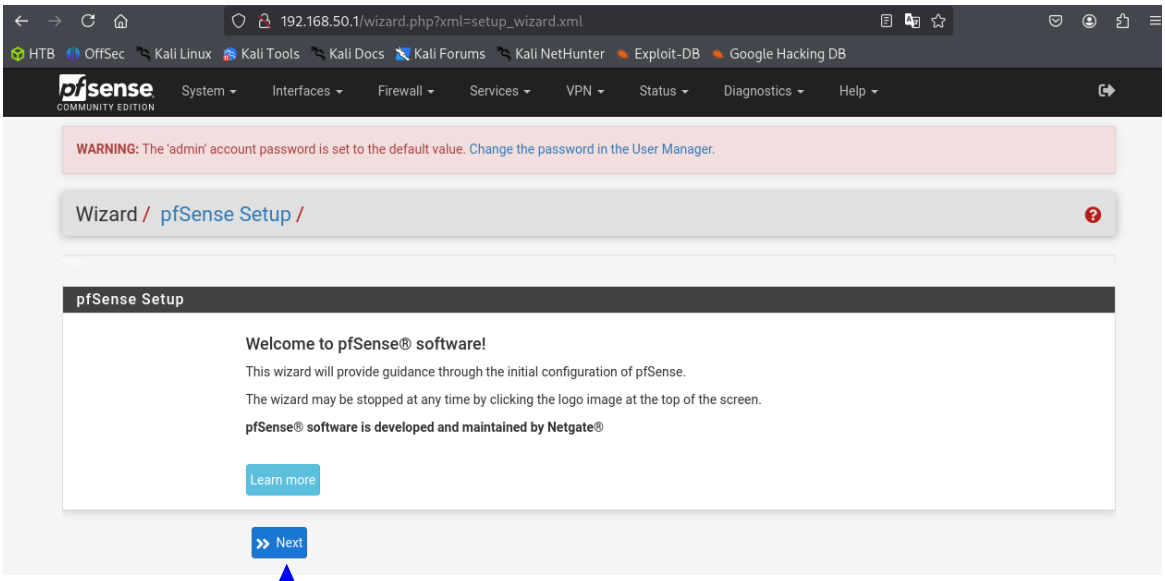
Nel caso la configurazione non fosse andata a buon fine è possibbile asseganre l'indirizzo IP corretto a pfSense in questo modo:

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.50.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.50.1/

Press <ENTER> to continue.
```

Dopo aver premuto ENTER ritornemo alla schermata iniziale



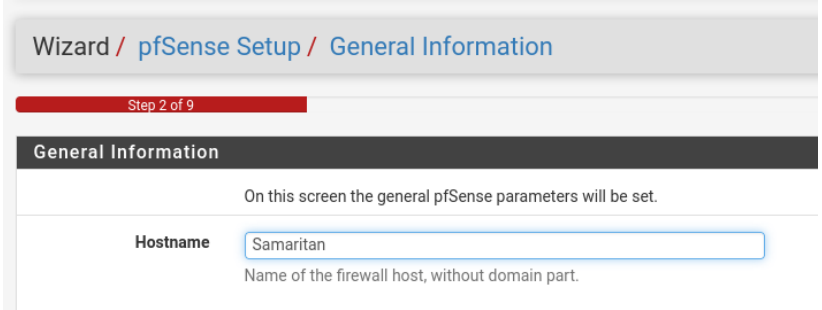
Proseguo con il login di pfSense inserendo le credenziali ed entro visualizzando questa schermata



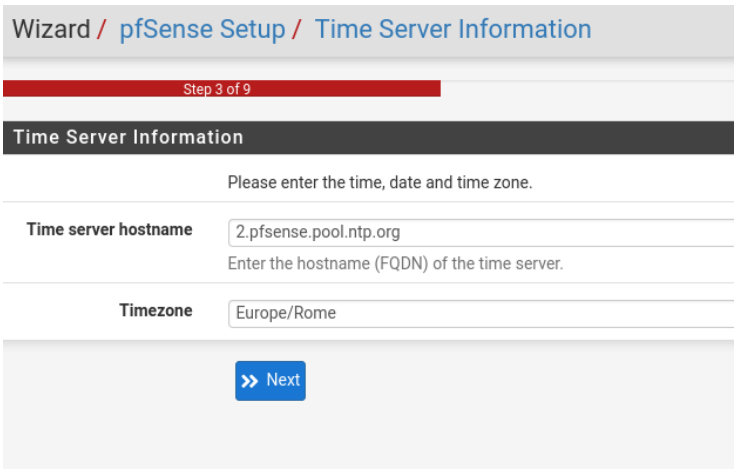
Setap

Per il setup proseguo con Next

Imposto Hostname e proseguo con Next

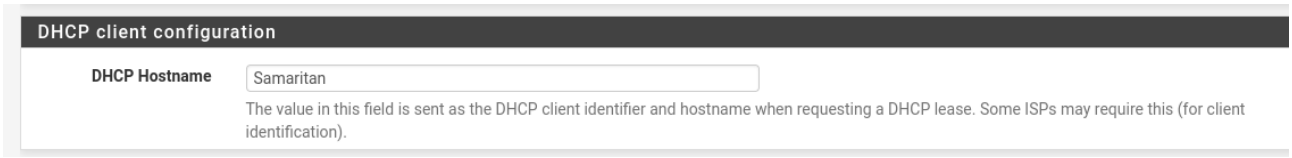


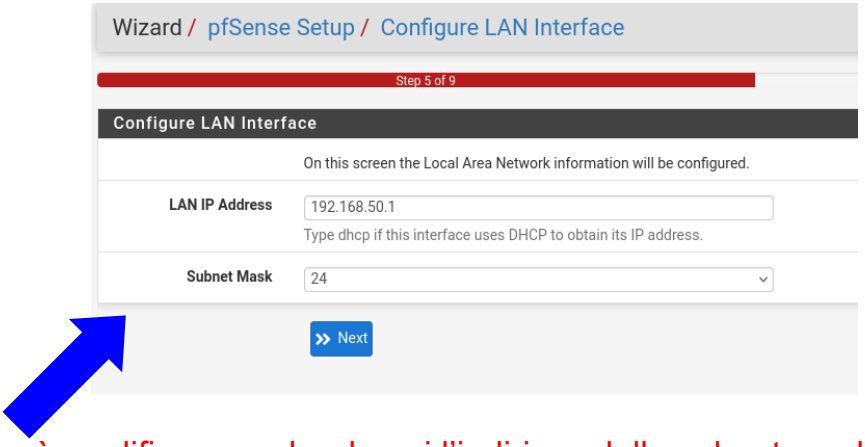
Proseguo con la **configurazione del Time Server Information**



Il time zone è rilevante perchè se non corrisponde non fa autenticare e gli attachi non funzionano, proseguo con Next

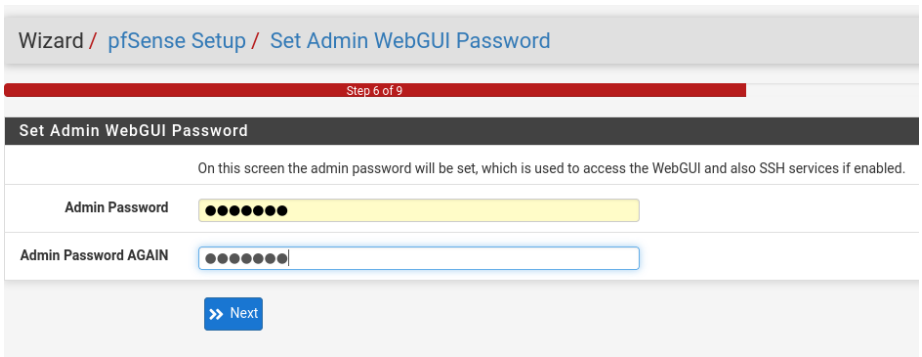
Proseguo con lo step 4 impostando solo il **DHCP client configuration** e proseguo con Next

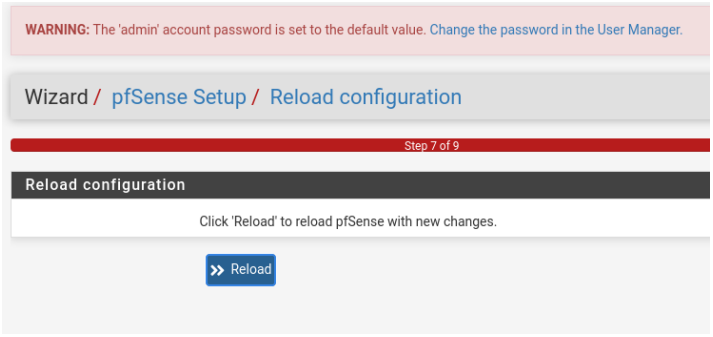




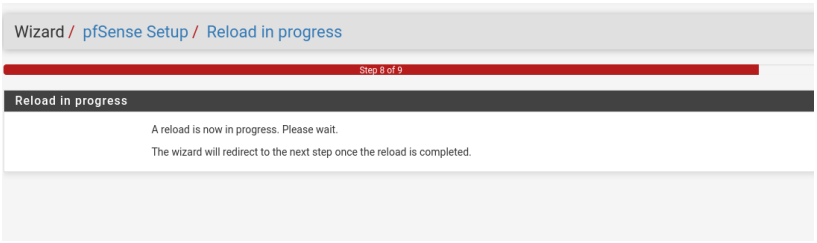
(Volendo si può modificare anche da qui l'indirizzo della subnet mask)

Proseguo con Next e lascio invariate le credenziali

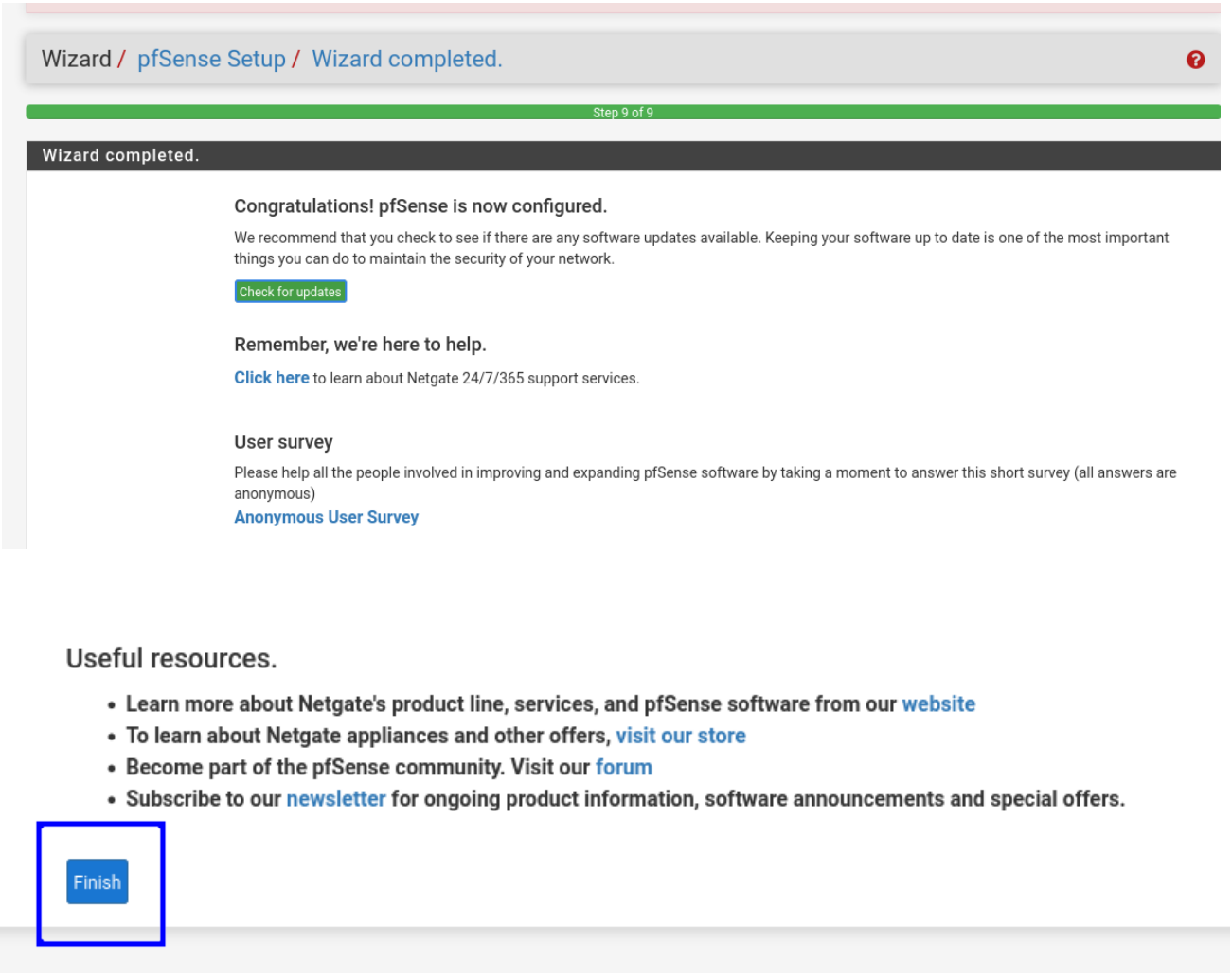




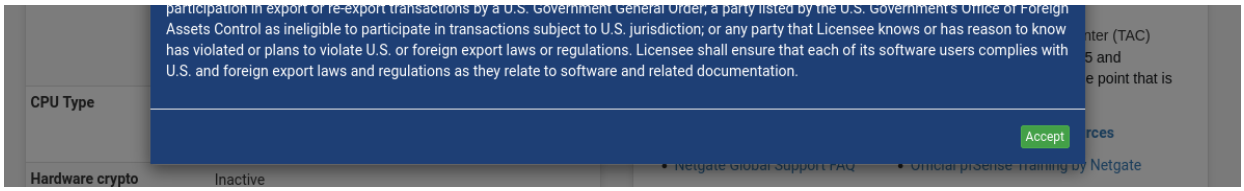
Clicco su Reload per ricaricare tutto

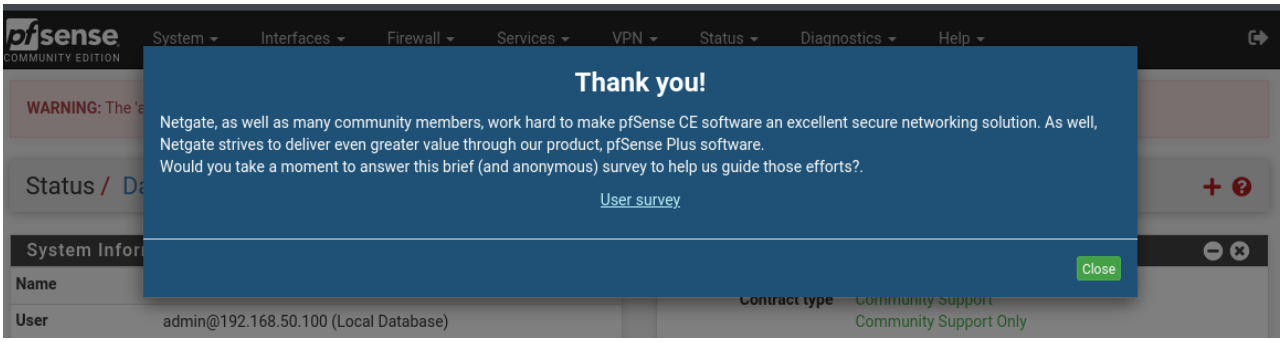


Ricevo la conferma della configurazione di pfSense e clicco su Finish



Infine Accept e Close





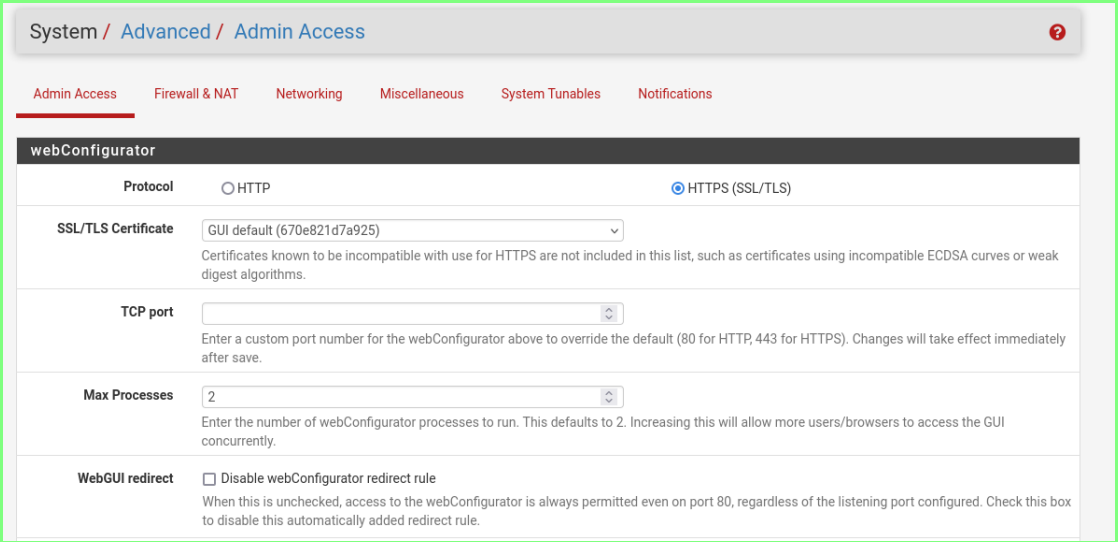
Per quando riguarda il problema riscontrato in call della pagina che non caricava https sono riuscito a capire il problema di seguito spiego come ho fatto

Configurazione certificato SSL

Vado su System ➡ Advanced ➡ Admin Access

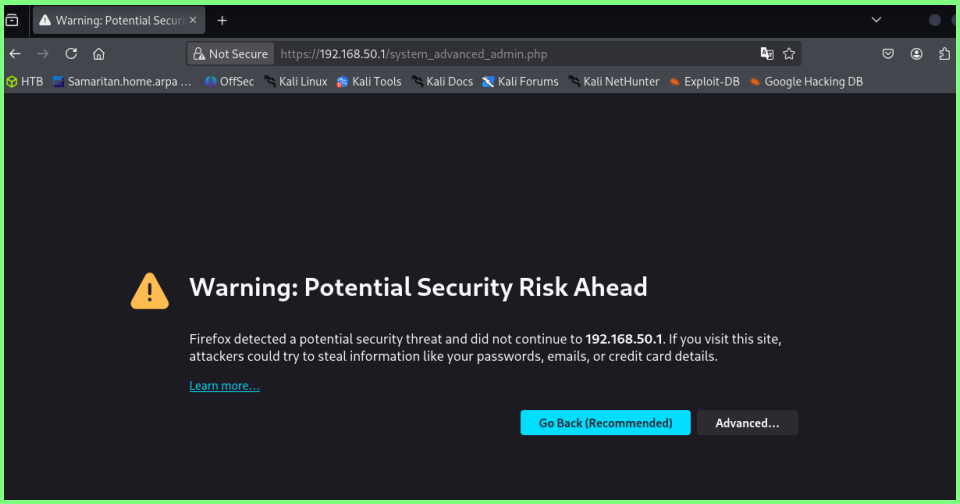
Nella sezione webConfigurator

- Ho selezionato HTTPS
- Mentre nel SSL Certificate jo scelto il certificato esistente oppure si puo crearne uno

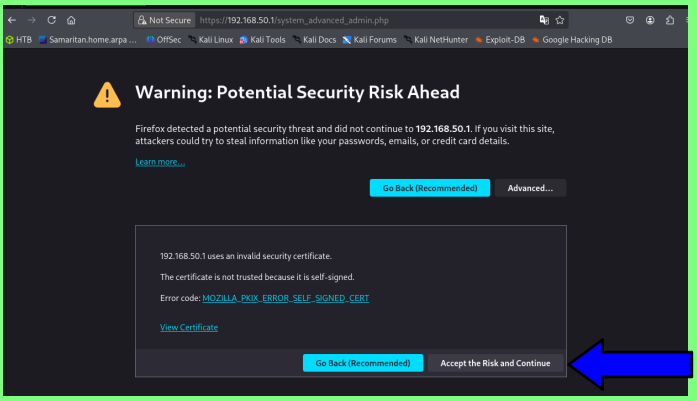


- Assegna il certificato appena creato in **Admin Access**

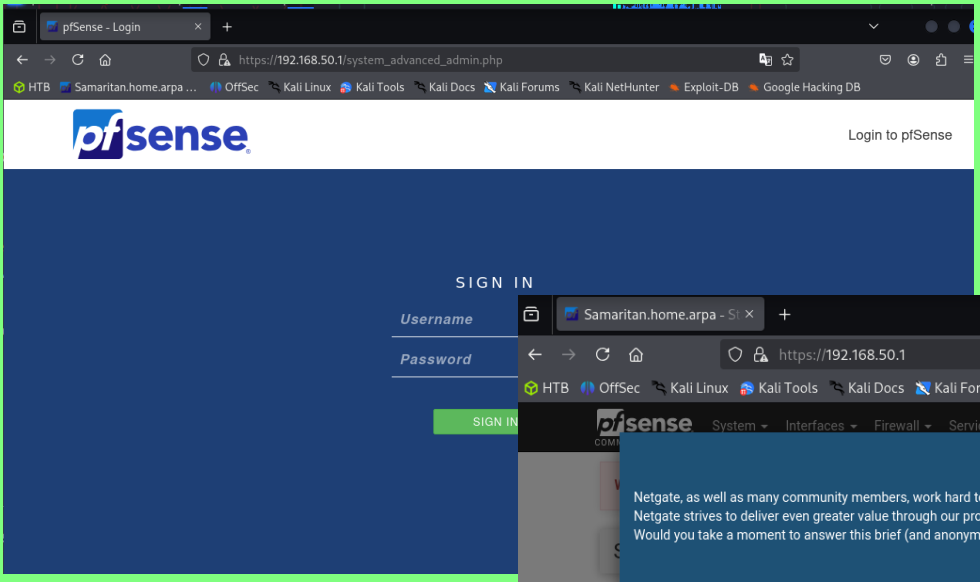
- Ricarico la pagina e mi compare questo messaggio

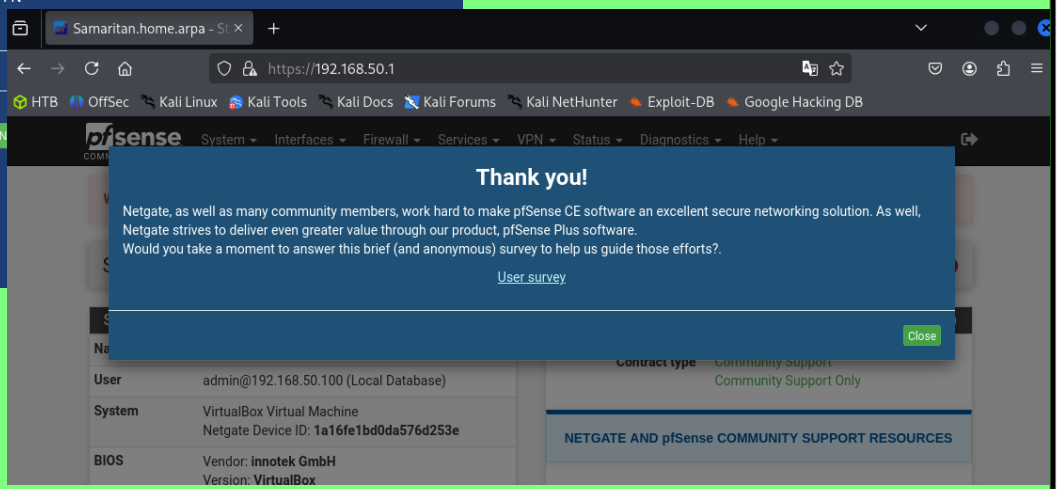


- **Accetto e proseguo**

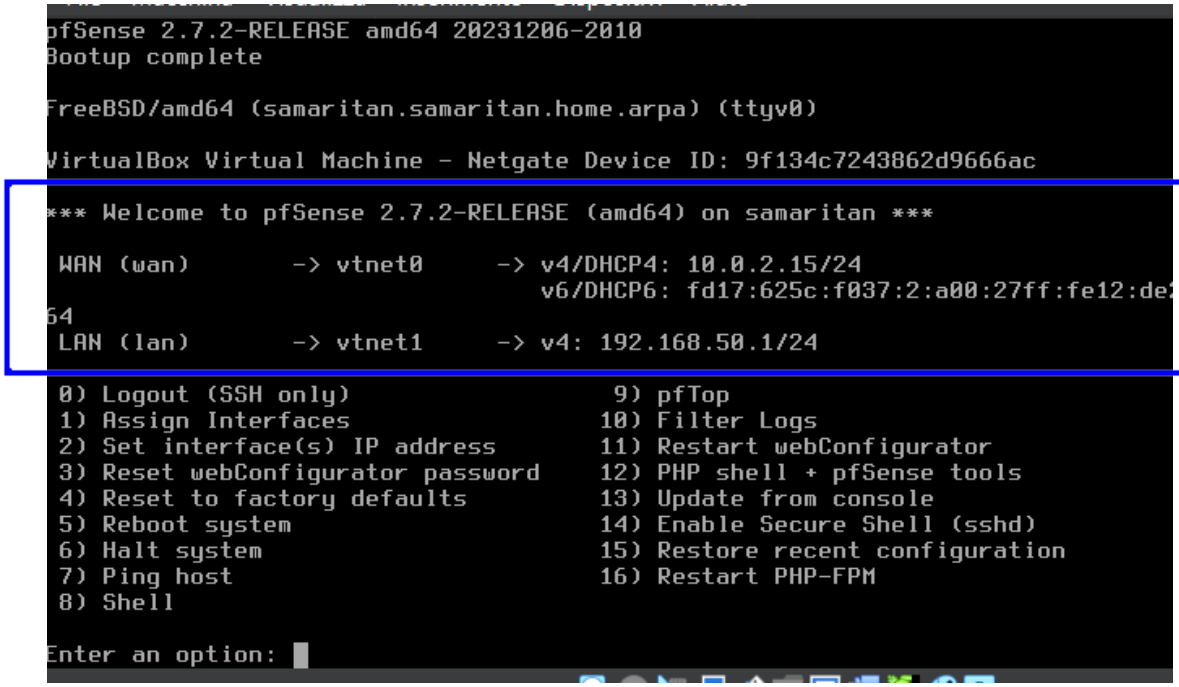


Funziona ! La pagina ssi apre in https come richiesto dalla traccia.





Avvio pfSense e controllo le interfacce di rete configurate e pronte all'uso:



Interfacce di rete:

- **WAN**: Collegata a vtnet0, con indirizzo IP 10.0.2.15/24 (ottenuto via DHCP, dal NAT di VirtualBox).
- **LAN**: Collegata a vtnet1, con indirizzo IP 192.168.50.1/24 (configurazione statica, coerente con l'architettura target).

Macchina Virtuale: Identificatore Netgate Device ID: 9f134c7243b62d9666ac, su un host chiamato "samaritan".

Installazione di pfSense e Configurazione dell'Architettura di Rete di Partenza (Architettura Target)

L'output precedente mi indica che pfSense è già installato e avviato con una configurazione iniziale.
Conferma che WAN e LAN sono riconosciute (vtnet0 e vtnet1).

Verifica e Aggiustamento della Configurazione di Rete

- L'IP WAN (10.0.2.15) è assegnato via DHCP, probabilmente dal NAT di Virtual-Box.
  Siccome devo connettermi a internet reale, mi assicuro che la scheda di rete WAN in VirtualBox sia su **Bridge Adapter** (come suggerito nella guida iniziale).

- L'IP LAN (192.168.50.1) è corretto per l'architettura target.
  Non devo fare nessuna modifica, ma verifico che le altre VM (Kali, Metasploitable2, Windows) siano configurate con IP nella subnet 192.168.50.0/24 (Kali: 192.168.50.100, Metasploitable2: 192.168.50.101, Windows: 192.168.50.102).

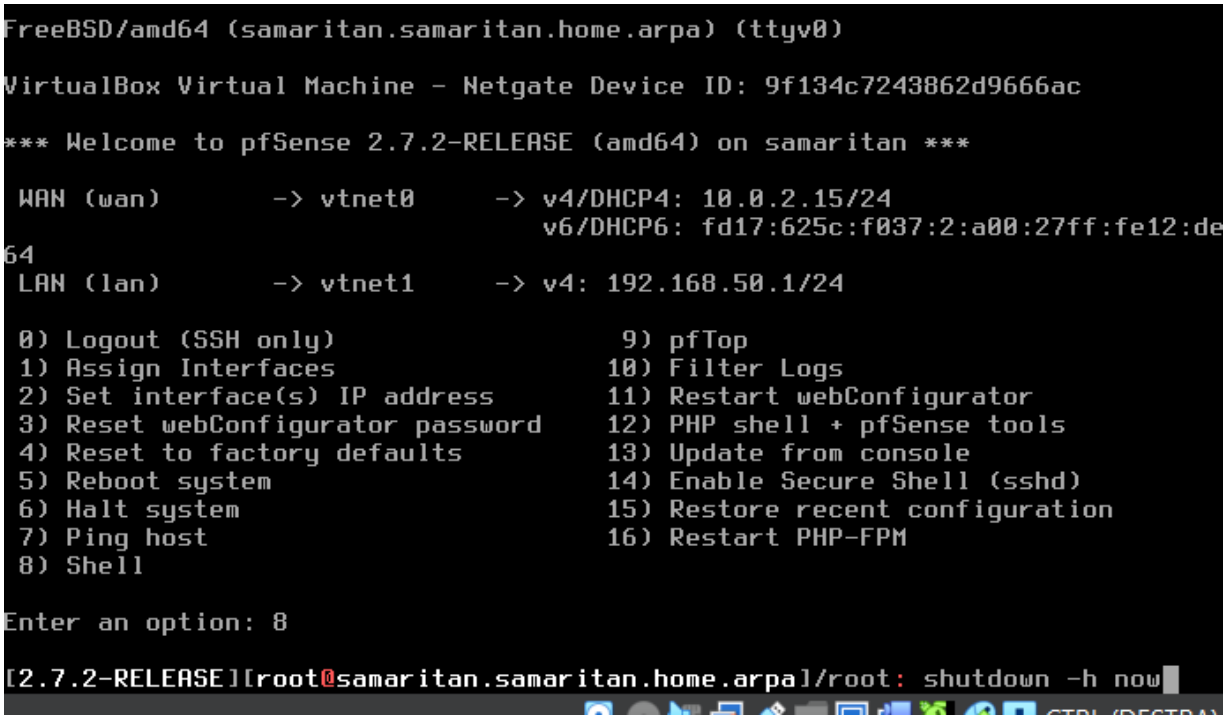
Proseguo con la configurazione dell'interfaccia WAN per connessione a internet reale

Attualmente l'IP WAN 10.0.2.15 è asseganto via DHCP dal Nat di VirtualBox, simula una connessione internet locale ma non mi permette di accedere a internet reale.
Cambierò la configurazione per usare **Bridge Adapter**.

- **Spengo la VM pfSense**

Dalla console di pfSense digito 8 per accedere alla schell ed eseguo

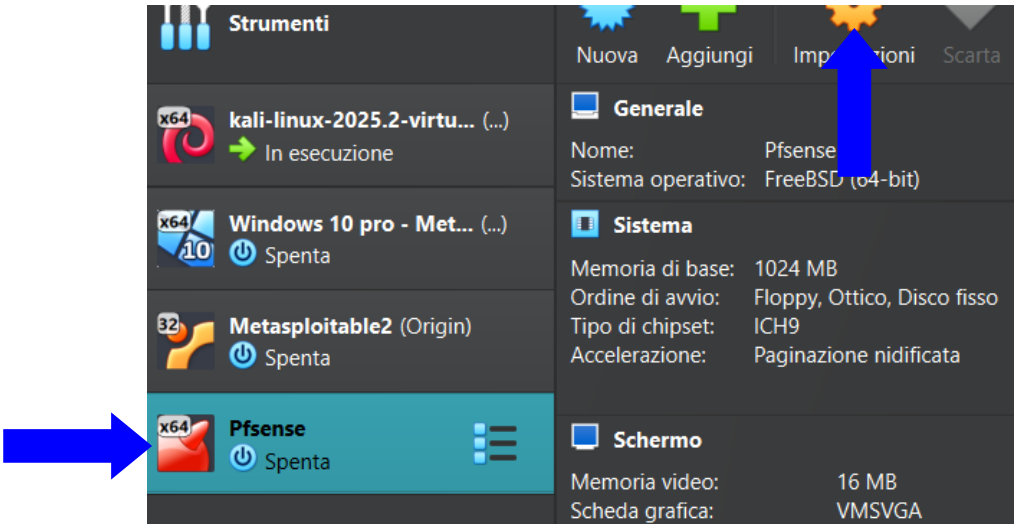
shutdown -h now



Premo invio e attendo che la VM si spenga comletamente e si rivvia in automatico e la spengo.

- **Accedo alle Impostazioni di Rete in VirtualBox**

Seleziono la VM pfSense in VirtualBox e clicco su Impostazioni

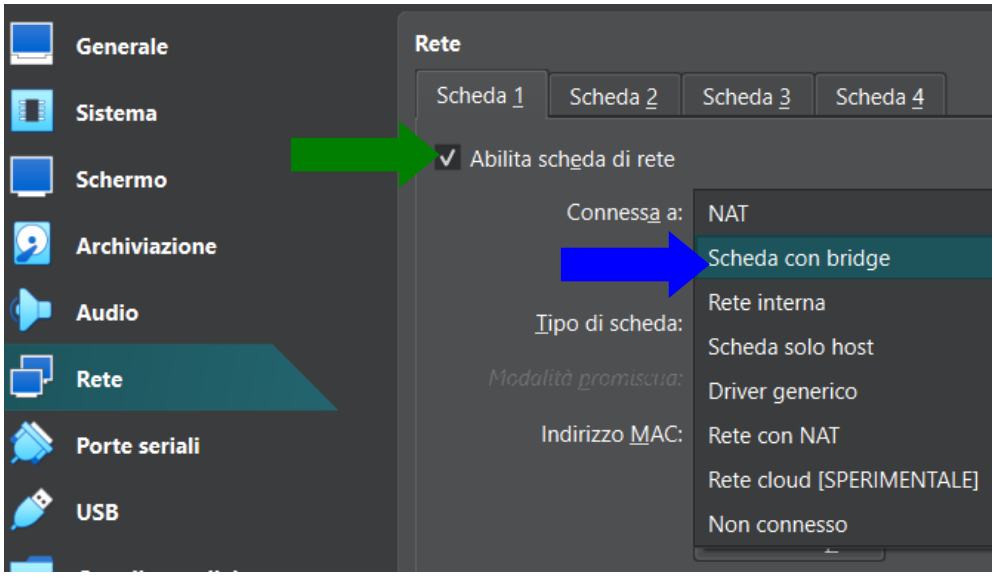


- **Configuro la Scheda 1 (WAN)**

❍ Vado alla scheda **Rete**.

❍ Mi assicuro che la **Scheda 1** sia abilitata

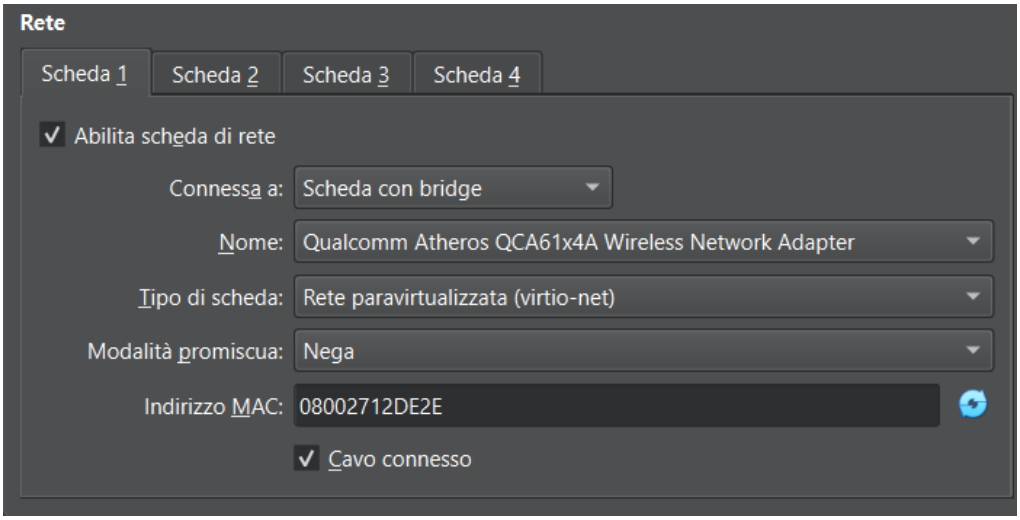
❍ Nel menu **Adattatore collegato a**, seleziono **Adattatore di rete in modalità bridge**.



- Nel menu a tendina **Nome**, scelgo l'adattatore di rete fisico del mio PC host che è connesso a internet (Wi-Fi" o "Ethernet"), verifico qual è attiva (di solito è quella con una connessione internet attiva). In questo caso è Wireless (la mia rete WI-FI) che hon controllato dal mio pannello di controllo di windows e seleziono:

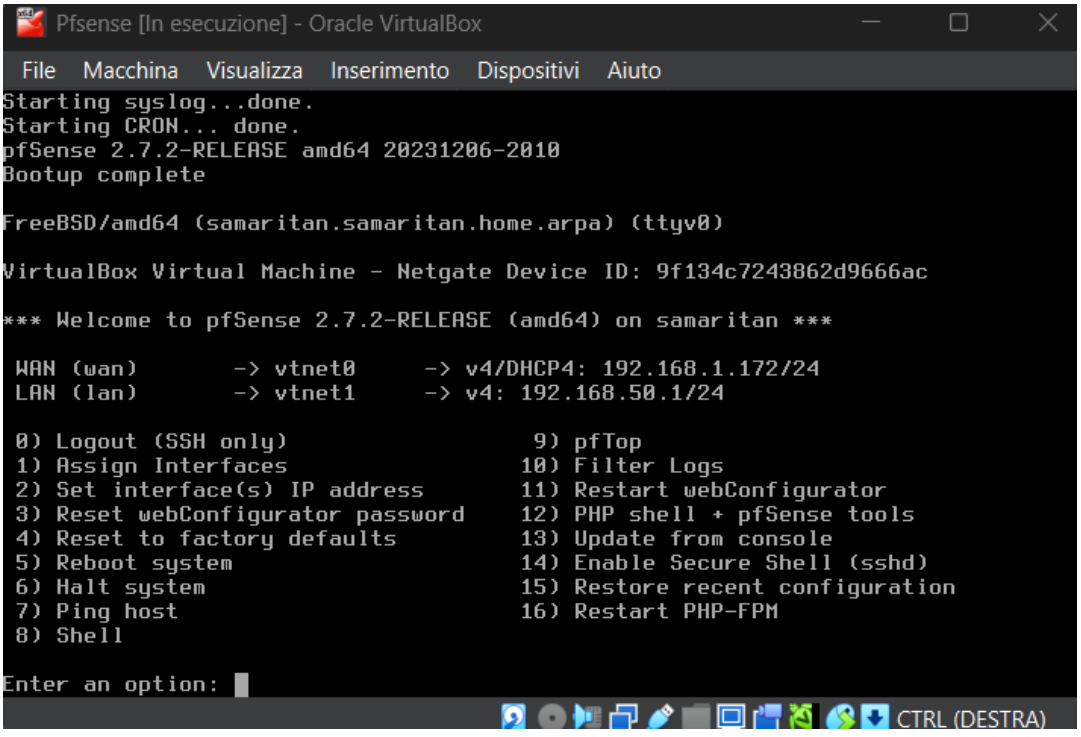
Qualcomm Atheros QCA61x4A Wireless Network Adapter

- Tipo di scheda di rete seleziono Rete paravirtualizzata
- Imposto la Modalità promiscua "Nega"



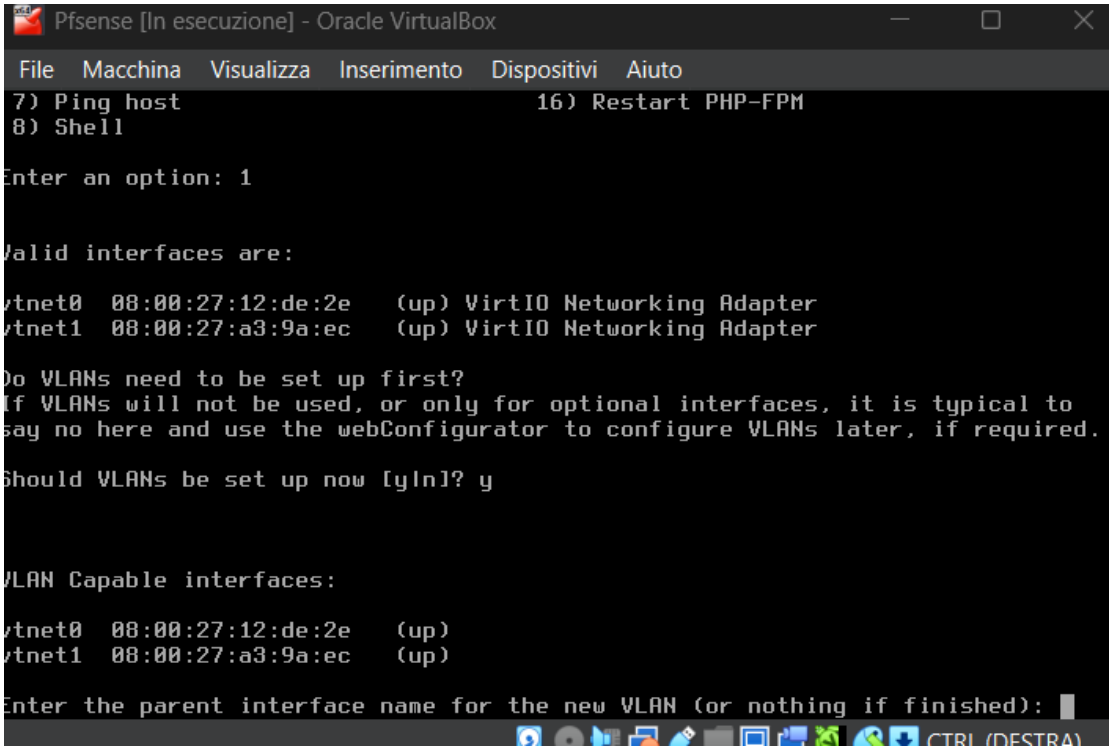
Salvo tutto .

- **Avvio la VM pfSense e verifico la Configurazione WAN**

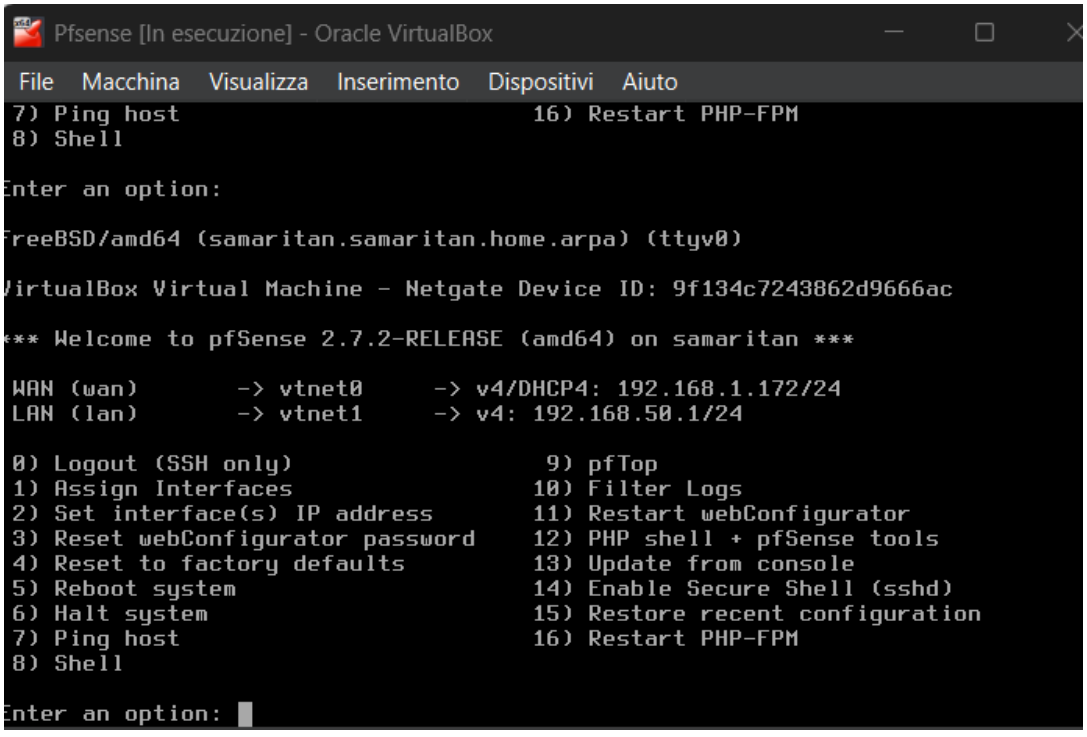


❍ Dopo l'avvio mi trovo nella schermata home di pfSense, digito 1

⇒ Assingn Interface e confermo le interfacce WAN su vtnet0, LAN su vtnet1 premendo y

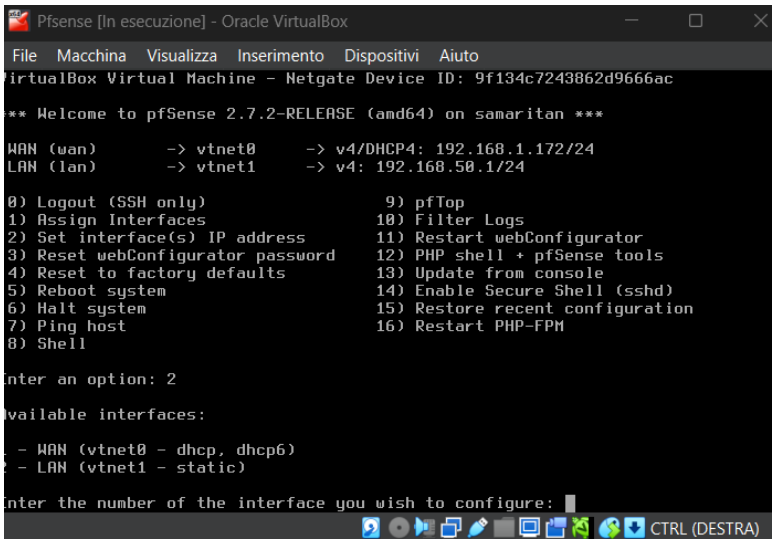


Dopo conferma, ricevo questo

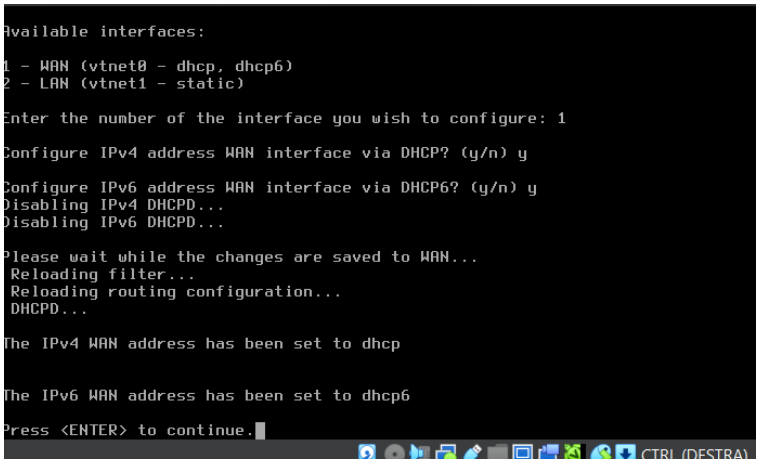


⇒ Poi digito 2

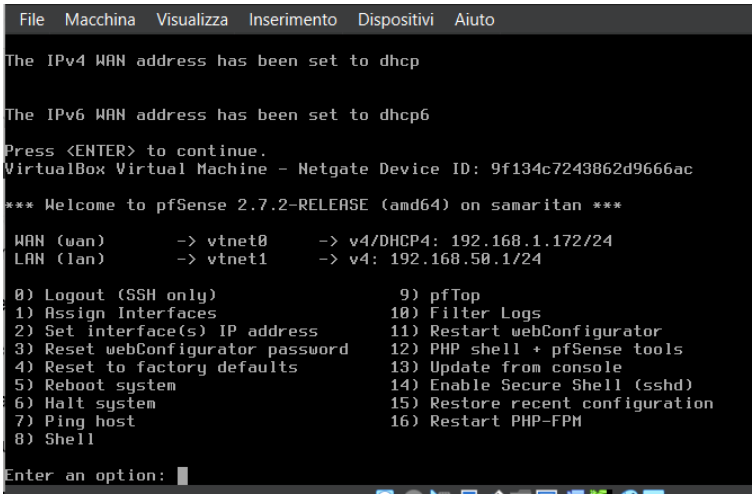
- Per WAN selezioni DHCP e confermo (lascio che pfSense ottenga un ip dal mio router)



Proseguo



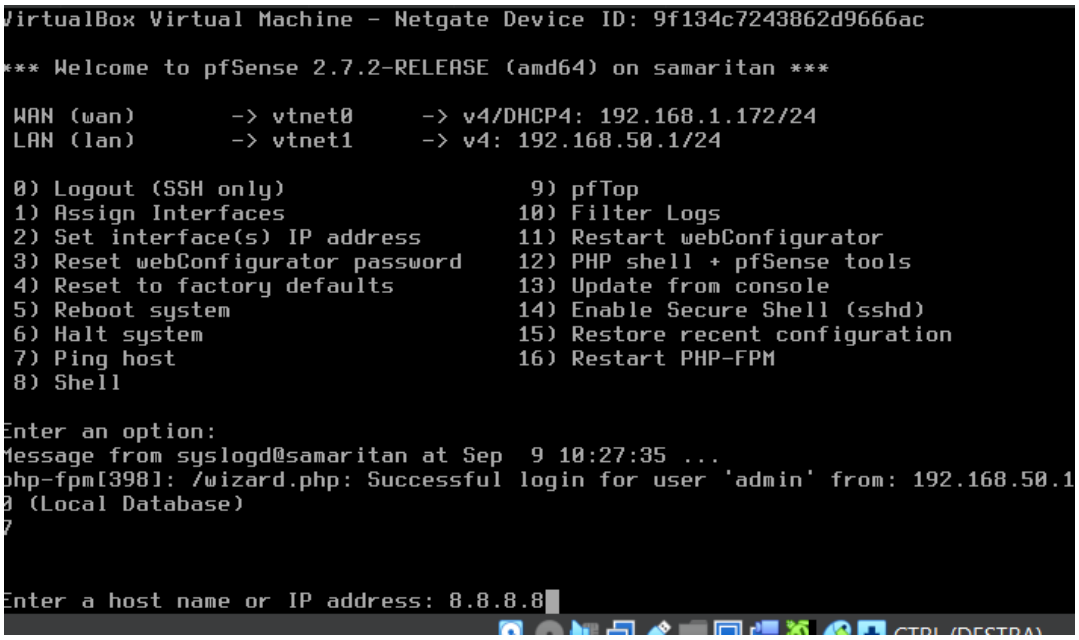
- Per LAN lascio 192.168.50.1/24 senza modificarlo



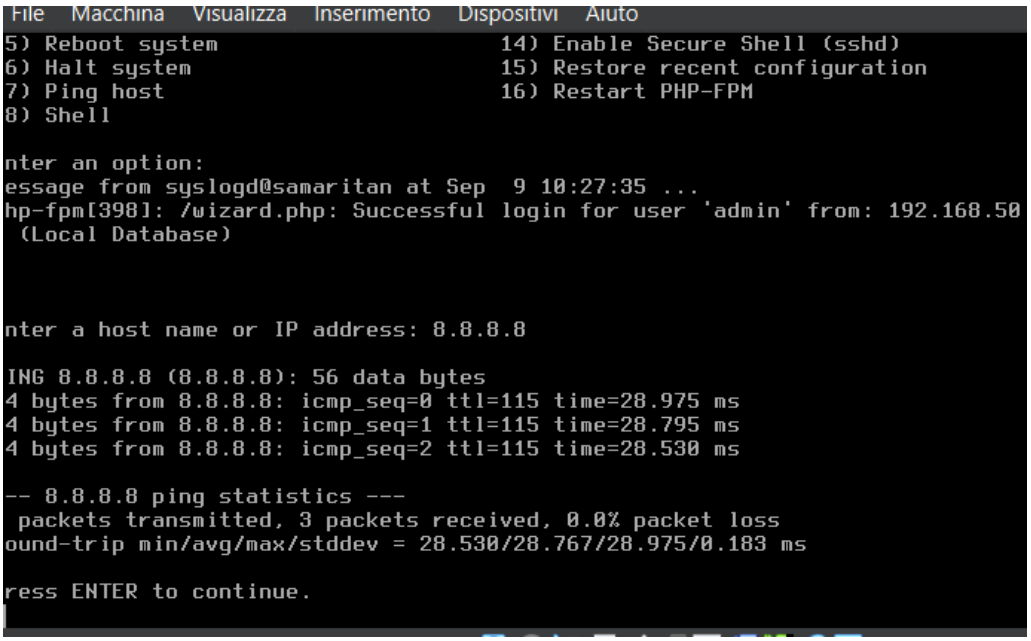
- Ora riavvio con 5 e poi Y e attendo il riavvio del servizio

- **Test della Connessione**

❍ Dalla console digito 7 per **Ping Host**



❍ Inserisco 8.8.8.8 e premo invio



❍ Vedo risposte quindi questo mi conferma che la configurazione della WAN è stata impostata con successo utilizzando l'adattatore **Qualcomm Atheros QCA61x4A Wireless Network Adapter** in modalità bridge, e pfSense sta comunicando con internet tramite DHCP

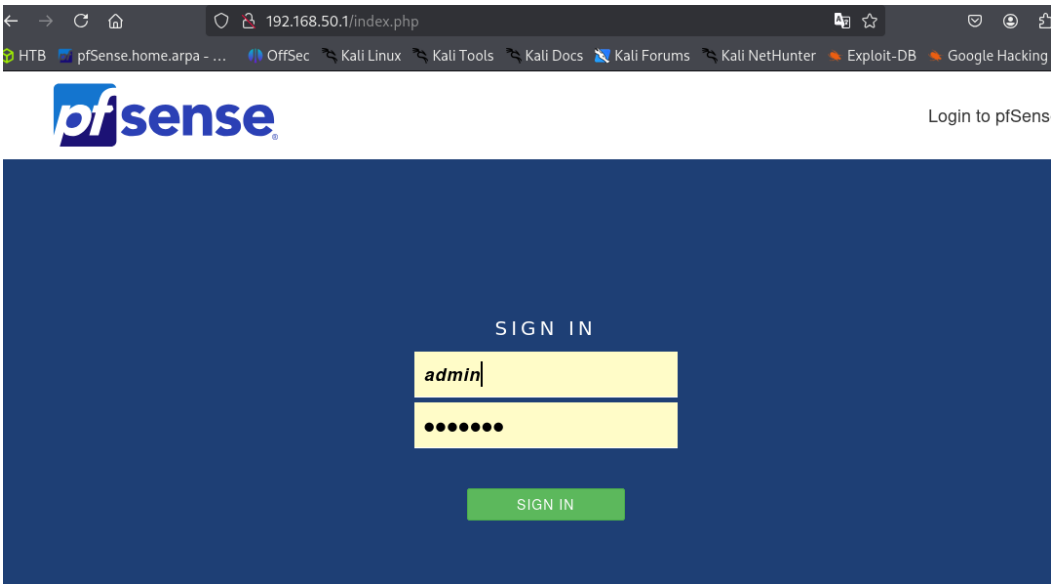
- **Recap attuale**

- **WAN** configurata e funzionante IP asseganto via DHCP, ping a 8.8.8.8 OK.
- **LAN** dovrebbe essere configurata su 192.168.50.1/24 come ho visto nella console iniziale, ma adesso devo verificare e assicurarmi che le altre VM (Kali, Metasploitable2 e Windows) si trovano nella subnet corretta.

Verifica della Configurazione LAN e delle Altre VM

- Ho verificato che l'IP LAN visibile nella console pfSense 192.168.50.1/24, corretto per l'architettura target

- Accedo alla Web GUI dal mio PC host Kalicon http://192.168.50.1

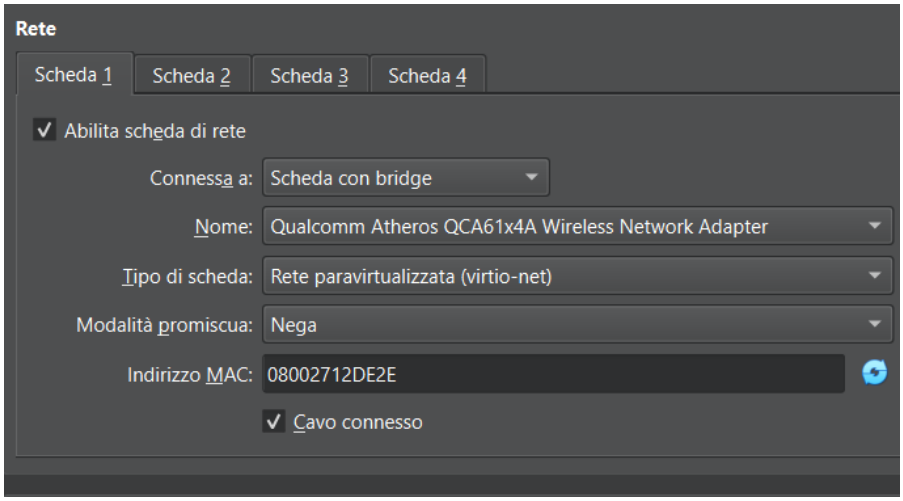


- Dopo conferma del login e apertura pagina spengo la Kali

- Proseguo con la configurazione della Rete:

- Vado su impostazioni ➡ rete ➡ **Scheda1** e imposto

- **Abilita scheda di rete** sia spuntata per la **Scheda 1**.
- Seleziono **Adattatore di rete in modalità bridge**.
- Nel menu a tendina **Nome**, scelgo **Qualcomm Atheros QCA61x4A Wireless Network Adapter** (deve corrispondere all'adattatore usato per la WAN di pfSense).
- **Tipo di scheda**: **Rete paravirtualizzata (virtio-net)** per compatibilità con pfSense.
- **Modalità promiscua**: Lascio su **Nega**.
- **Indirizzo MAC**: Lascio generato automaticamente.
- **Cavo connesso**: Mi assicuro che sia spuntata.



- Vado su impostazioni ➡ rete ➡ **Scheda 2** e imposto
  - Lascio su **NAT** in modo che Kali abbia accesso a internet direttamente (utile per test).
  - Disattivo (rimuovo la spunta da **Abilita scheda di rete**) pfSense gestirà tutto il traffico internet.
  - Per ora, lascio su NAT e disattivo solo se riscontro conflitti.
  - Salvo e avvio Kali

- **Avvio Kali e Configuro l'IP Statico**

- Verifico la configurazione con ip a

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::5d9e:1d92:795c:704b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e2:55:37 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
       valid_lft 85902sec preferred_lft 85902sec
    inet6 fd17:625c:f037:3:d3c4:66a2:d1e5:e265/64 scope global dynamic noprefixroute
       valid_lft 86345sec preferred_lft 14345sec
    inet6 fe80::c942:d1d7:8df7:8327/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

L'output di ip a mostra che la configurazione dell'IP statico su Kali è stata applicata correttamente, analizzo i dettagli e procedo con i prossimi passi.

- **Analisi dell'Output**

❍ **Interfaccia lo (1)** Loopback, funziona correttamente (127.0.0.1).
❍ **Interfaccia eth0 (2)**
- **MAC** 08:00:27:d1:f8:5d.
- **IP** 192.168.50.100/24, corrisponde all'IP statico configurato per la LAN di
- pfSense.
- **Broadcast** 192.168.50.255.
- **Gateway non esplicito** Non è visibile qui, ma dovrebbe essere 192.168.50.1 (pfSense), configurato tramite NetworkManager.
- Stato: UP, quindi attiva e pronta.

- **Interfaccia eth1 (3)**
- **MAC** 08:00:27:e2:55:37.
- **IP** 10.0.3.15/24, assegnato dinamicamente via DHCP (probabilmente dal NAT di VirtualBox, legato alla Scheda 2).
- Stato: UP, ma non rilevante per la LAN di pfSense.

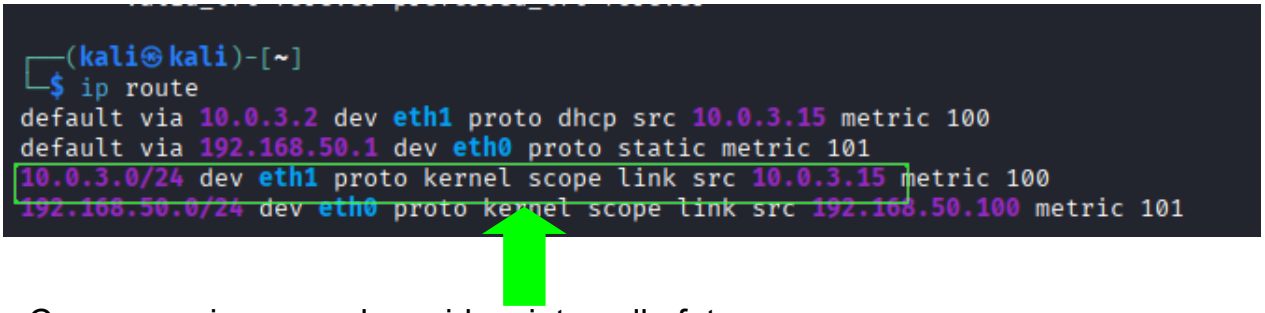
- **Verifiche**

L'IP 192.168.50.100 su eth0 è corretto per la subnet 192.168.50.0/24 gestita da pfSense, ora devo:

- Confermare che il gateway e il DNS siano corretti.
- Testare la connettività con pfSense
- Procedere con la configurazione di Metasploitable2 e Windows

❍ **Verifica del Gateway e DNS**

- Eseguo ip route



- Cerco una riga come ho evidenziato nella foto

- **Route Predefinite (Default Gateway)**:
- **default via 10.0.3.2 dev eth1 proto dhcp src 10.0.3.15 metric 100** E' la route predefinita impostata da DHCP sulla eth1 (probabilmente legata alla Scheda 2 con NAT in VirtualBox), con un indirizzo IP dinamico 10.0.3.15. Ha una metrica di 100.
- **default via 192.168.50.1 dev eth0 proto static metric 101** E' la route predefinita che ho configurato manualmente per la eth0 (Scheda 1 con bridge), con gateway 192.168.50.1 (pfSense) e IP statico 192.168.50.100. Ha una metrica di 101.

- **Route di Rete Locale**:
- **10.0.3.0/24 dev eth1 proto kernel scope link src 10.0.3.15 metric 100** E' la rete locale per eth1.
- **192.168.50.0/24 dev eth0 proto kernel scope link src 192.168.50.100 metric 101** E' la rete locale per eth0, che corrisponde alla LAN di pfSense.

Dopo la verifica ho rsicontrato un problema descrivo come ho risolto

- **Analisi**

Questo perchè risulta che Kali ha due **route predefinite** (default via 10.0.3.2 e default via 192.168.50.1), e il sistema operativo sceglierà quella con la metrica più bassa.
Qui, 10.0.3.2 (metrica 100) ha priorità su 192.168.50.1 (metrica 101).
Questo significa che il traffico di default (inclusi i ping e l'accesso alla Web GUI di pfSense) potrebbe essere instradato tramite eth1 (NAT) invece di eth0 (LAN pfSense), causando potenziali problemi di connettività con 192.168.50.1

- **Soluzione**

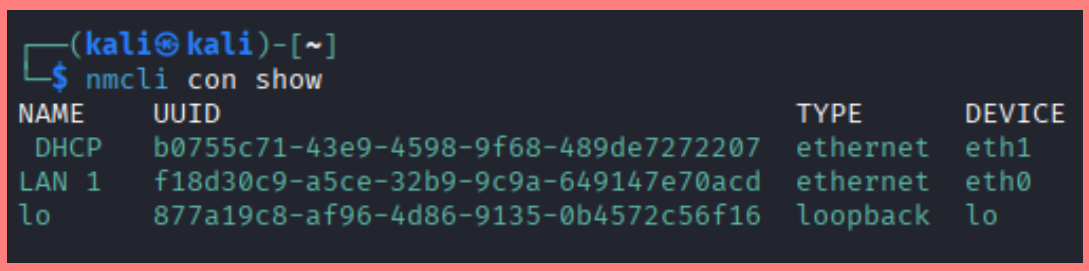
Devo assicurarmi che il gateway predefinito sia solo 192.168.50.1 su eth0, elimino o modifico la route DHCO su eth1.
Poichè sto usando NetworkManager aggiornerò la configurazione per dare la priorità a eth0

- **Modificare la Route DHCP su eth1**

❍ Ho deciso per proseguire di non elimare ma disattivare la connessione DHCP su eth1 eseguendo

nmcli con show

Riuscendo a vedere con chiarezza le connessioni di rete configurate su Kali Linux tramite NetworkManager



- **Analisi dell'Output**

❍ **Connessioni Attive**

◦ **DHCP** UUID: b0755c71-43e9-4598-9f68-489de7272207, Tipo: ethernet, Dispositivo: eth1

◦ Questa connessione è associata a eth1, che ha l'IP 10.0.3.15/24 (dal NAT di VirtualBox) e una route predefinita default via 10.0.3.2.

È la connessione DHCP che stop cercando di disattivare per dare priorità alla LAN.

- **LAN 1** UUID: f18d30c9-a5ce-32b9-9c9a-649147e70acd, Tipo: ethernet, Dispositivo: eth0
- Questa è la connessione statica che ho configurato su eth0 con l'IP 192.168.50.100/24 e gateway 192.168.50.1 (pfSense). È corretta per la LAN.

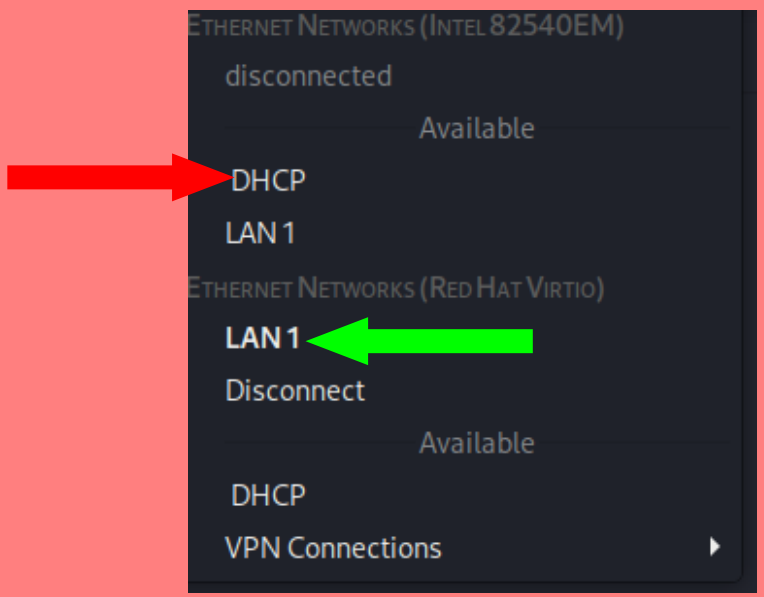
- **lo** UUID: 877a19c8-af96-4d86-9135-0b4572c56f16, Tipo: loopback, Dispositivo: lo
  La connessione loopback, funziona come previsto.

- **Problema e Soluzione**

La connessione DHCP su eth1 sta generando una route predefinita (default via 10.0.3.2) con metrica 100, che ha priorità sulla route statica su eth0 (metrica 101). Questo causa il routing del traffico di default tramite eth1 invece di eth0, interferendo con la connettività verso pfSense (192.168.50.1).

- Devo disattivare la connessione **DHCP** su **eth1** per rimuovere la route predefinita concorrente e garantire che il traffico passi attraverso **eth0 LAN 1** verso Pfsense.

- Disattivo in questo modo disconnettendo la rete DHCP e attivando la rete Lan1



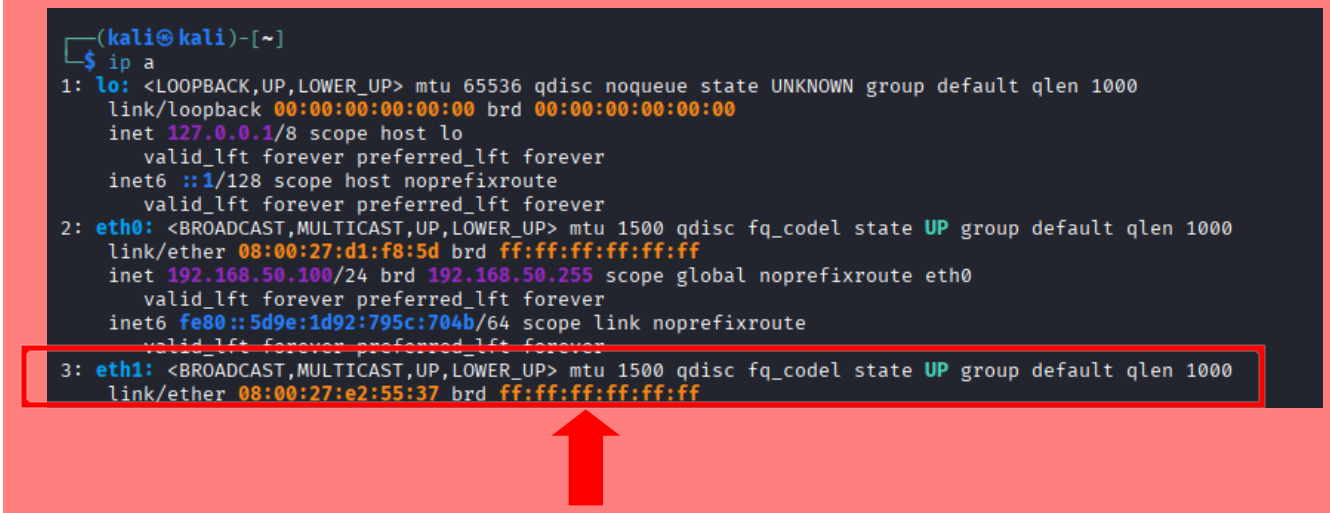
- Eseguo il ping di verifica su 192.168.50.1 con

ping 192.168.50.1

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=2.33 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.53 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=1.58 ms
^C
── 192.168.50.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 1.530/1.813/2.328/0.364 ms
```

- Adesso verifico l'effettiva disconnessione della rete DHCP con

ip a



- Ho conferma che il DHCP e disabilitato correttamente

- **Testo connettività internet**

- Ping a un server esternoda Kali con

ping 8.8.8.8

```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=30.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=31.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=31.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=30.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=30.0 ms
^C
── 8.8.8.8 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4045ms
rtt min/avg/max/mdev = 29.990/30.639/31.475/0.656 ms
```

- Funziona, pfSense sta instradndo il traffico WAN correttamente.

- Ping a un nome Dominio con

ping www.google.com

```
┌──(kali㉿kali)-[~]
└─$ ping www.google.com
PING www.google.com (142.250.180.132) 56(84) bytes of data.
64 bytes from mil04s43-in-f4.1e100.net (142.250.180.132): icmp_seq=1 ttl=114 time=27.7 ms
64 bytes from mil04s43-in-f4.1e100.net (142.250.180.132): icmp_seq=2 ttl=114 time=27.5 ms
64 bytes from mil04s43-in-f4.1e100.net (142.250.180.132): icmp_seq=3 ttl=114 time=27.5 ms
64 bytes from mil04s43-in-f4.1e100.net (142.250.180.132): icmp_seq=4 ttl=114 time=28.0 ms
^C
── www.google.com ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 7253ms
rtt min/avg/max/mdev = 27.503/27.686/28.043/0.220 ms
```

  - Funziona, il DNS è configurato.

- Ora traccio il percorso che un pacchetto di dati segue attraverso la rete per raggiugere un determinato indirizzo IP o dominio in questo caso www.google.com, è uno strumento di diagnostica di rete che:

  - Mostra ogni HOP (router o nodo) attraversato, con il reltivo indirizzo IP e il tempo di risposta in millisecondi

  - Aiuta a identificare dove si verficano problemi di connettività tipo un hop non risponde o ha tempi elevati.

- Eseguo traceroute www.google.com

```
┌──(kali㉿kali)-[~]
└─$ traceroute www.google.com

traceroute to www.google.com (142.250.180.132), 30 hops max, 60 byte packets
 1  samaritan.samaritan.home.arpa (192.168.50.1)  2.933 ms  2.798 ms  2.679 ms
 2  192.168.1.1 (192.168.1.1)  6.475 ms  6.359 ms  6.250 ms
 3  * * *
 4  172.18.16.144 (172.18.16.144)  14.691 ms 172.18.16.148 (172.18.16.148)  14.580 ms 172.18.16.144 (172.18.16.144)  13.217 ms
 5  172.18.16.202 (172.18.16.202)  13.085 ms 172.18.16.240 (172.18.16.240)  12.968 ms 172.18.16.206 (172.18.16.206)  14.111 ms
 6  172.19.177.86 (172.19.177.86)  21.025 ms  19.574 ms 172.19.177.90 (172.19.177.90)  16.971 ms
 7  172.19.177.4 (172.19.177.4)  29.523 ms 172.19.177.8 (172.19.177.8)  32.928 ms  30.201 ms
^C
```

Nel mio caso il traceroute mi ha mostrato :

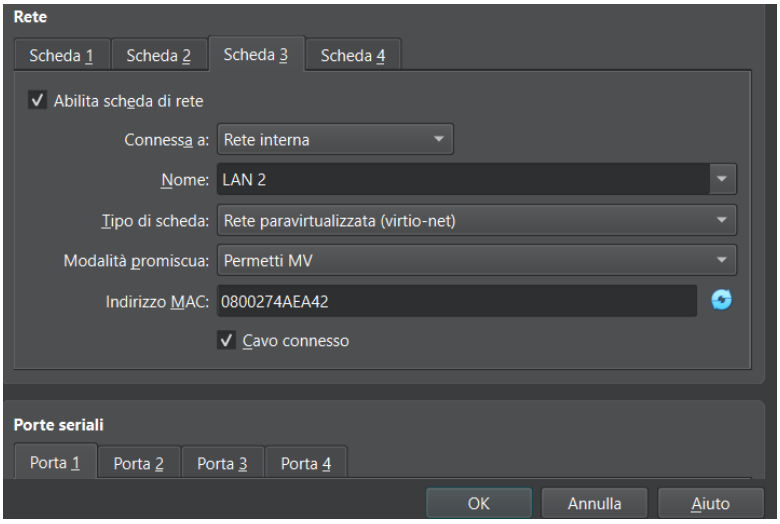
  - Il primo hop (192.168.50.1) è pfSense.
  - Il secondo hop (192.168.1.1) è probabilmente il mio router.
  - Gli hop successivi sono nodi della rete del mio ISP o di Google.

- Funziona, conferma che il traffico esce dalla LAN di pfSense verso internet, dopo test ho interrotto con ^C.

Per semplificare il tutto per far cominucare tutte le macchine in LAN o rete interna ho configurato per ogni macchina la sua scheda di rete interna in rete paravirtualizzata.

Scheda 3 pfSense

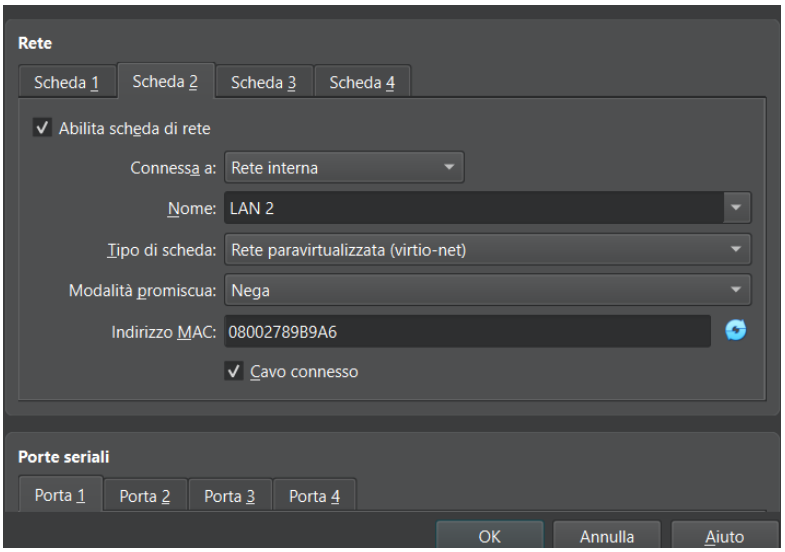
- Creo una terza rete su pfSense (scheda 3) allego foto con impostazioni eseguite



- Salvo e riavvio pfSense

Scheda 2 Metasploitable2

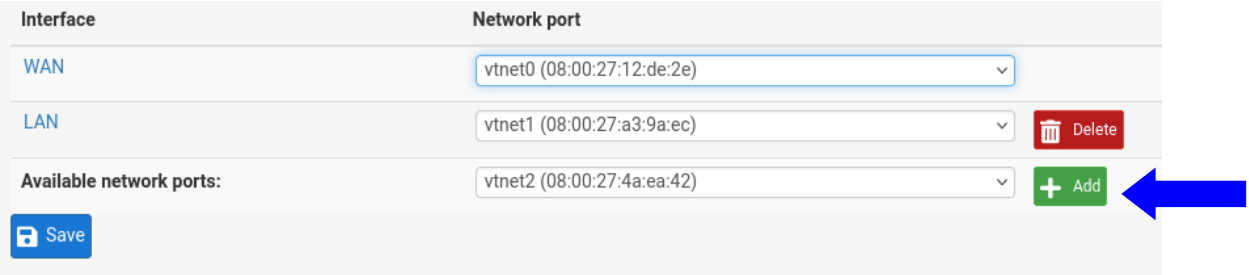
- Creo una seconda rete su Metasploitable2 (scheda 2) allego foto con impostazioni eseguite



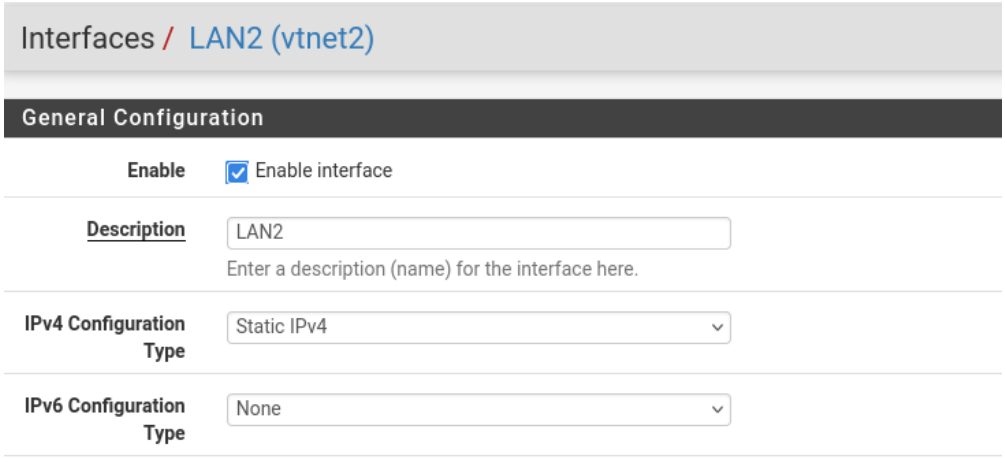
❍ Lancio Metasploitable

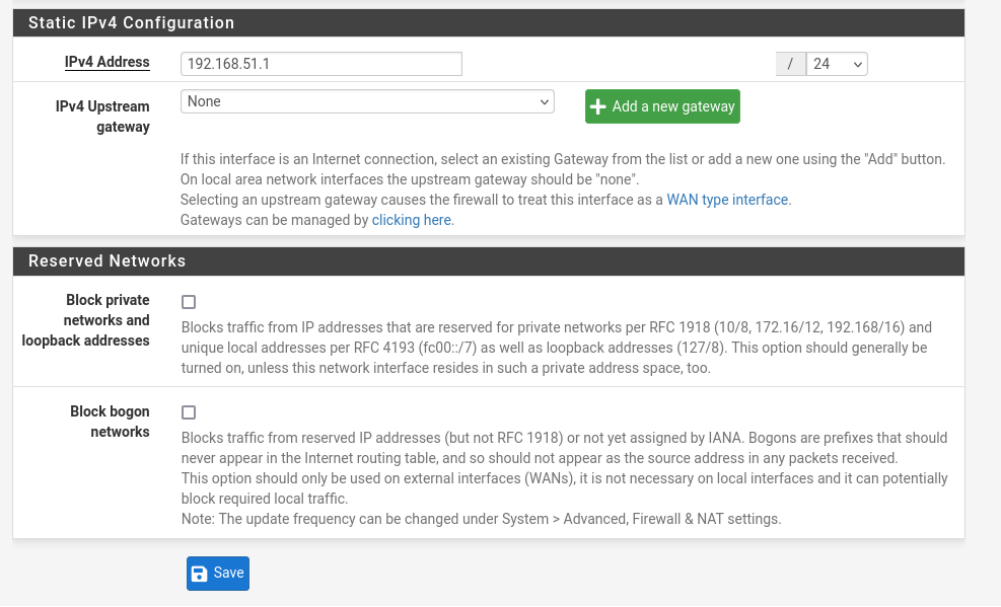
Configurazione la LAN 2

❍ Accedo a pfSense e in interfaces aggiungo un’altra rete LAN 2

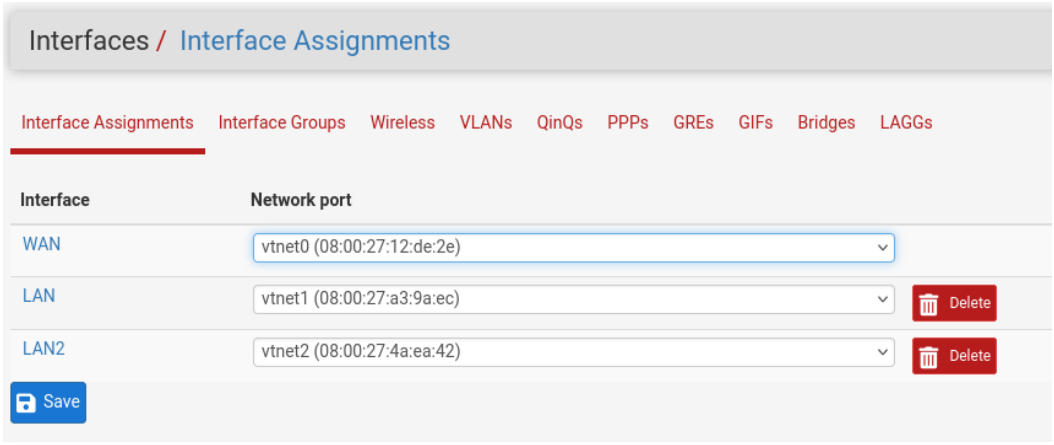


❍ Imposto la rete LAN 2 con impostazioni elencate nelle foto in basso

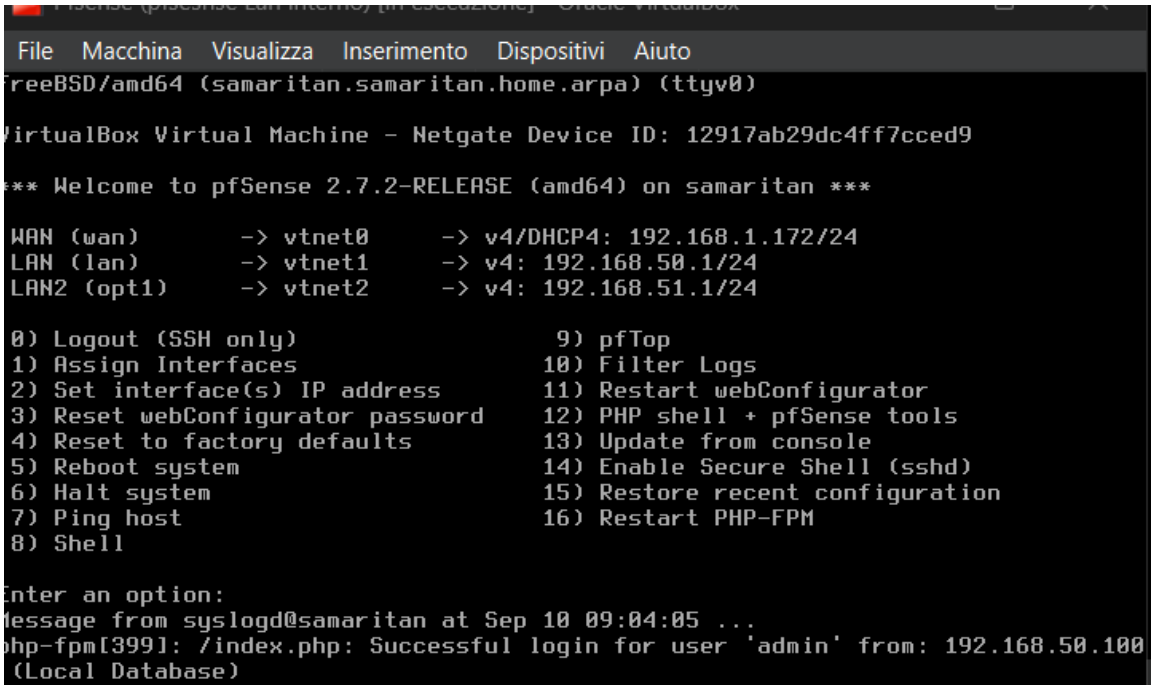




❍ Conferma della creazione della LAN 2



❍ Verifico su pfSense dopo il riavvio la presenza della LAN 2

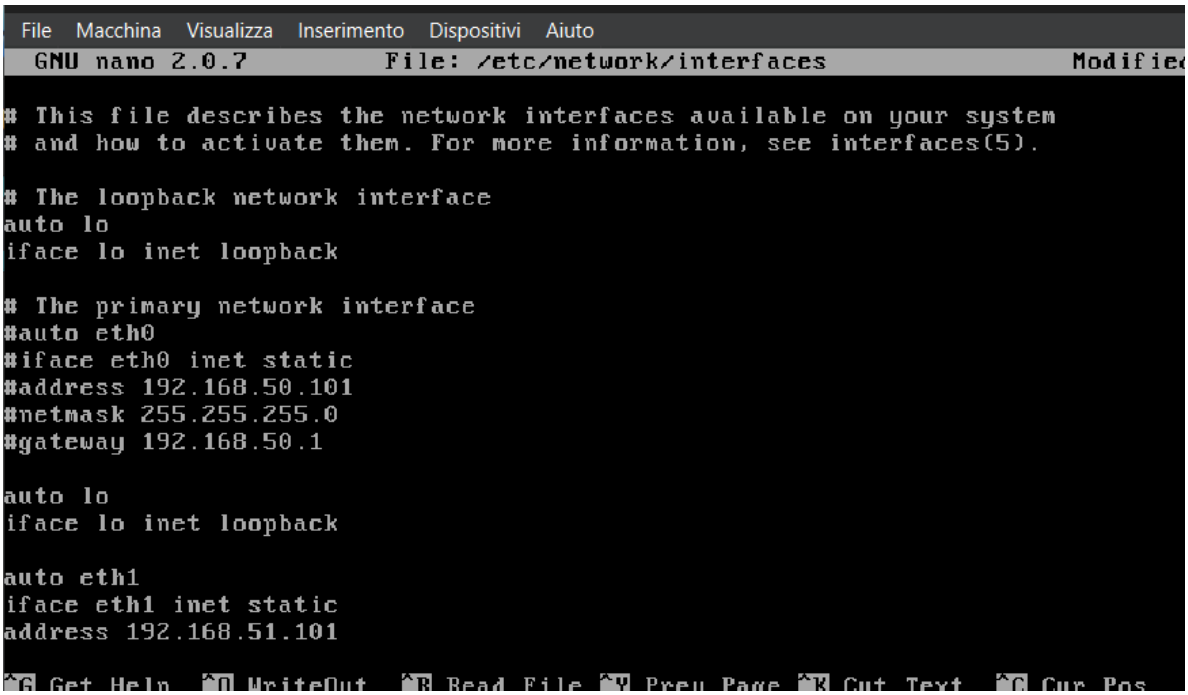


❍ LAN 2 OK

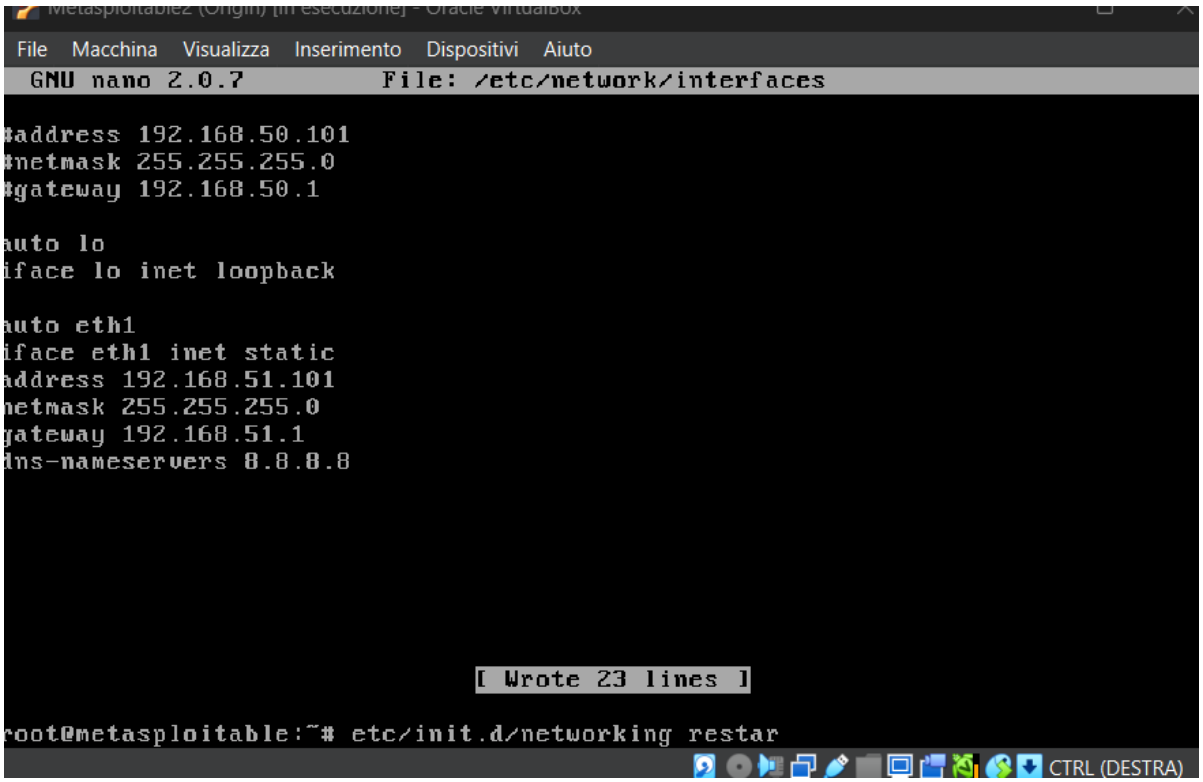
Configurazione LAN 2 su metasploitable 2

- Per attivare la LAN 2 su metasplitable2 modifico in qusto modo commentando il file

sudo /etc/network/interface



- Aggiungengo la nuova configurazione eth1 sotto eth0



- Salvo e riavvio la rete

/etc/init.d/networking restart

- Ho conferma della presenza degli IP configurati correttamente

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:38:94:a5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe38:94a5/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:54:62:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.101/24 brd 192.168.51.255 scope global eth1
    inet6 fe80::a00:27ff:fe54:629e/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

- Ora assegno manualmente gli IP nella LAN giusta perche eth0 aveva al suo interno anche 192.168.51.101 oltre a 192.168.50.101 procedendo in questo modo:

ip addr flush dev eth0
ip addr add 192.168.50.101/24 dev eth0
ip route add default via 192.168.50.1 dev eth0

ip addr flush dev eth1
ip addr add 192.168.51.101/24 dev eth1
ip route add default via 192.168.51.1 dev eth1

- Ora aggiungo la Rotta Predefinita su eth1 perche attualmente e su eth0

- Divento Root con sudo -i

- Controllo le Rotte Attuali con ip route e cerco la riga dove mi indica il defaul

```
root@metasploitable:~# ip route
192.168.50.0/24 dev eth0  proto kernel  scope link  src 192.168.50.101
192.168.51.0/24 dev eth1  proto kernel  scope link  src 192.168.51.101
default via 192.168.50.1 dev eth0
root@metasploitable:~# sudo ip route del default via 192.168.50.1 dev eth0
root@metasploitable:~# ip route
192.168.50.0/24 dev eth0  proto kernel  scope link  src 192.168.50.101
192.168.51.0/24 dev eth1  proto kernel  scope link  src 192.168.51.101
root@metasploitable:~# _
```

- Sostituendo con 192.168.51.101 in questo modo:
- Rimuovo la 50 (eventualmente)

sudo ip route del default via 192.168.50.1 dev eth0

- Aggiungola la 51

sudo ip route add default via 192.168.51.1 dev eth1

- Verifico con

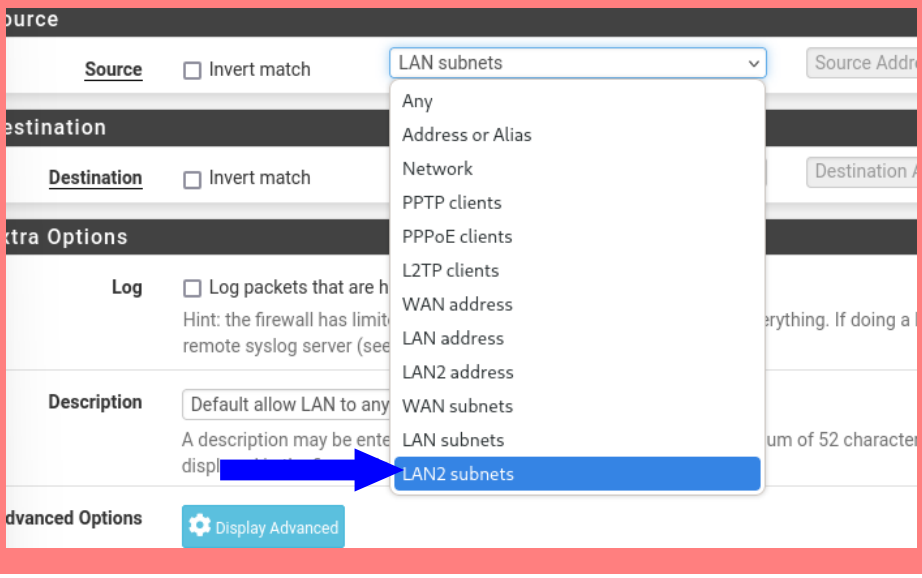
ip routr o i pr

```
msfadmin@metasploitable:~$ ip route
192.168.50.0/24 dev eth0  proto kernel  scope link  src 192.168.50.101
192.168.51.0/24 dev eth1  proto kernel  scope link  src 192.168.51.101
default via 192.168.51.1 dev eth1  metric 100
default via 192.168.50.1 dev eth0  metric 100
msfadmin@metasploitable:~$ _
```

- Ho conferma che il device è specificato sia sulle rotte che sulle default

Problema col Ping 192.168.51.101

- Non pinga 192.168.51.101 ho risolto in questo mdo
- Sono andato nel Firewall ➡ Rules ➡ LAN 2
- Nella sezione Source seleziono la LAN 2 impostata come da foto



❍ Il problema ancora non era risolto perchè avevo problemi con diversi PING:

❍ **Ping che non andavano a buon fine:**

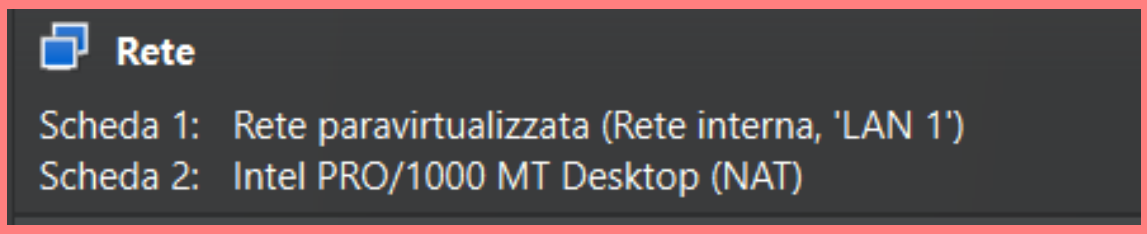
⇒ **Da Metasploitable**:
◇ 192.168.51.1 (pfSense LAN2)

⇒ **Da Kali**:
◇ 192.168.51.101 (Metasploitable su eth1, LAN2)

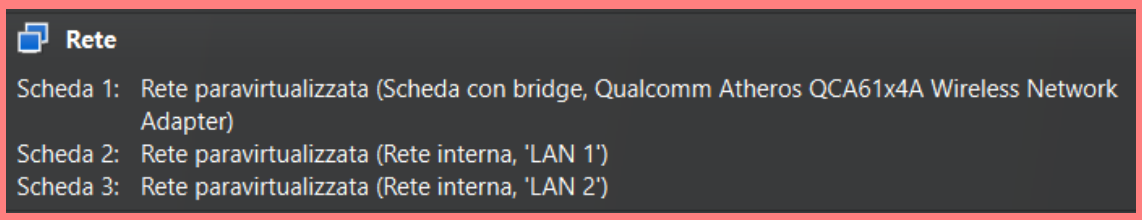
⇒ **Da pfSense**:
◇ 192.168.51.101 (Metasploitable su eth1, LAN2)

❍ **Riconfiguro le macchine in questo modo:**

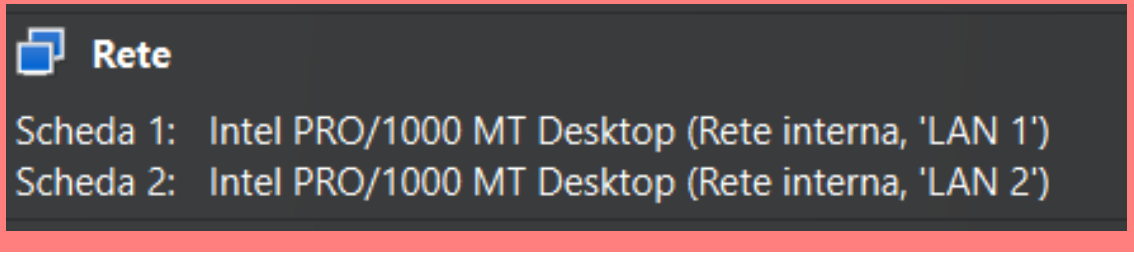
Kali



pfSsense



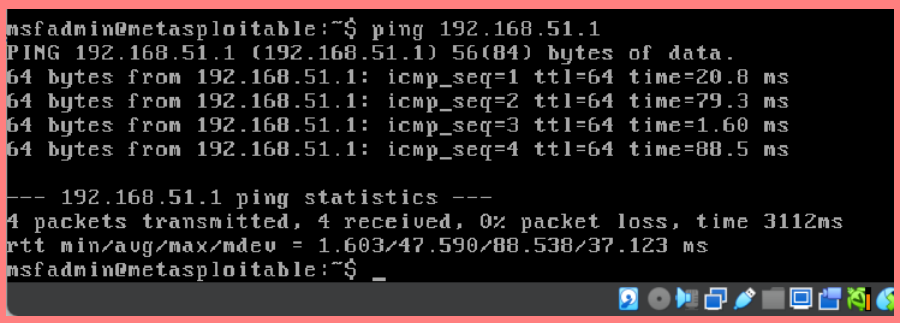
Metasploitable 2



❑ **Stato dei Ping**

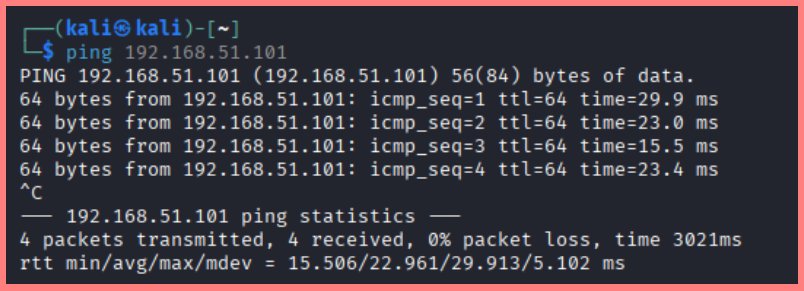
⇒ **Da Metasploitable**:

- 192.168.50.100 (Kali su LAN1)Funziona.
- 192.168.50.101 (se stesso su eth0, LAN1) Funziona.
- 192.168.50.1 (pfSense LAN1) Funziona.
- 192.168.51.101 (se stesso su eth1, LAN2) Funziona.
- 192.168.51.1 (pfSense LAN2): Funziona (ultimo aggiornamento conferma stabilità)



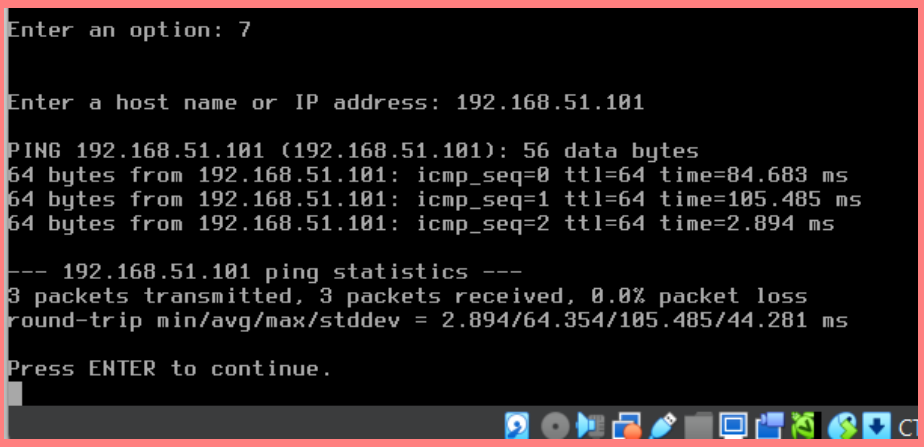
⇒ **Da Kali**:

- 192.168.50.101 (Metasploitable su eth0, LAN1) Funziona.
- 192.168.50.1 (pfSense LAN1) Funziona.
- 192.168.51.1 (pfSense LAN2) Funziona.
- 192.168.51.10 (Metasploitable su eth1, LAN2 (ultimo aggiornamento conferma stabilità)



⇒ **Da pfSense**:

- 192.168.50.101 (Metasploitable su eth0, LAN1) Funziona.
- 192.168.50.1 (se stesso su LAN1) Funziona.
- 192.168.51.1 (se stesso su LAN2) Funziona.
- 192.168.50.100 (Kali su LAN1) Funziona.
- 192.168.51.101 (Metasploitable su eth1, LAN2) (ultimo aggiornamento confer-ma stabilità)

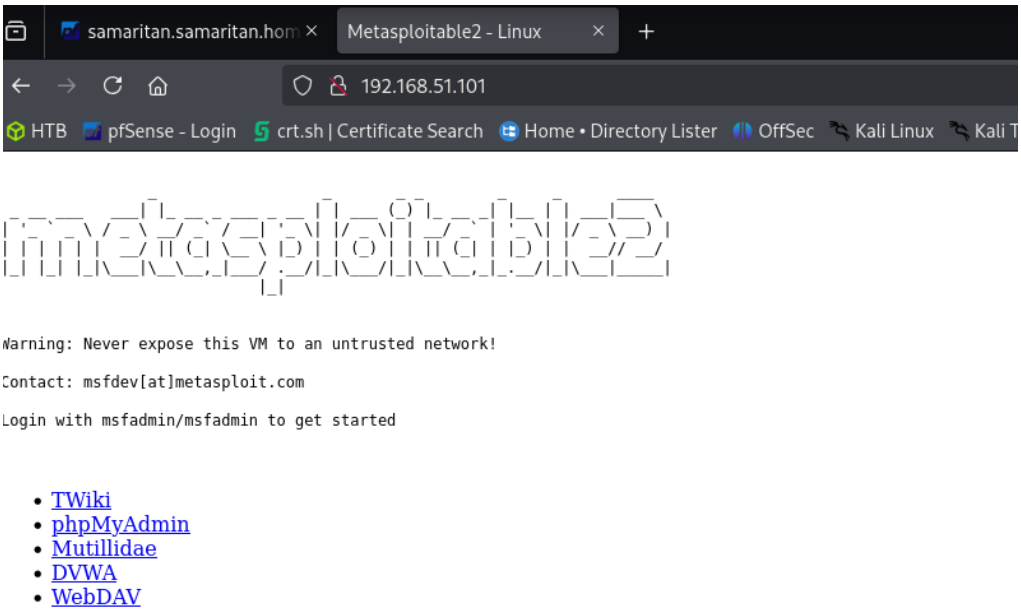


- Tutti i Ping funzionano correttamente, la connettività tra Metasploitable2, Kali e pfSense su entrambe le LAN (LAN1 e LAN2) è stabile.

- Posso procedere testando la DVWA e creando la regola firewall per bloccarlo.

Creazione regola firewall su pfSense per bloccarlo

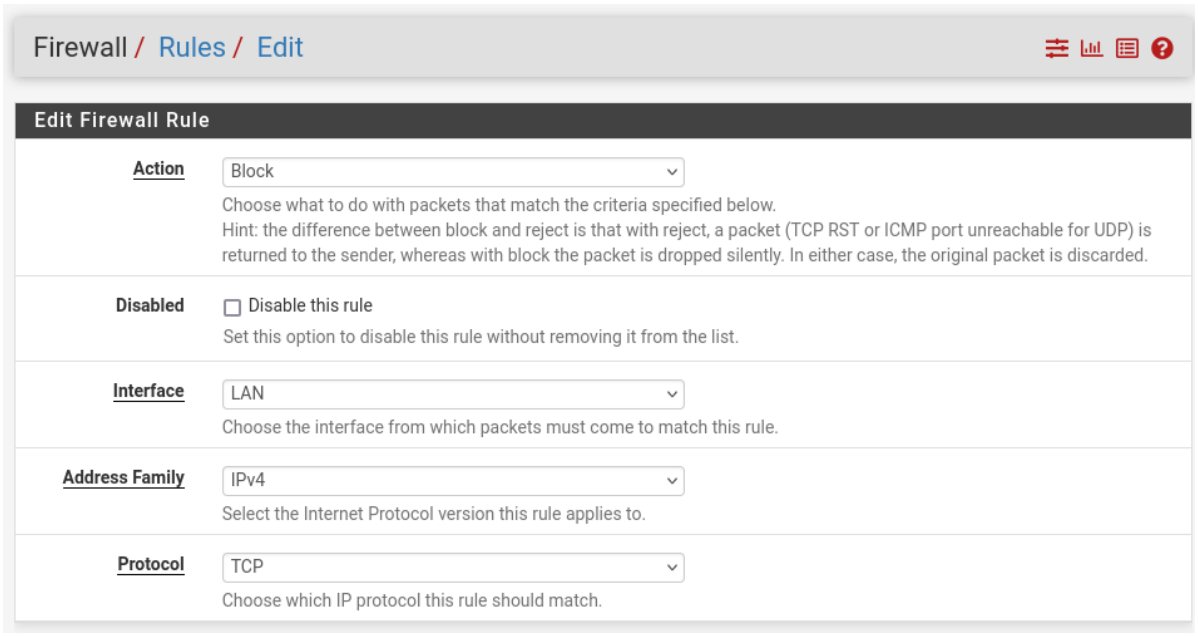
- Controllo che Kali parla con Metasploitable2

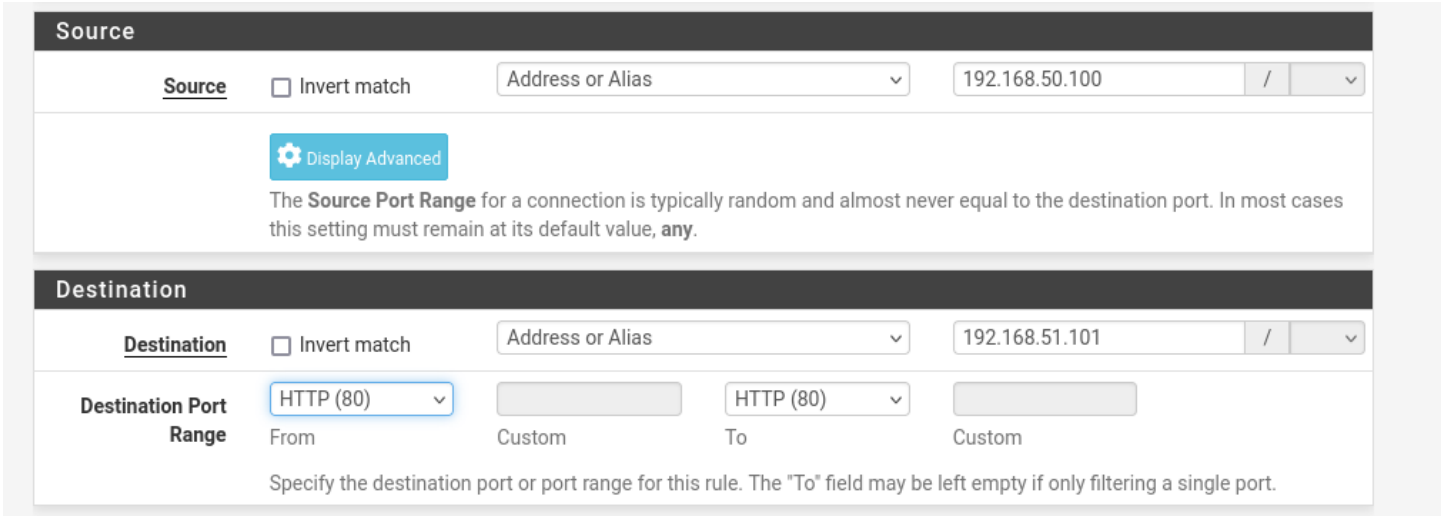


- Comunicano entrambe, proseguo

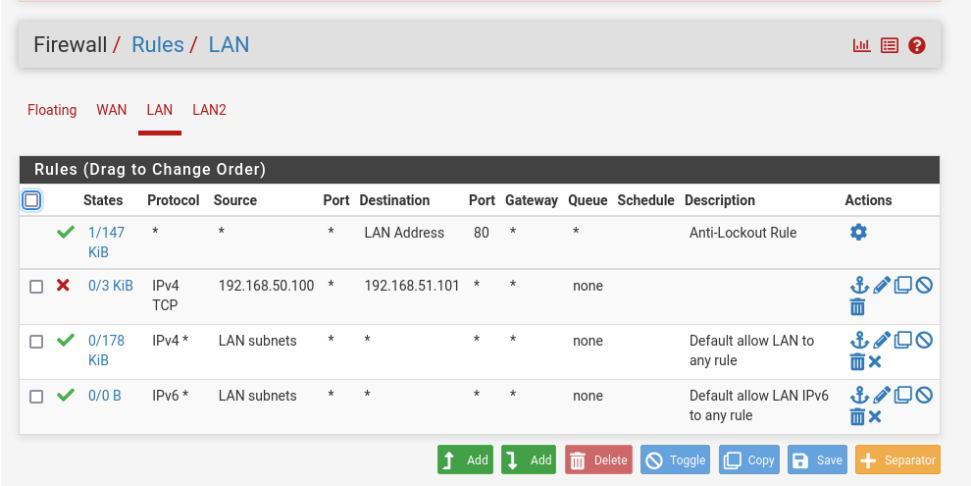
- Adesso Il firewall deve bloccare metsalploitable2 dalla kali

- Creo un nuovo edit firewall rute impostandola con i parametri che ho allegato

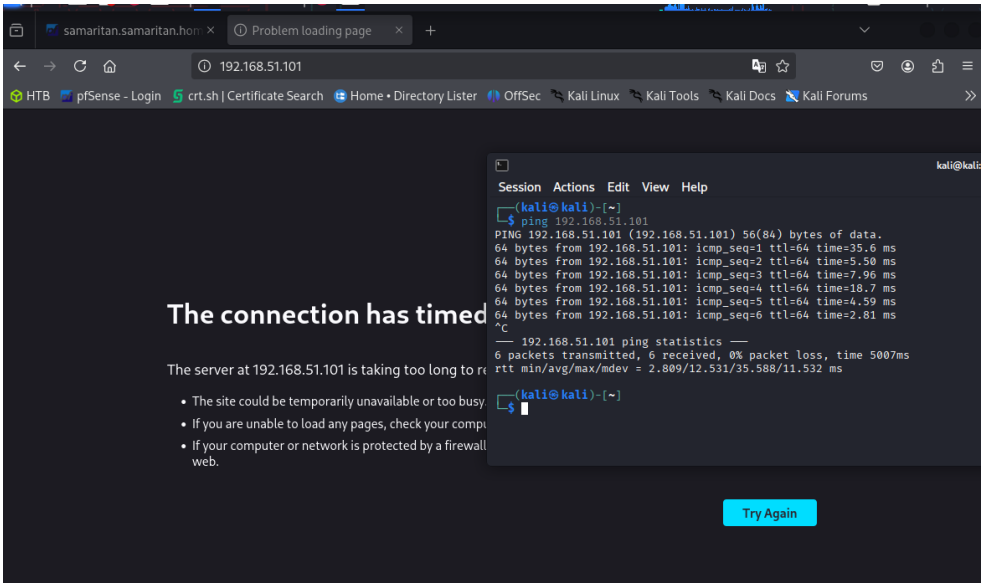




- **Verifico la nuova regola è la sposto in cima per far si che funzioni (logiche di pfSense)**



- **Salvo tutto e ricarico la pagina 192.168.51.101 per avere conferma del blocco**



- Ho conferma del funzionamento della nuova regola con la pagina che non carica e il ping continua a fuznionare.

Facoltativo

W9D4

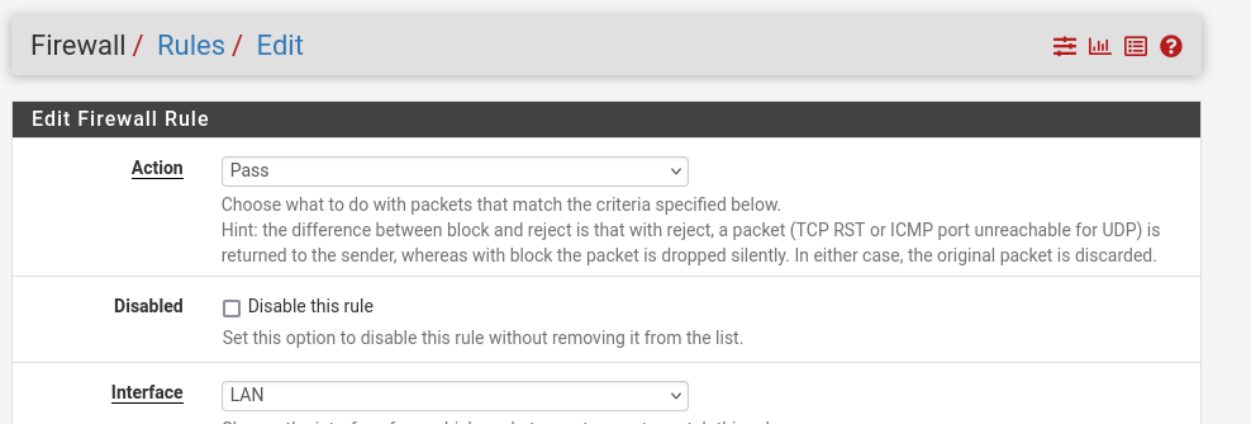
⇒ Obiettivo

- **Ispezionare i Log del Firewall**: Monitorare il traffico di rete, inclusi i ping e l'accesso a DVWA, prima e dopo la regola di blocco.

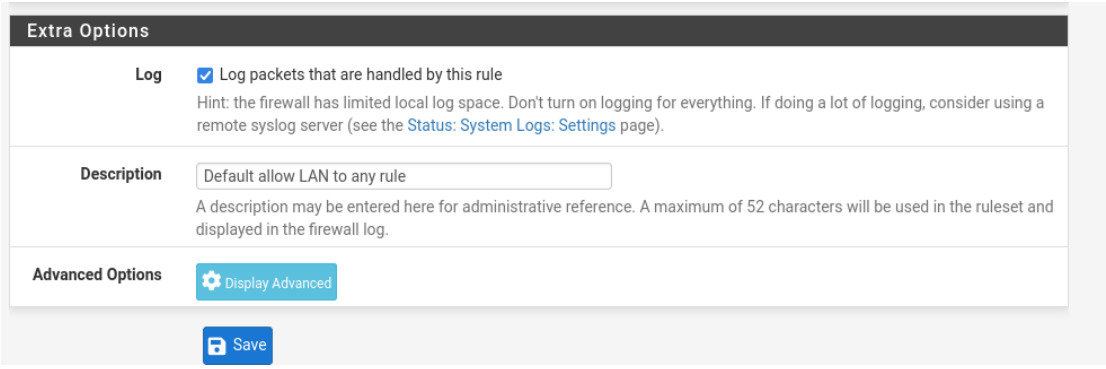
❍ Accedo alla Web GUI di pfSense aprendo un browers su Kali

- Nella barra degli indirizzi digito http://192.168.50.1 e premo invio
- Inseriaco le credeziali di accesso

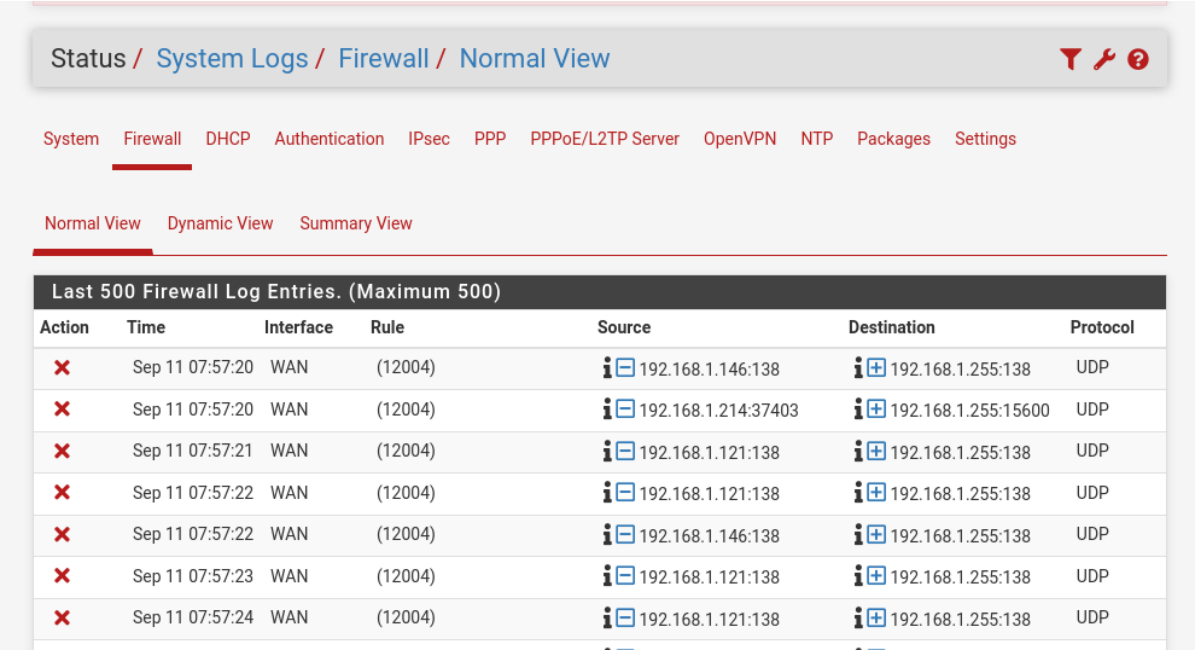
Ora vado al Log e per essere sicuro che il traffico gestito da regole specifiche venga tracciato, vado nella sezione Firewall ➡ Rules ➡ Edit



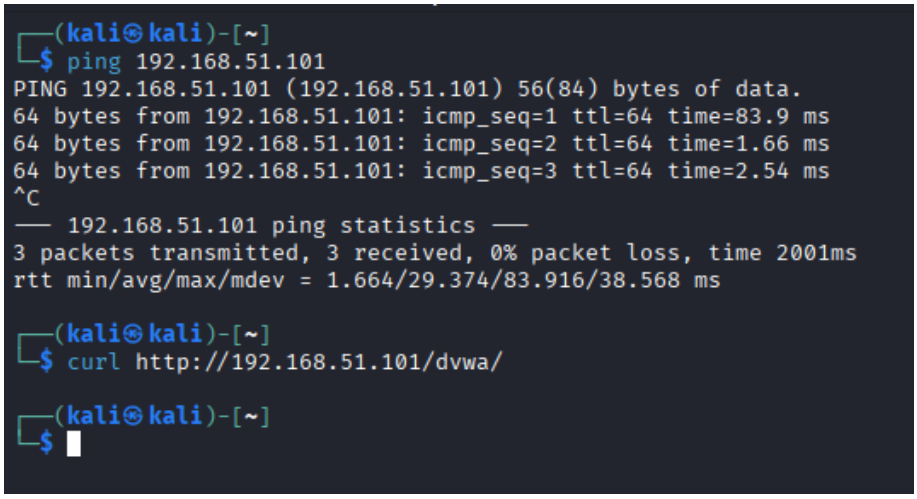
❍ Attivo Log packets that are handled by this rule



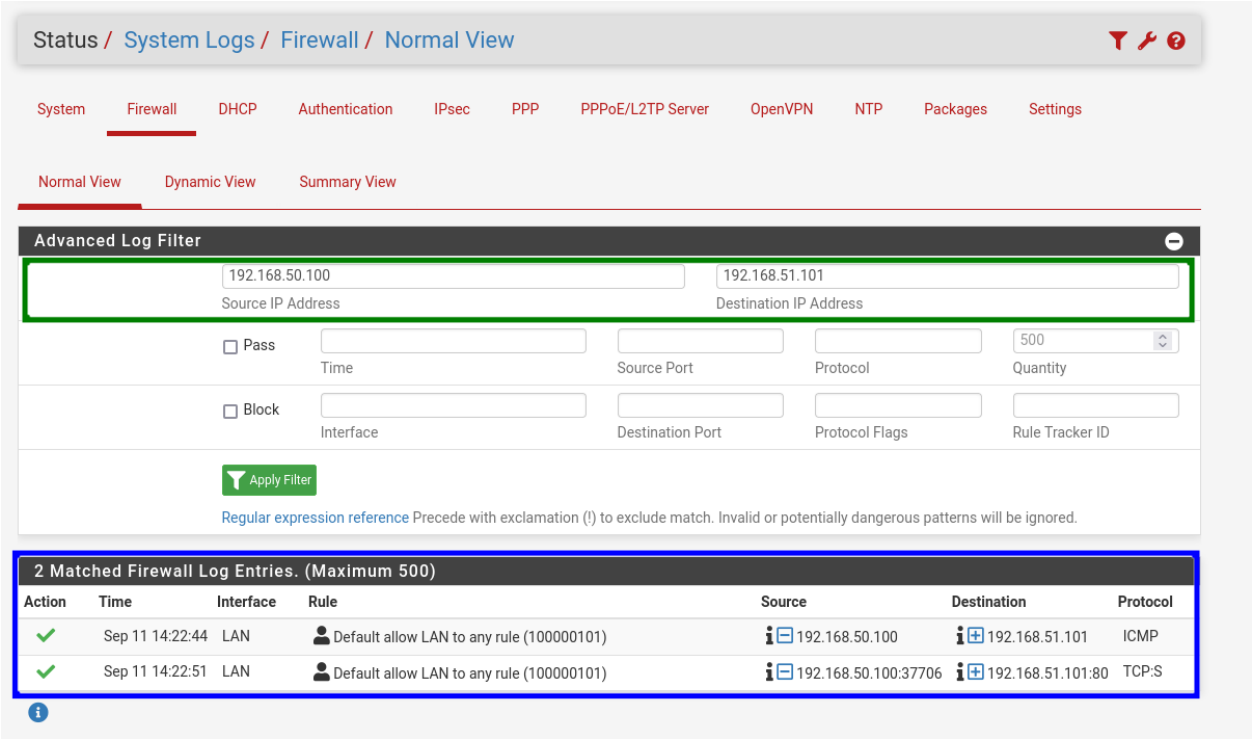
- Ora navigo ai log dei Firewall per filtrare ed ispezionare (percoso visible in foto)



- Adesso genero traffico con un ping 192.168.51.101
- Poi un curl http://192.168.51.101/dvwa/



- Ora verifico foltrando la ricerca, allego foto con dati di filtraggio e righe di LOG



❍ Analisi Righe dei Log

⇒ **1**

⇒ Sep 11 14:22:44 LAN Default allow LAN to any rule (100000101) 192.168.50.100 192.168.51.101 ICM

⇒ **Timestamp**: 14:22:44 (circa 10 minuti fa).

⇒ **Interfaccia**: LAN.

⇒ **Regola**: "Default allow LAN to any rule (100000101)" (regola predefinita che consente tutto il traffico LAN verso qualsiasi destinazione, a meno che non sia bloccato da regole specifiche).

⇒ **Source**: 192.168.50.100 (Kali).

⇒ **Destination**: 192.168.51.101 (Metasploitable su eth1, LAN2).

⇒ **Protocol**: ICMP (ping).

⇒ **Stato**: Pass (traffico consentito).

⇒ **2**

⇒Sep 11 14:22:51 LAN Default allow LAN to any rule (100000101) 192.168.50.100:37706 192.168.51.101:80 TCP:S

⇒**Timestamp**: 14:22:51 (circa 3 minuti dopo il ping).

⇒ **Interfaccia**: LAN.

⇒**Regola**: Stessa regola predefinita.

⇒**Source**: 192.168.50.100:37706 (Kali, porta sorgente 37706).

⇒**Destination**: 192.168.51.101:80 (Metasploitable, porta HTTP/DVWA).

⇒**Protocol**: TCP.

⇒**Flags**: S (SYN, indica un tentativo di stabilire una connessione TCP, probabilmente dal comando curl).

- Conclusione

  - Il ping da Kali a 192.168.51.101 è stato consentito, il che conferma che c'è una regola (o la regola predefinita) che permette il traffico ICMP.

  - Il tentativo TCP su porta 80 (da comando curl http://192.168.51.101/dvwa/) è stato registrato, ma non c'è indicazione di "PASS" o "BLOCK". Questo potrebbe significare che DVWA non è attivo o che la connessione non è stata completata (es. SYN inviato, ma nessuna risposta da Metasploitable).

  - I log sono stati generati correttamente, indicando che il logging è già attivo (probabilmente "Log packets that are handled by rules that match" è già abilitato o la regola predefinita include il logging).

- Infine come richiesto dall'esercizo ho fatto un pò di pratica per conto mio per affinare pfSene in differita per problema di tempo scadenza e consegna esame.