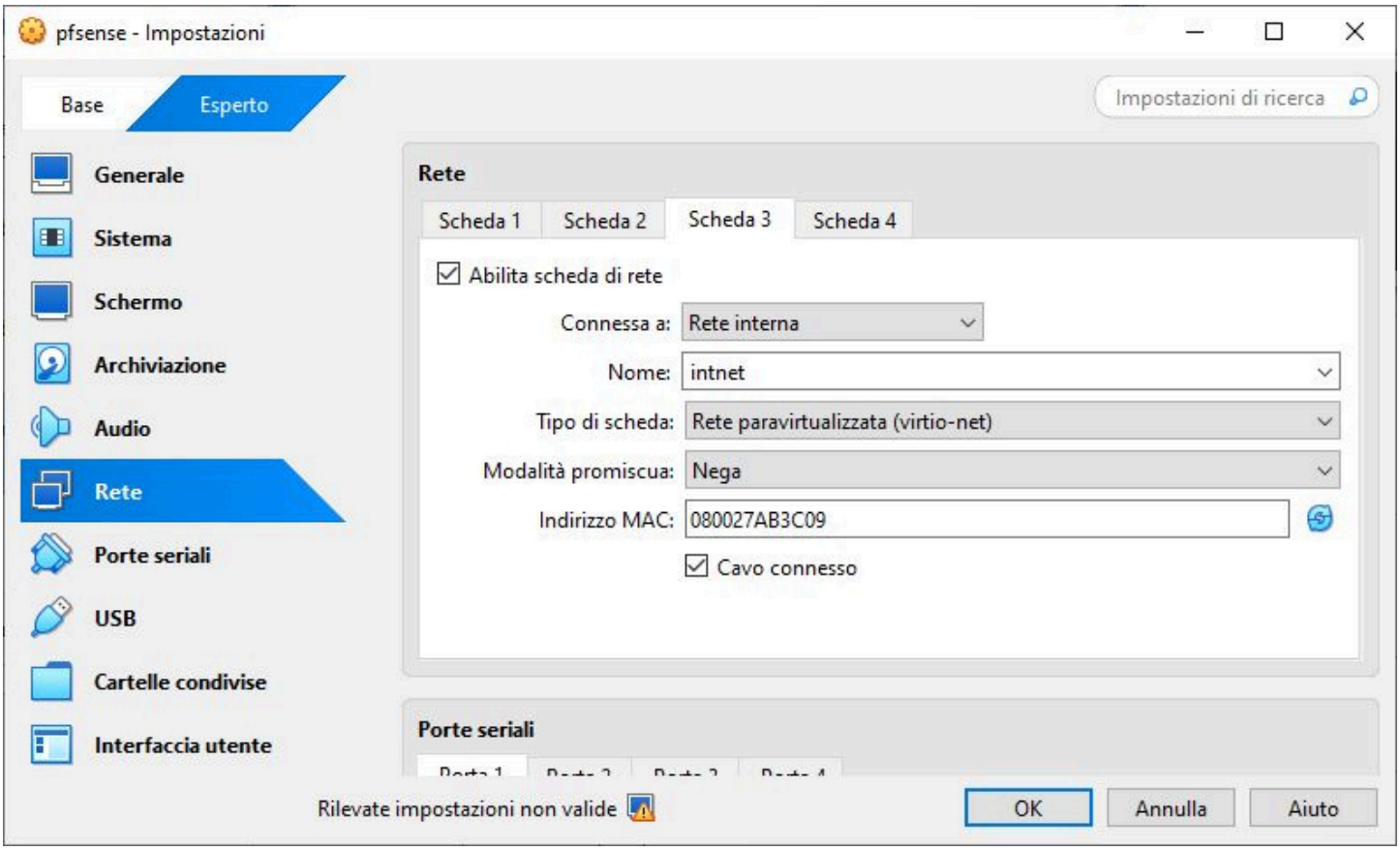
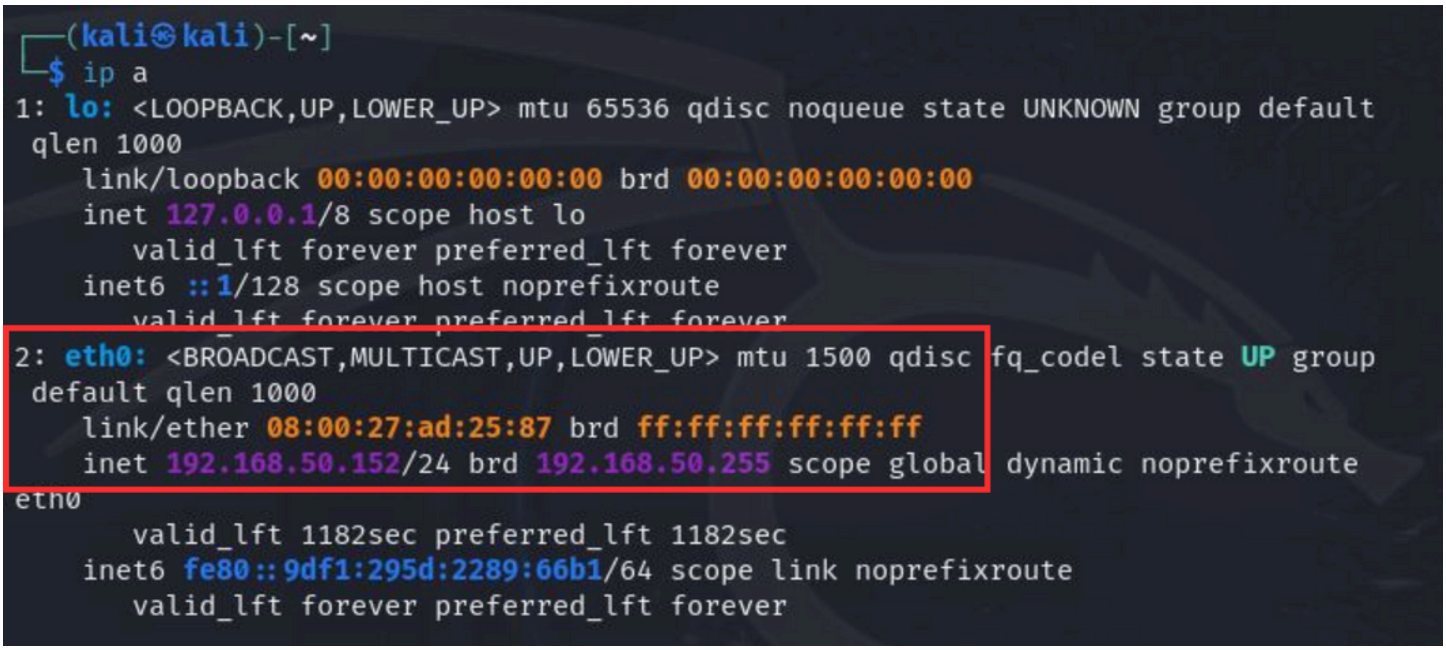
S3/L5 pfSense e DVWA

Il laboratorio di oggi richiedeva di configurare una nuova regola sul firewall pfSense per bloccare l'accesso alla DVWA su macchina virtuale metasploitable2 dalla macchina virtuale Kali Linux.

Ho modificato le impostazioni della macchina virtuale pfSense, abilitando una nuova scheda di rete, con impostazione rete interna.



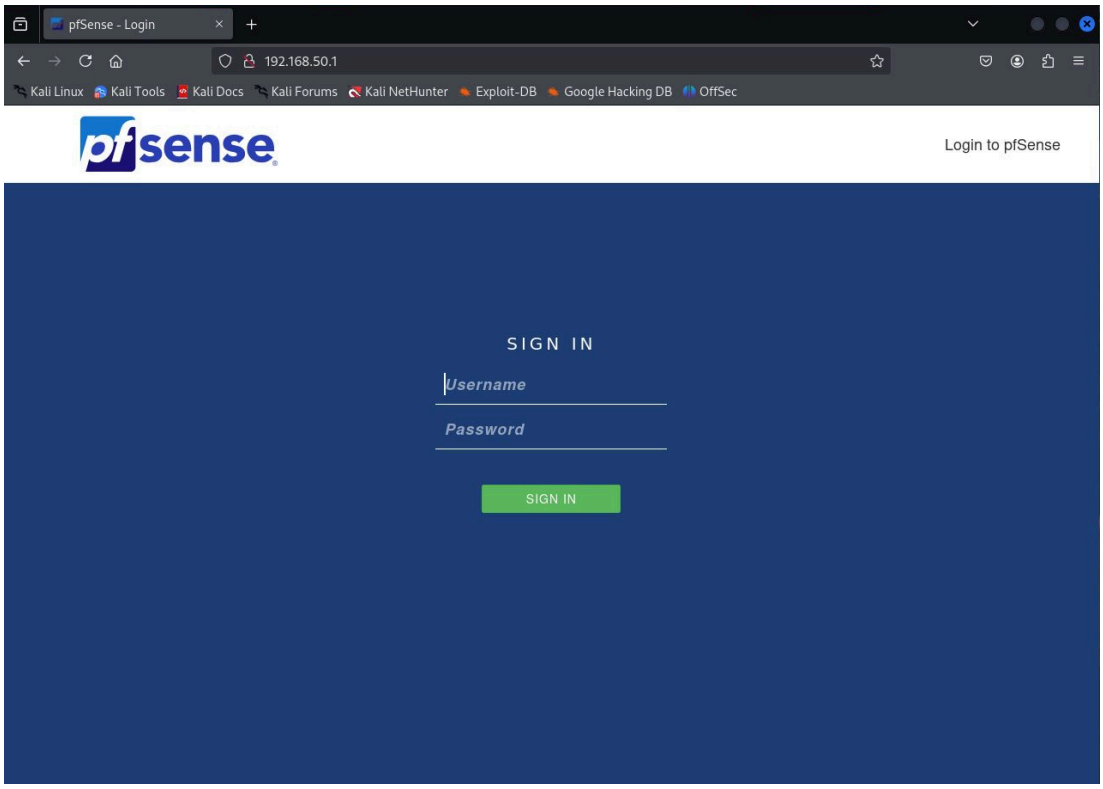
Ho avviato quindi tutte e tre le macchine virtuali (Kali Linux, pfSense e metasploitable2) ed impostato ad ogni macchina le proprie configurazioni di rete. Come mostrano le schermate seguenti, le macchine Kali e Metasploitable2 sono in due reti diverse come richiesto.



```
The IPv6 OPT1 address has been set to dhcp6

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 5ba1eadb67ddb362c364

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

WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
                                 v6/DHCP6: fd00::a00:27ff:fe98:d60/64
LAN (lan)       -> vtnet0     -> v4: 192.168.50.1/24
LAN2 (opt1)     -> vtnet1     -> v4: 192.168.40.1/24

 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
```

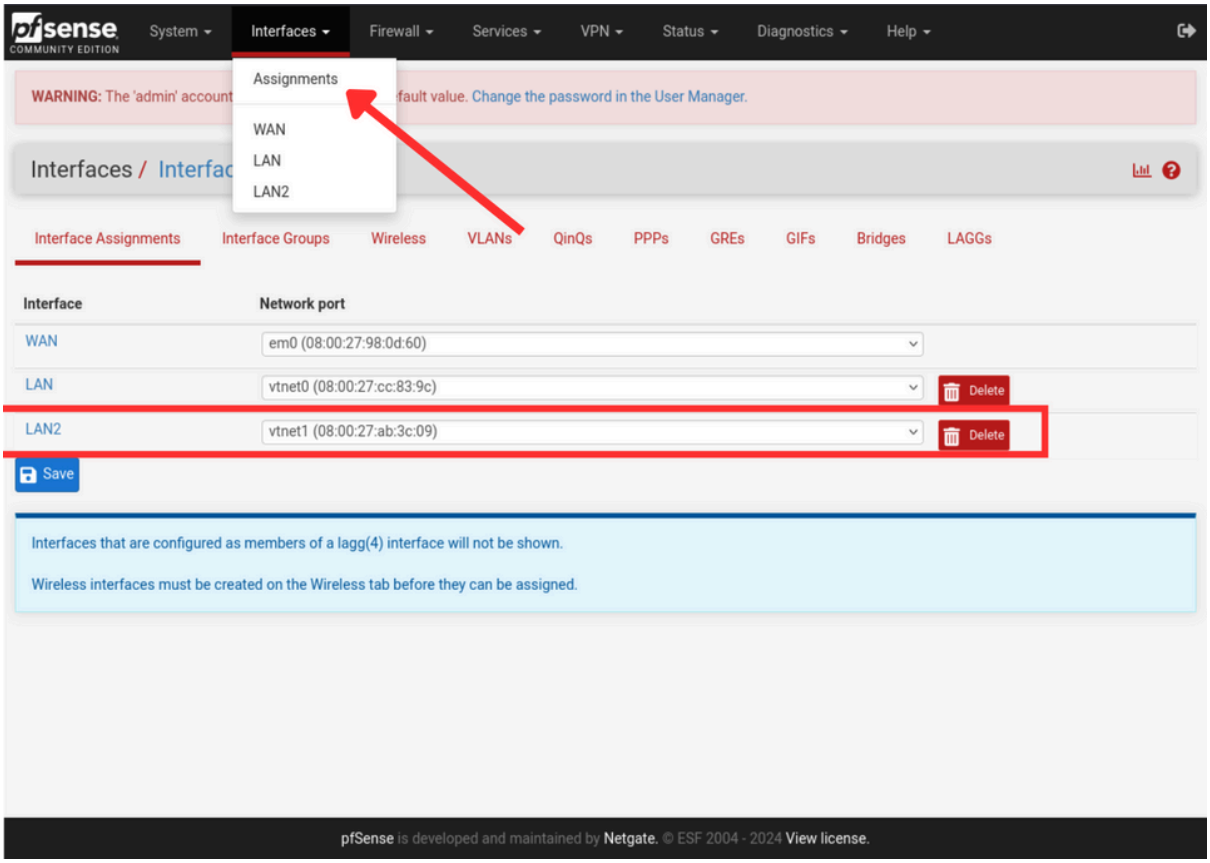
```
eth0      Link encap:Ethernet  HWaddr 08:00:27:6d:4b:19
          inet addr:192.168.40.153  Bcast:192.168.40.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6d:4b19/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1579 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1533 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:220855 (215.6 KB)  TX bytes:358727 (350.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2919 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2919 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1407133 (1.3 MB)  TX bytes:1407133 (1.3 MB)

msfadmin@metasploitable:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.40.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.40.1    0.0.0.0         UG    0      0        0 eth0
```

Tramite Kali Linux ho eseguito l'accesso all'interfaccia di configurazione di pfSense, collegandomi col browser web all'indirizzo IP della macchina virtuale pfsense 192.168.50.1.

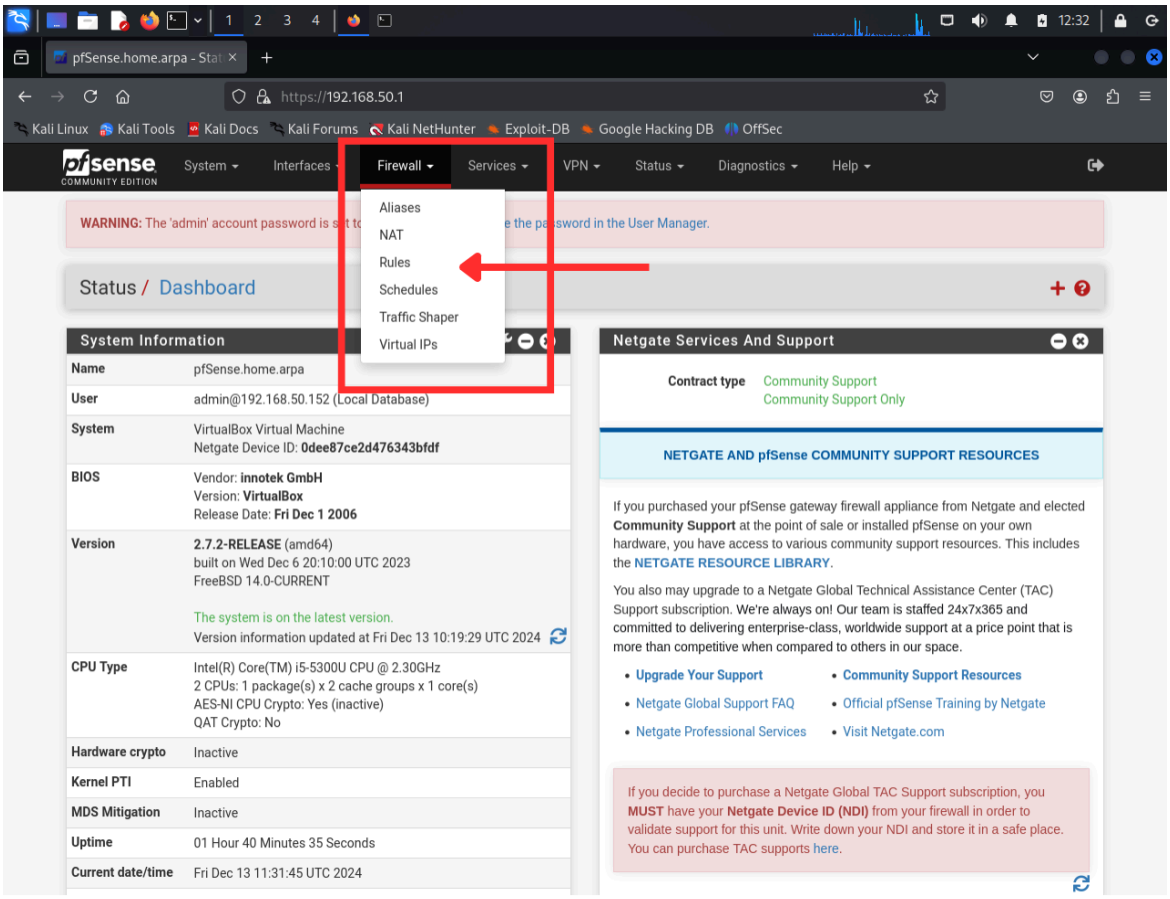


Ho inserito i valori di default “admin” per l’username e “pfsense” per la password. In questo modo sono entrato nell’interfaccia grafica di pfSense per eseguire le configurazioni richieste.

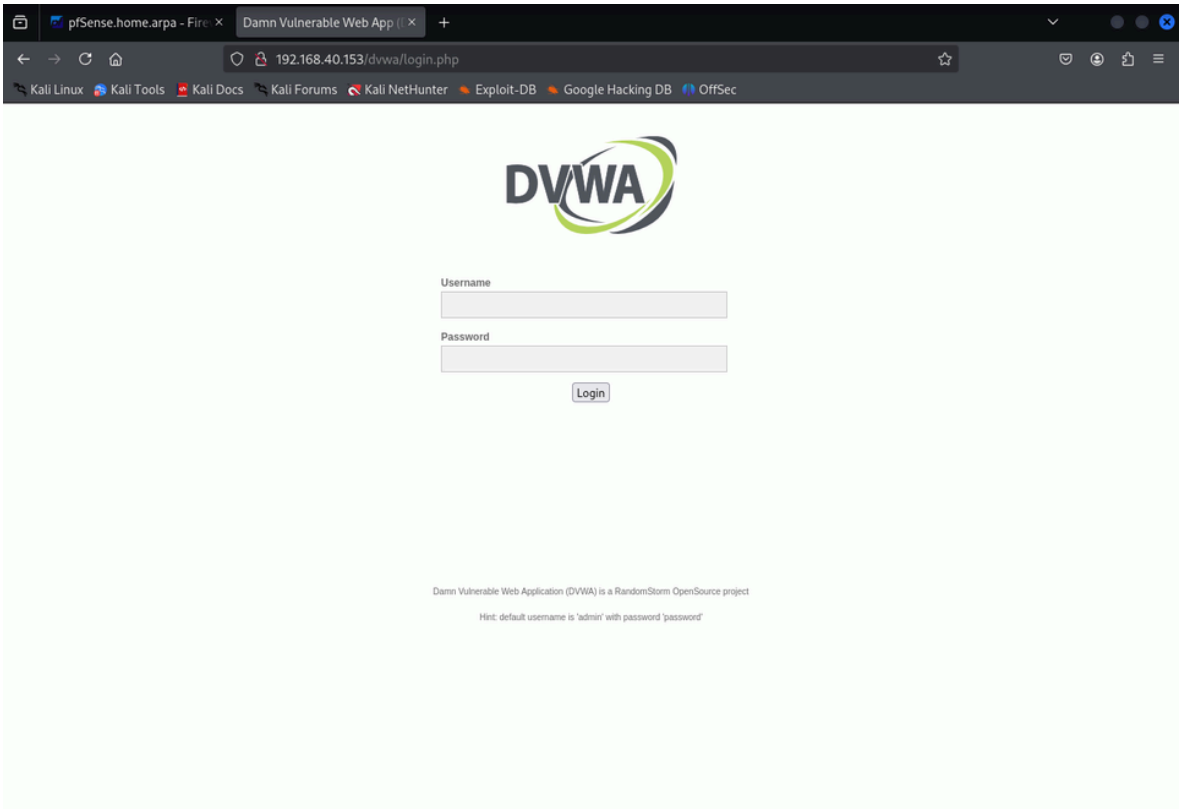
Entrando nella sezione interfacce > assignments, ho aggiunto la seconda rete che ho rinominato LAN2,



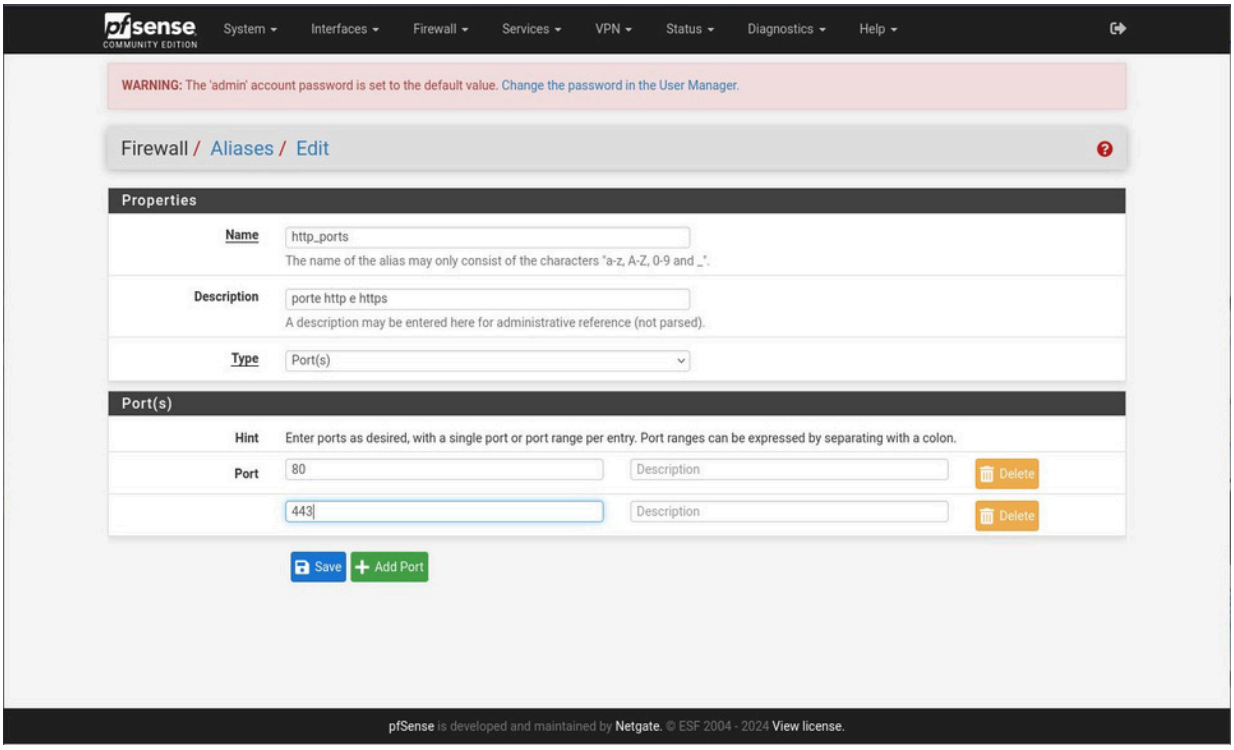
Per aggiungere una nuova regola, sono andato nella sezione Firewall > Rules.



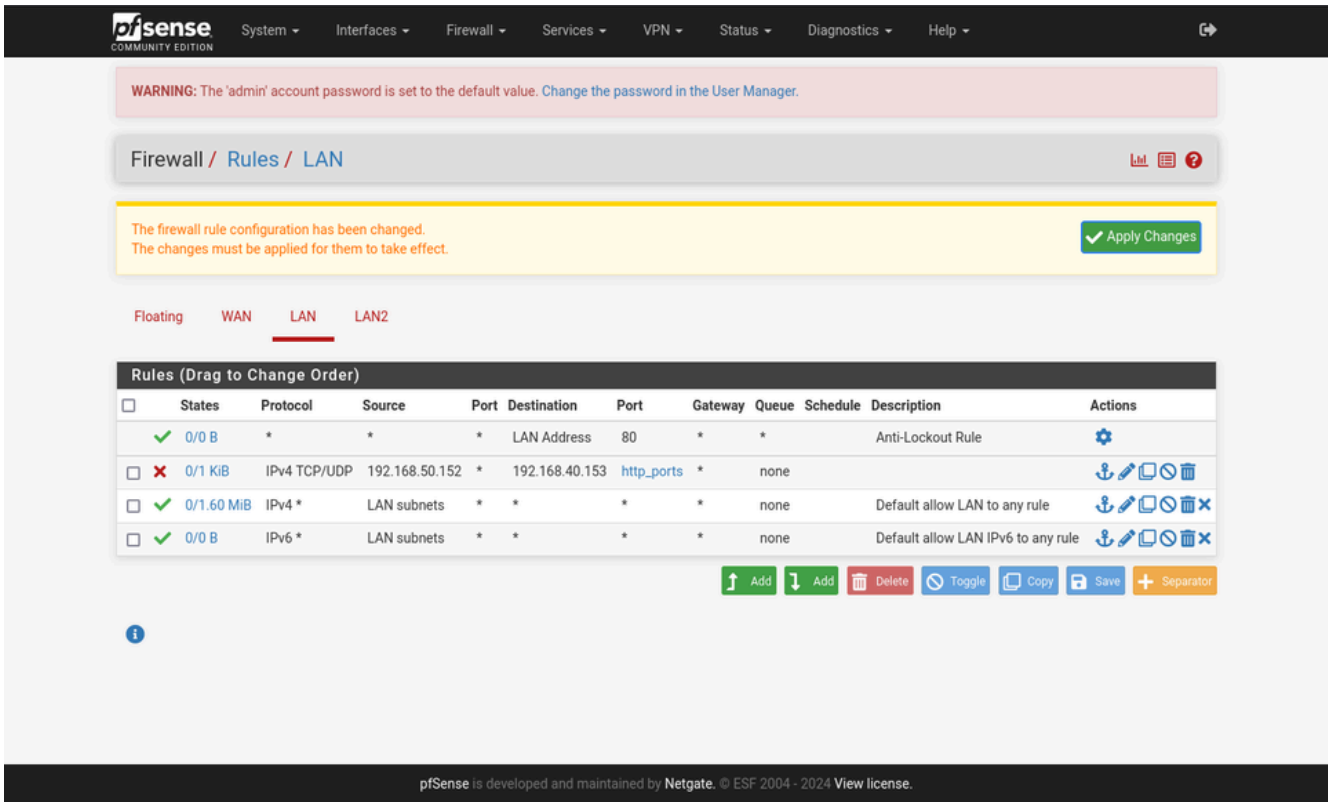
Lo screen mostra che prima dell'applicazione della regola, la connessione tra la macchina Kali Linux e DVWA su Metasploitable2 avviene correttamente:



Per comodità ho creato un alias per le porte 80 e 443 dei protocolli HTTP e HTTPS per configurare al meglio la regola.

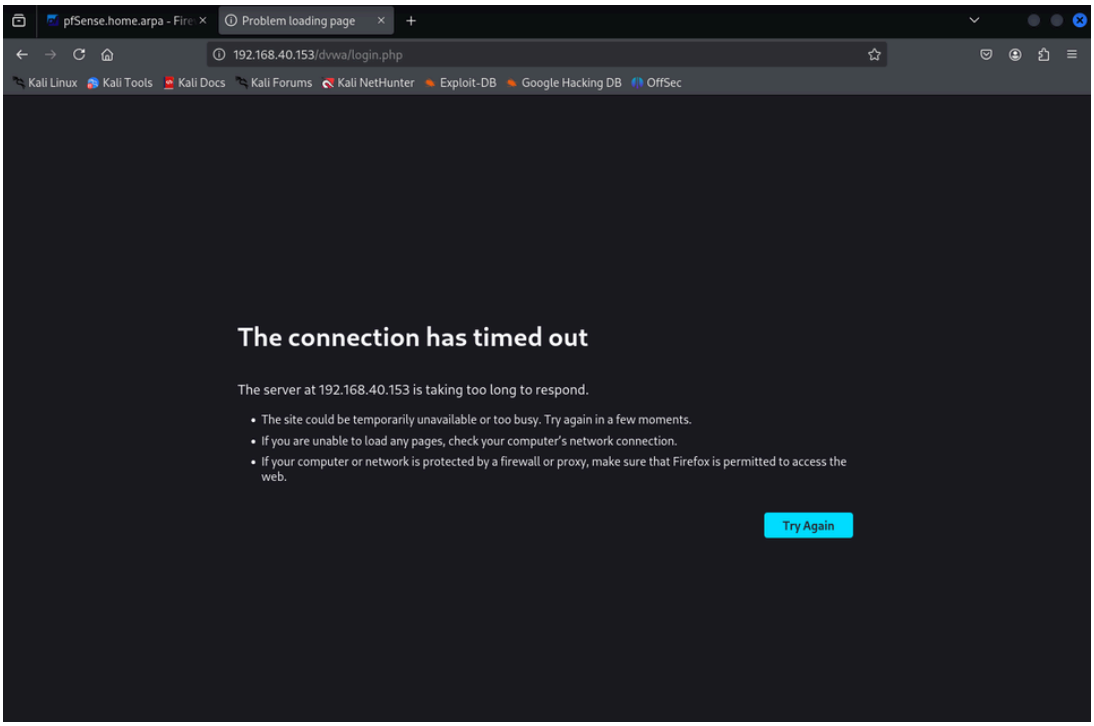


Ho creato una nuova regola nella sezione LAN, che impedisce la connessione in uscita dalla sorgente 192.168.50.152 (macchina Kali Linux) alla DVWA Metasploitable2 tramite i protocollo HTTP/HTTPS (porte 80 e 443).



La regola è posta in alto poiché le policy sono applicate con un approccio top-down quindi viene applicata la prima regola che matcha con la connessione.

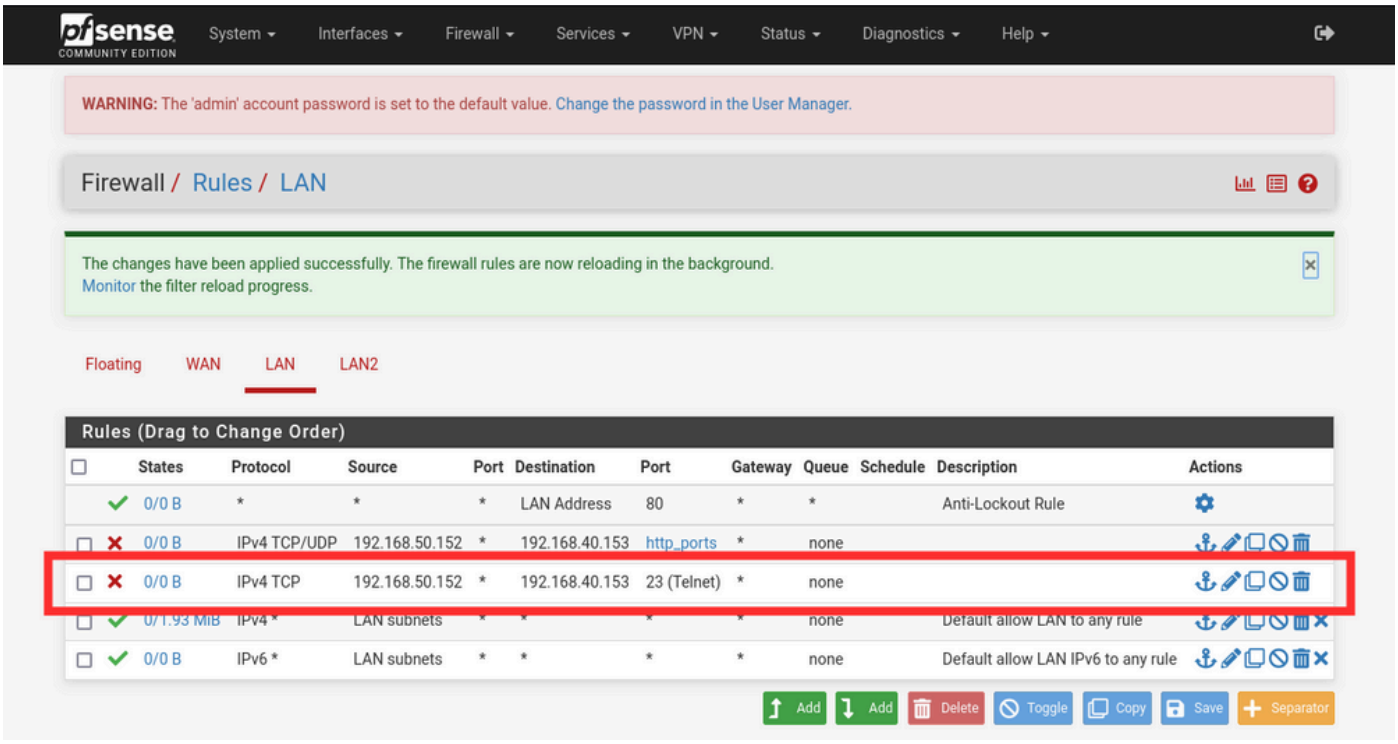
L'immagine mostra che dopo l'applicazione della regola, il firewall blocca la connessione tra la macchina Kali Linux e DVWA su metasploitable2.



Bonus: bloccare Telnet con firewall pfSense

L'esercizio bonus chiedeva di creare una nuova regola che impedisse la connessione tramite Telnet da Kali Linux a Metasploitable2.

Telnet è un protocollo non sicuro per l'accesso remoto ad una macchina. Non è sicuro poiché trasmette tutto in plaintext, senza alcuna crittografia ed è stato sostituito da protocolli più sicuri come SSH. Poiché il protocollo Telnet lavora sulla porta 23 di default, ho implementato una regola simile alla precedente, che però blocca il traffico sulla porta 23 della macchina Metasploitable2.



In questo modo, il Firewall impedirà ogni connessione sul protocollo Telnet tra le due macchine.