Lezione S3/L5

pfsense Firewall

Nel laboratorio di oggi dovevamo creare una regola Firewall da pfsense, questo ha richiesto innanzitutto il download del file iso e il setup della macchina virtuale per pfsense.

PRE- REQUIREMENT

Personalmente ho sempre utilizzato VMware come macchina virtuale ma il processo di installazione fallisce a causa di “mancanza di file login in” , è necessario avere virtualbox.
Quindi procedo alla installazione di virtual box , e scarico il file iso da internet.
A questo punto creo una nuova virtual box con il file iso e presto attenzione ad impostare:

- sistema operativo= FreeBSD

- rete:
  - scheda 1 = NAT
  - scheda 2 = Rete interna
  - scheda 3= Rete interna

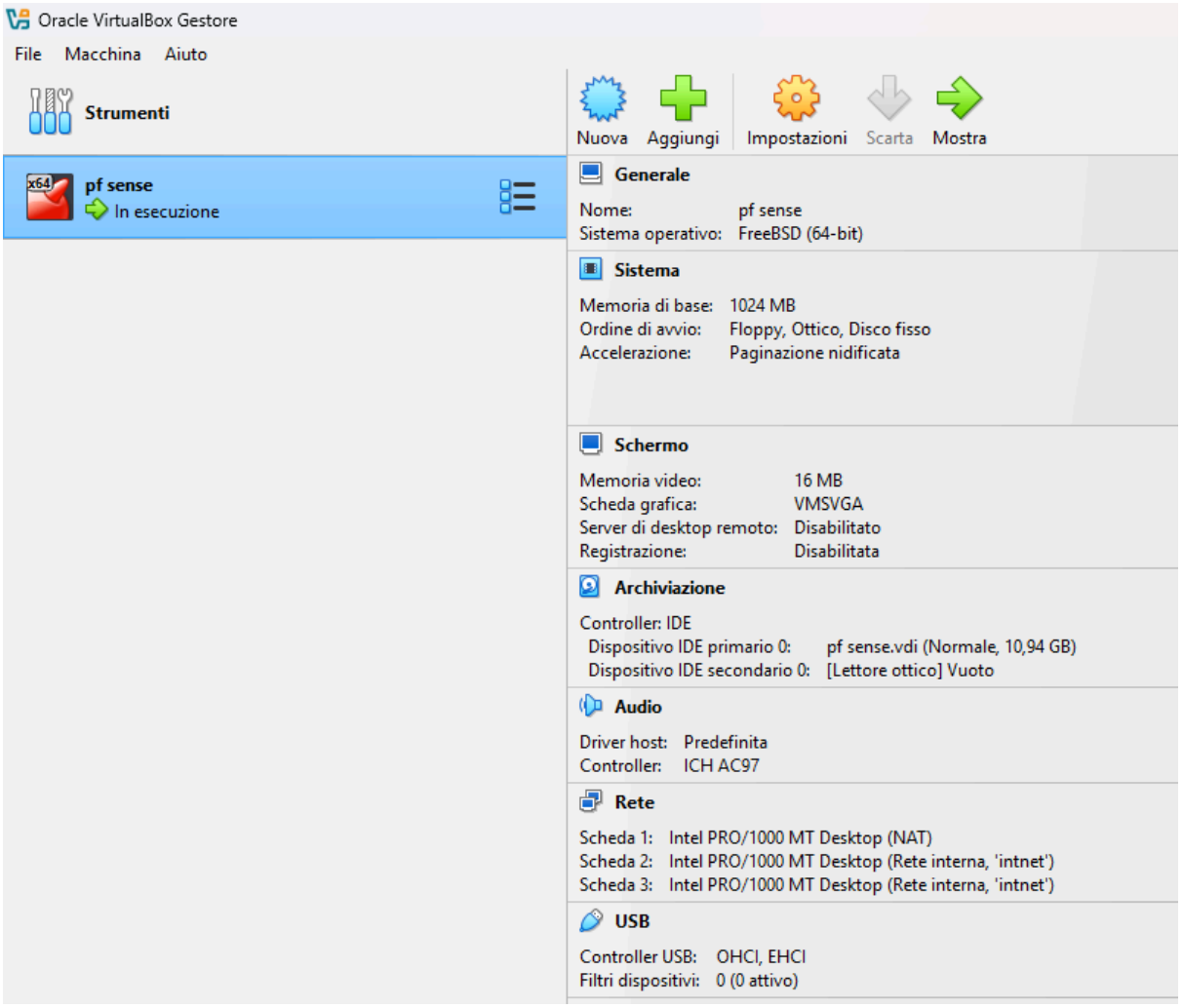


figura 1: impostazioni pfsense.

A questo punto accendo la macchina e seguo le impostazioni di installazione. a fine installazione devo però assicurarmi di rimuovere il file ISO e riavviare la macchina(figura 2)

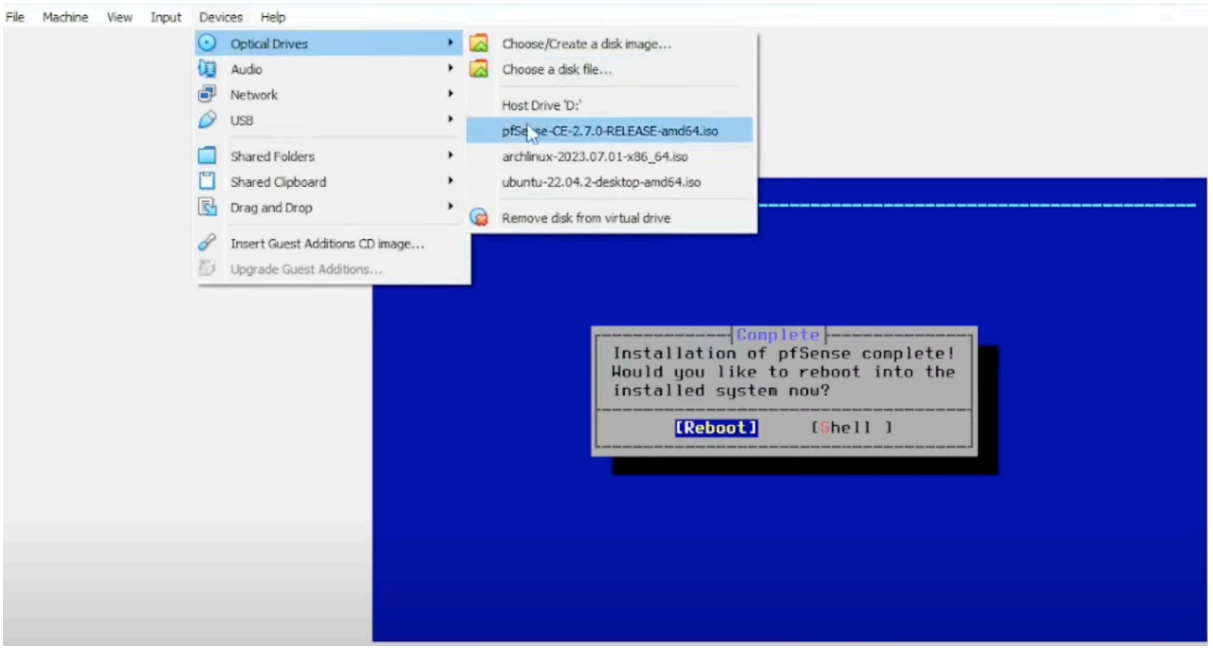


figura 2: rimozione .iso

Accendendo ora la macchina sono portato sulla schermata principale(figura 3).

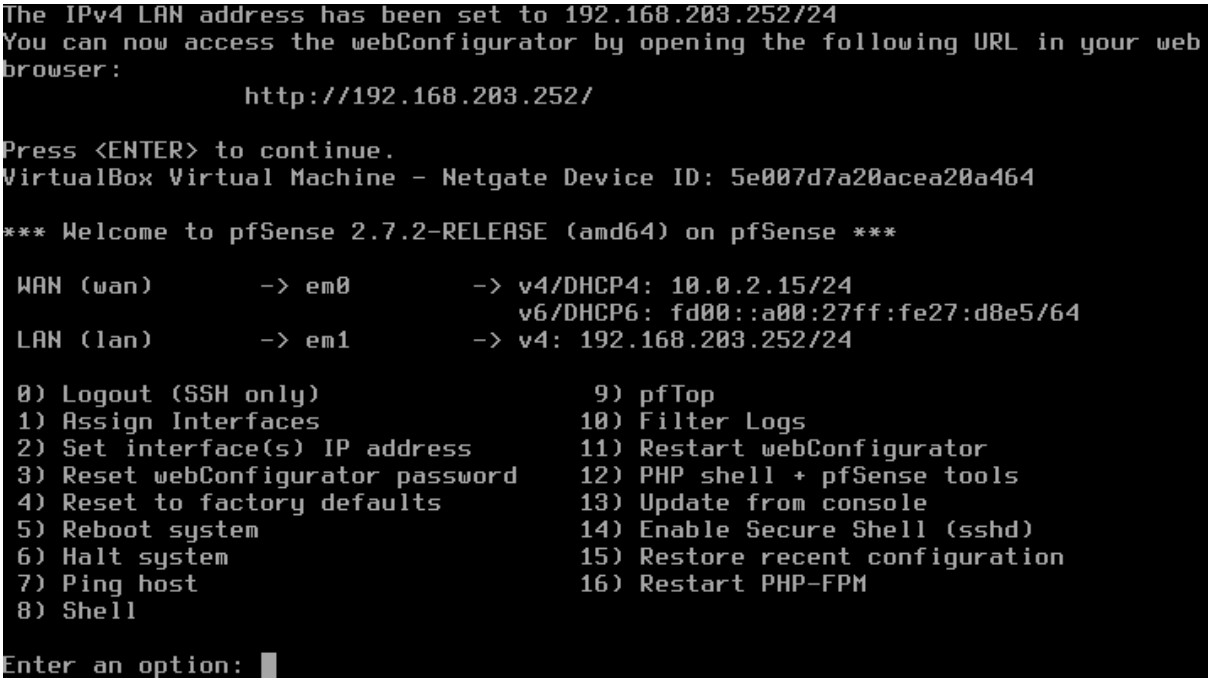


figura 3: schermata pfsense.

Possiamo ora accendere kali linux sulla stessa macchina virtuale e digitare l'indirizzo ip nel browser. dobbiamo switchare la rete da NAT a rete interna quando kali è attivo dopo pfsense ed otteniamo con ip a.

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 g
roup default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.0/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 192.168.2.3/24 brd 192.168.2.255 scope global dynamic noprefixroute
eth0
       valid_lft 6998sec preferred_lft 6998sec
    inet6 fe80::a92d:2b52:5481:d0c5/64 scope link noprefixroute
```

figura 4: kali browser.

una volta acceduti con le classiche credenziali “admin” e “pfsense” possiamo accedere alla schermata principale ed iniziare l’esercizio

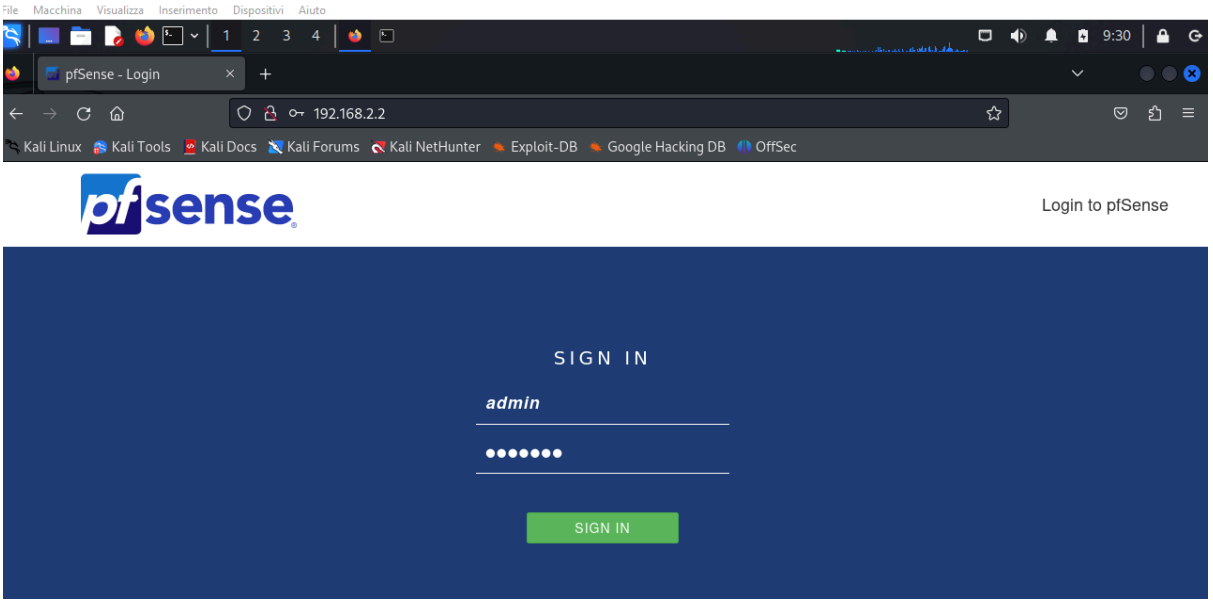


figura 5: schermata principale.

ESERCIZIO

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):

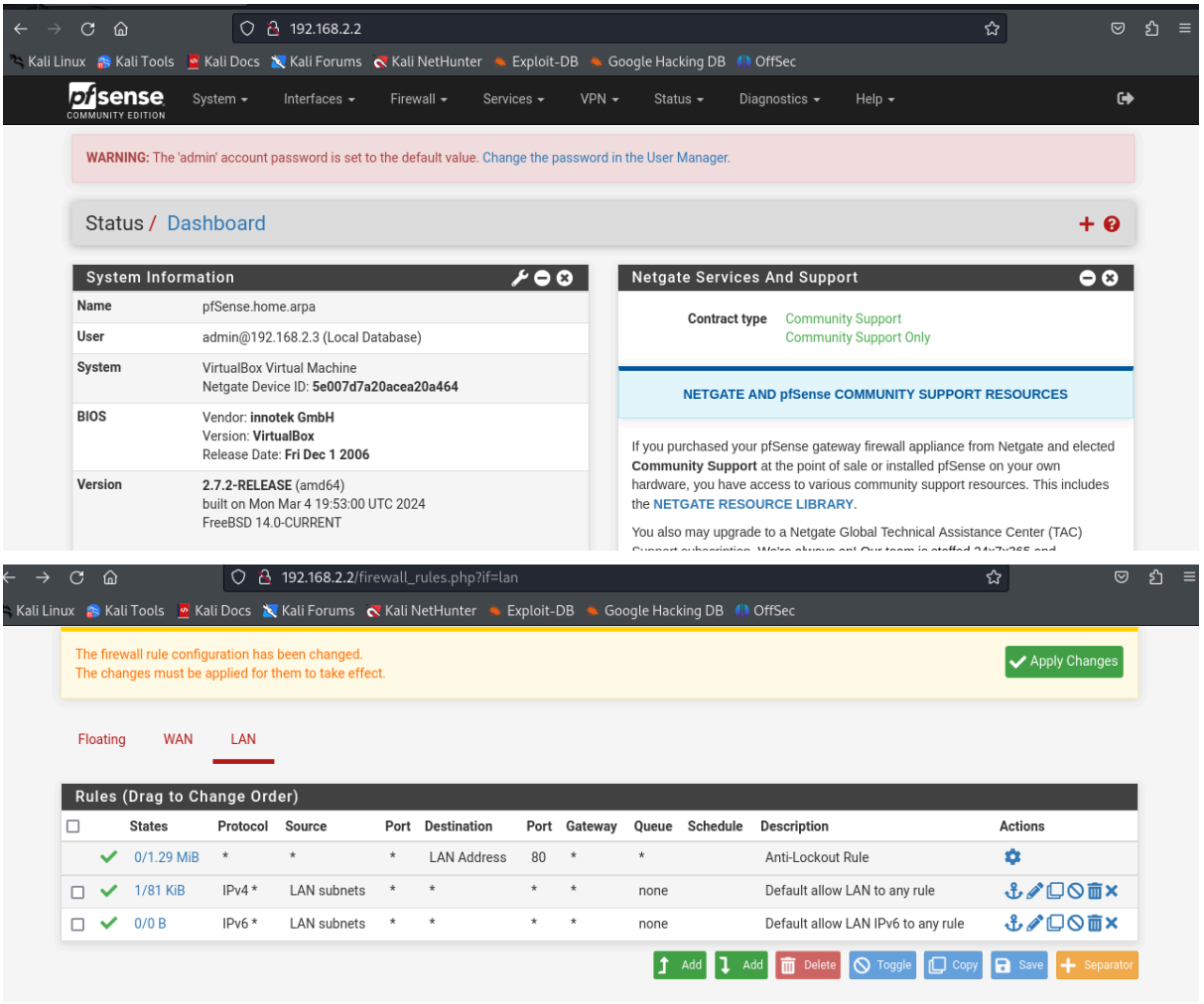


figura 6: schermata principale e add

Dobbiamo ora 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. Aggiungiamo ora una nuova interfaccia di rete a Pfsense in modo tale da gestire un'ulteriore rete. Connettiamoci poi in Web Gui per attivare la nuova interfaccia e configurarla.

accendiamo metasploitable 2 ed avviamo la macchina su reti diverse verificando che funziona correttamente

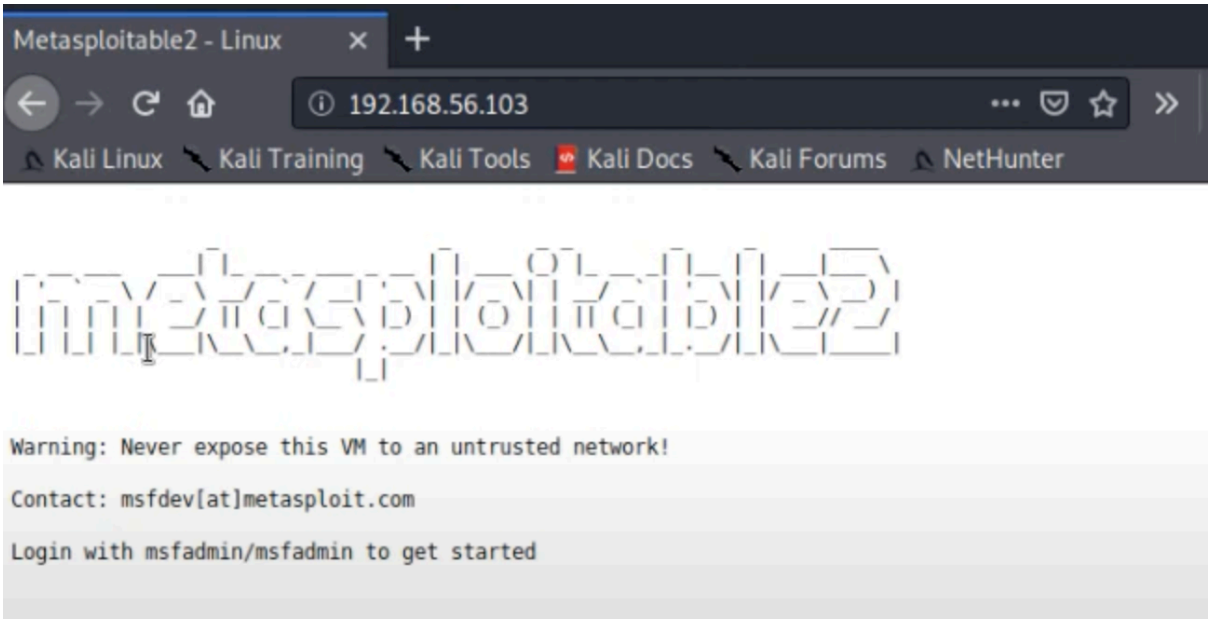


figura 7 : metasploit working

aggiungiamo ora la regola con l'indirizzo ip di metasploit per bloccare l’accesso.

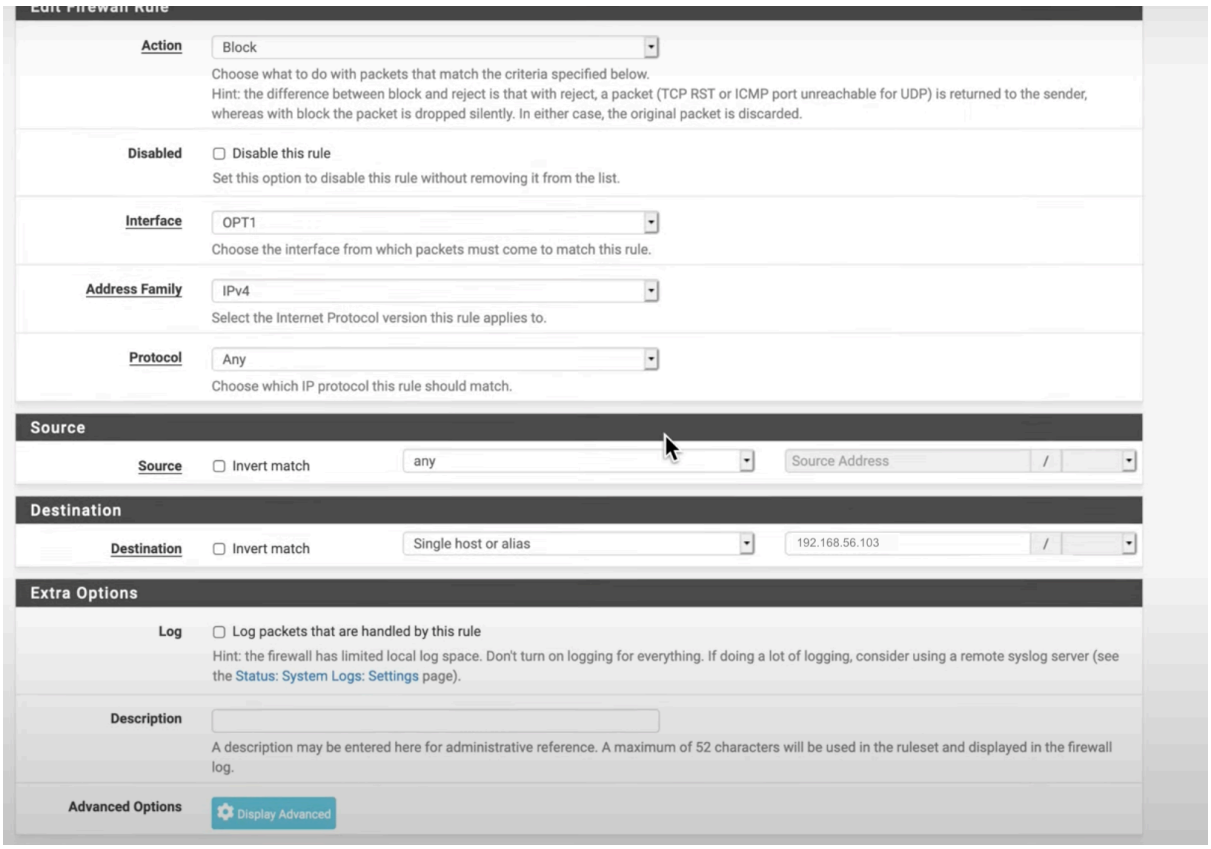
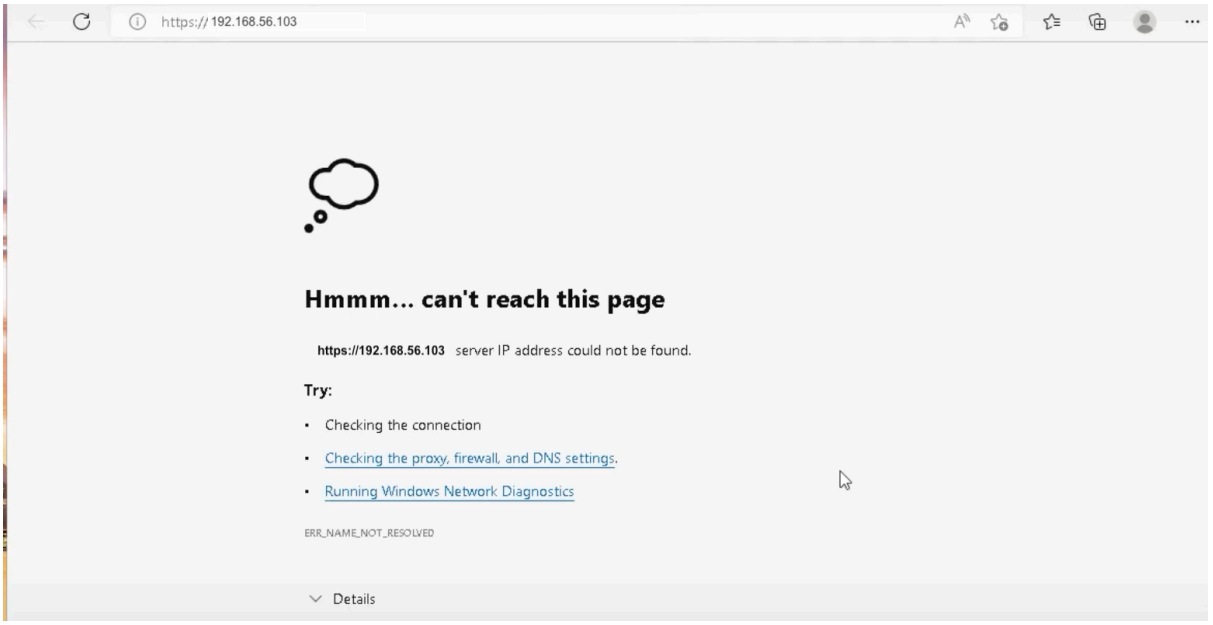


figura 8 : firewall rule

specificando l’indirizzo ip della macchina e verifichiamo che la macchina non si connette.


https:// 192.168.56.103
Hmmm... can't reach this page
https://192.168.56.103 server IP address could not be found.
Try:
Checking the connection
Checking the proxy, firewall, and DNS settings.
Running Windows Network Diagnostics
ERR_NAME_NOT_RESOLVED
Details