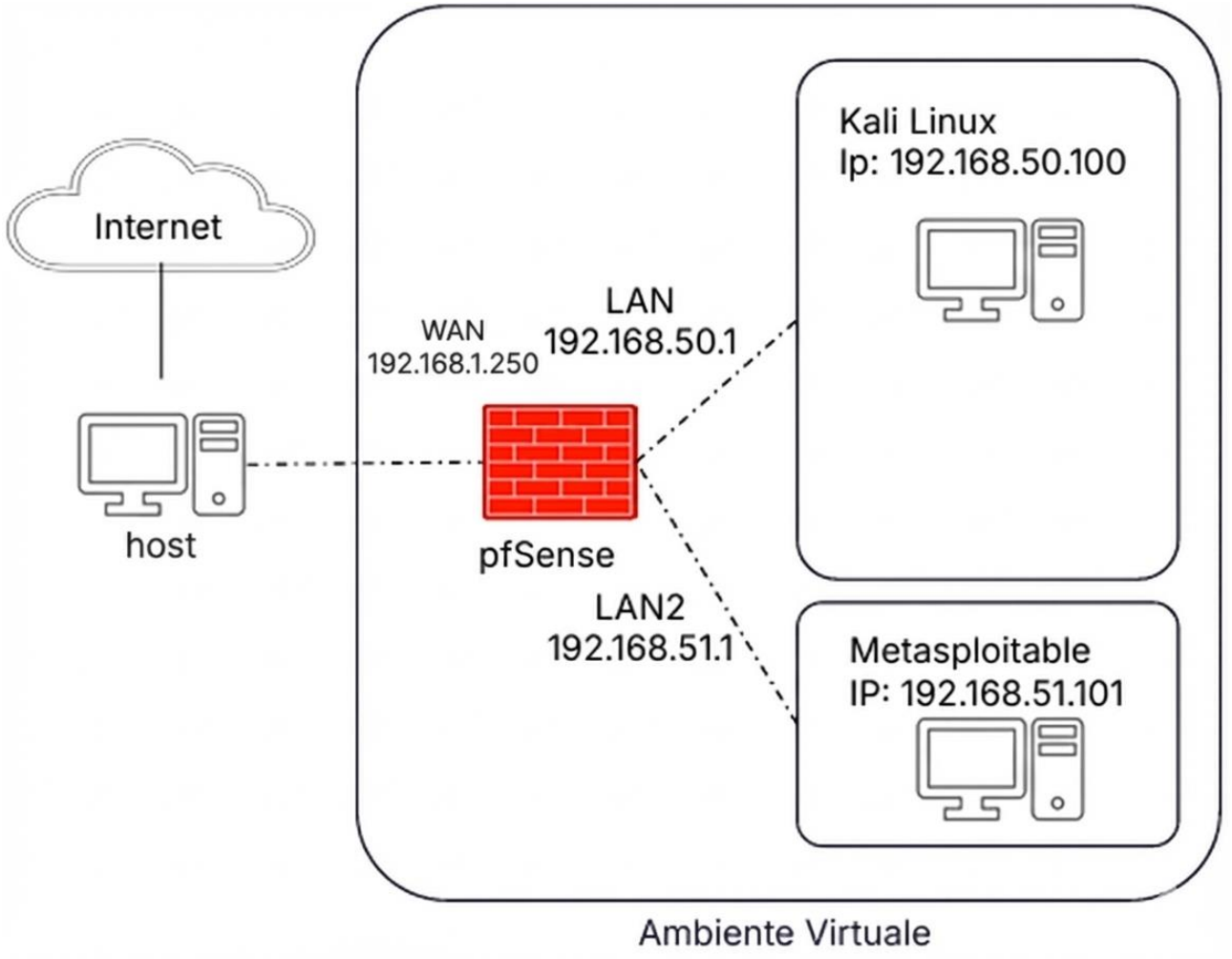
Pfsense e DVWA

In questo report andrò a mostrare le regole firewall che mi consentiranno/impediranno determinate attività nell'infrastruttura sottostante:



Dalla mia macchina host ho virtualizzato pfsense con virtualbox, per loggarmi alla web GUI ho inserito da browser di kali l'ip di LAN, visualizzabile da shell di pfsense (di default 192.168.1.125 cambiato in 192.168.50.1 da web GUI), ho poi creato una seconda rete locale LAN2 (ip 192.168.51.1). LAN e LAN2 di pfsense con 2 schede di rete virtualizzate in Internal Network rispettivamente 'intnet' e 'intnet2' e i loro endpoint (kali e meta) sono in ip statico, come si evidenzia nell'immagine sorpa. Configurazione extra: ho creato un Alias IPv4 per la rete WAN (192.168.1.250), per avere un ip statico su subnet 192.168.1.0/24.

```
LAN (lan)       -> em1        -> v4: 192.168.50.1/24
LAN2 (opt1)     -> em2        -> v4: 192.168.51.1/24
```

Settings interface kali

```
iface eth0 inet static

        address 192.168.50.100
        netmask 255.255.255.0
        gateway 192.168.50.1
```

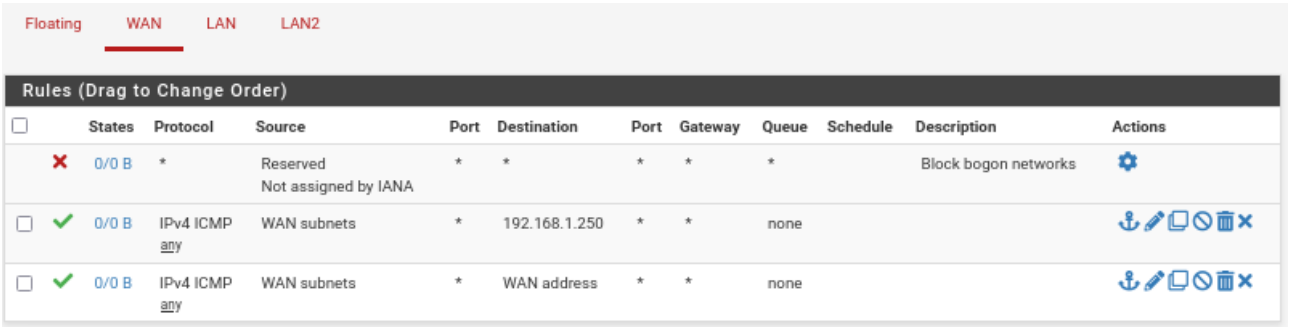
Settings interface metasploitable

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.51.101
netmask 255.255.255.0
gateway 192.168.51.1
```

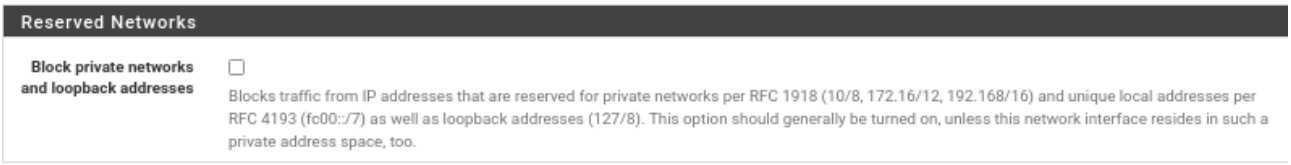
Stato iniziale del firewall

Su LAN rules ci sono regole preimpostate da pfsense, tra queste una regola serviva a consentire il raggiungimento della web GUI (interfaccia LAN address del FW), mentre le altre due consentivano l'accesso su internet (any destination) IPv4 e IPv6, da me disabilitate perchè non necessarie dato che la rete è configurata come Internal Network.

WAN rules

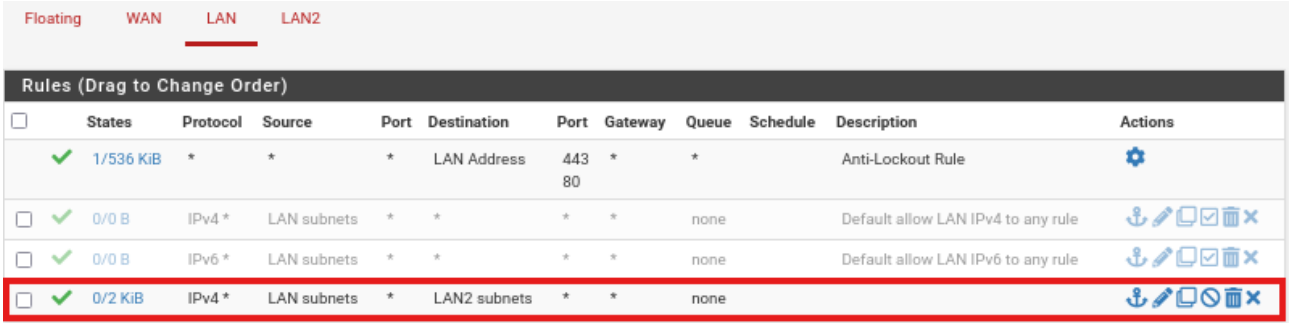


Le modifiche da me applicate riguardano la rimozione della regola default che blocca il traffico in entrata su WAN address da indirizzi appartenenti a reti private (come la mia), volendo testare il raggiungimento dell'interfaccia FW dalla mia rete domestica ho rimosso il flag su Interfaces>WAN>Reserved Networks



Ho poi aggiunto le regole che permettessero il traffico ICMP da WAN subnets (my host) all'ip 192.168.1.250 (alias di WAN interface) , e da WAN subnets a WAN address.

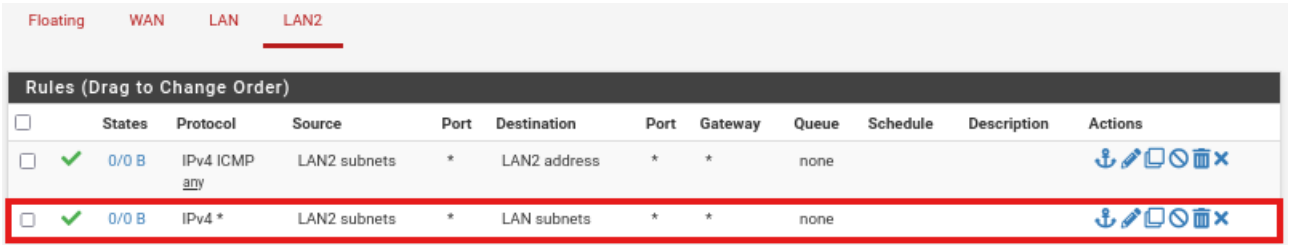
LAN rules



Qui ho creato una regola che consentisse il traffico dagli indirizzi di LAN a quelli di LAN2, regola cruciale per testare la raggiungibilità di Meta da Kali.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=3.67 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=9.52 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=4.05 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=1.61 ms
^C
── 192.168.51.101 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.611/4.712/9.523/2.928 ms
```

LAN2 rules



Qui invece ho creato 2 regole: una che consentisse il traffico ICMP dagli indirizzi di LAN2 a LAN address (necessaria per testare il ping da meta a FW interface), e la più importante evidenziata, regola che mi consente il traffico dagli indirizzi di LAN2 a quelli di LAN, utile per far comunicare meta verso kali. Di seguito le immagini rispettivamente di entrambi i test:

```
msfadmin@metasploitable:~$ ping 192.168.51.1
PING 192.168.51.1 (192.168.51.1) 56(84) bytes of data.
64 bytes from 192.168.51.1: icmp_seq=1 ttl=64 time=0.979 ms
64 bytes from 192.168.51.1: icmp_seq=2 ttl=64 time=1.39 ms
64 bytes from 192.168.51.1: icmp_seq=3 ttl=64 time=1.73 ms
64 bytes from 192.168.51.1: icmp_seq=4 ttl=64 time=1.52 ms

--- 192.168.51.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3193ms
rtt min/avg/max/mdev = 0.979/1.409/1.739/0.279 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=51.1 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=2.16 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.89 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=2.19 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3097ms
rtt min/avg/max/mdev = 1.891/14.351/51.155/21.249 ms
```

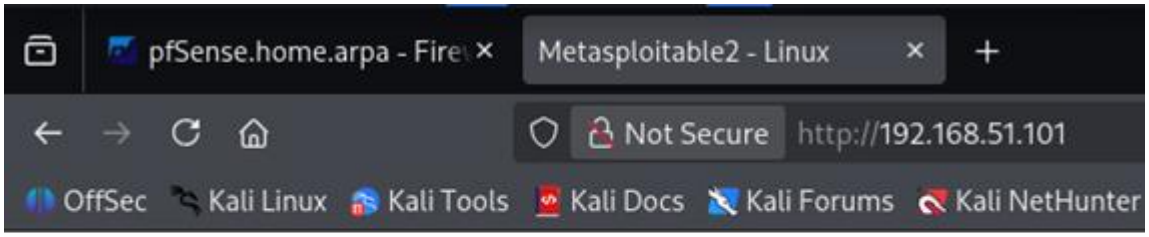
Start del servizio da esporre su Metasploitable

Per testare al meglio le regole ho startato la DVWA preinstallata su meta, il web service che si occupa della sua esposizione è apache2

```
root@metasploitable:/home/msfadmin# /etc/init.d/apache2 start
 * Starting web server apache2
httpd (pid 4751) already running
```

Una volta startato il servizio ho iniziato e testare il raggiungimento di quest'ultimo dalla rete LAN, utilizzando anche strumenti di scansione.

Raggiungimento della Web Application da Kali (LAN 50.0/24)



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Scansione generale di Meta

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 08:30 EST
Nmap scan report for 192.168.51.101
Host is up (0.028s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

Scansione con versione del servizio su porta 80

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.51.101 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:00 EST
Nmap scan report for 192.168.51.101
Host is up (0.0053s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 20.33 seconds
```

Scansione Aggressiva

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.51.101 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:33 EST
Nmap scan report for 192.168.51.101
Host is up (0.013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.50 ms 192.168.50.1
2   4.03 ms 192.168.51.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.90 seconds
```

La scansione con switch -A include diversi tipi di switch per una scansione dettagliata tra cui:
-sV → versione del servizio esposto

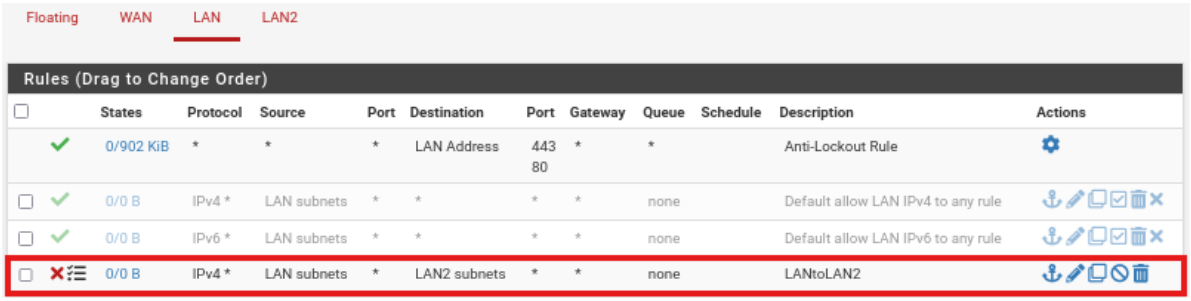
-O → rileva il sistema operativo

--traceroute → mappa il percorso di rete con i suoi hop

-sC → esegue controlli automatici secondo un motore interno (Nmap Script Engine), è quello che mi ha permesso di scoprire il titolo della pagina esposta

Test di modifica della regola FW

Di seguito riporto il cambiamento alla regola precedentemente creata, su LAN

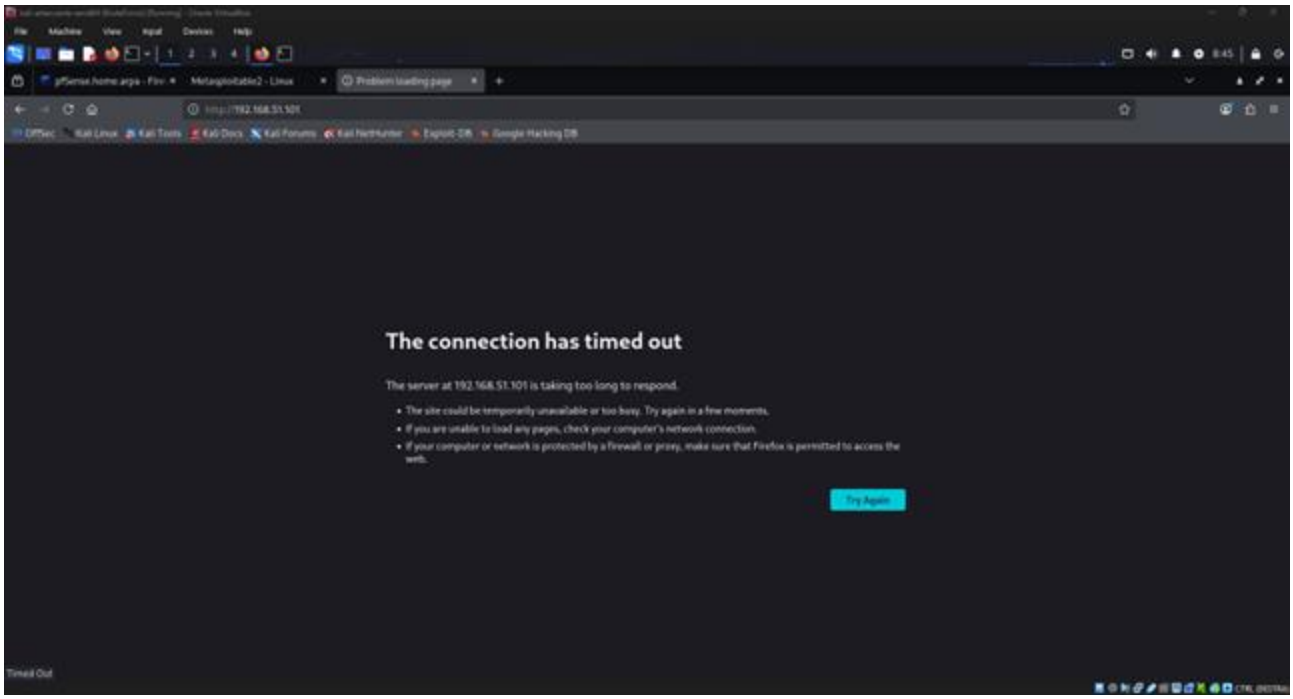


Risposta di Meta

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
── 192.168.51.101 ping statistics ──
7 packets transmitted, 0 received, 100% packet loss, time 6151ms
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 12:48 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds
```

Ora la DVWA di Meta non è più raggiungibile



Conclusione

Gli host kali e meta possono comunicare tra loro solo secondo le regole del firewall pfsense.

Più le regole sono mirate a consentire/impedire il passaggio di pacchetti specifici su porte specifiche più l'infrastruttura sarà sicura da minacce e vulnerabilità.