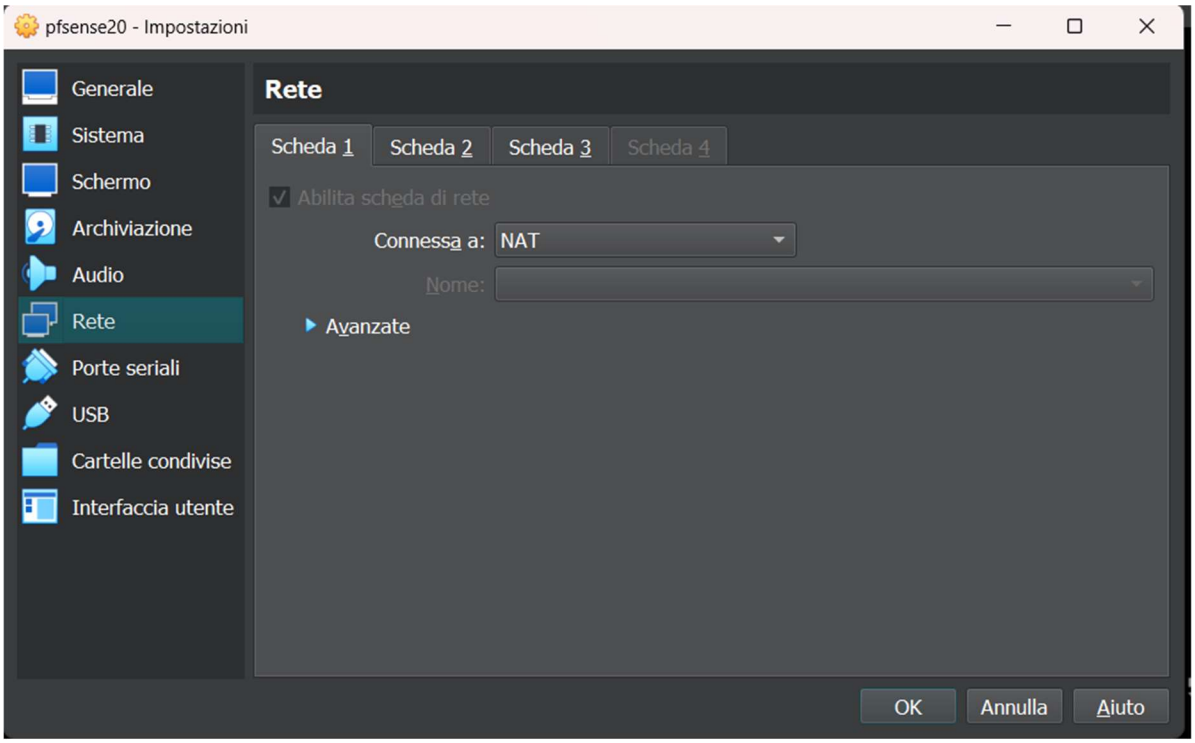
Configurazione macchine:

PFSENSE è stato configurato come segue:

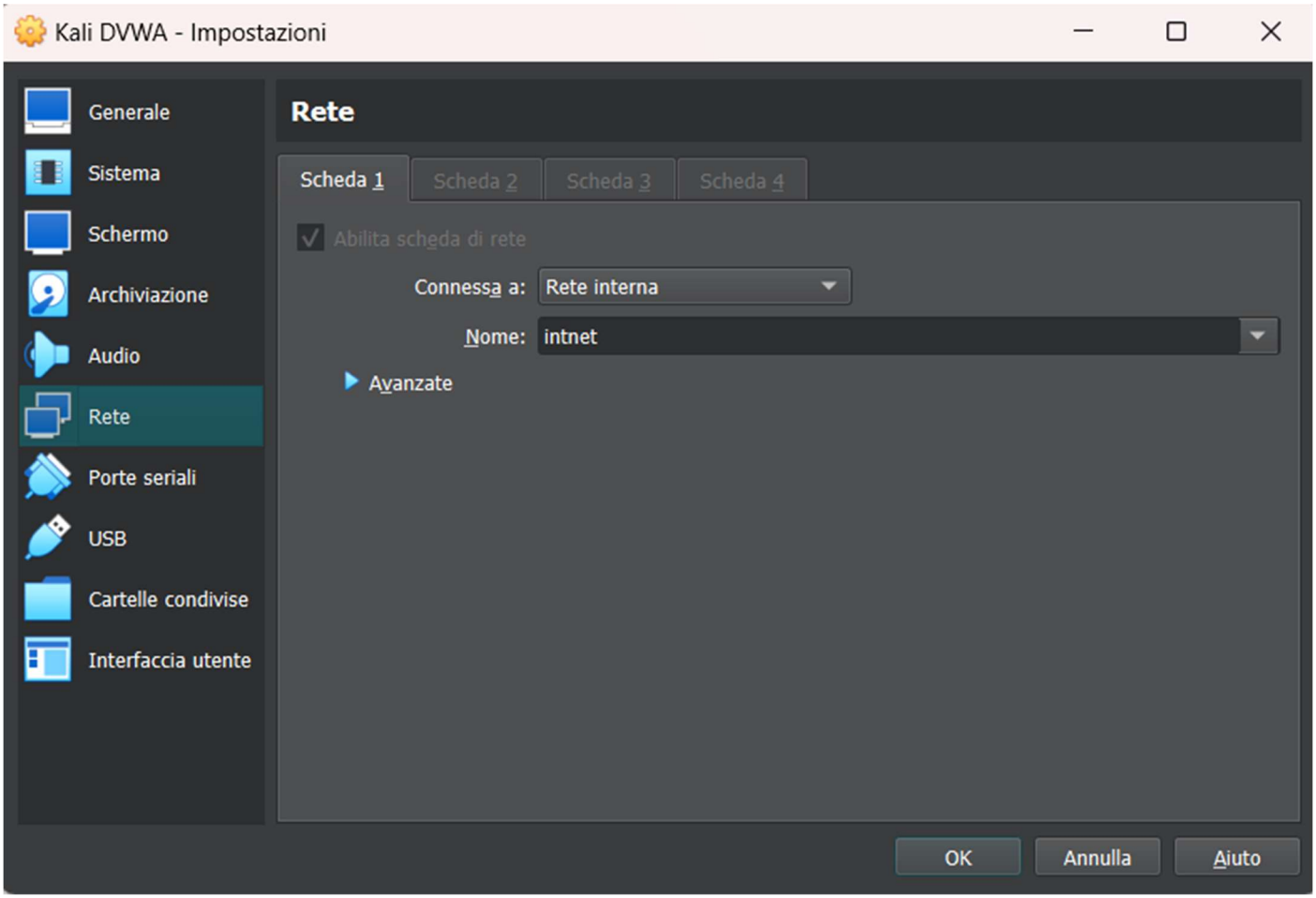
- Ha un accesso a internet sulla rete WAN
- Sulla rete LAN, con il gateway 192.168.50.1, è in connessione con la nostra macchina KALI
- Sulla rete LAN2, con il gateway 192.168.51.1, è in connessione con la nostra macchina METASPLOITABLE.

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 15ec8200ae99cfd56ade

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

 WAN (wan)       -> le0        -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> le1        -> v4: 192.168.50.1/24
 LAN2 (opt1)     -> em0        -> v4: 192.168.51.1/24

 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

Enter an option:
```



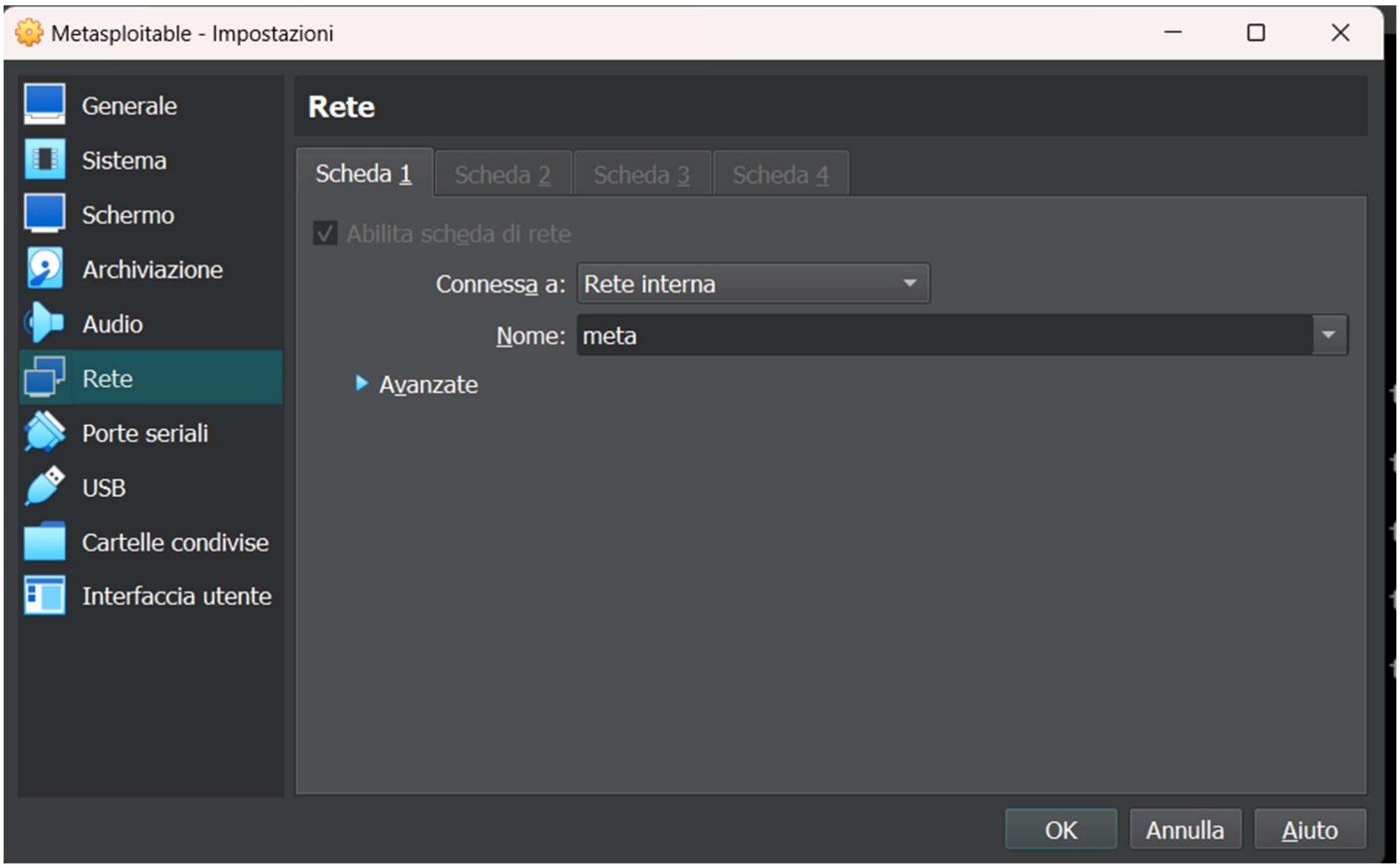
La nostra macchina KALI ha l'indirizzo IP 192.168.50.102 ed è collegata solamente a PFSENSE tramite LAN

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.102  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::1a2b:82e7:525c:aa75  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e2:a7:85  txqueuelen 1000  (Ethernet)
        RX packets 7049  bytes 5256539 (5.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4738  bytes 956064 (933.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 780 (780.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 780 (780.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



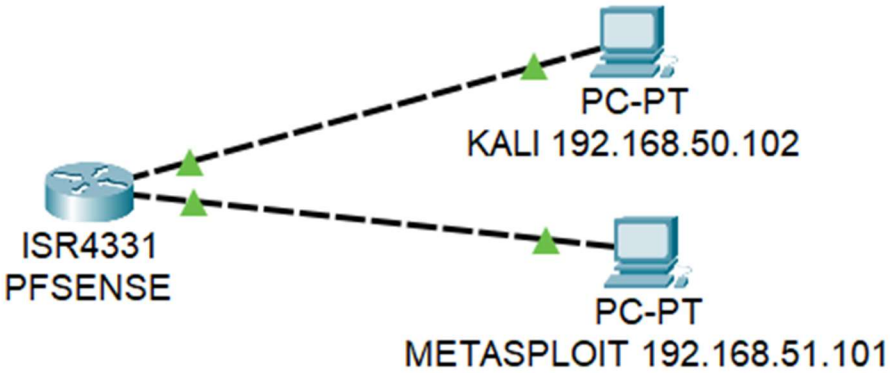
La nostra macchina METASPLOITABLE ha l'indirizzo 192.168.51.101 ed è collegata solamente a PFSENSE tramite LAN2

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:be:2a:6e
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febe:2a6e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 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:111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21285 (20.7 KB)  TX bytes:21285 (20.7 KB)

msfadmin@metasploitable:~$ _
```



Come schema semplificativo, ho sfruttato CISCO PACKET TRACER per fare un piccolo schema della situazione attuale della rete.

KALI, collegato sulla rete LAN e METASPLOITABLE collegato sulla rete LAN2, mentre PFSENSE ha un accesso a Internet e le due reti LAN che lo collegano rispettivamente alle due macchine.



Nonostante le due macchine appartengano a due reti diverse, noi riusciamo comunque a farle comunicare:

```
┌──(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=12.8 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=2.56 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=3.02 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=2.91 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=2.55 ms
^C
--- 192.168.51.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4122ms
rtt min/avg/max/mdev = 2.550/4.771/12.810/4.023 ms
```

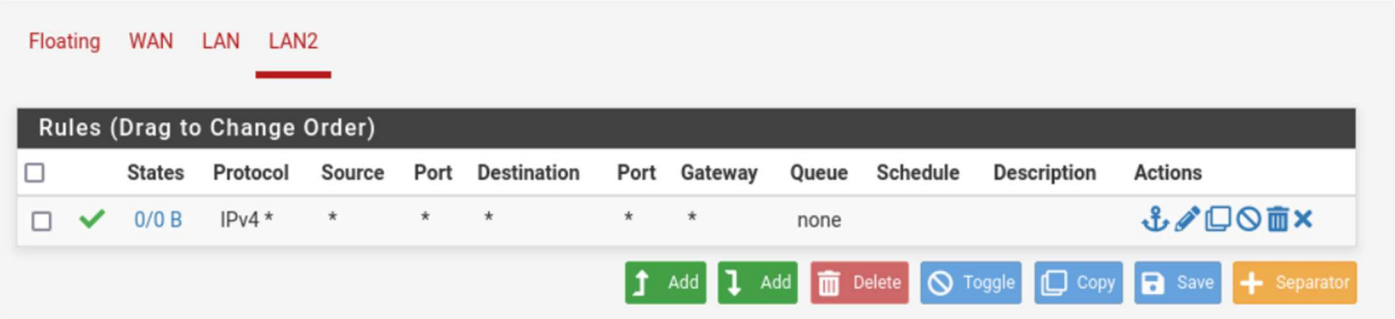
```
msfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=63 time=1.81 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=63 time=2.76 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=63 time=2.51 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=63 time=2.76 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=63 time=2.52 ms

--- 192.168.50.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 1.816/2.476/2.767/0.353 ms
```

Proviamo ora a far comunicare le due macchine con i server di google:

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (216.58.204.238) 56(84) bytes of data.
64 bytes from mil07s18-in-f14.1e100.net (216.58.204.238): icmp_seq=1 ttl=114
time=15.3 ms
64 bytes from mil07s18-in-f14.1e100.net (216.58.204.238): icmp_seq=2 ttl=114
time=14.7 ms
64 bytes from mil07s18-in-f14.1e100.net (216.58.204.238): icmp_seq=3 ttl=114
time=12.5 ms
64 bytes from mil07s18-in-f14.1e100.net (216.58.204.238): icmp_seq=4 ttl=114
time=14.8 ms
64 bytes from mil07s18-in-f14.1e100.net (216.58.204.238): icmp_seq=5 ttl=114
time=16.2 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4032ms
rtt min/avg/max/mdev = 12.532/14.690/16.198/1.207 ms
```

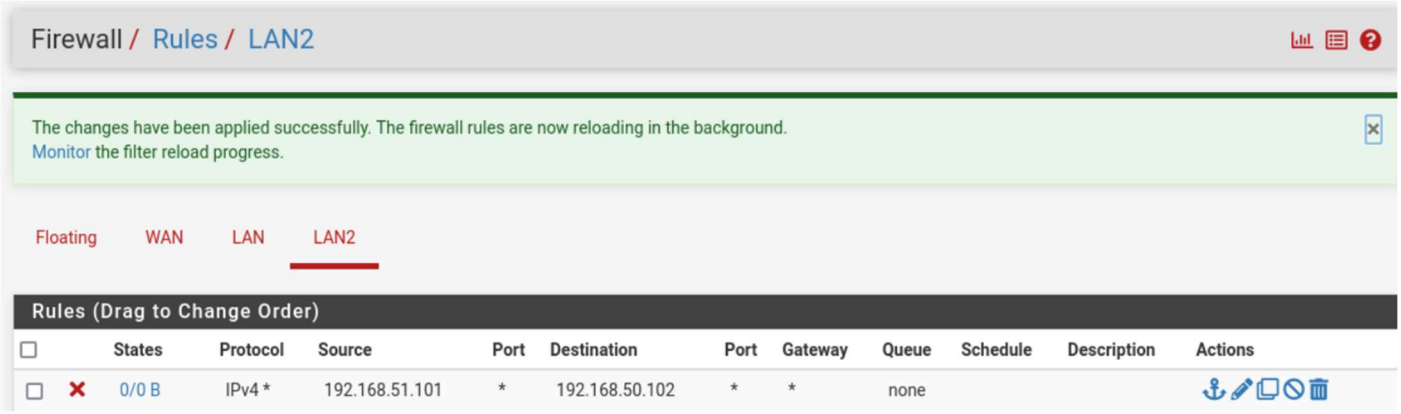
```
msfadmin@metasploitable:~$ ping google.com
PING google.com (216.58.209.46) 56(84) bytes of data.
64 bytes from waw02s05-in-f14.1e100.net (216.58.209.46): icmp_seq=1 ttl=115 time
=19.7 ms
64 bytes from mil07s12-in-f14.1e100.net (216.58.209.46): icmp_seq=2 ttl=115 time
=17.0 ms
64 bytes from waw02s05-in-f14.1e100.net (216.58.209.46): icmp_seq=3 ttl=115 time
=18.7 ms
64 bytes from waw02s05-in-f46.1e100.net (216.58.209.46): icmp_seq=4 ttl=115 time
=18.5 ms
64 bytes from waw02s05-in-f46.1e100.net (216.58.209.46): icmp_seq=5 ttl=115 time
=20.0 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 17.008/18.831/20.032/1.086 ms
msfadmin@metasploitable:~$
```

Per far si che tutto ciò funzioni, abbiamo creato una regola che consenta il traffico della rete LAN2, senza bloccare nulla:



Proviamo ora a inserire una regola nel firewall che impedisca a METASPLOITABLE di pingare KALI:

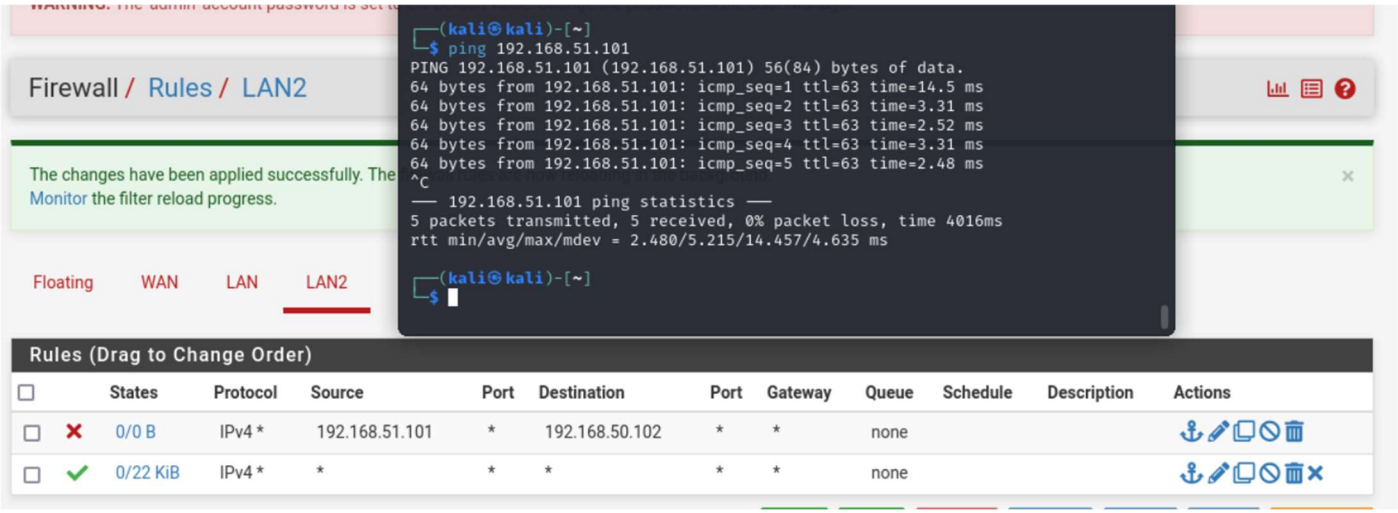
Creando una regola che si applica a tutti i protocolli dall'indirizzo di partenza 192.168.51.101 a 192.168.50.102



Riusciamo a fare in modo che non sia possibile pingare da METASPLOITABLE a KALI, lasciando la possibilità a METASPLOITABLE di accedere a internet.

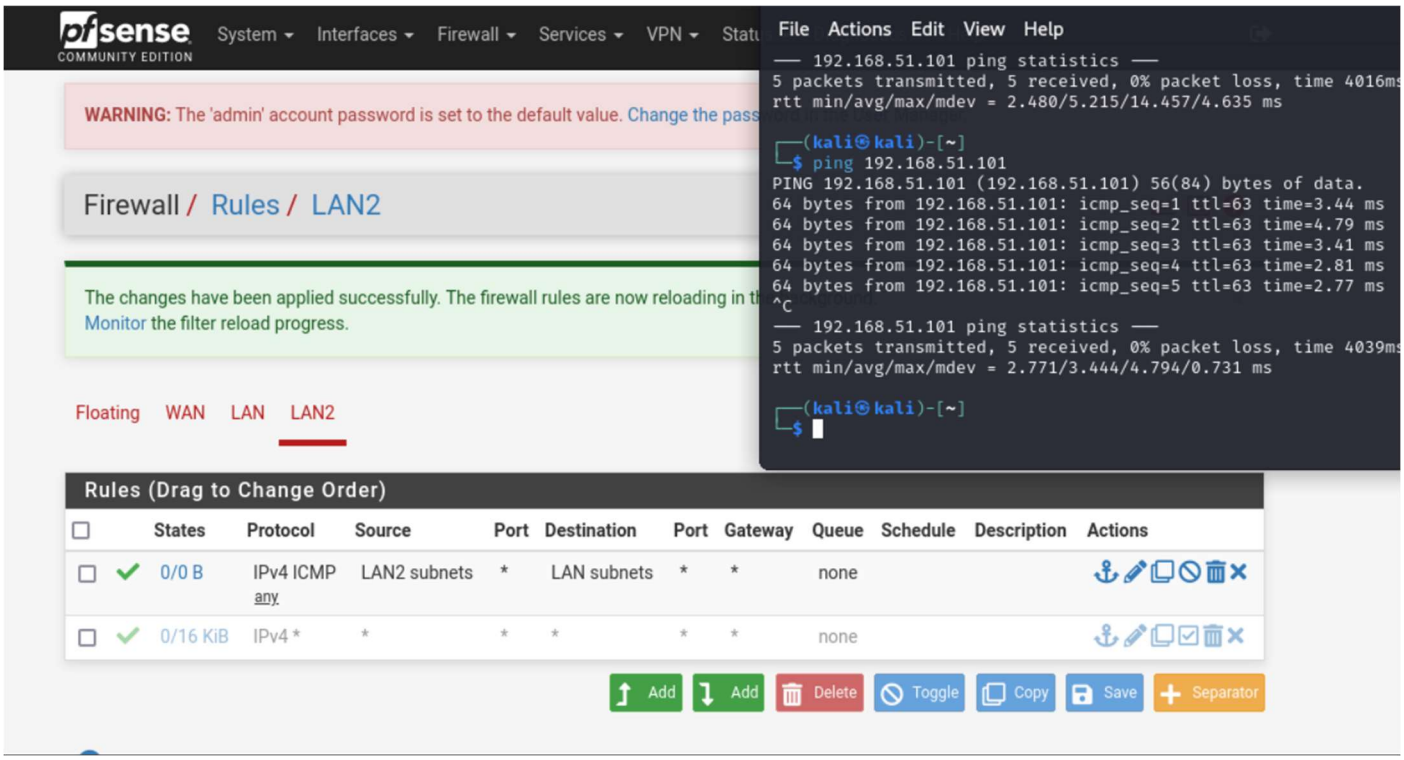
```
msfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.

--- 192.168.50.102 ping statistics ---
28 packets transmitted, 0 received, 100% packet loss, time 26999ms

msfadmin@metasploitable:~$ ping google.com
PING google.com (216.58.209.46) 56(84) bytes of data.
64 bytes from waw02s05-in-f14.1e100.net (216.58.209.46): icmp_seq=1 ttl=115 time
=64.9 ms
64 bytes from mil07s12-in-f14.1e100.net (216.58.209.46): icmp_seq=2 ttl=115 time
=16.7 ms
64 bytes from waw02s05-in-f46.1e100.net (216.58.209.46): icmp_seq=3 ttl=115 time
=17.3 ms
64 bytes from waw02s05-in-f46.1e100.net (216.58.209.46): icmp_seq=4 ttl=115 time
=16.5 ms
64 bytes from waw02s05-in-f14.1e100.net (216.58.209.46): icmp_seq=5 ttl=115 time
=17.3 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 16.591/26.591/64.904/19.158 ms
msfadmin@metasploitable:~$ _
```

Mentre il percorso inverso è ancora funzionante.



Con questa regola invece, possiamo bloccare i PING verso internet alla METASPLOITABLE, ma mantenere abilitati i ping verso le macchine delle altre sottoreti (KALI):

```
msfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=63 time=2.31 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=63 time=2.12 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=63 time=2.82 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=63 time=2.84 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=63 time=2.81 ms

--- 192.168.50.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 2.123/2.582/2.843/0.311 ms
msfadmin@metasploitable:~$ ping google.com

msfadmin@metasploitable:~$
```



Abbiamo disabilitato temporaneamente la regola iniziale che ci permetteva il traffico con la rete LAN2, per accettare solo traffico con protocollo ICMP (PING) dalla LAN2 alla LAN2.
Le due sottoreti comunicano quindi, però la LAN2 non riesce più a pingare il server google, non riceve alcuna risposta.