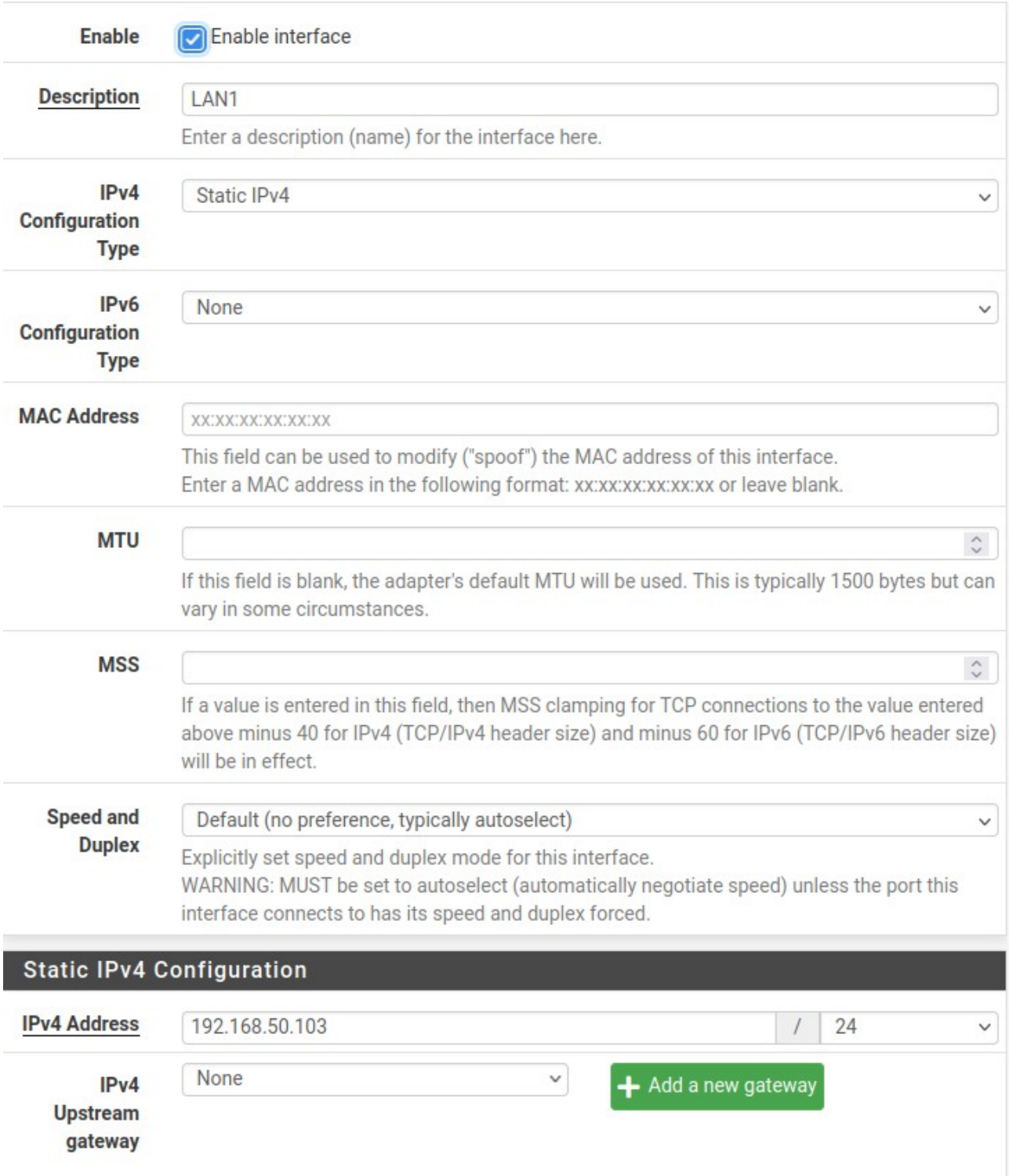
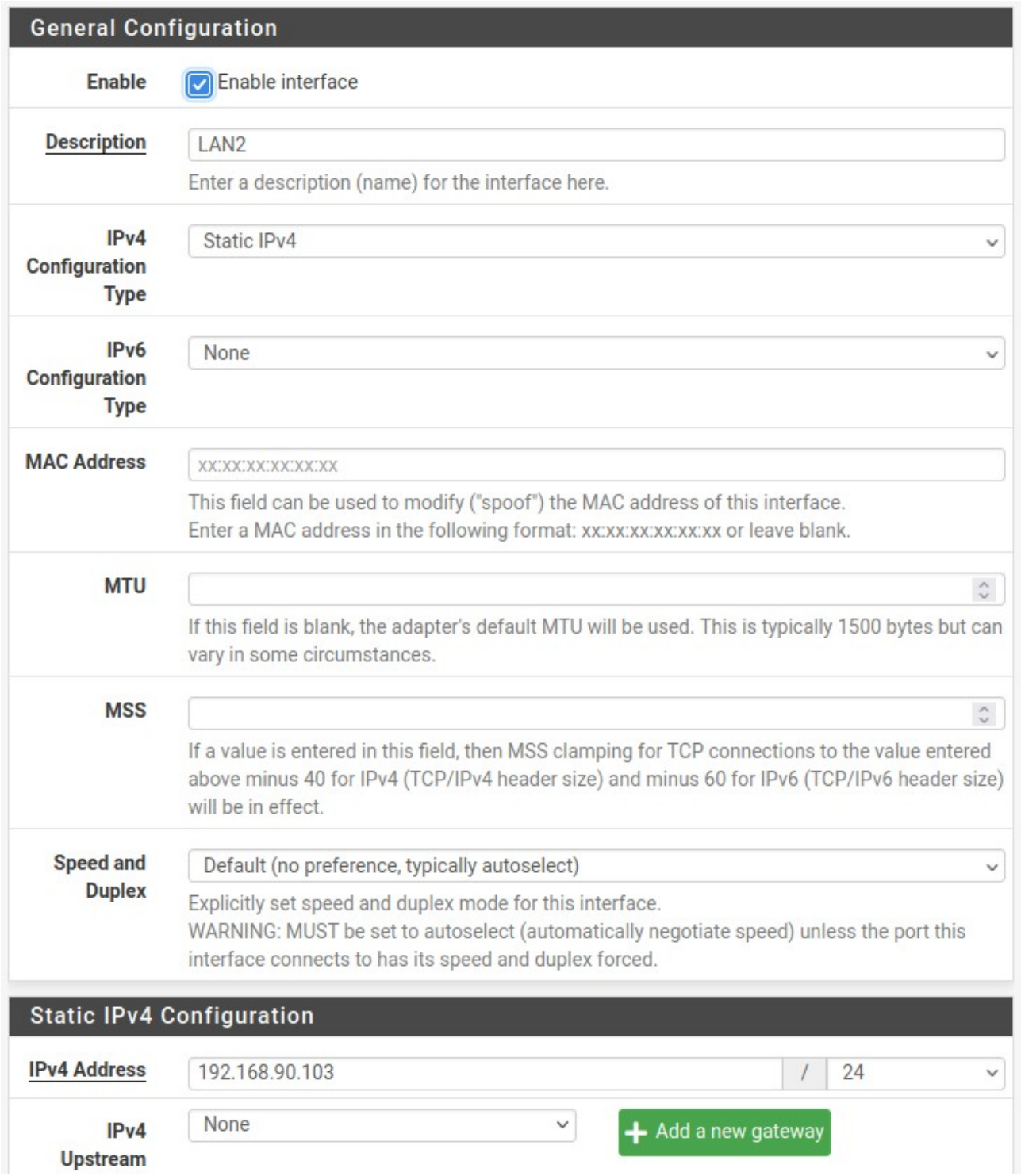
Alaimo Alessandro
21/11/2022

Creazione rules Firewall su PFSENSE

Per poter permettere la comunicazione tra due reti diverse, dobbiamo configurarle su Pfsense da terminale o da interfaccia grafica, nel mio caso:

- LAN1: 192.168.50.0
- LAN2: 192.168.90.0





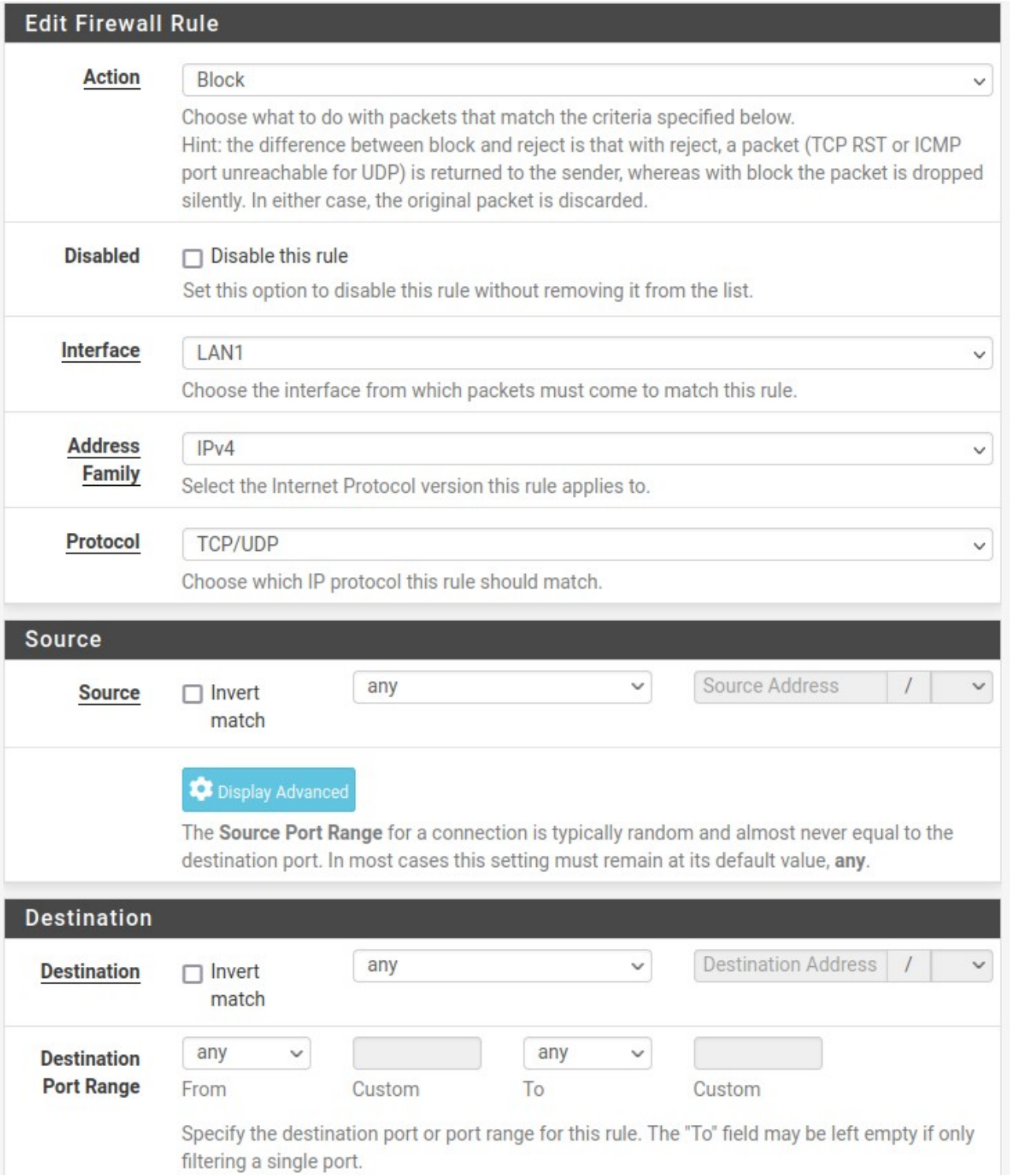
Fatto ciò possiamo cliccare su “Save” ed “Apply” per poi spostarci sulle regola da creare per il Firewall controllando prima però se le due macchine sono già in connessione e se Kali può scansionare Meta:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=64 time=0.303 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=64 time=0.210 ms
64 bytes from 192.168.90.101: icmp_seq=4 ttl=64 time=0.238 ms
64 bytes from 192.168.90.101: icmp_seq=5 ttl=64 time=0.401 ms
^C
--- 192.168.90.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4258ms
rtt min/avg/max/mdev = 0.203/0.271/0.401/0.073 ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.90.101 -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 10:07 EST
Nmap scan report for 192.168.90.101 (192.168.90.101)
Host is up (0.0017s 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 0.25 seconds
```

Adesso che abbiamo confermato la loro connessione e che lo scan viene eseguito e completato, impostiamo le regole del Firewall della LAN1 nel seguente modo:



Stesse regole per la LAN2. Adesso non ci rimane altro che provare a verificare se la connessione tra le due macchina è rimasta intatta bloccando però lo scan:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=64 time=0.315 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=64 time=0.226 ms
64 bytes from 192.168.90.101: icmp_seq=4 ttl=64 time=0.272 ms
^C
--- 192.168.90.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.90.101 -sS
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 09:48 EST
Nmap scan report for 192.168.90.101
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.90.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 37.42 seconds
```