

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

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN1"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="XX:XX:XX:XX:XX:XX"/> <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>

Static IPv4 Configuration

IPv4 Address	<input type="text" value="192.168.50.103"/>	/	<input type="text" value="24"/>
IPv4 Upstream gateway	<input type="text" value="None"/>	+ Add a new gateway	

General Configuration		
Enable	<input checked="" type="checkbox"/> Enable interface	
Description	<input type="text" value="LAN2"/> <p>Enter a description (name) for the interface here.</p>	
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>	
IPv6 Configuration Type	<input type="text" value="None"/>	
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> <p>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.</p>	
MTU	<input type="text"/> <p>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</p>	
MSS	<input type="text"/> <p>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</p>	
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <p>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</p>	
Static IPv4 Configuration		
IPv4 Address	<input type="text" value="192.168.90.103"/> / <input type="text" value="24"/>	
IPv4 Upstream	<input type="text" value="None"/>	<input type="button" value="+ Add a new gateway"/>

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

```

States	Protocol	Source	Port	Destination	Port
				LAN1	80

```

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:

Edit Firewall Rule

Action	Block		
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN1		
	Choose the interface from which packets must come to match this rule.		
Address Family	IPv4		
	Select the Internet Protocol version this rule applies to.		
Protocol	TCP/UDP		
	Choose which IP protocol this rule should match.		

Source

Source	<input type="checkbox"/> Invert match	any	Source Address	/	
<div>  Display Advanced </div> <p>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</p>					

Destination

Destination	<input type="checkbox"/> Invert match	any	Destination Address	/	
Destination Port Range	any	From	Custom	To	any
			Custom		Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.					

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
```