

## Creazione pratica di una regola Firewall.

Esercizio Pfsense 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).

Innanzitutto ho abilitato la terza scheda di rete su Pfsense, la prima rete è su Nat, seconda è su rete interna e la terza su bridge. Ho creato la terza interfaccia su Pfsense. Mi sono assicurata che kali e Metasploitable siano su reti diverse e ho assegnato a tutte le 3 macchine indirizzi ip diversi configurando anche i gateway. Ho configurato le reti su Kali e Metasploitable:

- Assegnato a **Metasploitable una rete separata**
- Assegnato a **Kali una rete collegata a OPT1**
- Verificato che **Kali e Metasploitable non siano sulla stessa rete.**

**ip kali :192.168.1.5 gateway: 192.168.1.1**

**ip meta: 192.168.26.101 gateway: 192.168.26.93**

**ip pfsense interfaccia OPT1: 192.168.20.1**

Dunque creo **la terza interface "OPT1"**

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / OPT1 (em1)

### General Configuration

**Enable** ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
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.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
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.

**Speed and Duplex**   
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.

### Static IPv4 Configuration

**IPv4 Address**  / 24

**IPv4 Upstream gateway**  [+ Add a new gateway](#)  
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.

Qua sotto metto gli screenshot degli indirizzi IP delle tre macchine.

## KALI

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    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
    link/ether 08:00:27:b8:94:d9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.5/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::59ef:ca7b:1e6f:104b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

## PFSENSE

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0    -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em1      -> v4: 192.168.20.1/24
```

## METASPLOITABLE

```
route {-h|--help} [<AF>]          Detailed usage syntax for specified
AF.
route {-V|--version}              Display version/author and exit.

-v, --verbose                     be verbose
-n, --numeric                     don't resolve names
-e, --extend                      display other/more information
-F, --fib                        display Forwarding Information Base (default)
-C, --cache                      display routing cache instead of FIB

<AF>=Use '-A <af>' or '--<af>'; default: inet
List of possible address families (which support routing):
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)
msfadmin@metasploitable:~$ route
Kernel IP routing table
  Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.26.0      *              255.255.255.0   U        0      0      0 eth0
default          192.168.26.93  0.0.0.0         UG        100    0      0 eth0
msfadmin@metasploitable:~$ ip route
192.168.26.0/24 dev eth0 proto kernel scope link src 192.168.26.101
default via 192.168.26.93 dev eth0 metric 100
msfadmin@metasploitable:~$
```

Adesso configuro di pfSense: creando la regola blocco l'accesso di Kali a Metasploitable:

Vado su **Firewall > Rules > OPT1** (la rete di Kali).

Aggiungo una regola che **blocca il traffico verso Metasploitable**:

- **Azione:** Block
- **Protocollo:** Any
- **Origine:** OPT1 (192.168.20.1/24)
- **Destinazione:** 192.168.26.101 (Metasploitable)
- **Porta:** Any per bloccare tutte le comunicazioni.

Firewall / Rules / Edit

### 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** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** OPT1  
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** Any  
Choose which IP protocol this rule should match.

**Source**  
☐ Invert match Address or Alias 192.168.20.1 /

**Destination**  
☐ Invert match Address or Alias 192.168.26.101 /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).





**Description**  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall








○


Firewall / Rules / OPT1

Floating WAN LAN **OPT1**

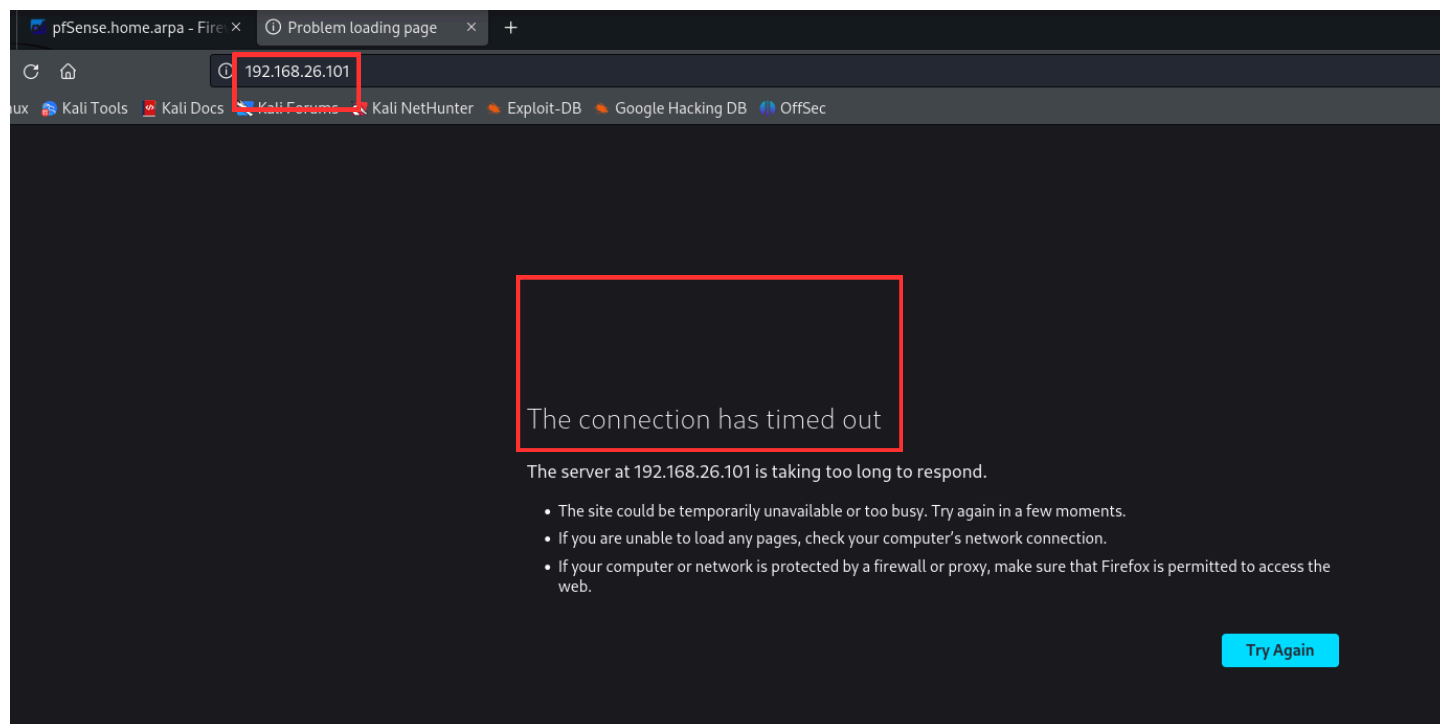
### Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.20.1	*	192.168.26.101	*	*	none			   

 Add  Add  Delete  Toggle  Copy  Save  Separator



Adesso scrivo l'ip di Metasploitable sul browser per vedere se me lo blocca il traffico oppure no e se la regola è stata appliccata.



Provando a pingare prima mi apriva la pagina perchè appunto se connetteva, mentre adesso pingando non me la trova la pagina dato che ho bloccato la connessione.

