

Creazione reti e regole firewall tramite pf sense

Kevin motti

Overview

Creare 3 reti diverse(LAN, WAN, OPT) utilizzando **pf sense** come router-firewall per collegare 2 LAN in reti diverse e 1 WAN.

Successivamente creare una regola che impedisca alla kali di accedere alla pagina DVWA di meta.

Obbiettivo 1 WAN:

Dentro il terminale di pf sense ho creato una rete WAN utilizzando il servizio DHCP del mio router, che ha assegnato automaticamente l'indirizzo IP.

Obbiettivo 2 kalinet (LAN):

Terminale pf sense:

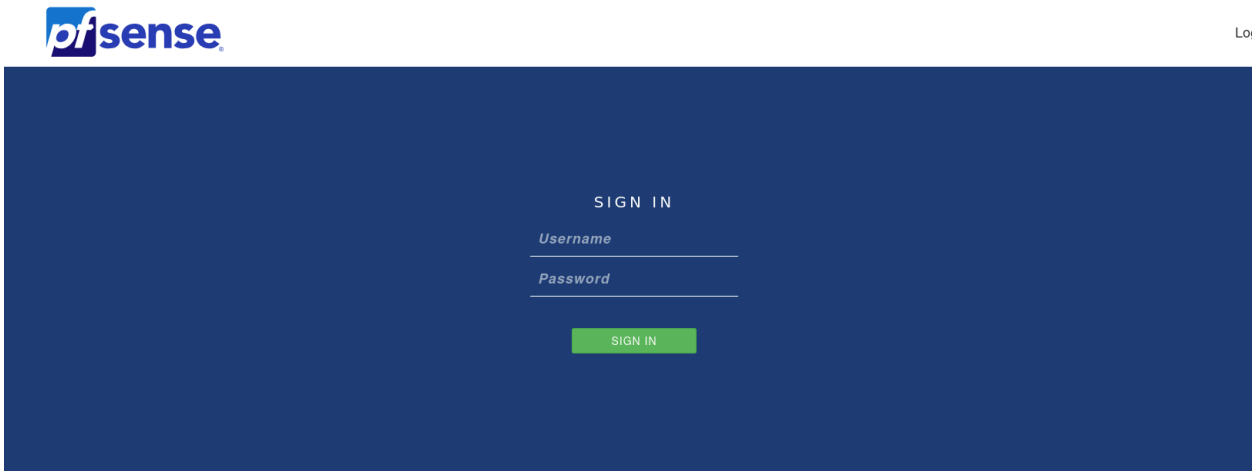
Da terminale ho settato manualmente l'indirizzo IP di pf sense e l'ho impostato come gateway con il seguente indirizzo: 192.168.50.1

Successivamente ho attivato il servizio DHCP per poter assegnare automaticamente l'indirizzo IP privato alla kali. L'indirizzo che è stato assegnato è il seguente:

```
valid_ttt forever  
eth0: <BROADCAST,MULTICAST  
link/ether 08:00:27:1  
inet 192.168.50.10/24
```

Obbiettivo 3 Creazione della terza rete per la meta:

Aprendo il browser dalla kali inserisco l'IP gateway di pfsense (192.168.50.1) che abbiamo impostato prima, così accedendo alla GUI di setup.

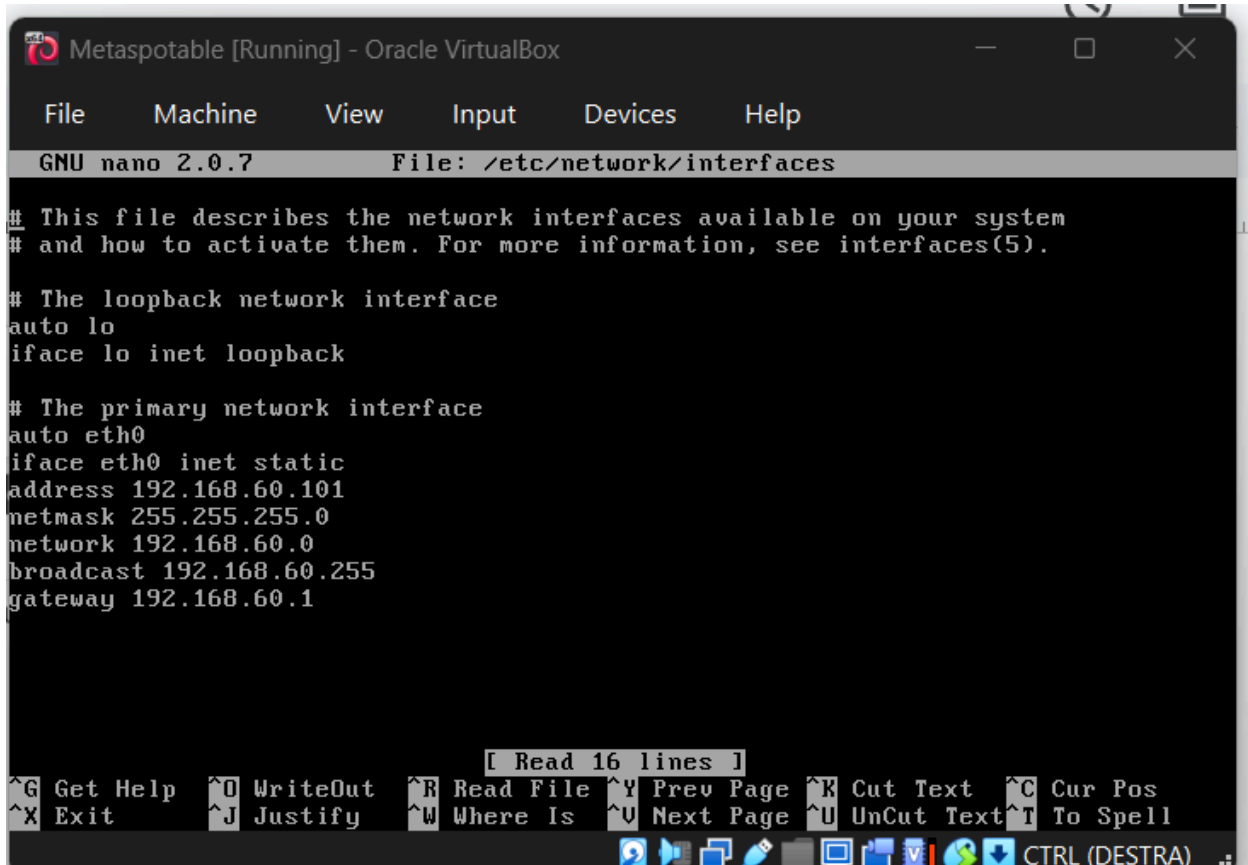


Dentro la pagina “interfaces” ho impostato l’indirizzo IP di gateway per questa rete (OPT):
192.168.60.1

IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	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 c</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 minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	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</small>
Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.60.1"/>
IPv4 Upstream gateway	None + Add a new gateway <small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the</small>

Meta:

Dentro il “pannello” per la configurazione degli IP di meta che ho aperto tramite comando: `sudo nano /etc/network/interfaces`



```
Metaspotable [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

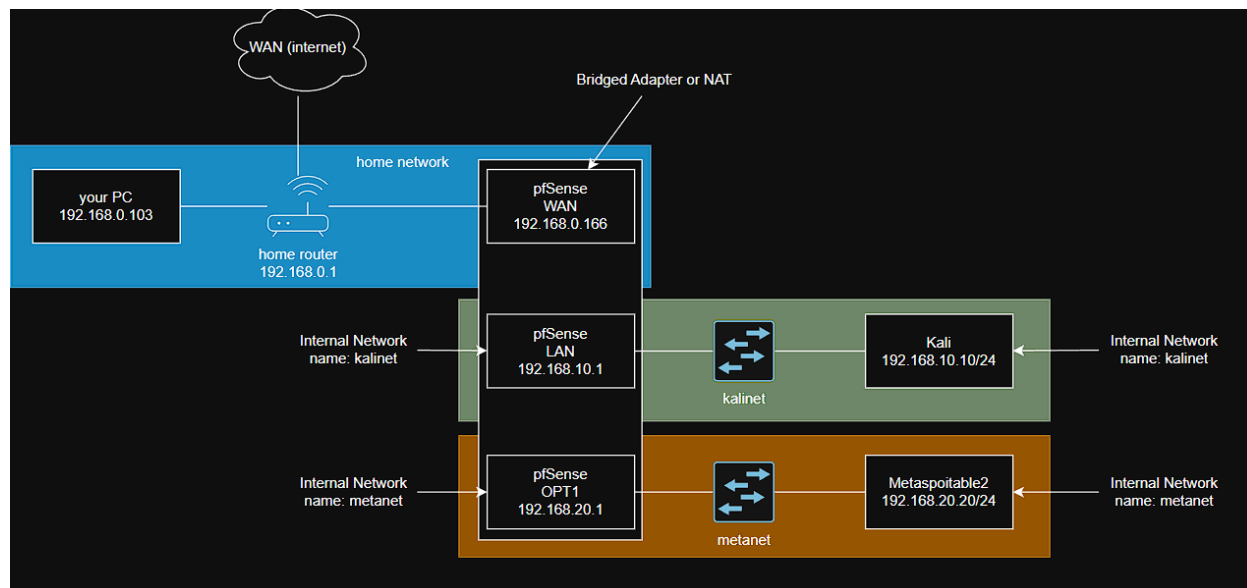
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.60.101
netmask 255.255.255.0
network 192.168.60.0
broadcast 192.168.60.255
gateway 192.168.60.1

[ Read 16 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

Ho impostato l'IP (192.168.60.101), il gateway corretto e il network (192.168.60.0)

Ora che tutte le impostazioni sono state salvate abbiamo 3 reti impostate in questo modo



RETE PRIVATA METANET: metasploitable (192.168.60.101) metanet (witch, rete) pf sense "192.168.60.1" (router, firewall)

RETE PRIVATA KALINET: kali (192.168.50.10) kalinet (switch, rete) pf sense "192.168.50.1" (router firewall)

PF SENSE WAN: 192.168.1.171/24 (via DHCP)

Se facciamo una prova di ping dalla kali alla meta:

```
(kali㉿kali)-[~]  
$ ping 192.168.60.101  
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.  
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=4.06 ms  
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=0.486 ms  
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=0.747 ms  
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=0.573 ms  
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=0.569 ms  
64 bytes from 192.168.60.101: icmp_seq=6 ttl=63 time=0.529 ms  
64 bytes from 192.168.60.101: icmp_seq=7 ttl=63 time=0.569 ms  
64 bytes from 192.168.60.101: icmp_seq=8 ttl=63 time=0.732 ms  
64 bytes from 192.168.60.101: icmp_seq=9 ttl=63 time=0.413 ms  
^C  
— 192.168.60.101 ping statistics —  
9 packets transmitted, 9 received, 0% packet loss, time 8149ms  
rtt min/avg/max/mdev = 0.413/0.964/4.059/1.098 ms
```

Tutto funziona correttamente.

Questa è la visuale da terminale pf sense:

```

Press <ENTER> to continue.
Message from syslogd@pfSense at Dec 13 11:11:53 ...
php-fpm[3961]: /index.php: Successful login for user 'admin' from: 192.168.50.10
(Local Database)

VirtualBox Virtual Machine - Netgate Device ID: 82cd135ff3fa3a938c5b

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

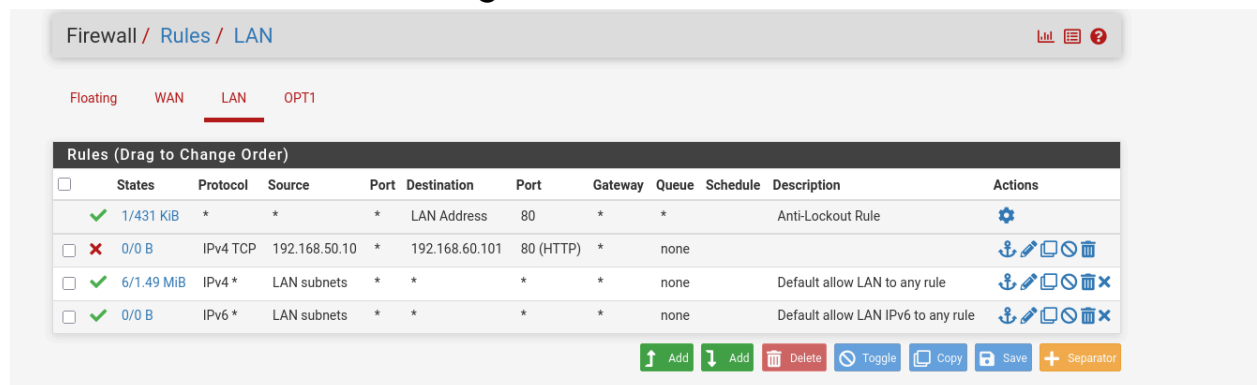
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.171/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0          -> v4: 192.168.60.1/24

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:

```

Obbiettivo 4 creazione regola firewall:



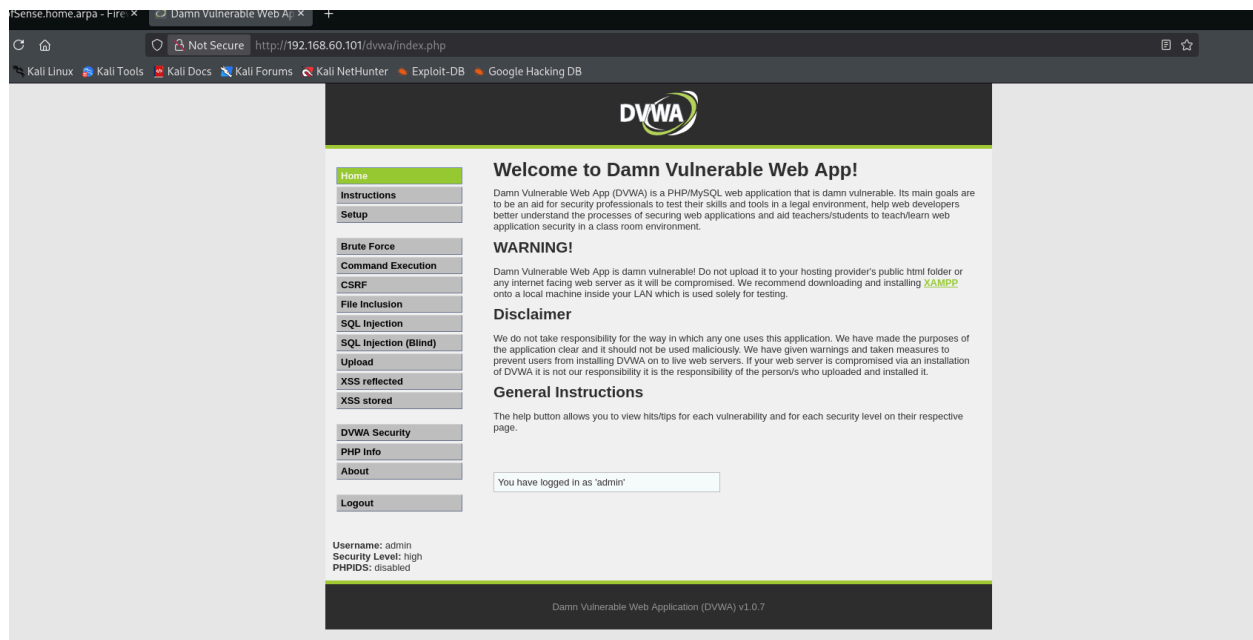
Dentro il pannello delle configurazioni del firewall scelgo di modificare le regole **LAN** (essendo una regola di blocco per la kali) e aggiungo **in cima alla lista** una regola che impedisca alla kali di scambiare protocolli TCP con l'IP di destinazione 192.168.60.101 (meta) alla **porta 80**.

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	LAN		
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		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.50.10 /
<input type="button" value="Display Advanced"/> <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	Address or Alias	192.168.60.101 /
Destination Port Range	HTTP (80) From Custom	HTTP (80) To Custom	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

(la posizione delle regole è di fondamentale importanza dato che il firewall le legge dall'alto verso il basso, per questo motivo se la regola di blocco è inferiore nella lista rispetto a una regola che permette il passaggio, la regola di blocco non avrà effetto.)

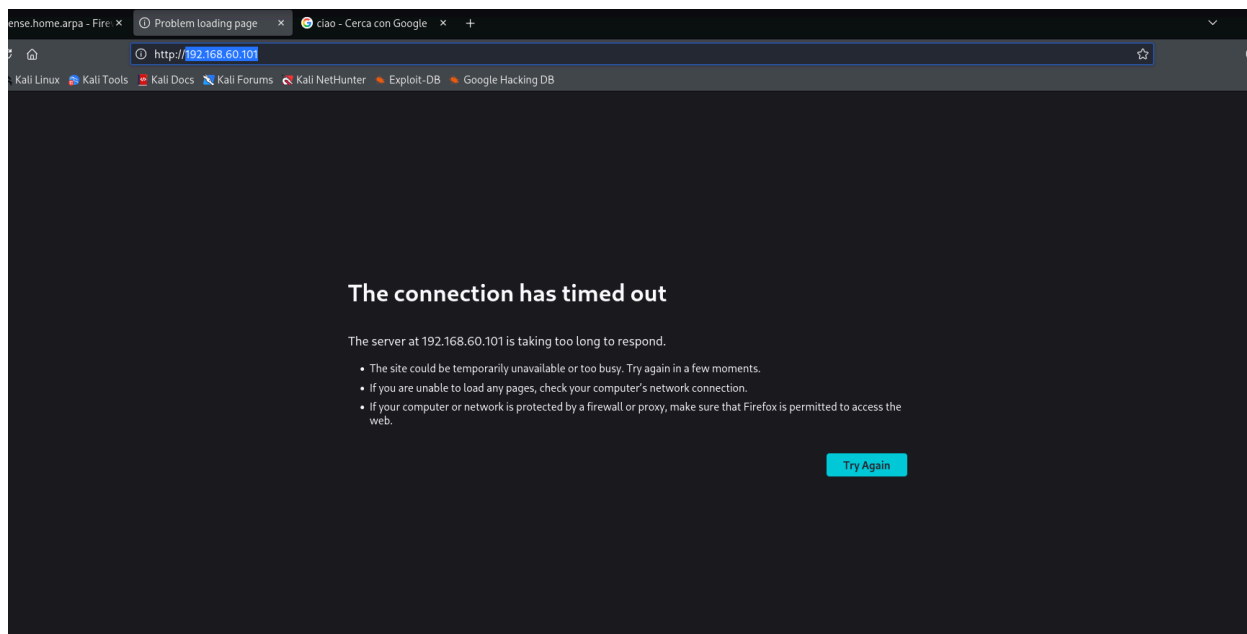
CONCLUSIONE:

Questa è una visuale del **prima** e del **dopo** la regola:



prima si può notare che inserendo nella barra di ricerca del browser di kali l'indirizzo IP della meta (192.168.60.101) arriviamo alla pagina della DVWA che è la pagina a cui vogliamo impedire l'accesso alla kali.

Dopo l'applicazione della regola possiamo vedere come l'accesso a quella pagina ora ci è stato negato.



Un'ultima prova di ping per confermare che ci sia ancora comunicazione tra le due macchine anche dopo l'applicazione della regola del firewall:

```
(kali@kali)-[~]
$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data:
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=0.585 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=0.679 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=0.820 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=0.681 ms
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=0.774 ms
64 bytes from 192.168.60.101: icmp_seq=6 ttl=63 time=0.737 ms
64 bytes from 192.168.60.101: icmp_seq=7 ttl=63 time=0.520 ms
64 bytes from 192.168.60.101: icmp_seq=8 ttl=63 time=0.915 ms
64 bytes from 192.168.60.101: icmp_seq=9 ttl=63 time=0.809 ms
^C
— 192.168.60.101 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8163ms
rtt min/avg/max/mdev = 0.520/0.724/0.915/0.115 ms
```

Tutto funziona correttamente.

Note aggiuntive:

Firewall / Rules / WAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/7 KIB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/2 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/1.59 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/3 KIB	IPv4 TCP	192.168.50.10	*	192.168.60.101	80 (HTTP)	*	none			
<input type="checkbox"/>	17/3.67 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Toggle Copy Save Separator

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"/>	0/1008 B	IPv4 ICMP any	192.168.60.101	*	This Firewall (self)	*	*	none			

↑ Add ↓ Add Delete Toggle Copy Save Separator

Queste sono le regole firewall per ogni rete.

Ho aggiunto una regola a OPT1 per permettere al protocollo ICMP di comunicare, in modo da poter testare la comunicazione tra la meta e pf sense.