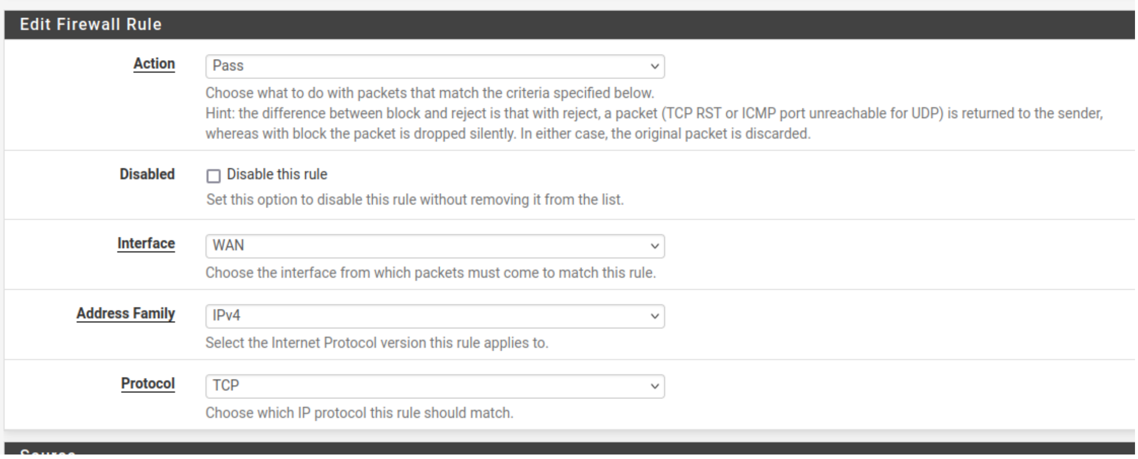
Creacion de regla pfsense para acceder desde la wan:



Edit Firewall Rule

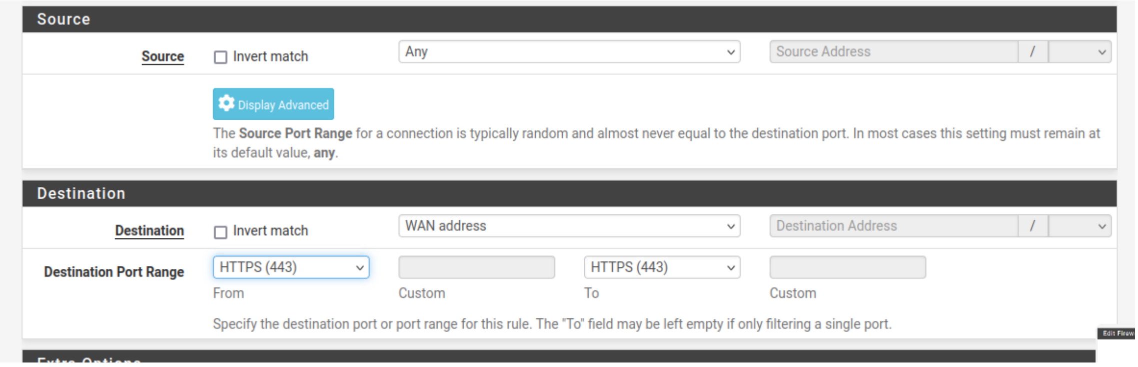
Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
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: □ Invert match | Any | Source Address /

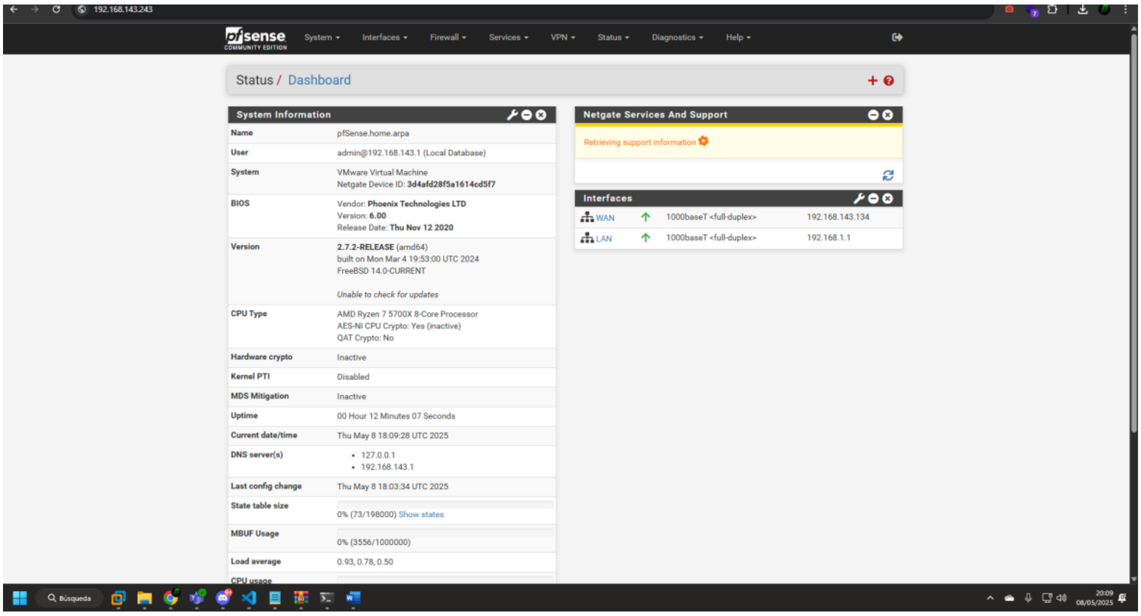
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | WAN address | Destination Address /

Destination Port Range: HTTPS (443) (From) | (Custom) | HTTPS (443) (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.



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.143.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **3d4afd28f5a1614cd5f7**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.7.2-RELEASE** (amd64) built on Mon Mar 4 19:53:00 UTC 2024 FreeBSD 14.0-CURRENT *Unable to check for updates*
CPU Type	AMD Ryzen 7 5700X 8-Core Processor AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 12 Minutes 07 Seconds
Current date/time	Thu May 8 18:09:28 UTC 2025
DNS server(s)	• 127.0.0.1 • 192.168.143.1
Last config change	Thu May 8 18:03:34 UTC 2025
State table size	0% (73/198000) Show states
MBUF Usage	0% (3556/1000000)
Load average	0.93, 0.78, 0.50
CPU usage	

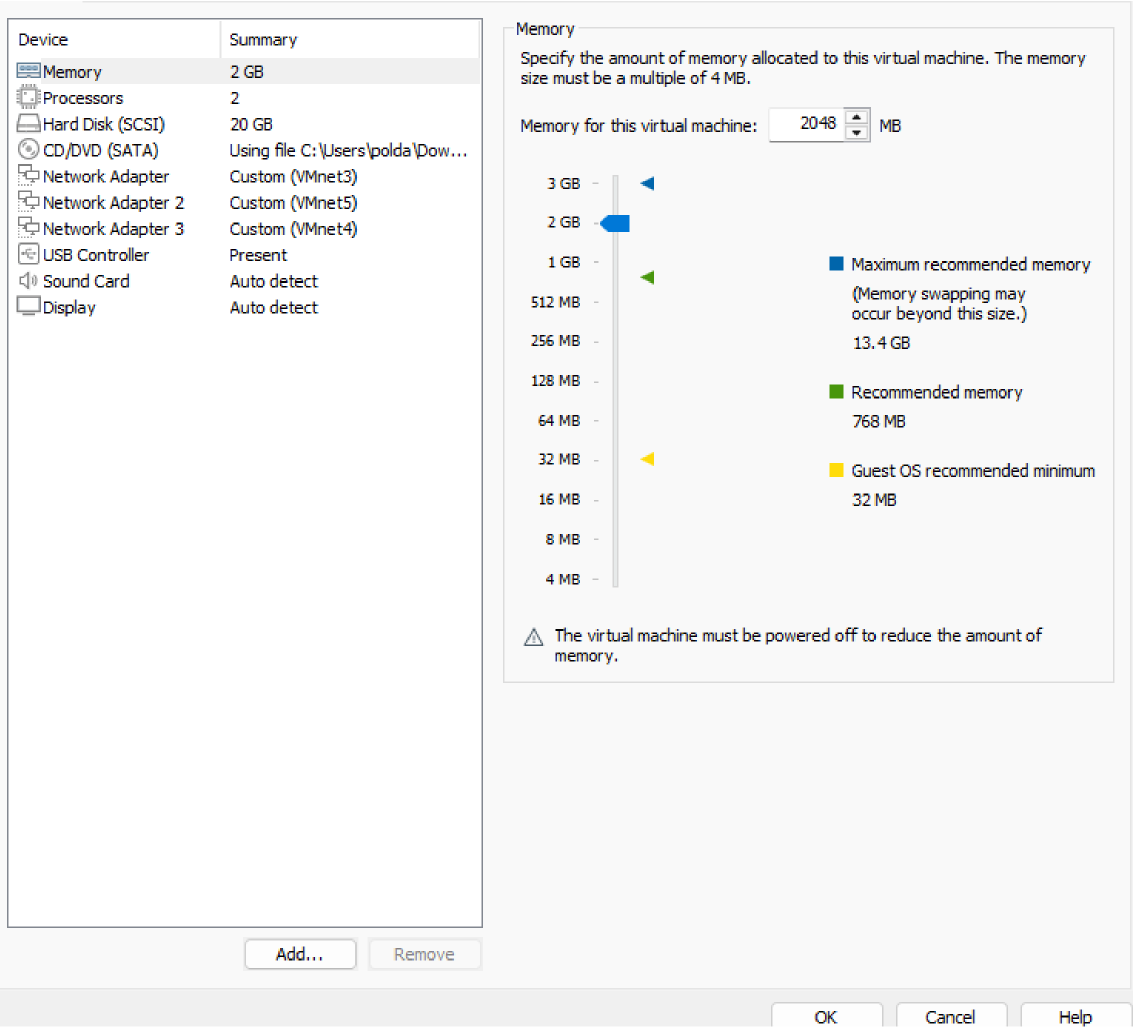
Netgate Services And Support

Retrieving support information

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.143.134
LAN	↑	1000baseT <full-duplex>	192.168.1.1

Ahora vamos a configurar el ipfire:



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Users\polda\Dow...
Network Adapter	Custom (VMnet3)
Network Adapter 2	Custom (VMnet5)
Network Adapter 3	Custom (VMnet4)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

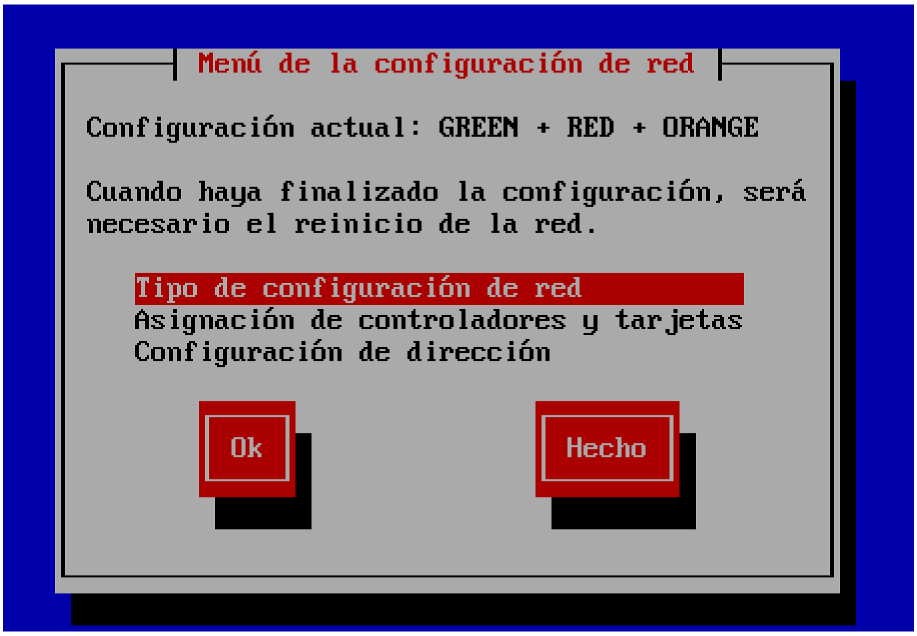
Memory for this virtual machine: 2048 MB

🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.4 GB

🟩 Recommended memory
768 MB

🟨 Guest OS recommended minimum
32 MB

⚠ The virtual machine must be powered off to reduce the amount of memory.

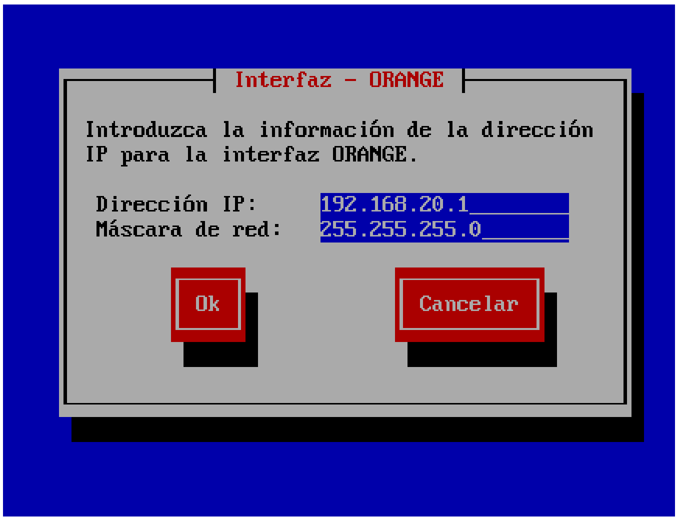


Menú de la configuración de red

Configuración actual: GREEN + RED + ORANGE

Cuando haya finalizado la configuración, será necesario el reinicio de la red.

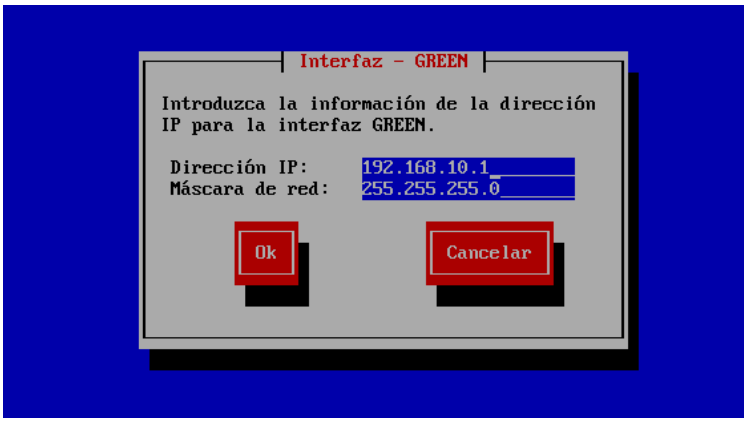
Tipo de configuración de red
Asignación de controladores y tarjetas
Configuración de dirección



Interfaz - ORANGE

Introduzca la información de la dirección
IP para la interfaz ORANGE.

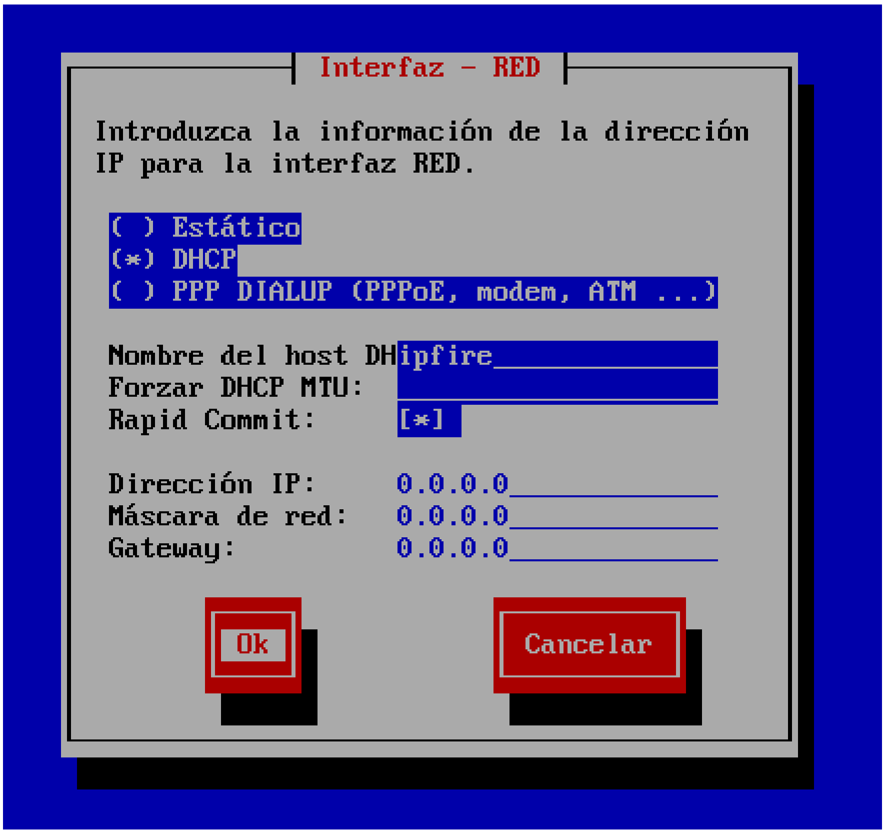
Dirección IP: 192.168.20.1
Máscara de red: 255.255.255.0



Interfaz - GREEN

Introduzca la información de la dirección
IP para la interfaz GREEN.

Dirección IP: 192.168.10.1
Máscara de red: 255.255.255.0



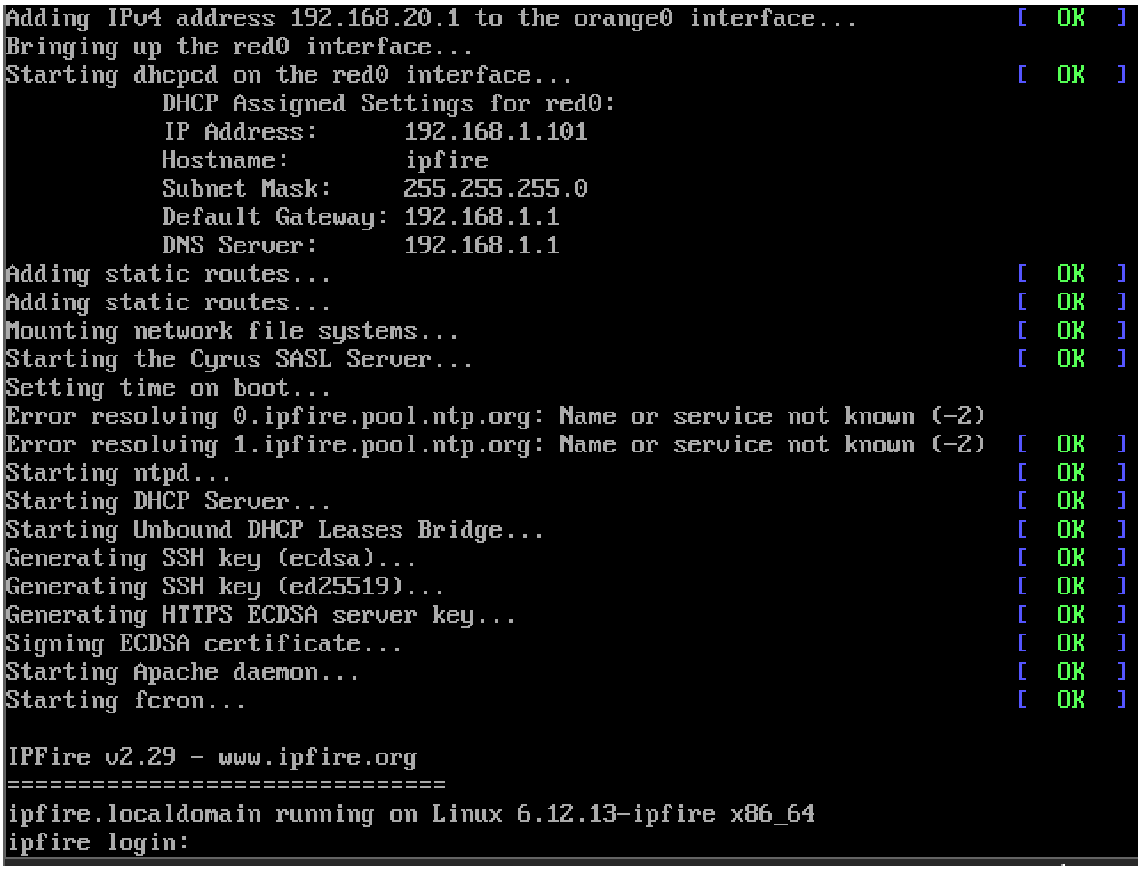
Interfaz - RED

Introduzca la información de la dirección
IP para la interfaz RED.

( ) Estático
(*) DHCP
( ) PPP DIALUP (PPPoE, modem, ATM ...)

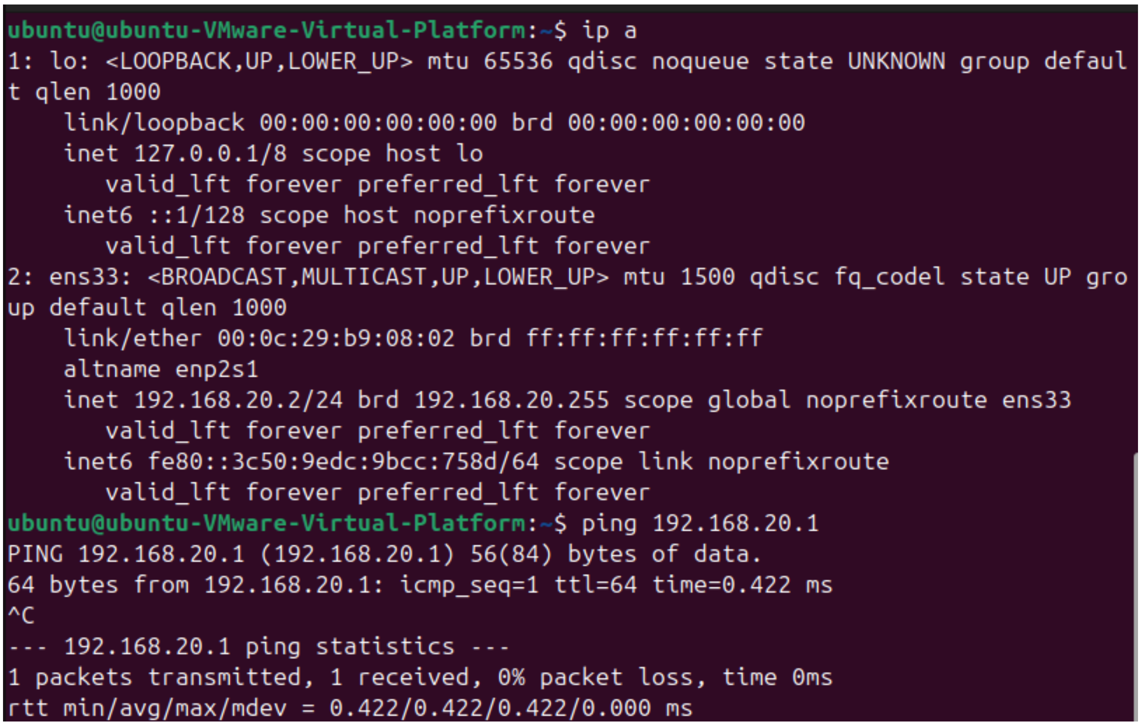
Nombre del host DHipfire
Forzar DHCP MTU:
Rapid Commit: [*]

Dirección IP: 0.0.0.0
Máscara de red: 0.0.0.0
Gateway: 0.0.0.0



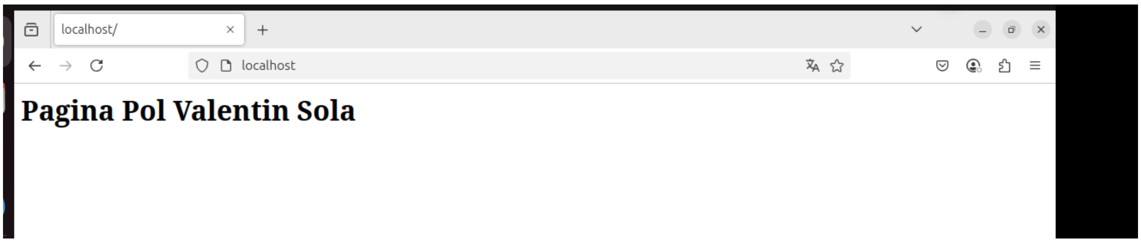
```
Adding IPv4 address 192.168.20.1 to the orange0 interface...          [  OK  ]
Bringing up the red0 interface...
Starting dhcpcd on the red0 interface...                              [  OK  ]
           DHCP Assigned Settings for red0:
           IP Address:       192.168.1.101
           Hostname:         ipfire
           Subnet Mask:      255.255.255.0
           Default Gateway:  192.168.1.1
           DNS Server:       192.168.1.1
Adding static routes...                                               [  OK  ]
Adding static routes...                                               [  OK  ]
Mounting network file systems...                                      [  OK  ]
Starting the Cyrus SASL Server...                                     [  OK  ]
Setting time on boot...
Error resolving 0.ipfire.pool.ntp.org: Name or service not known (-2)
Error resolving 1.ipfire.pool.ntp.org: Name or service not known (-2) [  OK  ]
Starting ntpd...                                                      [  OK  ]
Starting DHCP Server...                                               [  OK  ]
Starting Unbound DHCP Leases Bridge...                                [  OK  ]
Generating SSH key (ecdsa)...                                         [  OK  ]
Generating SSH key (ed25519)...                                       [  OK  ]
Generating HTTPS ECDSA server key...                                  [  OK  ]
Signing ECDSA certificate...                                          [  OK  ]
Starting Apache daemon...                                             [  OK  ]
Starting fcron...                                                     [  OK  ]

IPFire v2.29 - www.ipfire.org
===============================
ipfire.localdomain running on Linux 6.12.13-ipfire x86_64
ipfire login:
```

Servidor web – Orange:



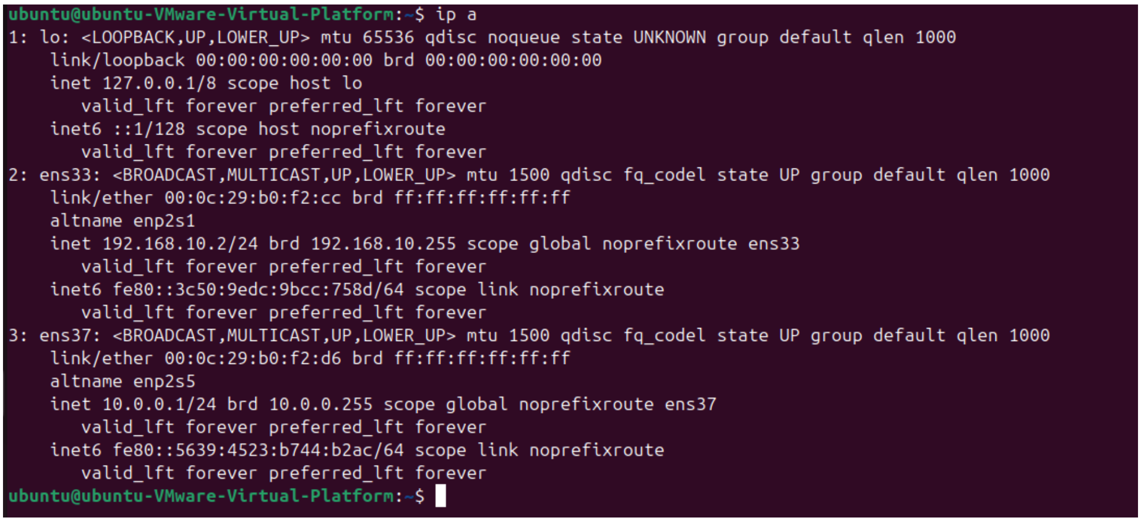
```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:b9:08:02 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.2/24 brd 192.168.20.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::3c50:9edc:9bcc:758d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=0.422 ms
^C
--- 192.168.20.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.422/0.422/0.422/0.000 ms
```

Pagina configurada amb apache:

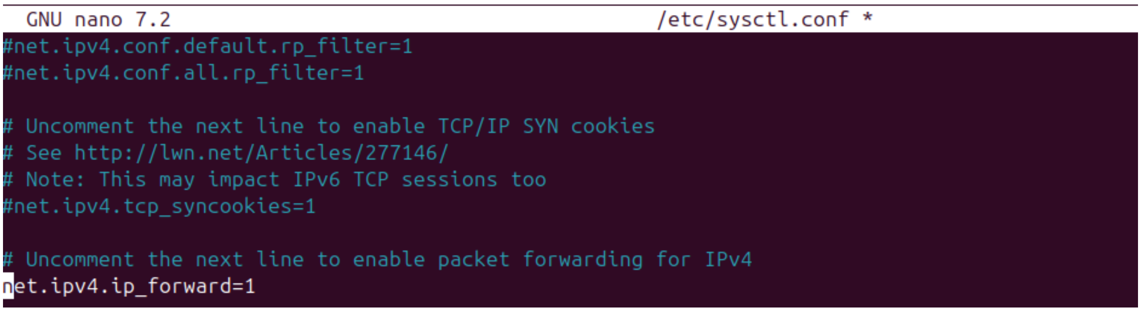


Pagina Pol Valentin Sola

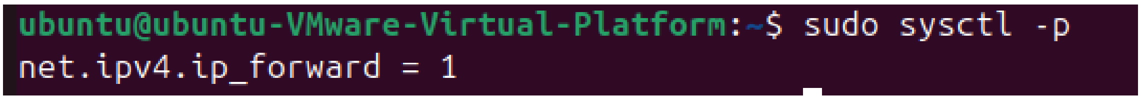
Ubuntu iptables:



```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b0:f2:cc brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.2/24 brd 192.168.10.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::3c50:9edc:9bcc:758d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b0:f2:d6 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.0.0.1/24 brd 10.0.0.255 scope global noprefixroute ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::5639:4523:b744:b2ac/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

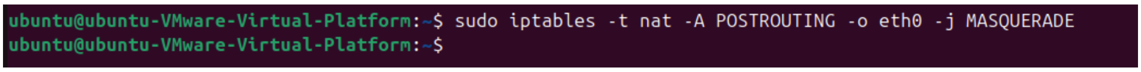


```
  GNU nano 7.2                              /etc/sysctl.conf *
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

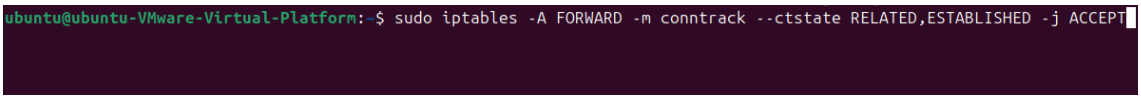


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
```

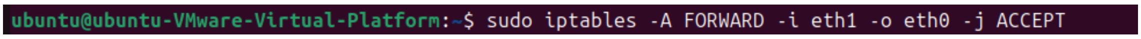
Iptables:



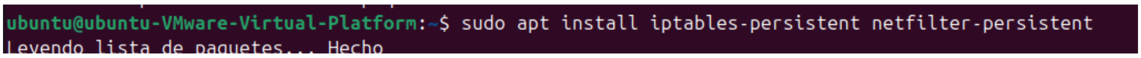
```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```



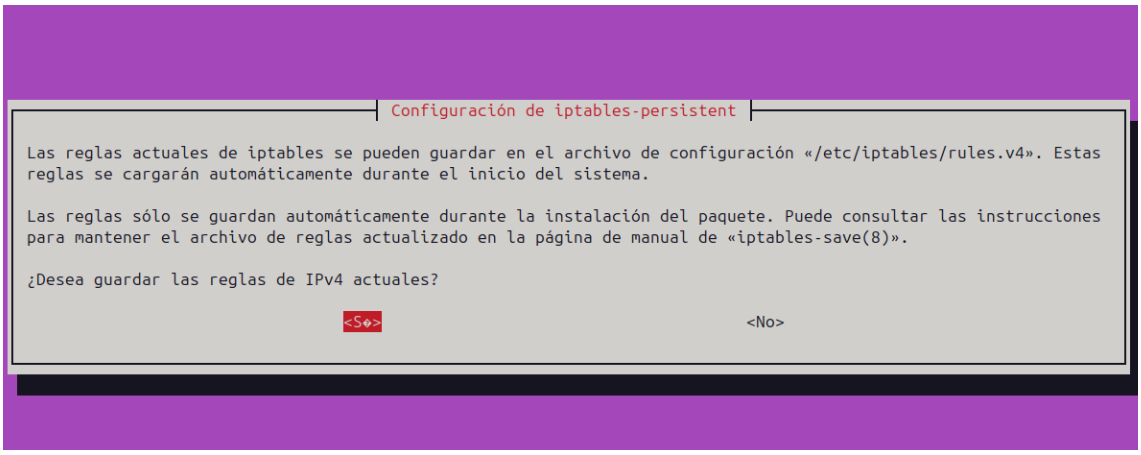
```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```



```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

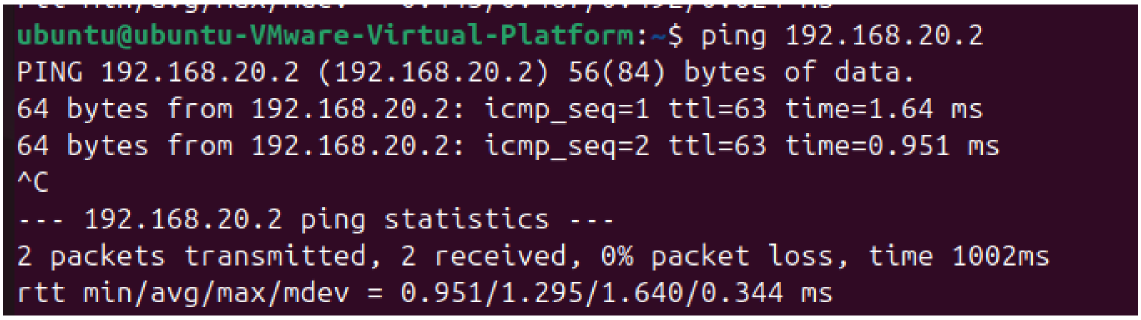


```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ sudo apt install iptables-persistent netfilter-persistent
Leyendo lista de paquetes... Hecho
```

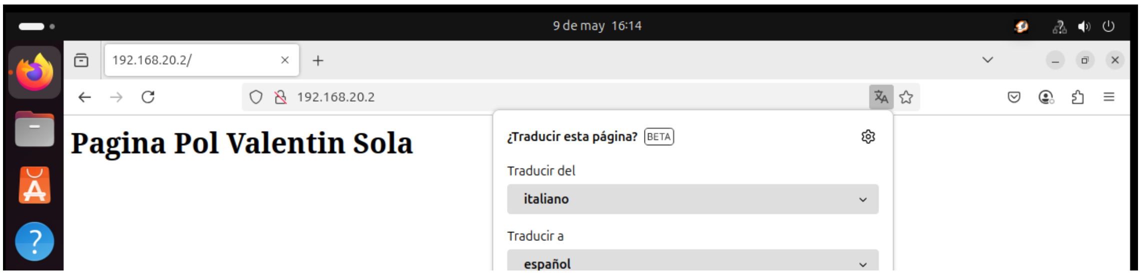


```
Configuración de iptables-persistent

Las reglas actuales de iptables se pueden guardar en el archivo de configuración «/etc/iptables/rules.v4». Estas
reglas se cargarán automáticamente durante el inicio del sistema.

Las reglas sólo se guardan automáticamente durante la instalación del paquete. Puede consultar las instrucciones
para mantener el archivo de reglas actualizado en la página de manual de «iptables-save(8)».

¿Desea guardar las reglas de IPv4 actuales?

                    <Sí>                                            <No>
```

Comprobamos que podemos acceder a la web:



```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=1.64 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=0.951 ms
^C
--- 192.168.20.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.951/1.295/1.640/0.344 ms
```



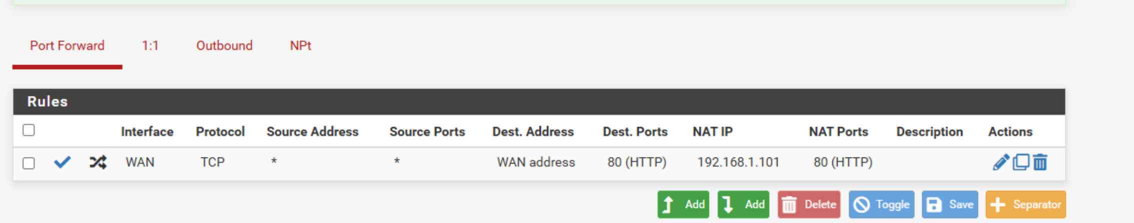
Pagina Pol Valentin Sola

¿Traducir esta página? BETA

Traducir del: italiano

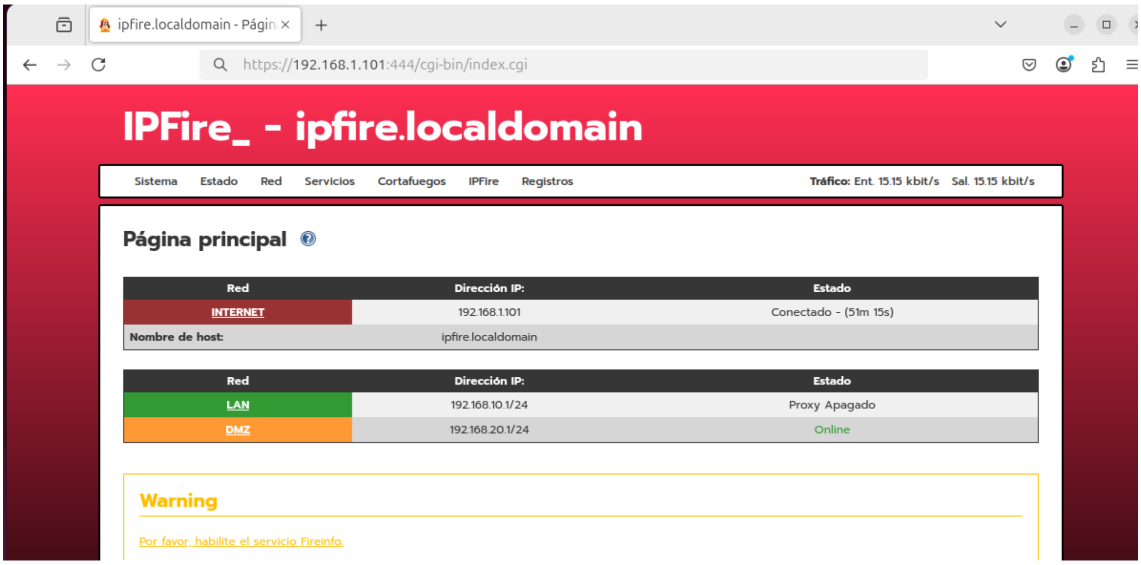
Traducir a: español

Creacion de reglas para redirigir las peticiones de WAN al IPFIRE:



Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.101	80 (HTTP)		


ipfire.localdomain - Págin ×
https://192.168.1.101:444/cgi-bin/index.cgi
Sistema
Estado
Red
Servicios
Cortafuegos
IPFire
Registros

IPFire_ - ipfire.localdomain

Tráfico: Ent. 15.15 kbit/s Sal. 15.15 kbit/s

Página principal

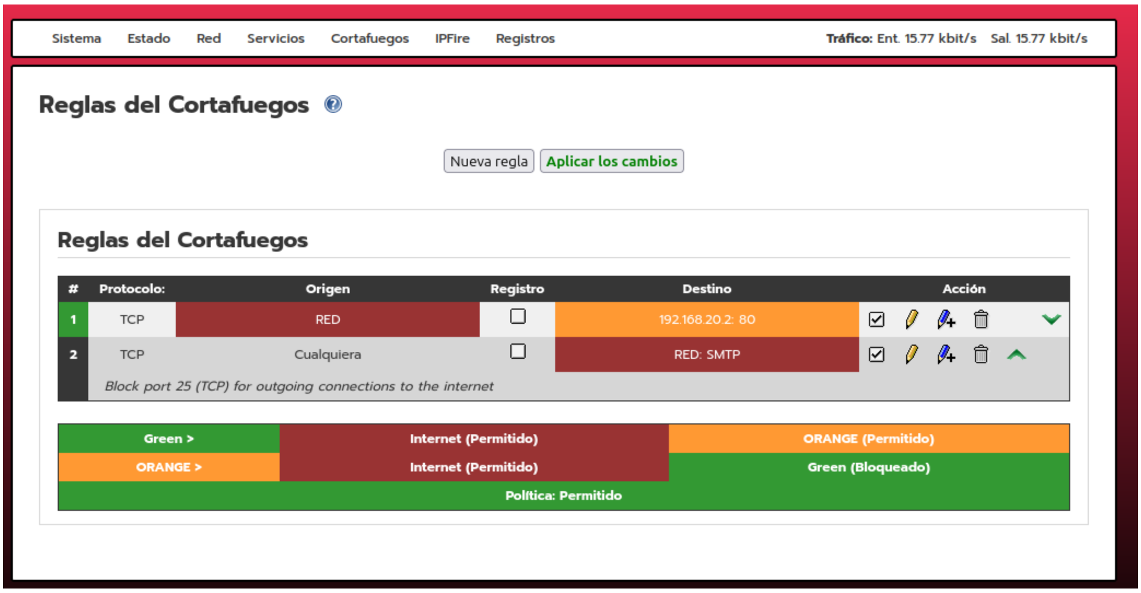
Red	Dirección IP:	Estado
INTERNET	192.168.1.101	Conectado - (51m 15s)
Nombre de host:	ipfire.localdomain	

Red	Dirección IP:	Estado
LAN	192.168.10.1/24	Proxy Apagado
DMZ	192.168.20.1/24	Online

Warning

Por favor, habilite el servicio Fireinfo.

Y ahora creamos la regla para redirigir las peticiones de la ip x.x.1.101 a la x.x.20.2 (orange)



Tráfico: Ent. 15.77 kbit/s Sal. 15.77 kbit/s

Reglas del Cortafuegos

Reglas del Cortafuegos

#	Protocolo:	Origen	Registro	Destino	Acción
1	TCP	RED	□	192.168.20.2: 80	☑
2	TCP	Cualquiera	□	RED: SMTP	☑
	Block port 25 (TCP) for outgoing connections to the internet				

Green >	Internet (Permitido)	ORANGE (Permitido)
ORANGE >	Internet (Permitido)	Green (Bloqueado)
Política: Permitido		