

Este seria el cortafuegos que e creado para mi router:

```
GNU nano 2.5.3 Archivo: cortafuegos.sh

#!/bin/bash

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

echo 1

#router
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

echo 1

#wifi (rojo)
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp -m multiport --dport 80,443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 3

#Verde
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s8 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s10 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
[ 50 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text ^J Justificar ^C Posición ^Y Pág. ant.
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar txt ^T Corrector ^_ Ir a línea ^U Pág. sig.
```

```
GNU nano 2.5.3 Archivo: cortafuegos.sh

iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

echo 1

#wifi (rojo)
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp -m multiport --dport 80,443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 3

#Verde
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s8 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s10 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 4

#http
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
echo 5

#internet
iptables -A FORWARD -i enp0s10 -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s8 -m state --state ESTABLISHED,RELATED -j ACCEPT
echo 6

#router
iptables -A INPUT -i enp0s3 -s 10.0.0.20 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -s 10.0.0.20 -j ACCEPT
echo 7

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text ^J Justificar ^C Posición ^Y Pág. ant.
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar txt ^T Corrector ^_ Ir a línea ^U Pág. sig.
```

Lo ejecutamos y vemos que no nos da ningún problema

```
root@route:/home/route# bash cortafuegos.sh
1
1
3
4
5
6
7
root@route:/home/route# _
```