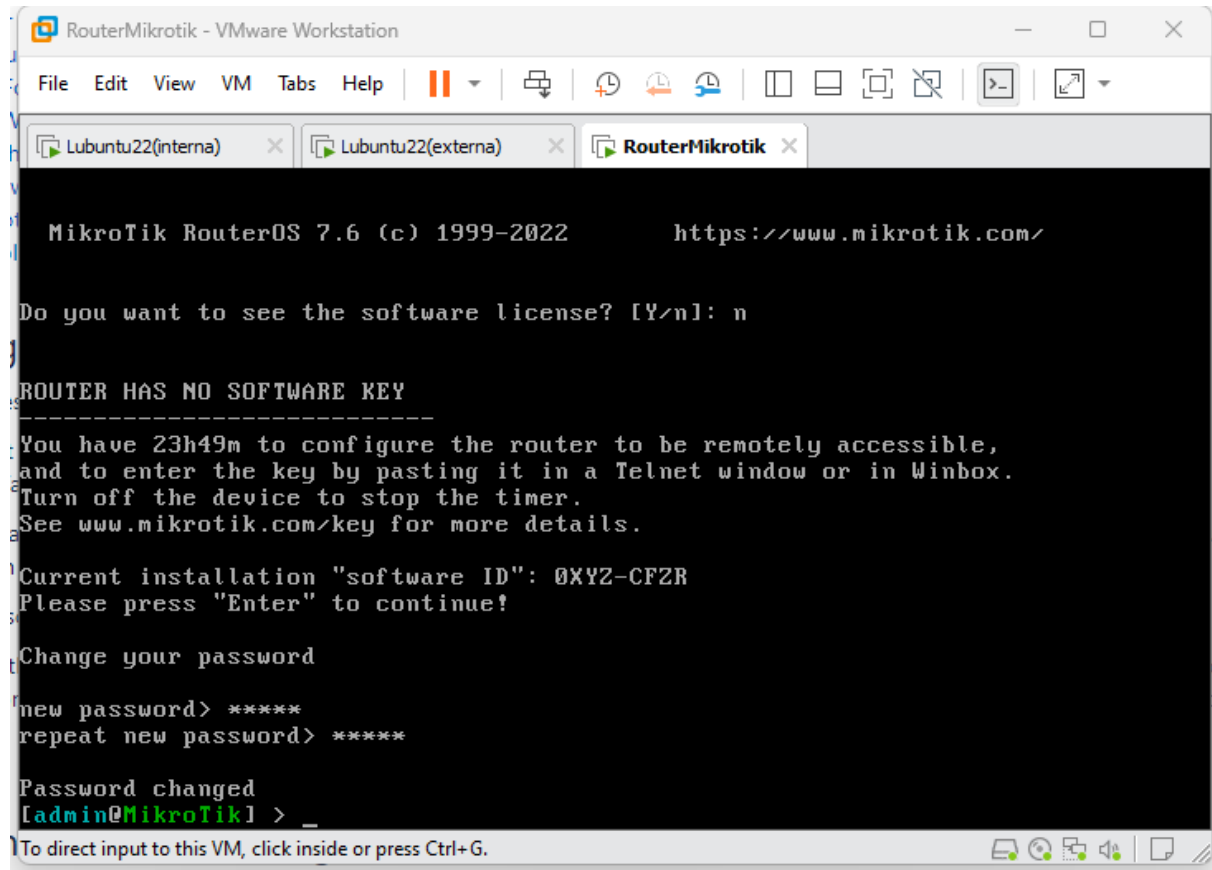


Practica Examen con Mikrotik

Configuración inicial.

Lo primero que nos aparece al arrancar por primera vez Mikrotik es una cuenta atrás de 24 horas, que es el periodo que tenemos para usarlo a menos que introduzcamos una clave.



```
RouterMikrotik - VMware Workstation
File Edit View VM Tabs Help
Lubuntu22(interna) x Lubuntu22(externa) x RouterMikrotik x

MikroTik RouterOS 7.6 (c) 1999-2022      https://www.mikrotik.com/

Do you want to see the software license? [Y/n]: n

ROUTER HAS NO SOFTWARE KEY
-----
You have 23h49m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.


Current installation "software ID": 0XYZ-CFZR
Please press "Enter" to continue!

Change your password
new password> *****
repeat new password> *****

Password changed
[admin@MikroTik] > _

To direct input to this VM, click inside or press Ctrl+G.
```

Conseguir una clave es tan fácil como registrarse en la pagina oficial e introducir el “software ID”.



HomeAboutBuyJobsHardwareSoftwareSupportTrainingAccount

My accountLog out cesgilher@gmail.com

Toggle menu

ACCOUNT INFORMATION

ome

alance

dit account details

dit email settings

UM registration history

anage employees

vents New

EB ORDERS

y web orders and invoices

urchase a RouterOS license key

OUTEROS KEYS

earch and view all keys

equest RouterBOARD license key

ansfer prepaid keys (none)

ake a demo key

HR LICENCES

il CHR keys

HR orders and invoices

ansfer CHR prepaid keys (none)

RAINING

y training sessions

y certificates

UPPORT

y support tickets

upport.rtf viewer

Make a demo key

Free Demo (Trial) License Key for RouterOS 2.9 and up

- demo (trial) license key is level 1 key
- has limits of maximum connections each for PPTP, PPPoE, Queues, NAT, EoIP, and DHCP
- does not have wireless interface support
- does not include version upgrades
- does not expire (no time limit)
- does not include support
- not for resale

After you install the router it will report a Software ID.

Place in folder:

Software ID

root

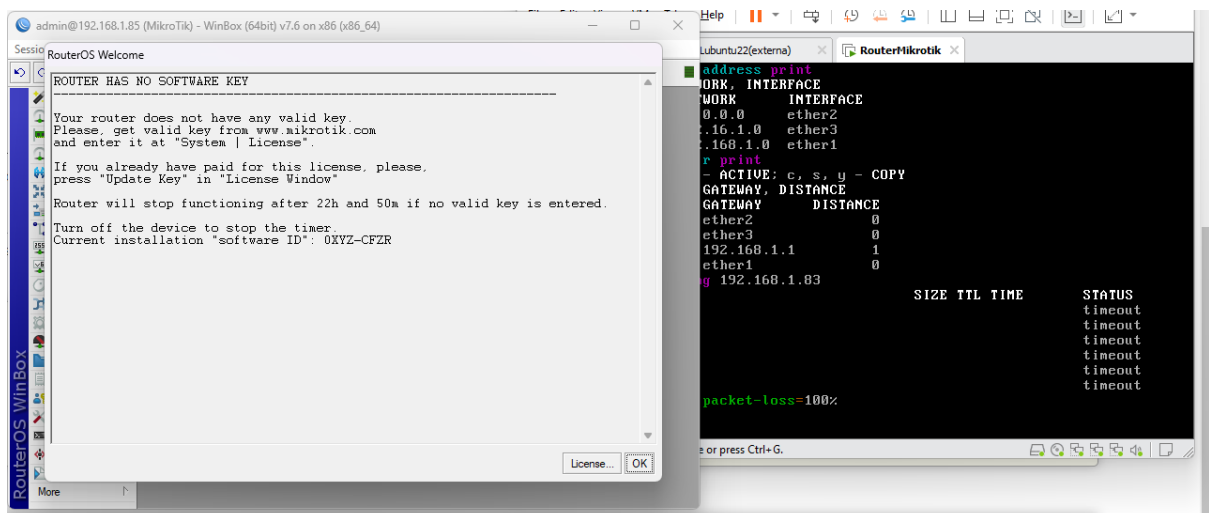
0XYZ-CFZR

☒ Send key to my email (cesgilher@gmail.com).

Note: This key works with any installation method. Only for 2.9 and up.

Generate

Ahora bien por ssh o telnet introducimos la clave que nos han proporcionado y activamos el producto. No tiene todas las aplicaciones que la versión de pago, pero suficientes para hacer la práctica. Yo en este caso he usado winbox poninedole el bridge a la maquina.



The screenshot shows the Mikrotik WinBox interface. The main window displays the "RouterOS Welcome" screen with the following text:

```
ROUTER HAS NO SOFTWARE KEY
-----
Your router does not have any valid key.
Please, get valid key from www.mikrotik.com
and enter it at "System | License".

If you already have paid for this license, please,
press "Update Key" in "License Window".

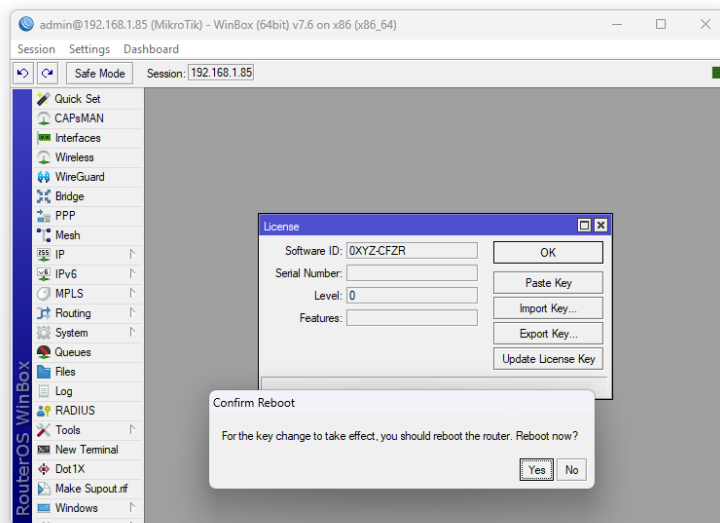
Router will stop functioning after 22h and 50m if no valid key is entered.
Turn off the device to stop the timer.
Current installation "software ID": 0XYZ-CFZR
```

Below the text is a "License..." button and an "OK" button. In the background, a terminal window is open, showing the output of the `print` command:

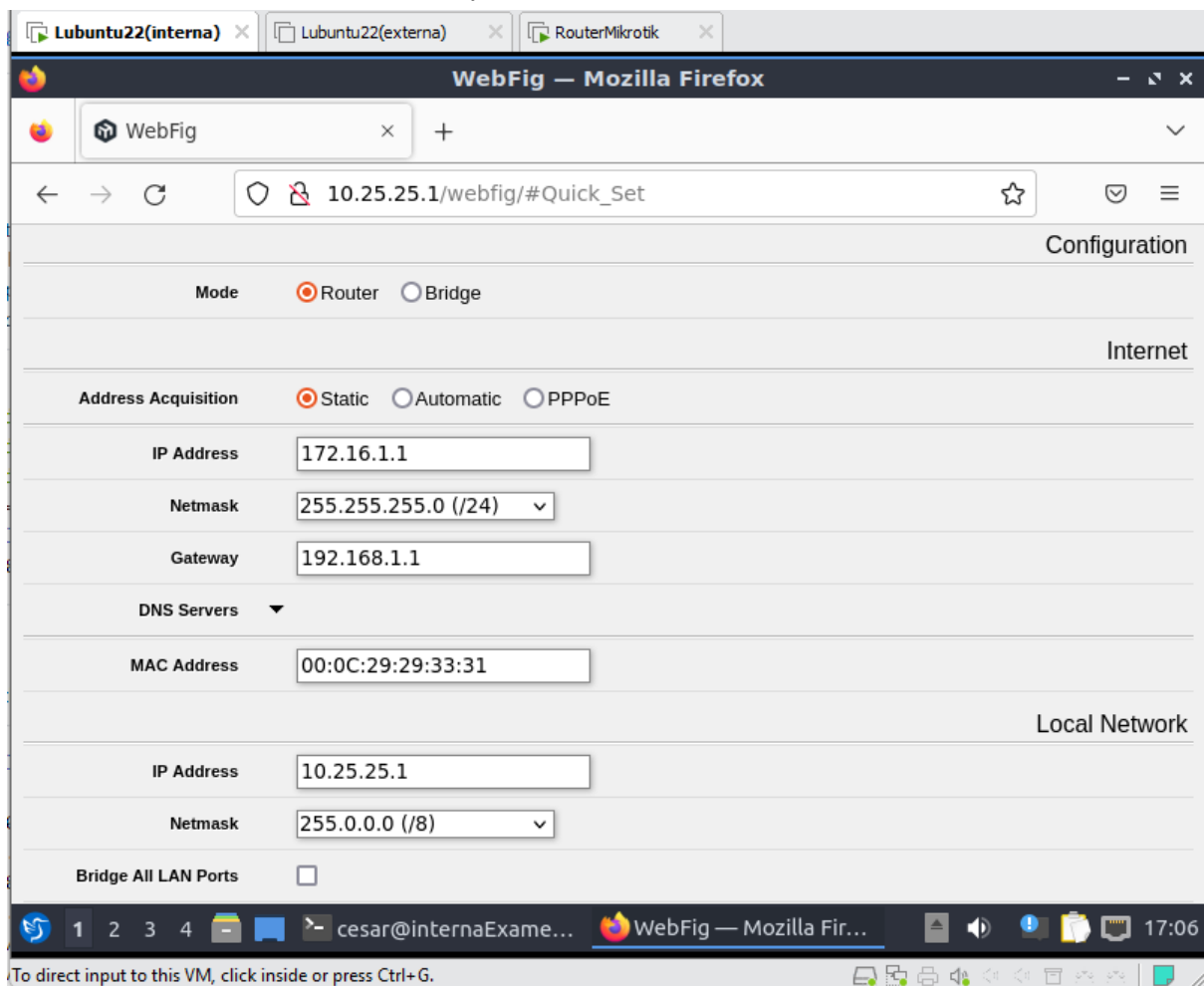
```
print
-----
ACTIVE; c, s, u - COPY
GATEWAY, DISTANCE
GATEWAY, DISTANCE
ether2, 0
ether3, 0
192.168.1.1, 1
ether1, 0
192.168.1.83
SIZE TTL TIME STATUS
timeout
timeout
timeout
timeout
timeout
packet-loss=100%
```

Añadimos la clave.

```
-----BEGIN MIKROTIK SOFTWARE KEY-----  
4hQ+1ew10QHxKSPJFRpOud4BYGxmHgHsl8gN/K1WRq  
wz+UznKJL1jEb8aLNUnOj+KVQuqnjLMh7W8Xccc2NA==  
-----END MIKROTIK SOFTWARE KEY-----
```



Ahora que ya tengo el producto activado, he quitado el birdge y he vuelto a poner las dos redes internas, la del cliente y la del servidor.



También he editado el nombre de los interfaces de red para tener mas claro cuál es cuál.

RouterOS v7.6 (stable)

Quick Set

WebFig

Terminal

Interface

Interface List

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VXLAN

Interface List

MACsec

Bonding

LTE

VRF

VRRP

VETH

Add New ▼

Detect Internet

2 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx
	R	ether2(EXTERNA)	Ethernet	1500		0 bps	0 bps
	R	ether3(INTERNA)	Ethernet	1500		11.8 kbps	4.3 kbps

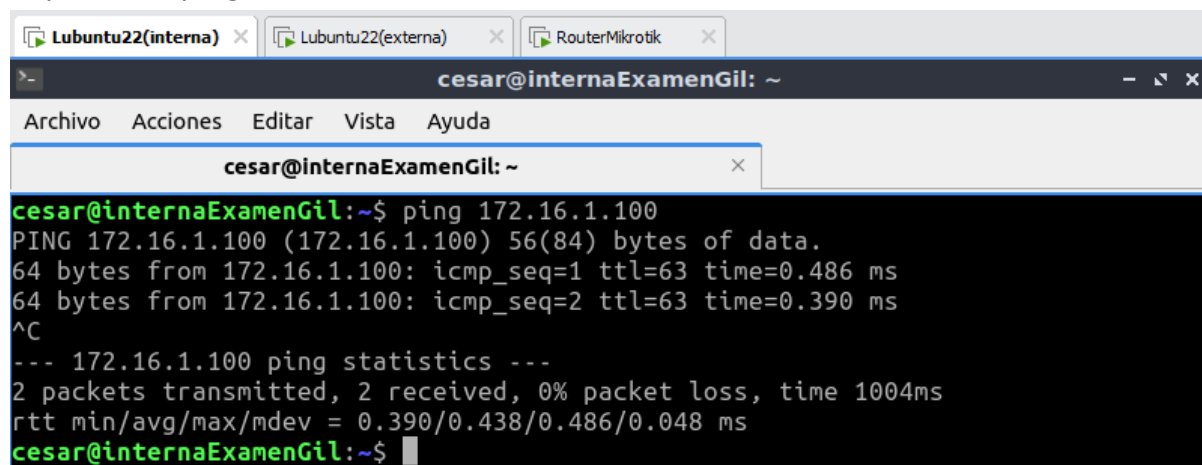
Tiene un montón de opciones a la hora de crear cada regla, no estoy ni medio en broma(todas esas opciones son para la misma regla).

The image is a collage of four screenshots from the RouterExamenGill web interface, showing different configuration tabs for a new firewall rule.

- Top Left:** The 'New Firewall Rule' dialog box is open, showing the 'General' tab. The rule is named 'New Firewall Rule at...stable' and is currently 'Enabled'. The 'Chain' is set to 'input'. The 'Src. Address', 'Dst. Address', 'Src. Address List', 'Dst. Address List', and 'Protocol' fields are visible.
- Top Right:** The 'New Firewall Rule' dialog box is open, showing the 'Action' tab. The 'Action' is set to 'accept'.
- Bottom Left:** The 'New Firewall Rule' dialog box is open, showing the 'Advanced' tab. This tab contains various settings including 'Connection Type', 'Connection State', 'Connection NAT State', 'Layer7 Protocol', 'Content', 'Connection Bytes', 'Connection Rate', 'Per Connection Classifier', 'Src. MAC Address', and 'Out. Bridge Port'.
- Bottom Right:** The 'New Firewall Rule' dialog box is open, showing the 'Statistics' tab. This tab displays a table of statistics including 'Bytes', 'Packets', 'Rate', and 'Packet Rate'. Below the table is a 'Rate Graph' section.

Ping interno a externo con todo en ACCEPT.

Captura del ping.

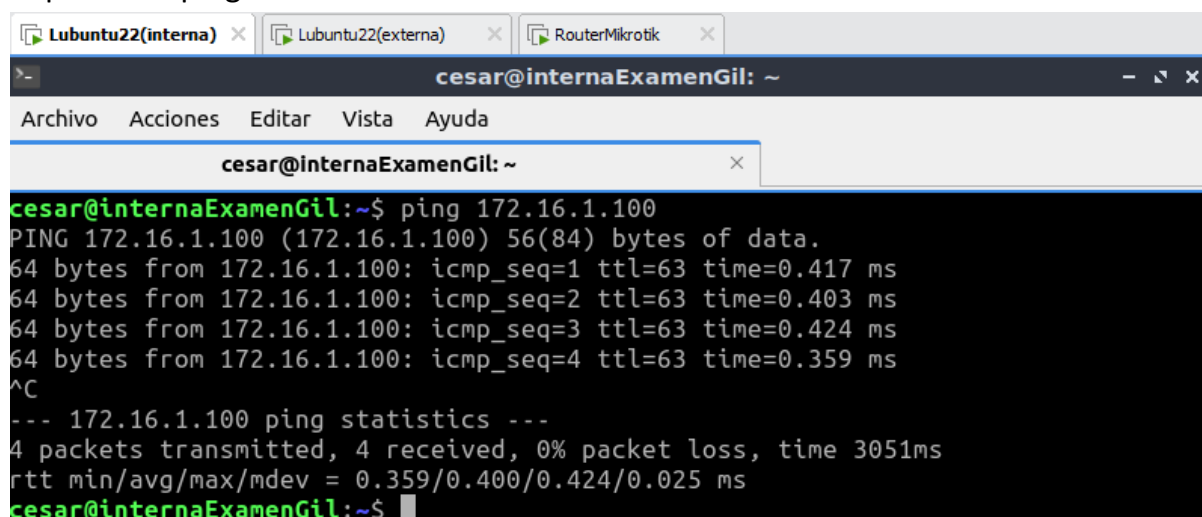


The screenshot shows a terminal window titled 'cesar@internaExamenGil: ~'. The terminal output shows a successful ping from 172.16.1.100 to 172.16.1.100. The ping statistics show 2 packets transmitted, 2 received, 0% packet loss, and a time of 1004ms. The round-trip times (rtt) are 0.390ms, 0.438ms, 0.486ms, and 0.048ms.

```
cesar@internaExamenGil:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=0.486 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=0.390 ms
^C
--- 172.16.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.390/0.438/0.486/0.048 ms
cesar@internaExamenGil:~$
```

Con todo en DROP, Ping interno a externo pero al revés no.

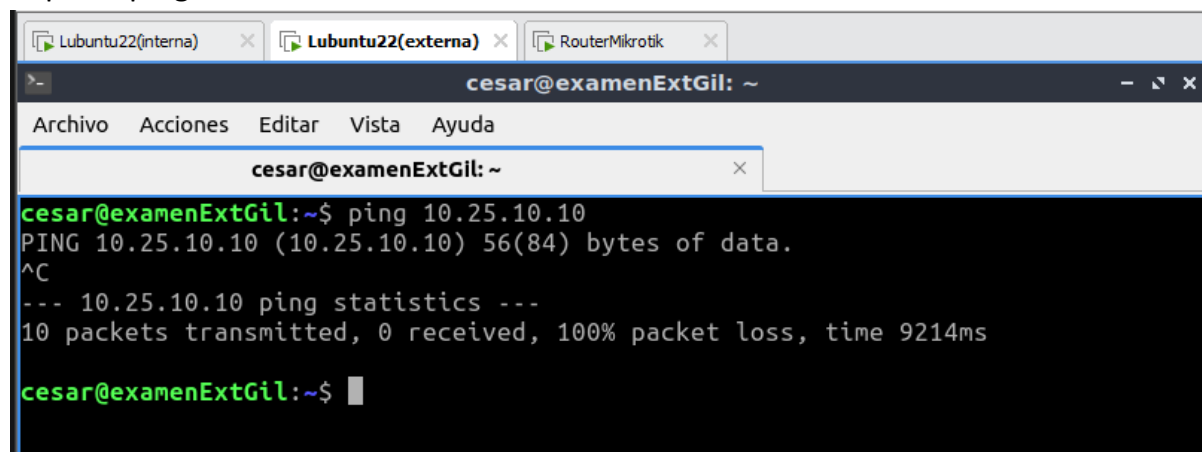
Captura del ping.



The screenshot shows a terminal window titled 'cesar@internaExamenGil: ~'. The terminal output shows a successful ping from 172.16.1.100 to 172.16.1.100. The ping statistics show 4 packets transmitted, 4 received, 0% packet loss, and a time of 3051ms. The round-trip times (rtt) are 0.359ms, 0.400ms, 0.424ms, and 0.025ms.

```
cesar@internaExamenGil:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=0.417 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=0.403 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=0.424 ms
64 bytes from 172.16.1.100: icmp_seq=4 ttl=63 time=0.359 ms
^C
--- 172.16.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.359/0.400/0.424/0.025 ms
cesar@internaExamenGil:~$
```

Captura ping fallido externo-interno.



The screenshot shows a terminal window titled 'cesar@examenExtGil: ~'. The terminal output shows a failed ping from 10.25.10.10 to 10.25.10.10. The ping statistics show 10 packets transmitted, 0 received, 100% packet loss, and a time of 9214ms.

```
cesar@examenExtGil:~$ ping 10.25.10.10
PING 10.25.10.10 (10.25.10.10) 56(84) bytes of data.
^C
--- 10.25.10.10 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9214ms
cesar@examenExtGil:~$
```

Regla para el ping con todo a drop.(tanto la norma desde el router como desde el entorno grafico).

```
[admin@routerExamenGil] > ip firewall filter print chain=forward
Flags: X - disabled, I - invalid; D - dynamic
 0 chain=forward action=accept protocol=icmp in-interface=ether3(INTERNA)
   out-interface=ether2(EXTERNA) icmp-options=8:0-255 log=no log-prefix=""

 1 chain=forward action=accept protocol=icmp in-interface=ether2(EXTERNA)
   out-interface=ether3(INTERNA) icmp-options=0:0-255 log=no log-prefix=""

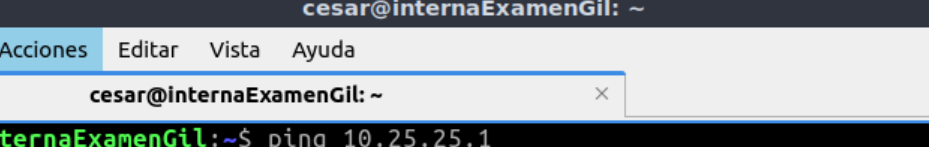
 2 chain=forward action=drop log=no log-prefix=""
[admin@routerExamenGil] >
```

Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Bytes	P
✔ accept	input					6 (tcp)		80		ether3(INT				615.5 KiB	3
✘ drop	input									all ethernet				852 B	1
✔ accept	forward					1 (icmp)				ether3(INT	ether2(EXT			588 B	7
✔ accept	forward					1 (icmp)				ether2(EXT	ether3(INT			588 B	7
✘ drop	forward													1932 B	2
✔ accept	output										ether3(INT			0 B	0
✔ accept	output					6 (tcp)					ether3(INT			1801.9 KiB	4
✘ drop	output													0 B	0

La única forma de poner las políticas en drop que he encontrado ha sido con una regla que los restrinja todo. Hay que tener cuidado del orden en que quedan las reglas, es decir, las drop deberían estar abajo del todo.

Ping interno a router pero al revés no.

Captura del ping.



The screenshot shows a terminal window titled "cesar@internaExamenGil: ~". The window has a menu bar with "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The terminal output shows a successful ping to 10.25.25.1. The first two lines of output are "PING 10.25.25.1 (10.25.25.1) 56(84) bytes of data." and "64 bytes from 10.25.25.1: icmp_seq=1 ttl=64 time=0.216 ms". The third line is "64 bytes from 10.25.25.1: icmp_seq=2 ttl=64 time=0.216 ms". The fourth line is "^C". The fifth line is "--- 10.25.25.1 ping statistics ---". The sixth line is "2 packets transmitted, 2 received, 0% packet loss, time 1021ms". The seventh line is "rtt min/avg/max/mdev = 0.216/0.216/0.216/0.000 ms". The eighth line is "cesar@internaExamenGil:~\$". The ninth line is "::1 ip6-localhost". The tenth line is "ff02::1 ip6-allnodes ip6-loopback". The eleventh line is "ff02::2 ip6-allrouters localhost". The twelfth line is "cesar@internaExamenGil:~\$".

```
cesar@internaExamenGil:~$ ping 10.25.25.1
PING 10.25.25.1 (10.25.25.1) 56(84) bytes of data.
64 bytes from 10.25.25.1: icmp_seq=1 ttl=64 time=0.216 ms
64 bytes from 10.25.25.1: icmp_seq=2 ttl=64 time=0.216 ms
^C
--- 10.25.25.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.216/0.216/0.216/0.000 ms
cesar@internaExamenGil:~$
::1 ip6-localhost
ff02::1 ip6-allnodes ip6-loopback
ff02::2 ip6-allrouters localhost
cesar@internaExamenGil:~$
```

Captura del ping fallido router-interno.

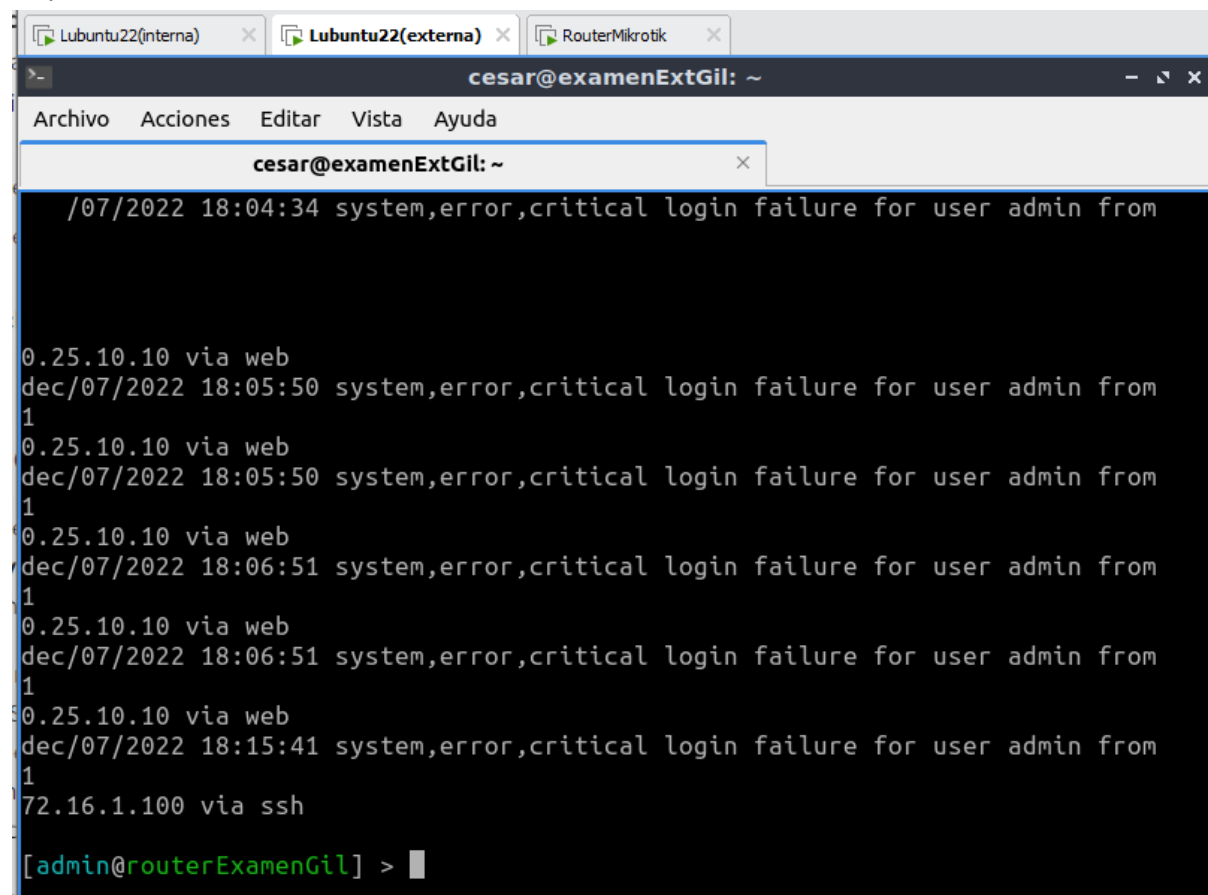
```
Lubuntu22(interna) x Lubuntu22(externa) x RouterMikrotik x
18:05:50 echo: system,error,critical login failure for user admin from 10.25.10
10 via web
[admin@routerExamenGil] >
18:06:51 echo: system,error,critical login failure for user admin from 10.25.10
10 via web
18:06:51 echo: system,error,critical login failure for user admin from 10.25.10
10 via web
[admin@routerExamenGil] > ping 10.25.10.10
  SEQ HOST                                SIZE TTL TIME                        STATUS
    0
    1
    2
    3
    4
    5
    6
    7
    8
    9
   10
sent=11 received=0 packet-loss=100%
[admin@routerExamenGil] >
```

Reglas para permitir el ping del interno al router y no al revés.

```
Lubuntu22(interna) x Lubuntu22(externa) x RouterMikrotik x
0 chain=input action=accept protocol=tcp in-interface=ether3(INTERNA)
  dst-port=80 log=no log-prefix=""
1 chain=input action=accept protocol=icmp in-interface=ether3(INTERNA)
  icmp-options=8:0-255 log=no log-prefix=""
2 chain=input action=drop in-interface=all-ethernet log=no log-prefix=""
3 chain=forward action=accept protocol=icmp in-interface=ether3(INTERNA)
  out-interface=ether2(EXTERNA) icmp-options=8:0-255 log=no log-prefix=""
4 chain=forward action=accept protocol=icmp in-interface=ether2(EXTERNA)
  out-interface=ether3(INTERNA) icmp-options=0:0-255 log=no log-prefix=""
5 chain=forward action=drop log=no log-prefix=""
6 chain=output action=accept connection-state=established
  connection-type="" out-interface=ether3(INTERNA) log=no log-prefix=""
7 chain=output action=accept protocol=tcp out-interface=ether3(INTERNA)
  log=no log-prefix=""
8 chain=output action=accept protocol=icmp out-interface=ether3(INTERNA)
  icmp-options=0:0-255 log=no log-prefix=""
- [Q quit] [D dump] [up] [down]
```

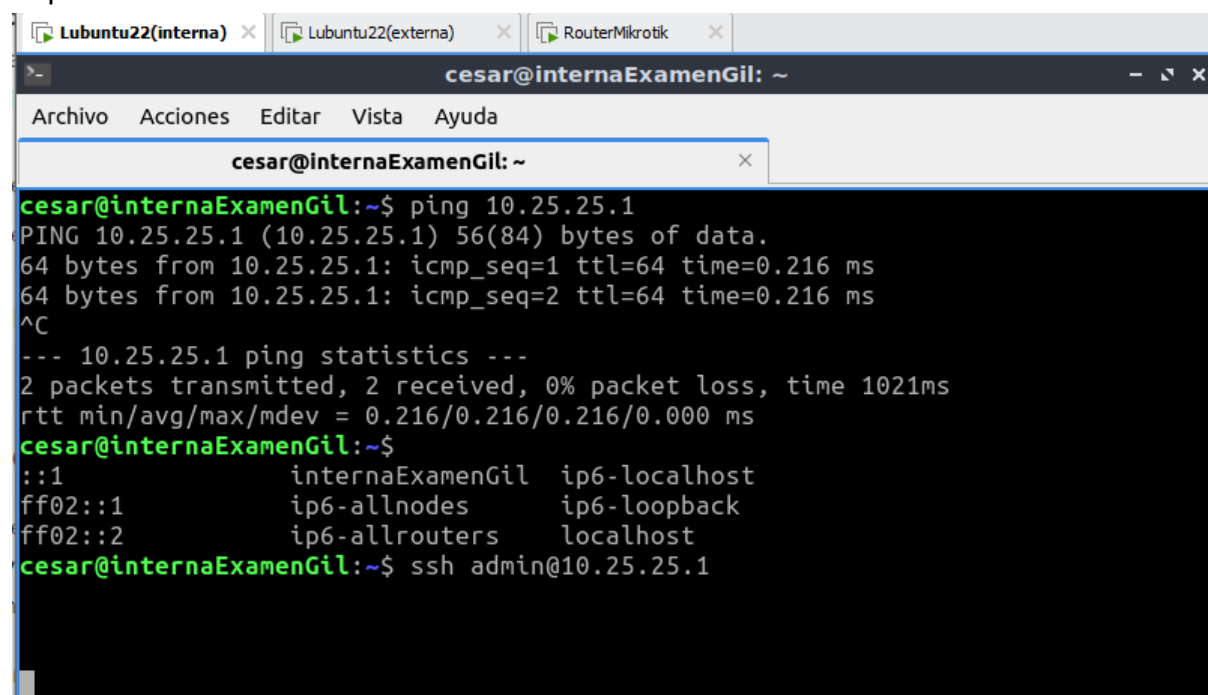

SSH a router desde externo pero no desde el interno.

Captura del ssh.



```
cesar@examenExtGil: ~  
/07/2022 18:04:34 system,error,critical login failure for user admin from  
0.25.10.10 via web  
dec/07/2022 18:05:50 system,error,critical login failure for user admin from  
1  
0.25.10.10 via web  
dec/07/2022 18:05:50 system,error,critical login failure for user admin from  
1  
0.25.10.10 via web  
dec/07/2022 18:06:51 system,error,critical login failure for user admin from  
1  
0.25.10.10 via web  
dec/07/2022 18:06:51 system,error,critical login failure for user admin from  
1  
0.25.10.10 via web  
dec/07/2022 18:15:41 system,error,critical login failure for user admin from  
1  
72.16.1.100 via ssh  
[admin@routerExamenGil] >
```

Captura del ssh desde el interno.



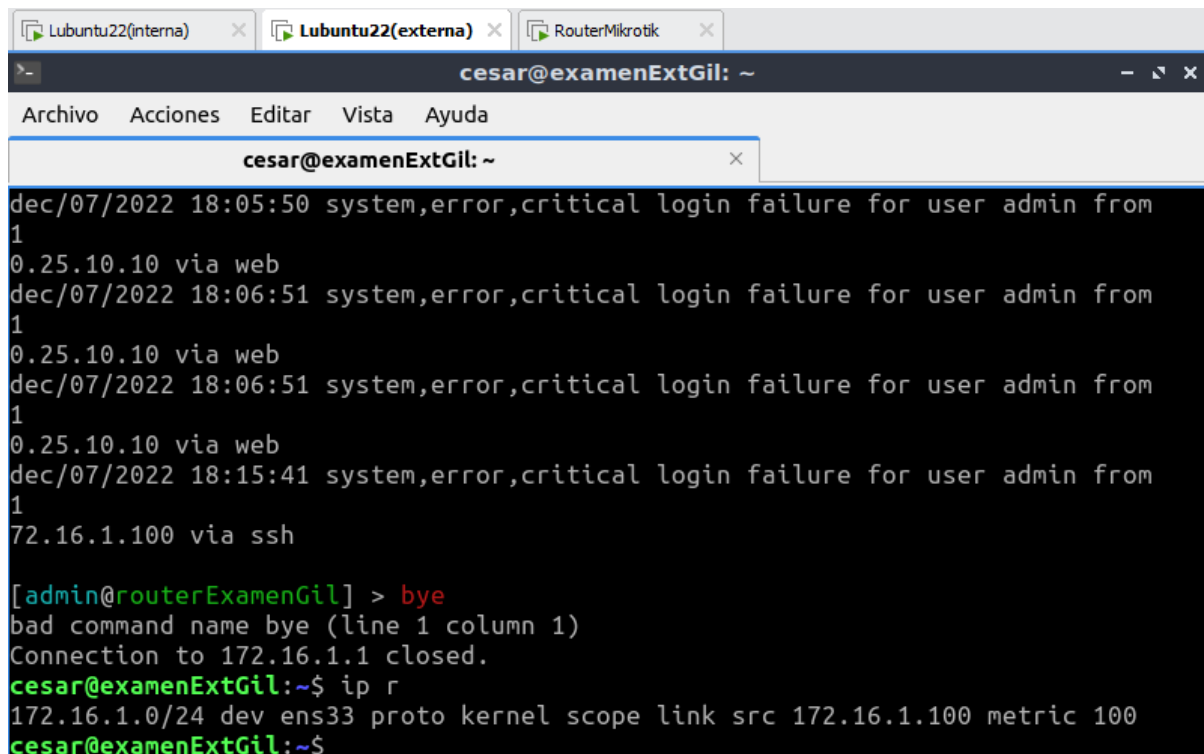
```
cesar@internaExamenGil: ~  
cesar@internaExamenGil:~$ ping 10.25.25.1  
PING 10.25.25.1 (10.25.25.1) 56(84) bytes of data.  
64 bytes from 10.25.25.1: icmp_seq=1 ttl=64 time=0.216 ms  
64 bytes from 10.25.25.1: icmp_seq=2 ttl=64 time=0.216 ms  
^C  
--- 10.25.25.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1021ms  
rtt min/avg/max/mdev = 0.216/0.216/0.216/0.000 ms  
cesar@internaExamenGil:~$  
::1          internaExamenGil    ip6-localhost  
ff02::1      ip6-allnodes      ip6-loopback  
ff02::2      ip6-allrouters    localhost  
cesar@internaExamenGil:~$ ssh admin@10.25.25.1
```

Regla para permitir el ssh.

[illegible]

Externo sin puerta de enlace.

Captura del ip r.

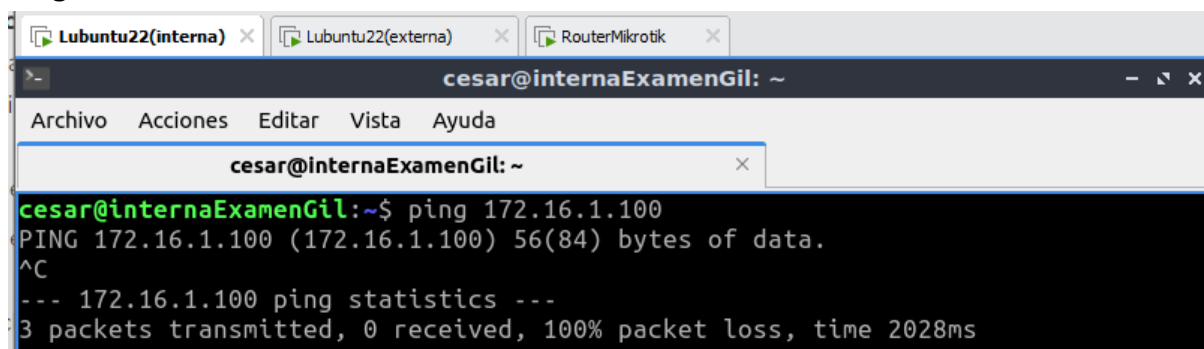


The screenshot shows a terminal window titled 'cesar@examenExtGil: ~'. The window has tabs for 'Lubuntu22(interna)', 'Lubuntu22(externa)', and 'RouterMikrotik'. The terminal output shows three login failure messages for user 'admin' from IP '10.25.10.10' via web, and one login failure for user 'admin' from IP '172.16.1.100' via ssh. The user then enters 'bye' in the router prompt, which results in a 'bad command name' error and a closed connection. Finally, the user runs 'ip r' in the terminal, showing the configuration for the 'ens33' interface.

```
dec/07/2022 18:05:50 system,error,critical login failure for user admin from
10.25.10.10 via web
dec/07/2022 18:06:51 system,error,critical login failure for user admin from
10.25.10.10 via web
dec/07/2022 18:06:51 system,error,critical login failure for user admin from
10.25.10.10 via web
dec/07/2022 18:15:41 system,error,critical login failure for user admin from
172.16.1.100 via ssh

[admin@routerExamenGil] > bye
bad command name bye (line 1 column 1)
Connection to 172.16.1.1 closed.
cesar@examenExtGil:~$ ip r
172.16.1.0/24 dev ens33 proto kernel scope link src 172.16.1.100 metric 100
cesar@examenExtGil:~$
```

Ping fallido interno-externo.



The screenshot shows a terminal window titled 'cesar@internaExamenGil: ~'. The window has tabs for 'Lubuntu22(interna)', 'Lubuntu22(externa)', and 'RouterMikrotik'. The user runs 'ping 172.16.1.100' in the terminal, which results in a '100% packet loss' message.

```
cesar@internaExamenGil:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
^C
--- 172.16.1.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2028ms
```

POSTROUTING para que el ping vuelva a funcionar.

Captura del ping.

```
Lubuntu22(interna) x Lubuntu22(externa) x RouterMikrotik x
cesar@internaExamenGil: ~
Archivo Acciones Editar Vista Ayuda
cesar@internaExamenGil: ~
^C
--- 172.16.1.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2044ms

cesar@internaExamenGil:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=0.494 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=0.489 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=0.561 ms
^C
--- 172.16.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.489/0.514/0.561/0.032 ms
cesar@internaExamenGil:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=0.418 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=0.446 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=0.394 ms
^C
--- 172.16.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.394/0.419/0.446/0.021 ms
```

Norma para activar el postrouting(te subo la regla desde los dos lados).

```
Lubuntu22(interna) x Lubuntu22(externa) x RouterMikrotik x
[admin@routerExamenGil] >
[admin@routerExamenGil] >
[admin@routerExamenGil] >
[admin@routerExamenGil] >
[admin@routerExamenGil] >
[admin@routerExamenGil] > ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
0 chain=srcnat action=masquerade protocol=icmp src-address=10.25.10.10
  out-interface=ether2(EXTERNA) icmp-options=8:0-255 log=no log-prefix=""
```

10.25.25.1/webfig/#IP:Firewall.NAT

Quick Set WebFig Terminal

Rule Raw Service Ports Connections Address Lists Layer7 Protocols Firewall

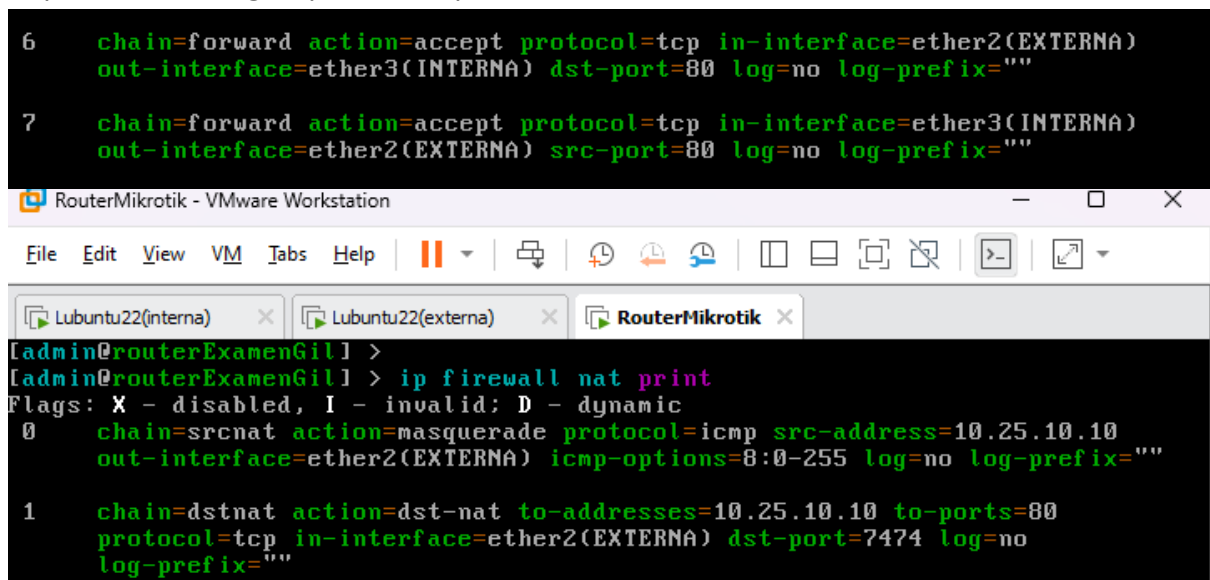
Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface
masquerade	srcnat	10.25.10.10				1 (icmp)					ether2(EXT

PREROUTING para permitir el HTTP desde el externo.

Captura de la conexión HTTP.



Captura de las reglas para el http tanto desde la tabla nat como la tabla filter.



Lista con todas las reglas usadas(se ven tan pequeñas porque es la única forma de que se vea entera todas la regla).

Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Bytes	
✔ accept	input					6 (tcp)		80		ether3(INT				1280.4 KiB	·
✔ accept	input					1 (icmp)				ether3(INT				0 B	·
✔ accept	input					6 (tcp)		22		ether2(EXT				18.6 KiB	·
✖ drop	input									all ethernet				11.4 KiB	·
✔ accept	forward					1 (icmp)				ether3(INT	ether2(EXT			17.0 KiB	·
✔ accept	forward					1 (icmp)				ether2(EXT	ether3(INT			504 B	·
✔ accept	forward					6 (tcp)		80		ether2(EXT	ether3(INT			5.8 KiB	·
✔ accept	forward					6 (tcp)	80			ether3(INT	ether2(EXT			3828 B	·
✖ drop	forward													6.5 KiB	·
✔ accept	output										ether3(INT			0 B	·
✔ accept	output					6 (tcp)					ether3(INT			7.6 MiB	·
✔ accept	output					1 (icmp)					ether3(INT			0 B	·
✔ accept	output					6 (tcp)	22				ether2(EXT			20.0 KiB	·
✖ drop	output													360 B	·
Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Bytes	
🔗 masquerade	srcnat	10.25.10.10				1 (icmp)					ether2(EXT			336 B	·
🔗 dst-nat	dstnat					6 (tcp)		7474		ether2(EXT				5.7 KiB	·