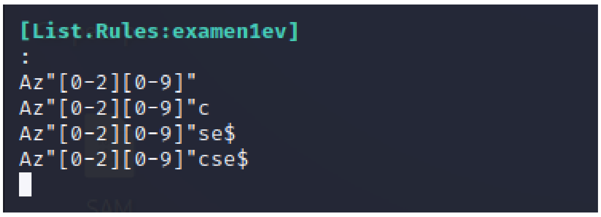
Cesar Gil Hernando ASIR 2022/23

Practica Examen 1ªEV

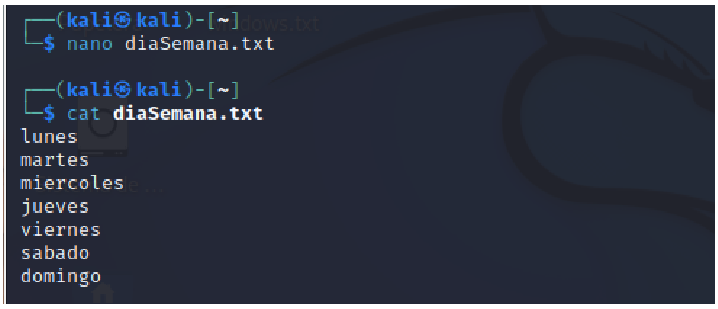
Hashes del zip:

Reglas para el zip.



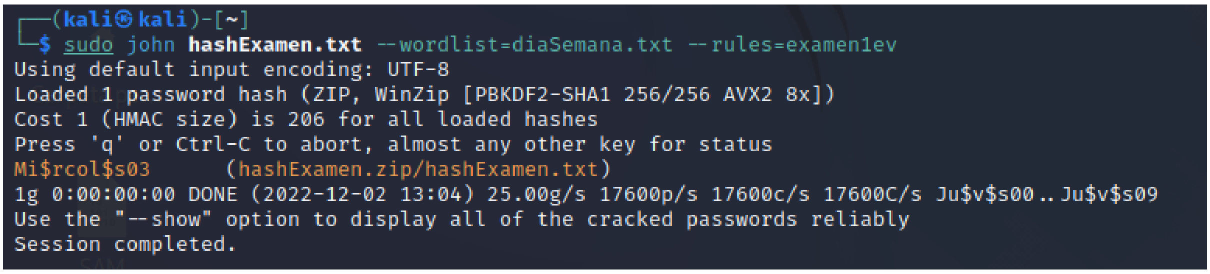
```
[List.Rules:examen1ev]
:
Az"[0-2][0-9]"
Az"[0-2][0-9]"c
Az"[0-2][0-9]"se$
Az"[0-2][0-9]"cse$
```

Diccionario para el zip.



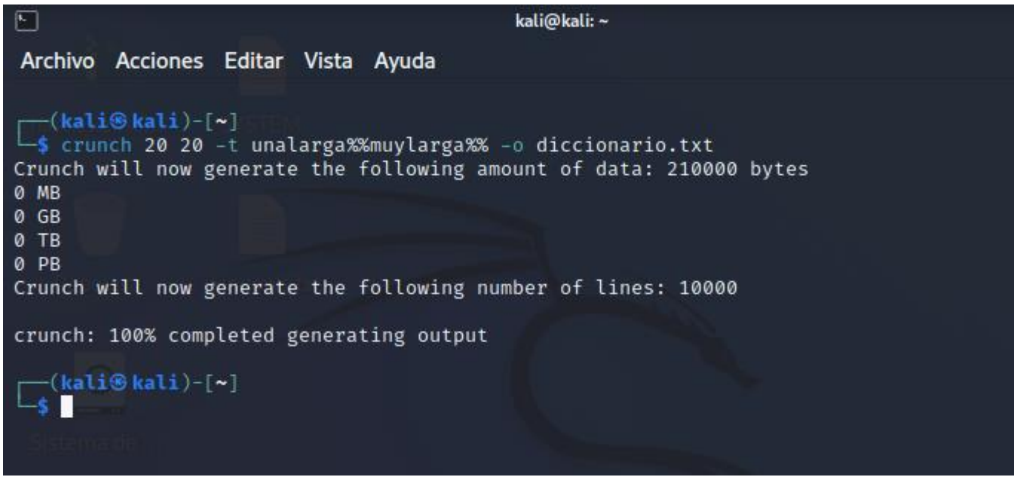
```
┌──(kali㉿kali)-[~]
└─$ nano diaSemana.txt

┌──(kali㉿kali)-[~]
└─$ cat diaSemana.txt
lunes
martes
miercoles
jueves
viernes
sabado
domingo
```

Captura de la contraseña del zip después de haber hecho el zip2john.



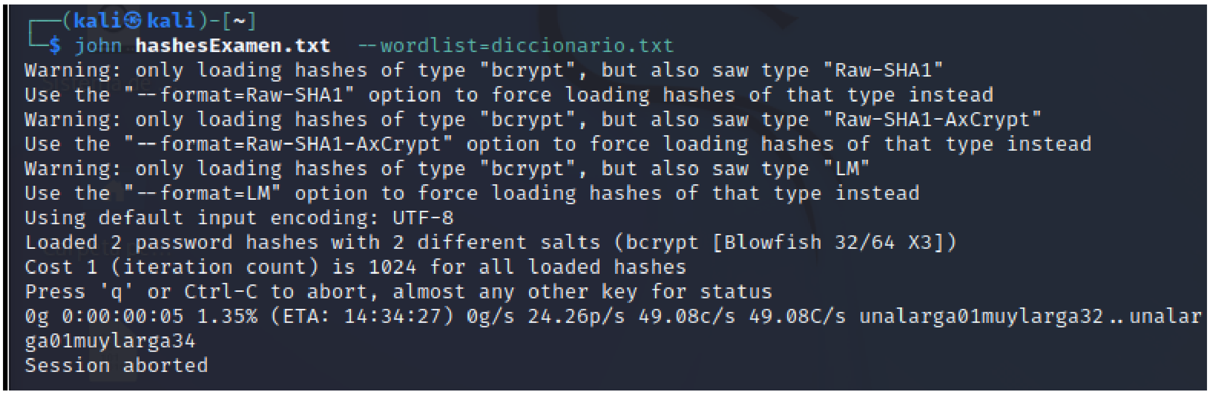
```
┌──(kali㉿kali)-[~]
└─$ sudo john hashExamen.txt --wordlist=diaSemana.txt --rules=examen1ev
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 206 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
Mi$rcol$s03      (hashExamen.zip/hashExamen.txt)
1g 0:00:00:00 DONE (2022-12-02 13:04) 25.00g/s 17600p/s 17600c/s 17600C/s Ju$v$s00..Ju$v$s09
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Crunch para los hashes de dentro del zip.

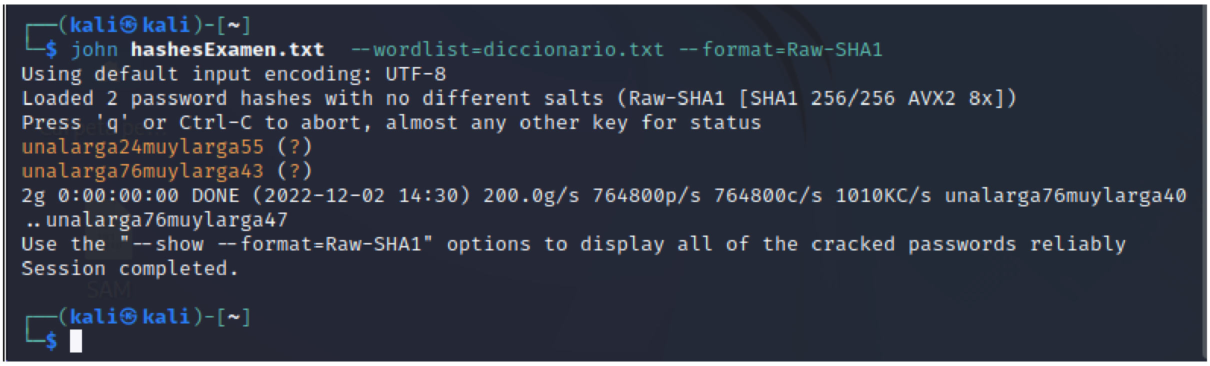


```
┌──(kali㉿kali)-[~]
└─$ crunch 20 20 -t unalarga%%muylarga%% -o diccionario.txt
Crunch will now generate the following amount of data: 210000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ 
```

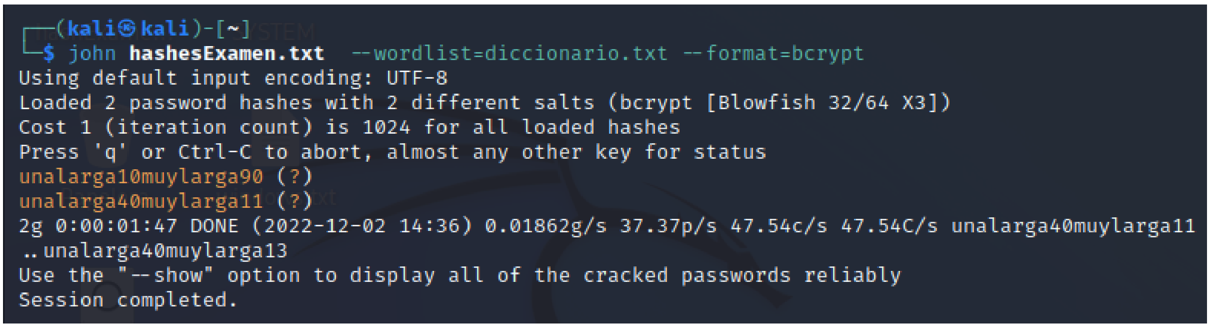
Hashes.



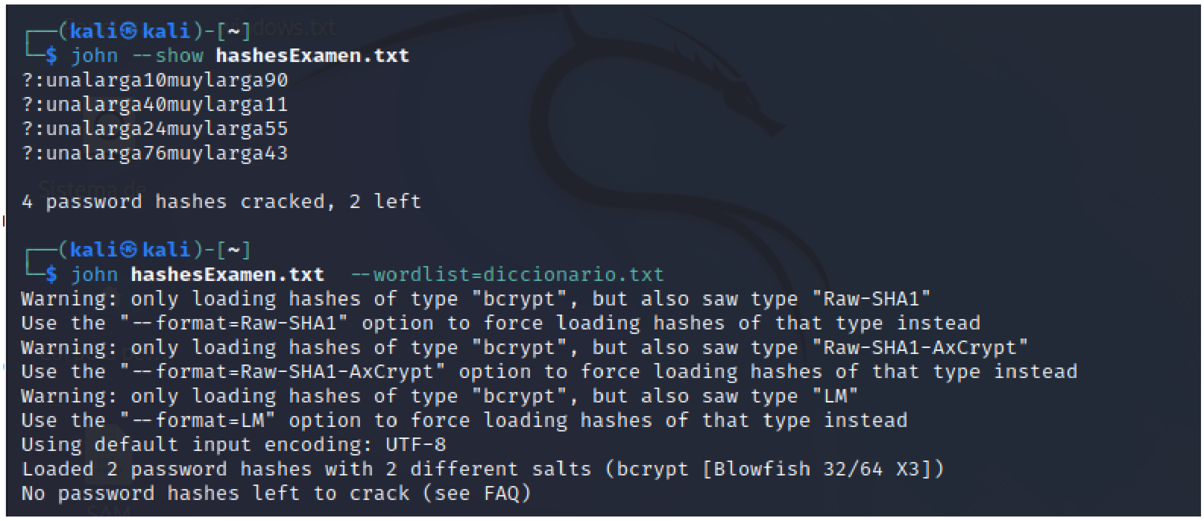
```
┌──(kali㉿kali)-[~]
└─$ john hashesExamen.txt  --wordlist=diccionario.txt
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 1.35% (ETA: 14:34:27) 0g/s 24.26p/s 49.08c/s 49.08C/s unalarga01muylarga32..unalar
ga01muylarga34
Session aborted
```



```
┌──(kali㉿kali)-[~]
└─$ john hashesExamen.txt  --wordlist=diccionario.txt --format=Raw-SHA1
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
unalarga24muylarga55 (?)
unalarga76muylarga43 (?)
2g 0:00:00:00 DONE (2022-12-02 14:30) 200.0g/s 764800p/s 764800c/s 1010KC/s unalarga76muylarga40
..unalarga76muylarga47
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ ▌
```



```
┌──(kali㉿kali)-[~]
└─$ john hashesExamen.txt  --wordlist=diccionario.txt --format=bcrypt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
unalarga10muylarga90 (?)
unalarga40muylarga11 (?)
2g 0:00:01:47 DONE (2022-12-02 14:36) 0.01862g/s 37.37p/s 47.54c/s 47.54C/s unalarga40muylarga11
..unalarga40muylarga13
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



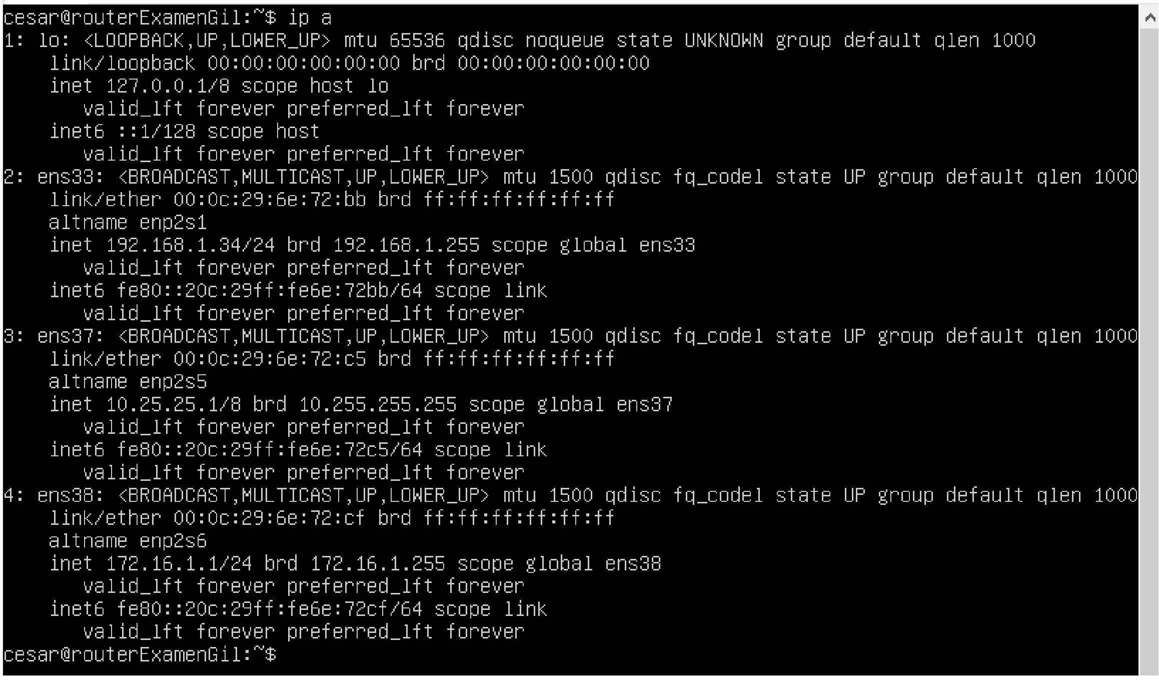
```
┌──(kali㉿kali)-[~]
└─$ john --show hashesExamen.txt
?:unalarga10muylarga90
?:unalarga40muylarga11
?:unalarga24muylarga55
?:unalarga76muylarga43

4 password hashes cracked, 2 left

┌──(kali㉿kali)-[~]
└─$ john hashesExamen.txt  --wordlist=diccionario.txt
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
No password hashes left to crack (see FAQ)
```

No entiendo muy bien como es posible que estén todas crackeadas y a la vez falten 2, pero ok.

Iptables:

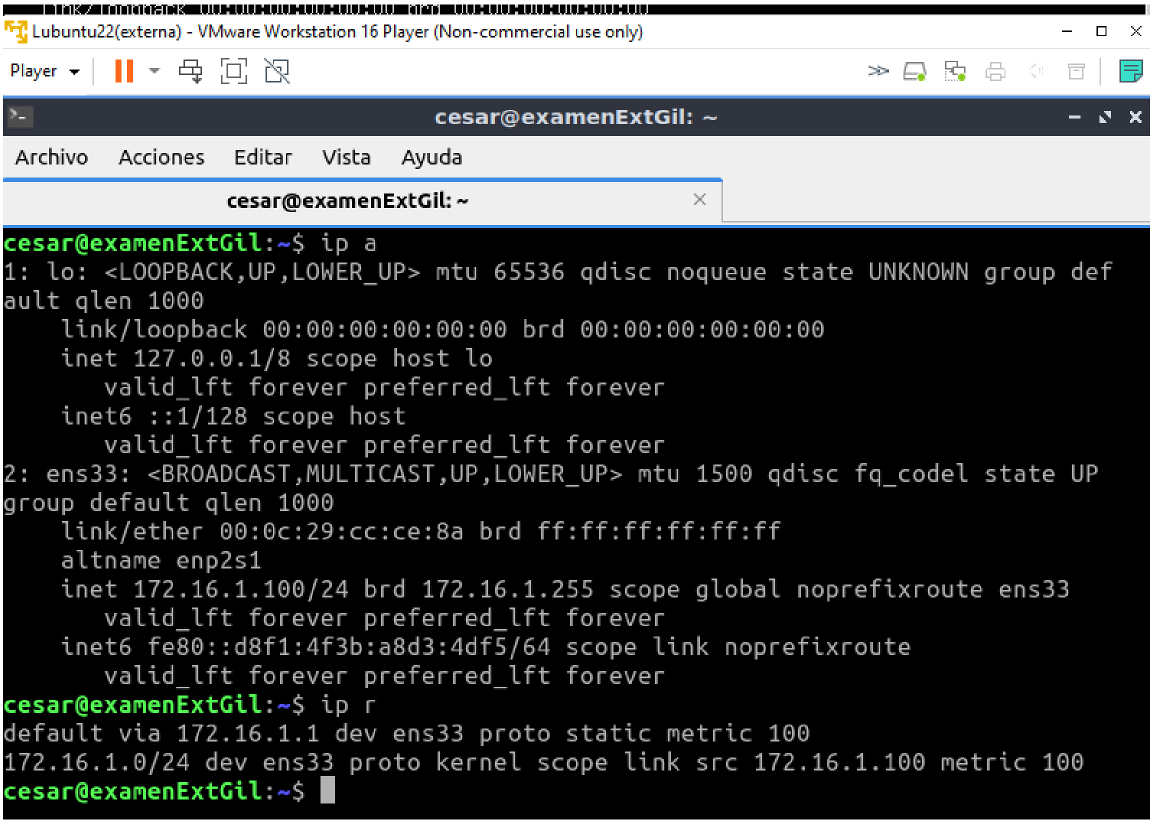
Configuración inicial.

IPs del router.



```
cesar@routerExamenGil:~$ 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
       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:29:6e:72:bb brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.34/24 brd 192.168.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72bb/64 scope link
       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:29:6e:72:c5 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.25.25.1/8 brd 10.255.255.255 scope global ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72c5/64 scope link
       valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6e:72:cf brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 172.16.1.1/24 brd 172.16.1.255 scope global ens38
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72cf/64 scope link
       valid_lft forever preferred_lft forever
cesar@routerExamenGil:~$
```

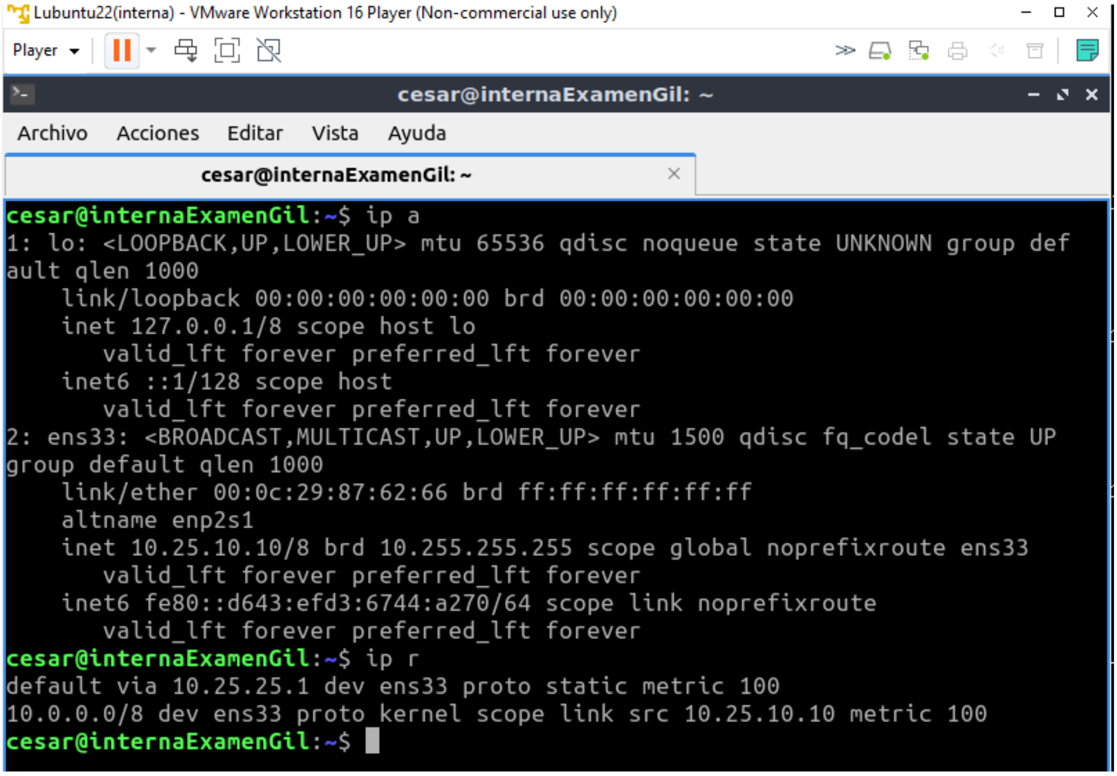
IP del cliente.



```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
cesar@examenExtGil:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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
       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:cc:ce:8a brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.1.100/24 brd 172.16.1.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::d8f1:4f3b:a8d3:4df5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
cesar@examenExtGil:~$ ip r
default via 172.16.1.1 dev ens33 proto static metric 100
172.16.1.0/24 dev ens33 proto kernel scope link src 172.16.1.100 metric 100
cesar@examenExtGil:~$
```

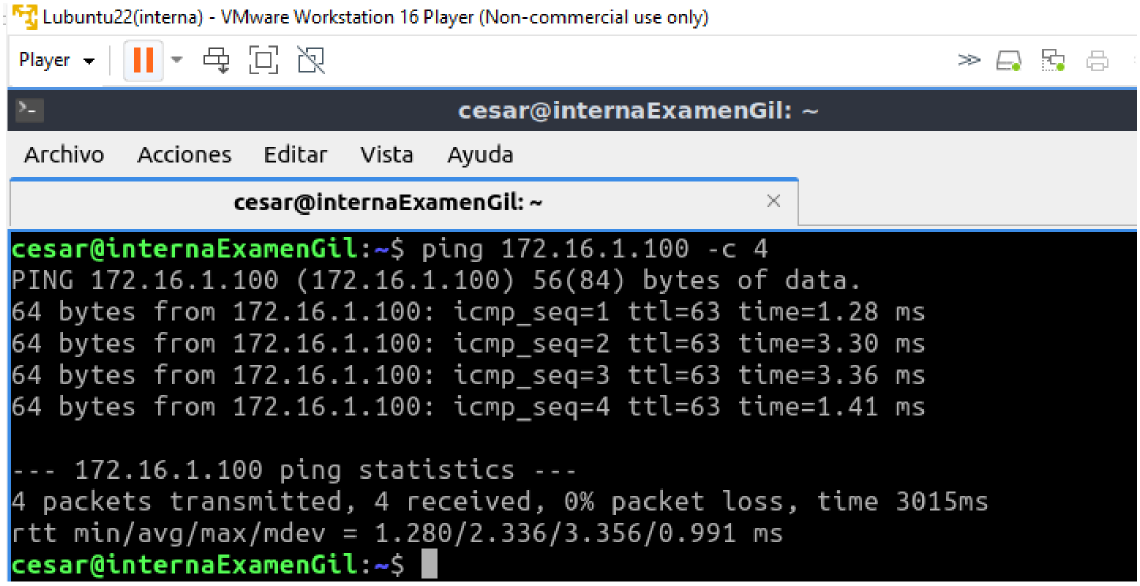
IP del servidor.


Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

```
cesar@internaExamenGil:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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
       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:29:87:62:66 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.25.10.10/8 brd 10.255.255.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::d643:efd3:6744:a270/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
cesar@internaExamenGil:~$ ip r
default via 10.25.25.1 dev ens33 proto static metric 100
10.0.0.0/8 dev ens33 proto kernel scope link src 10.25.10.10 metric 100
cesar@internaExamenGil:~$
```

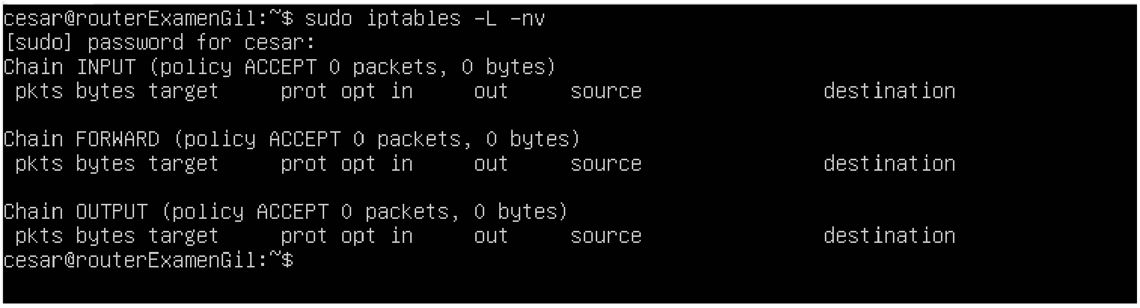
Ping interno a externo con todo en ACCEPT.

Captura del ping.


Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

```
cesar@internaExamenGil:~$ ping 172.16.1.100 -c 4
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=1.28 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=3.30 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=3.36 ms
64 bytes from 172.16.1.100: icmp_seq=4 ttl=63 time=1.41 ms

--- 172.16.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 1.280/2.336/3.356/0.991 ms
cesar@internaExamenGil:~$
```

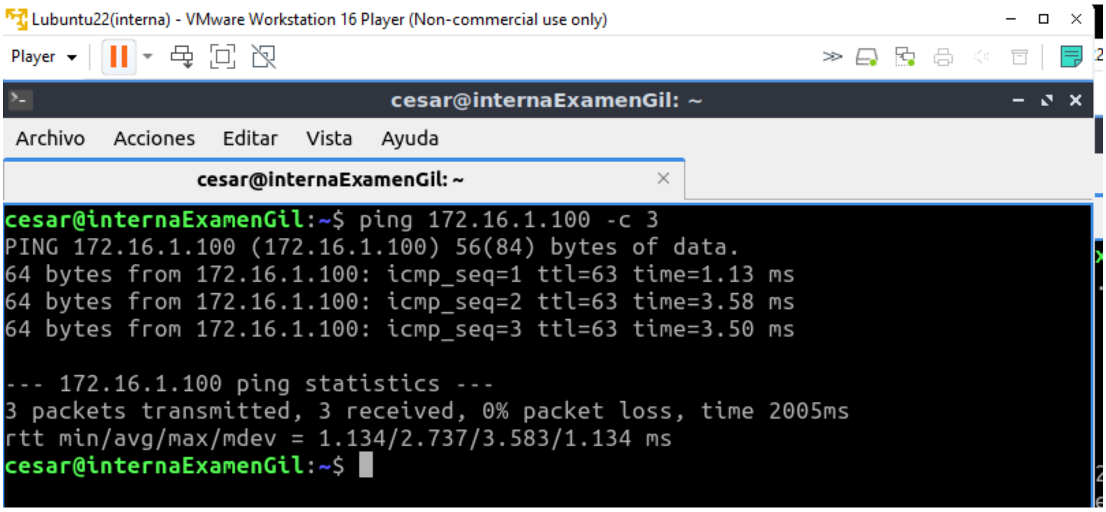
Iptables –L –nv.



```
cesar@routerExamenGil:~$ sudo iptables -L -nv
[sudo] password for cesar:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
cesar@routerExamenGil:~$
```

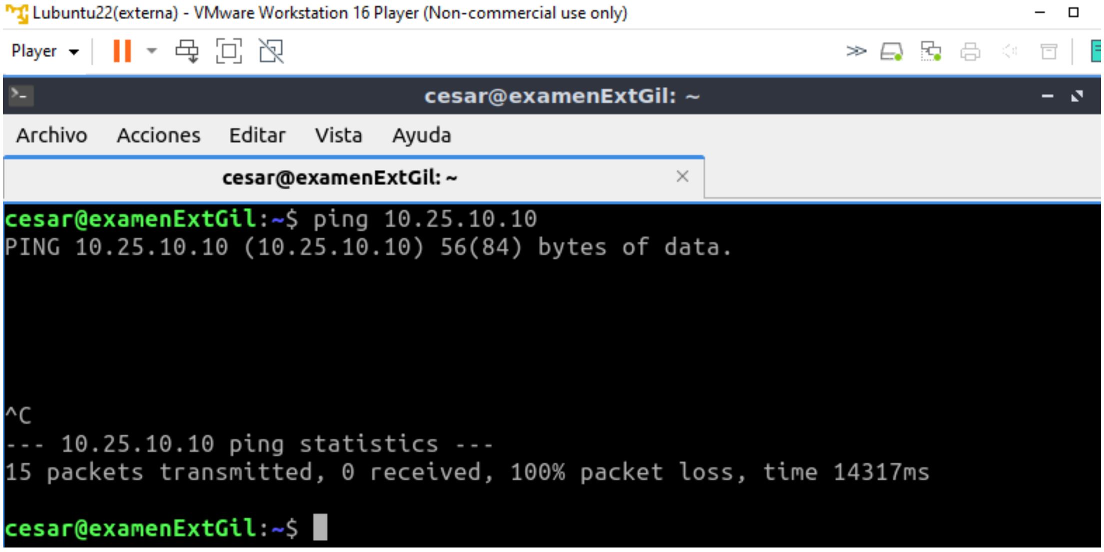
Con todo en DROP,Ping interno a externo pero al reves no.

Captura del ping.


Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

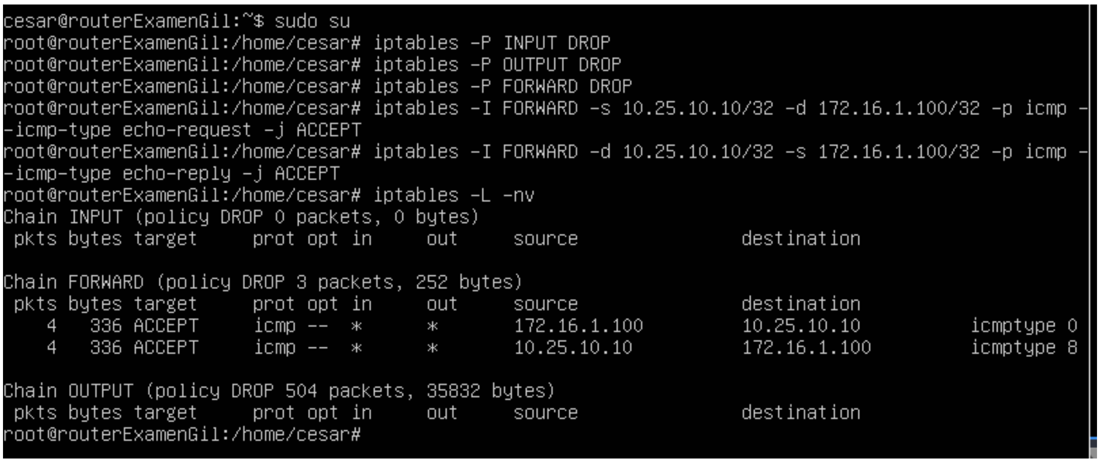
```
cesar@internaExamenGil:~$ ping 172.16.1.100 -c 3
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data.
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=1.13 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=3.58 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=3.50 ms

--- 172.16.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.134/2.737/3.583/1.134 ms
cesar@internaExamenGil:~$
```

Captura del ping fallido externo-interno.



```
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 ---
15 packets transmitted, 0 received, 100% packet loss, time 14317ms

cesar@examenExtGil:~$
```

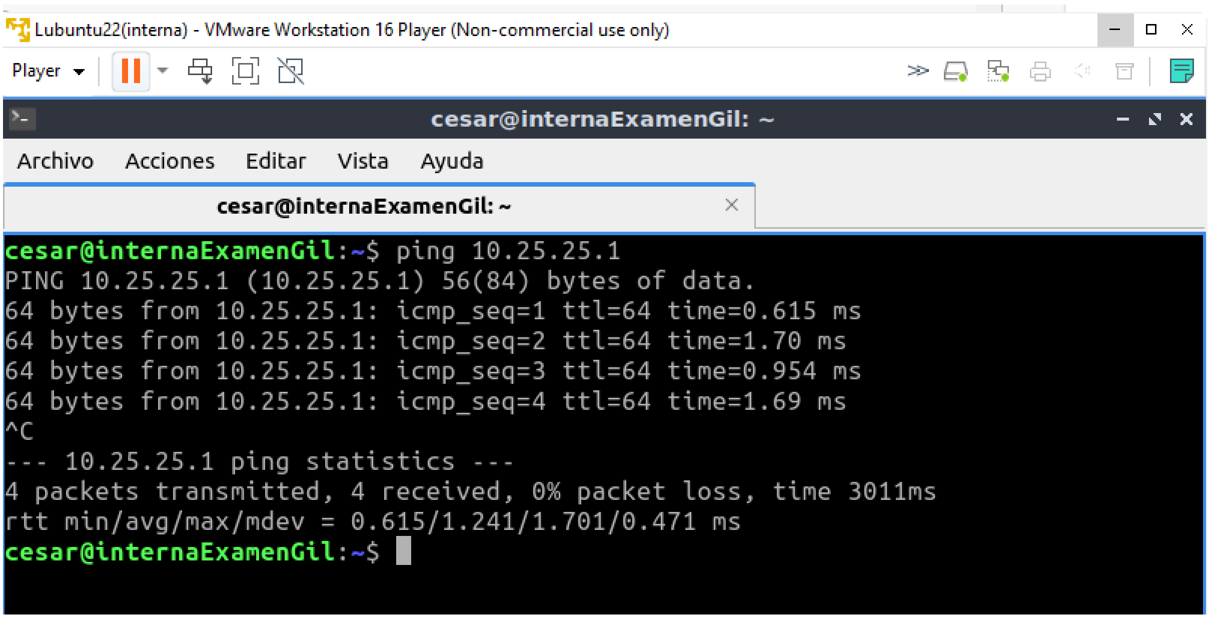
Iptables –L –nv.



```
cesar@routerExamenGil:~$ sudo su
root@routerExamenGil:/home/cesar# iptables -P INPUT DROP
root@routerExamenGil:/home/cesar# iptables -P OUTPUT DROP
root@routerExamenGil:/home/cesar# iptables -P FORWARD DROP
root@routerExamenGil:/home/cesar# iptables -I FORWARD -s 10.25.10.10/32 -d 172.16.1.100/32 -p icmp -
-icmp-type echo-request -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -I FORWARD -d 10.25.10.10/32 -s 172.16.1.100/32 -p icmp -
-icmp-type echo-reply -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 3 packets, 252 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   336 ACCEPT     icmp --  *      *       172.16.1.100         10.25.10.10          icmptype 0
    4   336 ACCEPT     icmp --  *      *       10.25.10.10          172.16.1.100         icmptype 8

Chain OUTPUT (policy DROP 504 packets, 35832 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@routerExamenGil:/home/cesar#
```

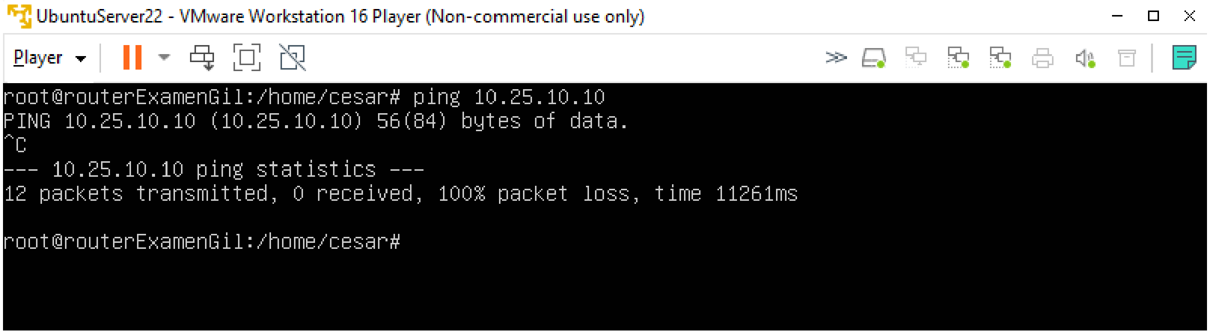
Ping interno a router pero no al revés.

Captura del ping.


Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

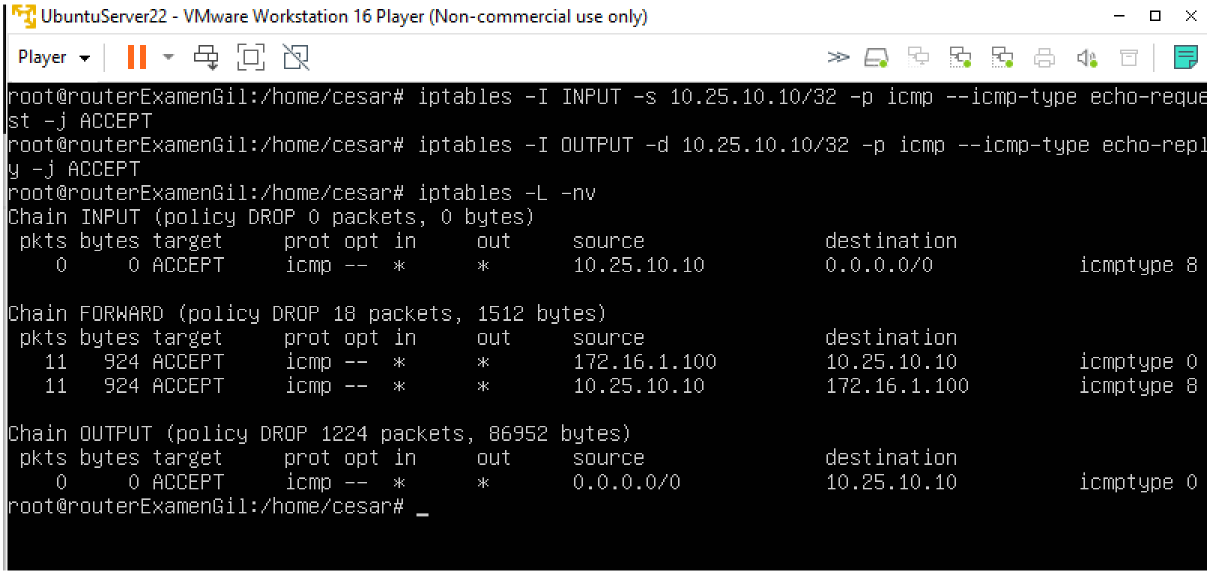
```
cesar@internaExamenGil:~$ ping 10.25.25.1
PING 10.25.25.1 (10.25.25.1) 56(84) bytes of data.
64 bytes from 10.25.25.1: icmp_seq=1 ttl=64 time=0.615 ms
64 bytes from 10.25.25.1: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 10.25.25.1: icmp_seq=3 ttl=64 time=0.954 ms
64 bytes from 10.25.25.1: icmp_seq=4 ttl=64 time=1.69 ms
^C
--- 10.25.25.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 0.615/1.241/1.701/0.471 ms
cesar@internaExamenGil:~$
```

Captura del ping fallido router-interno.


UbuntuServer22 - VMware Workstation 16 Player (Non-commercial use only)
Player

```
root@routerExamenGil:/home/cesar# 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 ---
12 packets transmitted, 0 received, 100% packet loss, time 11261ms

root@routerExamenGil:/home/cesar#
```

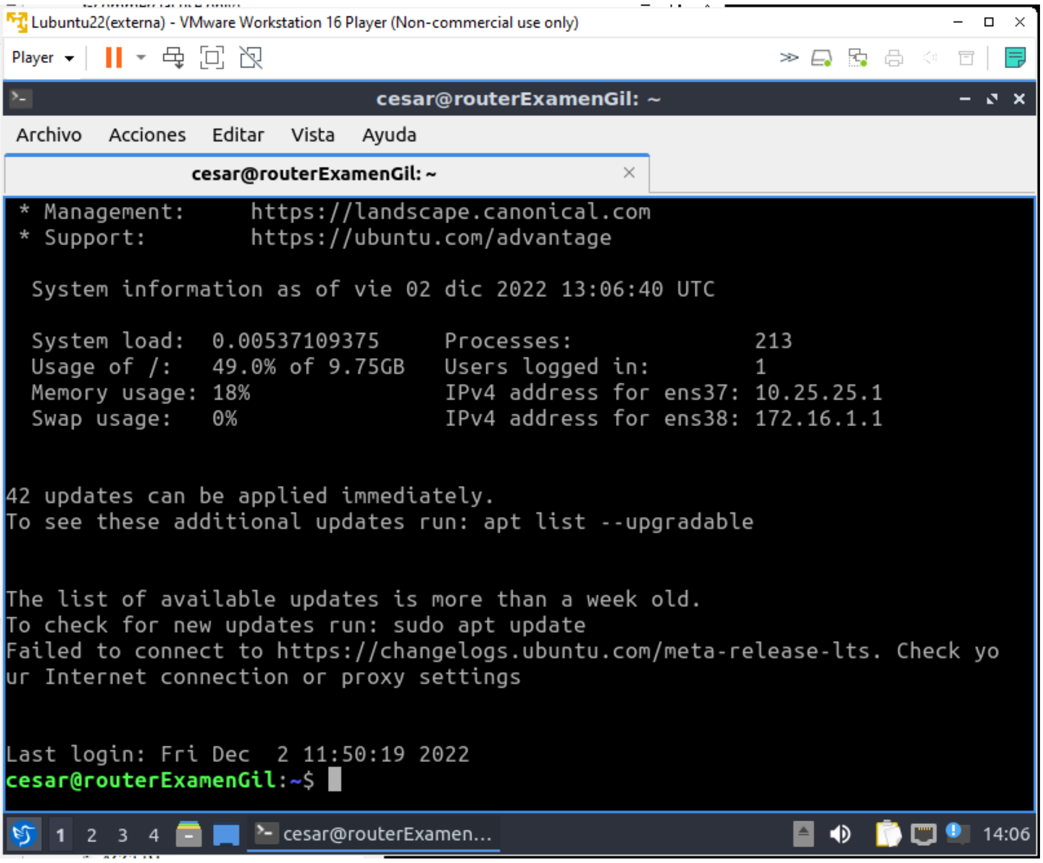
Iptables –L –nv.


UbuntuServer22 - VMware Workstation 16 Player (Non-commercial use only)
Player

```
root@routerExamenGil:/home/cesar# iptables -I INPUT -s 10.25.10.10/32 -p icmp --icmp-type echo-reque
st -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -I OUTPUT -d 10.25.10.10/32 -p icmp --icmp-type echo-repl
y -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       10.25.10.10          0.0.0.0/0            icmptype 8

Chain FORWARD (policy DROP 18 packets, 1512 bytes)
 pkts bytes target     prot opt in     out     source               destination
   11   924 ACCEPT     icmp --  *      *       172.16.1.100         10.25.10.10          icmptype 0
   11   924 ACCEPT     icmp --  *      *       10.25.10.10          172.16.1.100         icmptype 8

Chain OUTPUT (policy DROP 1224 packets, 86952 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            10.25.10.10          icmptype 0
root@routerExamenGil:/home/cesar# _
```

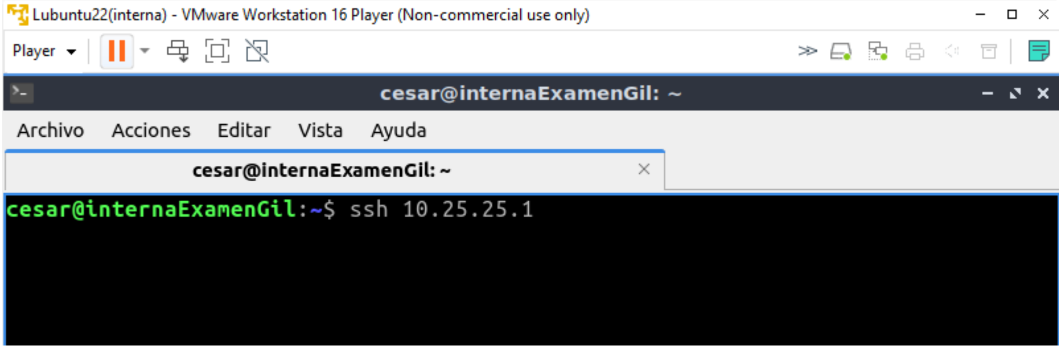
SSH a router desde externo.

Captura del SSH desde el externo.



```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of vie 02 dic 2022 13:06:40 UTC

  System load:  0.00537109375     Processes:             213
  Usage of /:   49.0% of 9.75GB   Users logged in:       1
  Memory usage: 18%               IPv4 address for ens37: 10.25.25.1
  Swap usage:   0%                IPv4 address for ens38: 172.16.1.1


42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
ur Internet connection or proxy settings


Last login: Fri Dec  2 11:50:19 2022
cesar@routerExamenGil:~$
```

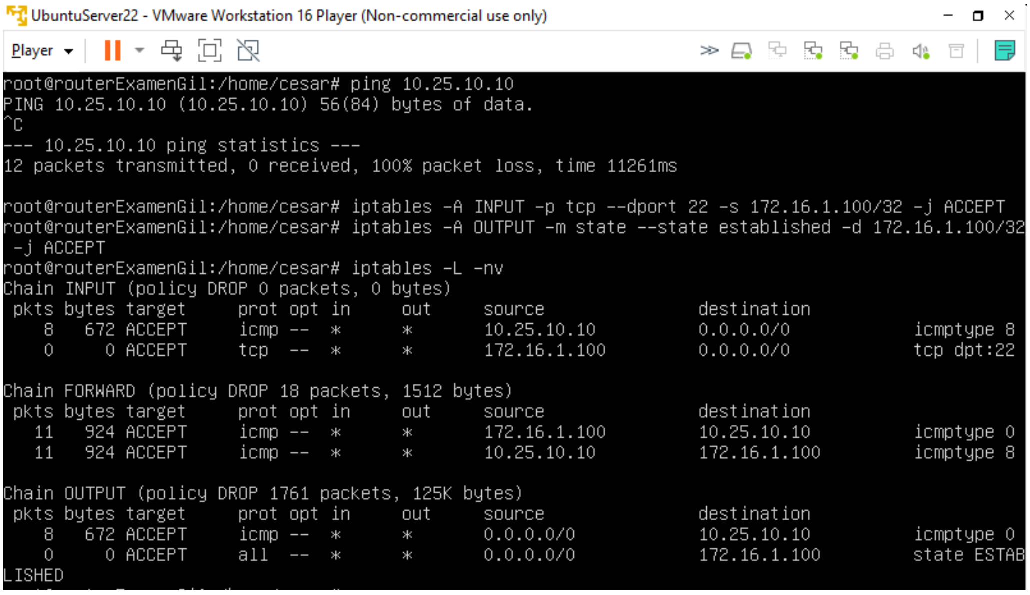
Captura del SSH fallido desde el interno.



Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

```
cesar@internaExamenGil:~$ ssh 10.25.25.1
```

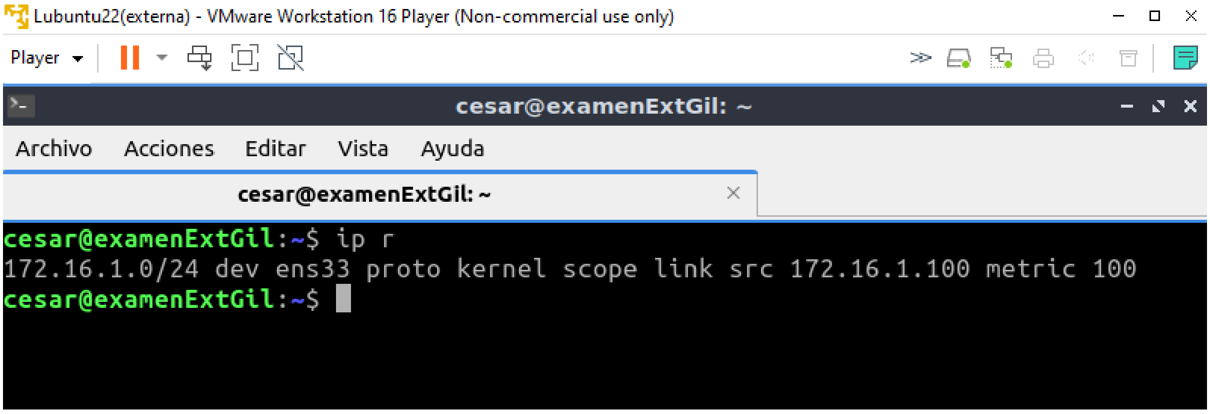
Iptables –L –nv.


UbuntuServer22 - VMware Workstation 16 Player (Non-commercial use only)
Player

```
root@routerExamenGil:/home/cesar# 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 ---
12 packets transmitted, 0 received, 100% packet loss, time 11261ms

root@routerExamenGil:/home/cesar# iptables -A INPUT -p tcp --dport 22 -s 172.16.1.100/32 -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -A OUTPUT -m state --state established -d 172.16.1.100/32
 -j ACCEPT
root@routerExamenGil:/home/cesar# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   672 ACCEPT     icmp --  *      *       10.25.10.10          0.0.0.0/0            icmptype 8
    0     0 ACCEPT     tcp  --  *      *       172.16.1.100         0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy DROP 18 packets, 1512 bytes)
 pkts bytes target     prot opt in     out     source               destination
   11   924 ACCEPT     icmp --  *      *       172.16.1.100         10.25.10.10          icmptype 0
   11   924 ACCEPT     icmp --  *      *       10.25.10.10          172.16.1.100         icmptype 8

Chain OUTPUT (policy DROP 1761 packets, 125K bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   672 ACCEPT     icmp --  *      *       0.0.0.0/0            10.25.10.10          icmptype 0
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            172.16.1.100         state ESTAB
LISHED
```

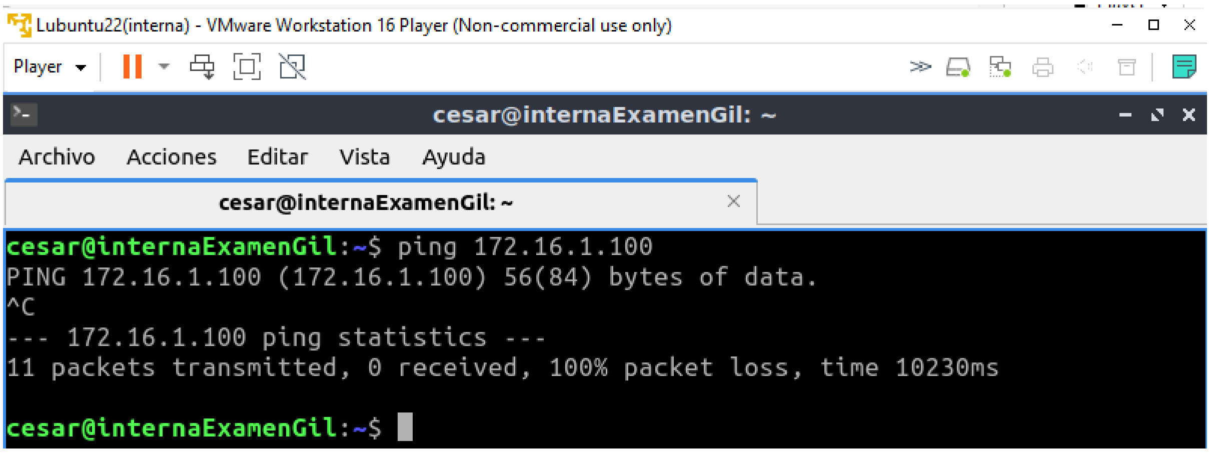
Externo sin puerta de enlace.

Captura del ip r del externo.



```
cesar@examenExtGil:~$ ip r
172.16.1.0/24 dev ens33 proto kernel scope link src 172.16.1.100 metric 100
cesar@examenExtGil:~$
```

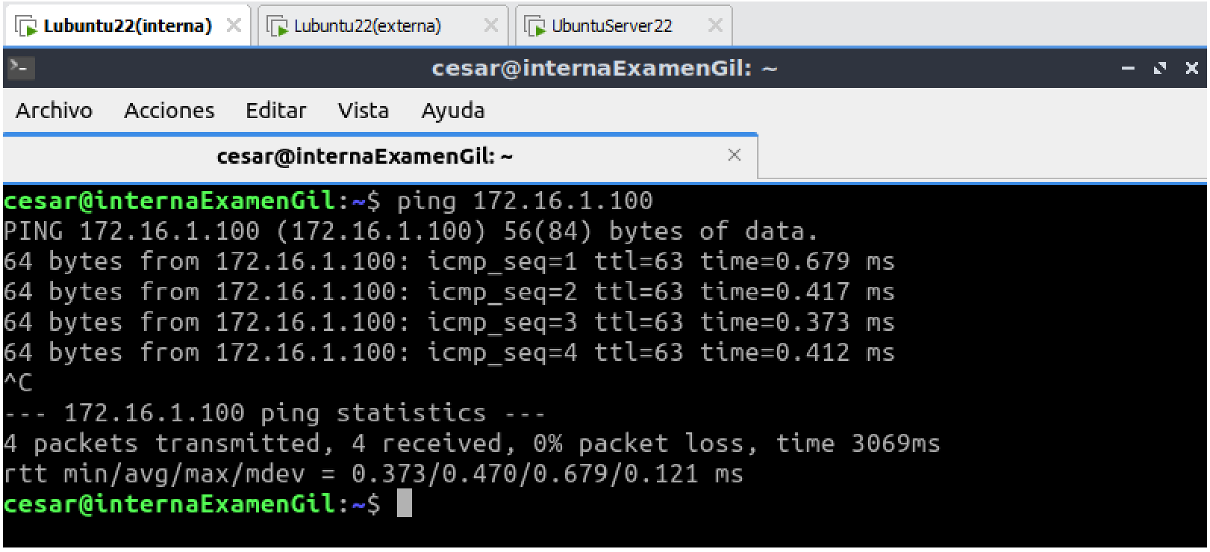
Captura del ping fallido.


Lubuntu22(interna) - VMware Workstation 16 Player (Non-commercial use only)
Player
cesar@internaExamenGil: ~
Archivo
Acciones
Editar
Vista
Ayuda
cesar@internaExamenGil: ~

```
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 ---
11 packets transmitted, 0 received, 100% packet loss, time 10230ms

cesar@internaExamenGil:~$
```

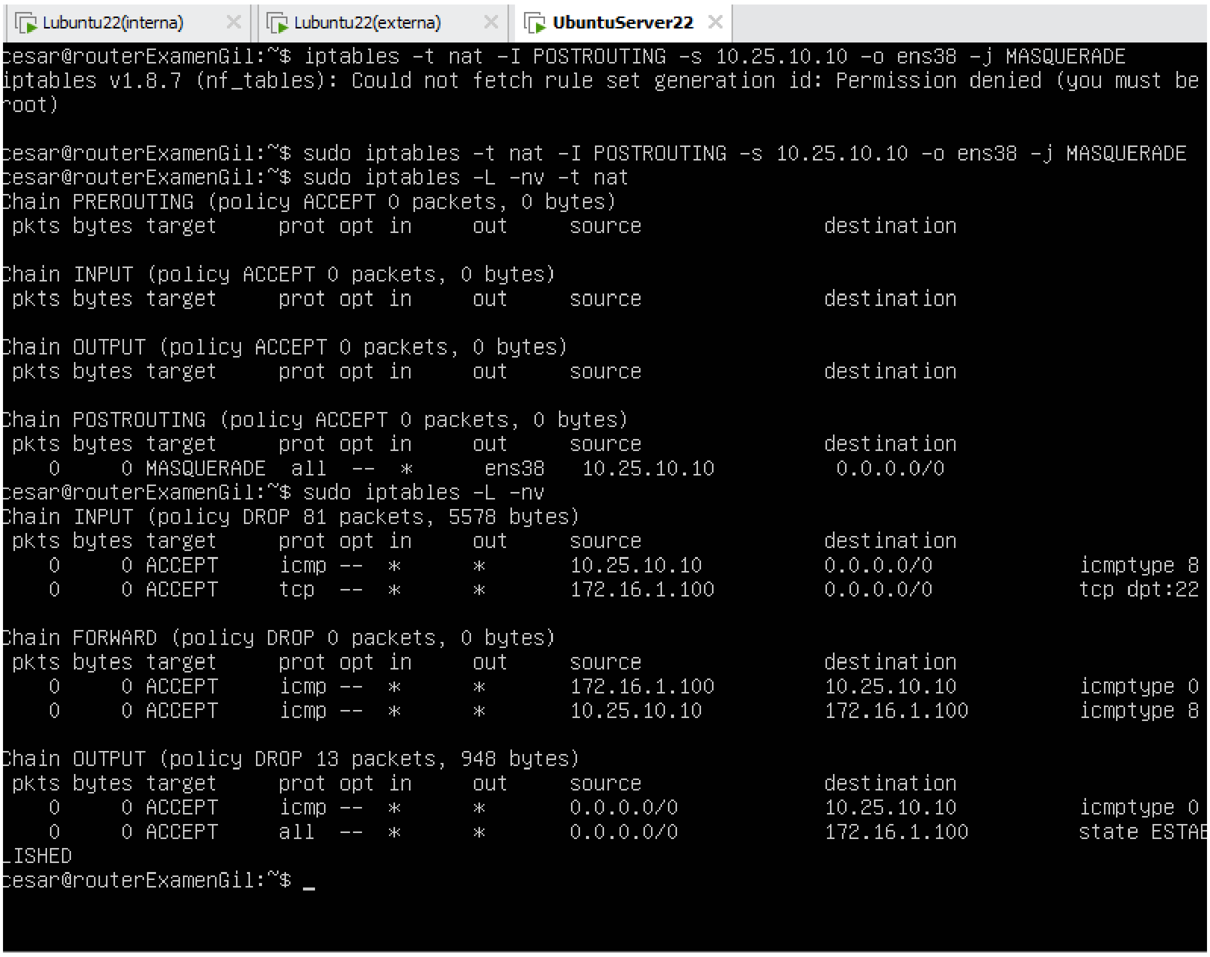
POSTROUTING para el ping.

Captura del ping.



```
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=0.679 ms
64 bytes from 172.16.1.100: icmp_seq=2 ttl=63 time=0.417 ms
64 bytes from 172.16.1.100: icmp_seq=3 ttl=63 time=0.373 ms
64 bytes from 172.16.1.100: icmp_seq=4 ttl=63 time=0.412 ms
^C
--- 172.16.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.373/0.470/0.679/0.121 ms
cesar@internaExamenGil:~$ 
```

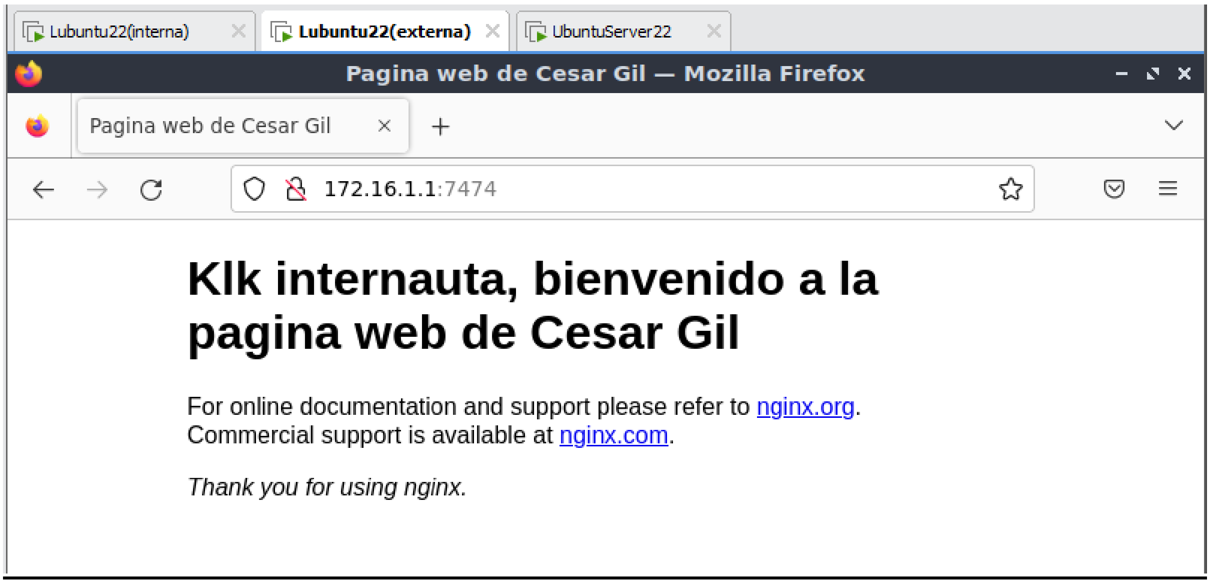
Iptables –L –nv.



```
cesar@routerExamenGil:~$ iptables -t nat -I POSTROUTING -s 10.25.10.10 -o ens38 -j MASQUERADE
iptables v1.8.7 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be
root)

cesar@routerExamenGil:~$ sudo iptables -t nat -I POSTROUTING -s 10.25.10.10 -o ens38 -j MASQUERADE
cesar@routerExamenGil:~$ sudo iptables -L -nv -t nat
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  all  --  *      ens38   10.25.10.10          0.0.0.0/0
cesar@routerExamenGil:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 81 packets, 5578 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       10.25.10.10          0.0.0.0/0            icmptype 8
    0     0 ACCEPT     tcp  --  *      *       172.16.1.100         0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       172.16.1.100         10.25.10.10          icmptype 0
    0     0 ACCEPT     icmp --  *      *       10.25.10.10          172.16.1.100         icmptype 8

Chain OUTPUT (policy DROP 13 packets, 948 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            10.25.10.10          icmptype 0
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            172.16.1.100         state ESTAB
LISHED
cesar@routerExamenGil:~$ _
```

PREROUTING para el http.

Captura de conexión HTTP.

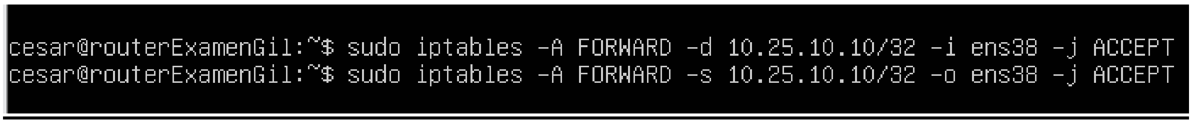


Klk internauta, bienvenido a la pagina web de Cesar Gil

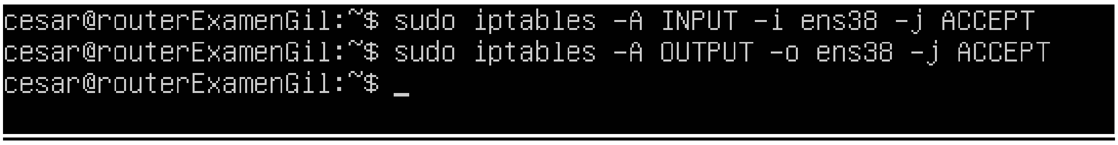
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

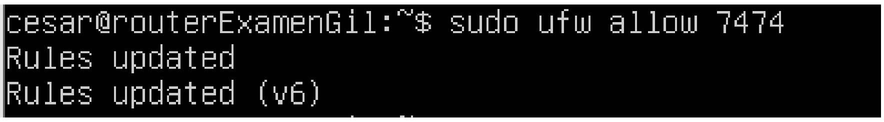
Seguro que hay formas mas seguras y restrictivas de permitir la conexión entre maquinas, pero así es como lo hicimos en la practicas de DNAT.



```
cesar@routerExamenGil:~$ sudo iptables -A FORWARD -d 10.25.10.10/32 -i ens38 -j ACCEPT
cesar@routerExamenGil:~$ sudo iptables -A FORWARD -s 10.25.10.10/32 -o ens38 -j ACCEPT
```

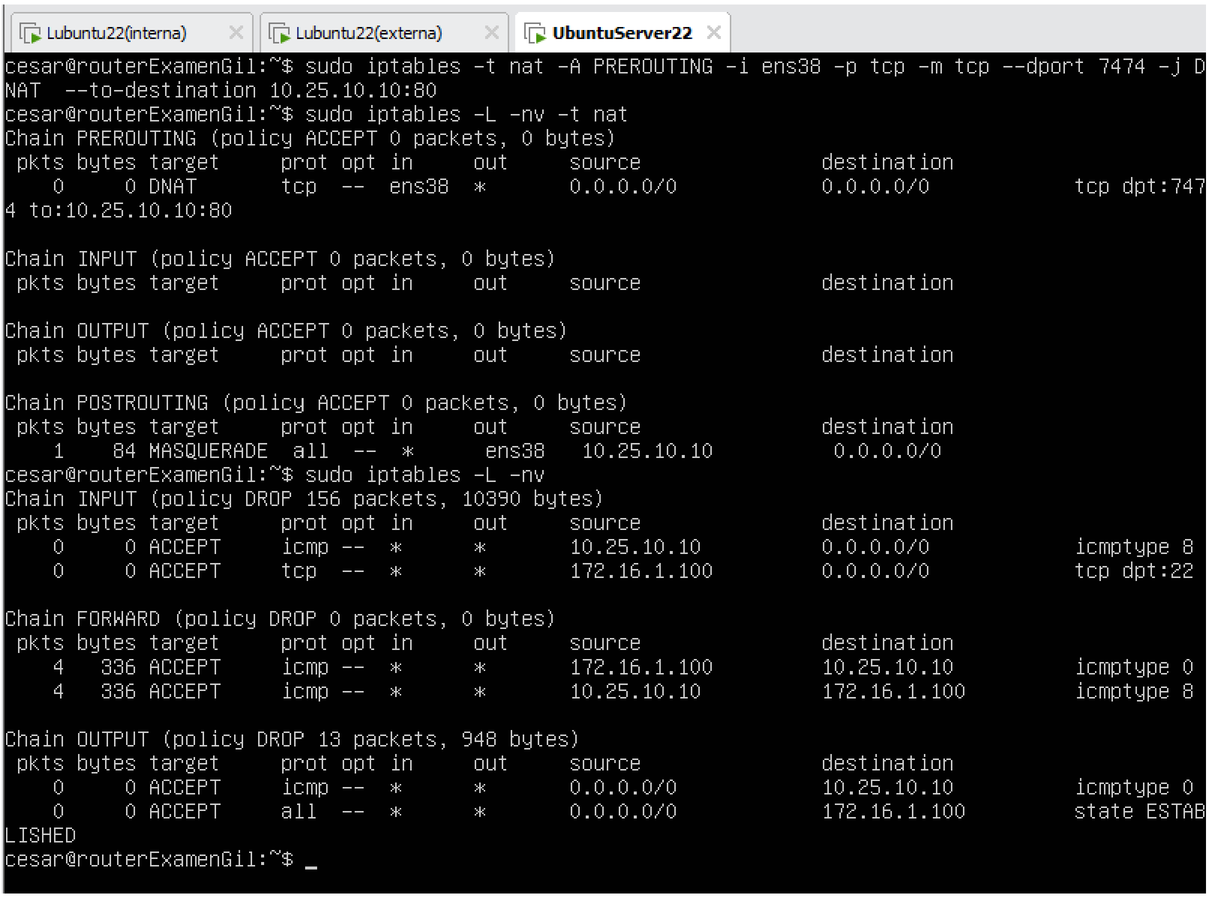


```
cesar@routerExamenGil:~$ sudo iptables -A INPUT -i ens38 -j ACCEPT
cesar@routerExamenGil:~$ sudo iptables -A OUTPUT -o ens38 -j ACCEPT
cesar@routerExamenGil:~$ _
```



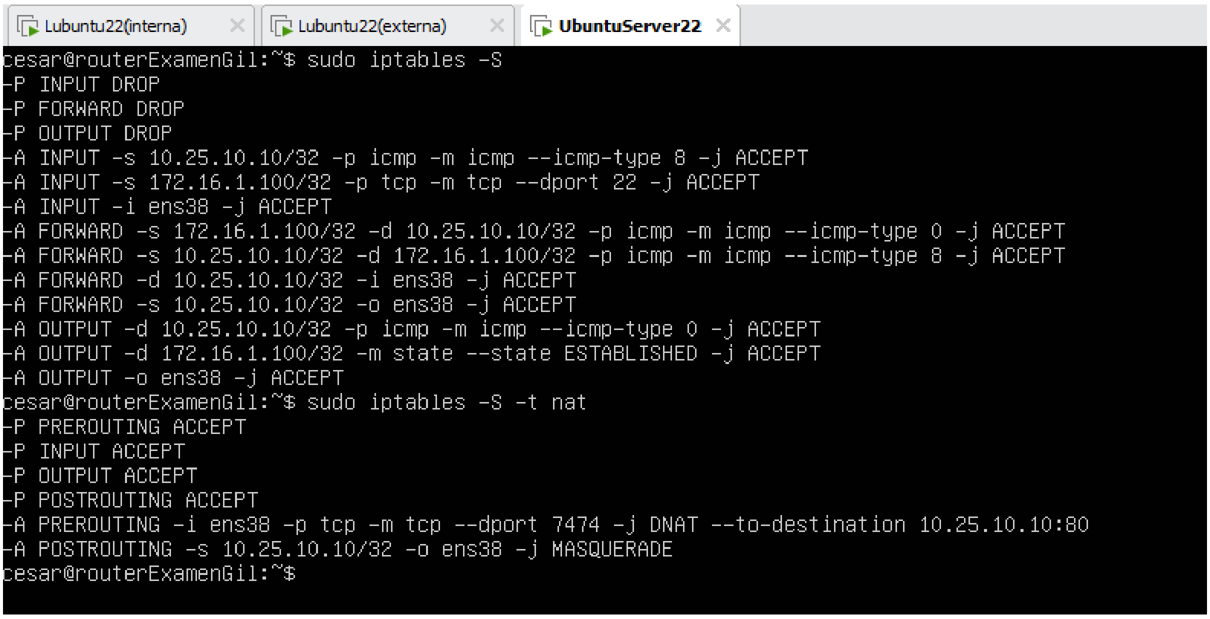
```
cesar@routerExamenGil:~$ sudo ufw allow 7474
Rules updated
Rules updated (v6)
```

Iptables –L –nv.



```
cesar@routerExamenGil:~$ sudo iptables -t nat -A PREROUTING -i ens38 -p tcp -m tcp --dport 7474 -j D
NAT  --to-destination 10.25.10.10:80
cesar@routerExamenGil:~$ sudo iptables -L -nv -t nat
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  ens38  *       0.0.0.0/0            0.0.0.0/0            tcp dpt:747
4 to:10.25.10.10:80

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    84 MASQUERADE  all  --  *      ens38   10.25.10.10          0.0.0.0/0
cesar@routerExamenGil:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 156 packets, 10390 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       10.25.10.10          0.0.0.0/0            icmptype 8
    0     0 ACCEPT     tcp  --  *      *       172.16.1.100         0.0.0.0/0            tcp dpt:22

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   336 ACCEPT     icmp --  *      *       172.16.1.100         10.25.10.10          icmptype 0
    4   336 ACCEPT     icmp --  *      *       10.25.10.10          172.16.1.100         icmptype 8

Chain OUTPUT (policy DROP 13 packets, 948 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            10.25.10.10          icmptype 0
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            172.16.1.100         state ESTAB
LISHED
cesar@routerExamenGil:~$ _
```

Lista de reglas utilizadas.



```
cesar@routerExamenGil:~$ sudo iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
-A INPUT -s 10.25.10.10/32 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -s 172.16.1.100/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i ens38 -j ACCEPT
-A FORWARD -s 172.16.1.100/32 -d 10.25.10.10/32 -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A FORWARD -s 10.25.10.10/32 -d 172.16.1.100/32 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A FORWARD -d 10.25.10.10/32 -i ens38 -j ACCEPT
-A FORWARD -s 10.25.10.10/32 -o ens38 -j ACCEPT
-A OUTPUT -d 10.25.10.10/32 -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -d 172.16.1.100/32 -m state --state ESTABLISHED -j ACCEPT
-A OUTPUT -o ens38 -j ACCEPT
cesar@routerExamenGil:~$ sudo iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A PREROUTING -i ens38 -p tcp -m tcp --dport 7474 -j DNAT --to-destination 10.25.10.10:80
-A POSTROUTING -s 10.25.10.10/32 -o ens38 -j MASQUERADE
cesar@routerExamenGil:~$
```