PRÁCTICA 6 (almellonesfernandez-practica6) – UD 4. U.D.4. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

En esta práctica hay que usar toda la estructura creada en el ejercicio anterior, pero en este caso vamos a realizar la seguridad perimetral de toda nuestra empresa que recae en el servidor firewall.XXxx y por supuesto de la seguridad de host de la misma (INPUT/OUTPUT) de nuestra empresa, que está formada por tres zonas (dmz, lan y wlan), y los equipos que hemos ubicado en cada zona. Esta estructura (y algunos equipos más que pondremos) los vamos a usar durante todo el año, así que muy importante la estabilidad de la misma.

CARACTERISTICAS GENERALES DE FIREWALL y A LA PRÁCTICA.

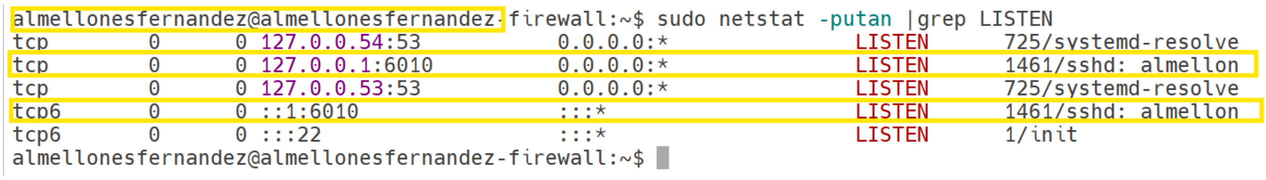
- El script de iptables se arrancará en el inicio de la máquina (/etc/rc.local) o mediante servicio.

- Usar comentarios en las mismas reglas de iptables, sobre todo en las de FORWARD, que son las nuevas.

- Uso de funciones, variables para facilitar el entendimiento y su modificación.

1. **(0,5 puntos).** Opciones por defecto y preparación del mismo.

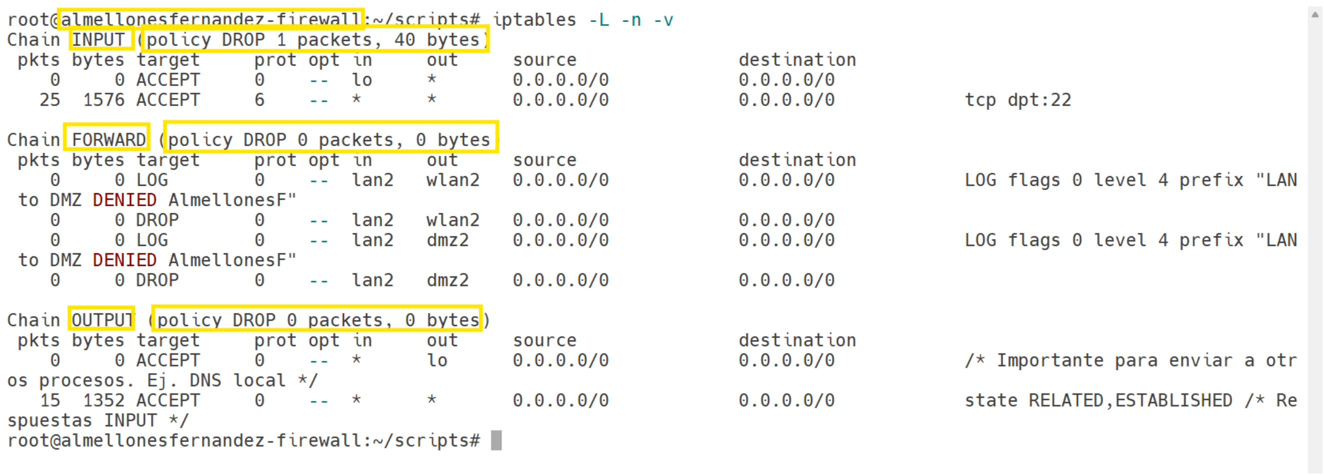
a) **Único** servicio instalado en la máquina, servicio SSHD.



```
almellonesfernandez@almellonesfernandez-firewall:~$ sudo netstat -putan |grep LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      725/systemd-resolve
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      1461/sshd: almellon
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      725/systemd-resolve
tcp6       0      0 ::1:6010                :::*                    LISTEN      1461/sshd: almellon
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
almellonesfernandez@almellonesfernandez-firewall:~$
```

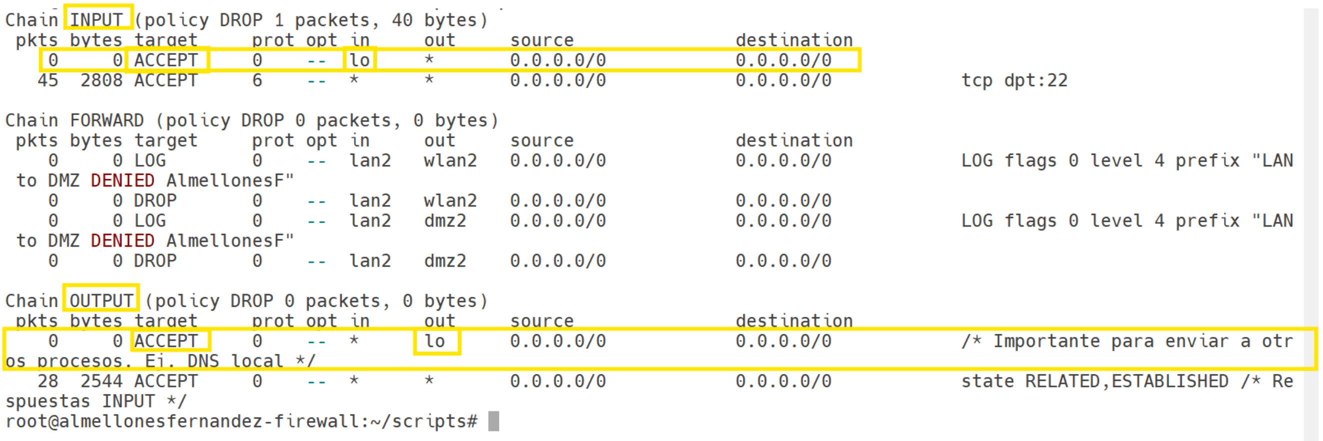
Álvaro Almellones Fernández

b) Reglas defecto DROP para la tabla filter en el firewall para INPUT/OUTPUT/FORWARD en las reglas de la tabla FILTER. Reglas de borrado por defecto.



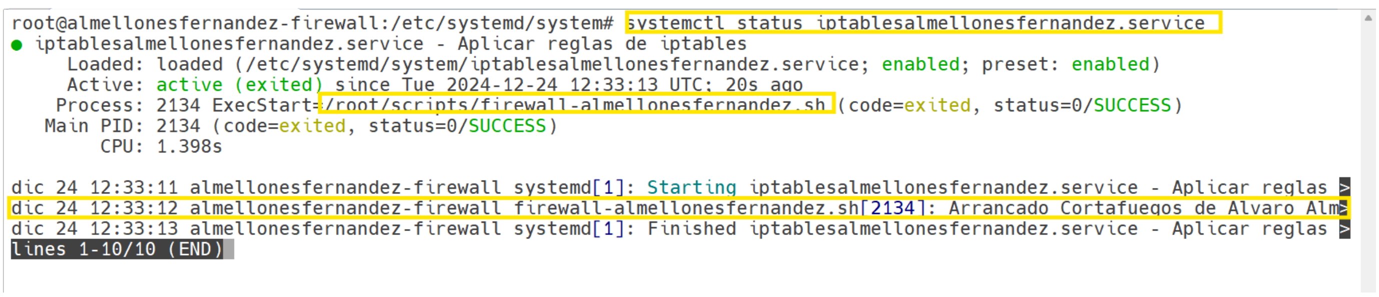
```
root@almellonesfernandez-firewall:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 40 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   25  1576 ACCEPT     6    --  *      *       0.0.0.0/0            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 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   15  1352 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts# 
```

c) Firewall consigo mismo se permitirá todo (loopback).



```
Chain INPUT (policy DROP 1 packets, 40 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   45  2808 ACCEPT     6    --  *      *       0.0.0.0/0            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 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   28  2544 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts# 
```

d) El script de iptables se arrancará en el inicio de la máquina (/etc/rc.local) o mediante servicio.

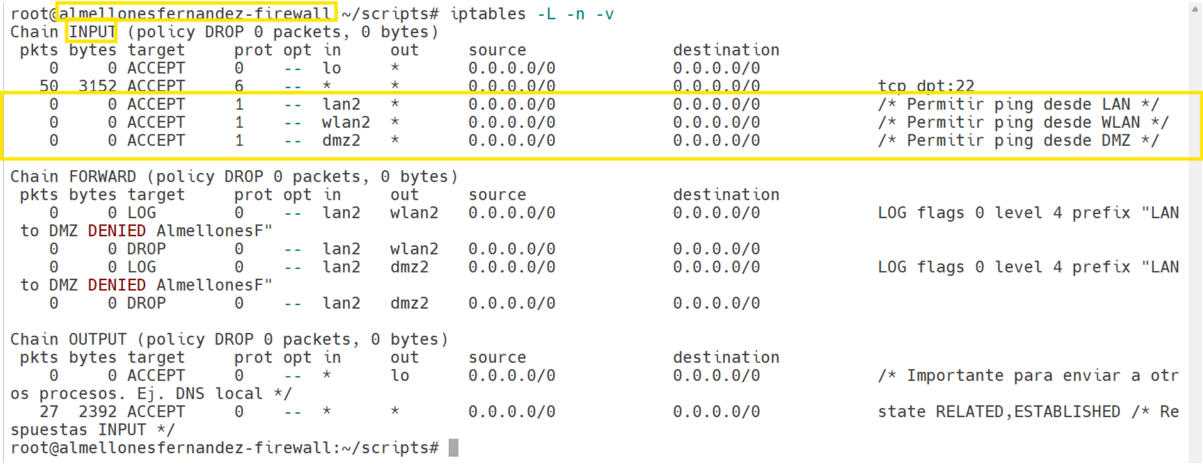


```
root@almellonesfernandez-firewall:/etc/systemd/system# systemctl status iptablesalmellonesfernandez.service
● iptablesalmellonesfernandez.service - Aplicar reglas de iptables
     Loaded: loaded (/etc/systemd/system/iptablesalmellonesfernandez.service; enabled; preset: enabled)
     Active: active (exited) since Tue 2024-12-24 12:33:13 UTC; 20s ago
    Process: 2134 ExecStart=/root/scripts/firewall-almellonesfernandez.sh (code=exited, status=0/SUCCESS)
   Main PID: 2134 (code=exited, status=0/SUCCESS)
        CPU: 1.398s

dic 24 12:33:11 almellonesfernandez-firewall systemd[1]: Starting iptablesalmellonesfernandez.service - Aplicar reglas >
dic 24 12:33:12 almellonesfernandez-firewall firewall-almellonesfernandez.sh[2134]: Arrancado Cortafuegos de Alvaro Alm>
dic 24 12:33:13 almellonesfernandez-firewall systemd[1]: Finished iptablesalmellonesfernandez.service - Aplicar reglas >
lines 1-10/10 (END)
```

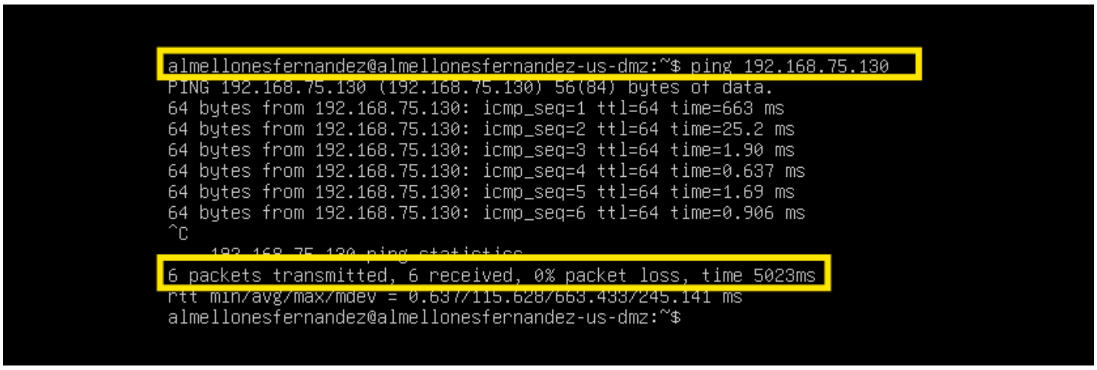
Álvaro Almellones Fernández

2. **(1 punto)** Reglas de INPUT. Vamos asegurar nuestro servidor de posibles ataques desde las cuatro tarjetas de red, para ello se configurará de la siguiente forma**.**

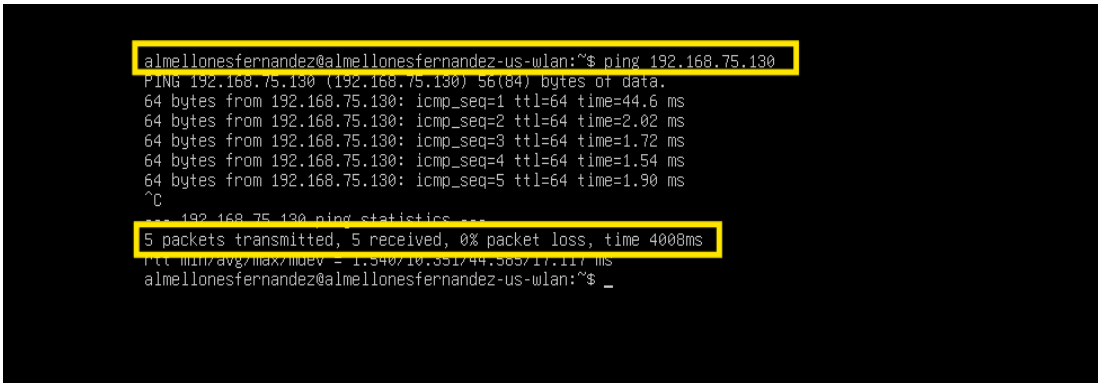
a) Se puede hacer ping al firewall desde cualquier sitio LAN, WLAN y DMZ, pero no desde WAN. Dejar después que se pueda hacer ping desde todas las subredes.



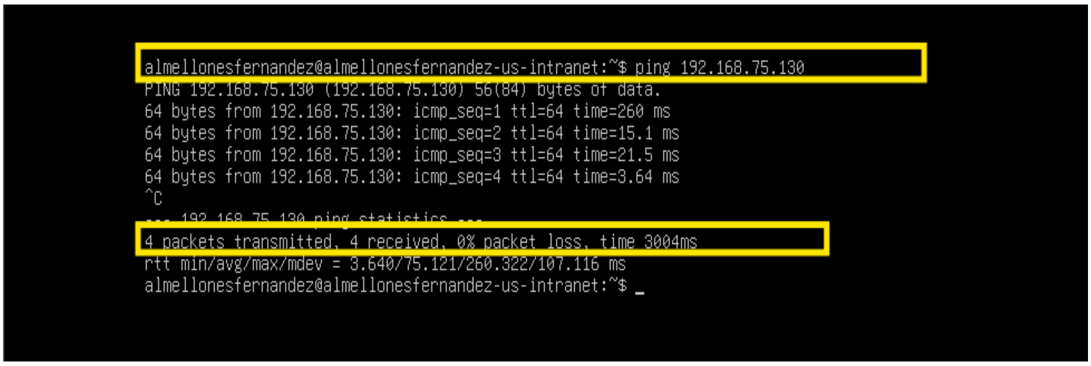
```
root@almellonesfernandez-firewall:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   50  3152 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     1    --  lan2   *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde LAN */
    0     0 ACCEPT     1    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde WLAN */
    0     0 ACCEPT     1    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde DMZ */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   27  2392 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts#
```



```
almellonesfernandez@almellonesfernandez-us-dmz:~$ ping 192.168.75.130
PING 192.168.75.130 (192.168.75.130) 56(84) bytes of data.
64 bytes from 192.168.75.130: icmp_seq=1 ttl=64 time=663 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=25.2 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=1.90 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=0.637 ms
64 bytes from 192.168.75.130: icmp_seq=5 ttl=64 time=1.69 ms
64 bytes from 192.168.75.130: icmp_seq=6 ttl=64 time=0.906 ms
^C
--- 192.168.75.130 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5023ms
rtt min/avg/max/mdev = 0.637/115.628/663.433/245.141 ms
almellonesfernandez@almellonesfernandez-us-dmz:~$
```



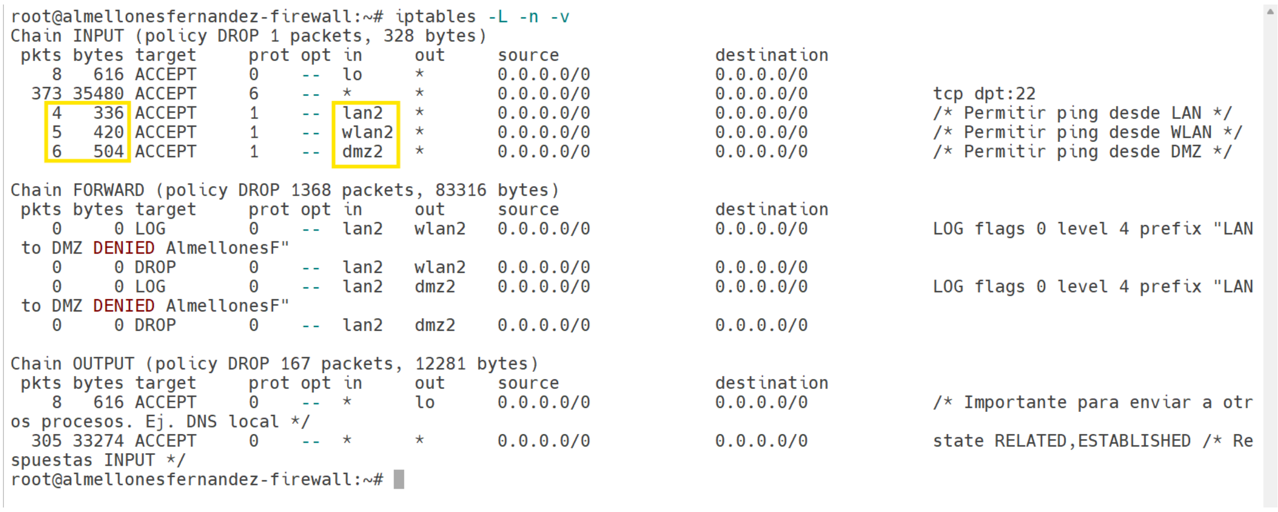
```
almellonesfernandez@almellonesfernandez-us-wlan:~$ ping 192.168.75.130
PING 192.168.75.130 (192.168.75.130) 56(84) bytes of data.
64 bytes from 192.168.75.130: icmp_seq=1 ttl=64 time=44.6 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=2.02 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=1.72 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=1.54 ms
64 bytes from 192.168.75.130: icmp_seq=5 ttl=64 time=1.90 ms
^C
--- 192.168.75.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.540/10.351/44.585/17.117 ms
almellonesfernandez@almellonesfernandez-us-wlan:~$ _
```



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ ping 192.168.75.130
PING 192.168.75.130 (192.168.75.130) 56(84) bytes of data.
64 bytes from 192.168.75.130: icmp_seq=1 ttl=64 time=260 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=15.1 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=21.5 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=3.64 ms
^C
--- 192.168.75.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.640/75.121/260.322/107.116 ms
almellonesfernandez@almellonesfernandez-us-intranet:~$ _
```

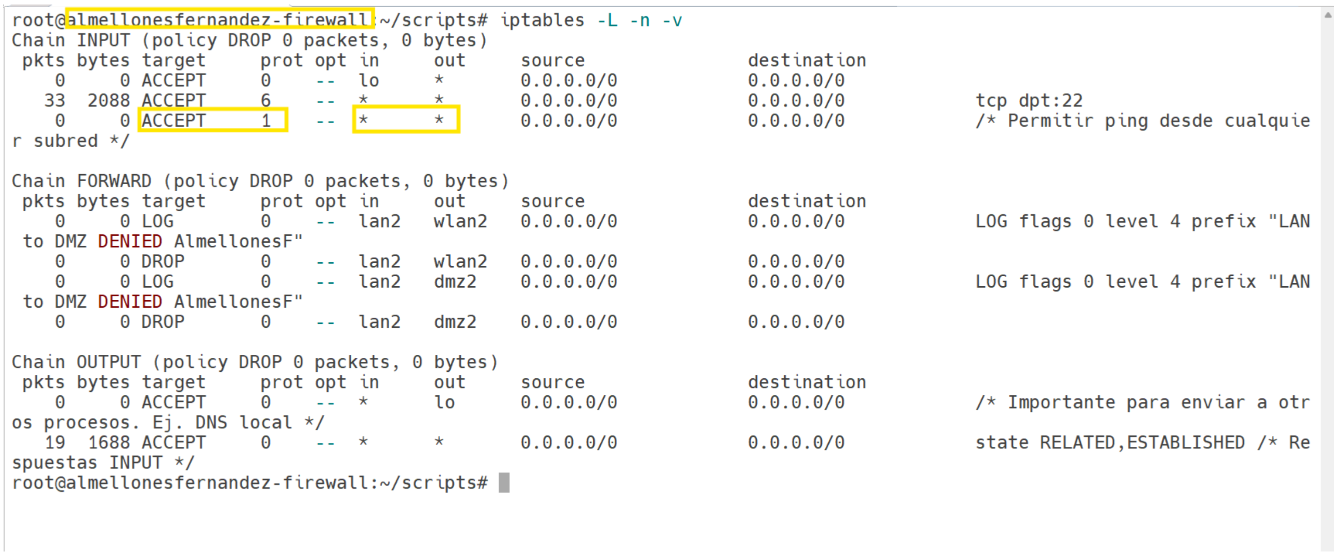
Álvaro Almellones Fernández

Se ve muy mal porque todavía no tengo los output configurados y no puedo hacer ssh a las máquinas pero son los ping a la máquina firewall desde las redes que permite el ping



```
root@almellonesfernandez-firewall:~# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   616 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
  373 35480 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    4   336 ACCEPT     1    --  lan2   *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde LAN */
    5   420 ACCEPT     1    --  wlan2  *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde WLAN */
    6   504 ACCEPT     1    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde DMZ */

Chain FORWARD (policy DROP 1368 packets, 83316 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 167 packets, 12281 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   616 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  305 33274 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~#
```

WAN no puede hacer ping porque la política por defecto está en DROP y no hay ninguna regla que acepte que WAN pueda hacer ping

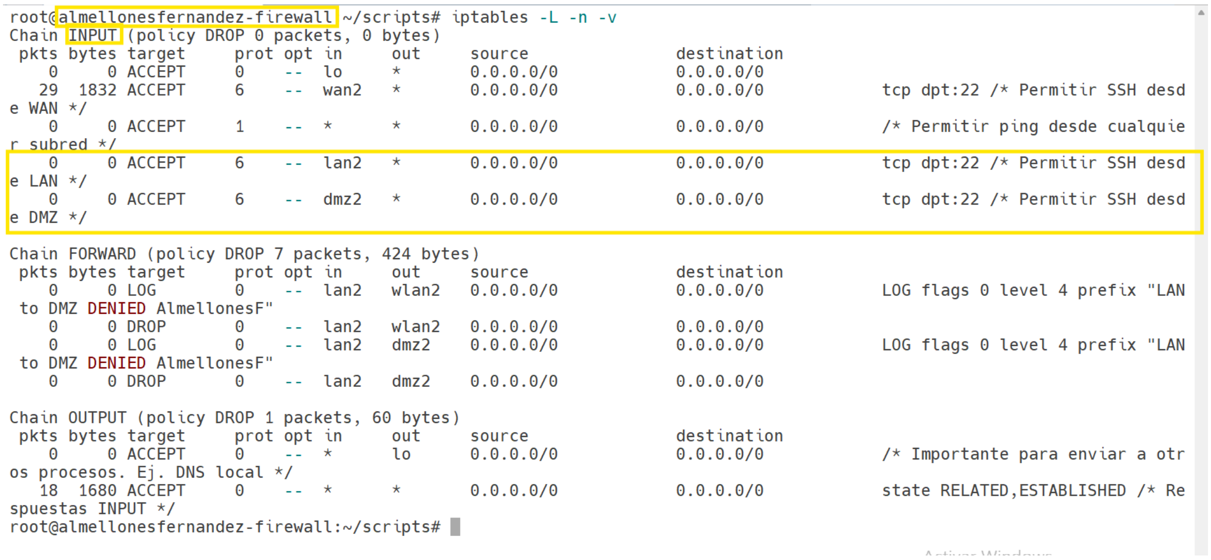


```
root@almellonesfernandez-firewall:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   33  2088 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   19  1688 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts#
```

Finalmente dejo que todas desde todas las redes se pueda hacer ping como se pide

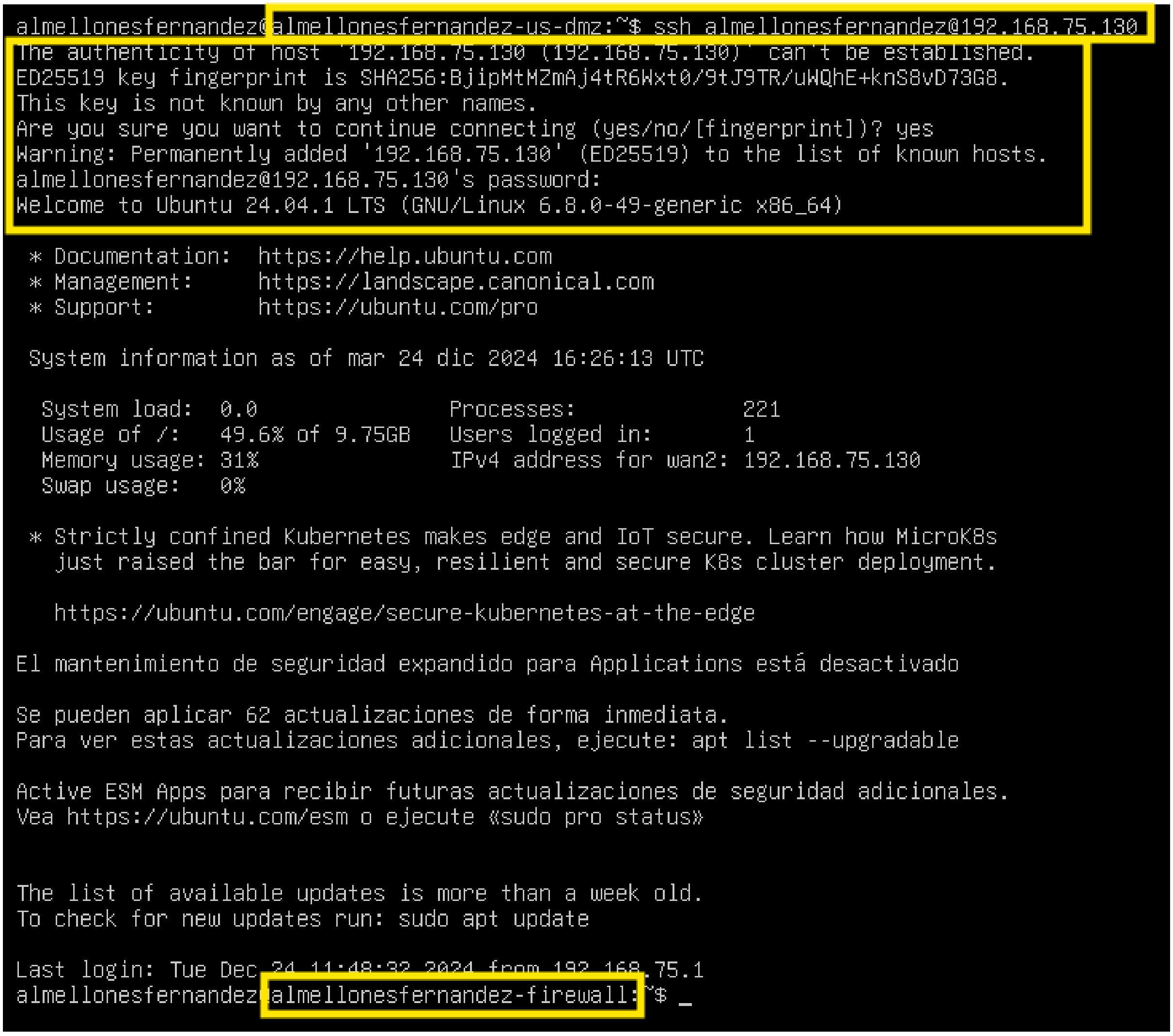
b) Se puede acceder al firewall vía ssh desde todas las interfaces menos desde la zona WLAN. Si la petición se realiza desde dentro (LAN y DMZ).

Álvaro Almellones Fernández



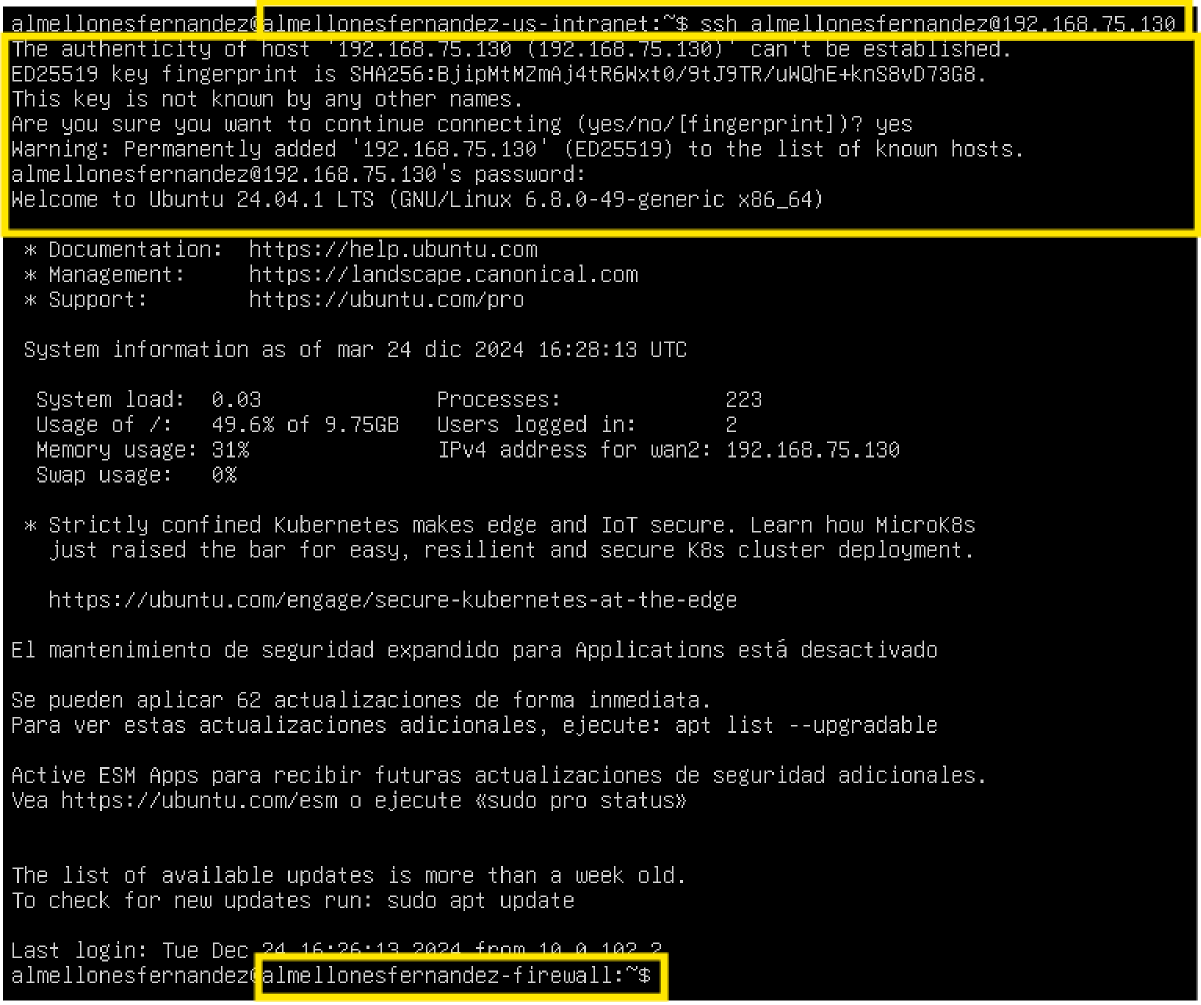
```
root@almellonesfernandez-firewall ~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   29  1832 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */

Chain FORWARD (policy DROP 7 packets, 424 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 1 packets, 60 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   18  1680 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts# █
```

He permitido que WAN pueda hacer ssh para que las capturas de firewall se vean en blanco



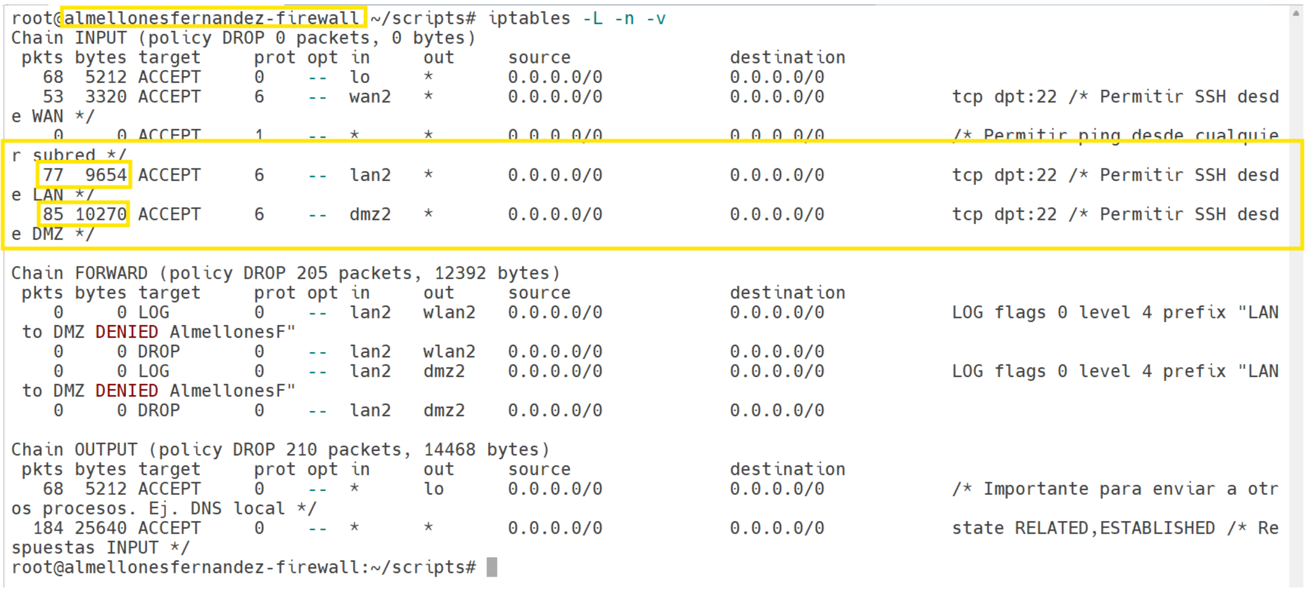
```
almellonesfernandez@almellonesfernandez-us-dmz:~$ ssh almellonesfernandez@192.168.75.130
The authenticity of host '192.168.75.130 (192.168.75.130)' can't be established.
ED25519 key fingerprint is SHA256:BjipMtMZmAj4tR6Wxt0/9tJ9TR/uWQhE+knS8vD73G8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.75.130' (ED25519) to the list of known hosts.
almellonesfernandez@192.168.75.130's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 24 dic 2024 16:26:13 UTC

  System load:  0.0               Processes:             221
  Usage of /:   49.6% of 9.75GB   Users logged in:       1
  Memory usage: 31%               IPv4 address for wan2: 192.168.75.130
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 62 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 24 11:48:32 2024 from 192.168.75.1
almellonesfernandez@almellonesfernandez-firewall:~$ _
```

Álvaro Almellones Fernández



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ ssh almellonesfernandez@192.168.75.130
The authenticity of host '192.168.75.130 (192.168.75.130)' can't be established.
ED25519 key fingerprint is SHA256:BjipMtMZmAj4tR6Wxt0/9tJ9TR/uWQhE+knS8vD73G8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.75.130' (ED25519) to the list of known hosts.
almellonesfernandez@192.168.75.130's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 24 dic 2024 16:28:13 UTC

  System load:  0.03               Processes:             223
  Usage of /:   49.6% of 9.75GB    Users logged in:       2
  Memory usage: 31%                IPv4 address for wan2: 192.168.75.130
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 62 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 24 16:26:13 2024 from 10.0.102.2
almellonesfernandez@almellonesfernandez-firewall:~$
```

Como no tengo los outputs configurados no puedo poner el fondo blanco para las capturas pero como se observa son los ssh desde las redes que si permito.



```
root@almellonesfernandez-firewall ~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   68  5212 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   53  3320 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
   77  9654 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
   85 10270 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */

Chain FORWARD (policy DROP 205 packets, 12392 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 210 packets, 14468 bytes)
 pkts bytes target     prot opt in     out     source               destination
   68  5212 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  184 25640 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
root@almellonesfernandez-firewall:~/scripts# 
```

Como podemos observar los contadores de las dos redes que permite hacer ssh aumenta

c) No se permitirá **nada** más.

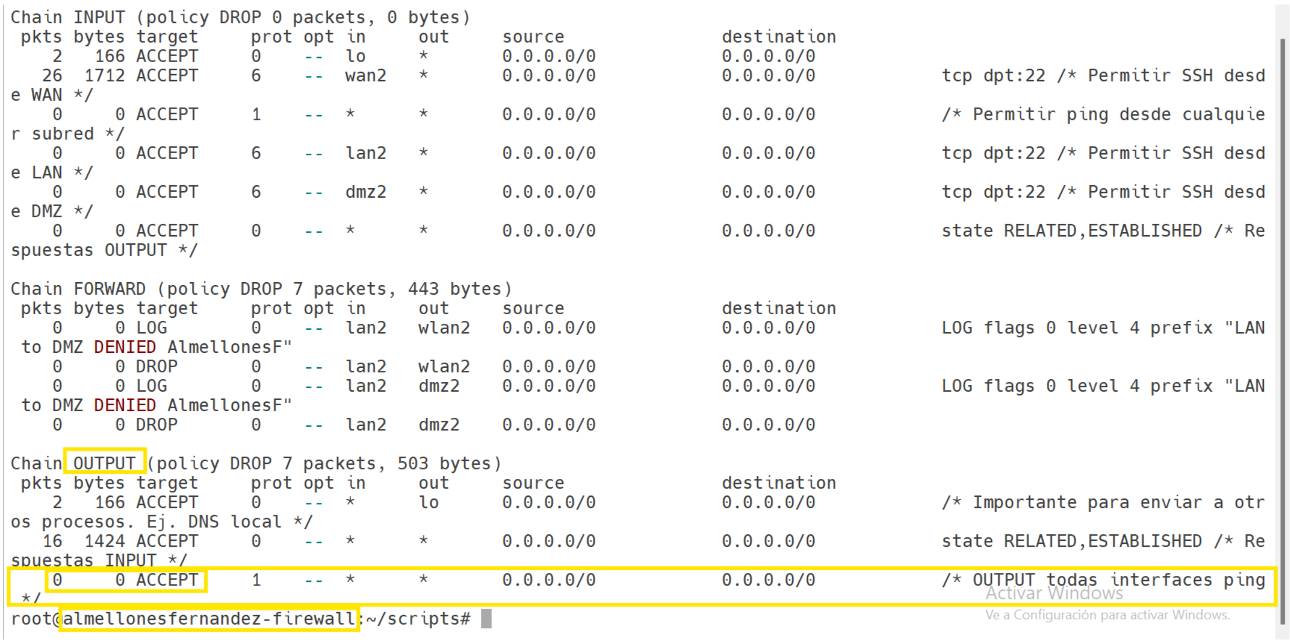
Al poner las políticas por defecto en DROP no se permite nada más a menos de que aplique en iptables una regla ACCEPT

Álvaro Almellones Fernández

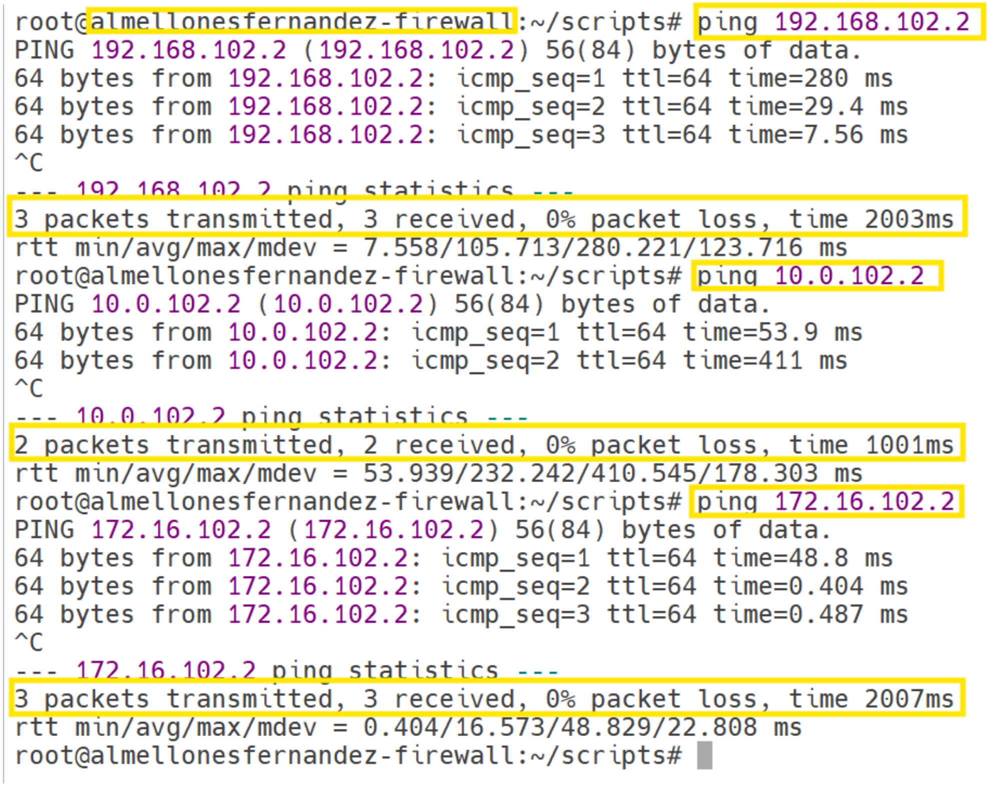
3. Reglas de OUTPUT, de la siguiente forma.

a) **(0,5 puntos)** Por todas las tarjetas de red, podrá:

• Realizar ping a todas las subredes a cualquier equipo que haya en dicha subred.

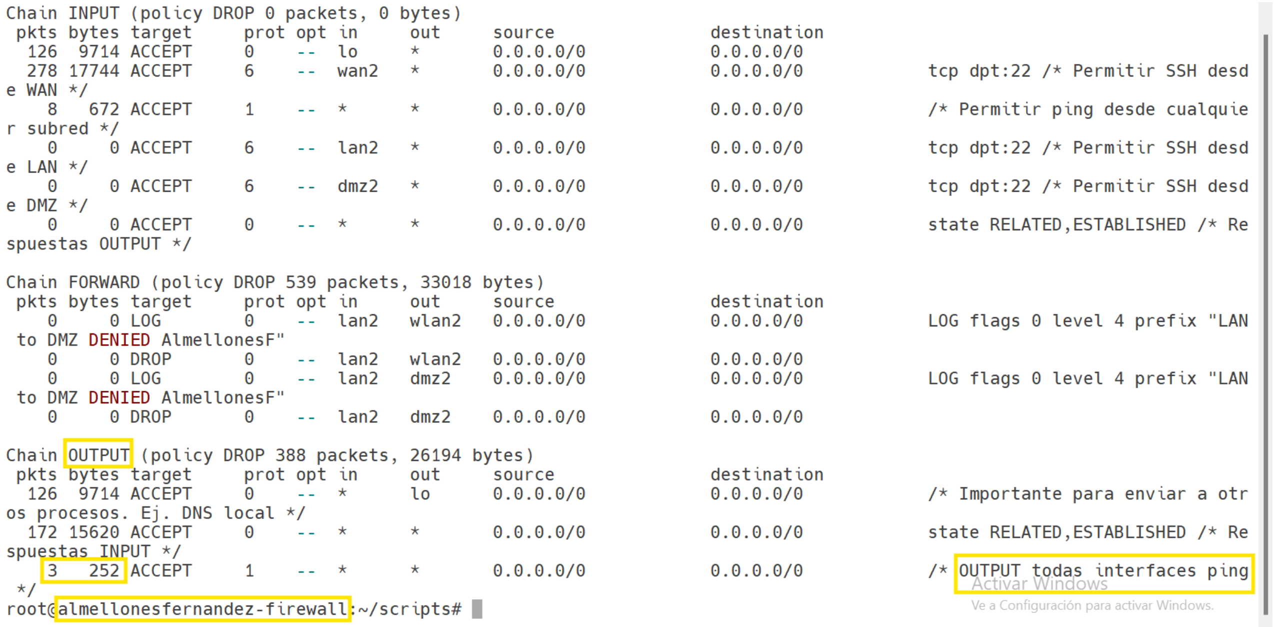


```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   166 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
   26  1712 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 7 packets, 443 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 7 packets, 503 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   166 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   16  1424 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
root@almellonesfernandez-firewall:~/scripts#
```



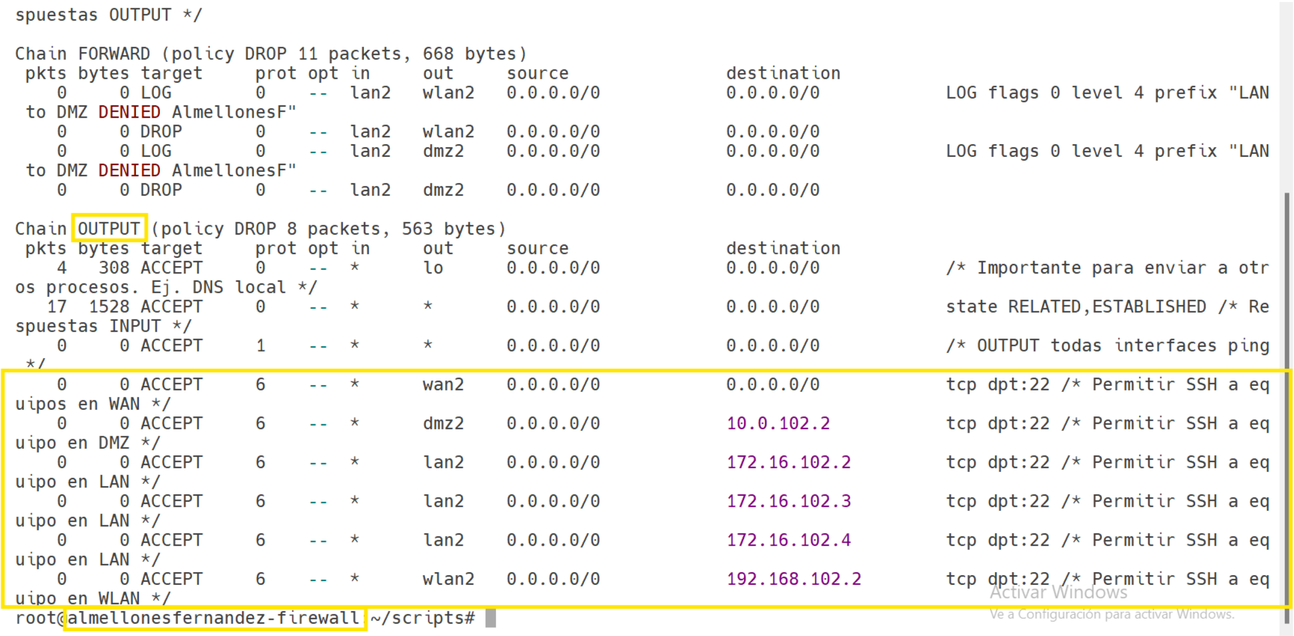
```
root@almellonesfernandez-firewall:~/scripts# ping 192.168.102.2
PING 192.168.102.2 (192.168.102.2) 56(84) bytes of data.
64 bytes from 192.168.102.2: icmp_seq=1 ttl=64 time=280 ms
64 bytes from 192.168.102.2: icmp_seq=2 ttl=64 time=29.4 ms
64 bytes from 192.168.102.2: icmp_seq=3 ttl=64 time=7.56 ms
^C
--- 192.168.102.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.558/105.713/280.221/123.716 ms
root@almellonesfernandez-firewall:~/scripts# ping 10.0.102.2
PING 10.0.102.2 (10.0.102.2) 56(84) bytes of data.
64 bytes from 10.0.102.2: icmp_seq=1 ttl=64 time=53.9 ms
64 bytes from 10.0.102.2: icmp_seq=2 ttl=64 time=411 ms
^C
--- 10.0.102.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 53.939/232.242/410.545/178.303 ms
root@almellonesfernandez-firewall:~/scripts# ping 172.16.102.2
PING 172.16.102.2 (172.16.102.2) 56(84) bytes of data.
64 bytes from 172.16.102.2: icmp_seq=1 ttl=64 time=48.8 ms
64 bytes from 172.16.102.2: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 172.16.102.2: icmp_seq=3 ttl=64 time=0.487 ms
^C
--- 172.16.102.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.404/16.573/48.829/22.808 ms
root@almellonesfernandez-firewall:~/scripts#
```

Álvaro Almellones Fernández



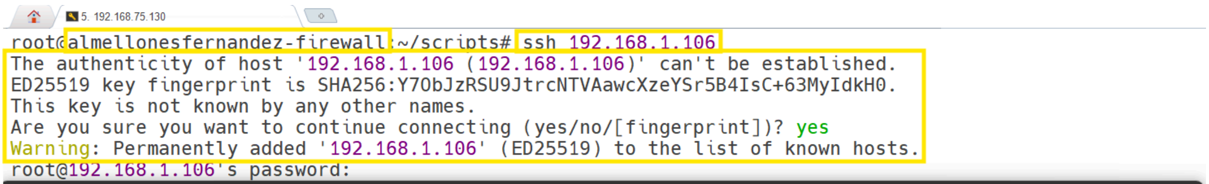
```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  126  9714 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
  278 17744 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e WAN */
    8   672 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 539 packets, 33018 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 388 packets, 26194 bytes)
 pkts bytes target     prot opt in     out     source               destination
  126  9714 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  172 15620 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    3   252 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
root@almellonesfernandez-firewall:~/scripts# 
```

- Conectarse por ssh a cualquier equipo de la red wan, y únicamente a las IP (que tenemos ahora, habrá que ir añadiendo a lo largo del curso, caso de que haga falta) de la zona DMZ, LAN y WLAN.

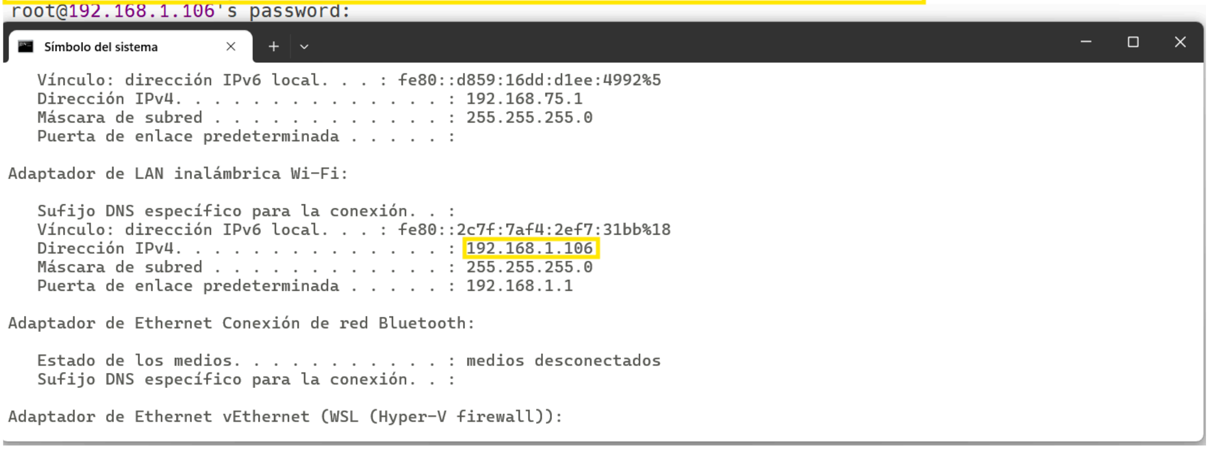


```
spuestas OUTPUT */

Chain FORWARD (policy DROP 11 packets, 668 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 8 packets, 563 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   308 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   17  1528 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
root@almellonesfernandez-firewall:~/scripts# 
```

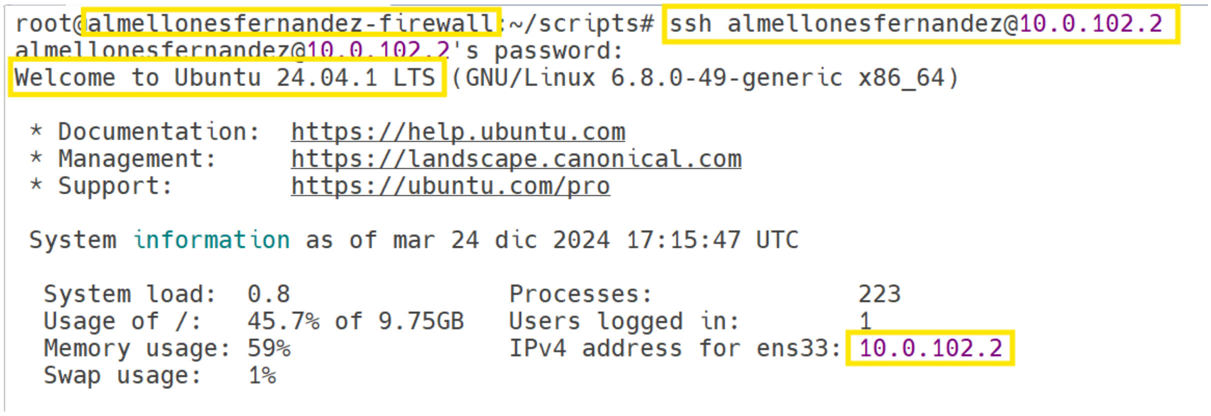
Álvaro Almellones Fernández



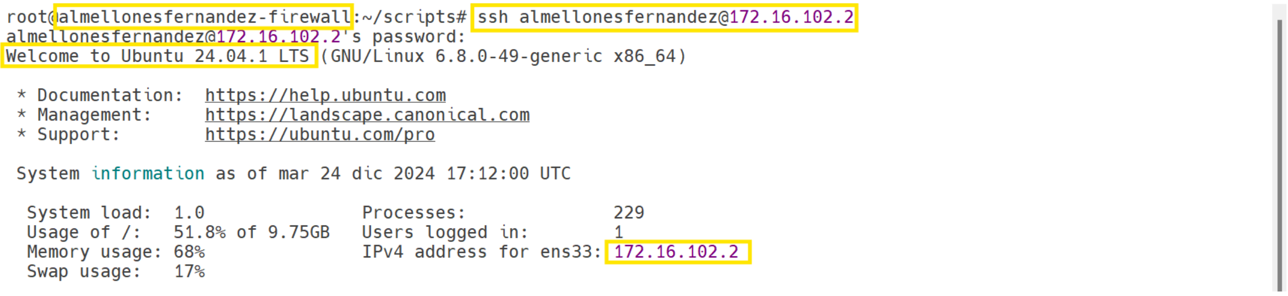
```
root@almellonesfernandez-firewall:~/scripts# ssh 192.168.1.106
The authenticity of host '192.168.1.106 (192.168.1.106)' can't be established.
ED25519 key fingerprint is SHA256:Y7ObJzRSU9JtrcNTVAawcXzeYSr5B4IsC+63MyIdkH0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.106' (ED25519) to the list of known hosts.
root@192.168.1.106's password:
```



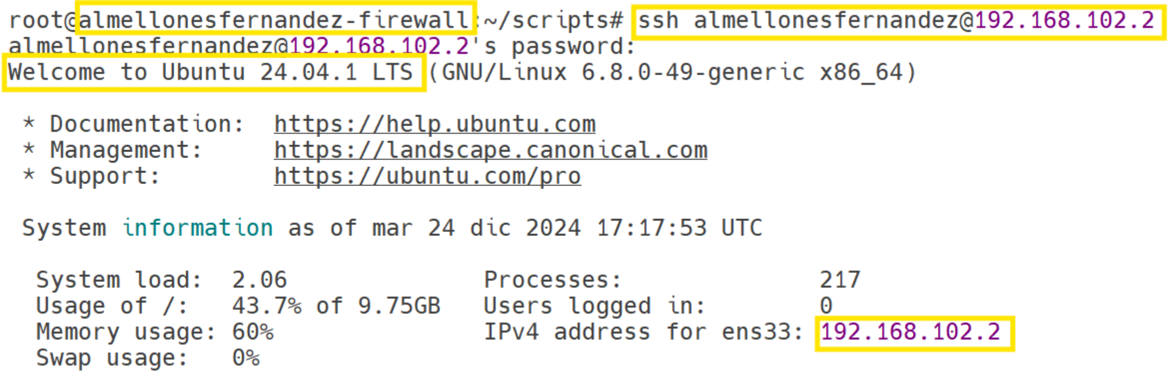
```
   Vínculo: dirección IPv6 local. . . : fe80::d859:16dd:d1ee:4992%5
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.75.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::2c7f:7af4:2ef7:31bb%18
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.106
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet vEthernet (WSL (Hyper-V firewall)):
```



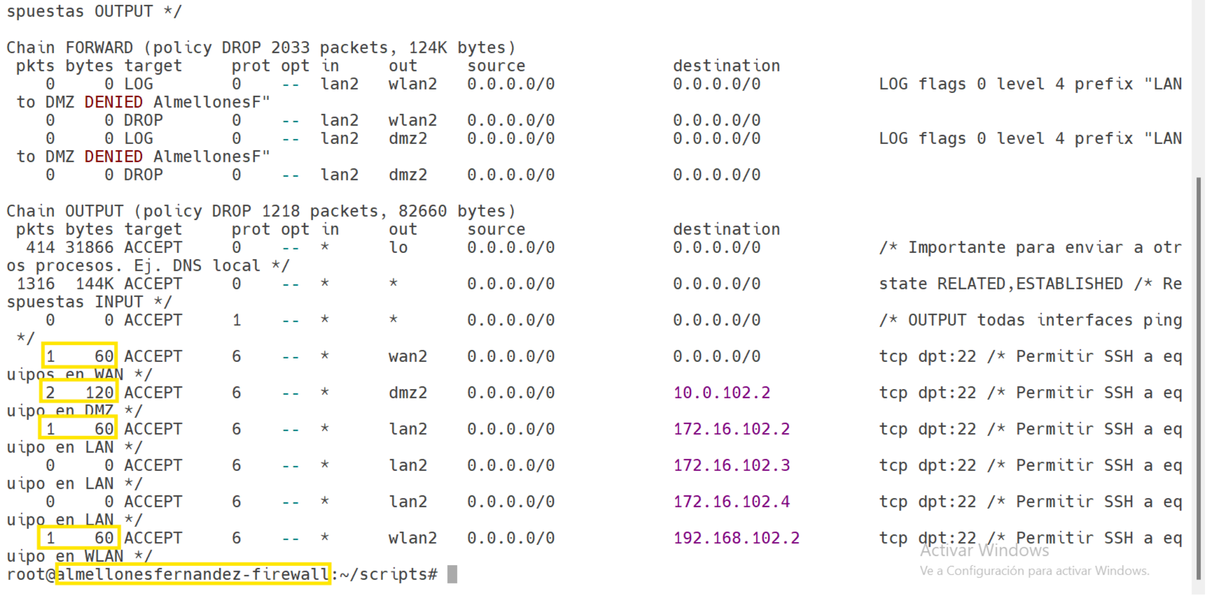
```
root@almellonesfernandez-firewall:~/scripts# ssh almellonesfernandez@10.0.102.2
almellonesfernandez@10.0.102.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 24 dic 2024 17:15:47 UTC

  System load:  0.8               Processes:             223
  Usage of /:   45.7% of 9.75GB   Users logged in:       1
  Memory usage: 59%               IPv4 address for ens33: 10.0.102.2
  Swap usage:   1%
```



```
root@almellonesfernandez-firewall:~/scripts# ssh almellonesfernandez@172.16.102.2
almellonesfernandez@172.16.102.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 24 dic 2024 17:12:00 UTC

  System load:  1.0               Processes:             229
  Usage of /:   51.8% of 9.75GB   Users logged in:       1
  Memory usage: 68%               IPv4 address for ens33: 172.16.102.2
  Swap usage:   17%
```



```
root@almellonesfernandez-firewall:~/scripts# ssh almellonesfernandez@192.168.102.2
almellonesfernandez@192.168.102.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 24 dic 2024 17:17:53 UTC

  System load:  2.06              Processes:             217
  Usage of /:   43.7% of 9.75GB   Users logged in:       0
  Memory usage: 60%               IPv4 address for ens33: 192.168.102.2
  Swap usage:   0%
```

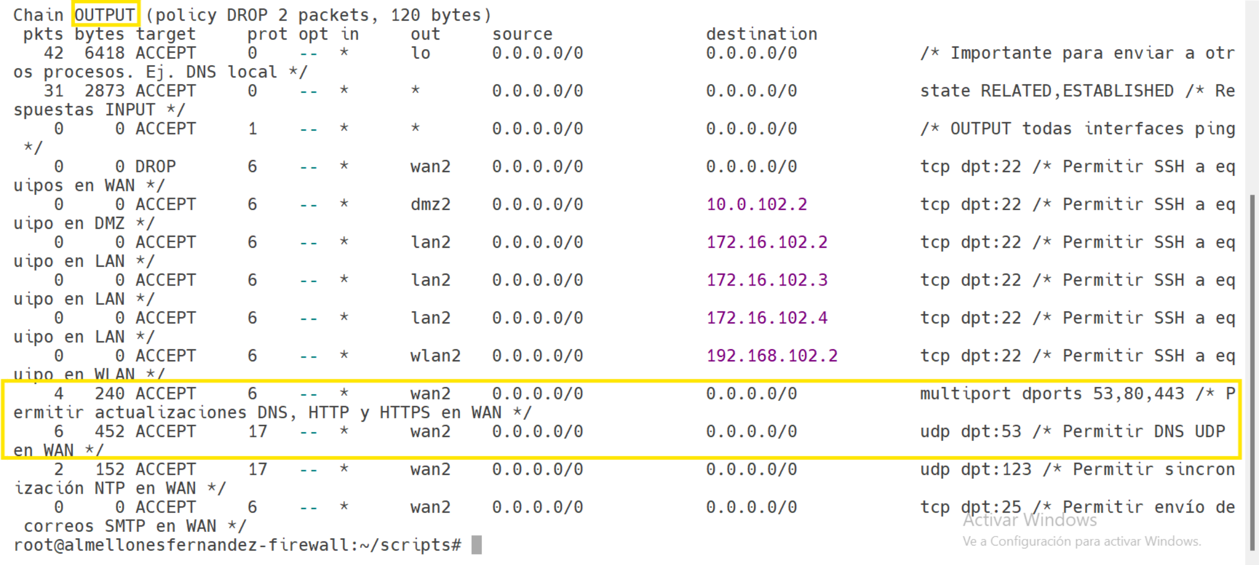


```
spuestas OUTPUT */

Chain FORWARD (policy DROP 2033 packets, 124K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 1218 packets, 82660 bytes)
 pkts bytes target     prot opt in     out     source               destination
  414 31866 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
 1316  144K ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    1    60 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    2   120 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    1    60 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    1    60 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
root@almellonesfernandez-firewall:~/scripts# 
```

Como podemos ver los contadores que permiten ssh que he comprobado han aumentado

b) **(0,5 puntos)** Por la tarjeta wan, únicamente como es obvio, podrá:

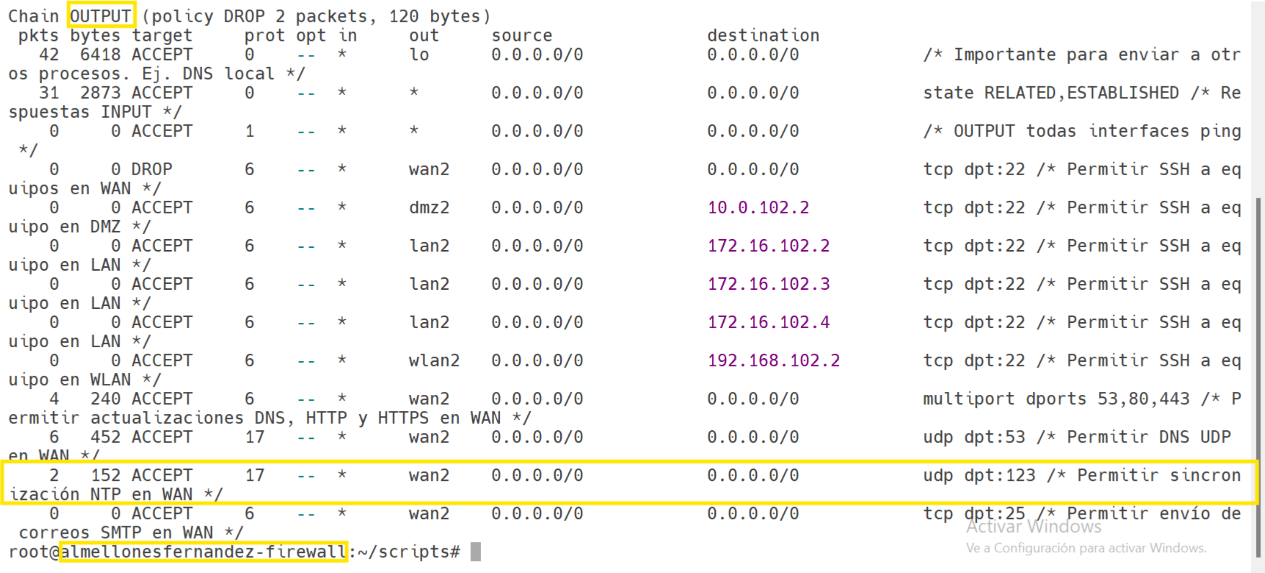
- Actualizarse (DNS, HTTP, HTTPS) y descargar páginas web (wget, curl, etc.)



```
Chain OUTPUT (policy DROP 2 packets, 120 bytes)
 pkts bytes target     prot opt in     out     source               destination
   42  6418 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   31  2873 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
    4   240 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            multiport dports 53,80,443 /* P
ermitir actualizaciones DNS, HTTP y HTTPS en WAN */
    6   452 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* Permitir DNS UDP
en WAN */
    2   152 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123 /* Permitir sincron
ización NTP en WAN */
    0     0 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:25 /* Permitir envío de
 correos SMTP en WAN */
root@almellonesfernandez-firewall:~/scripts# 
```

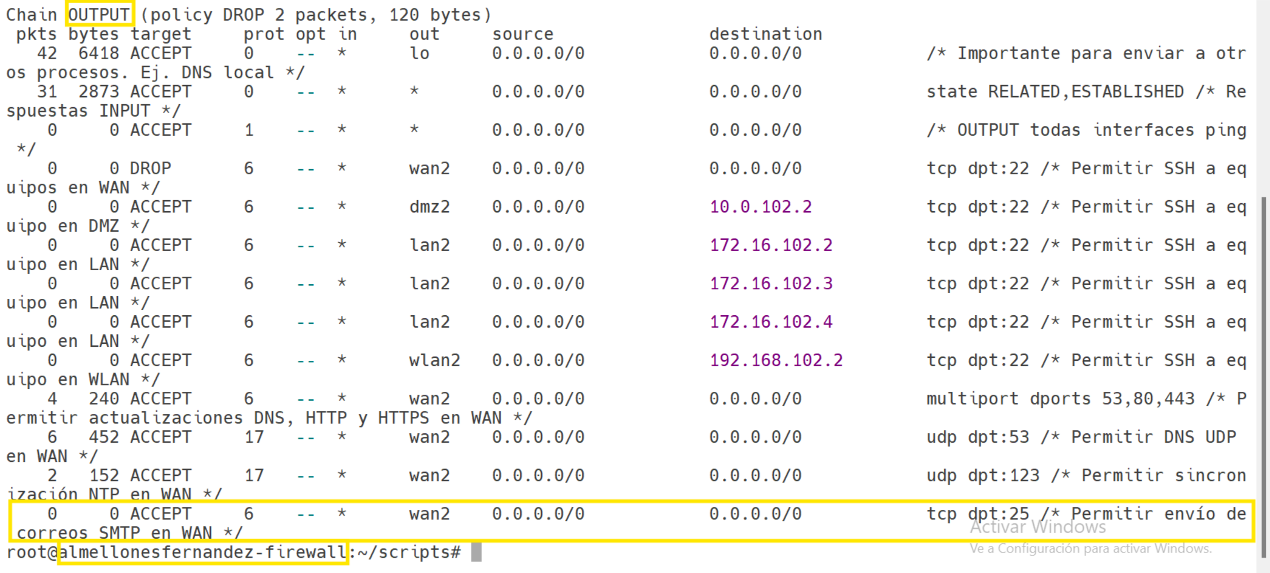
- Actualizar su hora.

Álvaro Almellones Fernández



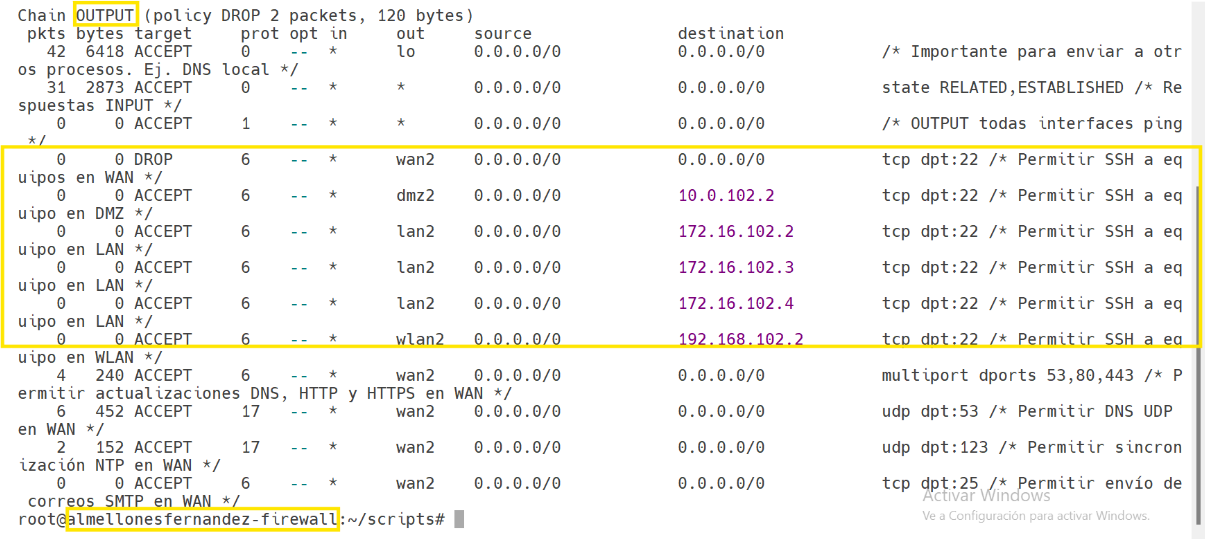
```
Chain OUTPUT (policy DROP 2 packets, 120 bytes)
 pkts bytes target     prot opt in     out     source               destination
   42  6418 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   31  2873 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
    4   240 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            multiport dports 53,80,443 /* P
ermitir actualizaciones DNS, HTTP y HTTPS en WAN */
    6   452 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* Permitir DNS UDP
en WAN */
    2   152 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123 /* Permitir sincron
ización NTP en WAN */
    0     0 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:25 /* Permitir envío de
 correos SMTP en WAN */
root@almellonesfernandez-firewall:~/scripts#
```

- Enviar email (puerto smtp 25).



```
Chain OUTPUT (policy DROP 2 packets, 120 bytes)
 pkts bytes target     prot opt in     out     source               destination
   42  6418 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   31  2873 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
    4   240 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            multiport dports 53,80,443 /* P
ermitir actualizaciones DNS, HTTP y HTTPS en WAN */
    6   452 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* Permitir DNS UDP
en WAN */
    2   152 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123 /* Permitir sincron
ización NTP en WAN */
    0     0 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:25 /* Permitir envío de
 correos SMTP en WAN */
root@almellonesfernandez-firewall:~/scripts#
```

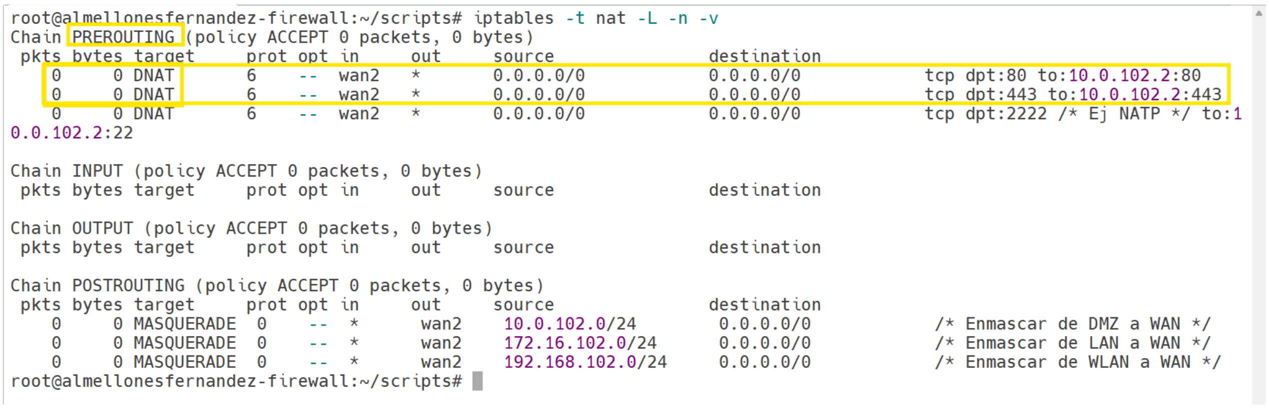
- Conectarse por ssh a todos los equipos de todas las zonas, menos a la WAN.



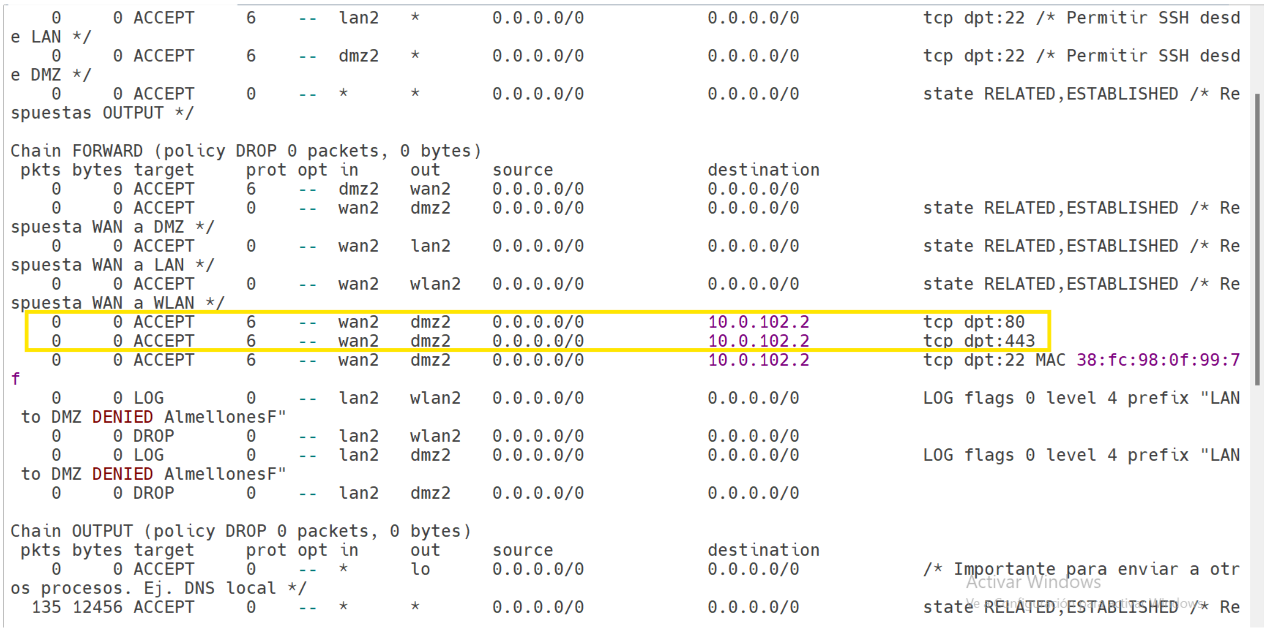
```
Chain OUTPUT (policy DROP 2 packets, 120 bytes)
 pkts bytes target     prot opt in     out     source               destination
   42  6418 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   31  2873 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
    0     0 ACCEPT     6    --  *      dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 /* Permitir SSH a eq
uipo en DMZ */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.2         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.3         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      lan2    0.0.0.0/0            172.16.102.4         tcp dpt:22 /* Permitir SSH a eq
uipo en LAN */
    0     0 ACCEPT     6    --  *      wlan2   0.0.0.0/0            192.168.102.2        tcp dpt:22 /* Permitir SSH a eq
uipo en WLAN */
    4   240 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            multiport dports 53,80,443 /* P
ermitir actualizaciones DNS, HTTP y HTTPS en WAN */
    6   452 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* Permitir DNS UDP
en WAN */
    2   152 ACCEPT     17   --  *      wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123 /* Permitir sincron
ización NTP en WAN */
    0     0 ACCEPT     6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:25 /* Permitir envío de
 correos SMTP en WAN */
root@almellonesfernandez-firewall:~/scripts#
```

4. **Reglas Filter Forward y NAT:** Accesos a la zona DMZ desde exclusivamente wan:

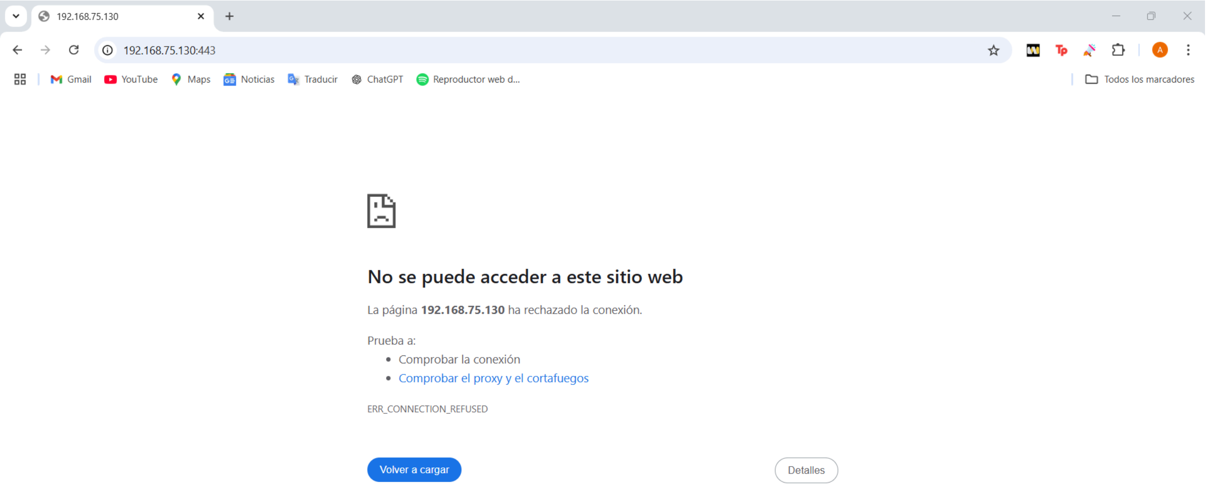
a) **(1,5 puntos)** Se puede acceder al servidor Web de la zona DMZ en los puertos 80 y 443.



```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP */ to:1
0.0.102.2:22

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  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WAN */
root@almellonesfernandez-firewall:~/scripts#
```



```
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 MAC 38:fc:98:0f:99:7
f
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  135 12456 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
```



No se puede acceder a este sitio web

La página **192.168.75.130** ha rechazado la conexión.

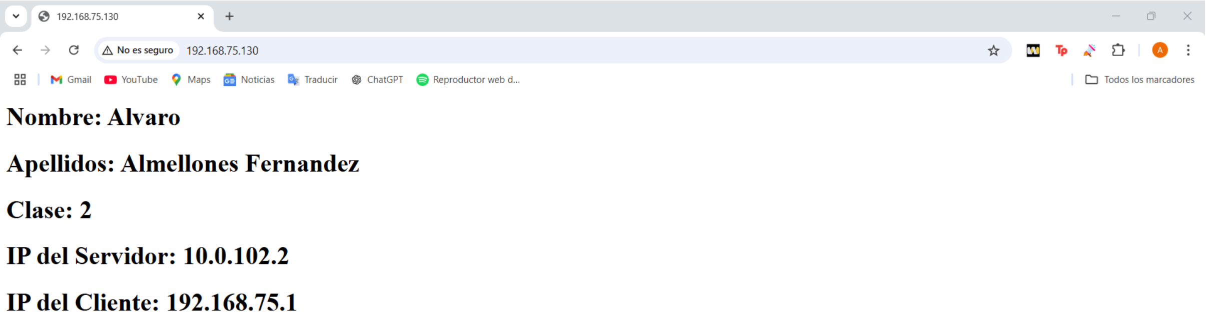
Prueba a:

- Comprobar la conexión
- Comprobar el proxy y el cortafuegos

ERR_CONNECTION_REFUSED

Álvaro Almellones Fernández

En el puerto 443 no aparece nada porque no tengo ningun servidor alojado



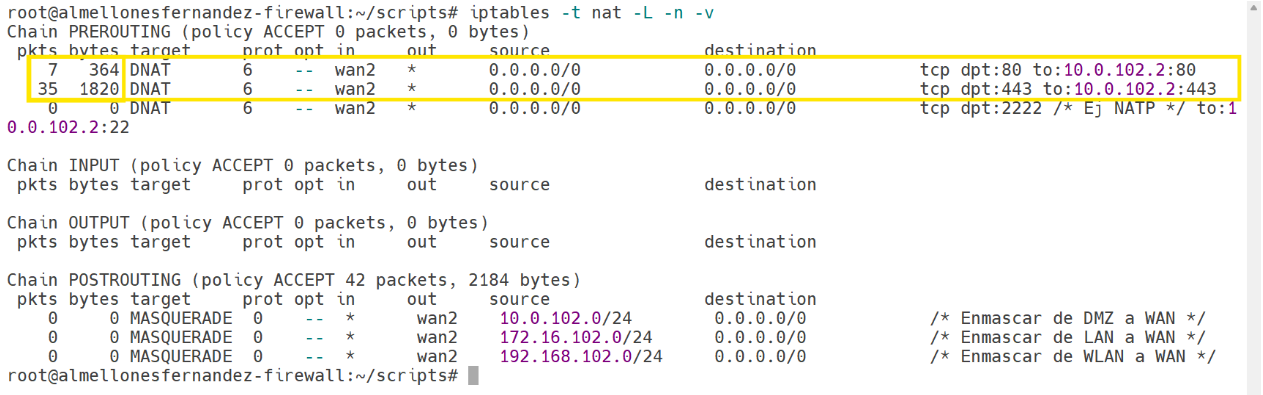
Nombre: Alvaro

Apellidos: Almellones Fernandez

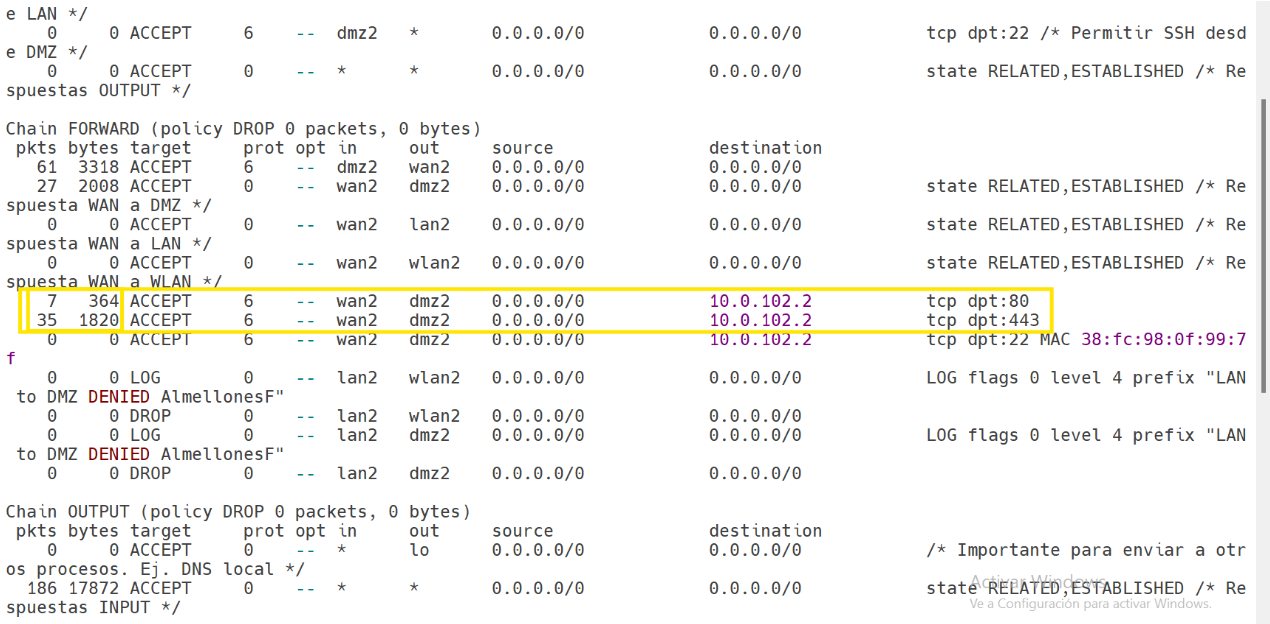
Clase: 2

IP del Servidor: 10.0.102.2

IP del Cliente: 192.168.75.1



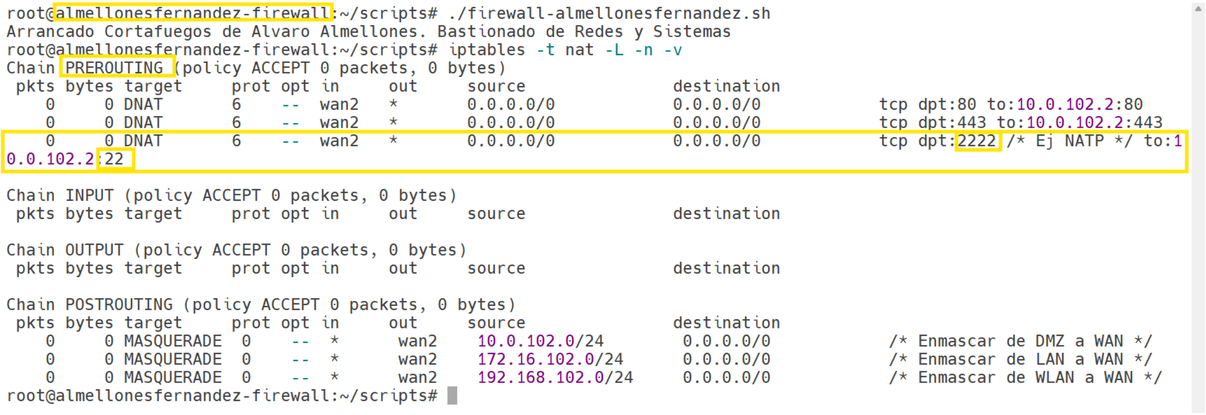
```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    7   364 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:80
   35  1820 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP */ to:1
0.0.102.2:22

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 42 packets, 2184 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24         0.0.0.0/0            /* Enmascar de DMZ a WAN */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24       0.0.0.0/0            /* Enmascar de LAN a WAN */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24      0.0.0.0/0            /* Enmascar de WLAN a WAN */
root@almellonesfernandez-firewall:~/scripts#
```



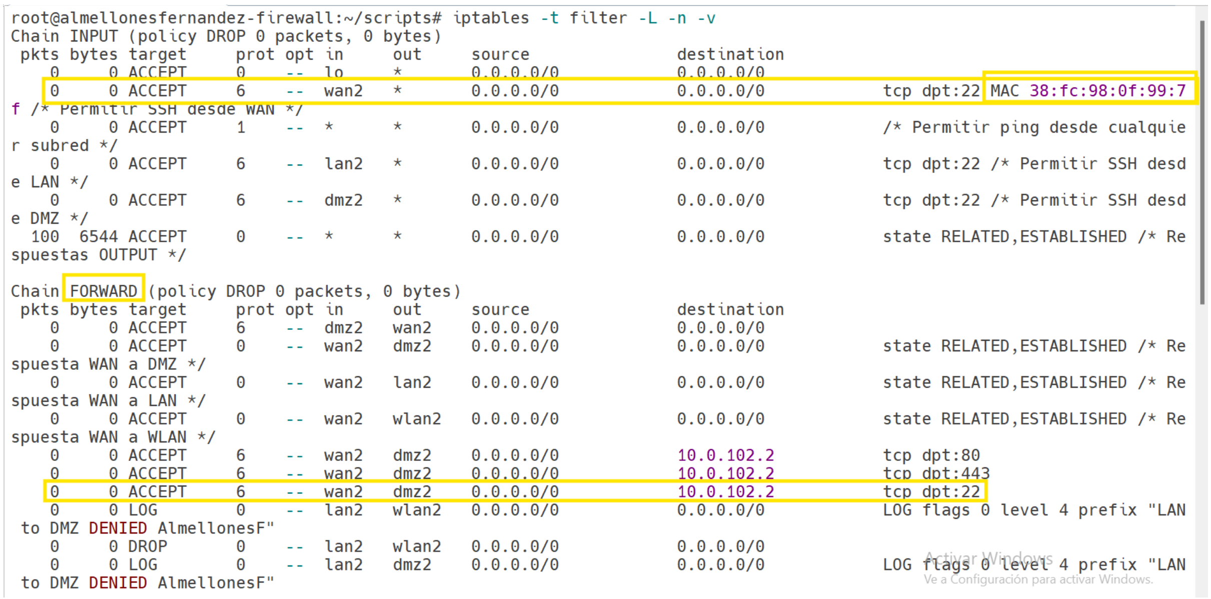
```
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   61  3318 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
   27  2008 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    7   364 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
   35  1820 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22 MAC 38:fc:98:0f:99:7
f
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  186 17872 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
```

Como podemos observar ha funcionado ya que los paquetes tanto de nat como de filter han aumentado, en el puerto 443 no ha aparecido nada ya que no tengo ningún index todavía

b) **(1,5 puntos)** Desde la zona WAN y desde únicamente los equipos de vuestra confianza (por ejemplo, mac de vuestro equipo anfitrión, etc), se podrá acceder al servidor SSH en la zona DMZ, por el puerto que se desee, ya que os recuerdo que el 22 está ocupado para el cortafuegos (INPUT). Se recomienda uso de variable.

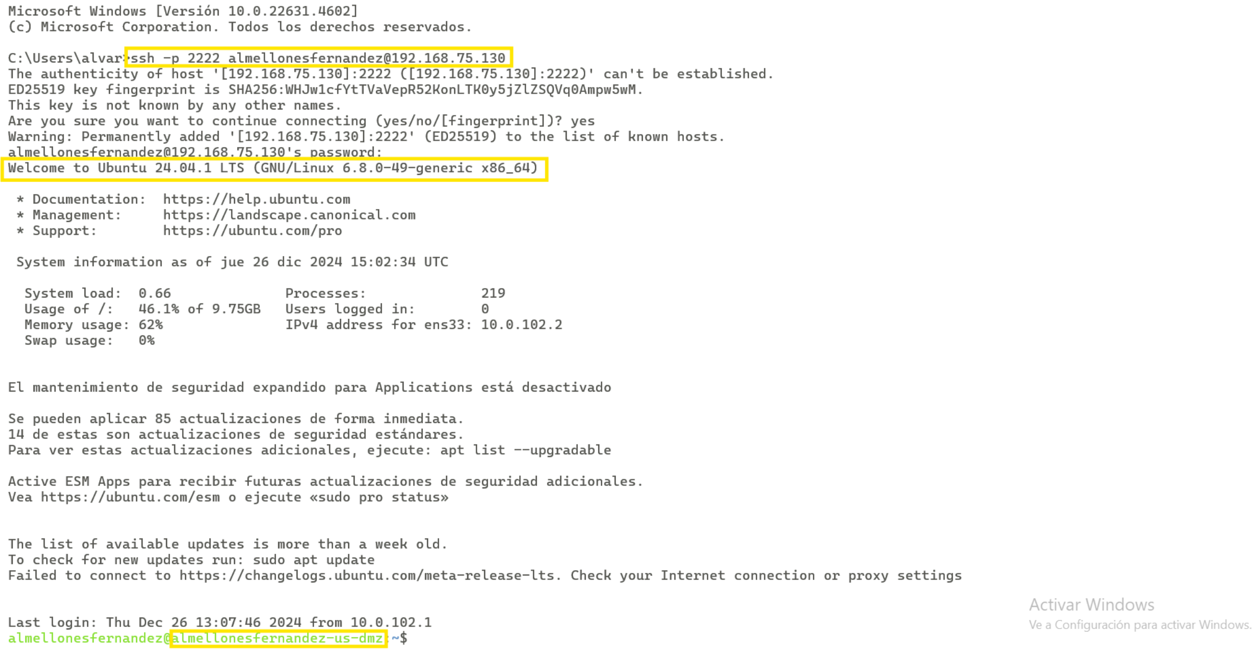


```
root@almellonesfernandez-firewall:~/scripts# ./firewall-almellonesfernandez.sh
Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2:443
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP */ to:1
0.0.102.2:22

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  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WAN */
root@almellonesfernandez-firewall:~/scripts# 
```

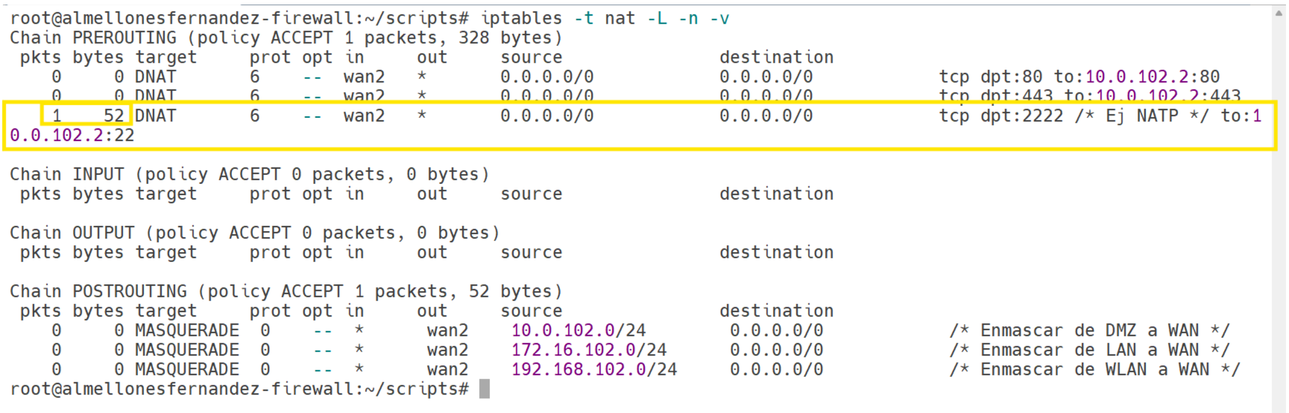


```
root@almellonesfernandez-firewall:~/scripts# iptables -t filter -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 MAC 38:fc:98:0f:99:7
f /* Permitir SSH desde WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
  100  6544 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
```

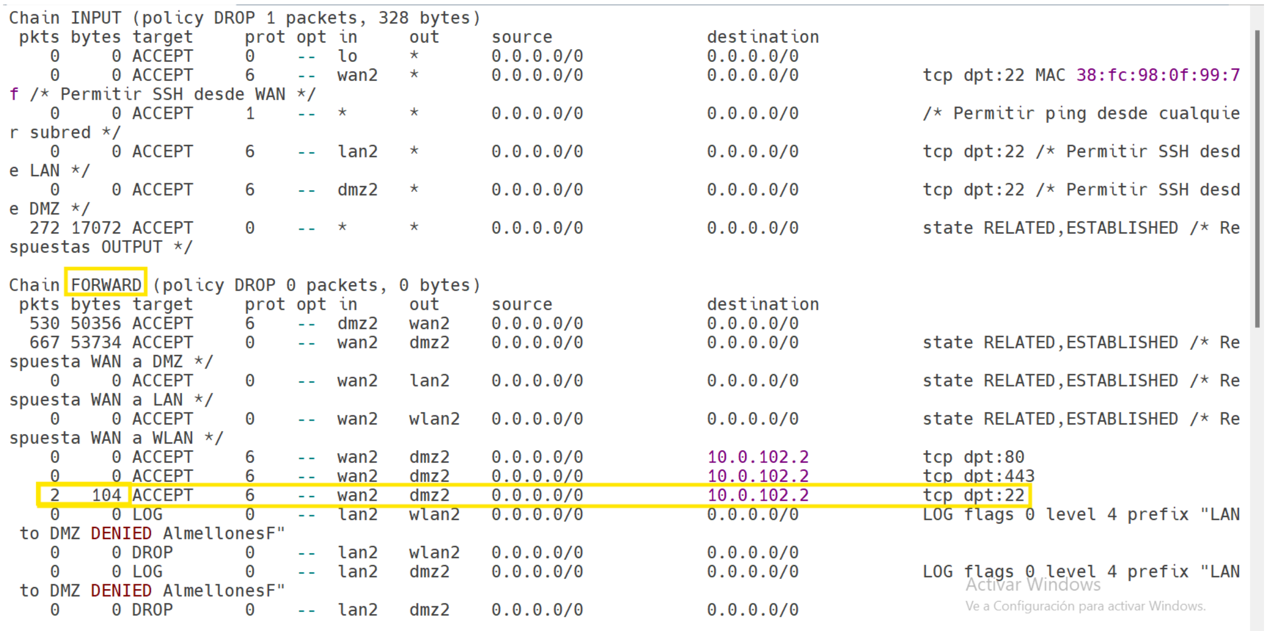
Álvaro Almellones Fernández



```
Microsoft Windows [Versión 10.0.22631.4602]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alvar>ssh -p 2222 almellonesfernandez@192.168.75.130
The authenticity of host '[192.168.75.130]:2222 ([192.168.75.130]:2222)' can't be established.
ED25519 key fingerprint is SHA256:WHJw1cfYtTVaVepR52KonLTK0y5jZlZSQVq0Ampw5wM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.75.130]:2222' (ED25519) to the list of known hosts.
almellonesfernandez@192.168.75.130's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of jue 26 dic 2024 15:02:34 UTC

  System load:  0.66              Processes:             219
  Usage of /:   46.1% of 9.75GB   Users logged in:       0
  Memory usage: 62%               IPv4 address for ens33: 10.0.102.2
  Swap usage:   0%


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 85 actualizaciones de forma inmediata.
14 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


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 your Internet connection or proxy settings


Last login: Thu Dec 26 13:07:46 2024 from 10.0.102.1
almellonesfernandez@almellonesfernandez-us-dmz:~$
```



```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:10.0.102.2:80
    0     0 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 to:10.0.102.2:443
    1    52 DNAT       6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:2222 /* Ej NATP */ to:1
0.0.102.2:22

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 1 packets, 52 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de DMZ a WAN */
    0     0 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de LAN a WAN */
    0     0 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de WLAN a WAN */
root@almellonesfernandez-firewall:~/scripts#
```

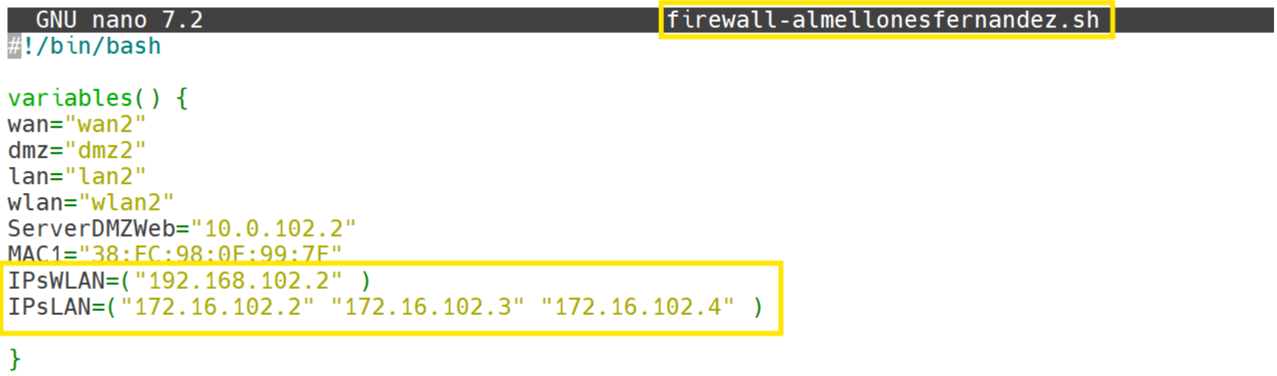


```
Chain INPUT (policy DROP 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     6    --  wan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 MAC 38:fc:98:0f:99:7
f /* Permitir SSH desde WAN */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* Permitir ping desde cualquie
r subred */
    0     0 ACCEPT     6    --  lan2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
  272 17072 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  530 50356 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
  667 53734 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    2   104 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0
```

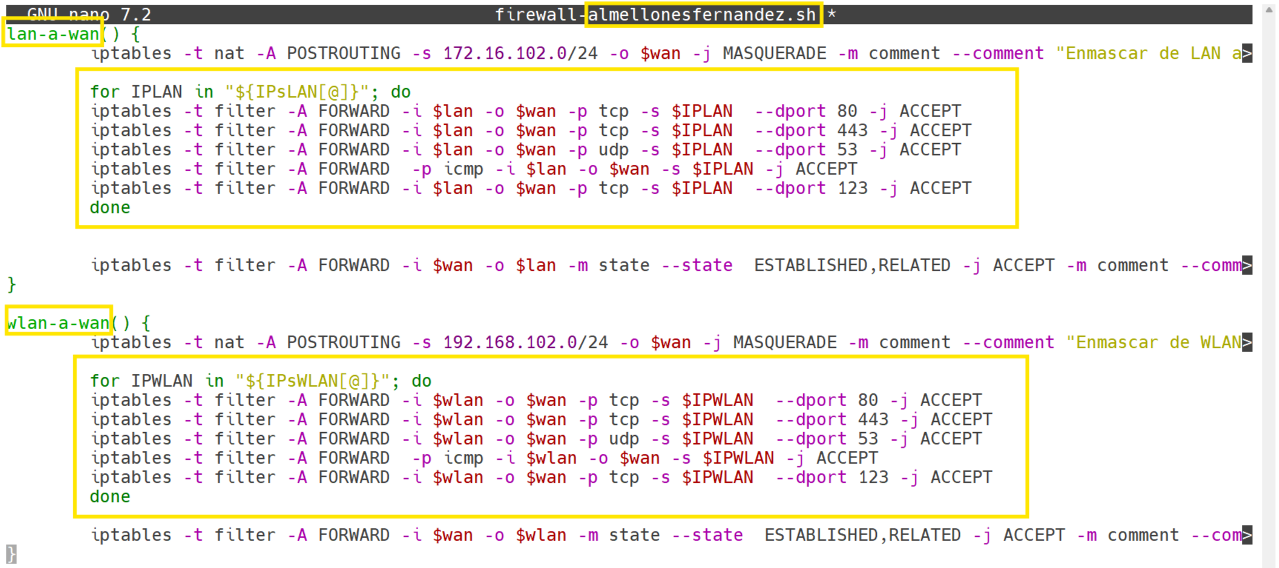
Al empezar la actividad 6 me he dado cuenta de que me estaba funcionando esto porque de dmz a wan lo estaba permitiendo todo,

pero lo que me faltaba era la regla RELATED ESTABLISHED. Lo he modificado y ya me funciona

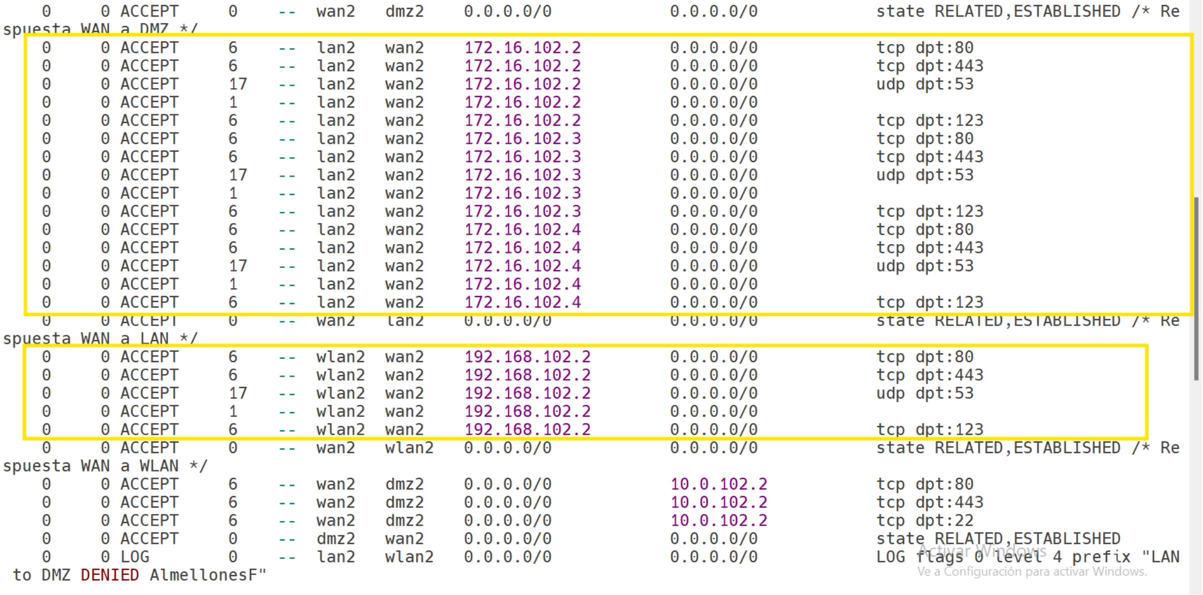
5. **(2 puntos) Filter Forward y NAT desde LAN y WLAN**. Accesos desde la zona LAN/WLAN a Internet (wan) permitidos (hay que usar para cara regla su interfaz correspondiente) y únicamente a los equipos que existan actualmente instalados en las diferentes zonas por su IP (172.16.102.2, 172.16.102.3, 192.168.0.102.2), usando para ello un **único bucle (para las dos interfaces)** que lea un fichero donde estarán escritas esas IP y que habrá que ir añadiendo a lo largo del curso cuando aparezcan más equipos. Únicamente se permitirá.



```
  GNU nano 7.2                    firewall-almellonesfernandez.sh
#!/bin/bash

variables() {
wan="wan2"
dmz="dmz2"
lan="lan2"
wlan="wlan2"
ServerDMZWeb="10.0.102.2"
MAC1="38:FC:98:0F:99:7F"
IPsWLAN=("192.168.102.2" )
IPsLAN=("172.16.102.2" "172.16.102.3" "172.16.102.4" )

}
```



```
  GNU nano 7.2                    firewall-almellonesfernandez.sh *
lan-a-wan() {
        iptables -t nat -A POSTROUTING -s 172.16.102.0/24 -o $wan -j MASQUERADE -m comment --comment "Enmascar de LAN a>

        for IPLAN in "${IPsLAN[@]}"; do
        iptables -t filter -A FORWARD -i $lan -o $wan -p tcp -s $IPLAN  --dport 80 -j ACCEPT
        iptables -t filter -A FORWARD -i $lan -o $wan -p tcp -s $IPLAN  --dport 443 -j ACCEPT
        iptables -t filter -A FORWARD -i $lan -o $wan -p udp -s $IPLAN  --dport 53 -j ACCEPT
        iptables -t filter -A FORWARD  -p icmp -i $lan -o $wan -s $IPLAN -j ACCEPT
        iptables -t filter -A FORWARD -i $lan -o $wan -p tcp -s $IPLAN  --dport 123 -j ACCEPT
        done


        iptables -t filter -A FORWARD -i $wan -o $lan -m state --state  ESTABLISHED,RELATED -j ACCEPT -m comment --comm>
}

wlan-a-wan() {
        iptables -t nat -A POSTROUTING -s 192.168.102.0/24 -o $wan -j MASQUERADE -m comment --comment "Enmascar de WLAN>

        for IPWLAN in "${IPsWLAN[@]}"; do
        iptables -t filter -A FORWARD -i $wlan -o $wan -p tcp -s $IPWLAN  --dport 80 -j ACCEPT
        iptables -t filter -A FORWARD -i $wlan -o $wan -p tcp -s $IPWLAN  --dport 443 -j ACCEPT
        iptables -t filter -A FORWARD -i $wlan -o $wan -p udp -s $IPWLAN  --dport 53 -j ACCEPT
        iptables -t filter -A FORWARD  -p icmp -i $wlan -o $wan -s $IPWLAN -j ACCEPT
        iptables -t filter -A FORWARD -i $wlan -o $wan -p tcp -s $IPWLAN  --dport 123 -j ACCEPT
        done

        iptables -t filter -A FORWARD -i $wan -o $wlan -m state --state  ESTABLISHED,RELATED -j ACCEPT -m comment --com>
}
```

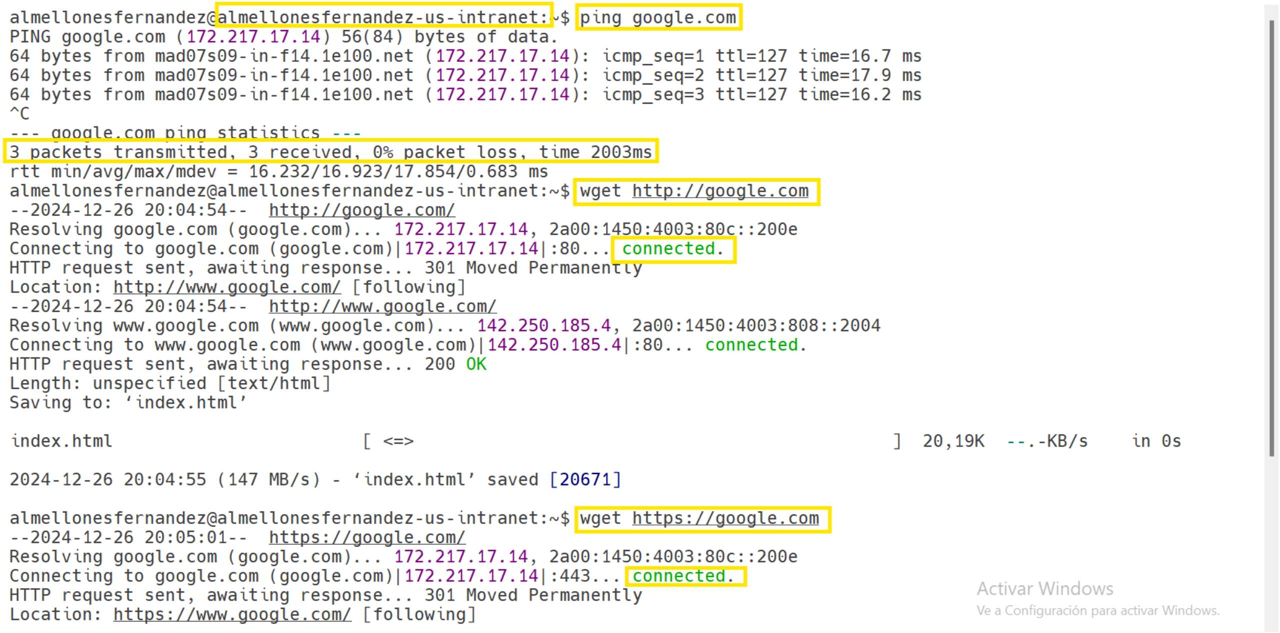


```
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.2         0.0.0.0/0
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:123
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:123
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:123
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:123
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
```

- Actualizarse (apt-get) y visitar páginas web (80 y 443) mediante dns

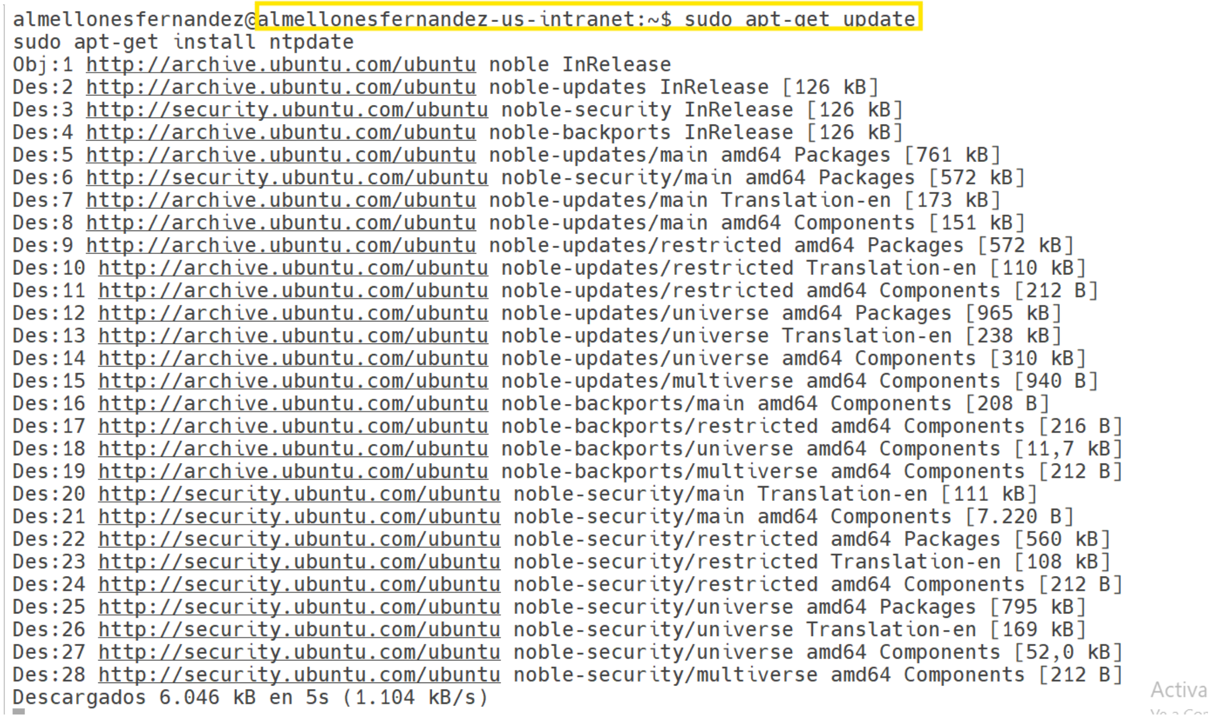
- Hacer ping.

- Actualizar su hora del sistema.



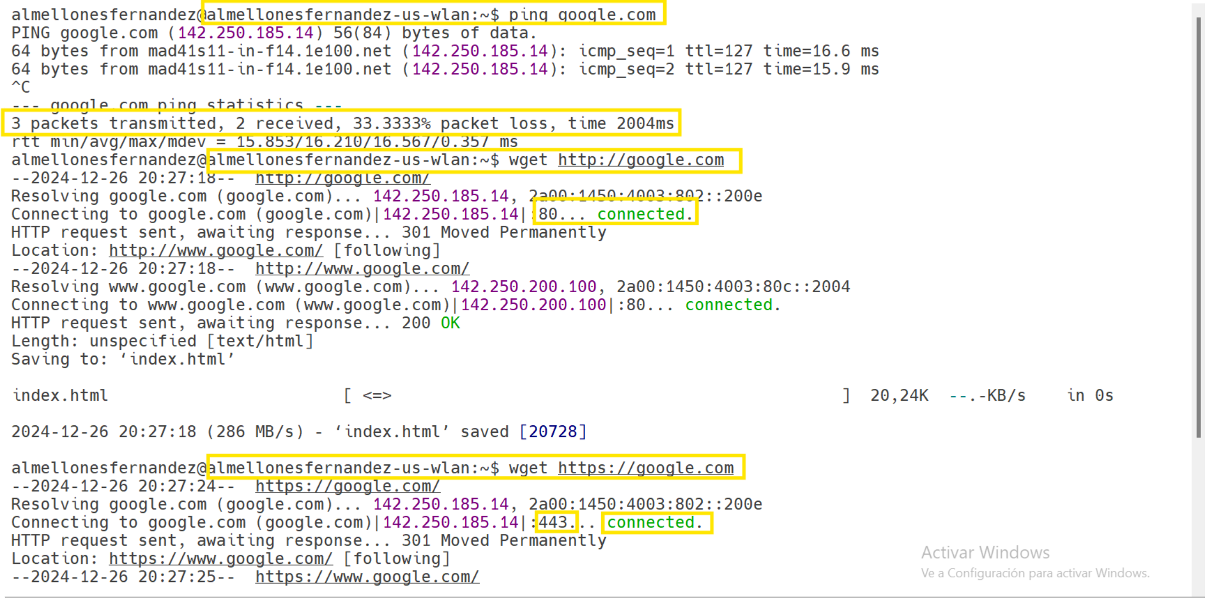
```
almellonesfernandez@almellonesfernandez-us-intranet:~$ ping google.com
PING google.com (172.217.17.14) 56(84) bytes of data.
64 bytes from mad07s09-in-f14.1e100.net (172.217.17.14): icmp_seq=1 ttl=127 time=16.7 ms
64 bytes from mad07s09-in-f14.1e100.net (172.217.17.14): icmp_seq=2 ttl=127 time=17.9 ms
64 bytes from mad07s09-in-f14.1e100.net (172.217.17.14): icmp_seq=3 ttl=127 time=16.2 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 16.232/16.923/17.854/0.683 ms
almellonesfernandez@almellonesfernandez-us-intranet:~$ wget http://google.com
--2024-12-26 20:04:54--  http://google.com/
Resolving google.com (google.com)... 172.217.17.14, 2a00:1450:4003:80c::200e
Connecting to google.com (google.com)|172.217.17.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2024-12-26 20:04:54--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.185.4, 2a00:1450:4003:808::2004
Connecting to www.google.com (www.google.com)|142.250.185.4|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html                        [ <=>                                          ]  20,19K  --.-KB/s    in 0s

2024-12-26 20:04:55 (147 MB/s) - ‘index.html’ saved [20671]

almellonesfernandez@almellonesfernandez-us-intranet:~$ wget https://google.com
--2024-12-26 20:05:01--  https://google.com/
Resolving google.com (google.com)... 172.217.17.14, 2a00:1450:4003:80c::200e
Connecting to google.com (google.com)|172.217.17.14|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
```

Álvaro Almellones Fernández



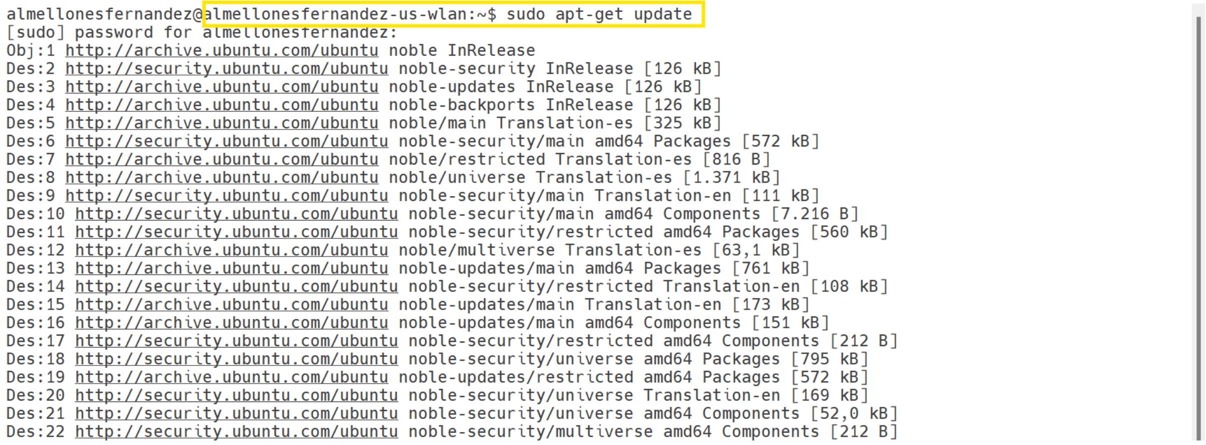
```
almellonesfernandez@almellonesfernandez-us-intranet:~$ sudo apt-get update
sudo apt-get install ntpdate
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [761 kB]
Des:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [572 kB]
Des:7 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [173 kB]
Des:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Des:9 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [572 kB]
Des:10 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [110 kB]
Des:11 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Des:12 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [965 kB]
Des:13 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [238 kB]
Des:14 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [310 kB]
Des:15 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Des:16 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Des:17 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Des:18 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11,7 kB]
Des:19 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Des:20 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [111 kB]
Des:21 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7.220 B]
Des:22 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [560 kB]
Des:23 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [108 kB]
Des:24 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:25 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [795 kB]
Des:26 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [169 kB]
Des:27 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,0 kB]
Des:28 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Descargados 6.046 kB en 5s (1.104 kB/s)
```

Actualizar la fecha lo ejecuta pero no encuentra servidor elegible , creo que me comentaste que alomejor el sistema se actualiza solo, porque si no funcionara no creo que me respondiera el comando

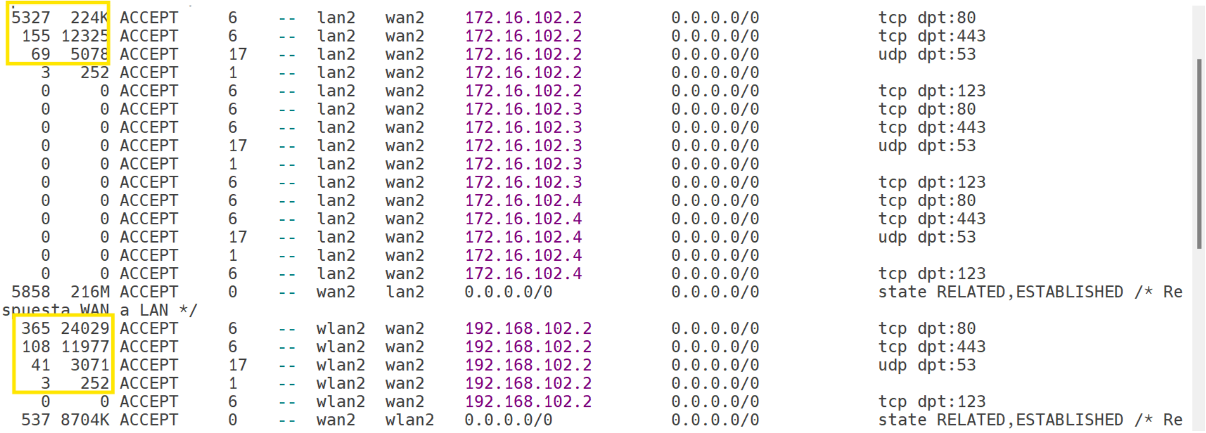


```
almellonesfernandez@almellonesfernandez-us-wlan:~$ ping google.com
PING google.com (142.250.185.14) 56(84) bytes of data.
64 bytes from mad41s11-in-f14.1e100.net (142.250.185.14): icmp_seq=1 ttl=127 time=16.6 ms
64 bytes from mad41s11-in-f14.1e100.net (142.250.185.14): icmp_seq=2 ttl=127 time=15.9 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2004ms
rtt min/avg/max/mdev = 15.853/16.210/16.567/0.357 ms
almellonesfernandez@almellonesfernandez-us-wlan:~$ wget http://google.com
--2024-12-26 20:27:18--  http://google.com/
Resolving google.com (google.com)... 142.250.185.14, 2a00:1450:4003:802::200e
Connecting to google.com (google.com)|142.250.185.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2024-12-26 20:27:18--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.200.100, 2a00:1450:4003:80c::2004
Connecting to www.google.com (www.google.com)|142.250.200.100|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html                        [ <=>                                         ]  20,24K  --.-KB/s    in 0s

2024-12-26 20:27:18 (286 MB/s) - ‘index.html’ saved [20728]

almellonesfernandez@almellonesfernandez-us-wlan:~$ wget https://google.com
--2024-12-26 20:27:24--  https://google.com/
Resolving google.com (google.com)... 142.250.185.14, 2a00:1450:4003:802::200e
Connecting to google.com (google.com)|142.250.185.14|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/ [following]
--2024-12-26 20:27:25--  https://www.google.com/
```

Álvaro Almellones Fernández

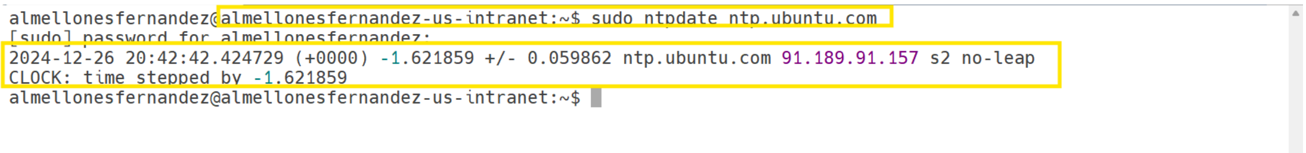


```
almellonesfernandez@almellonesfernandez-us-wlan:~$ sudo apt-get update
[sudo] password for almellonesfernandez:
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:5 http://archive.ubuntu.com/ubuntu noble/main Translation-es [325 kB]
Des:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [572 kB]
Des:7 http://archive.ubuntu.com/ubuntu noble/restricted Translation-es [816 B]
Des:8 http://archive.ubuntu.com/ubuntu noble/universe Translation-es [1.371 kB]
Des:9 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [111 kB]
Des:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7.216 B]
Des:11 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [560 kB]
Des:12 http://archive.ubuntu.com/ubuntu noble/multiverse Translation-es [63,1 kB]
Des:13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [761 kB]
Des:14 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [108 kB]
Des:15 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [173 kB]
Des:16 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Des:17 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:18 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [795 kB]
Des:19 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [572 kB]
Des:20 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [169 kB]
Des:21 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,0 kB]
Des:22 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
```

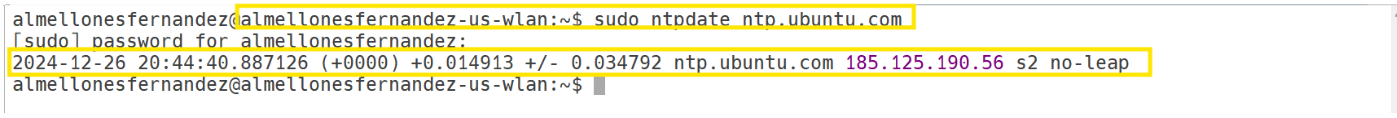


```
5327  224K ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:80
 155 12325 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:443
  69  5078 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:53
   3   252 ACCEPT     1    --  lan2   wan2    172.16.102.2         0.0.0.0/0
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.2         0.0.0.0/0            tcp dpt:123
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
   0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
   0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:123
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
   0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
   0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
   0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:123
5858  216M ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
 365 24029 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
 108 11977 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
  41  3071 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
   3   252 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
   0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:123
 537 8704K ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
```

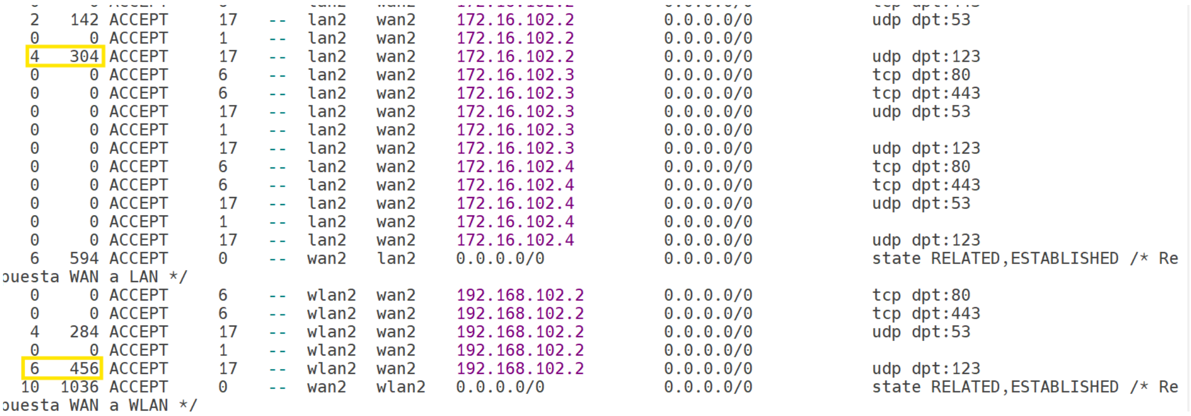
Solo ha aumentado en las ips de los Ubuntu Server porque son las máquinas que he probado, pero deben de funcionar todas. Te voy a mostrar a parte como se actualiza las horas ya que me he equivocado y le he puesto tcp en vez de udp uno me actualizaba la hora



```
almellonesfernandez@almellonesfernandez-us-intranet:~$ sudo ntpdate ntp.ubuntu.com
[sudo] password for almellonesfernandez:
2024-12-26 20:42:42.424729 (+0000) -1.621859 +/- 0.059862 ntp.ubuntu.com 91.189.91.157 s2 no-leap
CLOCK: time stepped by -1.621859
almellonesfernandez@almellonesfernandez-us-intranet:~$
```



```
almellonesfernandez@almellonesfernandez-us-wlan:~$ sudo ntpdate ntp.ubuntu.com
[sudo] password for almellonesfernandez:
2024-12-26 20:44:40.887126 (+0000) +0.014913 +/- 0.034792 ntp.ubuntu.com 185.125.190.56 s2 no-leap
almellonesfernandez@almellonesfernandez-us-wlan:~$
```



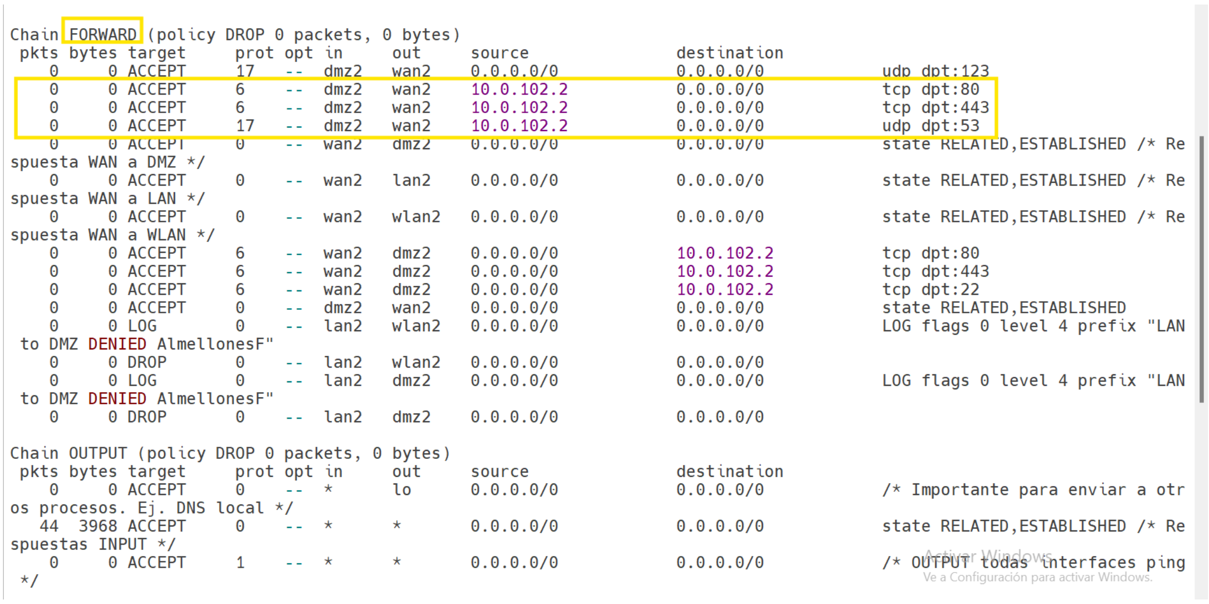
```
    2   142 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.2         0.0.0.0/0
    4   304 ACCEPT     17   --  lan2   wan2    172.16.102.2         0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.3         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.3         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.3         0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  lan2   wan2    172.16.102.4         0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  lan2   wan2    172.16.102.4         0.0.0.0/0
    0     0 ACCEPT     17   --  lan2   wan2    172.16.102.4         0.0.0.0/0            udp dpt:123
    6   594 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
puesta WAN a LAN */
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  wlan2  wan2    192.168.102.2        0.0.0.0/0            tcp dpt:443
    4   284 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     1    --  wlan2  wan2    192.168.102.2        0.0.0.0/0
    6   456 ACCEPT     17   --  wlan2  wan2    192.168.102.2        0.0.0.0/0            udp dpt:123
   10  1036 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
puesta WAN a WLAN */
```

Ahora si aumenta el contador , en la imagen de los contadores anteriores estaba a 0 y ahora aumente el número de las dos reglas

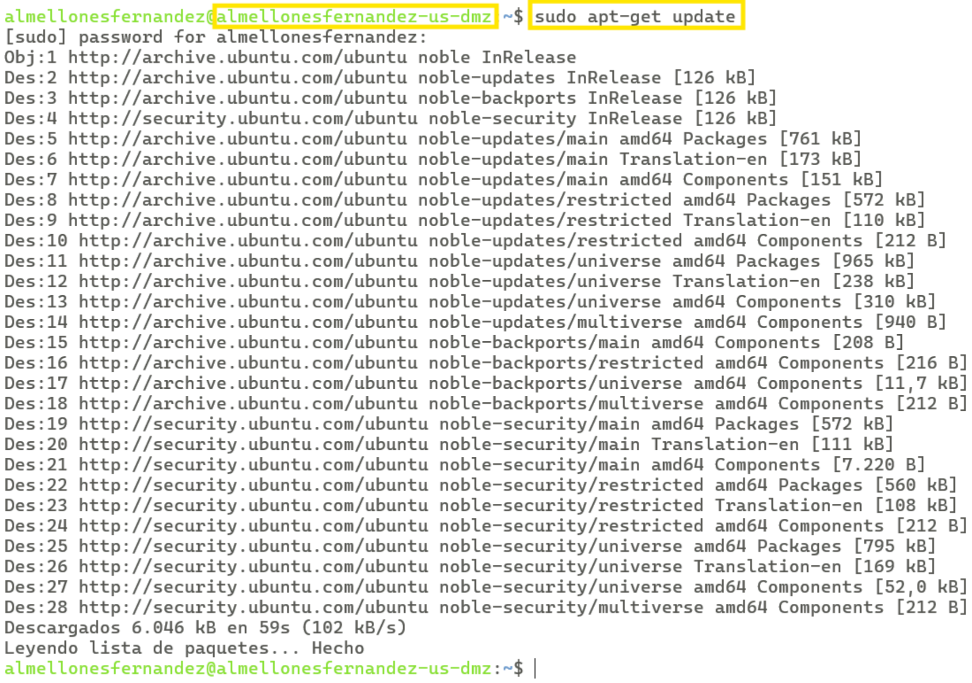
6. **Filter Forward y NAT desde DMZ** Accesos desde la zona DMZ a Internet (wan) permitidos:

- **(1 punto)** Actualizarse (apt-get) y visitar páginas web (80 y 443) mediante dns,

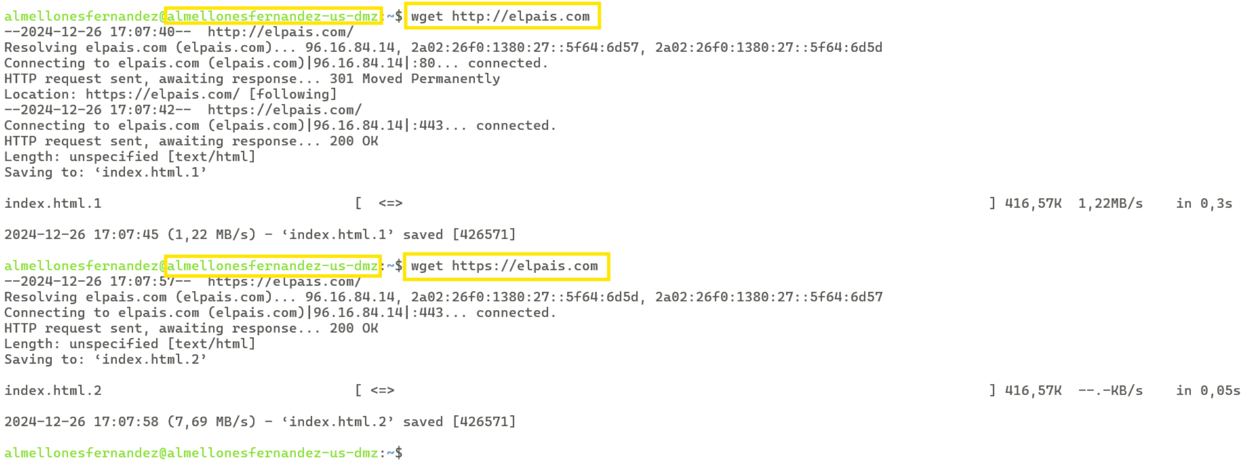
exclusivamente al único equipo que hay actualmente en dicha zona.



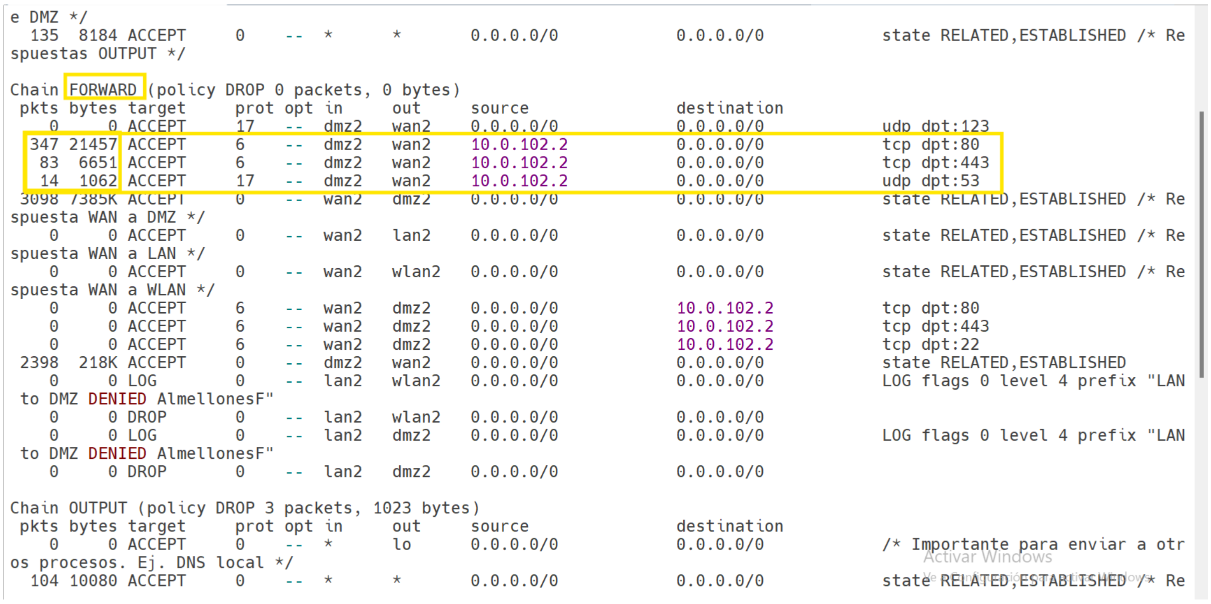
```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     17   --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  dmz2   wan2    10.0.102.2           0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   44  3968 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
```



```
almellonesfernandez@almellonesfernandez-us-dmz:~$ sudo apt-get update
[sudo] password for almellonesfernandez:
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [761 kB]
Des:6 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [173 kB]
Des:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Des:8 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [572 kB]
Des:9 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [110 kB]
Des:10 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Des:11 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [965 kB]
Des:12 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [238 kB]
Des:13 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [310 kB]
Des:14 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Des:15 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Des:16 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Des:17 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11,7 kB]
Des:18 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Des:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [572 kB]
Des:20 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [111 kB]
Des:21 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7.220 B]
Des:22 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [560 kB]
Des:23 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [108 kB]
Des:24 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:25 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [795 kB]
Des:26 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [169 kB]
Des:27 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,0 kB]
Des:28 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Descargados 6.046 kB en 59s (102 kB/s)
Leyendo lista de paquetes... Hecho
almellonesfernandez@almellonesfernandez-us-dmz:~$ |
```

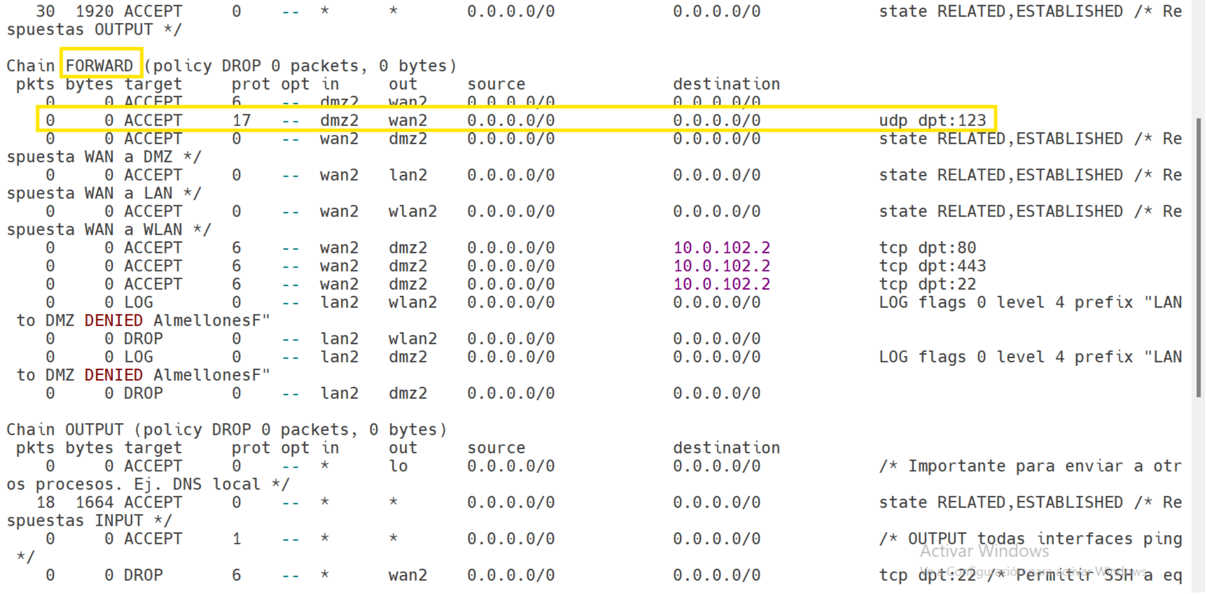


```
almellonesfernandez@almellonesfernandez-us-dmz:~$ wget http://elpais.com
--2024-12-26 17:07:40--  http://elpais.com/
Resolving elpais.com (elpais.com)... 96.16.84.14, 2a02:26f0:1380:27::5f64:6d57, 2a02:26f0:1380:27::5f64:6d5d
Connecting to elpais.com (elpais.com)|96.16.84.14|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://elpais.com/ [following]
--2024-12-26 17:07:42--  https://elpais.com/
Connecting to elpais.com (elpais.com)|96.16.84.14|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.1’

index.html.1                               [  <=>                                                                    ] 416,57K  1,22MB/s    in 0,3s

2024-12-26 17:07:45 (1,22 MB/s) - ‘index.html.1’ saved [426571]

almellonesfernandez@almellonesfernandez-us-dmz:~$ wget https://elpais.com
--2024-12-26 17:07:57--  https://elpais.com/
Resolving elpais.com (elpais.com)... 96.16.84.14, 2a02:26f0:1380:27::5f64:6d5d, 2a02:26f0:1380:27::5f64:6d57
Connecting to elpais.com (elpais.com)|96.16.84.14|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.2’

index.html.2                               [ <=>                                                                     ] 416,57K  --.-KB/s    in 0,05s

2024-12-26 17:07:58 (7,69 MB/s) - ‘index.html.2’ saved [426571]

almellonesfernandez@almellonesfernandez-us-dmz:~$
```

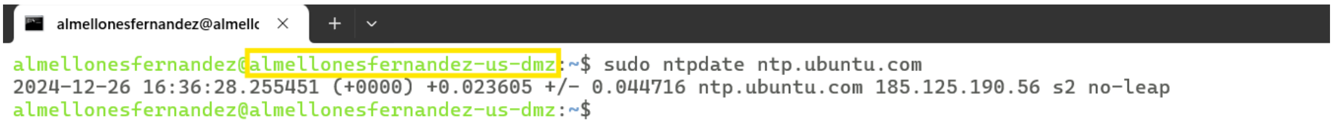


```
e DMZ */
  135  8184 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     17   --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123
  347 21457 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:80
   83  6651 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:443
   14  1062 ACCEPT     17   --  dmz2   wan2    10.0.102.2           0.0.0.0/0            udp dpt:53
 3098 7385K ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
 2398  218K ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 3 packets, 1023 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
  104 10080 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
```

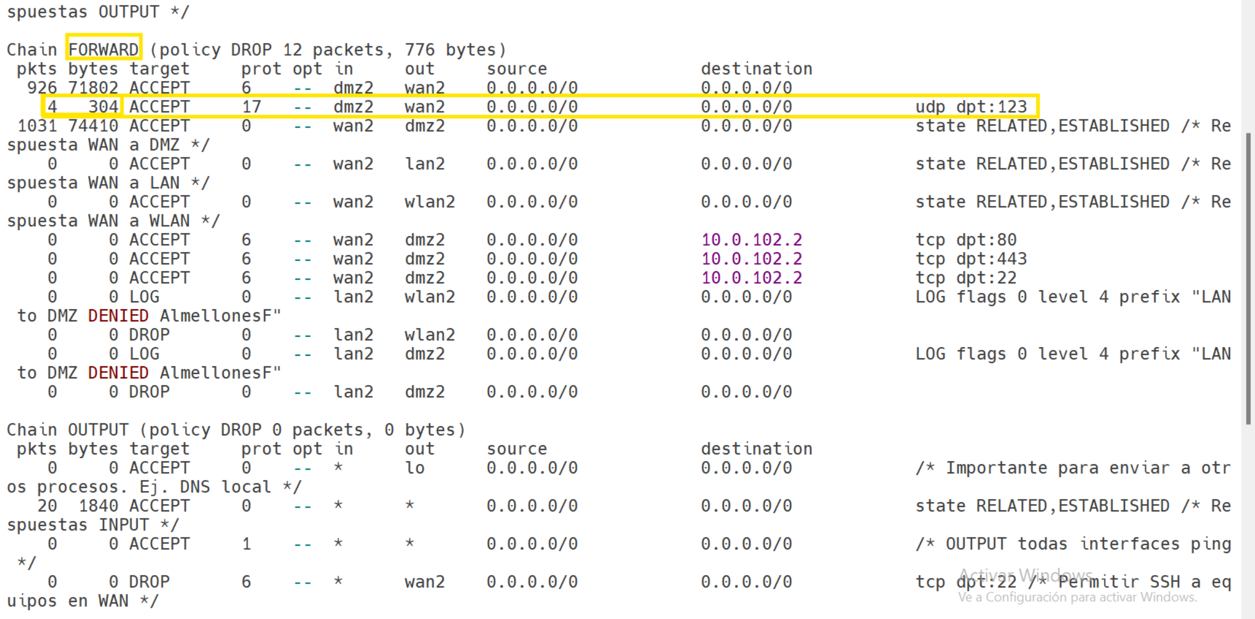
- **(0,5 puntos)** Actualizar la hora del sistema operativo.



```
   30  1920 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     17   --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   18  1664 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
```

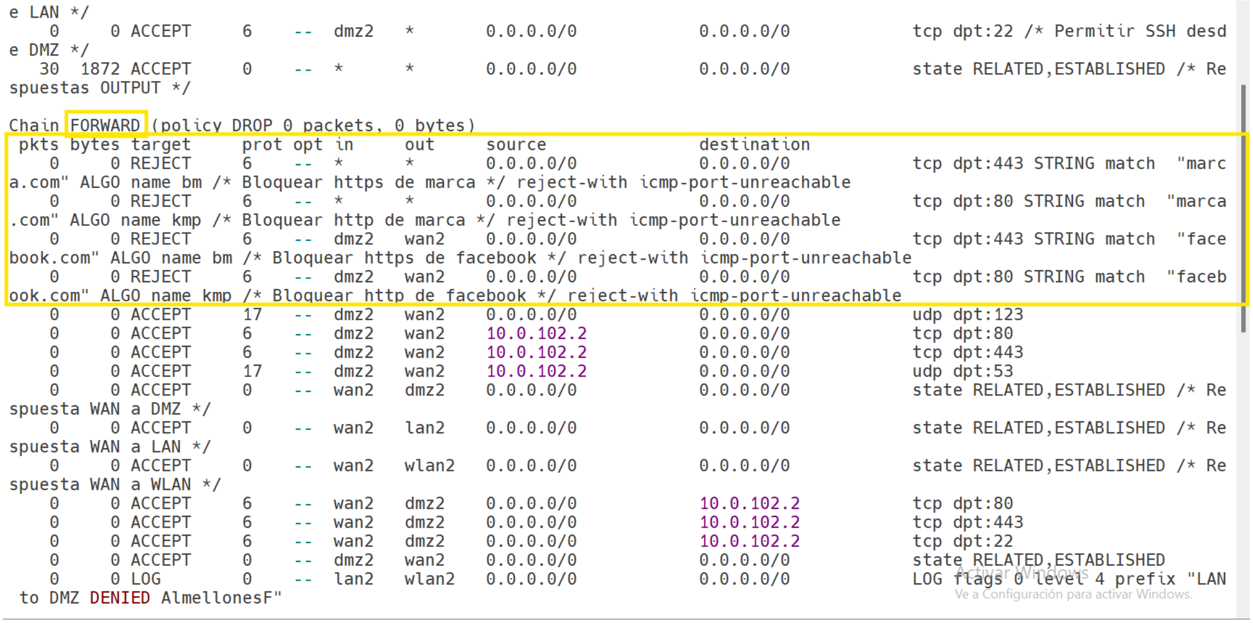


```
almellonesfernandez@almellonesfernandez-us-dmz:~$ sudo ntpdate ntp.ubuntu.com
2024-12-26 16:36:28.255451 (+0000) +0.023605 +/- 0.044716 ntp.ubuntu.com 185.125.190.56 s2 no-leap
almellonesfernandez@almellonesfernandez-us-dmz:~$
```



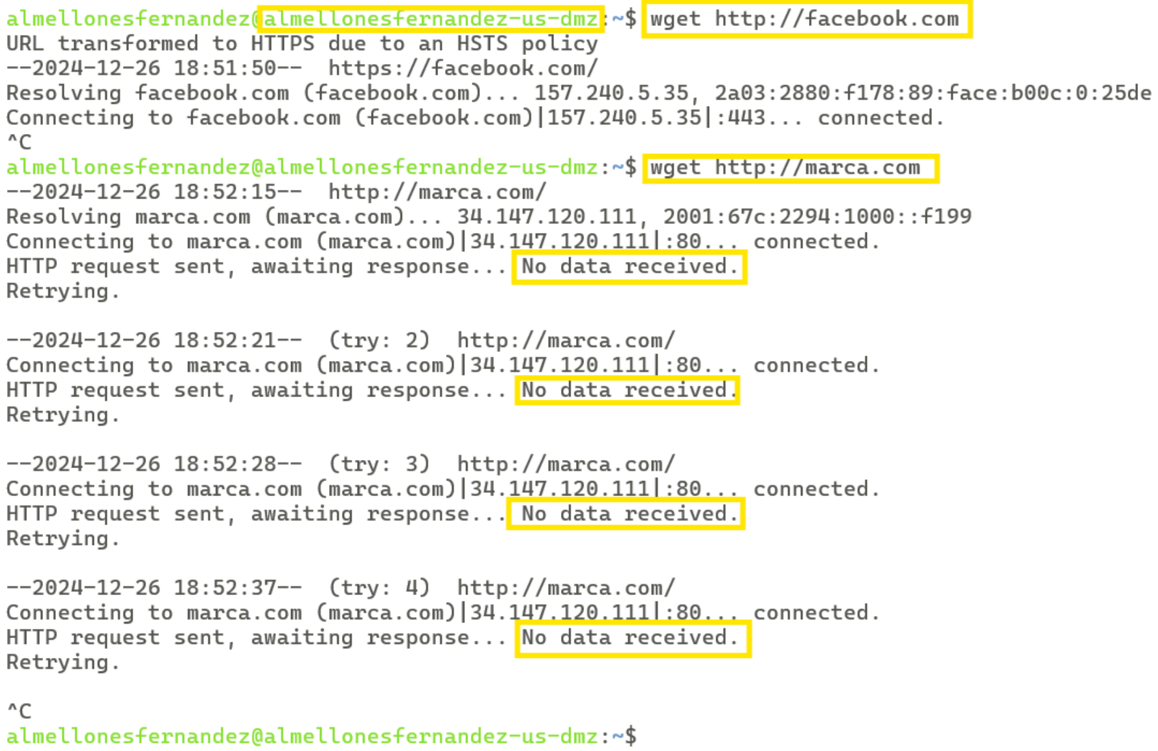
```
spuestas OUTPUT */

Chain FORWARD (policy DROP 12 packets, 776 bytes)
 pkts bytes target     prot opt in     out     source               destination
  926 71802 ACCEPT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0
    4   304 ACCEPT     17   --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123
 1031 74410 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0
    0     0 LOG        0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
    0     0 DROP       0    --  lan2   dmz2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      lo      0.0.0.0/0            0.0.0.0/0            /* Importante para enviar a otr
os procesos. Ej. DNS local */
   20  1840 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas INPUT */
    0     0 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0            /* OUTPUT todas interfaces ping
 */
    0     0 DROP       6    --  *      wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH a eq
uipos en WAN */
```

- **(1 punto)** No se permitirá la conexión a https://facebook.com , https://www.marca.com.

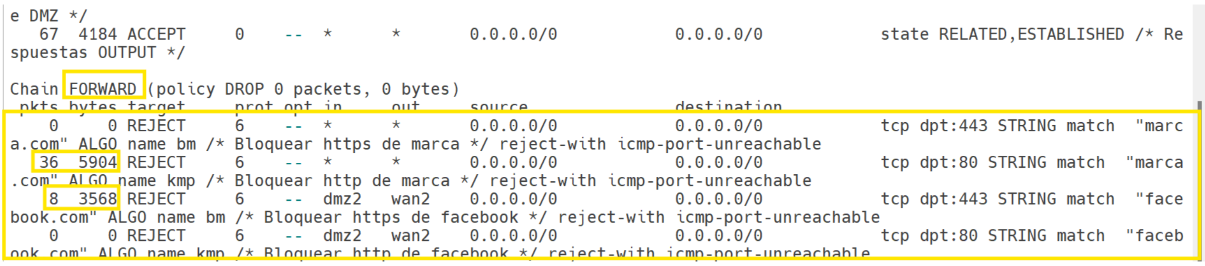


```
e LAN */
    0     0 ACCEPT     6    --  dmz2   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* Permitir SSH desd
e DMZ */
   30  1872 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 STRING match  "marc
a.com" ALGO name bm /* Bloquear https de marca */ reject-with icmp-port-unreachable
    0     0 REJECT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 STRING match  "marca
.com" ALGO name kmp /* Bloquear http de marca */ reject-with icmp-port-unreachable
    0     0 REJECT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443 STRING match  "face
book.com" ALGO name bm /* Bloquear https de facebook */ reject-with icmp-port-unreachable
    0     0 REJECT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:80 STRING match  "faceb
ook.com" ALGO name kmp /* Bloquear http de facebook */ reject-with icmp-port-unreachable
    0     0 ACCEPT     17   --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            udp dpt:123
    0     0 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  dmz2   wan2    10.0.102.2           0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     17   --  dmz2   wan2    10.0.102.2           0.0.0.0/0            udp dpt:53
    0     0 ACCEPT     0    --  wan2   dmz2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a DMZ */
    0     0 ACCEPT     0    --  wan2   lan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a LAN */
    0     0 ACCEPT     0    --  wan2   wlan2   0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuesta WAN a WLAN */
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:80
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:443
    0     0 ACCEPT     6    --  wan2   dmz2    0.0.0.0/0            10.0.102.2           tcp dpt:22
    0     0 ACCEPT     0    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 LOG        0    --  lan2   wlan2   0.0.0.0/0            0.0.0.0/0            LOG flags 0 level 4 prefix "LAN
 to DMZ DENIED AlmellonesF"
```

Álvaro Almellones Fernández



```
almellonesfernandez@almellonesfernandez-us-dmz:~$ wget http://facebook.com
URL transformed to HTTPS due to an HSTS policy
--2024-12-26 18:51:50--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.5.35, 2a03:2880:f178:89:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.5.35|:443... connected.
^C
almellonesfernandez@almellonesfernandez-us-dmz:~$ wget http://marca.com
--2024-12-26 18:52:15--  http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

--2024-12-26 18:52:21--  (try: 2)  http://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

--2024-12-26 18:52:28--  (try: 3)  http://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

--2024-12-26 18:52:37--  (try: 4)  http://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... No data received.
Retrying.

^C
almellonesfernandez@almellonesfernandez-us-dmz:~$
```



```
e DMZ */
   67  4184 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED /* Re
spuestas OUTPUT */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 STRING match  "marc
a.com" ALGO name bm /* Bloquear https de marca */ reject-with icmp-port-unreachable
   36  5904 REJECT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 STRING match  "marca
.com" ALGO name kmp /* Bloquear http de marca */ reject-with icmp-port-unreachable
    8  3568 REJECT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:443 STRING match  "face
book.com" ALGO name bm /* Bloquear https de facebook */ reject-with icmp-port-unreachable
    0     0 REJECT     6    --  dmz2   wan2    0.0.0.0/0            0.0.0.0/0            tcp dpt:80 STRING match  "faceb
ook.com" ALGO name kmp /* Bloquear http de facebook */ reject-with icmp-port-unreachable
```

CRITERIOS DE EVALUACIÓN	
4.a	Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
7.a	Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.