Álvaro Almellones Fernández

PRÁCTICA 5 (almellonesfernandez-practica5) – UD 4. U.D.4. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). SEGURIDAD PERIMETRAL. IPTABLES.

SEGMENTACIÓN DE RED FÍSICA Y ENRUTAMIENTO ENTRE REDES. ZONA DMZ. PRACTICA 5.1

1. **(2 puntos) (EQUIPO FIREWALL)** Montaje de un servidor Ubuntu Server (conexión únicamente por SSHD y conexión por key pública), con cuatro tarjetas de red con las siguientes características:

○ Nombre del servidor: firewall-XXxx. Para simplificar XXxx puede ser covadonga, zambrana, alvaro, etc.

```
5. 192.168.75.130
root@almellonesfernandez-firewall:/etc/netplan# cat /etc/hostname
almellonesfernandez-firewall
root@almellonesfernandez-firewall:/etc/netplan#
```

○ Nombre de interfaz para **usar en los scripts** (wan?, lan?, wlan? y dmz? – donde ? es el número de clase, previamente informado al alumno en clase (/etc/udev/rules.d/70-persistent-net.rules).

```
5. 192.168.75.130
root@almellonesfernandez-firewall:/etc/netplan# cat /etc/udev/rules.d/70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:0c:29:c3:df:c9", NAME="wan2"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:0c:29:c3:df:e7", NAME="lan2"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:0c:29:c3:df:d3", NAME="wlan2"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:0c:29:c3:df:dd", NAME="dmz2"
root@almellonesfernandez-firewall:/etc/netplan#
```

○ Las Ip ((ifconfig, ping, dmesg, fichero de configuración)/Redes del firewall-XXxx, serán las siguientes:

▪ (Modo Bridge) Red WAN, red roja o Internet, por DHCP o IP fija si se encuentra usted en casa (tracepath, route)

▪ (Red 1) Red DMZ, red naranja, ip fija 10.0.10?.1/24. (Red Privada Tipo A)

▪ (Red 2) Red Intranet, red verde o zona lan. ip fija 172.16.10?.1/24. (Red Privada Tipo B)

▪ (Red 3) Red WLAN, red azul, 192.168.10?.1/24. (Red Privada Tipo C).

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:/etc/netplan# cat 50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    wan2:
      dhcp4: true  # DHCP para la red WAN (roja)
    lan2:
      dhcp4: no
      addresses:
        - 172.16.102.1/24  # Red LAN (verde)
    wlan2:
      dhcp4: no
      addresses:
        - 192.168.102.1/24  # Red WLAN (azul)
    dmz2:
      dhcp4: no
      addresses:
        - 10.0.102.1/24  # Red DMZ (naranja)

root@almellonesfernandez-firewall:/etc/netplan#
```

```
root@almellonesfernandez-firewall:/etc/netplan# ifconfig
dmz2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.102.1  netmask 255.255.255.0  broadcast 10.0.102.255
        inet6 fe80::20c:29ff:fec3:dfdd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:dd  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1006 (1.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.102.1  netmask 255.255.255.0  broadcast 172.16.102.255
        inet6 fe80::20c:29ff:fec3:dfe7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:e7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1006 (1.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 84  bytes 6352 (6.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 6352 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.130  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::20c:29ff:fec3:dfc9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:c9  txqueuelen 1000  (Ethernet)
```



```
        RX packets 466  bytes 45176 (45.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 349  bytes 44816 (44.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.102.1  netmask 255.255.255.0  broadcast 192.168.102.255
        inet6 fe80::20c:29ff:fec3:dfd3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c3:df:d3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1006 (1.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@almellonesfernandez-firewall:/etc/netplan#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:/etc/netplan# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 wan2
10.0.102.0      0.0.0.0         255.255.255.0   U     0      0        0 dmz2
172.16.102.0    0.0.0.0         255.255.255.0   U     0      0        0 lan2
192.168.75.0    0.0.0.0         255.255.255.0   U     100    0        0 wan2
_gateway        0.0.0.0         255.255.255.255 UH    100    0        0 wan2
192.168.102.0   0.0.0.0         255.255.255.0   U     0      0        0 wlan2
root@almellonesfernandez-firewall:/etc/netplan#
```

2. **(EQUIPOS DE LAS SUBREDES)**

○ **(2 puntos)** Montaje de **tres** máquinas virtuales Ubuntu Server (uno por cada red, 512 MB de RAM), con servicio SSHD instalado con autentificación por cifrado asimétrico, net-tools instalados, actualizadas, en redes privadas (LAN segment de VM) con las siguientes IP y con los siguientes servicios adicionales instalados.

▪ Red 1: nombre (dmz-US-Xxxx), IP (10.0.10?.2/24), Gateway (10.0.10?.1) (ifconfig, route, fichero de configuración)

○ Servidor apache2 escuchando en el puerto 80, con php instalado.

○ Página web personalizada dónde aparezca nombre y apellidos del alumno, número de clase, y que aparezca la IP del servidor (obtenga del S.O., nada fijo), y la IP del cliente que solicita la página web.

```
almellonesfernandez@almellonesfernandez-us-dmz:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.102.2  netmask 255.255.255.0  broadcast 10.0.102.255
        inet6 fe80::20c:29ff:fe41:aa51  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:41:aa:51  txqueuelen 1000  (Ethernet)
        RX packets 26452  bytes 18522179 (18.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16387  bytes 1764853 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 142  bytes 13477 (13.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 142  bytes 13477 (13.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

almellonesfernandez@almellonesfernandez-us-dmz:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.102.1               ether   00:0c:29:c3:df:dd   C                     ens33
almellonesfernandez@almellonesfernandez-us-dmz:~$
```

He encontrado el comando arp -n que te muestra la gateway de este server y la mac de la tarjeta del gateway

```
almellonesfernandez@almellonesfernandez-us-dmz:~$ netstat -putan
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0     52 10.0.102.2:22           10.0.102.1:32790        ESTABLISHED -
udp        0      0 127.0.0.54:53           0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
almellonesfernandez@almellonesfernandez-us-dmz:~$ sudo nano /var/www/html/index.php
```

Álvaro Almellones Fernández

```
  GNU nano 7.2                                  /var/www/html/index.php
<?php
$server_ip = $_SERVER['SERVER_ADDR'];
$client_ip = $_SERVER['REMOTE_ADDR'];
echo "<h1>Nombre: Alvaro </h1>";
echo "<h1>Apellidos: Almellones Fernandez</h1>";
echo "<h1>Clase: 2</h1>";
echo "<h1>IP del Servidor: $server_ip</h1>";
echo "<h1>IP del Cliente: $client_ip</h1>";
?>

                                              [ Read 9 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

▪ Red 2: nombre (intranet-US-Xxxx), IP (172.16.10?.2/24), Gateway (172.16.10?.1).

(ifconfig, route, fichero de configuración)

- Servidor apache2 escuchando en el puerto 80, con php instalado.
- Página web personalizada dónde aparezca nombre y apellidos del alumno, número de clase, que aparezca la IP del servidor (obtenga del S.O., nada fijo), y la IP del cliente que solicita la página web.
- Servidor mysql-server instalado y configurado para poder acceder desde la red, no sólo desde localhost.
- Servidor vsftpd instalado.

```
root@almellonesfernandez-us-intranet:/# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.102.2  netmask 255.255.255.0  broadcast 172.16.102.255
        inet6 fe80::20c:29ff:fe9c:d0e9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:9c:d0:e9  txqueuelen 1000  (Ethernet)
        RX packets 55083  bytes 50037611 (50.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26476  bytes 2899083 (2.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1074  bytes 84235 (84.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1074  bytes 84235 (84.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@almellonesfernandez-us-intranet:/# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.102.1             ether   00:0c:29:c3:df:e7   C                     ens33
root@almellonesfernandez-us-intranet:/#
```

```
root@almellonesfernandez-us-intranet:/# netstat -putan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      11036/mysqld
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      728/systemd-resolve
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      11036/mysqld
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      728/systemd-resolve
tcp6       0      0 :::21                   :::*                    LISTEN      10154/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0      0 :::80                   :::*                    LISTEN      9888/apache2
tcp6       0     52 172.16.102.2:22         172.16.102.1:60144      ESTABLISHED 2425/sshd: almellon
udp        0      0 127.0.0.54:53           0.0.0.0:*                           728/systemd-resolve
udp        0      0 127.0.0.53:53           0.0.0.0:*                           728/systemd-resolve
root@almellonesfernandez-us-intranet:/# nano /var/www/html/index.php
```

Álvaro Almellones Fernández

```
  GNU nano 7.2                                  /var/www/html/index.php
<?php
$server_ip = $_SERVER['SERVER_ADDR'];
$client_ip = $_SERVER['REMOTE_ADDR'];
echo "<h1>Nombre: Alvaro</h1>";
echo "<h1>Apellidos: Almellones Fernandez</h1>";
echo "<h1>Clase: 2</h1>";
echo "<h1>IP del Servidor: $server_ip</h1>";
echo "<h1>IP del Cliente: $client_ip</h1>";
?>

                                              [ Read 9 lines ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

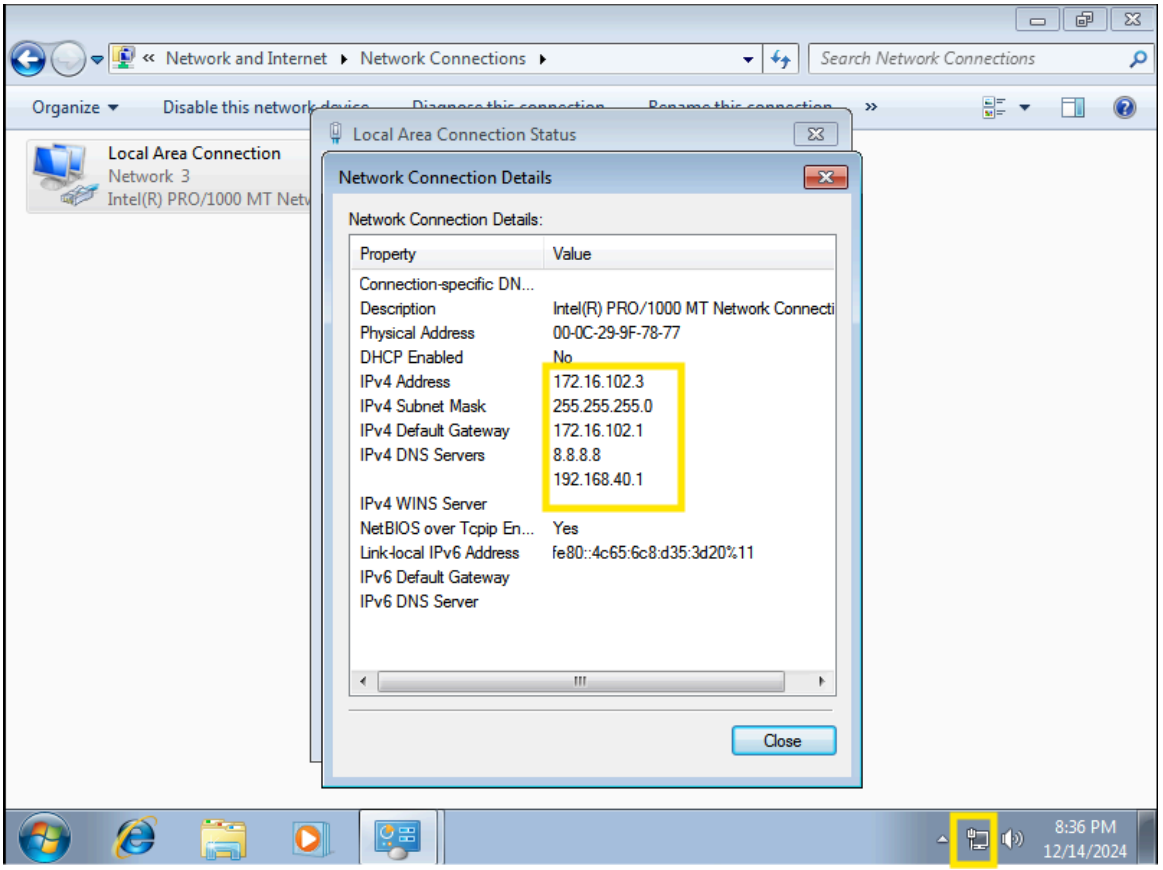
▪ Red 3: nombre (wlan-US-Xxxx), IP (192.1680.0.10?.2/24), Gateway (192.168.10?.1).

(ifconfig, route, fichero de configuración)

```
almellonesfernandez@almellonesfernandez-us-wlan:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.102.2  netmask 255.255.255.0  broadcast 192.168.102.255
        inet6 fe80::20c:29ff:fe21:9bc2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:21:9b:c2  txqueuelen 1000  (Ethernet)
        RX packets 5576  bytes 2792432 (2.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5416  bytes 524597 (524.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1041  bytes 80724 (80.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1041  bytes 80724 (80.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

almellonesfernandez@almellonesfernandez-us-wlan:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.102.1            ether   00:0c:29:c3:df:d3   C                     ens33
almellonesfernandez@almellonesfernandez-us-wlan:~$
```

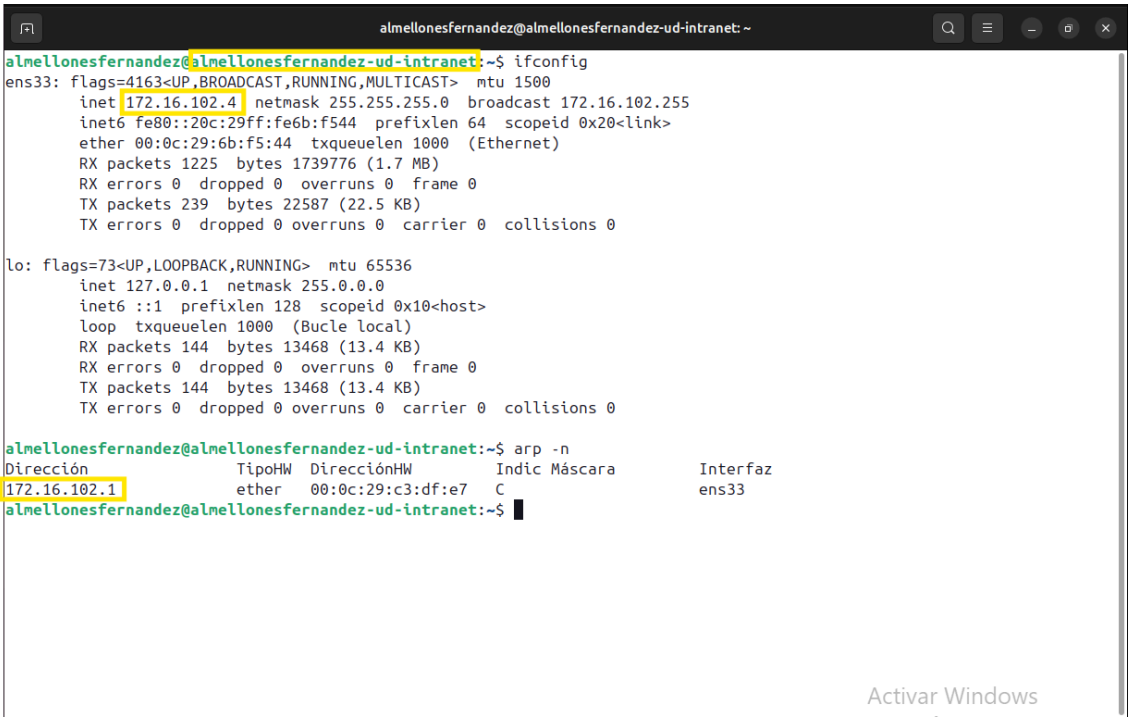
○ **(1 punto)** Montaje de una máquina virtual Microsoft Windows en la red 2 (intranet), con nombre (intranet-MS-XXxx), IP fija (172.16.10?.3/24), Gateway (172.16.10?.1). (ifconfig, route, traceroute)

Álvaro Almellones Fernández



Me sale abajo a la derecha que ya tengo internet porque estoy haciendo las capturas de comprobación una vez realizada toda la práctica entera

○ **(1 punto)** Montaje de una máquina virtual Ubuntu Desktop en la red 2 (intranet), con nombre (intranet-UD-XXxx), IP fija (172.16.10?.4/24), Gateway (172.16.10?.1).



Álvaro Almellones Fernández

3. **(1 punto)** Comprobaciones de que se puede acceder desde el cortafuegos a todas las máquinas de cada subred, mediante ping y ssh, y wget/curl a los servidores webs (red dmz, red intranet).

```
root@almellonesfernandez-firewall:~# 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=67.0 ms
64 bytes from 10.0.102.2: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 10.0.102.2: icmp_seq=3 ttl=64 time=1.17 ms
^C
--- 10.0.102.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.174/23.179/67.009/30.992 ms
root@almellonesfernandez-firewall:~# 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=29.5 ms
64 bytes from 172.16.102.2: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 172.16.102.2: icmp_seq=3 ttl=64 time=1.20 ms
^C
--- 172.16.102.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.010/10.574/29.513/13.391 ms
root@almellonesfernandez-firewall:~# 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=108 ms
64 bytes from 192.168.102.2: icmp_seq=2 ttl=64 time=22.5 ms
64 bytes from 192.168.102.2: icmp_seq=3 ttl=64 time=1.24 ms
^C
--- 192.168.102.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.237/43.944/108.067/46.167 ms
root@almellonesfernandez-firewall:~#
```

En el ejercicio anterior se observa como entro a las distintas maquinas por ssh, por eso lo he omitido en este ejercicio

```
root@almellonesfernandez-firewall:~# wget 10.0.102.2
--2024-12-14 18:29:34--  http://10.0.102.2/
Connecting to 10.0.102.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 152 [text/html]
Saving to: 'index.html'

index.html                    100%[===================================================>]     152  --.-KB/s    in 0s

2024-12-14 18:29:34 (30,9 MB/s) - 'index.html' saved [152/152]

root@almellonesfernandez-firewall:~# cat index.html
<h1>Nombre: Alvaro </h1><h1>Apellidos: Almellones Fernandez</h1><h1>Clase: 2</h1><h1>IP del Servidor: 10.0.102.2</h1><h1
>IP del Cliente: 10.0.102.1</h1>root@almellonesfernandez-firewall:~#
```

```
root@almellonesfernandez-firewall:~# wget 172.16.102.2
--2024-12-14 19:06:25--  http://172.16.102.2/
Connecting to 172.16.102.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 155 [text/html]
Saving to: 'index.html.1'

index.html.1                  100%[===================================================>]     155  --.-KB/s    in 0s

2024-12-14 19:06:30 (9,31 MB/s) - 'index.html.1' saved [155/155]

root@almellonesfernandez-firewall:~# ls
index.html  index.html.1  scripts
root@almellonesfernandez-firewall:~# cat index.html.1
<h1>Nombre: Alvaro</h1><h1>Apellidos: Almellones Fernandez</h1><h1>Clase: 2</h1><h1>IP del Servidor: 172.16.102.2</h1><h
1>IP del Cliente: 172.16.102.1</h1>root@almellonesfernandez-firewall:~#
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~# ping 172.16.102.4
PING 172.16.102.4 (172.16.102.4) 56(84) bytes of data.
64 bytes from 172.16.102.4: icmp_seq=1 ttl=64 time=118 ms
64 bytes from 172.16.102.4: icmp_seq=2 ttl=64 time=10.2 ms
64 bytes from 172.16.102.4: icmp_seq=3 ttl=64 time=6.60 ms
64 bytes from 172.16.102.4: icmp_seq=4 ttl=64 time=13.0 ms
64 bytes from 172.16.102.4: icmp_seq=5 ttl=64 time=0.902 ms
64 bytes from 172.16.102.4: icmp_seq=6 ttl=64 time=2.27 ms
^C
--- 172.16.102.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.902/25.152/117.966/41.717 ms
root@almellonesfernandez-firewall:~# ssh 172.16.102.4
^C
root@almellonesfernandez-firewall:~# ssh almellonesfernandez@172.16.102.4
The authenticity of host '172.16.102.4 (172.16.102.4)' can't be established.
ED25519 key fingerprint is SHA256:PQihOqT8KbvXmaYjCHZAMU8ab+8KaLUu535e7KPmJJQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Esta es la comprobación del Ubuntu desktop

No he conseguido hacer ping a windows lo cual me resulta raro porque tiene red (recuerdo que algunas capturas de comprobaciones las estoy haciendo una vez he realizado la practica entera)

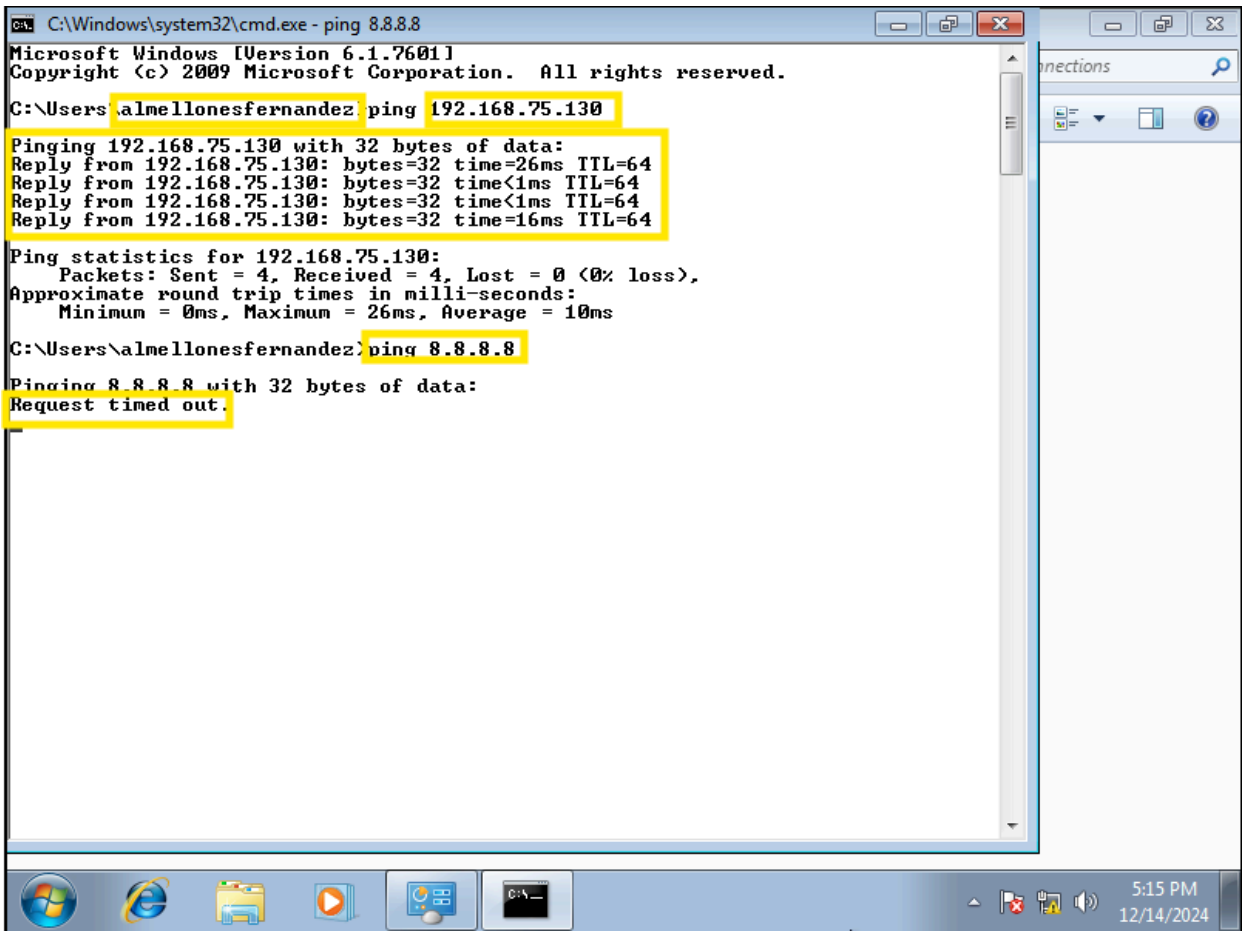
4. **(1 punto)** Comprobación de que se puede acceder desde cada equipo de red, al firewall (ping, ssh), pero no se puede acceder a internet (actualizar, ping, o lo que prefiera).

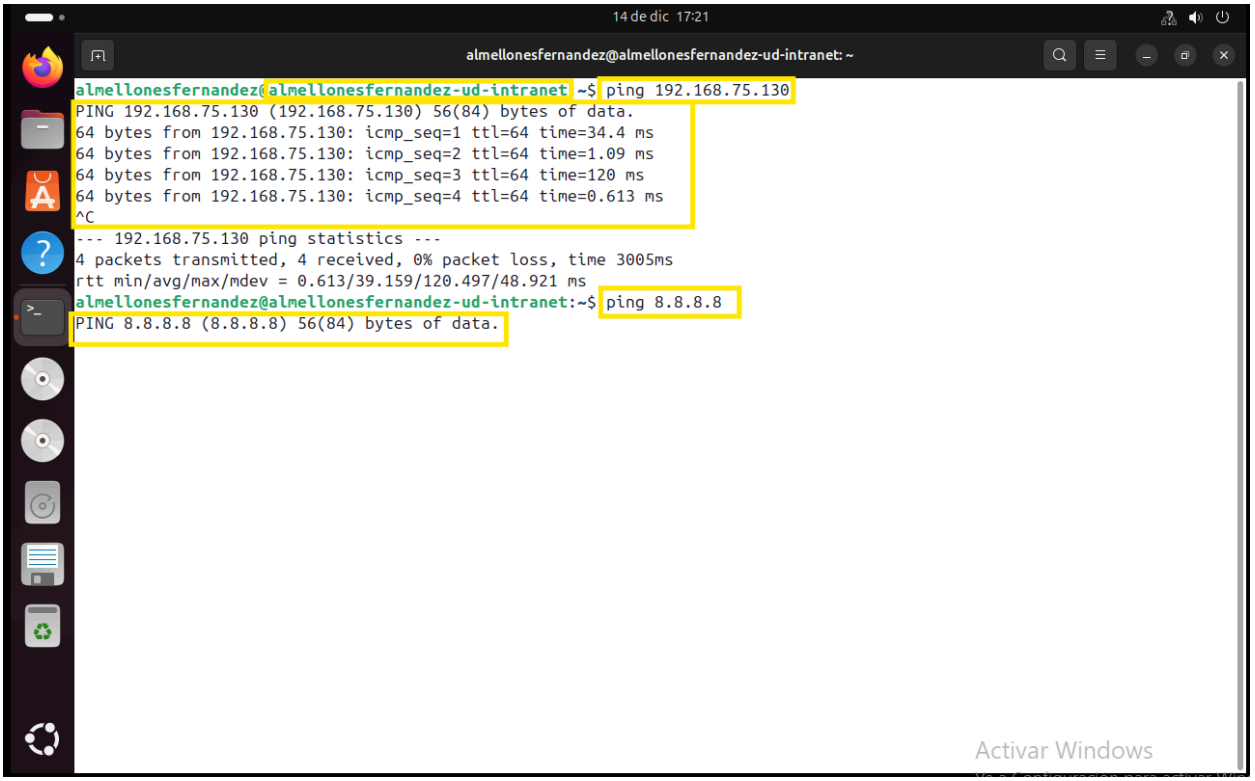
```
almellonesfernandez@almellonesfernandez-us-dmz:~$ ping 192.168.75.130
PING 192.168.75.130 (192.168.75.130) 56(84) bytes of data.
64 bytes from 192.168.75.130: icmp_seq=1 ttl=64 time=42.0 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=1.04 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=0.842 ms
64 bytes from 192.168.75.130: icmp_seq=5 ttl=64 time=1.23 ms

^C--- 192.168.75.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.690/9.159/42.002/16.422 ms
almellonesfernandez@almellonesfernandez-us-dmz:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4128ms

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=74.7 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=0.723 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=0.612 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=0.665 ms
64 bytes from 192.168.75.130: icmp_seq=5 ttl=64 time=0.613 ms
^C
--- 192.168.75.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.612/15.469/74.733/29.631 ms
almellonesfernandez@almellonesfernandez-us-wlan:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4150ms

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=0.413 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=1.54 ms
^C
--- 192.168.75.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.413/1.095/1.536/0.416 ms
almellonesfernandez@almellonesfernandez-us-intranet:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4125ms

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

Álvaro Almellones Fernández





5. Realizar un script (firewall.sh) que: permita **enmascarar** entre las siguientes redes.

○ **(1 punto)** Permita enmascarar desde la red DMZ (naranja), intranet (verde) y wlan (azul) hacía la red wan (roja). Evidenciar qué desde cualquier máquina de esa red, se permite acceder a equipos de la zona wan, es decir internet (ifconfig, ping, apt-get update, wget, dns y ntpdate).

```
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

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 5 packets, 396 bytes)
 pkts bytes target     prot opt in     out     source               destination
    7   484 MASQUERADE  0    --  *      wan2    10.0.102.0/24        0.0.0.0/0            /* Enmascar de
 DMZ a WAN */
    6   418 MASQUERADE  0    --  *      wan2    172.16.102.0/24      0.0.0.0/0            /* Enmascar de
 LAN a WAN */
   10   760 MASQUERADE  0    --  *      wan2    192.168.102.0/24     0.0.0.0/0            /* Enmascar de
 WLAN a WAN */
root@almellonesfernandez-firewall:~/scripts#
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=141 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=18.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=18.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=18.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=18.4 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7013ms
rtt min/avg/max/mdev = 17.693/35.760/141.075/42.995 ms
almellonesfernandez@almellonesfernandez-us-intranet:~$
```

```
almellonesfernandez@almellonesfernandez-us-wlan ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=17.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=18.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=20.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=18.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=18.1 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 17.704/18.752/20.215/0.792 ms
almellonesfernandez@almellonesfernandez-us-wlan:~$
```

```
almellonesfernandez@almellonesfernandez-us-dmz:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=18.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=22.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=18.6 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 18.051/19.115/22.056/1.490 ms
almellonesfernandez@almellonesfernandez-us-dmz:~$
```

Álvaro Almellones Fernández

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\almellonesfernandez>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=37ms TTL=127
Reply from 8.8.8.8: bytes=32 time=19ms TTL=127
Reply from 8.8.8.8: bytes=32 time=17ms TTL=127
Reply from 8.8.8.8: bytes=32 time=17ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 37ms, Average = 22ms

C:\Users\almellonesfernandez>_
```

```
14 de dic 20:52
almellonesfernandez@almellonesfernandez-ud-intranet: ~
almellonesfernandez@almellonesfernandez-ud-intranet:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=18.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=22.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=37.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=30.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=19.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=18.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=19.4 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 18.413/23.818/37.295/6.833 ms
almellonesfernandez@almellonesfernandez-ud-intranet:~$
```

Activar Windows

- **(1 punto)** No se permita enmascarar (-j LOG, para ver que se está intentando acceder,

aunque no enmascare), desde:

- Equipos de la red lan a equipo de la red wlan.
- Equipos de la red lan a equipo de la red dmz.

```
  GNU nano 7.2                          firewall-almellonesfernandez.sh
        iptables -t filter -A FORWARD  -p icmp -i $wlan -o $wan -j ACCEPT
        iptables -t filter -A FORWARD -i $wan -o $wlan -m state --state  ESTABLISHED,RELATED -j ACCEPT >
}

lan-a-wlan() {
iptables -A FORWARD -i $lan -o $wlan -j LOG --log-prefix "LAN to DMZ DENIED AlmellonesFernandez: "
iptables -A FORWARD -i $lan -o $wlan -j DROP


}

lan-a-dmz() {
iptables -A FORWARD -i $lan -o $dmz -j LOG --log-prefix "LAN to DMZ DENIED AlmellonesFernandez: "
iptables -A FORWARD -i $lan -o $dmz -j DROP
}


echo "Arrancado Cortafuegos de Alvaro Almellones. Bastionado de Redes y Sistemas"

variables # Carga de variables
generales # Reglas generales
loopback # Reglas de loopback
dmz-a-wan # Reglas de dmz (zona naranja) a WAN
lan-a-wan # Reglas de intranet-lan (zona verde) a WAN
wlan-a-wan # Reglas de intranet-wlan (zona azul) a WAN
lan-a-wlan
lan-a-dmz
```

```
almellonesfernandez@almellonesfernandez-us-intranet:~$ ping 10.2.102.2
PING 10.2.102.2 (10.2.102.2) 56(84) bytes of data.
^C
--- 10.2.102.2 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3070ms

almellonesfernandez@almellonesfernandez-us-intranet:~$ ping 192.168.102.2
PING 192.168.102.2 (192.168.102.2) 56(84) bytes of data.
^C
--- 192.168.102.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4080ms

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=33.4 ms
64 bytes from 192.168.75.130: icmp_seq=2 ttl=64 time=0.530 ms
64 bytes from 192.168.75.130: icmp_seq=3 ttl=64 time=0.551 ms
64 bytes from 192.168.75.130: icmp_seq=4 ttl=64 time=0.608 ms
^C
--- 192.168.75.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3083ms
rtt min/avg/max/mdev = 0.530/8.761/33.355/14.199 ms
almellonesfernandez@almellonesfernandez-us-intranet:~$
```

Como se puede observar no llega a hacer ping con las máquinas de dmz ni wlan pero a la tarjeta de red wan si

Álvaro Almellones Fernández

```
root@almellonesfernandez-firewall:~/scripts# tail -f /var/log/syslog
2024-12-14T17:54:32.710971+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED: IN=lan2 OUT=wla
n2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS=0x00 PREC
=0x00 TTL=63 ID=25930 DF PROTO=ICMP TYPE=8 CODE=0 ID=2165 SEQ=1
2024-12-14T17:54:33.760650+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED: IN=lan2 OUT=wla
n2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS=0x00 PREC
=0x00 TTL=63 ID=26672 DF PROTO=ICMP TYPE=8 CODE=0 ID=2165 SEQ=2
2024-12-14T17:54:34.784589+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED: IN=lan2 OUT=wla
n2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS=0x00 PREC
=0x00 TTL=63 ID=27458 DF PROTO=ICMP TYPE=8 CODE=0 ID=2165 SEQ=3
2024-12-14T17:54:35.808574+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED: IN=lan2 OUT=wla
n2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS=0x00 PREC
=0x00 TTL=63 ID=28129 DF PROTO=ICMP TYPE=8 CODE=0 ID=2165 SEQ=4
2024-12-14T17:55:02.040222+00:00 almellonesfernandez-firewall CRON[1842]: (root) CMD (command -v debian-
sa1 > /dev/null && debian-sa1 1 1)
2024-12-14T17:57:03.151206+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED AlmellonesFIN=la
n2 OUT=wlan2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS
=0x00 PREC=0x00 TTL=63 ID=16301 DF PROTO=ICMP TYPE=8 CODE=0 ID=2266 SEQ=1
2024-12-14T17:57:04.179090+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED AlmellonesFIN=la
n2 OUT=wlan2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS
=0x00 PREC=0x00 TTL=63 ID=17282 DF PROTO=ICMP TYPE=8 CODE=0 ID=2266 SEQ=2
2024-12-14T17:57:05.183974+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED AlmellonesFIN=la
n2 OUT=wlan2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS
=0x00 PREC=0x00 TTL=63 ID=17982 DF PROTO=ICMP TYPE=8 CODE=0 ID=2266 SEQ=3
2024-12-14T17:57:06.225021+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED AlmellonesFIN=la
n2 OUT=wlan2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS
=0x00 PREC=0x00 TTL=63 ID=18729 DF PROTO=ICMP TYPE=8 CODE=0 ID=2266 SEQ=4
2024-12-14T17:57:07.231839+00:00 almellonesfernandez-firewall kernel: LAN to DMZ DENIED AlmellonesFIN=la
n2 OUT=wlan2 MAC=00:0c:29:c3:df:e7:00:0c:29:9c:d0:e9:08:00 SRC=172.16.102.2 DST=192.168.102.2 LEN=84 TOS
=0x00 PREC=0x00 TTL=63 ID=19056 DF PROTO=ICMP TYPE=8 CODE=0 ID=2266 SEQ=5
```


Nose si no permitir enmascarar se refiere a otra cosa pero con los forward he conseguido que no se pueda acceder desde lan ni wlan ni a dmz

**** Sería bueno realizar un snapshot final de cada de este servidor Ubuntu Server, con explicación de lo que hace. Muestre, aunque no se valorará.*

**** Este es el escenario inicial que se recomienda para tener para todo el curso.*

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.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.