

INSTALACIÓN Y CONFIGURACIÓN DE FIREWALLS

Raúl Arribas Redondo

SAD

1 Contenido

2	Apartado 1: Configuración de reglas Iptables en la máquina dmzd.....	2
2.1	Pon en marcha el servicio <i>apache2</i>	2
2.2	Muestra, mediante el comando correspondiente, la política que actualmente tiene configurada la máquina.....	4
2.3	Lleva a cabo un escaneo de puertos desde la máquina base y explica el resultado obtenido.....	5
2.4	Cambia la política de las cadenas <i>INPUT</i> y <i>FORWARD</i> para que, por defecto, tengan una política restrictiva.....	7
2.5	Permite el tráfico entrante a través de la interfaz de <i>loopback</i>	9
2.6	Permite conexiones entrantes SSH desde la máquina base.....	10
2.7	Permite consultas entrantes de tipo ICMP.....	11
2.8	Vuelve a repetir el escaneo de puertos desde la máquina base y explica el resultado obtenido. ¿Qué diferencias observas con respecto al resultado previamente obtenido? Justifica la respuesta.....	12
2.9	Realiza las siguientes comprobaciones:	13
3	Apartado 2: Configuración de reglas Iptables en la máquina fw	16
3.1	Borra todas las reglas existente en fw y establece los contadores a cero.	16
3.2	Establece que la política por defecto sea restrictiva.....	17
3.3	Permite que solo la máquina <i>exta</i> se pueda conectar al <i>servidor VPN</i> instalado y configurado en la máquina <i>dmzc</i>	18
3.4	Utiliza el túnel VPN existente entre <i>exta</i> y <i>dmzc</i> para conectarte a su servicio guacamole, y desde él, conéctate por SSH al servidor web <i>dmza</i>	19
3.5	Permite el tráfico correspondiente a nuevas conexiones dirigidas hacia el servidor web (<i>dmza</i>), tanto accediendo por HTTP como por HTTPS.....	19
3.6	Permite el tráfico correspondiente a nuevas conexiones dirigidas hacia el servidor FTP (<i>dmzb</i>).....	20
3.7	Permite el tráfico correspondiente a conexiones establecidas y/o relacionadas.....	20
3.8	Añade las reglas necesarias para ocultar la estructura interna de las redes.....	21
3.9	Haz que todas las reglas anteriores sean persistentes.....	22
4	Uso de <i>hping</i>	24
4.1	Utiliza <i>hping</i> para verificar si el servicio FTP está activado y si se encuentra redireccionado en un host interno.....	24

2 Apartado 1: Configuración de reglas Iptables en la máquina dmzd

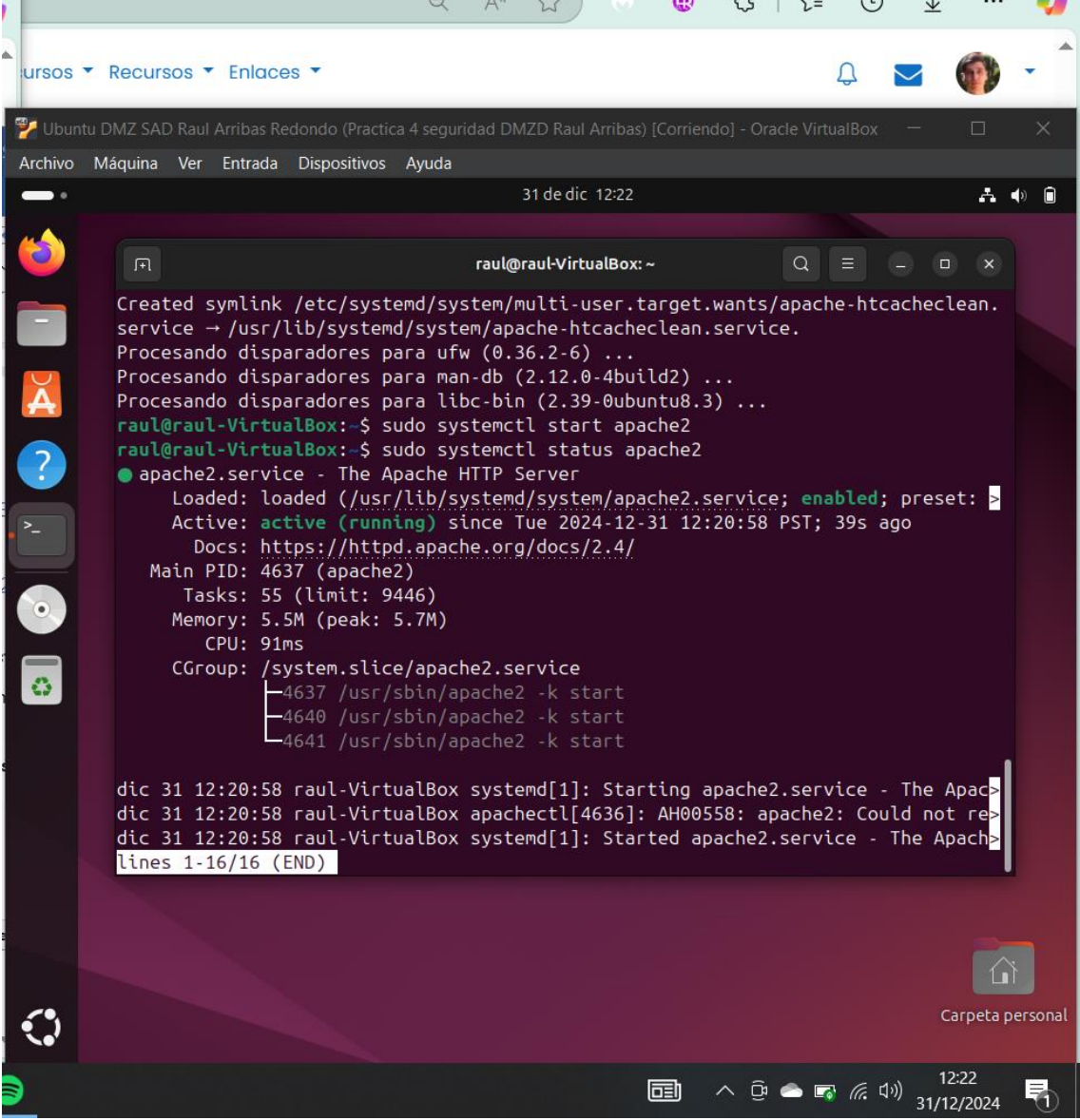
2.1 Pon en marcha el servicio *apache2*.

Ejecutamos **sudo apt install apache2 -y**

Iniciamos el servicio de Apache: **sudo systemctl start apache2**

Habilitamos Apache para que cuando reiniciemos se inicie automáticamente: **sudo systemctl enable apache2**

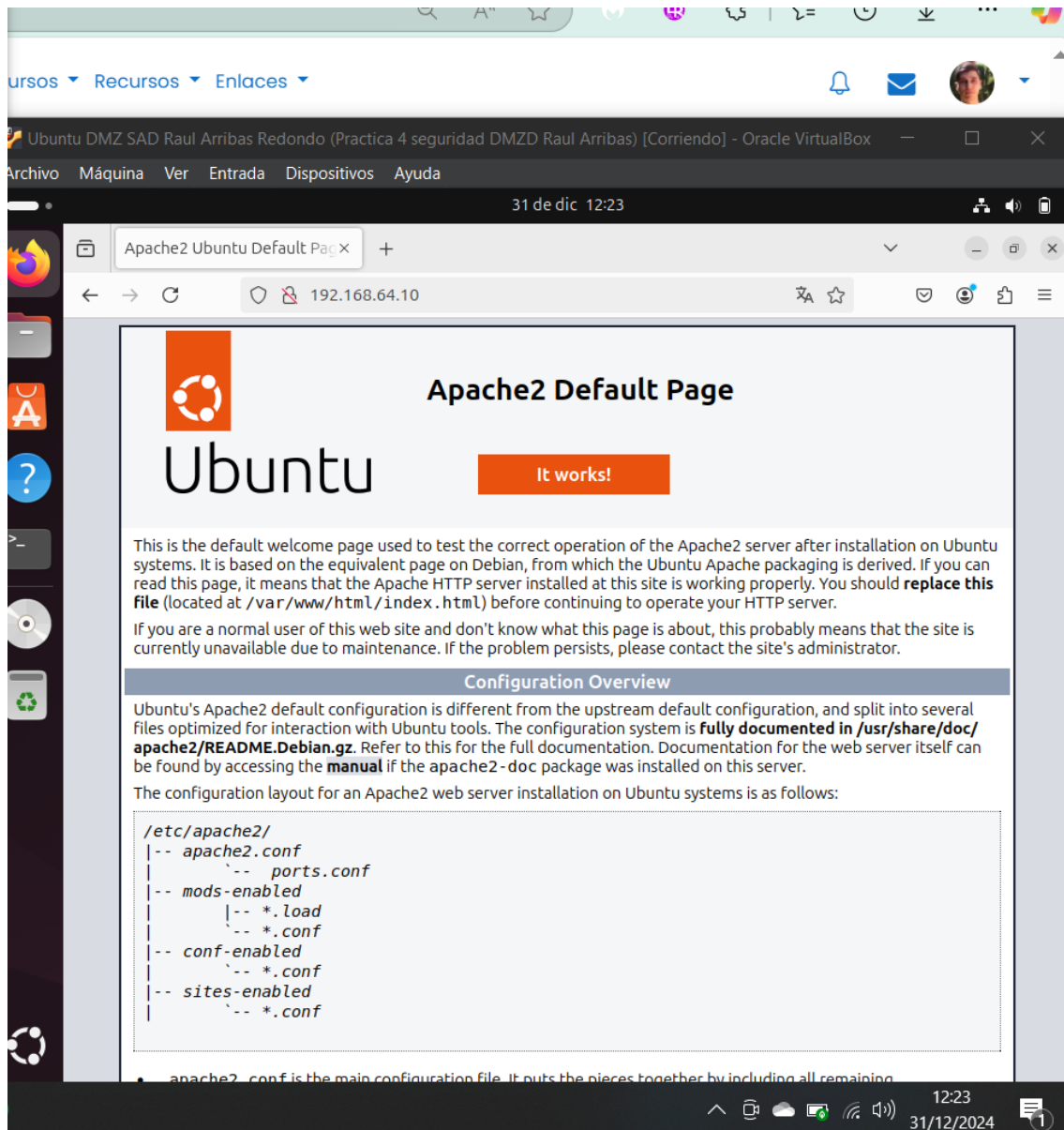
Verificamos que Apache está corriendo: **sudo systemctl status apache2**



```
raul@raul-VirtualBox: ~  
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean.service.  
Procesando disparadores para ufw (0.36.2-6) ...  
Procesando disparadores para man-db (2.12.0-4build2) ...  
Procesando disparadores para libc-bin (2.39-0ubuntu8.3) ...  
raul@raul-VirtualBox:~$ sudo systemctl start apache2  
raul@raul-VirtualBox:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: >  
   Active: active (running) since Tue 2024-12-31 12:20:58 PST; 39s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Main PID: 4637 (apache2)  
    Tasks: 55 (limit: 9446)  
  Memory: 5.5M (peak: 5.7M)  
     CPU: 91ms  
   CGroup: /system.slice/apache2.service  
           └─4637 /usr/sbin/apache2 -k start  
             └─4640 /usr/sbin/apache2 -k start  
               └─4641 /usr/sbin/apache2 -k start  
  
dic 31 12:20:58 raul-VirtualBox systemd[1]: Starting apache2.service - The Apac>  
dic 31 12:20:58 raul-VirtualBox apachectl[4636]: AH00558: apache2: Could not re>  
dic 31 12:20:58 raul-VirtualBox systemd[1]: Started apache2.service - The Apac>  
lines 1-16/16 (END)
```

Instalación y configuración de firewalls

Comprobación desde el navegador:

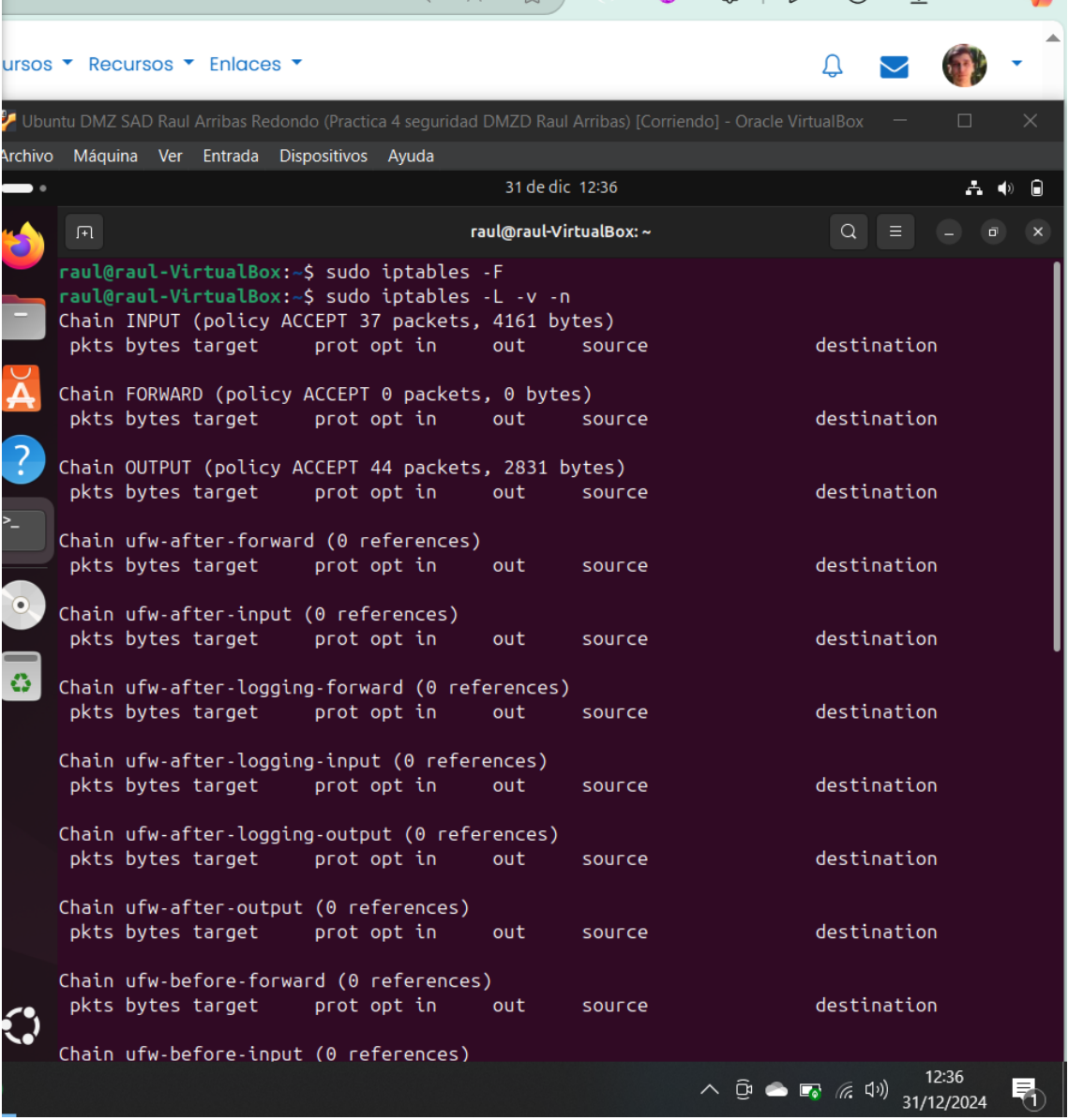


Instalación y configuración de firewalls

2.2 Muestra, mediante el comando correspondiente, la política que actualmente tiene configurada la máquina.

Para consultar las reglas actuales que tenemos configuradas de Iptables, ejecutamos el siguiente comando en la terminal:

sudo iptables -L -v -n



```
raul@raul-VirtualBox:~$ sudo iptables -F
raul@raul-VirtualBox:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 37 packets, 4161 bytes)
 pkts bytes target     prot opt in     out     source                   destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 44 packets, 2831 bytes)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-forward (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-input (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-logging-forward (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-logging-input (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-logging-output (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-after-output (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-before-forward (0 references)
 pkts bytes target     prot opt in     out     source                   destination
Chain ufw-before-input (0 references)
```

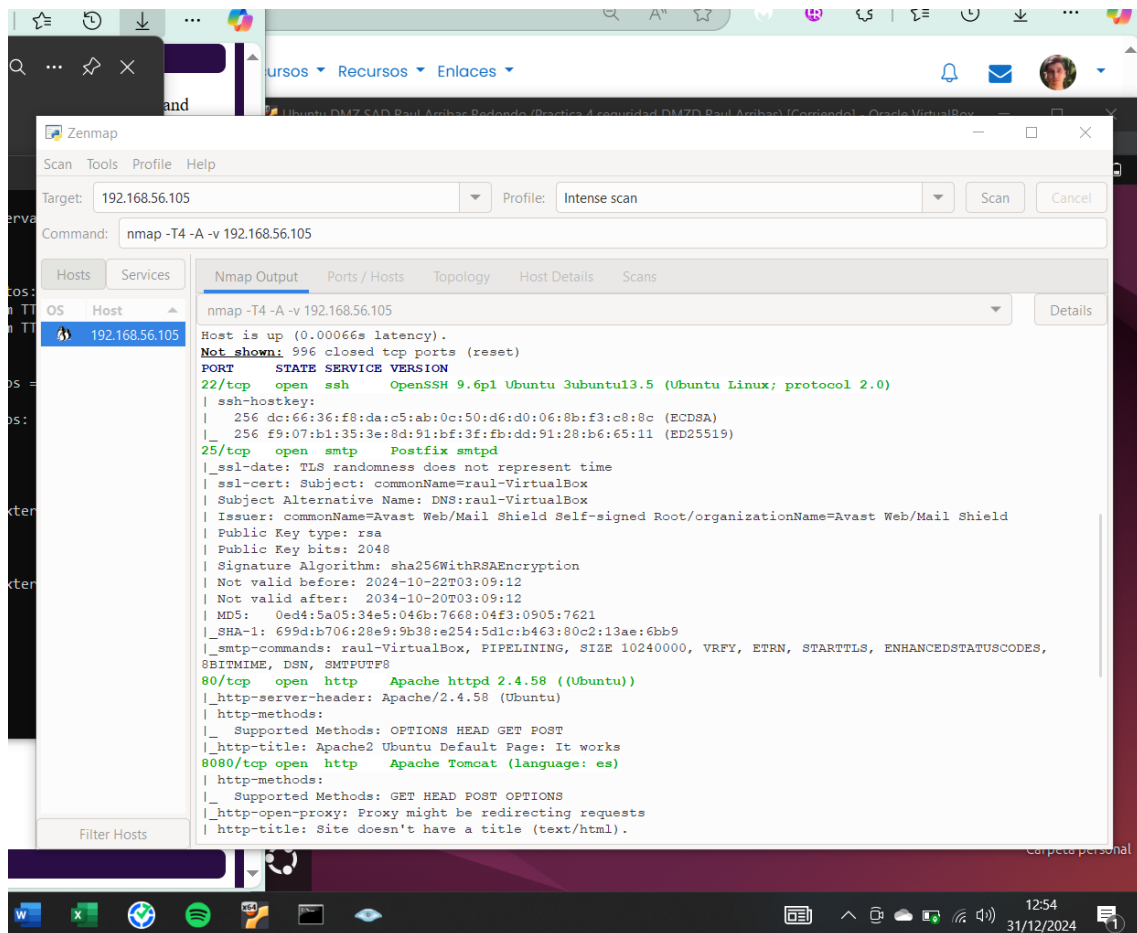
Instalación y configuración de firewalls

- **Chain INPUT:** Maneja el tráfico entrante. Actualmente, tiene una política por defecto de ACCEPT (aceptar todo el tráfico). Se han recibido 37 paquetes (4161 bytes) en total.
- **Chain FORWARD:** Maneja el tráfico que pasa a través de la máquina (enrutamiento). También está configurado para ACCEPT, pero no ha procesado ningún paquete.
- **Chain OUTPUT:** Maneja el tráfico saliente desde tu máquina. También tiene una política ACCEPT y ha procesado 44 paquetes (2831 bytes).

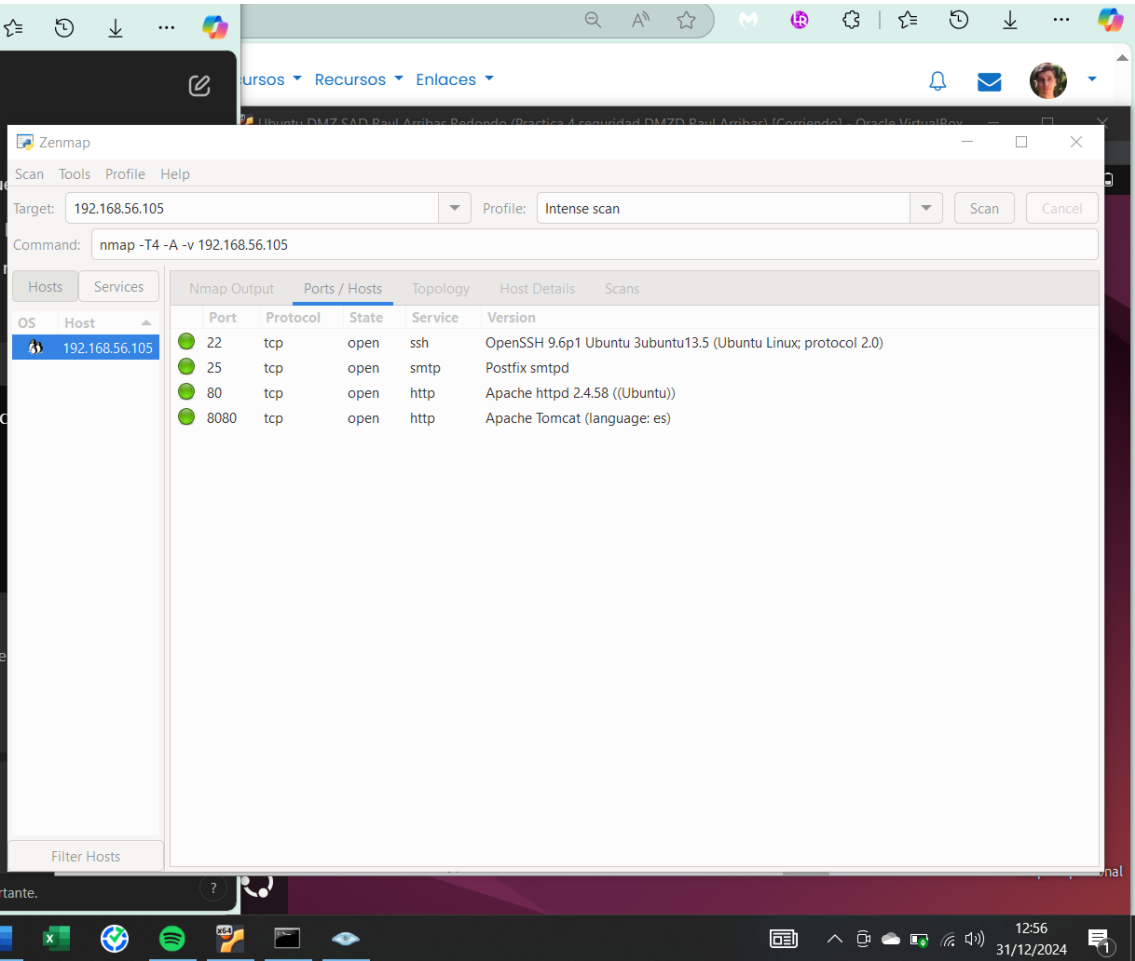
Aunque **UFW** ya no está controlando el tráfico activamente, las cadenas asociadas a su configuración aún existen, pero están "huérfanas" (no están siendo referenciadas por las cadenas principales).

2.3 Lleva a cabo un escaneo de puertos desde la máquina *base* y explica el resultado obtenido.

Hemos escaneado la maquina DMZD desde nuestra maquina Host y este es el resultado obtenido, aparecen los puertos 22,25,80 y 8080 abiertos:



Instalación y configuración de firewalls



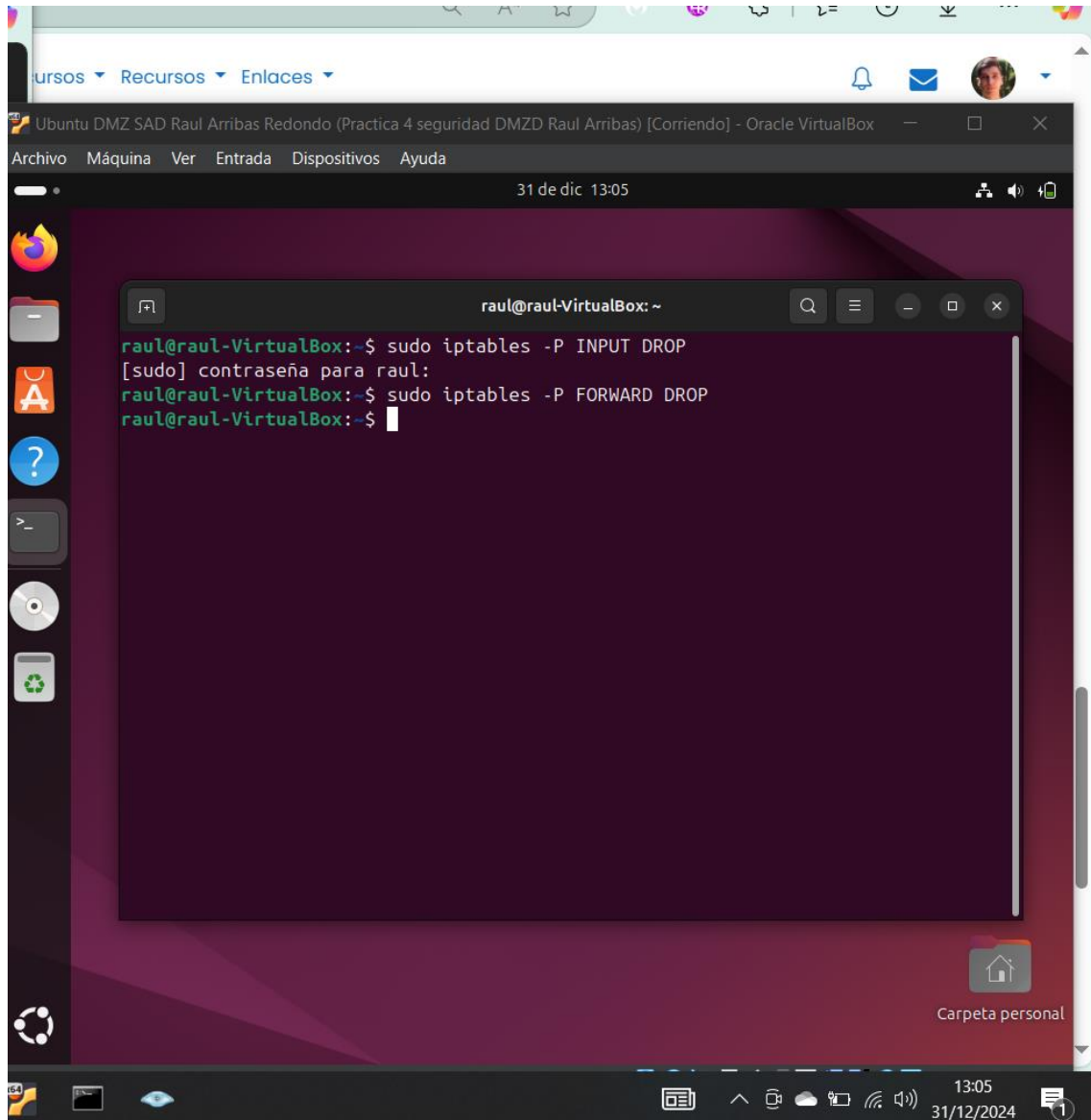
Instalación y configuración de firewalls

2.4 Cambia la política de las cadenas *INPUT* y *FORWARD* para que, por defecto, tengan una política restrictiva.

Para que tengan una política mas restrictivas las politicas de entrada y redirección, tenemos que modificar las Iptables, ponemos el siguiente comando:

sudo iptables -P INPUT DROP

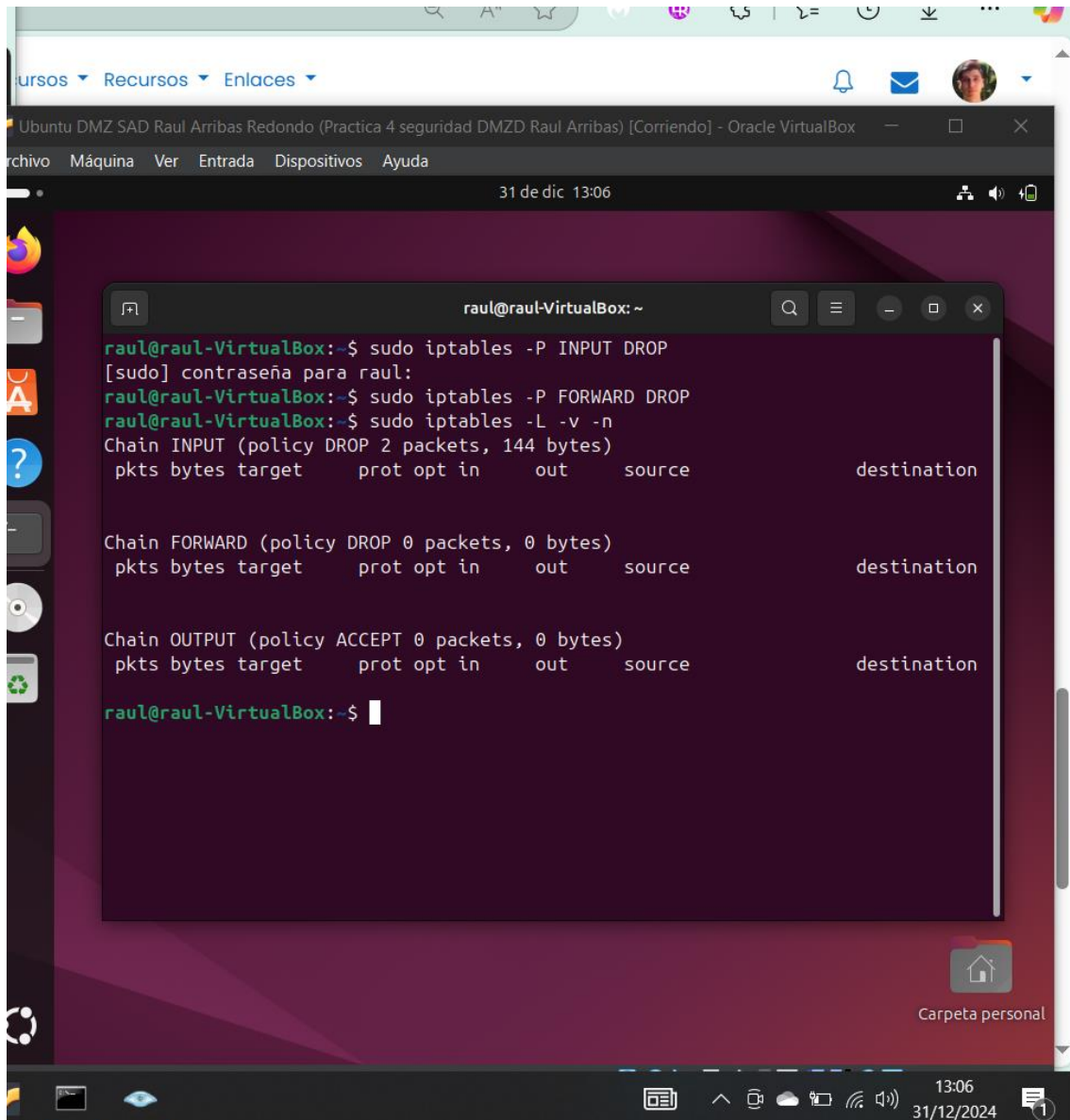
sudo iptables -P FORWARD DROP



Instalación y configuración de firewalls

Verificamos los cambios: **sudo iptables -L -v -n**

Como vemos nos sale INPUT Y FORWARD como DROP.



```
raul@raul-VirtualBox:~$ sudo iptables -P INPUT DROP
[sudo] contraseña para raul:
raul@raul-VirtualBox:~$ sudo iptables -P FORWARD DROP
raul@raul-VirtualBox:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 2 packets, 144 bytes)
 pkts bytes target    prot opt in     out     source                   destination

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

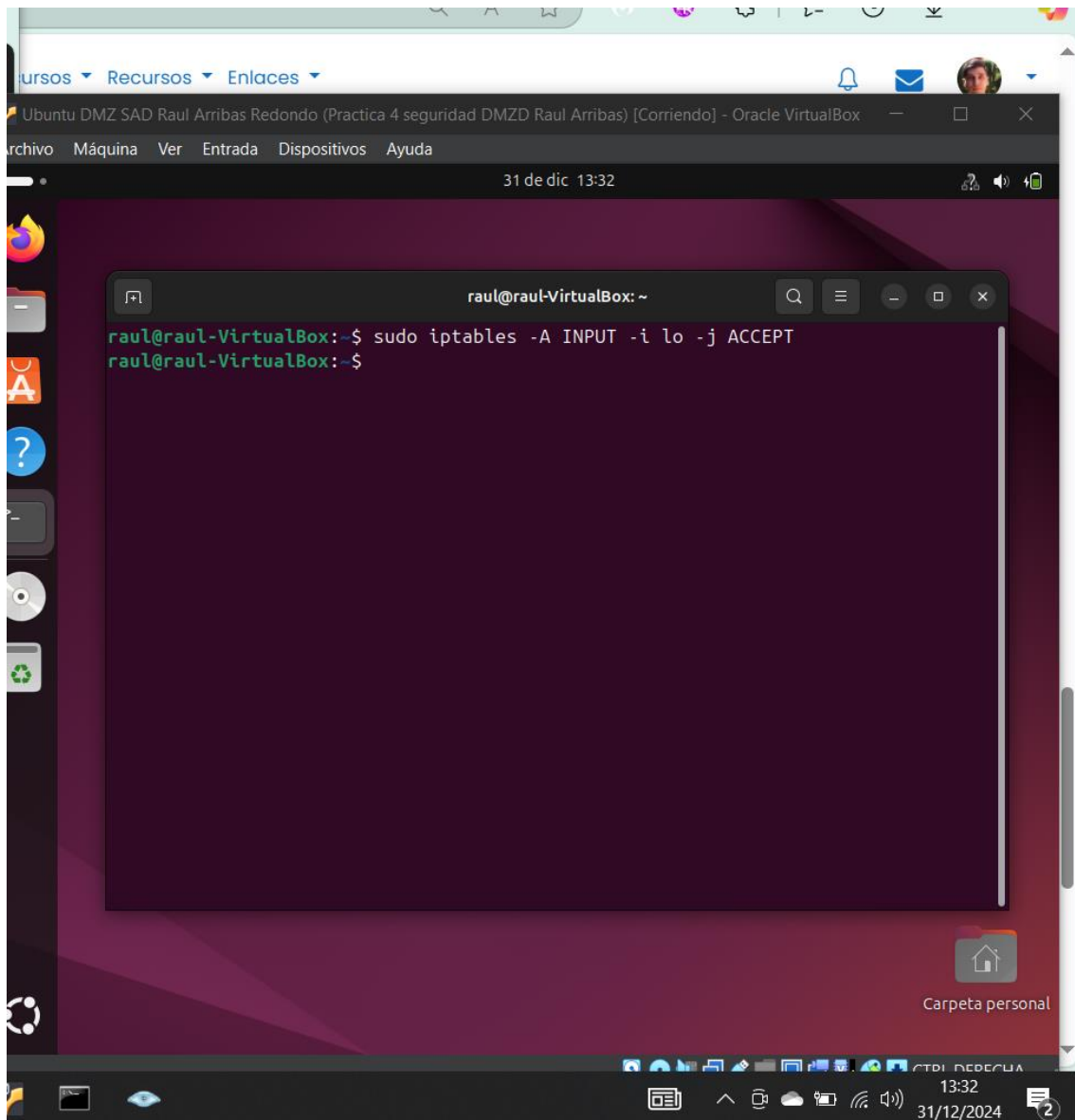
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

raul@raul-VirtualBox:~$
```

Instalación y configuración de firewalls

2.5 Permite el tráfico entrante a través de la interfaz de *loopback*.

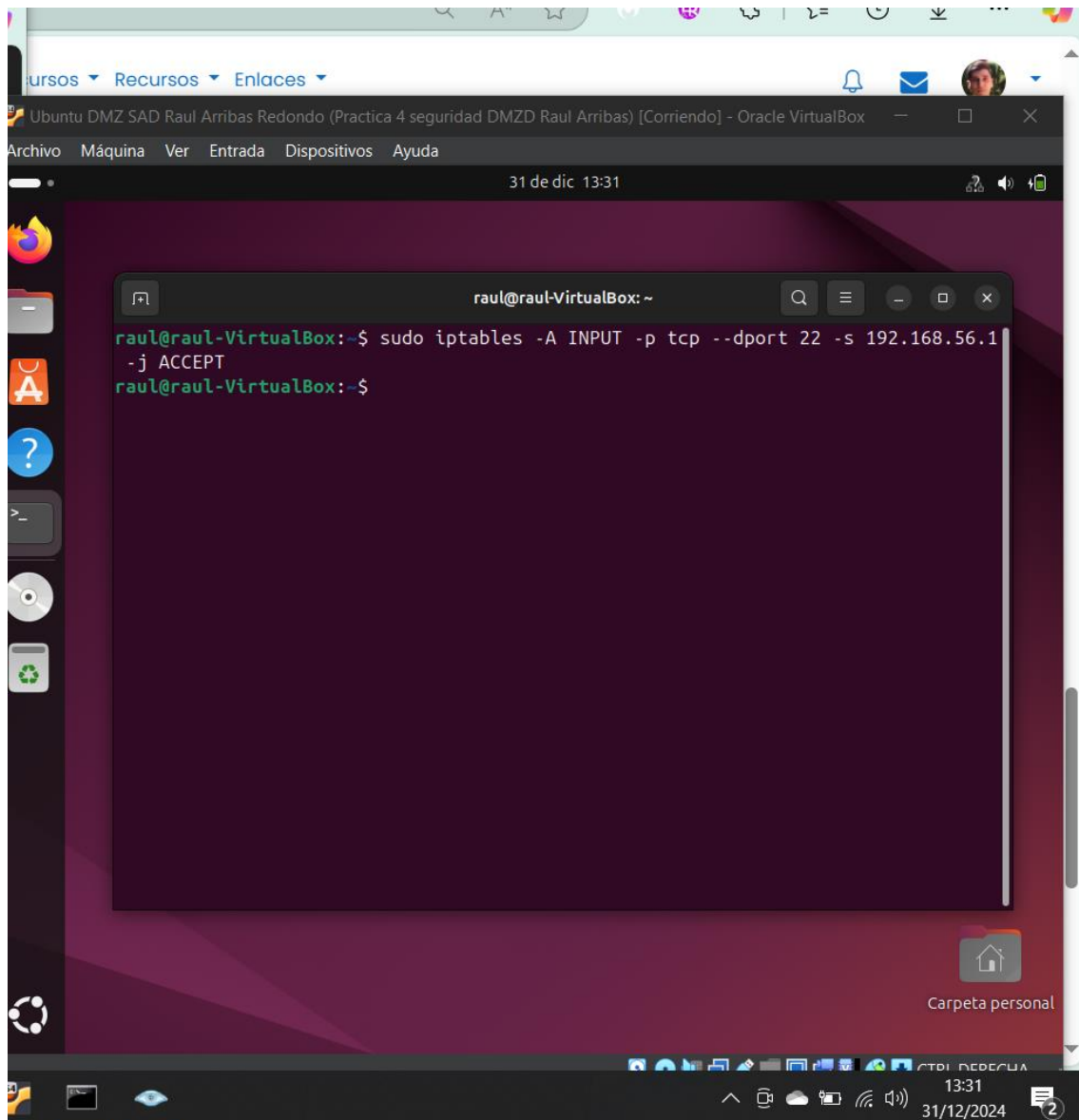
Permitimos el tráfico en la interfaz de loopback: **sudo iptables -A INPUT -i lo -j ACCEPT**



Instalación y configuración de firewalls

2.6 Permite conexiones entrantes SSH desde la máquina base.

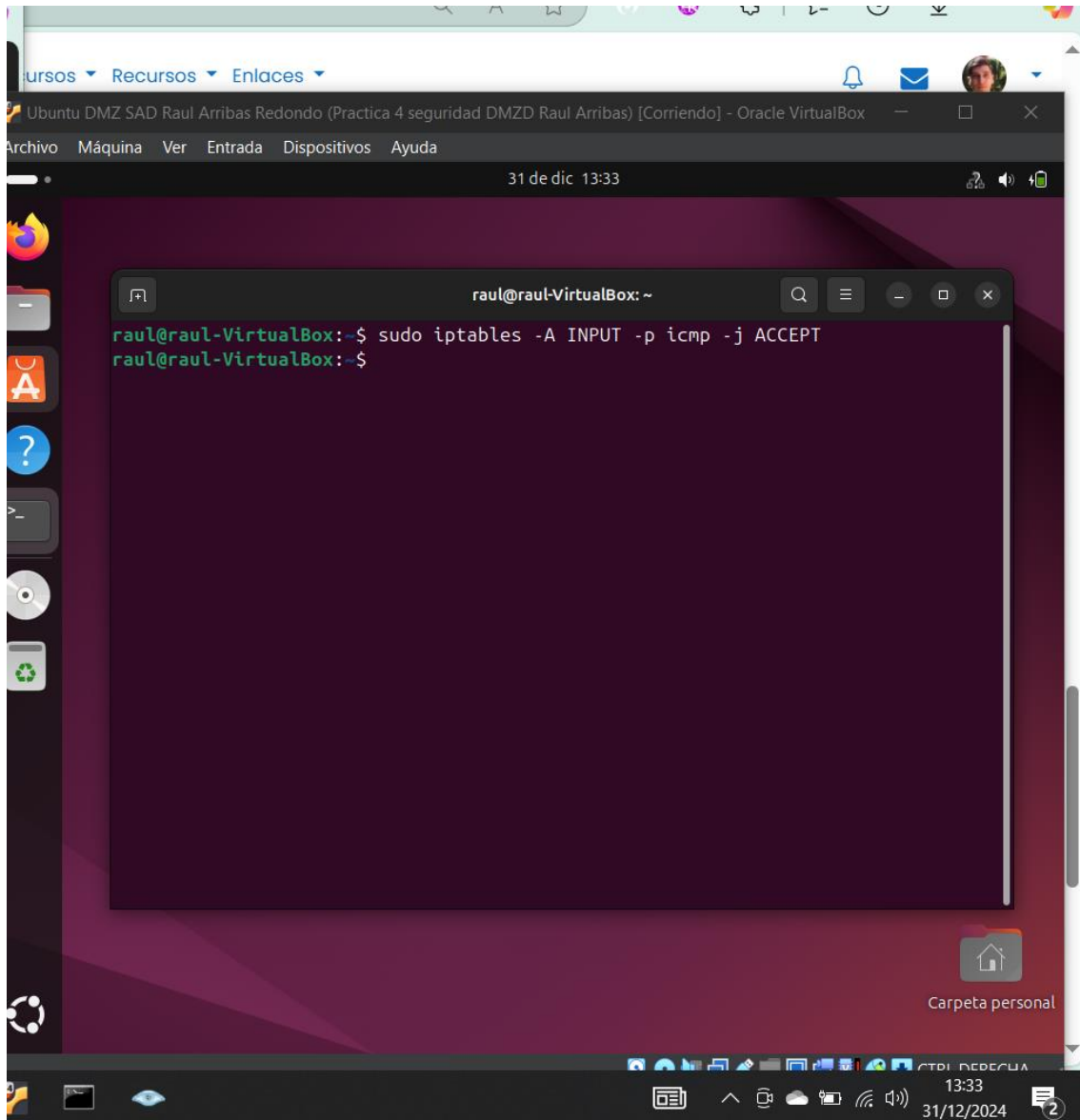
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.56.1 -j ACCEPT



Instalación y configuración de firewalls

2.7 Permite consultas entrantes de tipo ICMP.

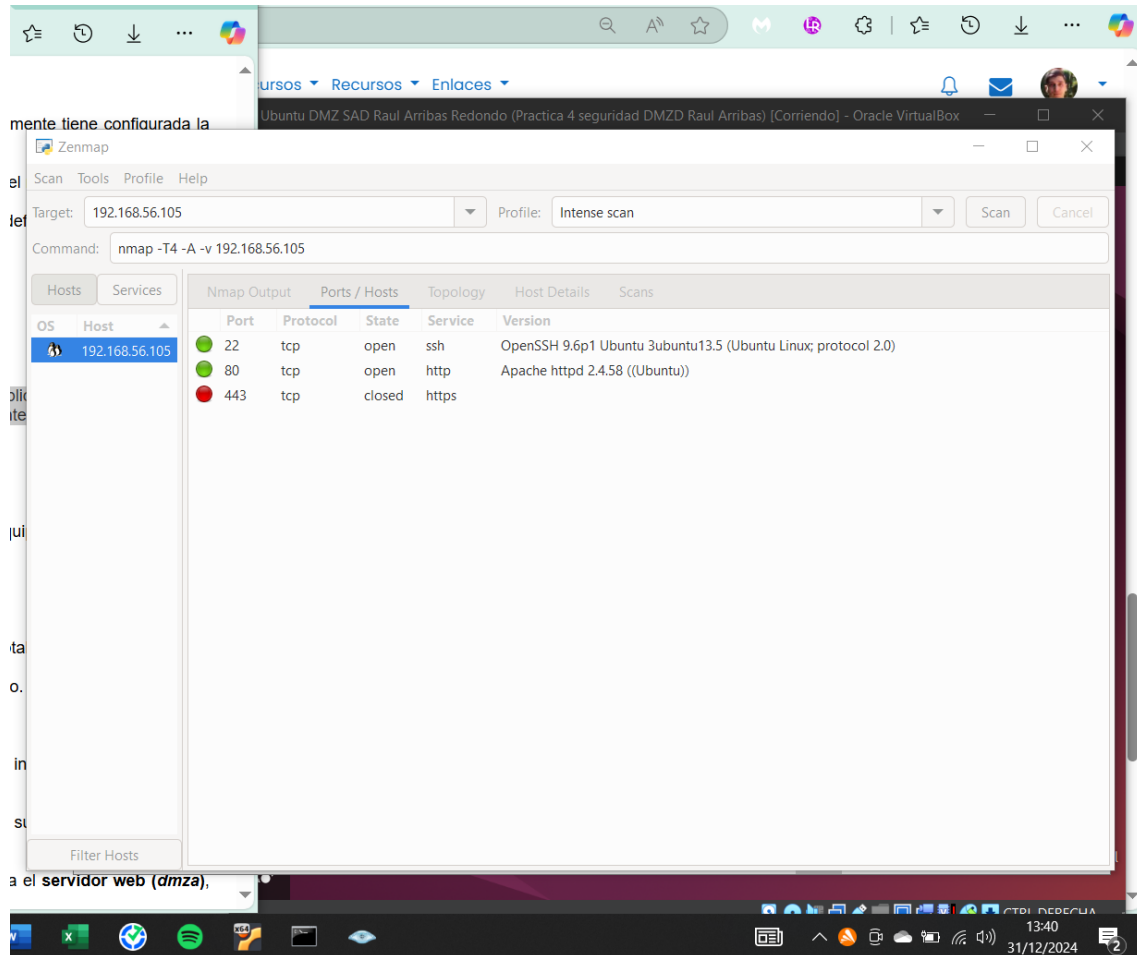
sudo iptables -A INPUT -p icmp -j ACCEPT



Instalación y configuración de firewalls

2.8 Vuelve a repetir el escaneo de puertos desde la máquina base y explica el resultado obtenido. ¿Qué diferencias observas con respecto al resultado previamente obtenido? Justifica la respuesta.

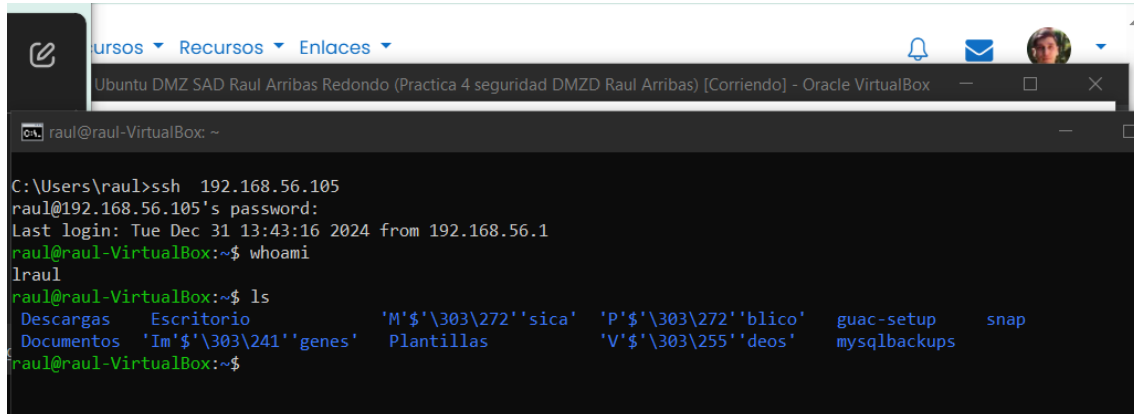
Hacemos el escaneo de nuevo y vemos que el puerto 443 ahora esta CLOSED:



Instalación y configuración de firewalls

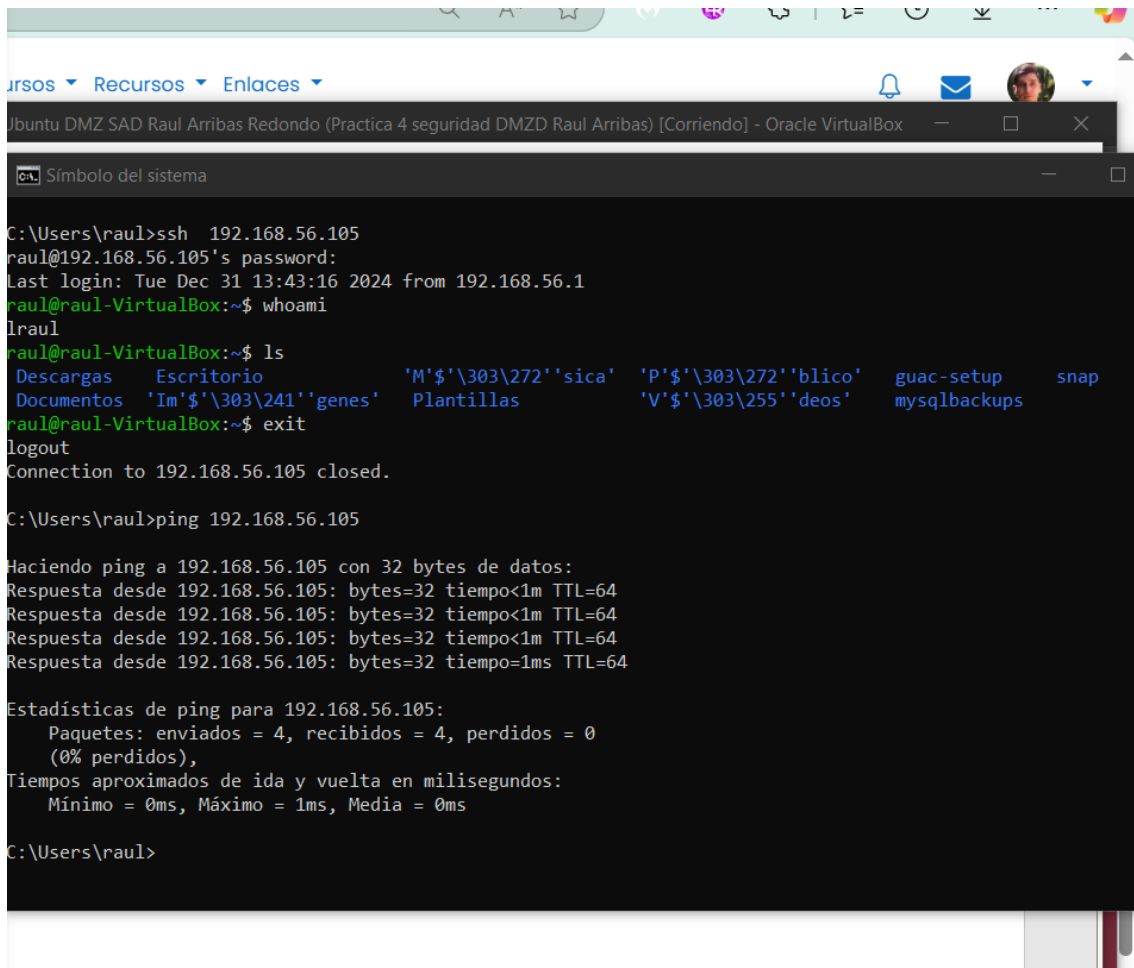
2.9 Realiza las siguientes comprobaciones:

- Es posible conectarse por SSH desde base.



```
C:\Users\raul>ssh 192.168.56.105
raul@192.168.56.105's password:
Last login: Tue Dec 31 13:43:16 2024 from 192.168.56.1
raul@raul-VirtualBox:~$ whoami
raul
raul@raul-VirtualBox:~$ ls
Descargas  Escritorio  'M'$'\303\272'sica'  'P'$'\303\272'blico'  guac-setup  snap
Documentos 'Im'$'\303\241'genes' Plantillas  'V'$'\303\255'deos'  mysqlbackups
raul@raul-VirtualBox:~$
```

- Responde a un ping desde base.



```
C:\Users\raul>ssh 192.168.56.105
raul@192.168.56.105's password:
Last login: Tue Dec 31 13:43:16 2024 from 192.168.56.1
raul@raul-VirtualBox:~$ whoami
raul
raul@raul-VirtualBox:~$ ls
Descargas  Escritorio  'M'$'\303\272'sica'  'P'$'\303\272'blico'  guac-setup  snap
Documentos 'Im'$'\303\241'genes' Plantillas  'V'$'\303\255'deos'  mysqlbackups
raul@raul-VirtualBox:~$ exit
logout
Connection to 192.168.56.105 closed.

C:\Users\raul>ping 192.168.56.105

Haciendo ping a 192.168.56.105 con 32 bytes de datos:
Respuesta desde 192.168.56.105: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.56.105: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.56.105: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.56.105: bytes=32 tiempo=1ms TTL=64

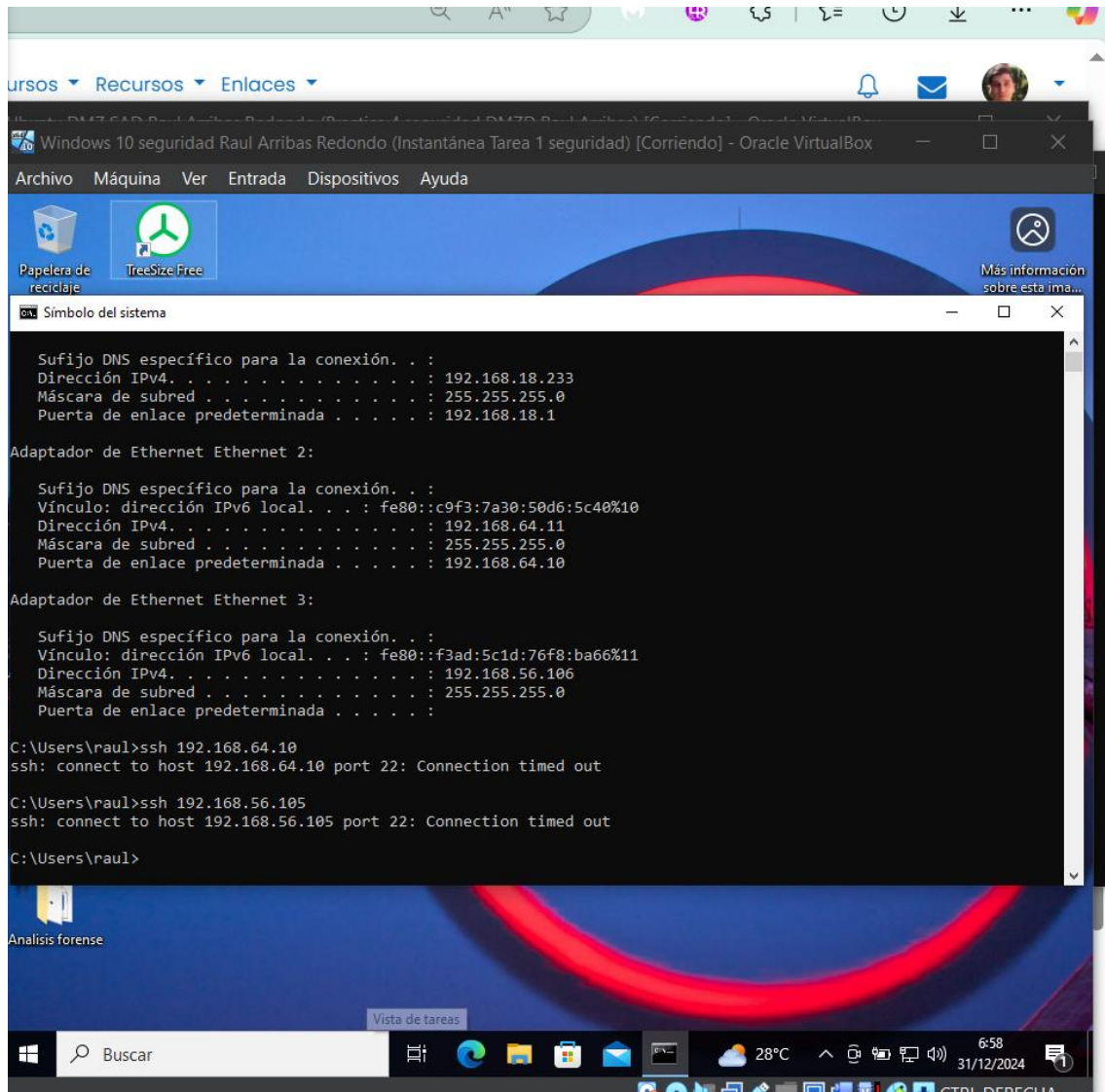
Estadísticas de ping para 192.168.56.105:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\raul>
```

Instalación y configuración de firewalls

- No es posible conectarse por SSH desde cualquier otro equipo del entorno pero sí responde a un ping.

No es posible conectarse desde otro equipo diferente por ssh:



```
Sufijo DNS específico para la conexión. . . :
Dirección IPv4. . . . . : 192.168.18.233
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.18.1

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::c9f3:7a30:50d6:5c40%10
Dirección IPv4. . . . . : 192.168.64.11
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.64.10

Adaptador de Ethernet Ethernet 3:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::f3ad:5c1d:76f8:ba66%11
Dirección IPv4. . . . . : 192.168.56.106
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :

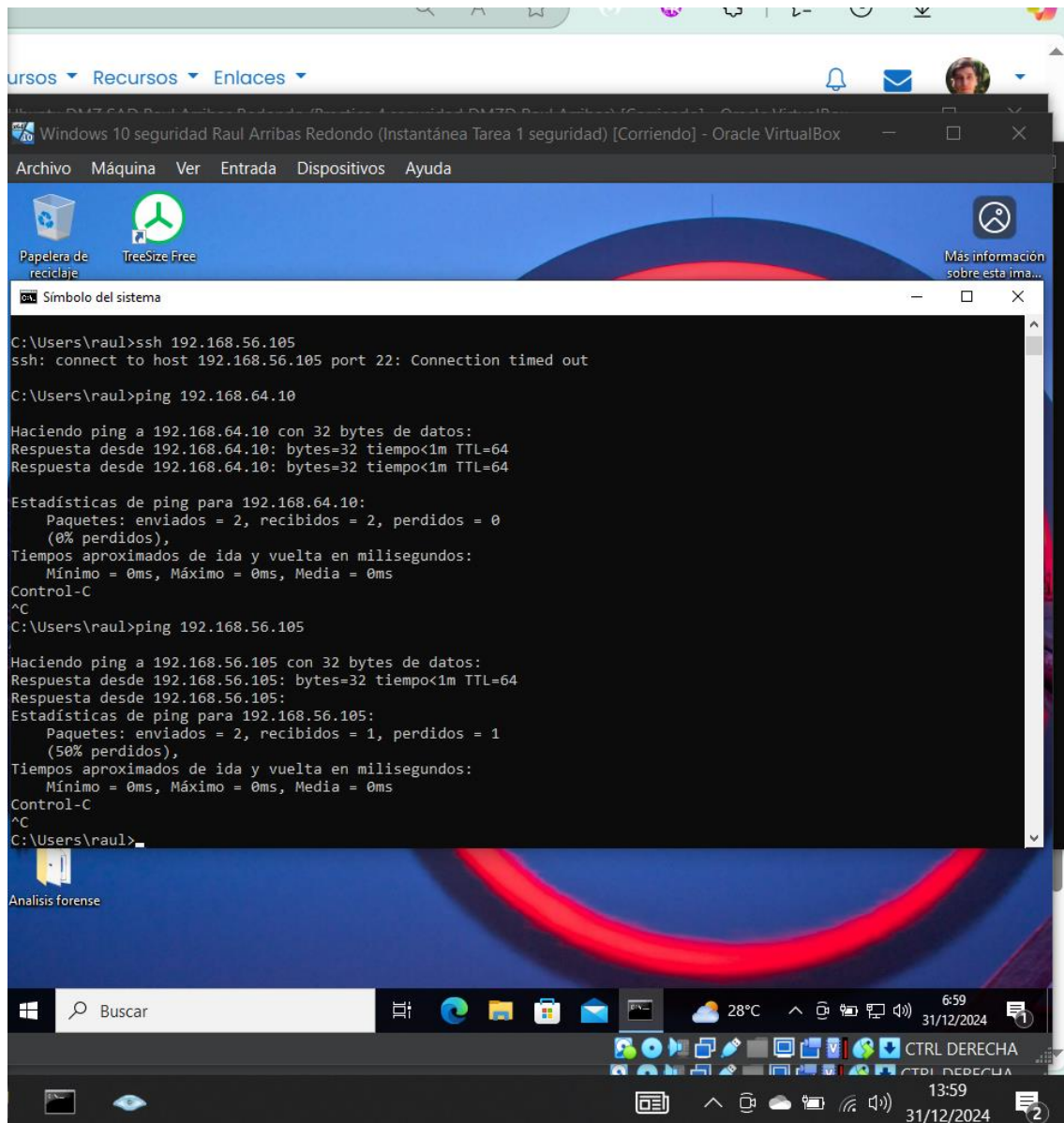
C:\Users\raul>ssh 192.168.64.10
ssh: connect to host 192.168.64.10 port 22: Connection timed out

C:\Users\raul>ssh 192.168.56.105
ssh: connect to host 192.168.56.105 port 22: Connection timed out

C:\Users\raul>
```

Instalación y configuración de firewalls

Pero en cambio mediante un PING funciona correctamente:



3 Apartado 2: Configuración de reglas Iptables en la máquina fw

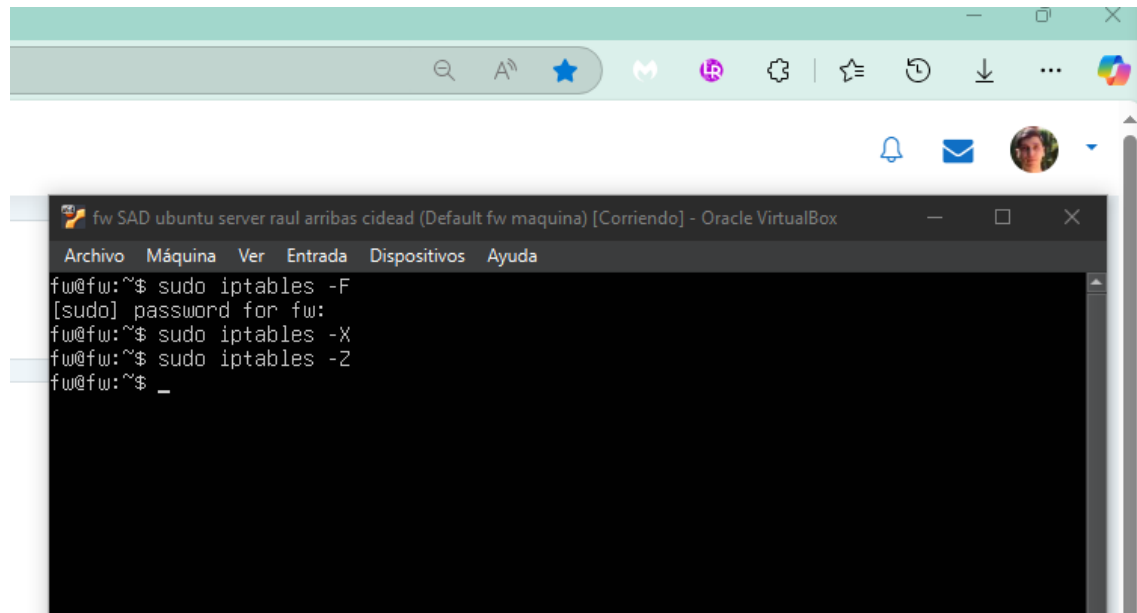
3.1 Borra todas las reglas existente en fw y establece los contadores a cero.

Esta máquina actuará como el firewall principal, para configurar las reglas de Iptables tenemos que hacer lo siguiente:

sudo iptables -F # Borra todas las reglas de las cadenas actuales

sudo iptables -X # Borra todas las cadenas definidas por el usuario

sudo iptables -Z # Reinicia los contadores a cero



Instalación y configuración de firewalls

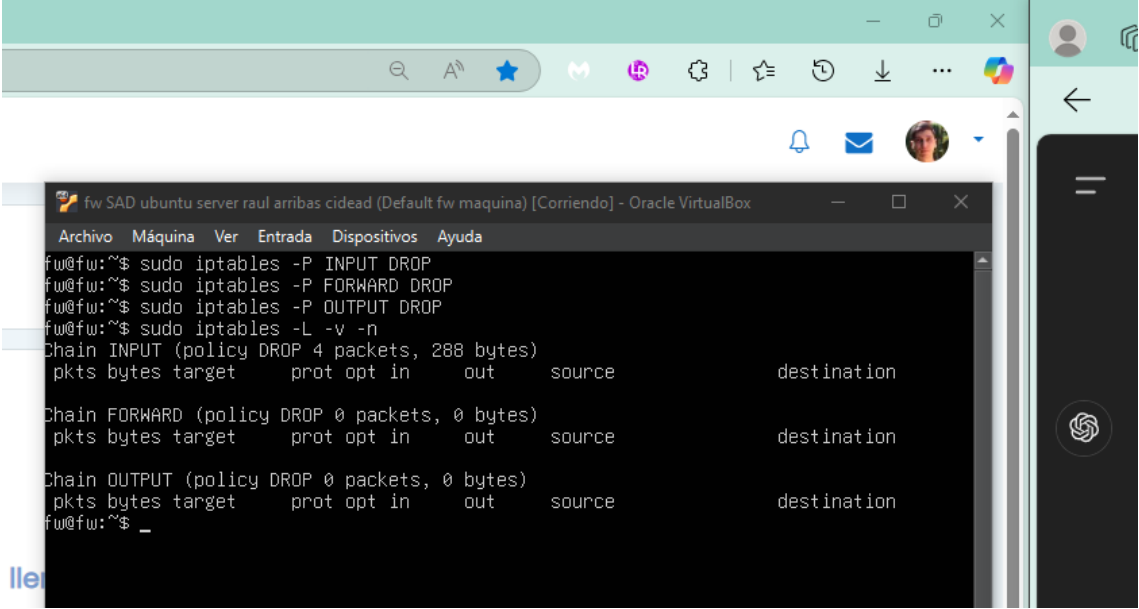
3.2 Establece que la política por defecto sea restrictiva.

Esto bloquea todo el tráfico por defecto

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT DROP



The screenshot shows a terminal window titled "fw SAD ubuntu server raul arribas cidead (Default fw maquina) [Corriendo] - Oracle VirtualBox". The terminal displays the following commands and output:

```
fw@fw:~$ sudo iptables -P INPUT DROP
fw@fw:~$ sudo iptables -P FORWARD DROP
fw@fw:~$ sudo iptables -P OUTPUT DROP
fw@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 4 packets, 288 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
fw@fw:~$ _
```

Instalación y configuración de firewalls

3.3 Permite que solo la máquina *exta* se pueda conectar al *servidor VPN* instalado y configurado en la máquina *dmzc*.

Nuestras Ip de maquinas exta y dmzc:

Exta: 192.168.1.23

Dmzc: 192.168.1.21

El servidor VPN utiliza el puerto 1194 (OPENVPN)

sudo iptables -A INPUT -s 192.168.1.23 -d 192.168.1.21 -p udp --dport 1194 -j ACCEPT

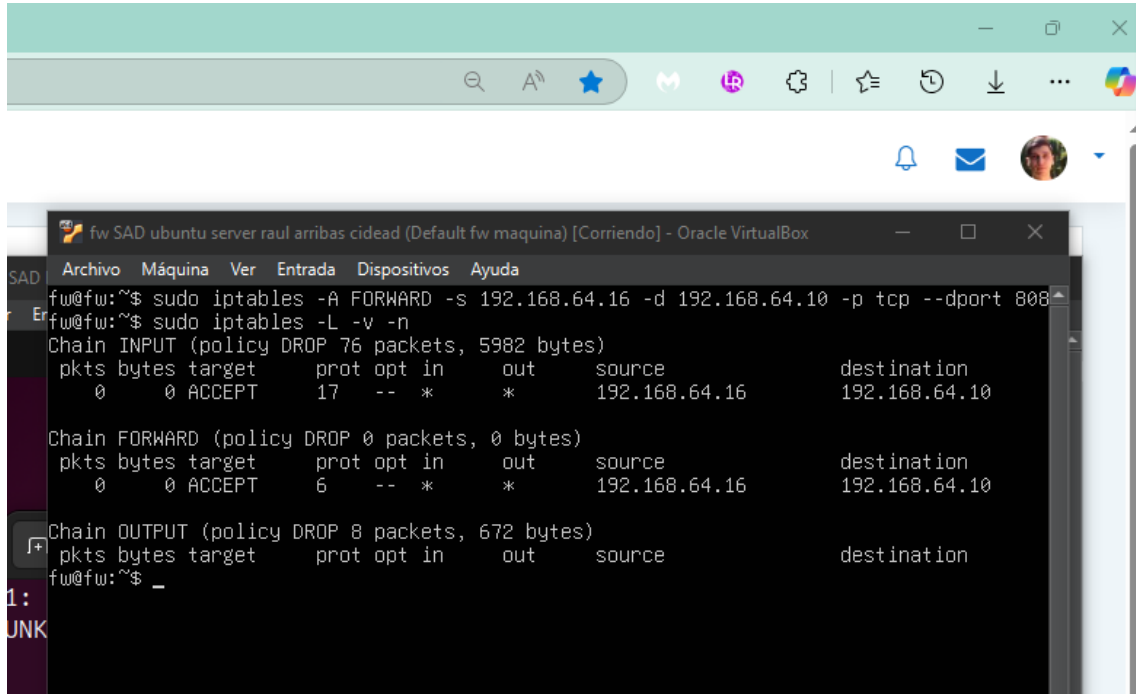
```
fw SAD ubuntu server raul arribas cidead (Default fw maquina) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
fw@fw:~$ sudo iptables -A INPUT -s 192.168.1.23 -d 192.168.1.21 -p udp --dport 1194 -j ACCEPT
fw@fw:~$ sudo iptables -L -n -v
Chain INPUT (policy DROP 588 packets, 40027 bytes)
 pkts bytes target     prot opt in     out     source               destination           udp dpt:1194
  0      0 ACCEPT     17    --    *      *       192.168.1.23         192.168.1.21          udp dpt:1194
  9    771 ACCEPT     0      --    *      *       0.0.0.0/0            0.0.0.0/0             ctstate RELATED
  0      0 ACCEPT     0      --    *      *       0.0.0.0/0            0.0.0.0/0             ctstate RELATED
  0      0 ACCEPT     17    --    *      *       192.168.1.23         192.168.1.21          udp dpt:1194
Chain FORWARD (policy DROP 440 packets, 27173 bytes)
 pkts bytes target     prot opt in     out     source               destination           tcp dpt:8080
  0      0 ACCEPT     6      --    *      *       192.168.64.16        192.168.64.10         tcp dpt:22
  0      0 ACCEPT     6      --    *      *       192.168.64.10        192.168.64.13         tcp dpt:21
  0      0 ACCEPT     6      --    *      *       0.0.0.0/0            192.168.64.15         multiport dpor
  5347 8632K ACCEPT     0      --    *      *       0.0.0.0/0            0.0.0.0/0             ctstate RELATE
  61   3996 ACCEPT     0      --    *      *       enp0s3               0.0.0.0/0
Chain OUTPUT (policy ACCEPT 6 packets, 504 bytes)
 pkts bytes target     prot opt in     out     source               destination           udp dpt:53
  3    243 ACCEPT     17    --    *      *       0.0.0.0/0            0.0.0.0/0             tcp dpt:53
  0      0 ACCEPT     6      --    *      *       0.0.0.0/0            0.0.0.0/0             tcp dpt:80
  0      0 ACCEPT     6      --    *      *       0.0.0.0/0            0.0.0.0/0             tcp dpt:443
fw@fw:~$
```

Instalación y configuración de firewalls

3.4 Utiliza el túnel VPN existente entre exta y dmzc para conectarte a su servicio guacamole, y desde él, conéctate por SSH al servidor web dmza.

Vamos a permitir ahora que el servicio de guacamole utilice el puerto 8080

sudo iptables -A FORWARD -s 192.168.64.16 -d 192.168.64.10 -p tcp --dport 8080 -j ACCEPT



```
fw@fw:~$ sudo iptables -A FORWARD -s 192.168.64.16 -d 192.168.64.10 -p tcp --dport 8080 -j ACCEPT
fw@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 76 packets, 5982 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT    17  --  *      *        192.168.64.16         192.168.64.10

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT    6  --  *      *        192.168.64.16         192.168.64.10

Chain OUTPUT (policy DROP 8 packets, 672 bytes)
 pkts bytes target     prot opt in     out     source               destination
fw@fw:~$
```

3.5 Permite el tráfico correspondiente a nuevas conexiones dirigidas hacia el servidor web (dmza), tanto accediendo por HTTP como por HTTPS.

Nuestro DMZA tiene la ip: 192.168.64.13

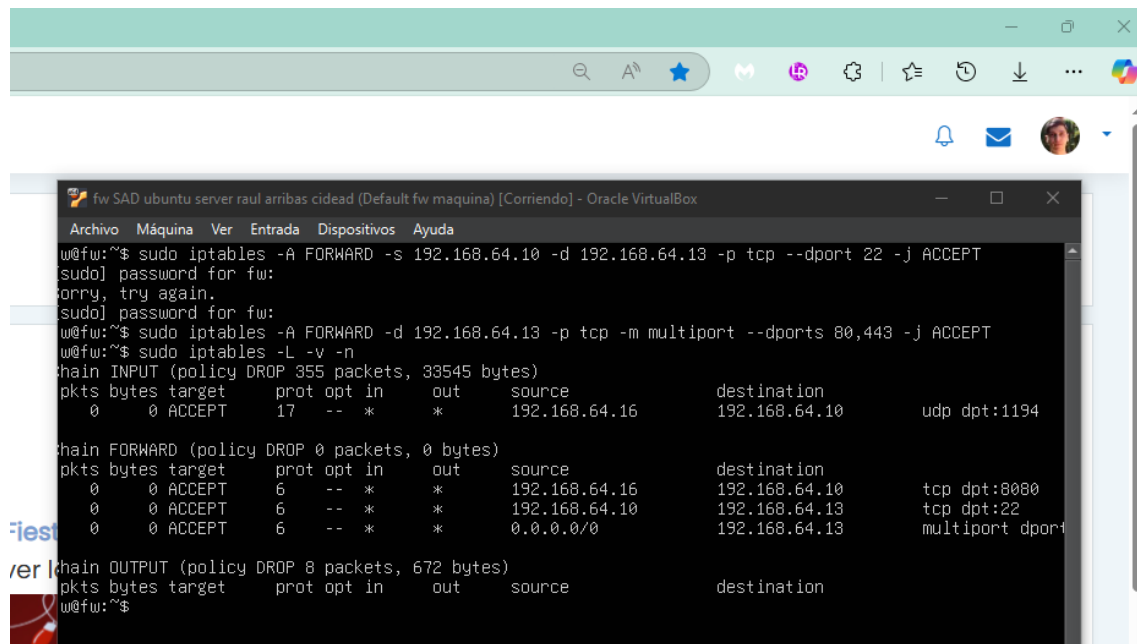
Vamos a permitir conexiones hacia el servidor web dmza, usando el túnel VPN, como SSH utiliza el puerto 22 vamos a habilitar este puerto.

Para conexiones HTTP Y HTTP habilitaremos los puertos 80 y 443.

sudo iptables -A FORWARD -s 192.168.64.10 -d 192.168.64.13 -p tcp --dport 22 -j ACCEPT

sudo iptables -A FORWARD -d 192.168.64.13 -p tcp -m multiport --dports 80,443 -j ACCEPT

Instalación y configuración de firewalls



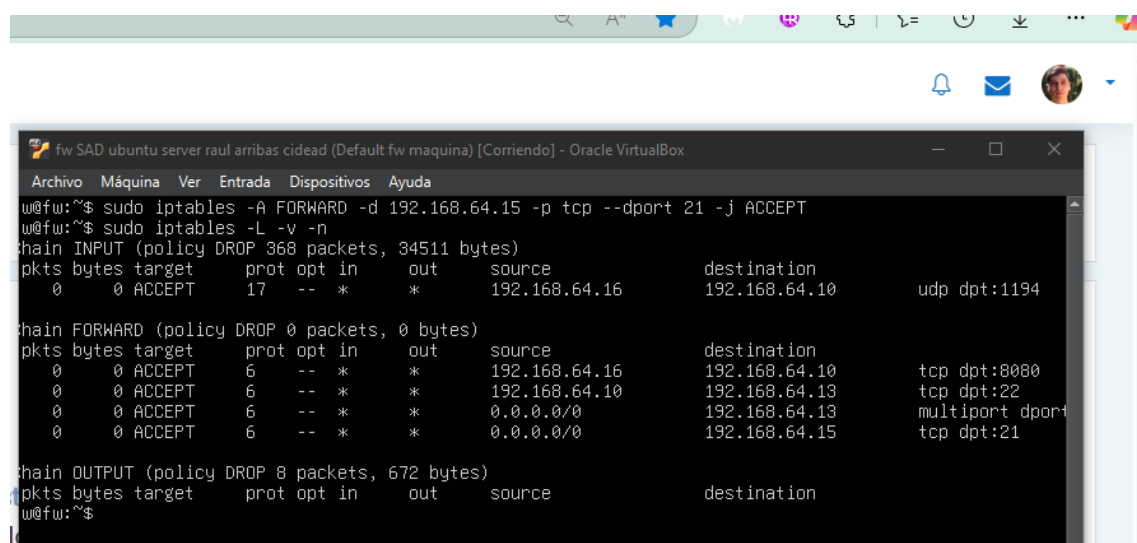
```
w@fw:~$ sudo iptables -A FORWARD -s 192.168.64.10 -d 192.168.64.13 -p tcp --dport 22 -j ACCEPT
[sudo] password for fw:
sorry, try again.
[sudo] password for fw:
w@fw:~$ sudo iptables -A FORWARD -d 192.168.64.13 -p tcp -m multiport --dports 80,443 -j ACCEPT
w@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 355 packets, 33545 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT     17  --  *      *        192.168.64.16        192.168.64.10        udp dpt:1194

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT     6  --  *      *        192.168.64.16        192.168.64.10        tcp dpt:8080
    0      0 ACCEPT     6  --  *      *        192.168.64.10        192.168.64.13        tcp dpt:22
    0      0 ACCEPT     6  --  *      *        0.0.0.0/0            192.168.64.13        multiport dport

Chain OUTPUT (policy DROP 8 packets, 672 bytes)
  pkts bytes target     prot opt in     out     source               destination
w@fw:~$
```

3.6 Permite el tráfico correspondiente a nuevas conexiones dirigidas hacia el servidor FTP (dmzb).

sudo iptables -A FORWARD -d 192.168.64.15 -p tcp --dport 21 -j ACCEPT



```
w@fw:~$ sudo iptables -A FORWARD -d 192.168.64.15 -p tcp --dport 21 -j ACCEPT
w@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 368 packets, 34511 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT     17  --  *      *        192.168.64.16        192.168.64.10        udp dpt:1194

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT     6  --  *      *        192.168.64.16        192.168.64.10        tcp dpt:8080
    0      0 ACCEPT     6  --  *      *        192.168.64.10        192.168.64.13        tcp dpt:22
    0      0 ACCEPT     6  --  *      *        0.0.0.0/0            192.168.64.13        multiport dport
    0      0 ACCEPT     6  --  *      *        0.0.0.0/0            192.168.64.15        tcp dpt:21

Chain OUTPUT (policy DROP 8 packets, 672 bytes)
  pkts bytes target     prot opt in     out     source               destination
w@fw:~$
```

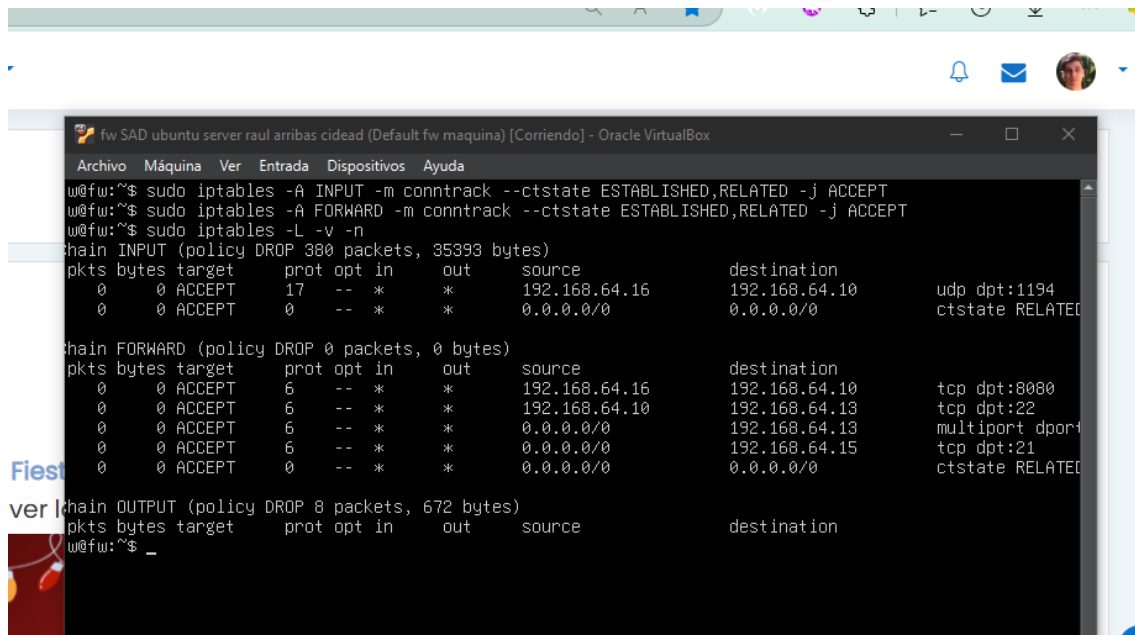
3.7 Permite el tráfico correspondiente a conexiones establecidas y/o relacionadas.

Esto nos asegurará que las respuestas a conexiones existentes sean permitidas:

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Instalación y configuración de firewalls



```
fw SAD ubuntu server raul arribas cidead (Default fw maquina) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
w@fw:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
w@fw:~$ sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
w@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 380 packets, 35393 bytes)
  pkts bytes target     prot opt in     out     source               destination
  0      0 ACCEPT    17  --  *      *       192.168.64.16        192.168.64.10      udp dpt:1194
  0      0 ACCEPT    0  --  *      *       0.0.0.0/0            0.0.0.0/0          ctstate RELATED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
  0      0 ACCEPT    6  --  *      *       192.168.64.16        192.168.64.10      tcp dpt:8080
  0      0 ACCEPT    6  --  *      *       192.168.64.10        192.168.64.13      tcp dpt:22
  0      0 ACCEPT    6  --  *      *       0.0.0.0/0            192.168.64.13      multiport dport
  0      0 ACCEPT    6  --  *      *       0.0.0.0/0            192.168.64.15      tcp dpt:21
  0      0 ACCEPT    0  --  *      *       0.0.0.0/0            0.0.0.0/0          ctstate RELATED

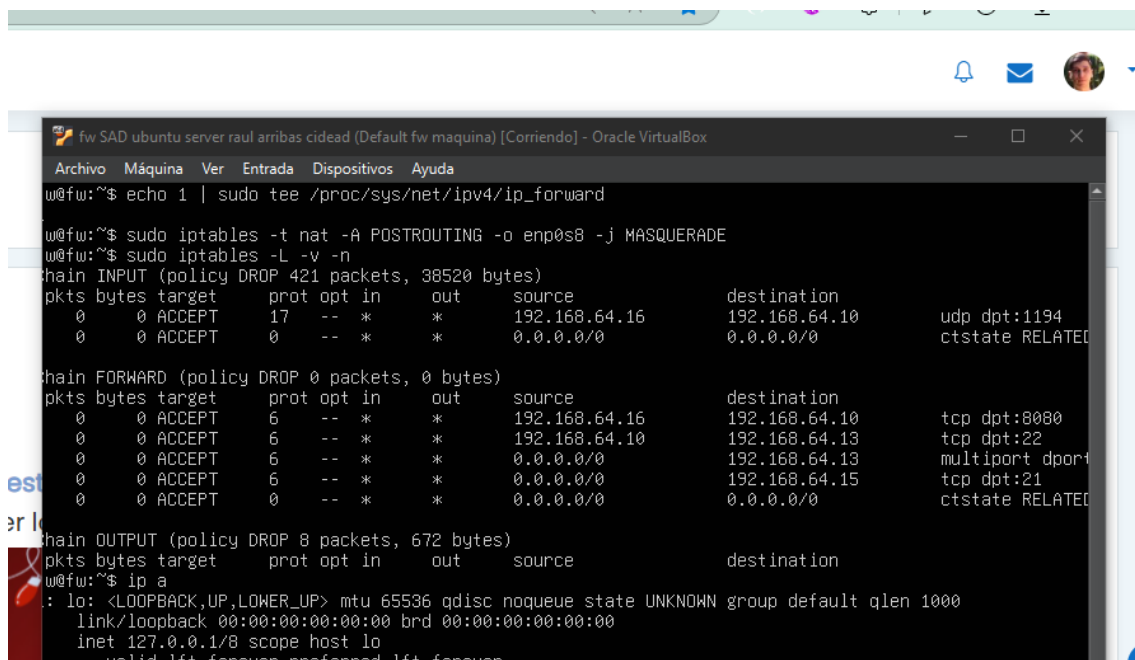
Chain OUTPUT (policy DROP 8 packets, 672 bytes)
  pkts bytes target     prot opt in     out     source               destination
w@fw:~$
```

3.8 Añade las reglas necesarias para ocultar la estructura interna de las redes.

Vamos a ocultar la red interna de la maquina fw:

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

sudo iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE



```
fw SAD ubuntu server raul arribas cidead (Default fw maquina) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
w@fw:~$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
w@fw:~$ sudo iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
w@fw:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 421 packets, 38520 bytes)
  pkts bytes target     prot opt in     out     source               destination
  0      0 ACCEPT    17  --  *      *       192.168.64.16        192.168.64.10      udp dpt:1194
  0      0 ACCEPT    0  --  *      *       0.0.0.0/0            0.0.0.0/0          ctstate RELATED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
  0      0 ACCEPT    6  --  *      *       192.168.64.16        192.168.64.10      tcp dpt:8080
  0      0 ACCEPT    6  --  *      *       192.168.64.10        192.168.64.13      tcp dpt:22
  0      0 ACCEPT    6  --  *      *       0.0.0.0/0            192.168.64.13      multiport dport
  0      0 ACCEPT    6  --  *      *       0.0.0.0/0            192.168.64.15      tcp dpt:21
  0      0 ACCEPT    0  --  *      *       0.0.0.0/0            0.0.0.0/0          ctstate RELATED

Chain OUTPUT (policy DROP 8 packets, 672 bytes)
  pkts bytes target     prot opt in     out     source               destination
w@fw:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
```

3.9 Haz que todas las reglas anteriores sean persistentes.

Para que las reglas no se pierdan al reiniciar, instalamos iptables-persistent, nos preguntará si guardamos las reglas que tenemos predefinidas de IPV e IPV6, le damos a aceptar.

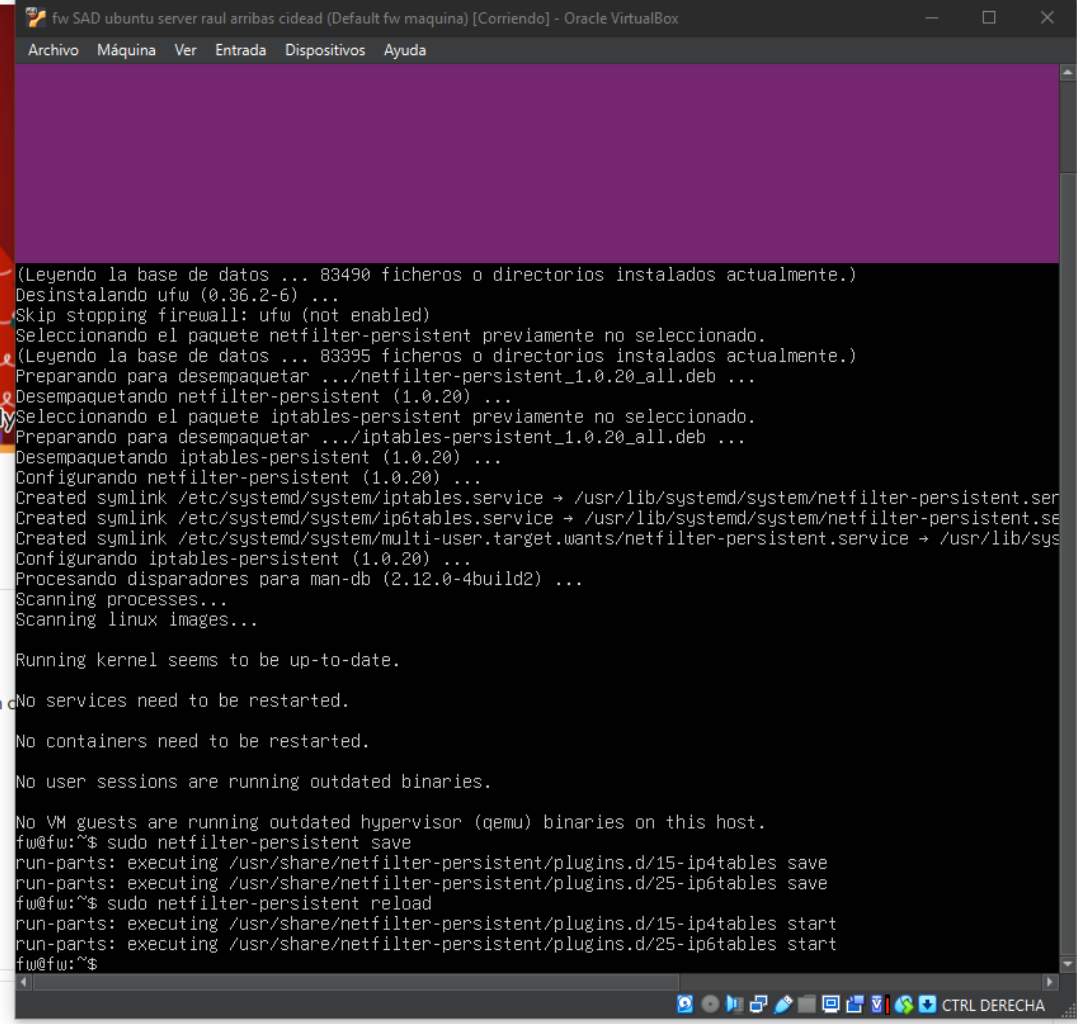
sudo apt install iptables-persistent

Y después ejecutamos los siguientes comandos para que se queden siempre activas aunque reiniciemos la maquina:

sudo netfilter-persistent save

sudo netfilter-persistent reload

Instalación y configuración de firewalls



```
fw SAD ubuntu server raul arribas cidead (Default fw maquina) [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

(Leyendo la base de datos ... 83490 ficheros o directorios instalados actualmente.)
Desinstalando ufw (0.36.2-6) ...
Skip stopping firewall: ufw (not enabled)
Seleccionando el paquete netfilter-persistent previamente no seleccionado.
(Leyendo la base de datos ... 83395 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../netfilter-persistent_1.0.20_all.deb ...
Desempaquetando netfilter-persistent (1.0.20) ...
Seleccionando el paquete iptables-persistent previamente no seleccionado.
Preparando para desempaquetar .../iptables-persistent_1.0.20_all.deb ...
Desempaquetando iptables-persistent (1.0.20) ...
Configurando netfilter-persistent (1.0.20) ...
Created symlink /etc/systemd/system/iptables.service → /usr/lib/systemd/system/netfilter-persistent.service
Created symlink /etc/systemd/system/ip6tables.service → /usr/lib/systemd/system/netfilter-persistent.service
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /usr/lib/systemd/system/netfilter-persistent.service
Configurando iptables-persistent (1.0.20) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
fw@fw:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
fw@fw:~$ sudo netfilter-persistent reload
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables start
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables start
fw@fw:~$
```

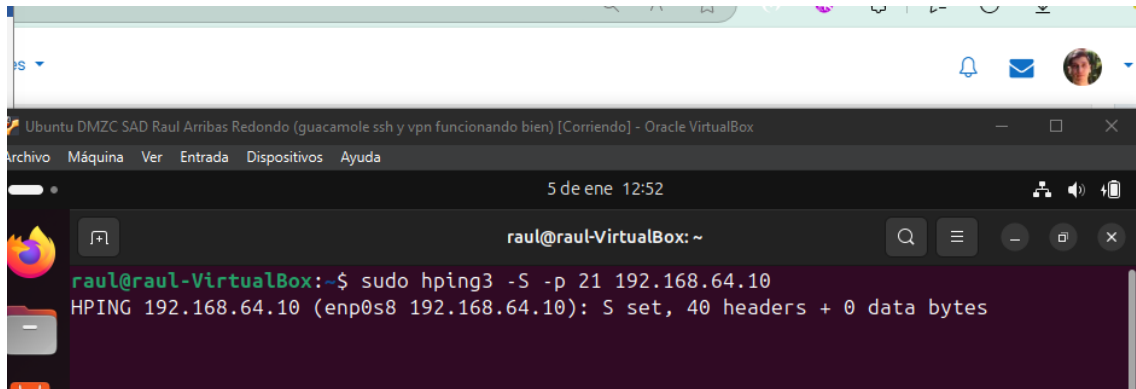
4 Uso de hping

4.1 Utiliza hping para verificar si el servicio FTP está activado y si se encuentra redireccionado en un host interno.

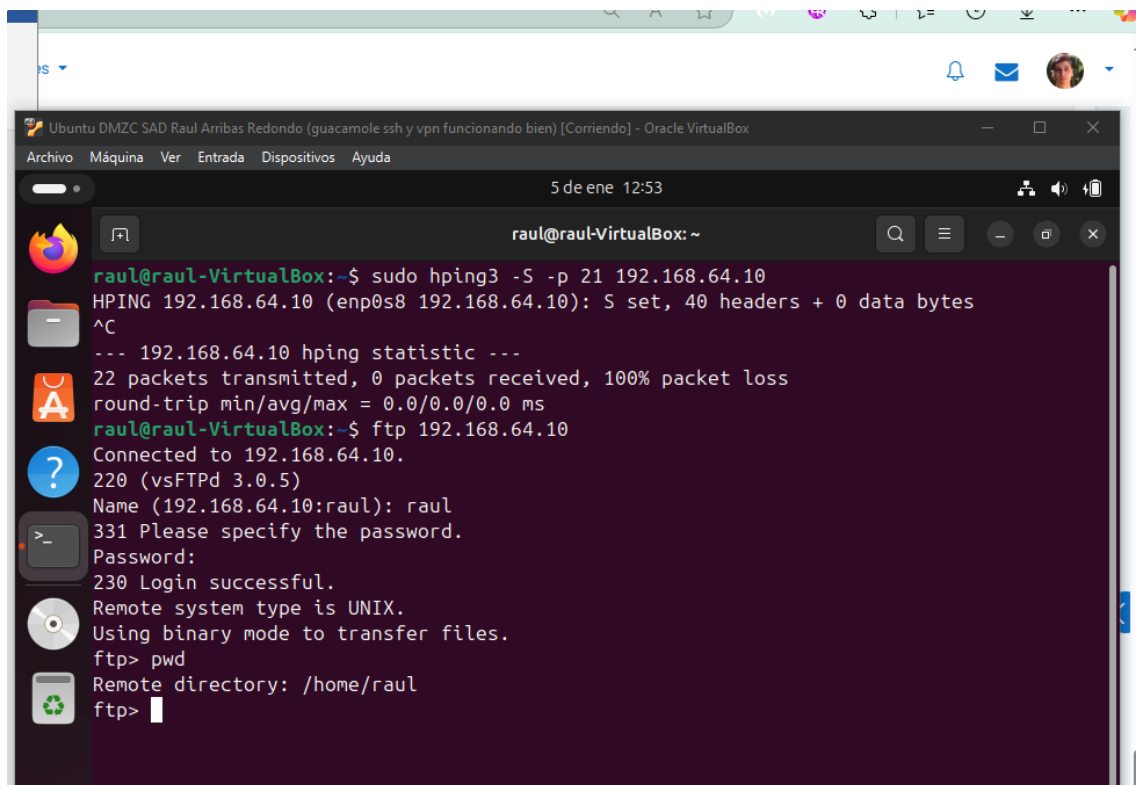
Vamos a usar hping para hacer un escaneo del puerto 21 en la dirección IP del host interno:

```
sudo hping3 -S -p 21 192.168.64.10
```

He intentado que esto funcione pero no hay manera, se queda así pensando, y el puerto 21 está funcionando bien.



A screenshot of a terminal window titled "raul@raul-VirtualBox: ~". The terminal shows the command `sudo hping3 -S -p 21 192.168.64.10` being executed. The output is `HPING 192.168.64.10 (enp0s8 192.168.64.10): S set, 40 headers + 0 data bytes`. The window's title bar indicates it's an Oracle VM VirtualBox window for "Ubuntu DMZC SAD Raul Arribas Redondo (guacamole ssh y vpn funcionando bien) [Corriendo]".



A screenshot of a terminal window titled "raul@raul-VirtualBox: ~". The terminal shows the command `sudo hping3 -S -p 21 192.168.64.10` being executed. The output is `HPING 192.168.64.10 (enp0s8 192.168.64.10): S set, 40 headers + 0 data bytes`. The user then presses `^C` and runs `hping statistic`, which shows `22 packets transmitted, 0 packets received, 100% packet loss` and `round-trip min/avg/max = 0.0/0.0/0.0 ms`. The user then runs `ftp 192.168.64.10`, which shows `Connected to 192.168.64.10.`, `220 (vsFTPd 3.0.5)`, `Name (192.168.64.10:raul): raul`, `331 Please specify the password.`, `Password:`, `230 Login successful.`, `Remote system type is UNIX.`, `Using binary mode to transfer files.`, `ftp> pwd`, `Remote directory: /home/raul`, and `ftp>`. The window's title bar indicates it's an Oracle VM VirtualBox window for "Ubuntu DMZC SAD Raul Arribas Redondo (guacamole ssh y vpn funcionando bien) [Corriendo]".