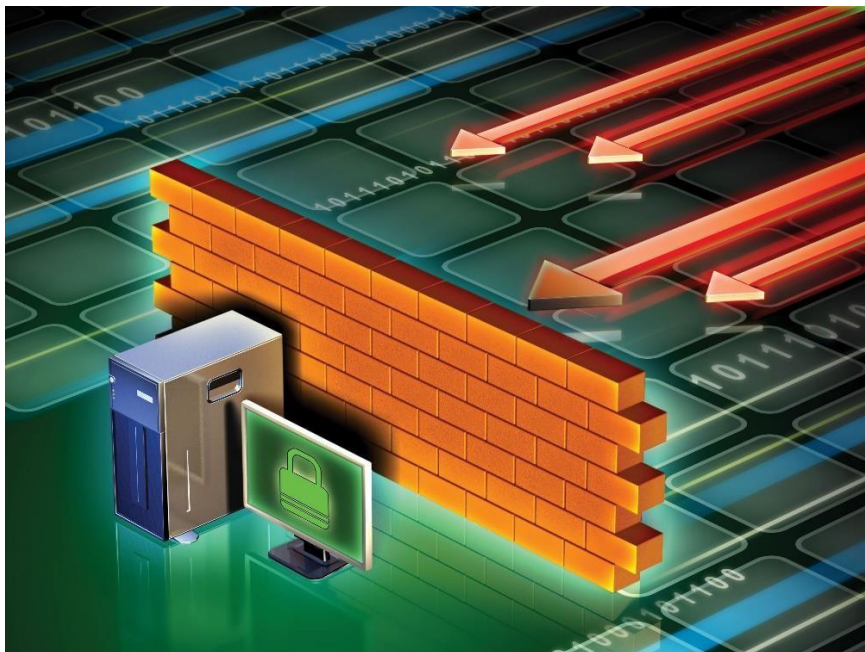


IES Valle Inclán



Configuración de IpTables como Firewall Local y Perimetral

Contenido

1 - Introducción a IpTables.....	3
2 - Firewall a nivel local.....	4
3 - Configuración de reglas	9
4 - IpTables como Cortafuegos Perimetral.....	21
5 - Configuración de Reglas	29
6 - Punto Extra.....	35

1 - Introducción a IpTables

En esta práctica vamos a configurar un Firewall en Linux. Primero se hará a nivel local y luego con una estructura de DMZ usándolo como cortafuegos perimetral.

Además, se configurará tanto con una política restrictiva en la que se irán añadiendo reglas para aceptar diferentes situaciones, como con una política permisiva en la que iremos estableciendo distintas reglas para negar.

El Firewall se centra básicamente en filtrar el tráfico de red, de manera que solo se permita el tráfico que cumpla con las reglas que hemos establecido. Para la práctica vamos a utilizar “IpTables” que ya viene por defecto con Linux en su propio Kernel, es decir viene por defecto sin tener que instalarlo.

Por defecto, en “IpTables”, tenemos 3 tipos de reglas o cadenas, que son INPUT, OUTPUT y FORWARD. Los demás parámetros que se utilizan se van explicando durante la práctica.

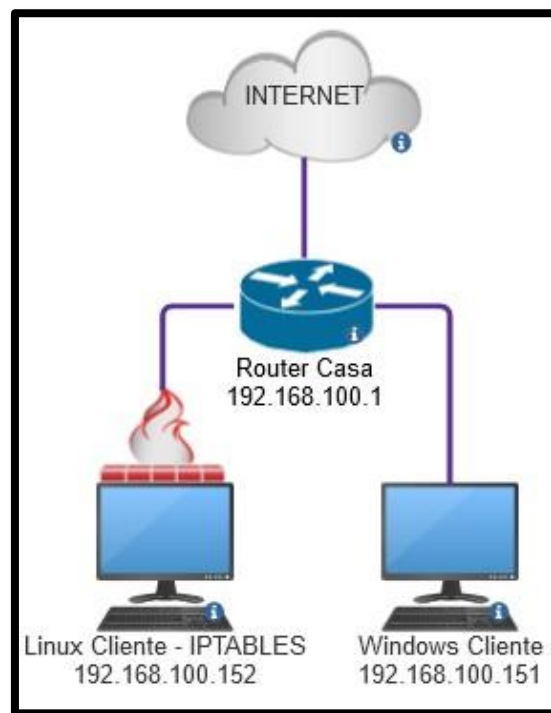
- INPUT: entrada. Es el tráfico que entra en el equipo/firewall, la dirección IP de destino es el equipo firewall.
- OUTPUT: salida. El tráfico saliente del equipo/firewall (lo hemos generado en nuestro equipo). En este caso, la dirección IP de origen del paquete es el equipo firewall.
- FORWARD: reenvío. Es tráfico que atraviesa/pasa por el firewall. Tanto el origen como el destino son equipos distintos al nuestro. Esta la veremos en la segunda parte utilizando IpTables como cortafuegos perimetral.

2 - Firewall a nivel local

Aquí lo utilizaremos a nivel local de usuario, con dos máquinas virtuales. La configuración de red será “adaptador puente”. Una de ellas será una distribución de Linux con “IpTables” y la otra una máquina de Windows. Configuraremos distintas reglas para hacer pruebas entre ellas.

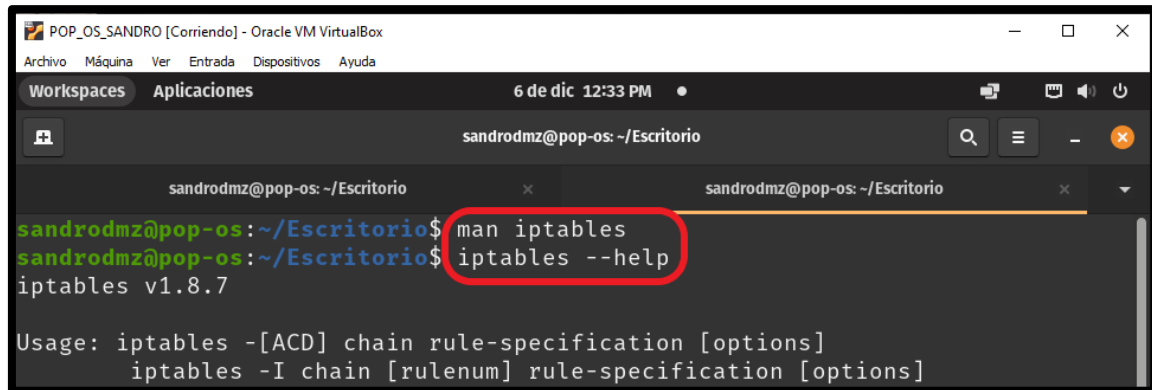
En esta primera parte aplicaremos por defecto la política restrictiva, que en mi opinión es la forma más segura de trabajar, aunque luego se usará también la permisiva en la segunda parte para poder ver las 2 políticas en la práctica.

Estructura de la red:



Firewall a nivel local

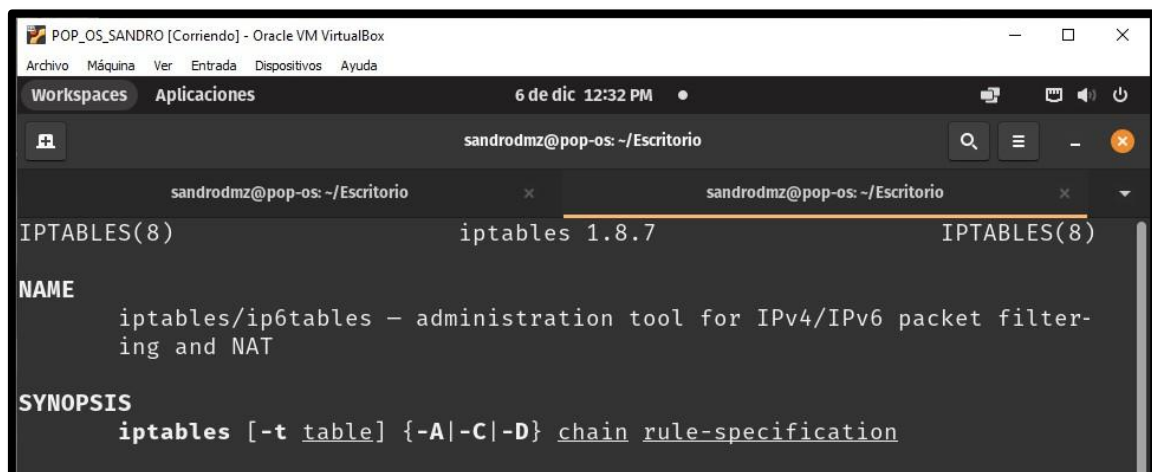
Lo primero que podemos hacer es comprobar que tenemos efectivamente el Firewall instalado. Para ello podemos usar tanto “man iptables” como “iptables --help”. Nos debería mostrar la ayuda en ambos casos:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Workspaces  Aplicaciones  6 de dic 12:33 PM
sandrodms@pop-os: ~/Escritorio

sandrodms@pop-os: ~/Escritorio
sandrodms@pop-os: ~/Escritorio$ man iptables
sandrodms@pop-os: ~/Escritorio$ iptables --help
iptables v1.8.7

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
```



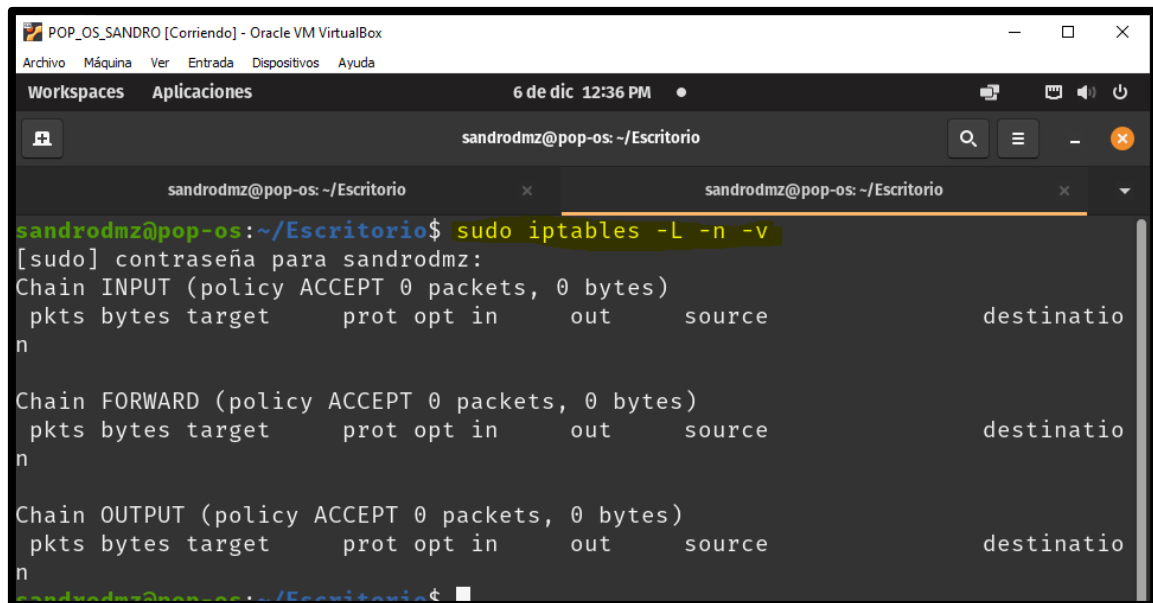
```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Workspaces  Aplicaciones  6 de dic 12:32 PM
sandrodms@pop-os: ~/Escritorio

sandrodms@pop-os: ~/Escritorio
sandrodms@pop-os: ~/Escritorio$ man iptables
IPTABLES(8)          iptables 1.8.7          IPTABLES(8)

NAME
    iptables/ip6tables - administration tool for IPv4/IPv6 packet filter-
    ing and NAT

SYNOPSIS
    iptables [-t table] {-A|-C|-D} chain rule-specification
```

Para poder ver las reglas configuradas usamos “iptables -L -n -v”. Con “-L” listas todas las cadenas, “-n” porque no tenemos servidor DNS y se verán directamente las direcciones luego cuando pongamos reglas. Y “-v” es para que te dé más información, es la típica opción de “verbose”. Por defecto tenemos todas las cadenas como “PERMITIDO”:



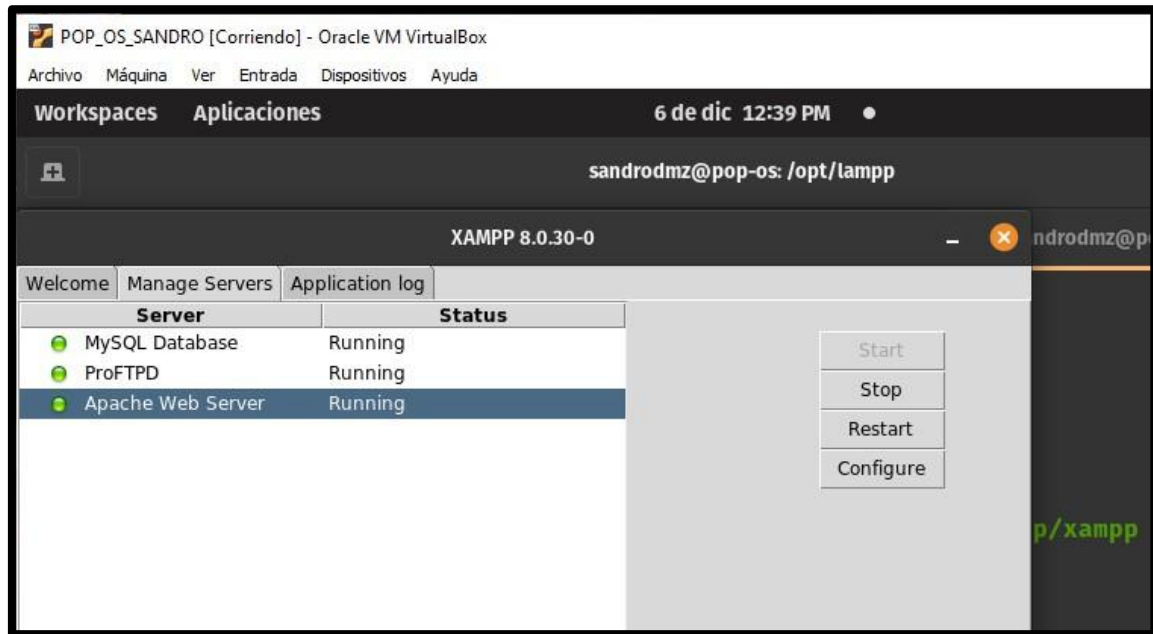
```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Workspaces  Aplicaciones  6 de dic 12:36 PM
sandrodmz@pop-os: ~/Escritorio

sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os: ~/Escritorio$ sudo iptables -L -n -v
[sudo] contraseña para sandrodmz:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
```

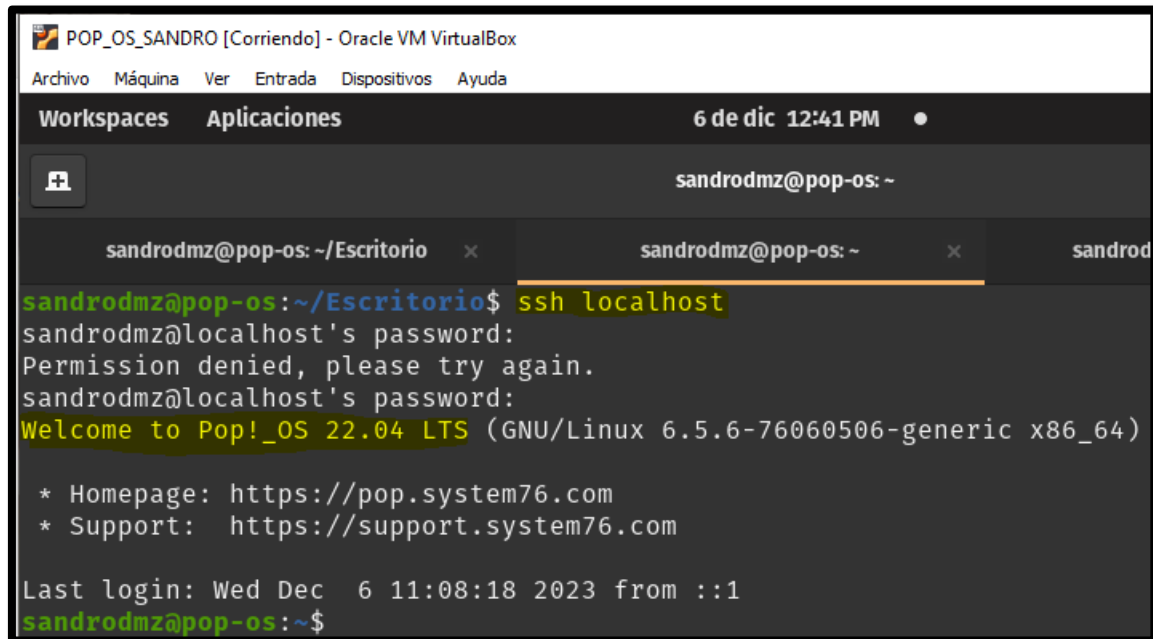
Ahora haremos una serie de comprobaciones de las cosas que he instalado para luego poder establecer reglas y cortarlas. Lo podemos hacer todo ya que por defecto lo tenemos permitido.

En esta máquina tenemos un servidor web apache, y un servidor ssh.

Servidor Web:



Servidor SSH:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Workspaces  Aplicaciones  6 de dic 12:41 PM

sandrodmz@pop-os: ~

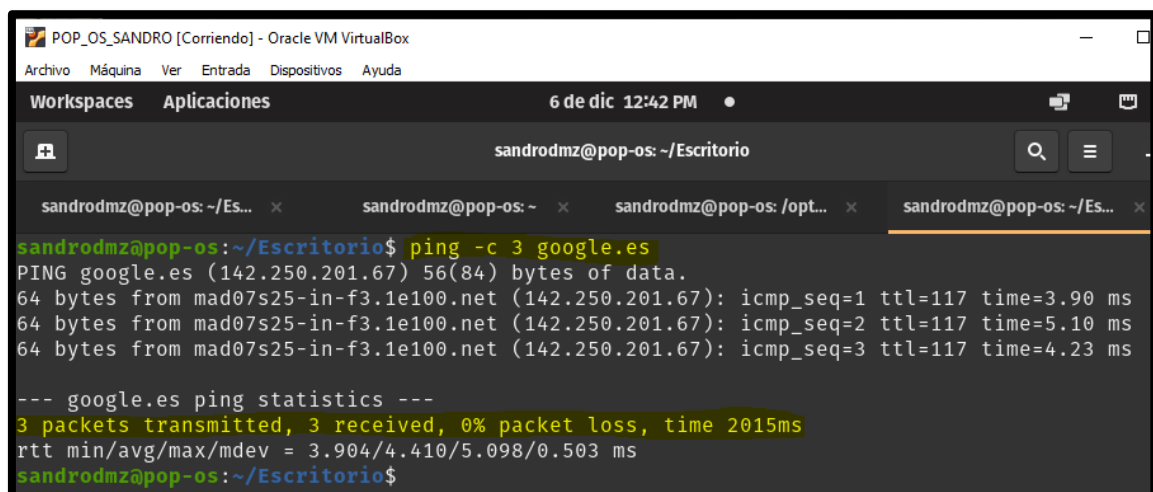
sandrodmz@pop-os: ~/Escritorio x sandrodmz@pop-os: ~ x sandrodmz@pop-os: ~

sandrodmz@pop-os:~/Escritorio$ ssh localhost
sandrodmz@localhost's password:
Permission denied, please try again.
sandrodmz@localhost's password:
Welcome to Pop!_OS 22.04 LTS (GNU/Linux 6.5.6-76060506-generic x86_64)

* Homepage: https://pop.system76.com
* Support: https://support.system76.com

Last login: Wed Dec 6 11:08:18 2023 from ::1
sandrodmz@pop-os:~$
```

También comprobamos que tenemos salida a internet:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Workspaces  Aplicaciones  6 de dic 12:42 PM

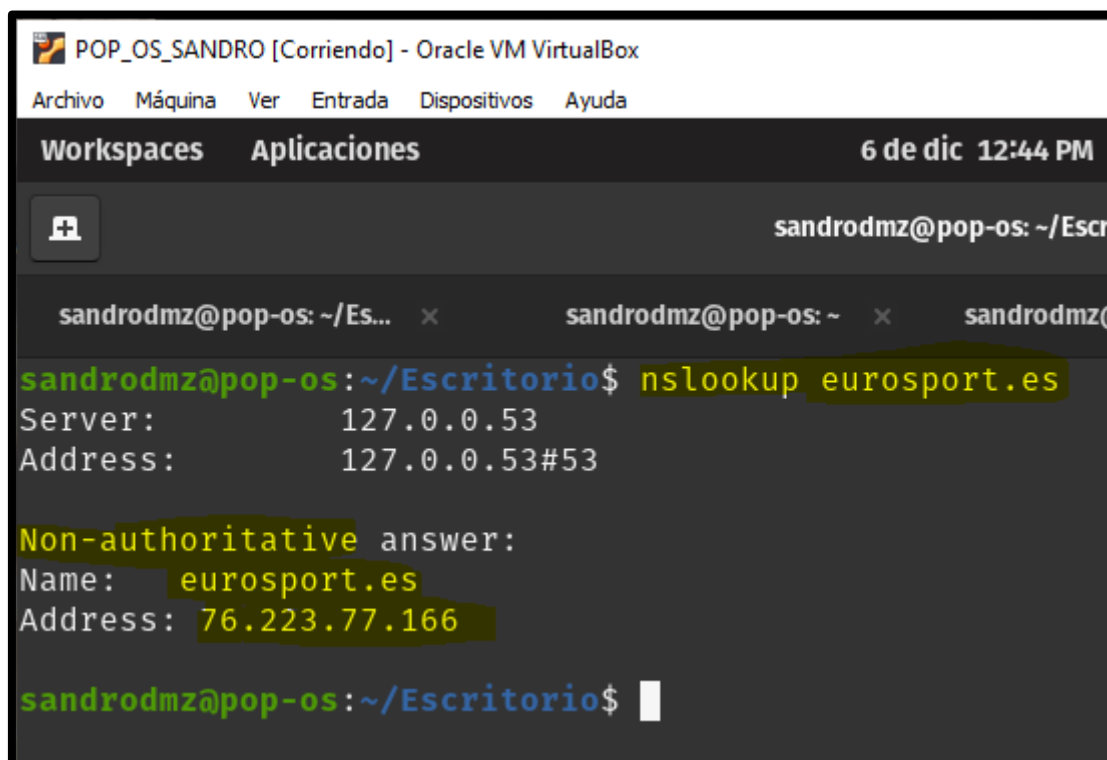
sandrodmz@pop-os: ~/Escritorio

sandrodmz@pop-os: ~/Es... x sandrodmz@pop-os: ~ x sandrodmz@pop-os: /opt... x sandrodmz@pop-os: ~/Es... x

sandrodmz@pop-os:~/Escritorio$ ping -c 3 google.es
PING google.es (142.250.201.67) 56(84) bytes of data.
64 bytes from mad07s25-in-f3.1e100.net (142.250.201.67): icmp_seq=1 ttl=117 time=3.90 ms
64 bytes from mad07s25-in-f3.1e100.net (142.250.201.67): icmp_seq=2 ttl=117 time=5.10 ms
64 bytes from mad07s25-in-f3.1e100.net (142.250.201.67): icmp_seq=3 ttl=117 time=4.23 ms

--- google.es ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 3.904/4.410/5.098/0.503 ms
sandrodmz@pop-os:~/Escritorio$
```


Y podemos resolver nombres:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Workspaces  Aplicaciones  6 de dic 12:44 PM
sandrodmz@pop-os: ~/Escr
sandrodmz@pop-os: ~/Es... x sandrodmz@pop-os: ~ x sandrodmz@
sandrodmz@pop-os:~/Escritorio$ nslookup eurosport.es
Server:          127.0.0.53
Address:         127.0.0.53#53

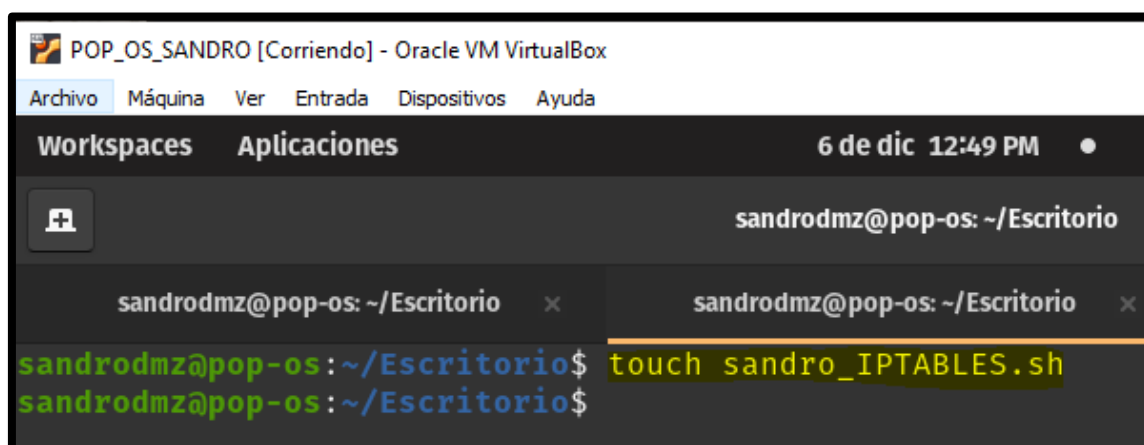
Non-authoritative answer:
Name:   eurosport.es
Address: 76.223.77.166

sandrodmz@pop-os:~/Escritorio$
```

3 - Configuración de reglas

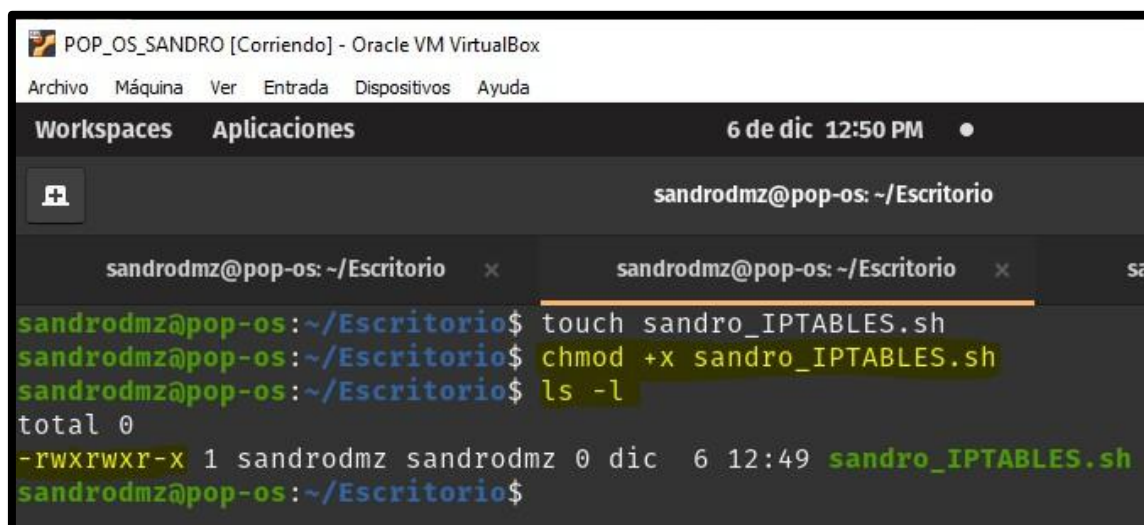
Lo que vamos a hacer es trabajar mediante un script ya que todo lo que hagamos va a ser mediante comandos del firewall.

Creamos un script, por ejemplo, en el escritorio:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Workspaces  Aplicaciones  6 de dic 12:49 PM
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os: ~/Escritorio x sandrodmz@pop-os: ~/Escritorio x
sandrodmz@pop-os:~/Escritorio$ touch sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio$
```

Le damos permisos de ejecución:



```
POP_OS_SANDRO [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Workspaces  Aplicaciones  6 de dic 12:50 PM

sandrodmz@pop-os: ~/Escritorio

sandrodmz@pop-os: ~/Escritorio x  sandrodmz@pop-os: ~/Escritorio x  sa
sandrodmz@pop-os:~/Escritorio$ touch sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio$ chmod +x sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio$ ls -l
total 0
-rwxrwxr-x 1 sandrodmz sandrodmz 0 dic  6 12:49 sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio$
```

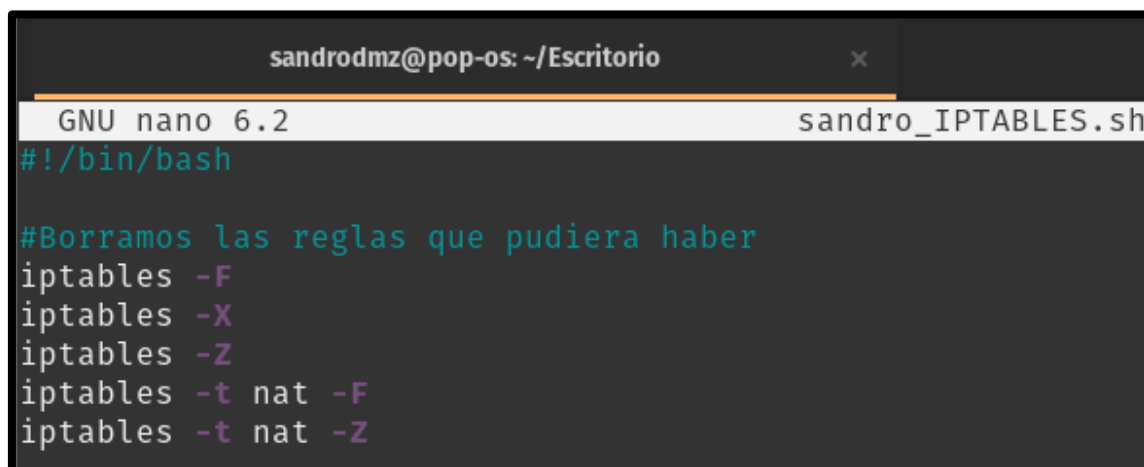
Ahora lo que vamos a hacer es trabajar con una política “RESTRICTIVA”. Todo estará denegado y solo vamos a permitir lo que nosotros establezcamos de manera explícita.

Tenemos 3 tipos de tablas principalmente que son MANGLE, NAT y FILTER.

- MANGLE: estas son para reglas que permitan modificar diversos campos de los paquetes. Son conceptos muy avanzados que no se van a ver aquí.
- NAT: para la traducción de direcciones de red y son útiles para el reenvío de puertos o el enmascaramiento. Se puede usar por ejemplo para dar salida a Internet a las máquinas en la segunda parte.
- FILTER: es la que se usa por defecto y sirve para establecer las reglas de filtrado. Es la más utilizada y la que usa por defecto si no estableces ninguna tabla.

Lo primero es limpiar las posibles reglas que pudiera haber de antes. Con la opción “-F” borramos todas las reglas de una cadena. Con “-X” borramos cadenas vacías. También es siempre recomendable hacerlo con la NAT por si tuviéramos algo, por eso se utiliza la opción “-t” para pasar una tabla de reglas en concreto. Por último, con la opción “-Z” limpiarías los contadores de las reglas, pero este es opcional.

Además, si no especificas por defecto se van a hacer sobre “FILTER”, por eso las primeras no especifico:



```
sandrodmz@pop-os: ~/Escritorio
GNU nano 6.2 sandro_IPTABLES.sh
#!/bin/bash

#Borramos las reglas que pudiera haber
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -Z
```

Ahora lo que vamos a hacer es establecer por defecto la política restrictiva. Estas son las que se van a aplicar cuando no se cumpla ninguna de las reglas, con la opción “-P”, de manera que denegamos todo el tráfico en las 3 cadenas. Para denegar se usa “DROP” y para aceptar se usa “ACCEPT”:

```
sandrodmz@pop-os: ~/Escritorio
GNU nano 6.2 sandro_IPTABLES.sh
#!/bin/bash

#Borramos las reglas que pudiera haber
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -Z

#Política restrictiva por defecto (DENIEGO TODO)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Ahora podríamos comprobar ejecutando el script con permisos de superusuario ya que es necesario para utilizar la herramienta “IpTables”:

```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os: ~/Escritorio$ nano sandro_IPTABLES.sh
sandrodmz@pop-os: ~/Escritorio$ sudo ./sandro_IPTABLES.sh
sandrodmz@pop-os: ~/Escritorio$
```

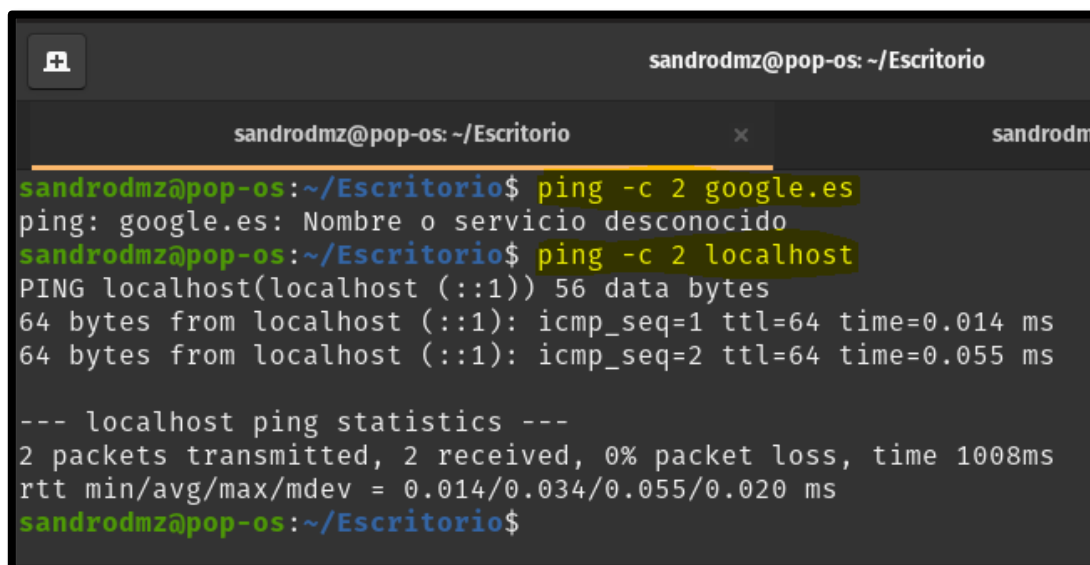
Volvemos a listar las reglas y veremos que tenemos la política por defecto de las 3 cadenas en modo “DENEGAR/DROP”:

```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os: ~/Escritorio$ sudo iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 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 5 packets, 534 bytes)
 pkts bytes target    prot opt in     out     source    destination
sandrodmz@pop-os: ~/Escritorio$
```

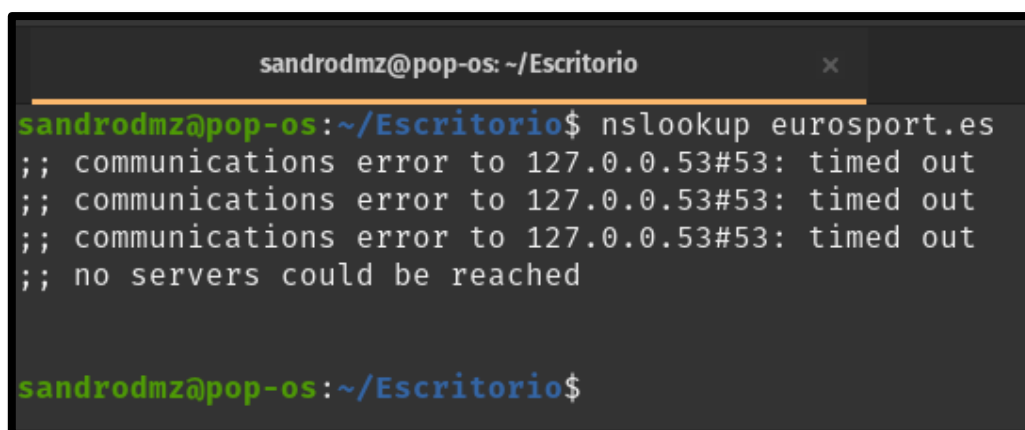
Ahora podemos ver que no tenemos salida a Internet:



```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os:~/Escritorio$ ping -c 2 google.es
ping: google.es: Nombre o servicio desconocido
sandrodmz@pop-os:~/Escritorio$ ping -c 2 localhost
PING localhost (localhost (:::1)) 56 data bytes
64 bytes from localhost (:::1): icmp_seq=1 ttl=64 time=0.014 ms
64 bytes from localhost (:::1): icmp_seq=2 ttl=64 time=0.055 ms

--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.014/0.034/0.055/0.020 ms
sandrodmz@pop-os:~/Escritorio$
```

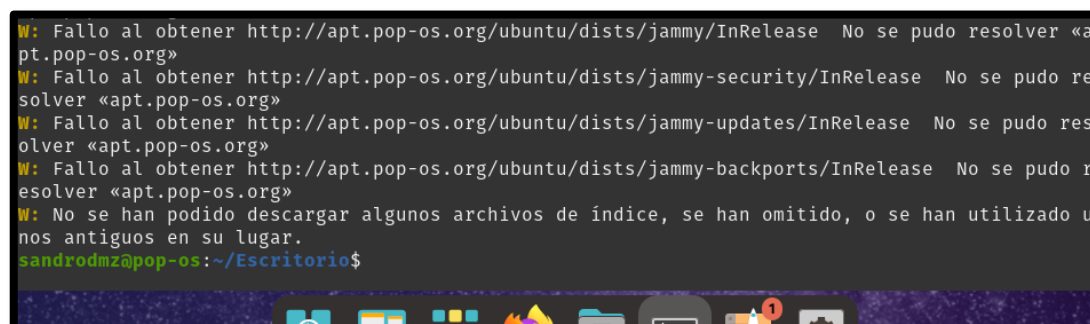
De igual modo no tenemos resolución de nombres:



```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os:~/Escritorio$ nslookup eurosport.es
;; communications error to 127.0.0.53#53: timed out
;; communications error to 127.0.0.53#53: timed out
;; communications error to 127.0.0.53#53: timed out
;; no servers could be reached

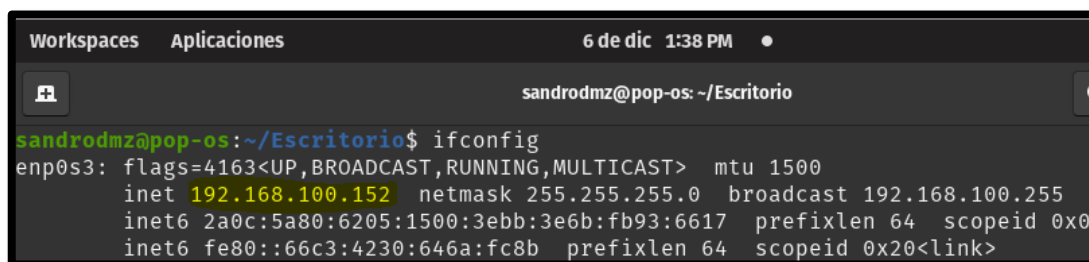
sandrodmz@pop-os:~/Escritorio$
```

Ni podremos actualizar los repositorios con “apt”:



```
W: Fallo al obtener http://apt.pop-os.org/ubuntu/dists/jammy/InRelease No se pudo resolver «apt.pop-os.org»
W: Fallo al obtener http://apt.pop-os.org/ubuntu/dists/jammy-security/InRelease No se pudo resolver «apt.pop-os.org»
W: Fallo al obtener http://apt.pop-os.org/ubuntu/dists/jammy-updates/InRelease No se pudo resolver «apt.pop-os.org»
W: Fallo al obtener http://apt.pop-os.org/ubuntu/dists/jammy-backports/InRelease No se pudo resolver «apt.pop-os.org»
W: No se han podido descargar algunos archivos de índice, se han omitido, o se han utilizado unos antiguos en su lugar.
sandrodmz@pop-os:~/Escritorio$
```

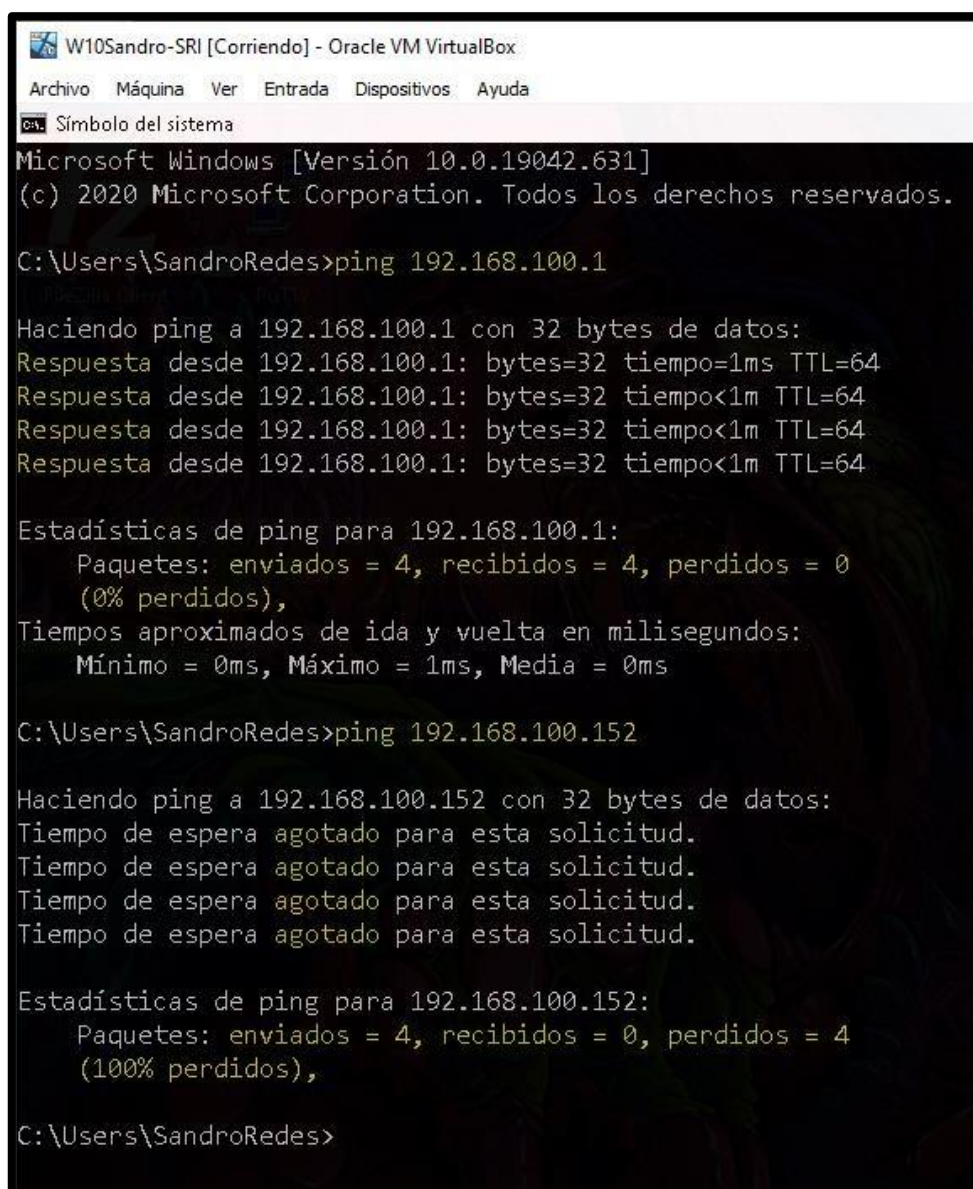
Ahora miramos la dirección IP:



```
Workspaces  Aplicaciones  6 de dic  1:38 PM  ●
sandrodmz@pop-os: ~/Escritorio

sandrodmz@pop-os:~/Escritorio$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.152  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 2a0c:5a80:6205:1500:3ebb:3e6b:fb93:6617  prefixlen 64  scopeid 0x0
        inet6 fe80::66c3:4230:646a:fc8b  prefixlen 64  scopeid 0x20<link>
```

Intentamos hacerle ping con otra máquina y veremos que el firewall lo corta, pero sí llegamos a la puerta de enlace:



```
W10Sandro-SRI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
0% Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.631]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\SandroRedes>ping 192.168.100.1

Haciendo ping a 192.168.100.1 con 32 bytes de datos:
Respuesta desde 192.168.100.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.100.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.100.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.100.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.100.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

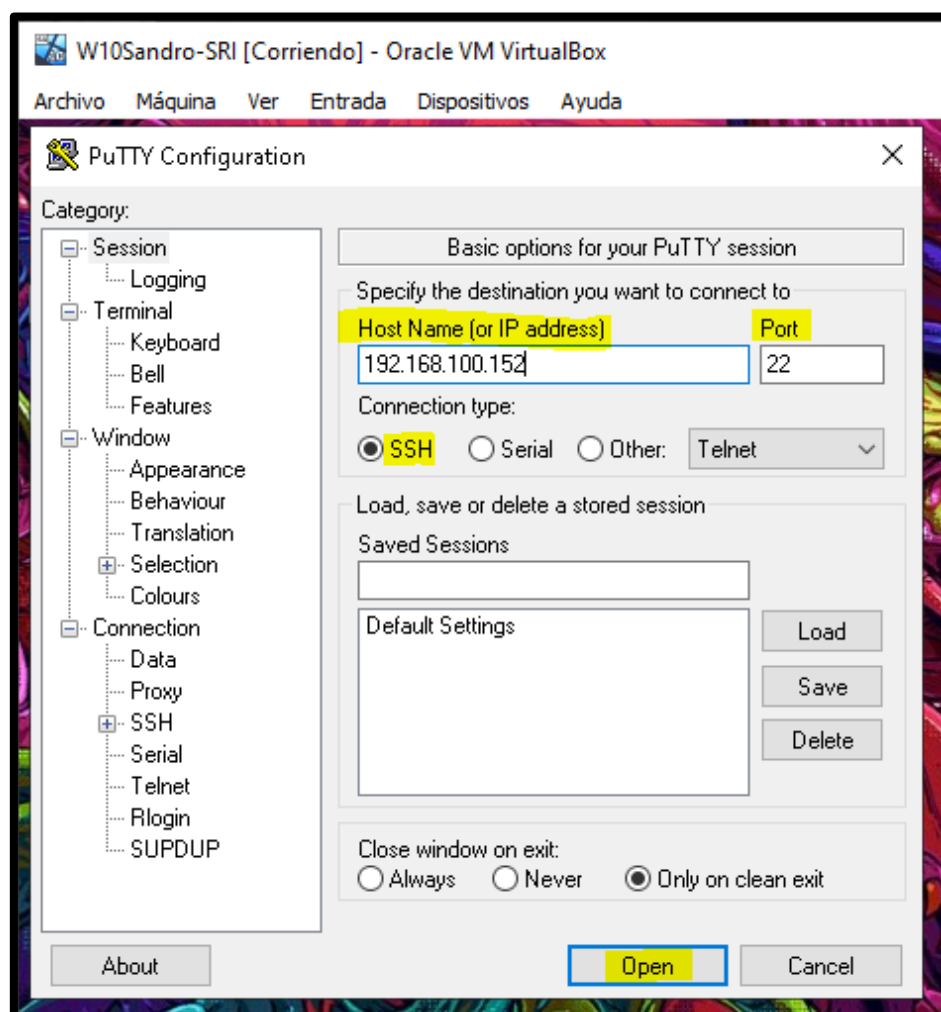
C:\Users\SandroRedes>ping 192.168.100.152

Haciendo ping a 192.168.100.152 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.100.152:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
        (100% perdidos),

C:\Users\SandroRedes>
```

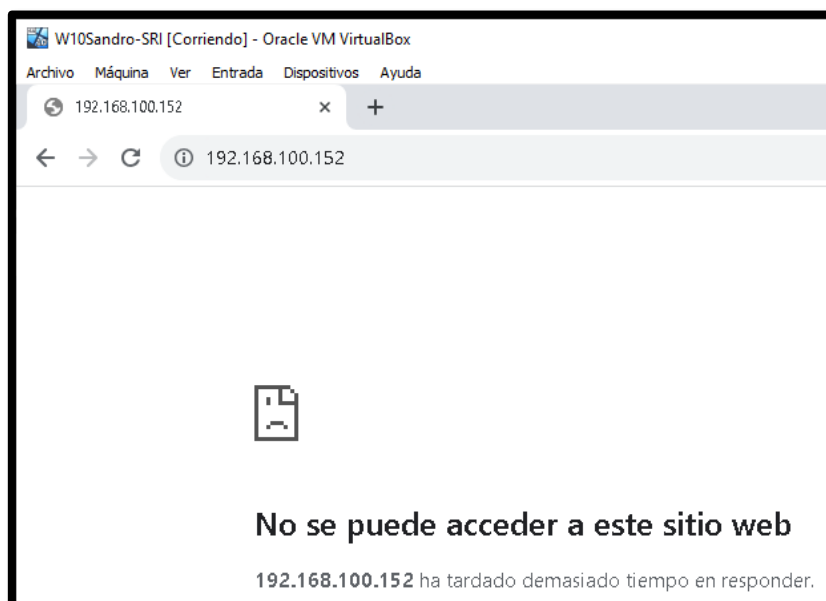
Y si intentamos por SSH:



Tampoco nos va a dejar:



Al servidor web tampoco:



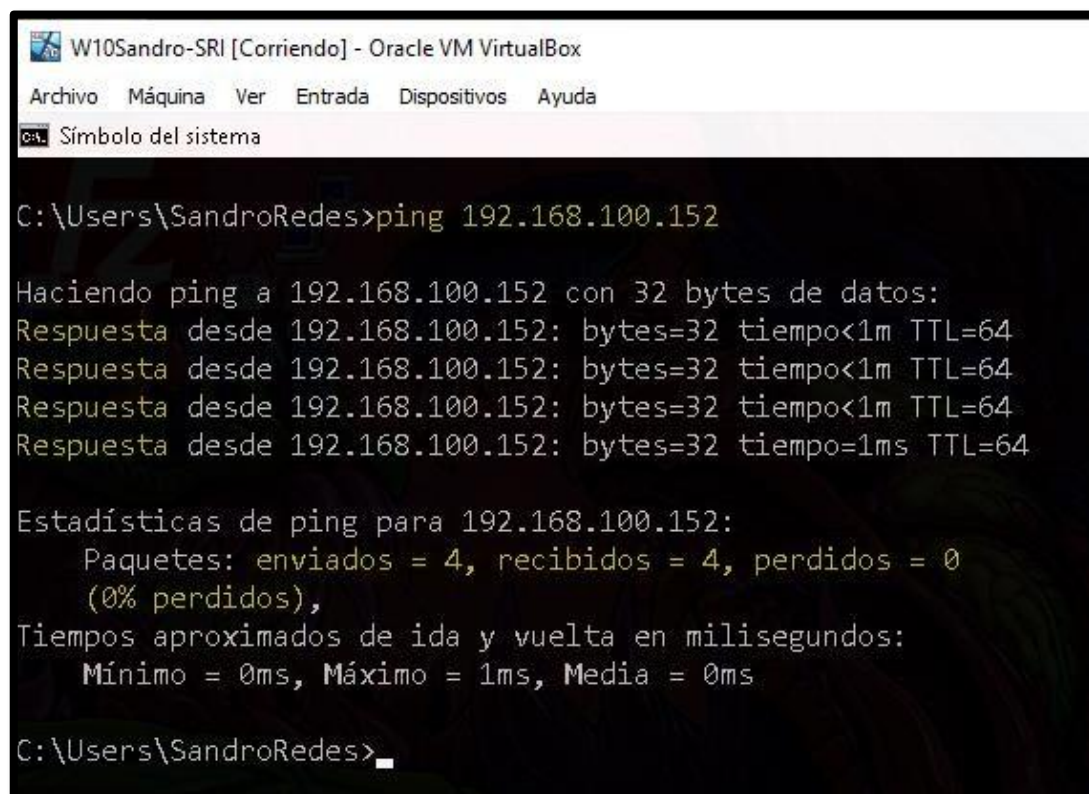
Empezamos creando una regla que permita el ping solo desde el cliente "192.168.100.151". "-i" es para indicarle la interfaz de red. "-s" es la dirección de origen del paquete. "-d" para la dirección destino. "-p" es filtrar el protocolo. Y "-j" es la acción "PERMITIR/DENEGAR":

```
# Permito PING solo desde la máquina CLIENTE 192.168.100.151
iptables -A INPUT -i enp0s3 -s 192.168.100.151 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p icmp --icmp-type echo-reply -j ACCEPT
```

Y lo ejecutamos:

A screenshot of a terminal window with the prompt "sandrodmz@pop-os: ~/Escritorio". The user enters the following commands:
sandrodmz@pop-os:~/Escritorio\$ nano sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio\$ sudo ./sandro_IPTABLES.sh
sandrodmz@pop-os:~/Escritorio\$

Entonces ahora SI se puede hacer ping desde la máquina cliente:



```
W10Sandro-SRI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
C:\> Símbolo del sistema

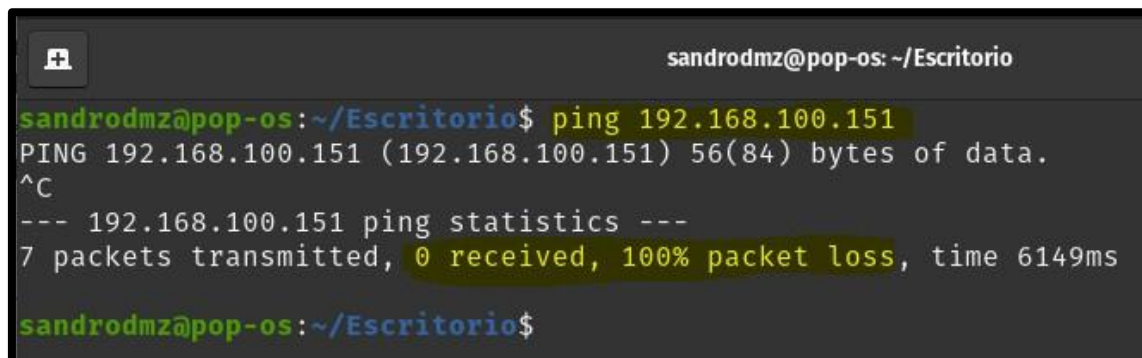
C:\Users\SandroRedes>ping 192.168.100.152

Haciendo ping a 192.168.100.152 con 32 bytes de datos:
Respuesta desde 192.168.100.152: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.100.152: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.100.152: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.100.152: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.100.152:
    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\SandroRedes>
```

Pero NO desde la máquina Linux:



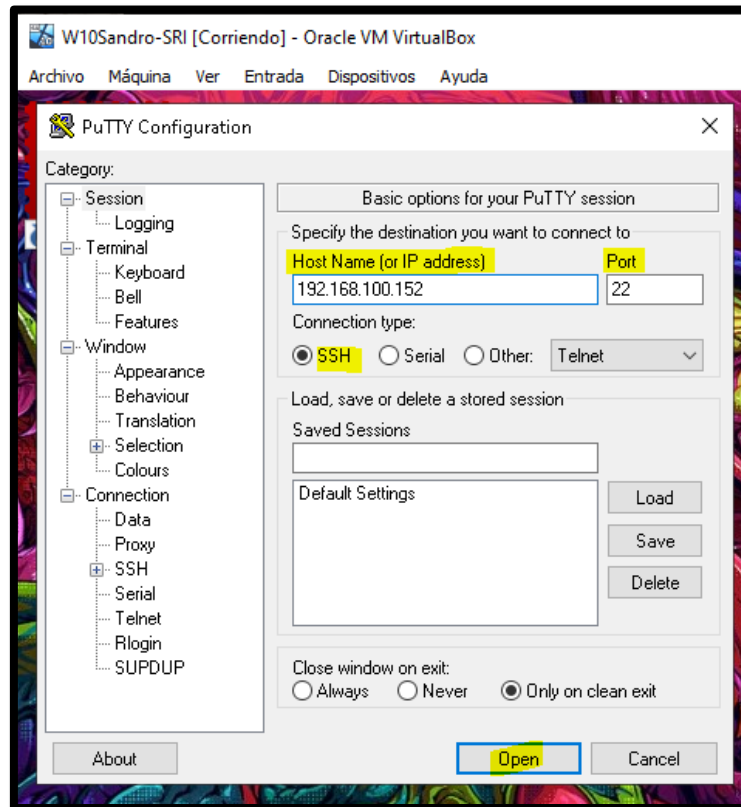
```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os:~/Escritorio$ ping 192.168.100.151
PING 192.168.100.151 (192.168.100.151) 56(84) bytes of data.
^C
--- 192.168.100.151 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6149ms

sandrodmz@pop-os:~/Escritorio$
```

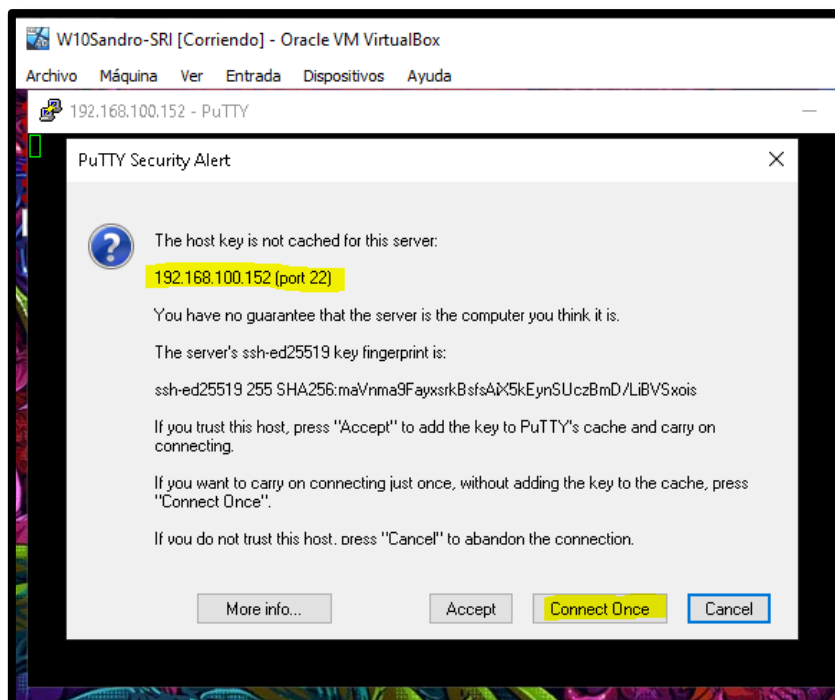
Ahora permitimos el SSH desde la máquina cliente. NOTA: He tenido que permitir el TCP porque "ssh" como parámetro de "-p" no te lo reconoce:

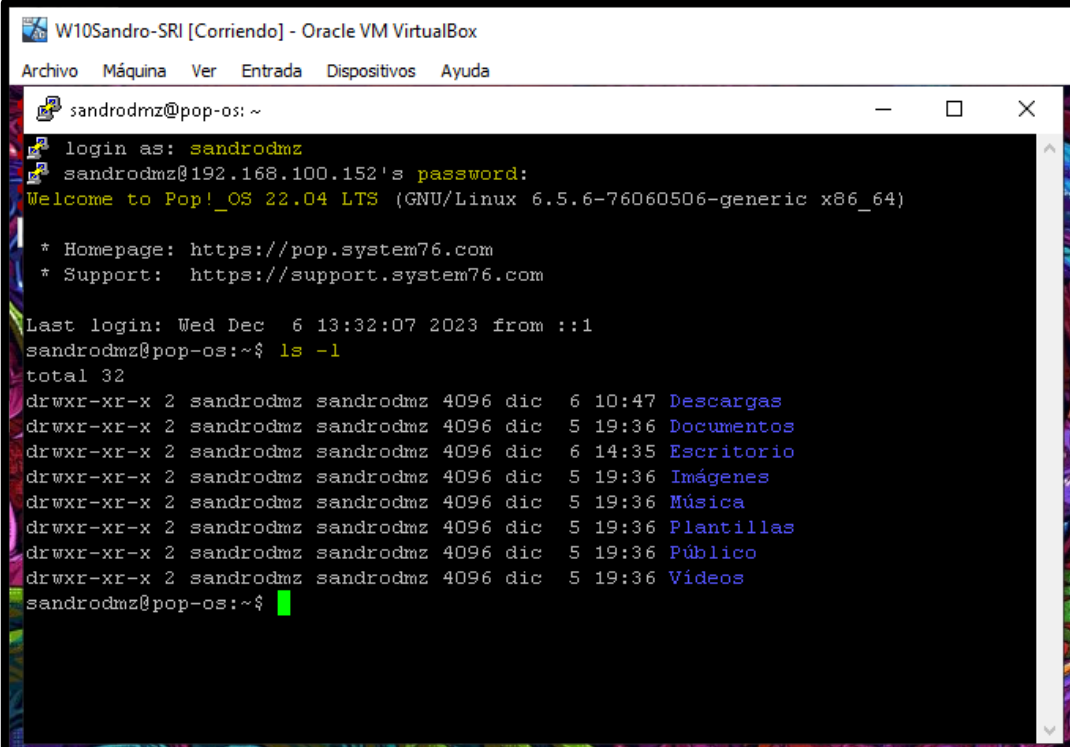
```
# Permitir conexiones SSH desde la máquina CLIENTE 192.168.100.151
iptables -A INPUT -s 192.168.100.151 -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p tcp -j ACCEPT
```

Creamos de nuevo una conexión desde PuTTY:



Y ahora Sí nos funciona:





```
W10Sandro-SRI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

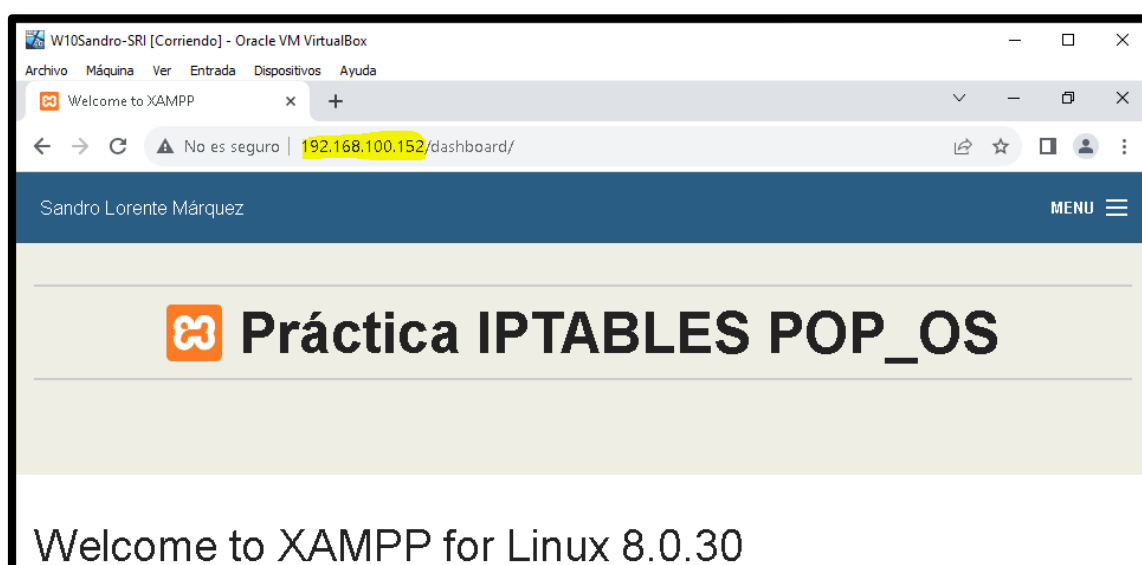
sandrodmz@pop-os: ~
login as: sandrodmz
sandrodmz@192.168.100.152's password:
Welcome to Pop!_OS 22.04 LTS (GNU/Linux 6.5.6-76060506-generic x86_64)

* Homepage: https://pop.system76.com
* Support: https://support.system76.com

Last login: Wed Dec  6 13:32:07 2023 from ::1
sandrodmz@pop-os:~$ ls -l
total 32
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  6 10:47 Descargas
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Documentos
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  6 14:35 Escritorio
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Imágenes
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Música
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Plantillas
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Público
drwxr-xr-x 2 sandrodmz sandrodmz 4096 dic  5 19:36 Vídeos
sandrodmz@pop-os:~$
```

Y para acabar, permitimos que desde el cliente “192.168.100.151” se pueda acceder al servidor web:

```
#Permitir conexiones al servidor web apache desde CLIENTE 192.168.100.151
iptables -A INPUT -s 192.168.100.151 -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p tcp -j ACCEPT
```



Aquí finalizo este apartado y te muestro el script al completo:

```
Workspaces Aplicaciones 6 de dic 2:44 PM
sandrodmz@pop-os: ~/Escritorio
GNU nano 6.2 sandro_IPTABLES.sh
#!/bin/bash

#Borramos las reglas que pudiera haber
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -Z

#Política restrictiva por defecto (DENIEGO TODO)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Permiso PING solo desde la máquina CLIENTE 192.168.100.151
iptables -A INPUT -i enp0s3 -s 192.168.100.151 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p icmp --icmp-type echo-reply -j ACCEPT

# Permitir conexiones SSH desde la máquina CLIENTE 192.168.100.151
iptables -A INPUT -s 192.168.100.151 -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p tcp -j ACCEPT

#Permitir conexiones al servidor web apache desde CLIENTE 192.168.100.151
iptables -A INPUT -s 192.168.100.151 -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -d 192.168.100.151 -p tcp -j ACCEPT
```

Y el estado en el firewall:

```
Workspaces Aplicaciones 6 de dic 2:47 PM
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os:~/Escritorio$ sudo iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
  0      0 ACCEPT    icmp -- enp0s3 *    192.168.100.151      0.0.0.0/0            icmpt
type 8
  0      0 ACCEPT    tcp  -- *    *    192.168.100.151      0.0.0.0/0            tcp d
pt:22
  0      0 ACCEPT    tcp  -- *    *    192.168.100.151      0.0.0.0/0            tcp d
pt:80

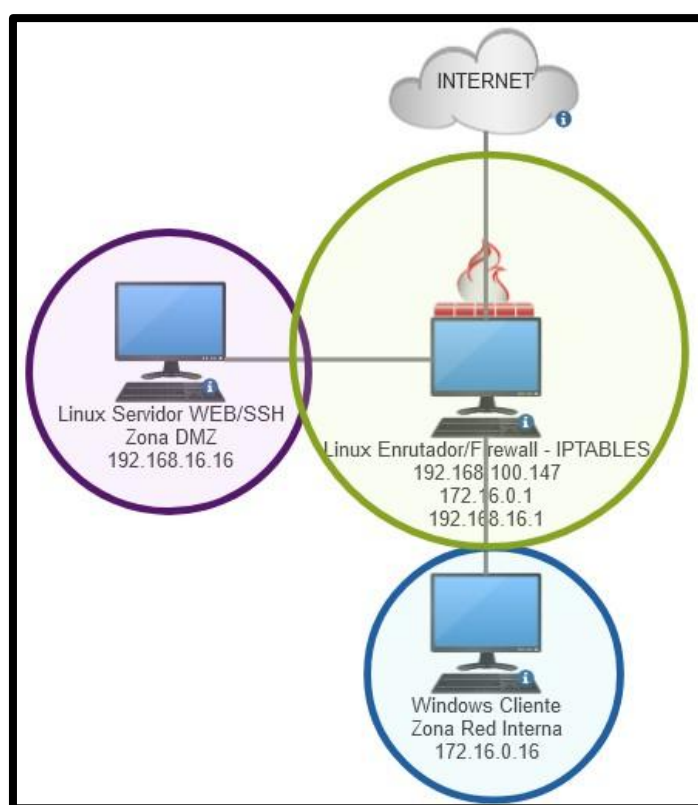
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy DROP 2 packets, 126 bytes)
 pkts bytes target    prot opt in     out     source               destination
  0      0 ACCEPT    icmp -- *    *    0.0.0.0/0            192.168.100.151      icmpt
type 0
  0      0 ACCEPT    tcp  -- *    *    0.0.0.0/0            192.168.100.151
  0      0 ACCEPT    tcp  -- *    *    0.0.0.0/0            192.168.100.151
sandrodmz@pop-os:~/Escritorio$
```

4 - IpTables como Cortafuegos Perimetral

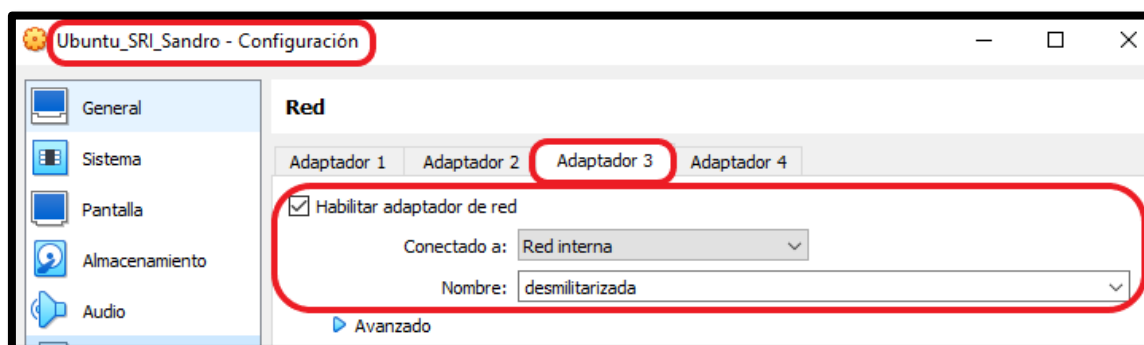
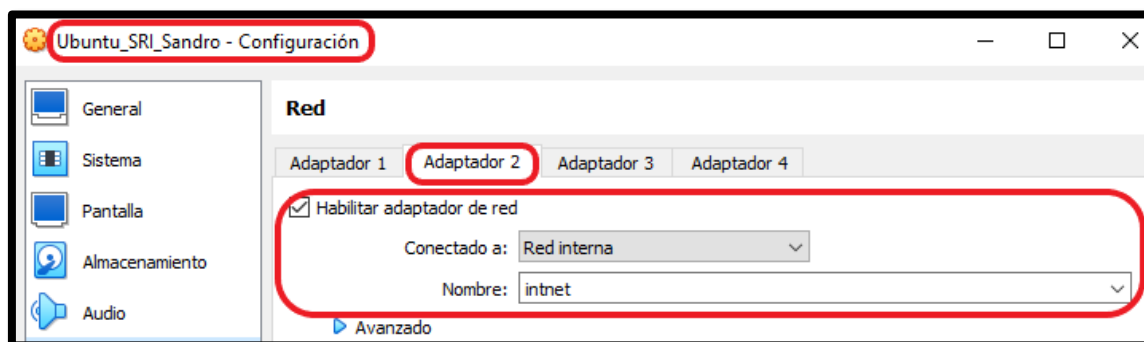
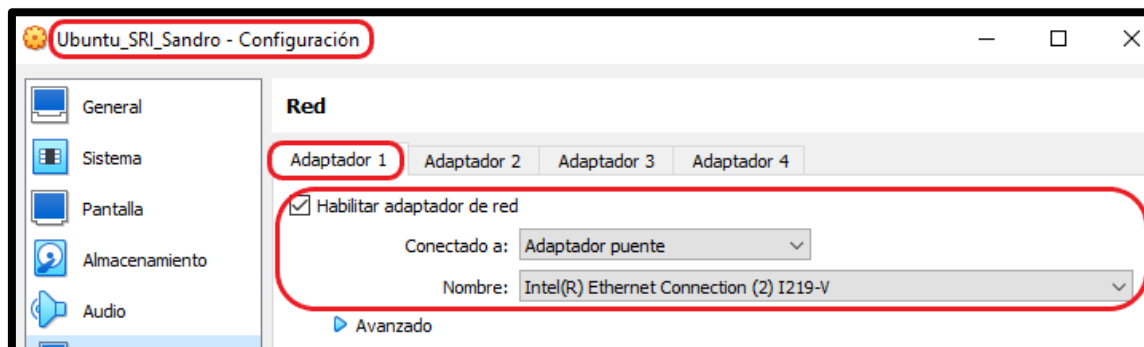
Para la segunda parte vamos a establecer “iptables” como firewall perimetral para proteger nuestra red desmilitarizada y la red interna de los clientes. Esto sería más parecido a un caso real en el que tienes que separar las redes para poder protegerlas correctamente contra los peligros que puedan venir desde el exterior.

Aunque es menos recomendable voy a aplicar por defecto la política permisiva, ya que en el primer caso apliqué la restrictiva, pero siempre debería hacerse todo de manera restrictiva. Utilizaremos 3 máquinas virtuales y la estructura será de la siguiente manera:

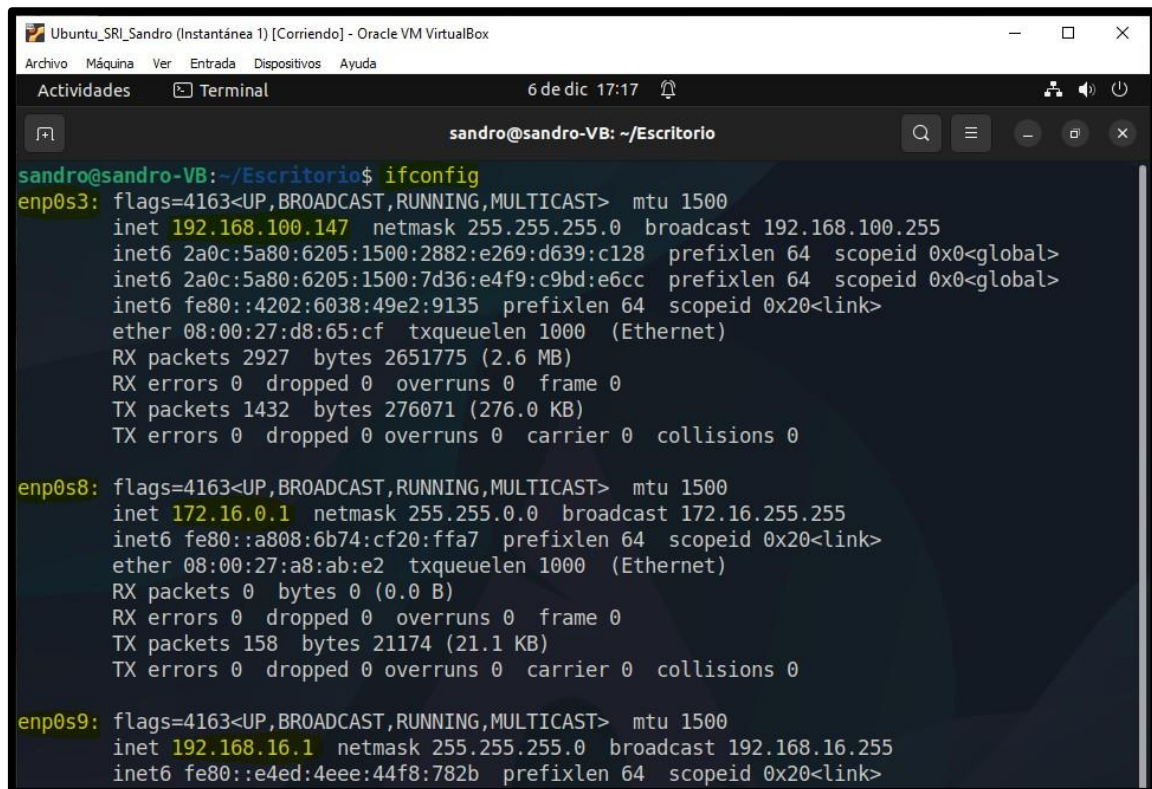


Firewall a nivel perimetral

Primero la máquina Linux que va a enrutar y proporcionarnos la función de Firewall. Tiene 3 interfaces de red:



La primera va a la red de casa mediante DHCP. La segunda es para la zona DMZ y la tercera es para la red interna. La puerta de enlace no es necesaria ni para la DMZ ni para la interna.

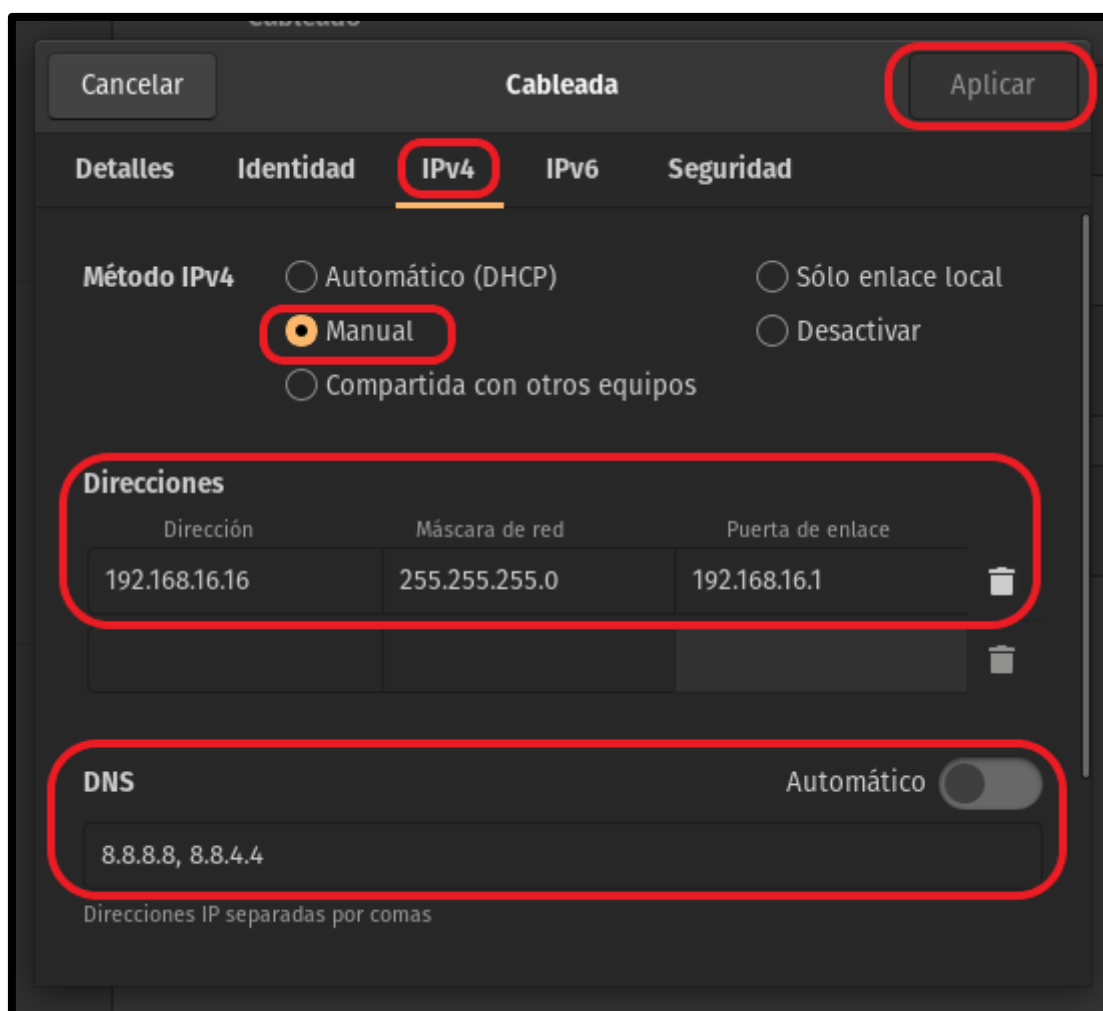
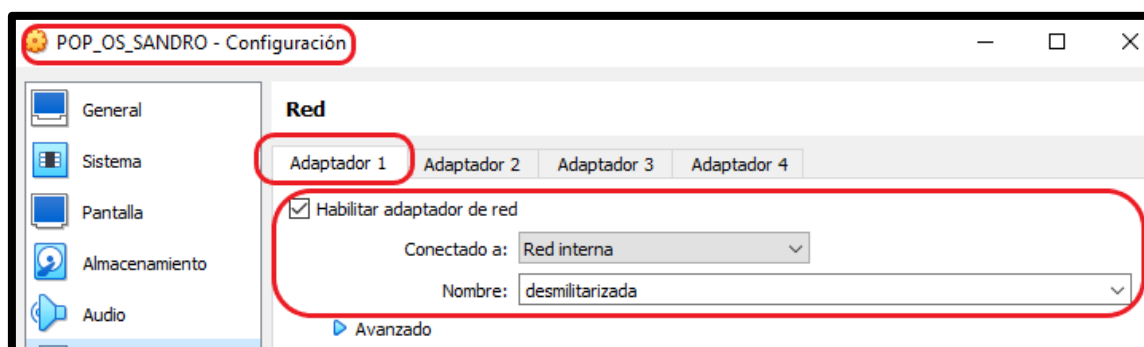


```
sandro@sandro-VB: ~/Escritorio
sandro@sandro-VB:~/Escritorio$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.147 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 2a0c:5a80:6205:1500:2882:e269:d639:c128 prefixlen 64 scopeid 0x0<global>
    inet6 2a0c:5a80:6205:1500:7d36:e4f9:c9bd:e6cc prefixlen 64 scopeid 0x0<global>
    inet6 fe80::4202:6038:49e2:9135 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d8:65:cf txqueuelen 1000 (Ethernet)
    RX packets 2927 bytes 2651775 (2.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1432 bytes 276071 (276.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.0.1 netmask 255.255.0.0 broadcast 172.16.255.255
    inet6 fe80::a808:6b74:cf20:ffa7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a8:ab:e2 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 158 bytes 21174 (21.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.16.1 netmask 255.255.255.0 broadcast 192.168.16.255
    inet6 fe80::e4ed:4eee:44f8:782b prefixlen 64 scopeid 0x20<link>
```

Ahora vamos a la máquina Linux de la zona DMZ y le ponemos la siguiente configuración de red:



Comprobamos que hace ping a la puerta de enlace y que desde la puerta de enlace también llegamos a ella:

```
Workspaces  Aplicaciones  6 de dic  7:14 PM  ●
sandrodmz@pop-os: ~/Escritorio

sandrodmz@pop-os:~/Escritorio$ ping -c 2 192.168.16.1
PING 192.168.16.1 (192.168.16.1) 56(84) bytes of data.
64 bytes from 192.168.16.1: icmp_seq=1 ttl=64 time=0.369 ms
64 bytes from 192.168.16.1: icmp_seq=2 ttl=64 time=0.973 ms

--- 192.168.16.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1023ms
rtt min/avg/max/mdev = 0.369/0.671/0.973/0.302 ms
sandrodmz@pop-os:~/Escritorio$
```

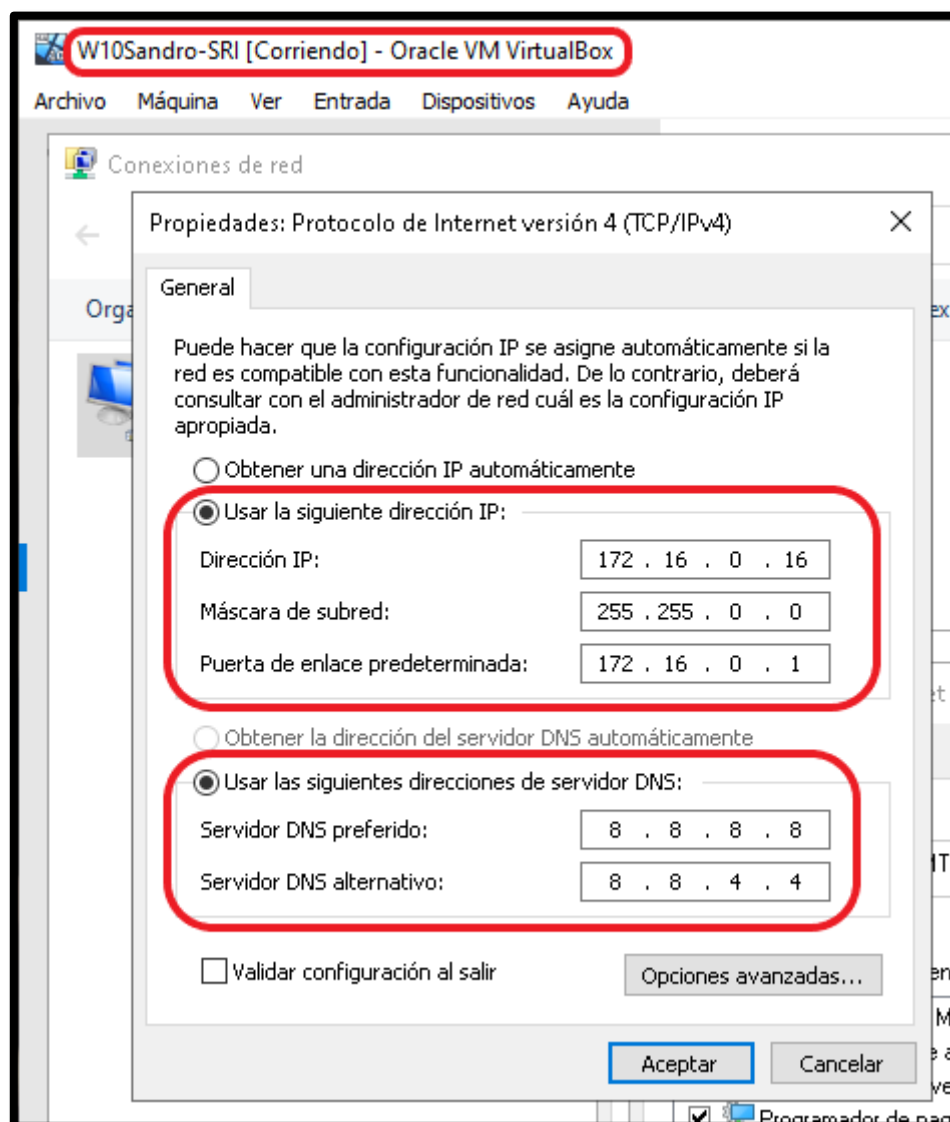
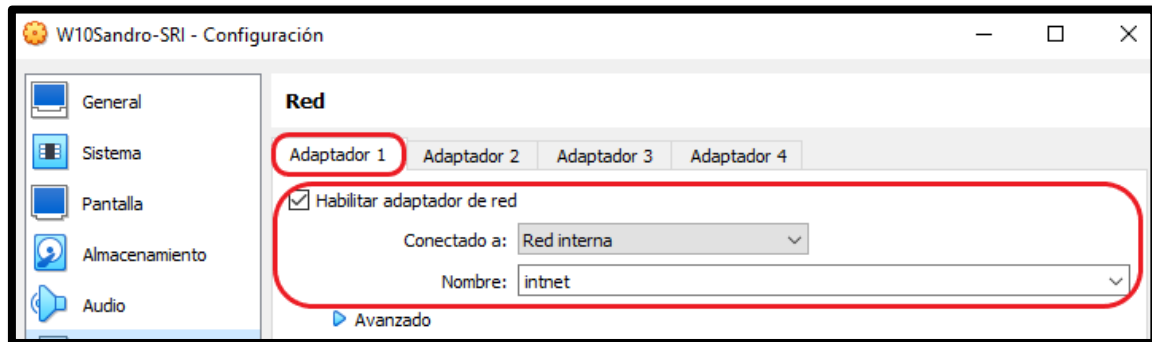
```
Ubuntu_SRI_Sandro (Instantánea 1) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  6 de dic  19:15  🔔

sandro@sandro-VB: ~/Escritorio

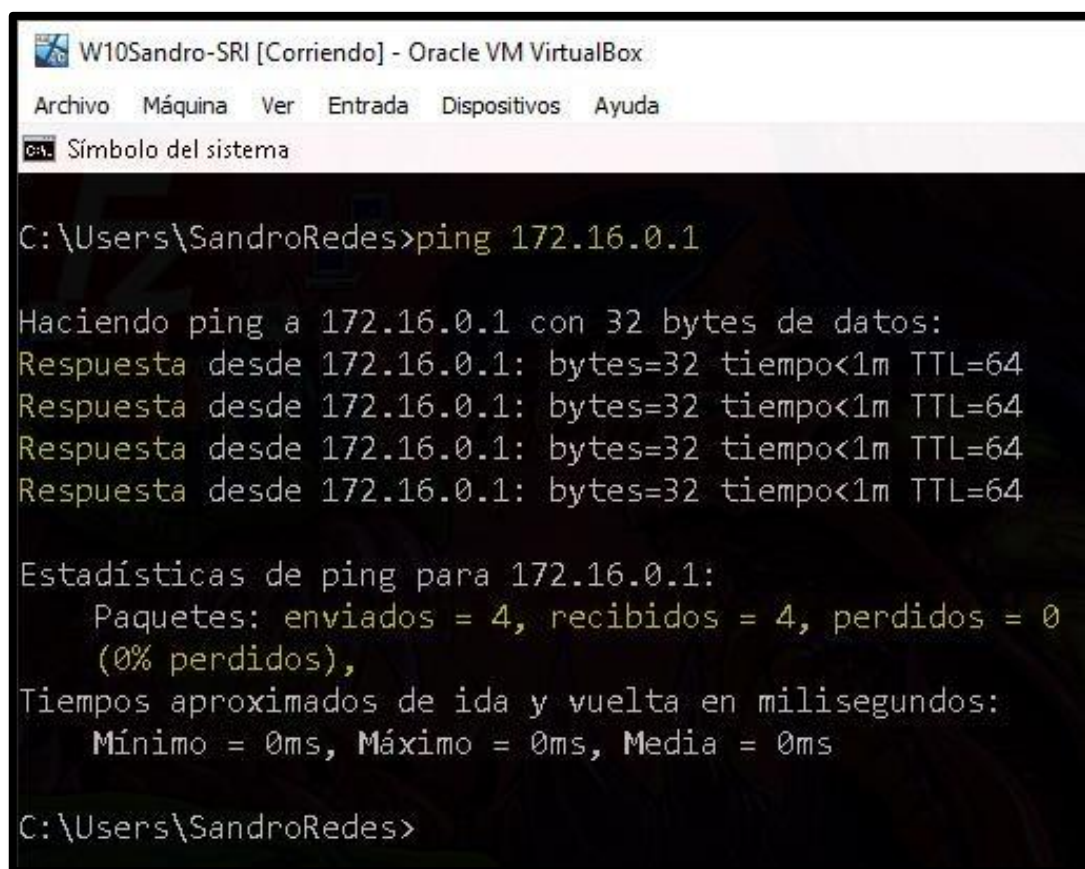
sandro@sandro-VB:~/Escritorio$ ping -c 2 192.168.16.16
PING 192.168.16.16 (192.168.16.16) 56(84) bytes of data.
64 bytes from 192.168.16.16: icmp_seq=1 ttl=64 time=0.379 ms
64 bytes from 192.168.16.16: icmp_seq=2 ttl=64 time=0.773 ms

--- 192.168.16.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.379/0.576/0.773/0.197 ms
sandro@sandro-VB:~/Escritorio$
```

En la máquina Windows también cambiamos la configuración de red:



Y le hacemos ping a su puerta de enlace y desde la puerta también para comprobar que se ven ambas:



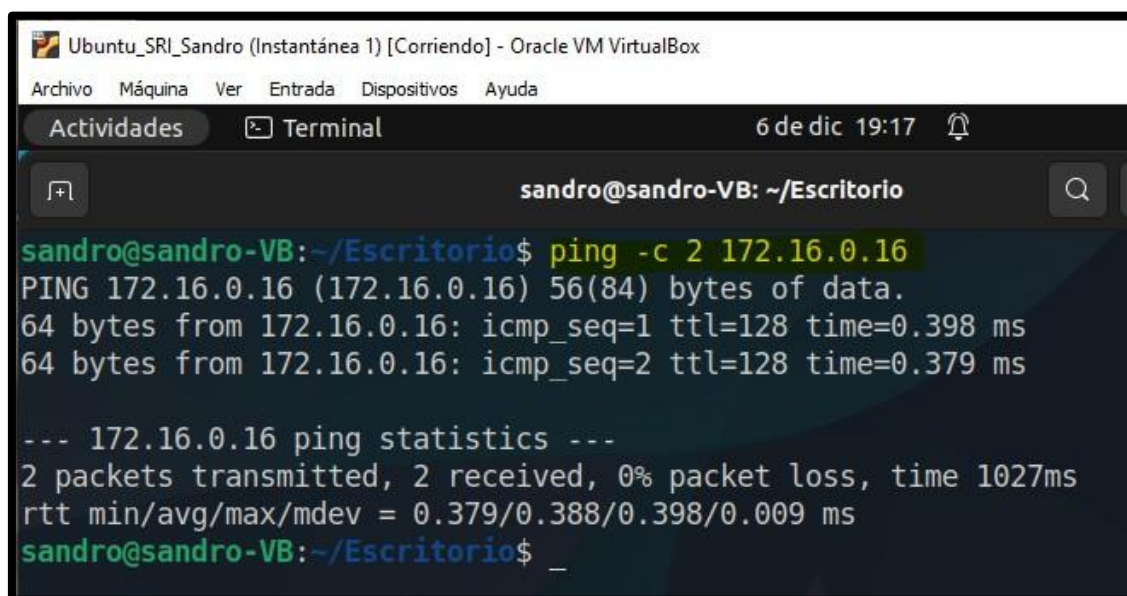
```
W10Sandro-SRI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Símbolo del sistema

C:\Users\SandroRedes>ping 172.16.0.1

Haciendo ping a 172.16.0.1 con 32 bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\SandroRedes>
```



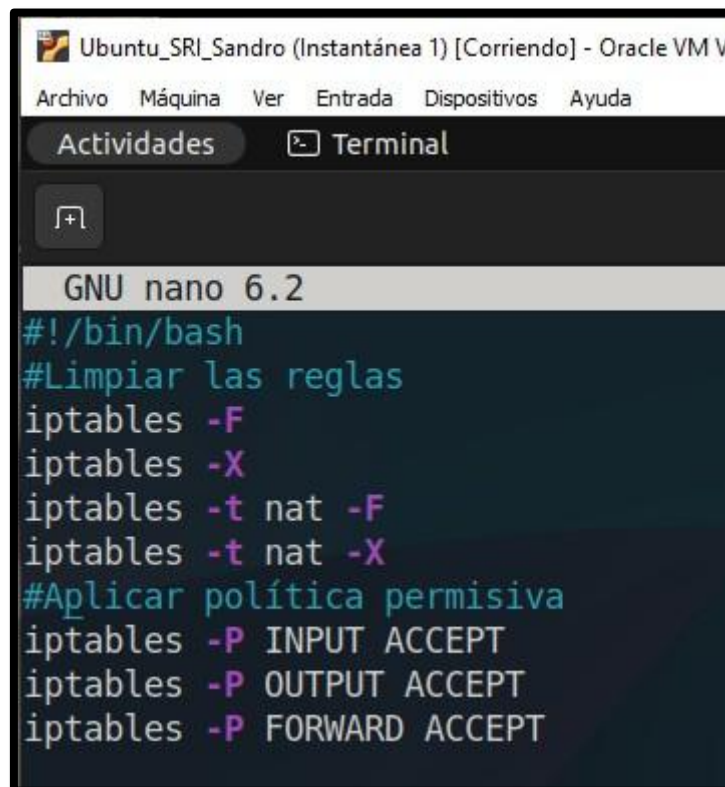
```
Ubuntu_SRI_Sandro (Instantánea 1) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  6 de dic 19:17

sandro@sandro-VB: ~/Escritorio

sandro@sandro-VB:~/Escritorio$ ping -c 2 172.16.0.16
PING 172.16.0.16 (172.16.0.16) 56(84) bytes of data.
64 bytes from 172.16.0.16: icmp_seq=1 ttl=128 time=0.398 ms
64 bytes from 172.16.0.16: icmp_seq=2 ttl=128 time=0.379 ms

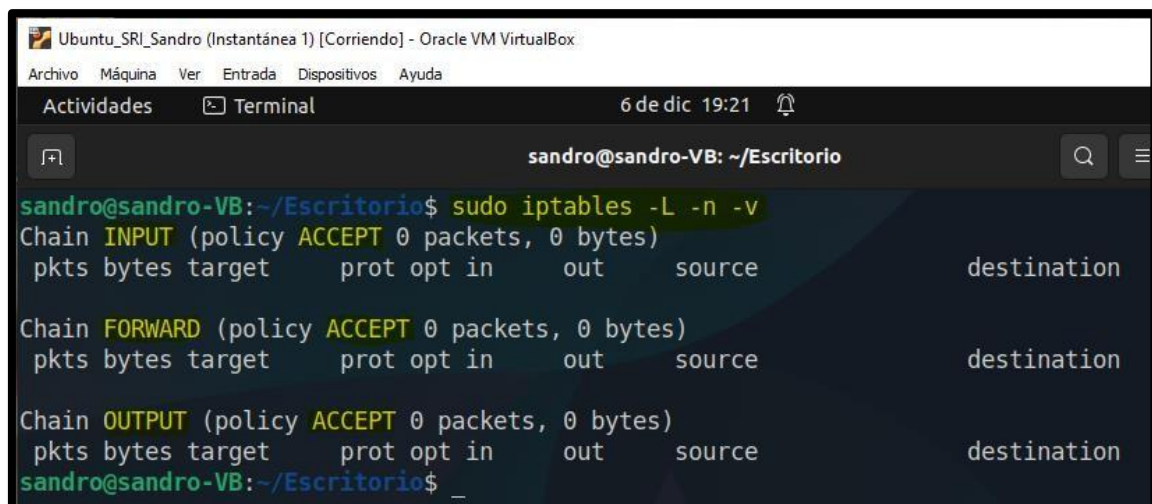
--- 172.16.0.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.379/0.388/0.398/0.009 ms
sandro@sandro-VB:~/Escritorio$ _
```

Y para cambiar la forma con el primero aplico una política permisiva:



```
Ubuntu_SRI_Sandro (Instantánea 1) [Corriendo] - Oracle VM V
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
GNU nano 6.2
#!/bin/bash
#Limpiar las reglas
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
#Aplicar política permisiva
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Y comprobamos que esté correcto en el firewall:



```
Ubuntu_SRI_Sandro (Instantánea 1) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
6 de dic 19:21
sandro@sandro-VB: ~/Escritorio
sandro@sandro-VB:~/Escritorio$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source   destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source   destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source   destination
sandro@sandro-VB:~/Escritorio$ _
```


5 - Configuración de Reglas

Lo primero es que las máquinas de ambas redes puedan tener salida a internet. Con “-o” le indicamos la interfaz de salida. “-j MASQUERADE” para que se modifique la dirección de los paquetes por los de la interfaz “enp0s3”. Aquí si le especificamos la tabla de “NAT”:

```
#Doy salida a internet a la dmz y a la red interna
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Y activar el bit de “forward” o “reenvío de paquetes” poniéndolo a “1”:

```
sandro@sandro-VB: ~/Escritorio
sandro@sandro-VB:~/Escritorio$ sudo echo "1" > sudo /proc/sys/net/ipv4/ip_forward
sandro@sandro-VB:~/Escritorio$ cat /proc/sys/net/ipv4/ip_forward
1
sandro@sandro-VB:~/Escritorio$
```

Ahora tenemos acceso a Internet tanto desde la red interna de clientes:

```
W10Sandro-SRI [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Simbolo del sistema

C:\Users\SandroRedes>ping 172.16.0.1

Haciendo ping a 172.16.0.1 con 32 bytes de datos:
Respuesta desde 172.16.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 172.16.0.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 172.16.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

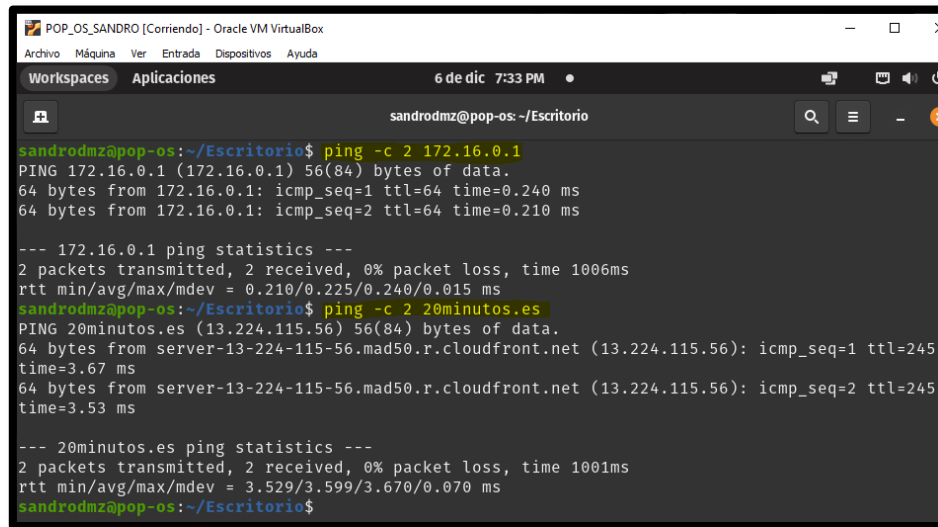
C:\Users\SandroRedes>ping google.es

Haciendo ping a google.es [142.250.200.67] con 32 bytes de datos:
Respuesta desde 142.250.200.67: bytes=32 tiempo=3ms TTL=117
Respuesta desde 142.250.200.67: bytes=32 tiempo=4ms TTL=117
Respuesta desde 142.250.200.67: bytes=32 tiempo=3ms TTL=117
Respuesta desde 142.250.200.67: bytes=32 tiempo=4ms TTL=117

Estadísticas de ping para 142.250.200.67:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 4ms, Media = 3ms

C:\Users\SandroRedes>
```

Como desde la zona desmilitarizada:



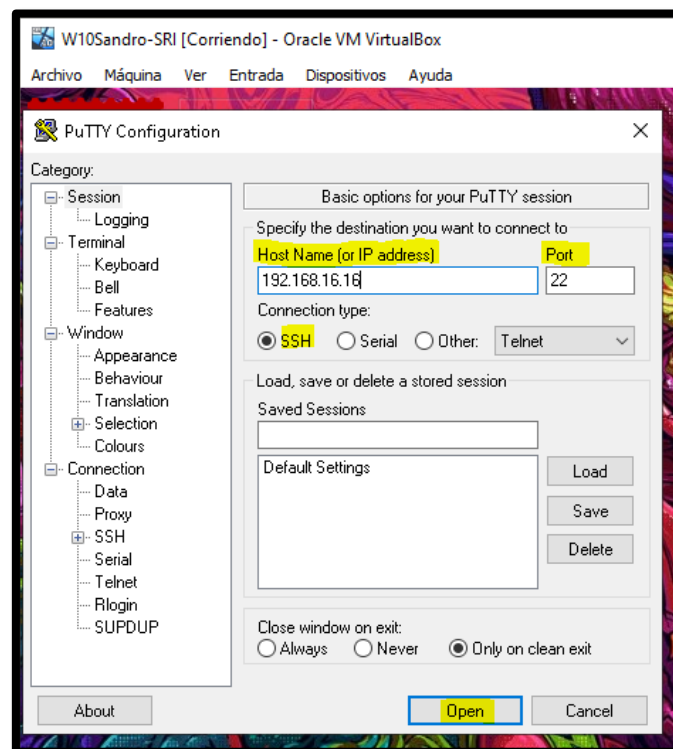
```
sandrodmz@pop-os: ~/Escritorio
sandrodmz@pop-os:~/Escritorio$ ping -c 2 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data:
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=0.240 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=64 time=0.210 ms

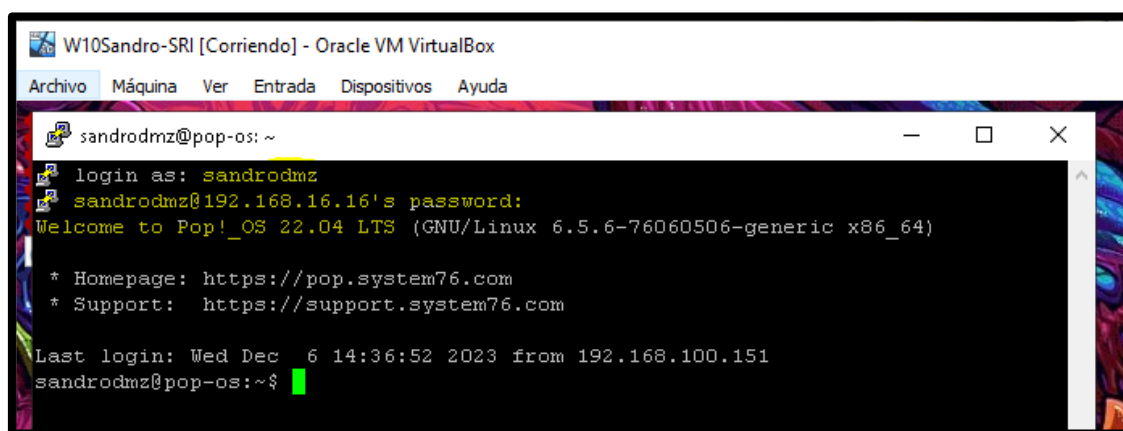
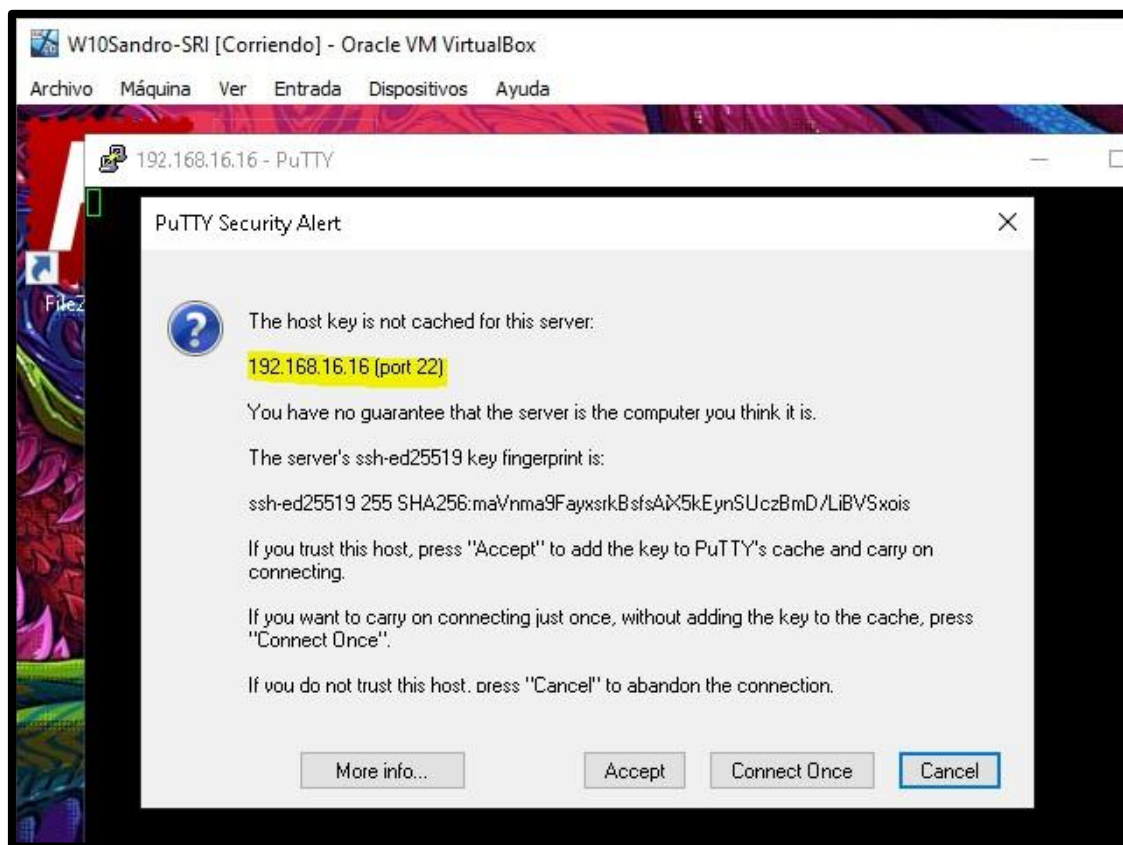
--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.210/0.225/0.240/0.015 ms
sandrodmz@pop-os:~/Escritorio$ ping -c 2 20minutos.es
PING 20minutos.es (13.224.115.56) 56(84) bytes of data:
64 bytes from server-13-224-115-56.mad50.r.cloudfront.net (13.224.115.56): icmp_seq=1 ttl=245
time=3.67 ms
64 bytes from server-13-224-115-56.mad50.r.cloudfront.net (13.224.115.56): icmp_seq=2 ttl=245
time=3.53 ms

--- 20minutos.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.529/3.599/3.670/0.070 ms
sandrodmz@pop-os:~/Escritorio$
```

Ahora vamos a aplicar reglas restrictivas entre la red interna de clientes y la red DMZ.

Primero podemos observar que podemos llegar al servidor ssh de la zona DMZ:

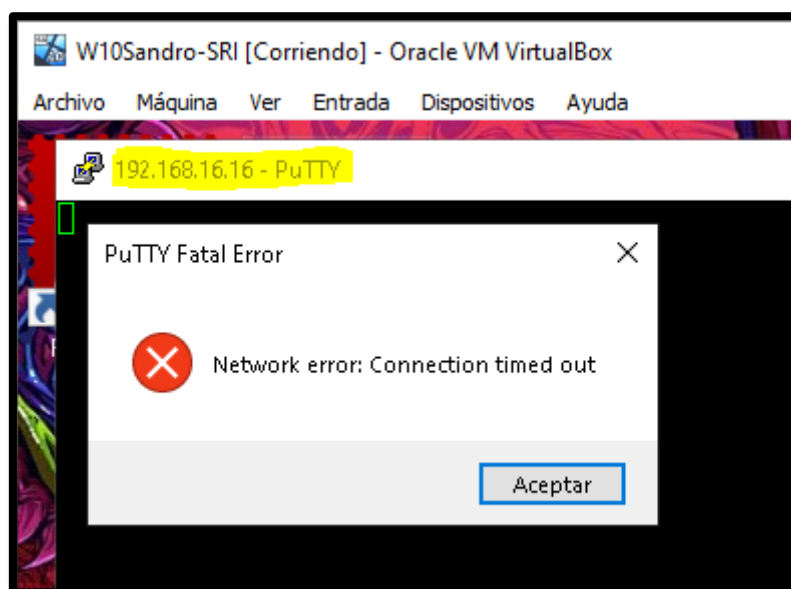




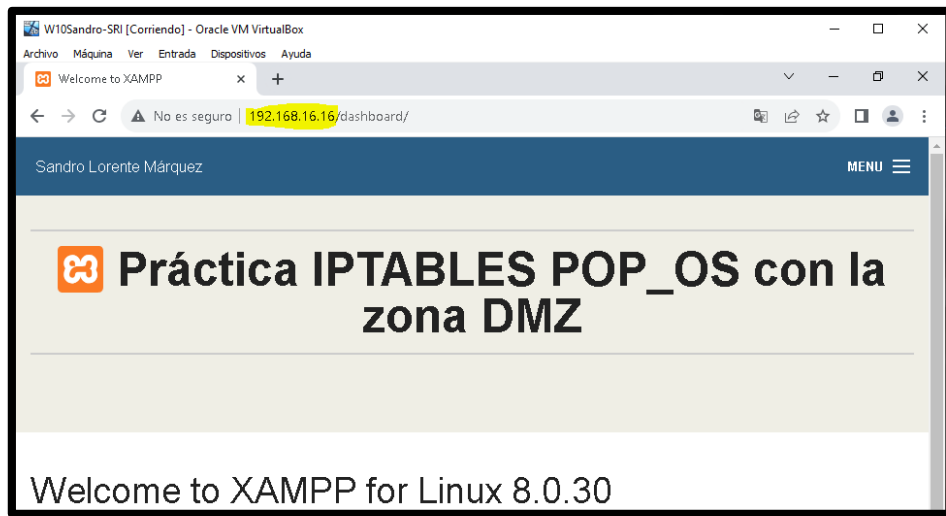
Por lo que vamos a aplicar una política restrictiva que impida acceder desde la red interna al servidor ssh de la zona DMZ. Ahora sí usamos “FORWARD” porque son paquetes que atraviesan, es decir, ni se originan ni su destino es el firewall. Aquí necesitamos establecer tanto origen como destino pudiendo ser direcciones concretas o direcciones de red:

```
#voy salida a internet a la dmz y a la red interna  
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE  
  
#Impedir el acceso al servidor SSH  
sudo iptables -A FORWARD -s 172.16.0.0/16 -d 192.168.16.16 -p tcp --dport 22 -j DROP
```

Entonces ahora, nos va a rechazar la conexión:



Ahora también vamos a restringir la conexión al servidor web, ya que podemos seguir accediendo:

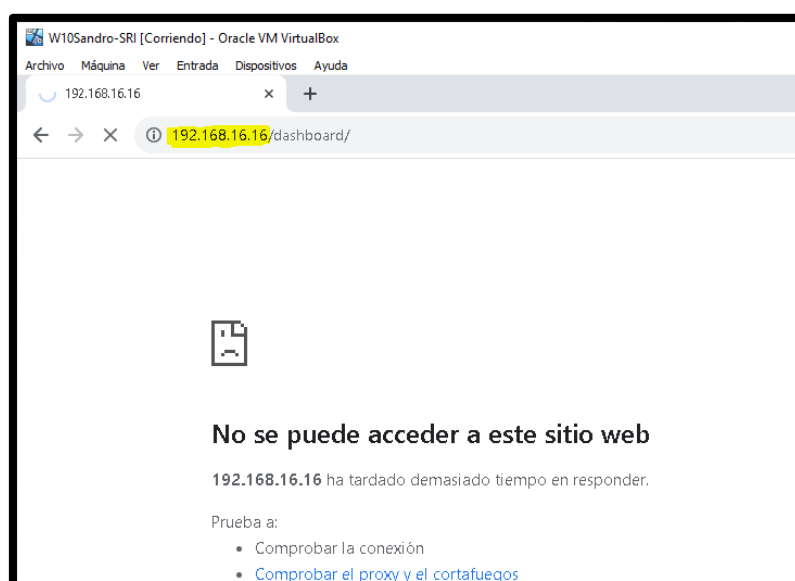


Añadimos la regla a “Iptables”:

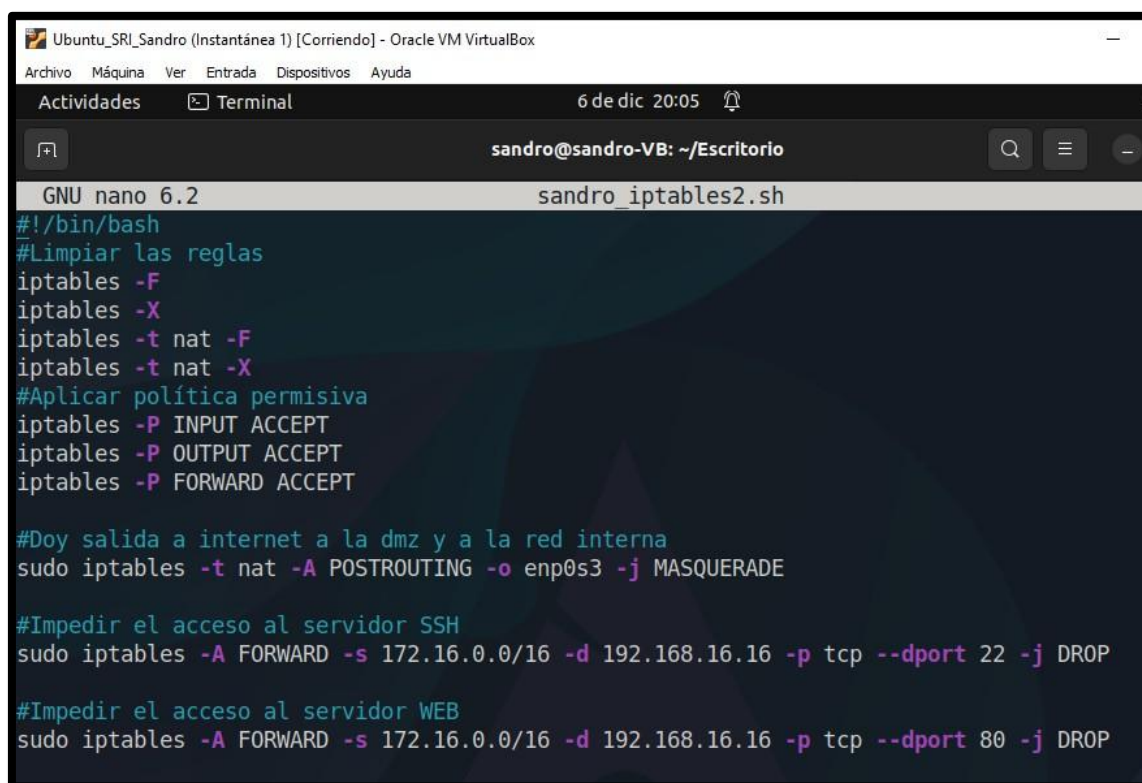
```
#Impedir el acceso al servidor SSH
sudo iptables -A FORWARD -s 172.16.0.0/16 -d 192.168.16.16 -p tcp --dport 22 -j DROP

#Impedir el acceso al servidor WEB
sudo iptables -A FORWARD -s 172.16.0.0/16 -d 192.168.16.16 -p tcp --dport 80 -j DROP
```

Y entonces lo hemos bloqueado:



Para acabar, se muestra tanto el contenido de todo el script como del estado de “IpTables” cuando lo ejecutas al completo:



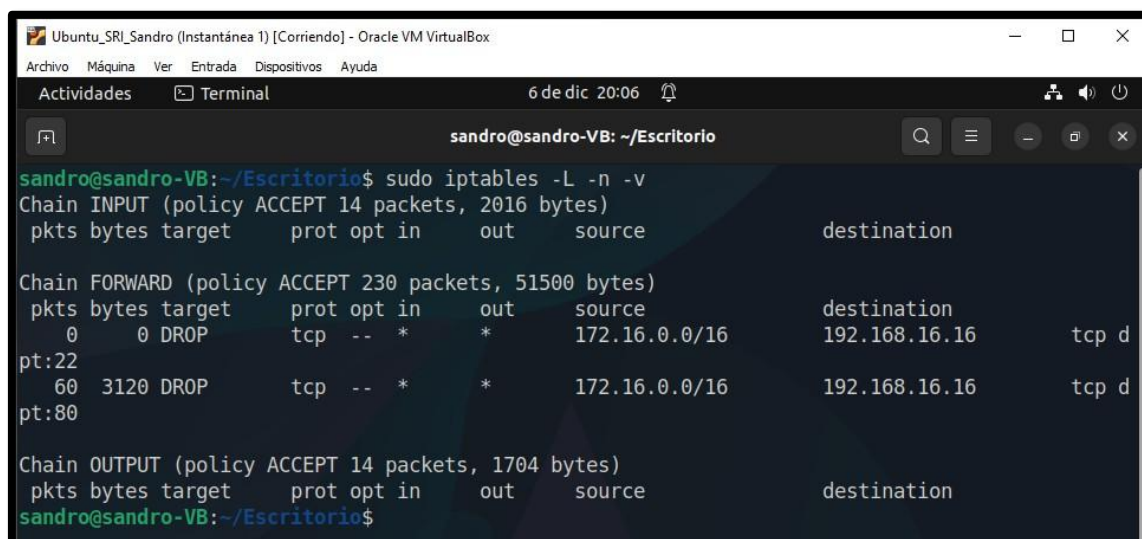
```

GNU nano 6.2                                sandro_iptables2.sh
#!/bin/bash
#Limpiar las reglas
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
#Aplicar política permisiva
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

#Doy salida a internet a la dmz y a la red interna
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

#Impedir el acceso al servidor SSH
sudo iptables -A FORWARD -s 172.16.0.0/16 -d 192.168.16.16 -p tcp --dport 22 -j DROP

#Impedir el acceso al servidor WEB
sudo iptables -A FORWARD -s 172.16.0.0/16 -d 192.168.16.16 -p tcp --dport 80 -j DROP
  
```



```

sandro@sandro-VB:~/Escritorio$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 14 packets, 2016 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 230 packets, 51500 bytes)
 pkts bytes target    prot opt in     out     source                   destination
  0      0 DROP      tcp  --  *      *       172.16.0.0/16            192.168.16.16            tcp d
pt:22
  60    3120 DROP      tcp  --  *      *       172.16.0.0/16            192.168.16.16            tcp d
pt:80

Chain OUTPUT (policy ACCEPT 14 packets, 1704 bytes)
 pkts bytes target    prot opt in     out     source                   destination
sandro@sandro-VB:~/Escritorio$
  
```

6 - Punto Extra

Nota: para que se quede guardada la configuración de iptables en caso de que reinicies, debes instalar el siguiente paquete y ejecutar el comando:

sudo apt-get install iptables-persistent

sudo netfilter-persistent save