IES Fernando Aguilar Quignon

2º Administración de Sistemas Informáticos en Red

Seguimiento del Curso iptables.

José María Riol Sánchez

14 de febrero de 2023

Índice

Introducción a la tarea

Vamos a seguir un curso de Alberto Molina de OpenWebinars acerca de iptables en el que llevaremos a cabo una serie de ejercicios.

El esquema que usaremos es el que tiene pensado Alberto de forma simplificada para no tener muchas máquinas con las que hacer la demostración, tendremos una DMZ con un equipo servidor que se encontrará en la red **192.168.200.0/24** y luego nuestra red local con nuestro equipo que se encontrará en la red **192.168.100.0/24**. En ambas redes tendremos un Switch para hacer más fiel la simulación, para el caso en el que hubiera más de un equipo en cada subred.

Luego nuestro Router/firewall es el que hace de firewall con 3 interfaces, una para la DMZ, otra para la red interna local y otra con el router isp actuándo como firewall perimetral. Por último nuestro isp llamado router es el que estará conectado con el exterior y con nuestro firewall

El laboratorio que usaremos para hacer las prácticas se pueden encontrar en mi GitHub, por si se quiere descargar y hacer uso de él y realizar los ejercicios reflejados en este documento.

Esquema.

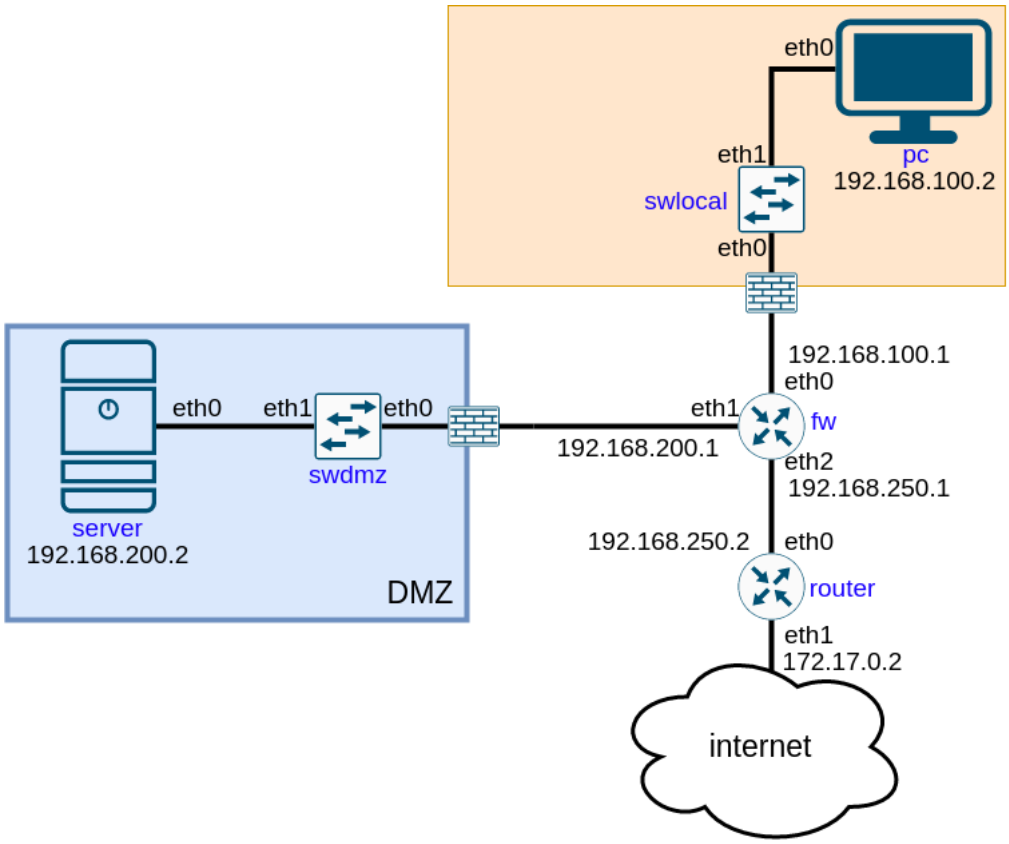

Figura 1: Esquema de la red a usar.

1. Prueba de vida.

Sintaxis de iptables MIN 11:51

1.1. Implementar un cortafuegos personal.

Probamos primero a hacer ping a un DNS (1.1.1.1) y lo hace sin problema, incluso puede navegar por la red sin problemas.

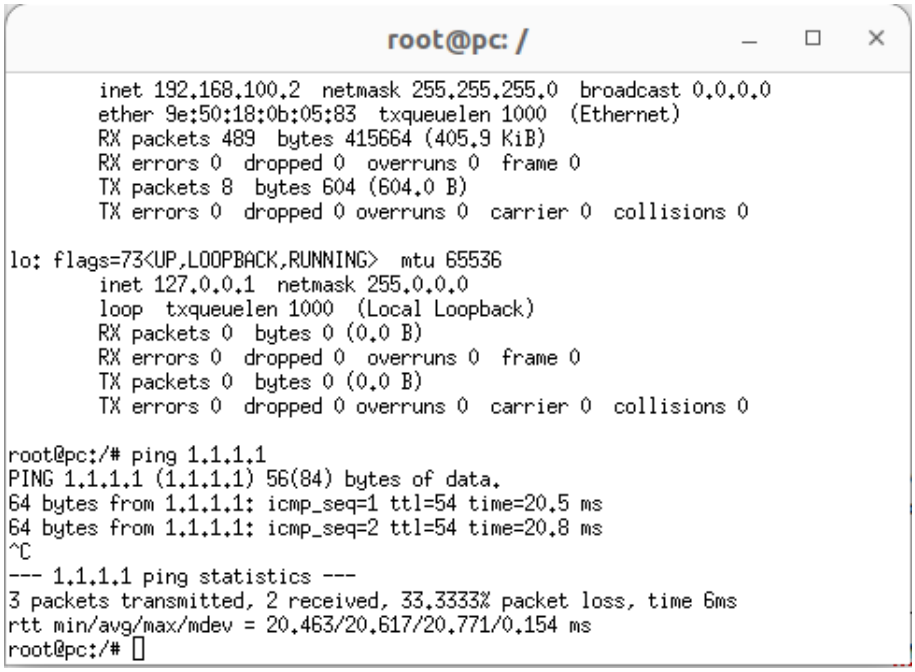

Figura 2: Ping al DNS.

Hacemos un curl porque no tiene GUI nuestra máquina.

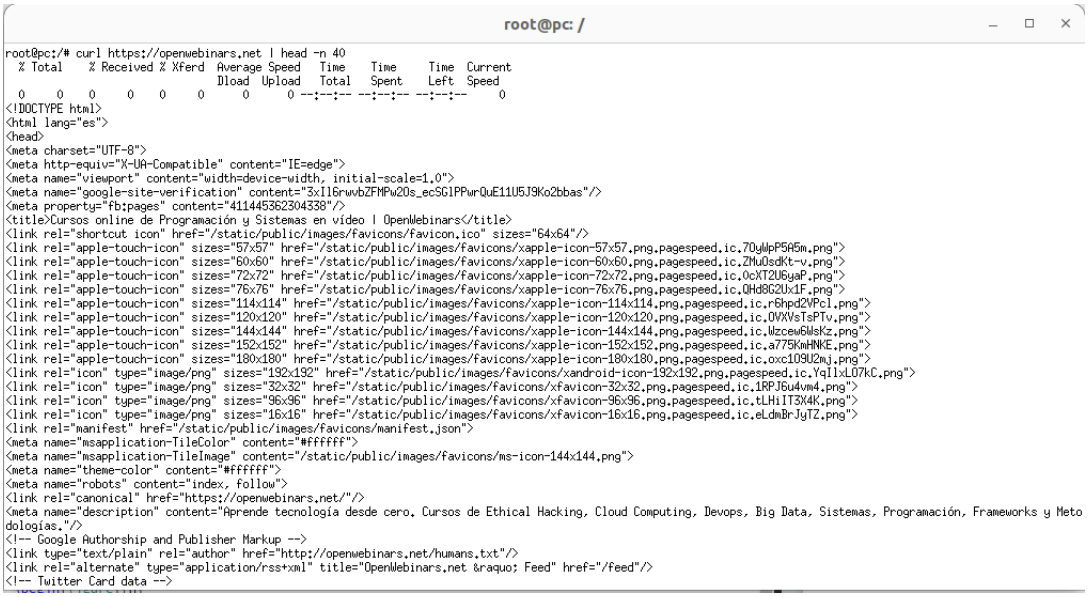

Figura 3: Puede navegar por la red.

Vemos si hay alguna regla para hacer flush o no.

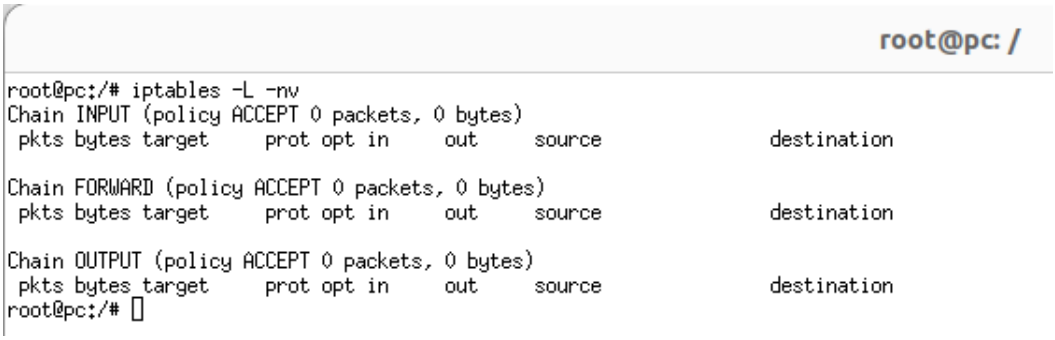

Figura 4: Listado de reglas.

Cambiamos las iptables haciendo que no tenga conexión ninguna.

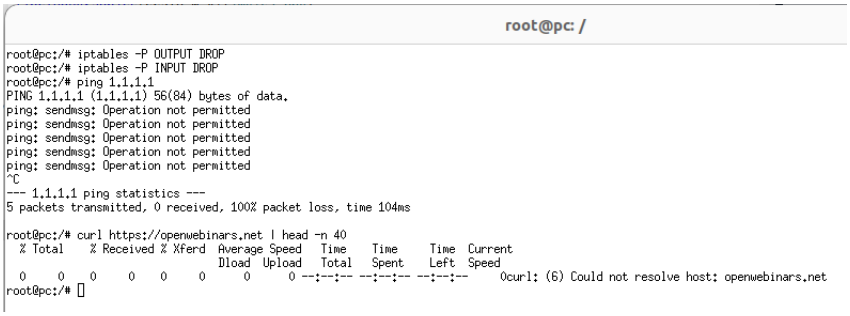

Figura 5: Cambio en la iptables a drop dejándolo sin conexión.

Si llevamos a cabo un iptables para permitir el ping, esta vez permitirá la operación pero no tendremos respuesta, porque los paquetes que le llegan tienen la política drop entonces no los recibe.

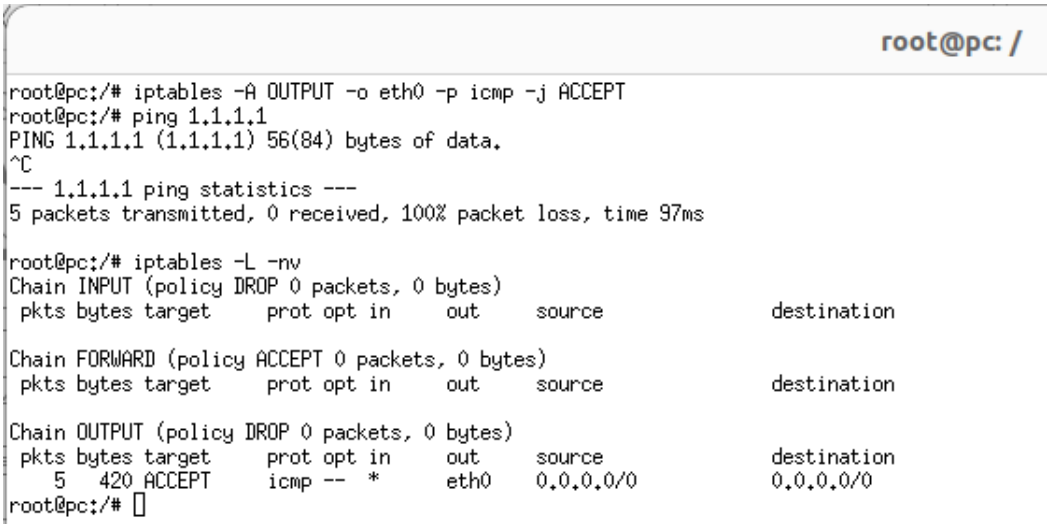

Figura 6: Hace ping pero no le llega las respuestas.

Recordemos que las reglas van por pares así que tengo que hacer otra regla INPUT que me permita tener los paquetes de vuelta sin problemas.

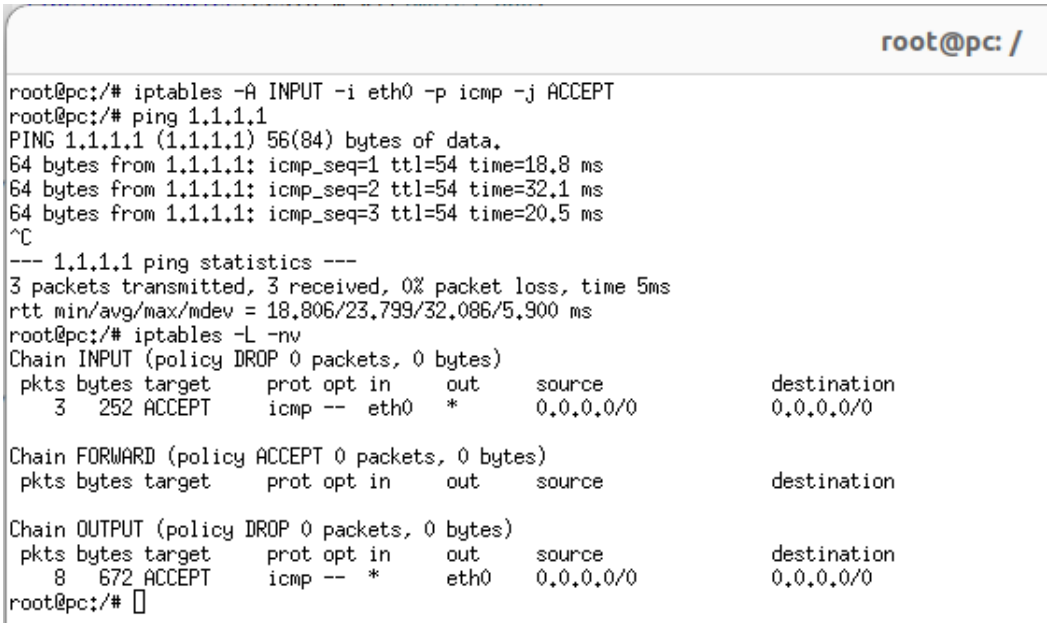

Figura 7: Hace ping pero no le llega las respuestas.

Es bueno observar los paquetes enviados y recibidos en la figura 6 y 7, en la figura 6 tenemos enviados 5 y recibidos ninguno y luego en la figura 7 enviados 8 y recibidos 3.

Las reglas toman la interfaz 0 como entrada/salida, si hacemos ping al 127.0.0.1 que es nuestra propia máquina volverá a ser una operación no permitida.

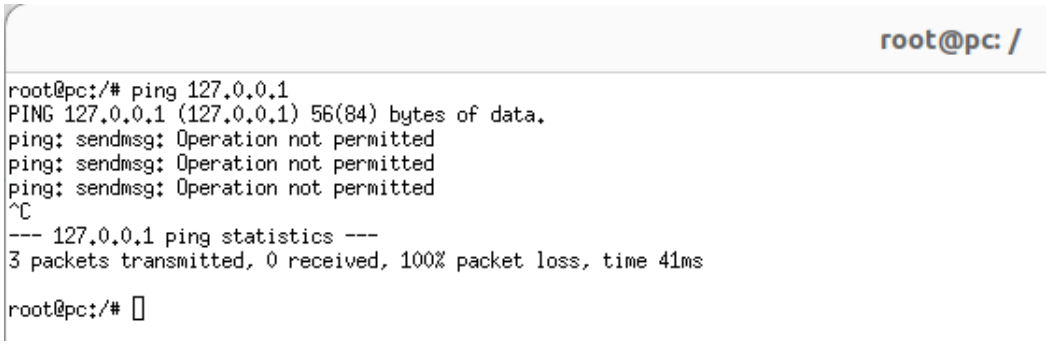

Figura 8: Ping interno.

Para permitirlo pondremos las reglas **iptables -A INPUT -i lo -j ACCEPT** y **iptables -A OUTPUT -o lo -j ACCEPT** siendo lo loopback.

No podríamos hacer consultas DNS como por ejemplo con dig, para ello, debemos poner también reglas que permitan ese tipo de tráfico, para ello...

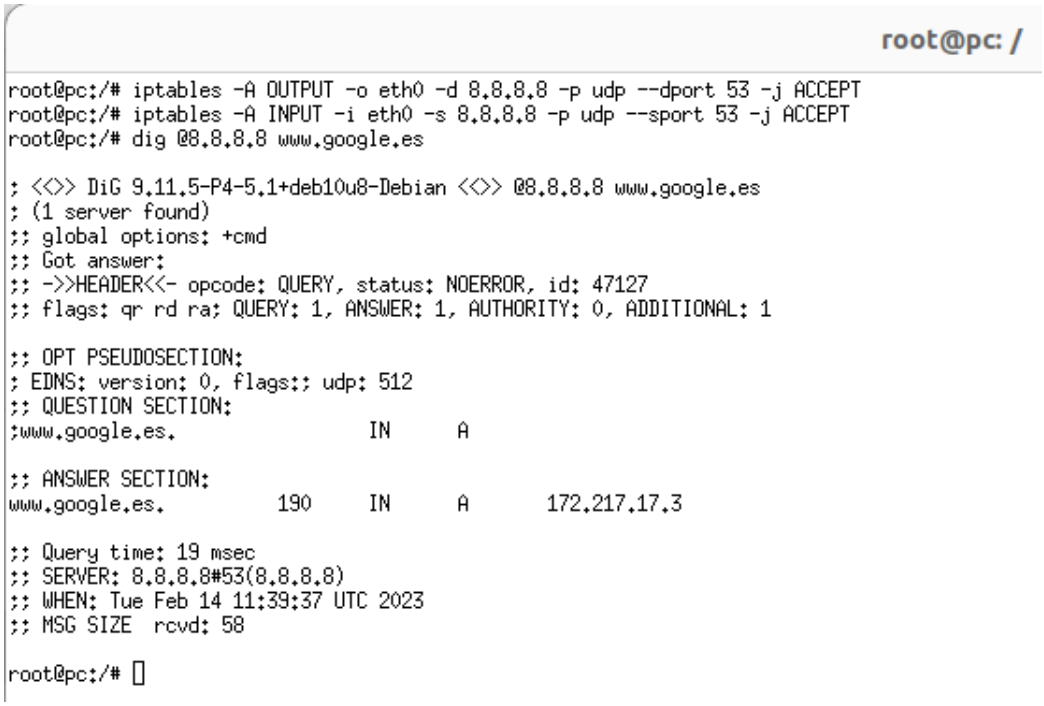

Figura 9: Consulta DNS.

Seguimos sin tener tráfico web, como podremos observar.

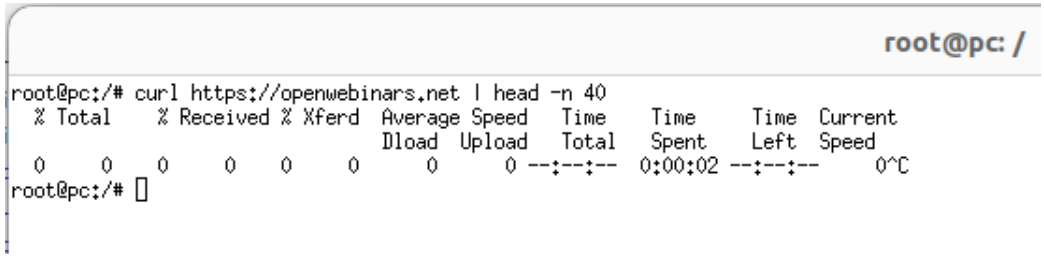

Figura 10: Sin tráfico web.

Por ello tenemos que añadir las reglas de ACCEPT para los puertos 80 y 443 tanto de entrada como salida.

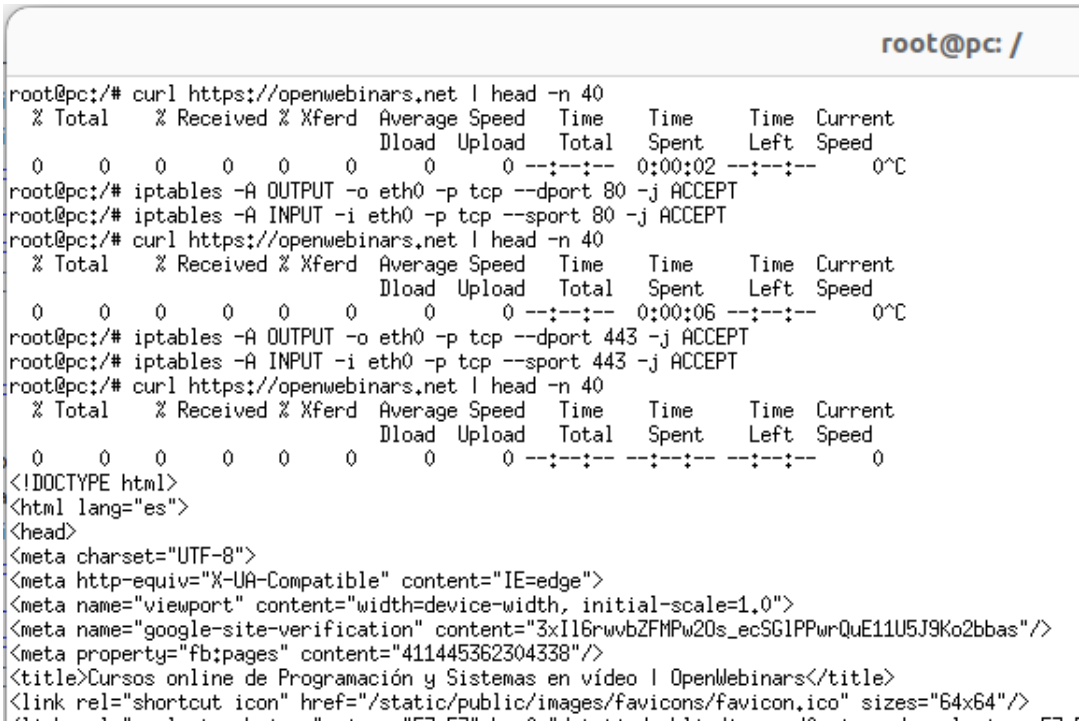

Figura 11: Con tráfico web.