sEGURIDAD EN REDES

Aarón Cañamero Mochales

04/03/2021

Índice:

[ESCENARIO 1: 2](#_Toc66201103)

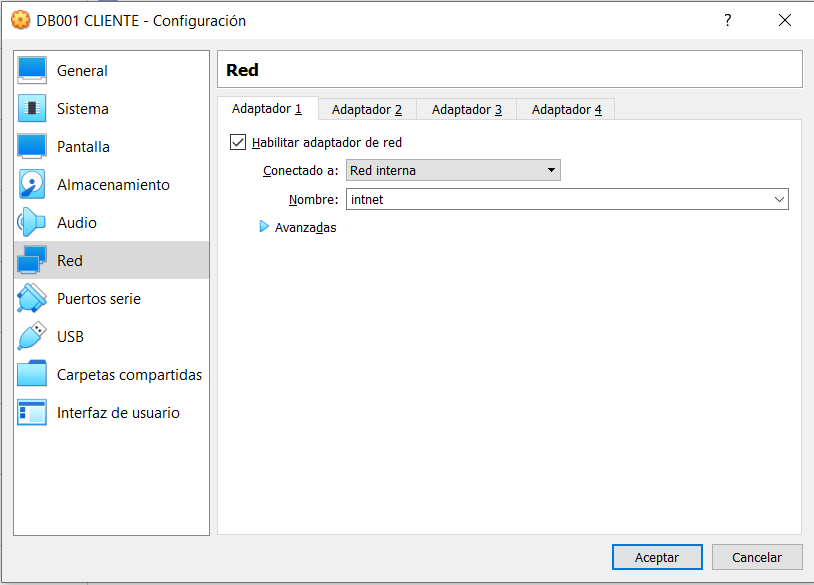
[ESCENARIO 2: 11](#_Toc66201104)

[ENCENARIO 3: 22](#_Toc66201105)

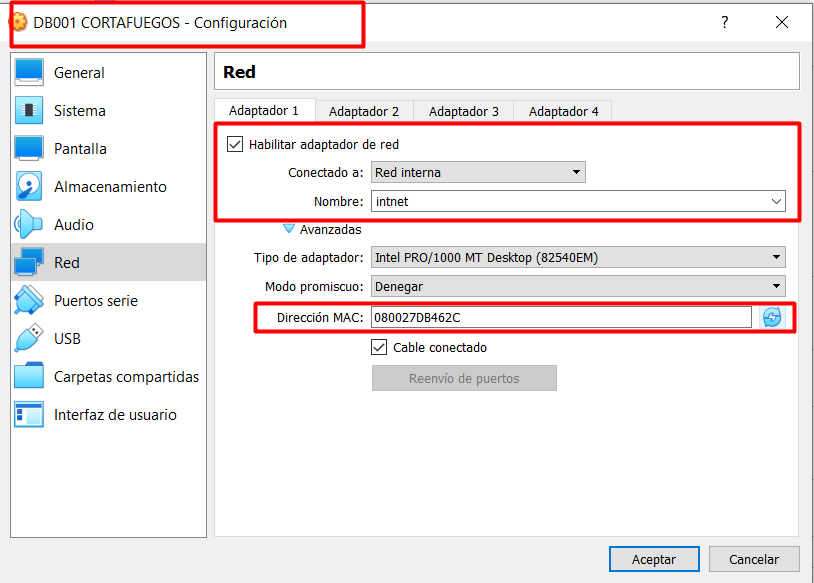
ESCENARIO 1:

En un primer escenario, tenemos una máquina conectada a internet, y queremos protegerla con un cortafuego.

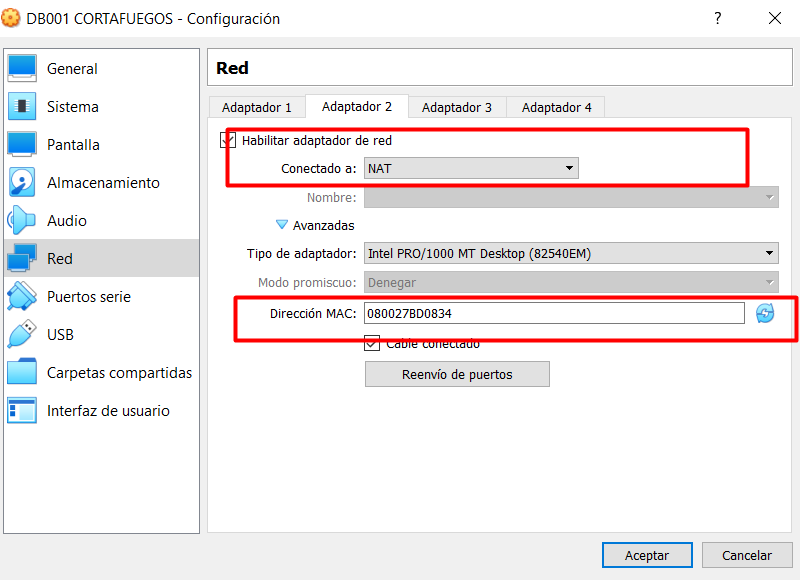
Configuramos el **CLIENTE** y lo ponemos en **RED INTERNA**.



Configuramos el cortafuego, lo ponemos en red interna y cambiamos la **MAC**, para asegurarnos que tienen diferentes.



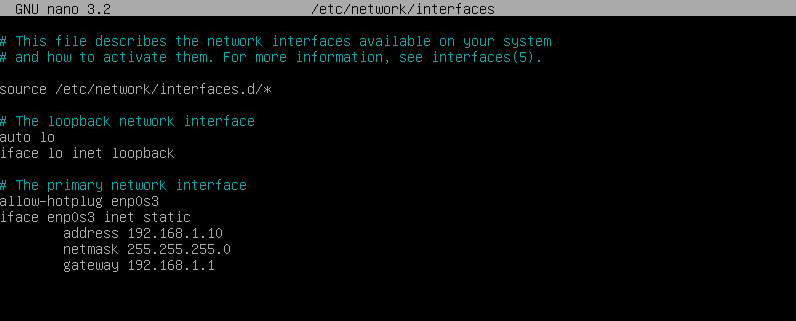
Esta máquina va a tener dos patas, una en red interna como hemos visto y la otra en red **NAT**, para que pueda tener acceso a internet.



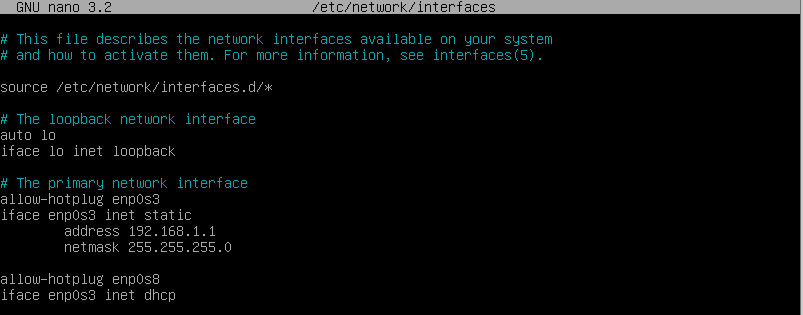
Cambiamos el nombre del cliente.



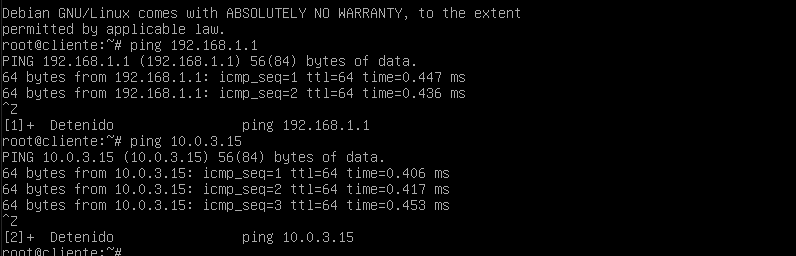
Configuramos los parámetros de red, en este caso el cliente va a tener un **IP STATIC**, y la puerta de enlace del cortafuego.



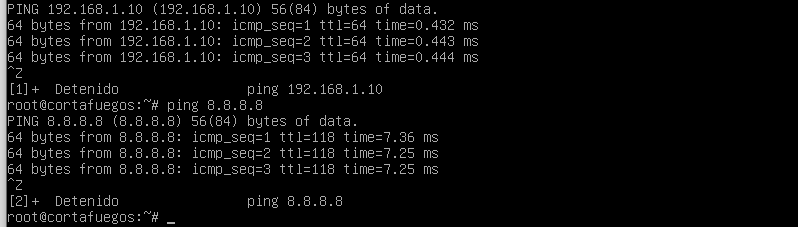
En el cortafuego tiene dos tarjetas de red, entonces vamos a configurar las dos, una en **STATIC** y la otra en **DHCP**.



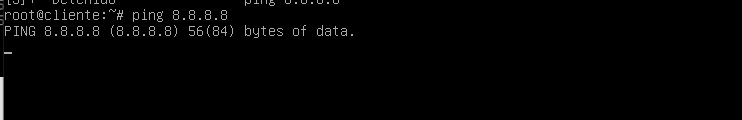
Hacemos un **PING** del cliente a las dos tarjetas de red del cortafuego.



Ahora hacemos **PING**, del cortafuego a **INTERNET** y otro al cliente.



Hacemos un **PING** desde el cliente a internet y veremos que no tenemos acceso a internet.



Ahora vamos a crear un **SCRIPT**, esto lo creamos dando la extensión **.SH.**

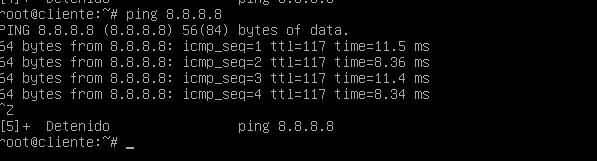


Creamos el SCRIPT poniendo **#!bin/bash**, después tenemos que crear un regla que nos cambie en el archivo IP\_FORWARD, el bit 0 por el bit 1.

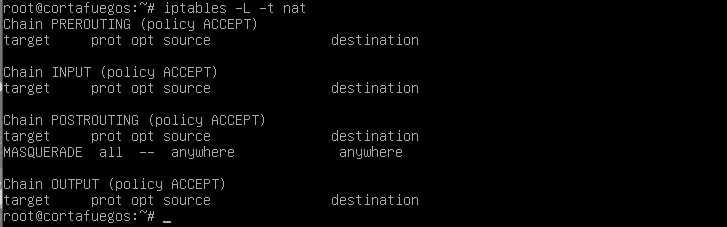
Para poder salir a internet tenemos que tener la siguiente iptable, que quiere decir que **–t nat –A POSTROUTIN –o enp0s3 –j MASQUERADE**, con esta línea le estamos diciendo que todo lo que pase por enp0s8 pueda tener conexión a internet, entonces el cliente tiene que tener conexión.



Hacemos el **PING** a internet desde el cliente y veremos que ahora si tenemos conexión.



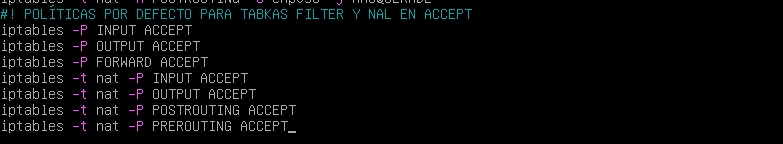
Para poder ver las iptables, en este caso las de nat, hacemos el siguiente comando y veremos las IPtables que hemos hecho.



Reglas que debes de definir:

• Políticas por defecto para tablas filter y nat en ACCEPT.

Las políticas por defecto están en **ACCEPT**, pero nosotros igualmente las vamos a poner, para ello tenemos que saber algunas cosas antes, con la letra –t le decimos que van a ser de nat, sino podemos nada por defecto son de filter y estas son las dos únicas con las que vamos a trabajar, después filter tiene 3 estados **INPUT(ENTRADA), OUTPUT(SALIDA), FORWARD(PASO)**, ponemos todas estas en **ACCEPT**, luego con nat tenemos **POSTRUTING Y PREROUTING**, las de nat se usa para redes.



Ahora vamos a ver las iptables de nat.

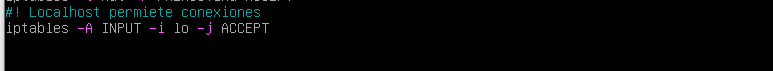


Después veremos las iptables de filter.



• Localhost permite conexiones.

Con la siguiente tabla le decimos que todas las entradas, mediante localhost, esto lo decimos con –i lo y luego ponemos todo en **ACCEPT**.

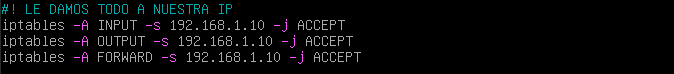


Ahora hacemos un filtrado de paquetes y veremos que la regla se ha ejecutado correctamente.

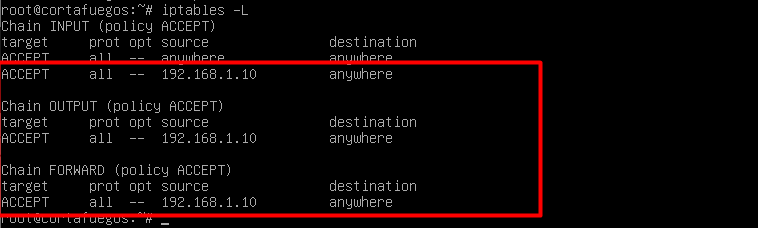


• A nuestra IP le dejamos todo.

Esto lo hacemos exactamente igual que aceptando cualquier política. Lo único que cambia es que le esta tiene puesto la **IP**, se lo estamos diciendo específicamente a nuestro cliente.



Ahora haremos un listado de todas las iptables y veremos que se han ejecutado correctamente, vemos que la IP está en **ACCEPT** en los 3 tipos de política de iptables que hay.

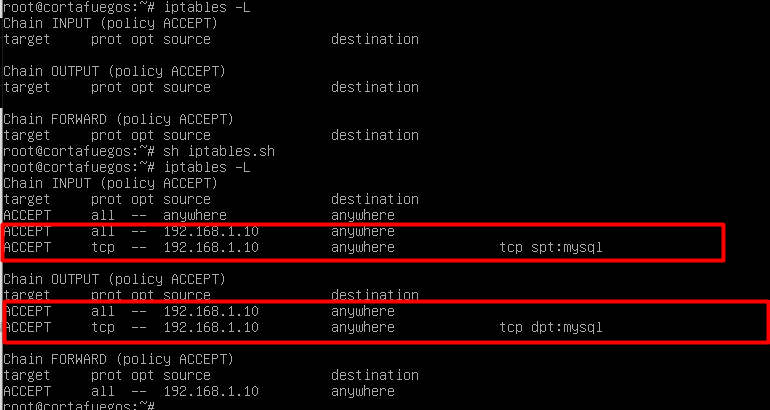


• A un compañero de trabajo, le dejamos acceder a mysql (3306).

Lo que vamos a hacer es que el cliente, solamente el cliente tenga acceso a 3306, le tenemos que decir el protocolo que va usar, luego tenemos que tirar 2 reglas, un dport y un sport.

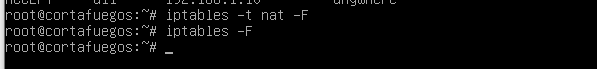


Ahora haremos un listado de iptables, para comprobar que las iptables que hemos lanzado se han generado correctamente.



• A un proveedor le permitimos acceso ftp.

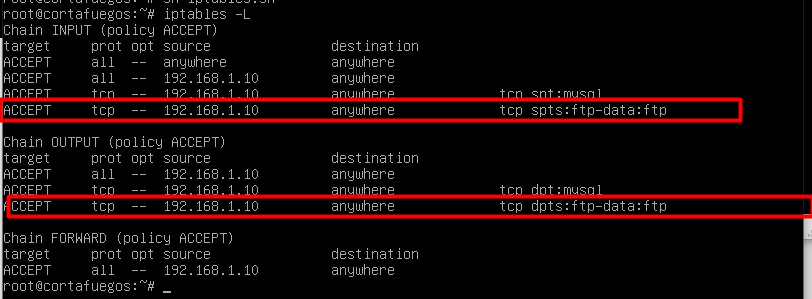
Para eliminar las iptables que tenemos anteriormente en el sistema, utilizamos los siguientes comandos, para eliminar las de **NAT** y las de **FILTER**.



Para permitir el acceso a **FTP**, hacemos los siguientes iptables, a la **IP** específica y a los puertos específicos de **FTP** y lo tenemos que poner en **ACCEPT**.



Hacemos un listado de las iptables y veremos que se han aplicado perfectamente.

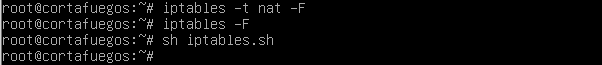


• El puerto 80 debe de estar abierto.

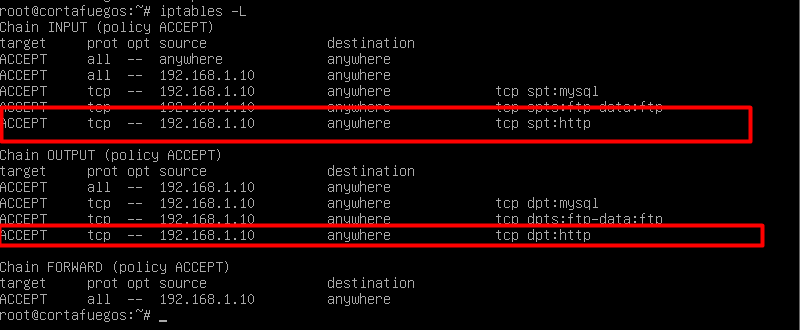
Para habilitar el puerto 80 hacemos lo mismo que hemos hecho anteriormente, para habilitar otros puertos, pero en este caso tenemos que poner que el puerto es el 80.



Eliminamos las iptables que teníamos de antes.

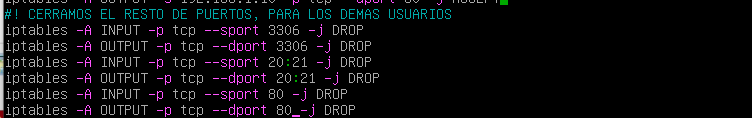


Vemos las iptables que acabamos de crear.

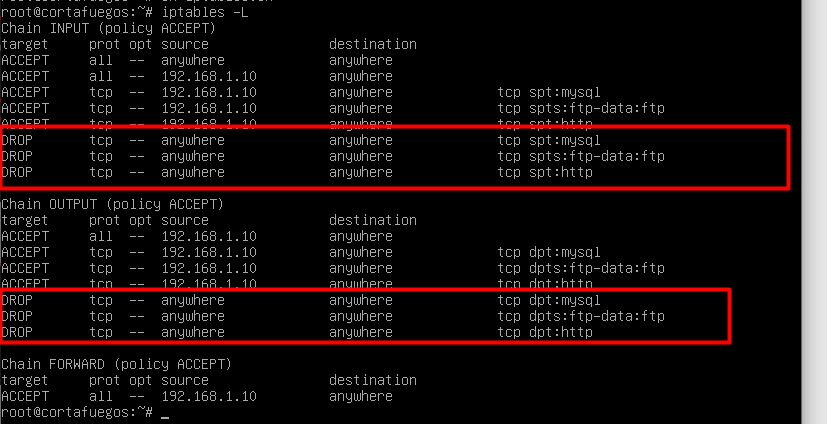


• El resto de puertos los cerramos, incluso los abiertos, para el resto de usuarios.

En este caso, tenemos que ver que puertos están abierto, en nuestro sistema y ver cuáles son, ponerlo y decirle que en vez de **ACCEPT**, ponerlos en **DROP**, que quiere decir que no les deja pasar, que está cerrado.

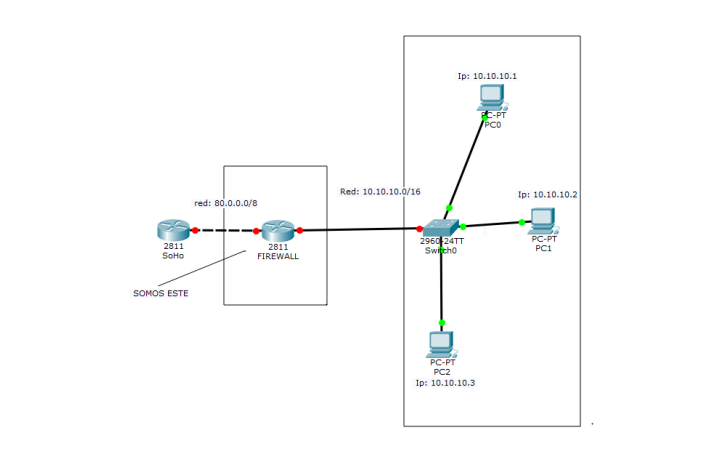


Ahora tenemos que ver las iptables que hemos lanzado con el comando **IPTABLES –L** y señalamos en rojo cuales son, para que visualmente sepamos mejor cuales son.

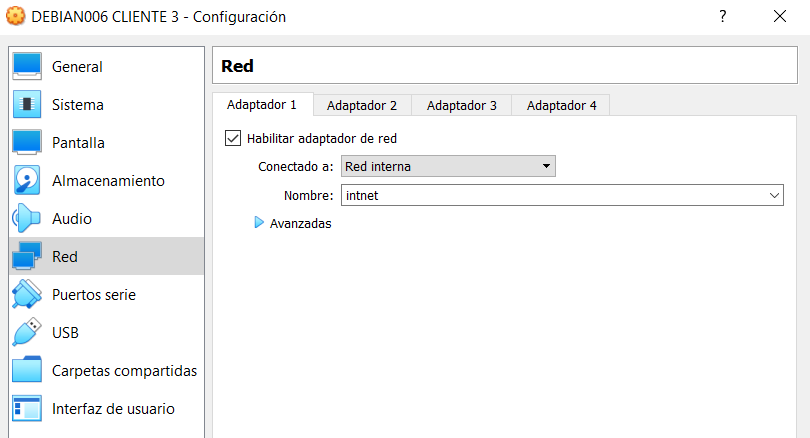


ESCENARIO 2:

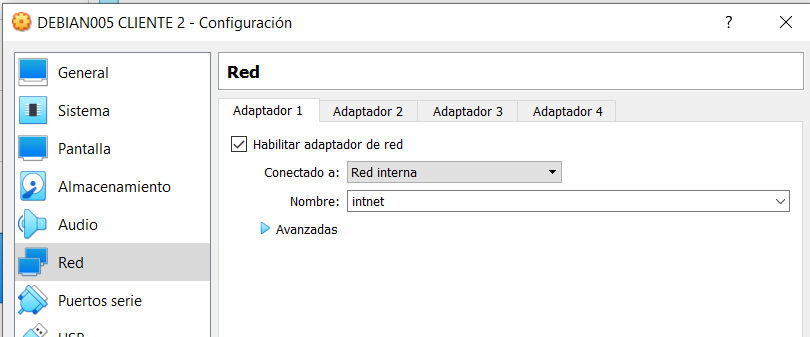
En un segundo escenario, tenemos una red local que se conecta a internet a través de un router SoHo, y queremos configurar un cortafuego que ponemos en el medio.



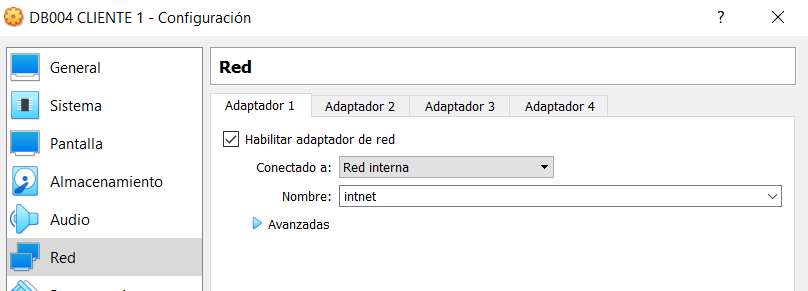
Empezamos configurando el escenario, poniendo las maquinas cliente en interna.



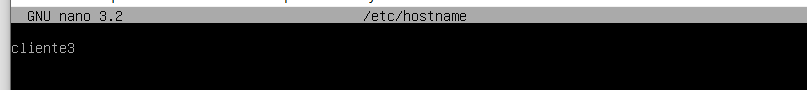
Ahora lo hacemos con la maquina cliente 2.



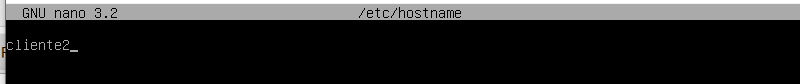
Por ultimo lo hacemos con la maquina cliente 1.



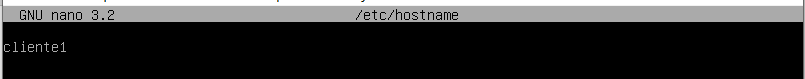
Cambiamos el nombre las maquinas en cada cada caso.



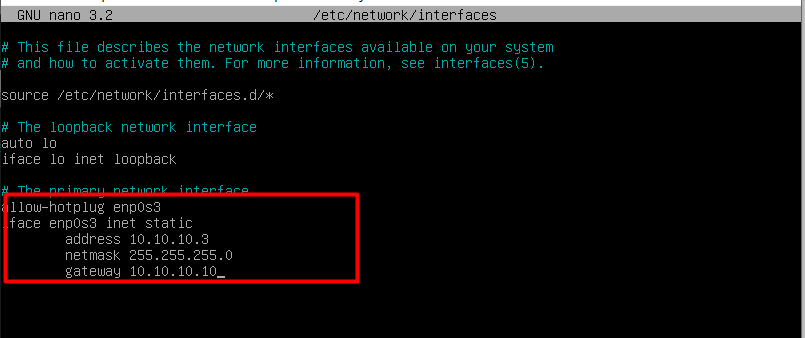
Ahora lo hacemos con el cliente 2.



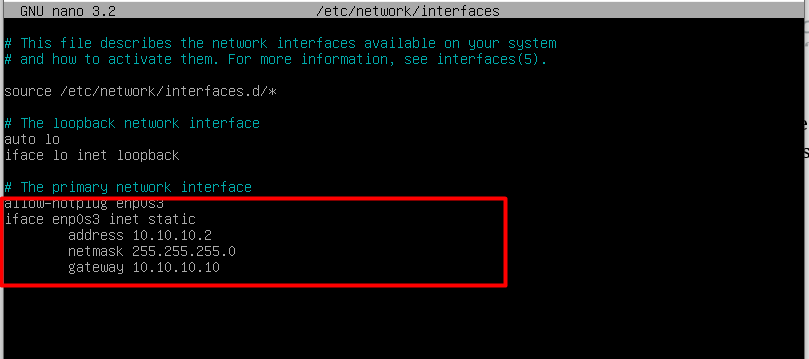
Ahora lo hacemos con el cliente 1.



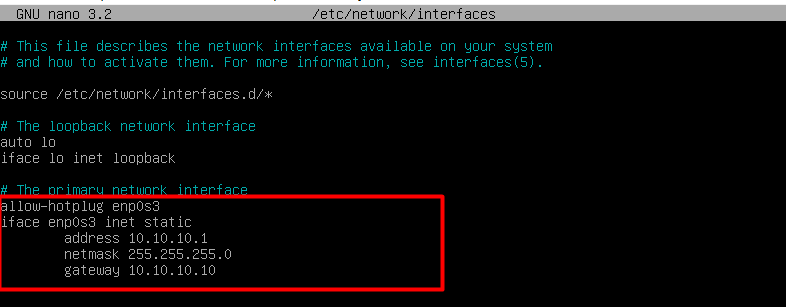
Configuramos la red de cada 1, con las **IP** dadas anteriormente en el escenario 2.



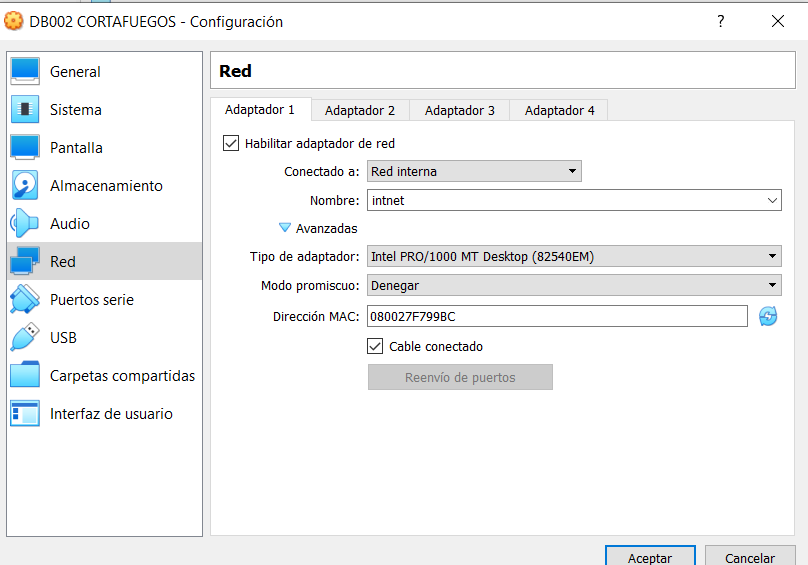
Hacemos lo mismo con el cliente 2.



Por ultimo configuramos el cliente 3 con los parámetros necsarios.



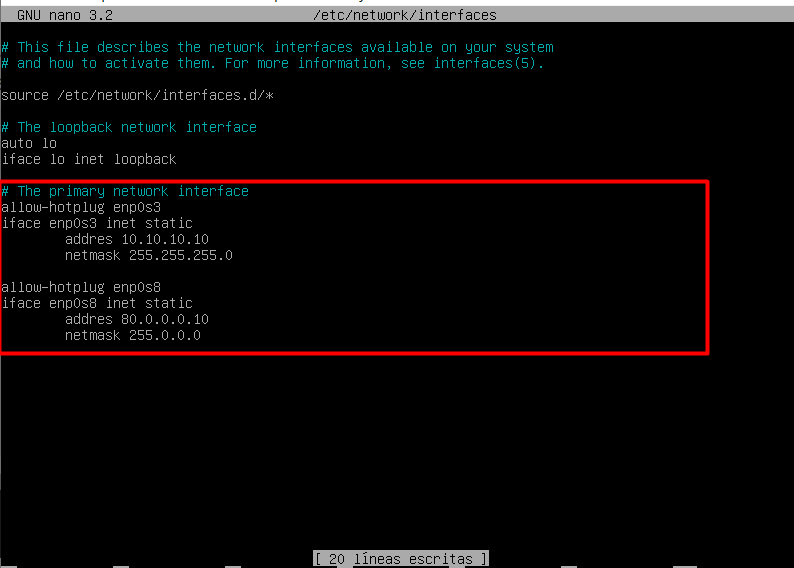
Ahora vamos a configurar el cortafuego, el cual va tener dos tarjetas de red, las dos en interna, para poder comunicarse con las dos redes que va tener, ósea va tener dos patas en dos redes diferentes.



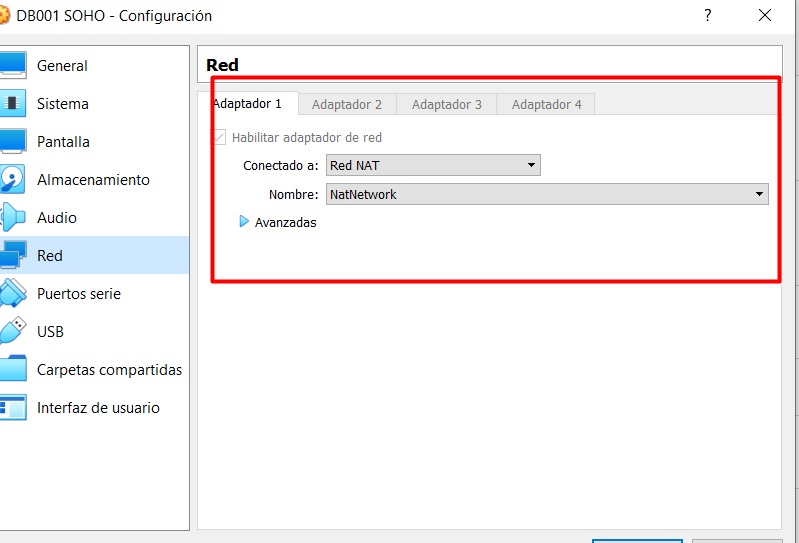
Ahora cambiamos el nombre del equipo que va ser nuestro cortafuego.



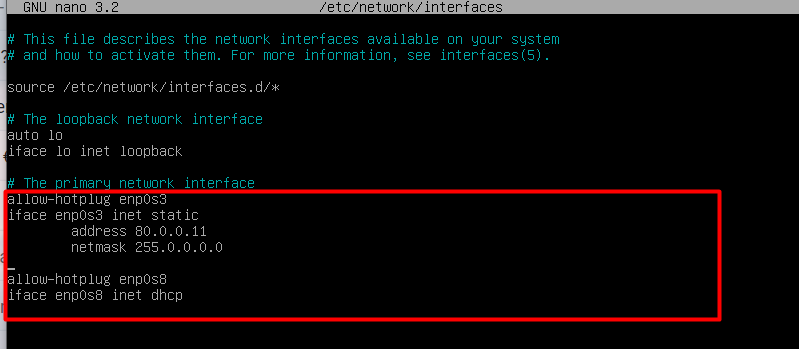
En este caso, tenemos que darle los parámetros necesarios a cada pata que tiene, es decir tenemos dos tarjetas de red y cada una tiene su configuración.



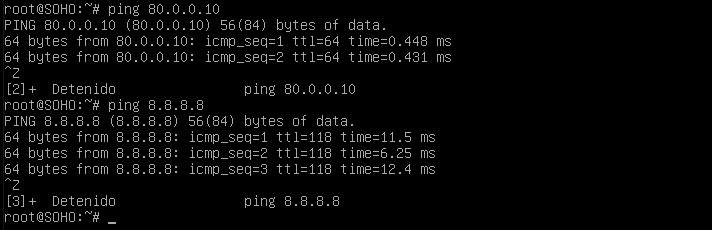
Por ultimo nos vamos a meter con nuestro **ROUTER** el cual va a tener una red nat y otra en interna, mediante dos tarjetas de red.



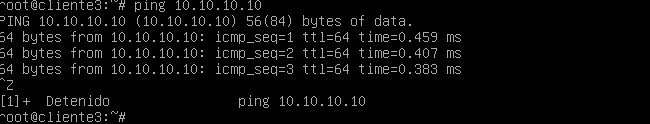
Como podemos apreciar una es mediante **DHCP**, la cual va ser la que tenga conexión a internet y la otra la que tenga conexión con la red de área local, la cual va a estar en **STATIC**.



Con esta máquina ahora hacemos ping a nuestro cortafuego, vemos que tenemos comunicación y otro a internet el cual también vemos que tenemos conexión.



Si probamos de un cliente cualquiera conexión con nuestro contafuegos tambien podremos ver que no hace ping, osea que tenemos comunicación entre ellos.



Ahora vamos a configurar el **ROUTER SOHO**, para poder tener conexión en nuestro cortafuego y en nuestro cliente, para ello primero tenemos que crear un script y decirle que en el fichero ip\_forward cambie el bit 0 por el bit 1, después tiramos una iptables que diga que podemos pasar hacia la otra enp0s8.



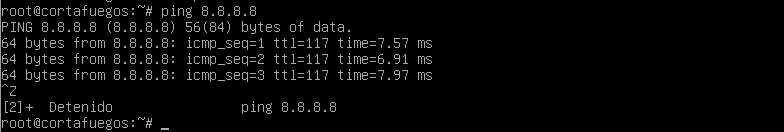
Ejecutamos el **SCRIPT**.



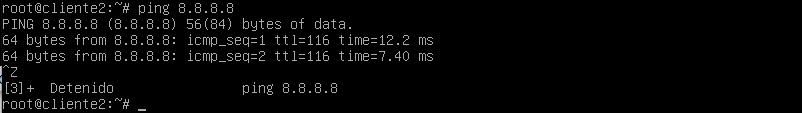
Ahora tienes que hacer lo mismo en nuestra máquina de cortafuegos.



Ahora realizamos un ping del cortafuego a internet y podemos comprobar que tenemos conexión a internet.



Ahora hacemos ping del cliente a internet.



Reglas que debes de definir:

• Elimina cualquier regla que pueda existir.

Lo primero que tendremos que hacer es crear un **SCRIPT** con el siguiente comando.



Ahora vamos a crear la regla de cambiar el primer bit a 1 y después vamos a decirle que elimine cualquier regla que haya en nat y en filter esto lo hacemos con las siguientes iptables.

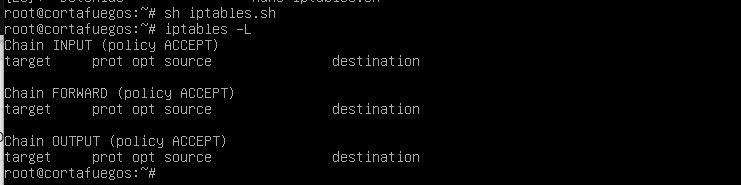


• Políticas por defecto para tablas filter y nat en ACCEPT.

Las políticas por sí están por defecto, pero nosotros igualmente se las vamos a poner como hicimos en el anterior escenario.



Luego vamos comprobar que esta todo en accept.



• Al cortafuego se tiene acceso desde la red local.

Para decirle al cortafuego que tenga acceso de área local, le tenemos que decir la red y la máscara que es, porque para va a entrar y salir y decirle que este en **ACCEPT**, esto es lo que quiere decir esta iptable.



Ahora vemos las iptables que hemos tirado anteriormente con el comando iptables –l.



• Activa el bit de FORWARDING.

Esto es lo más importante que podemos hacer al empezar a tirar iptables, porque necesitamos cambiar el bit a 1, para que puedan funcionar, luego yo podría dos reglas para eliminar todos las iptables que hubiesen antes, para tenerlo todo más limpio y ordenado.

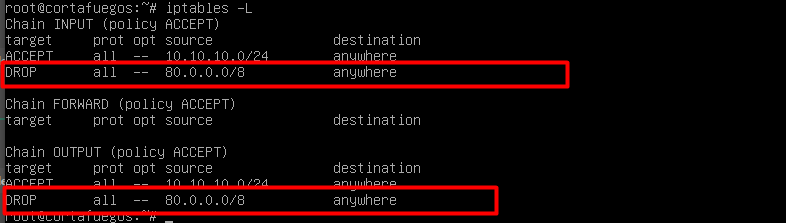


• Al cortafuego NO se tiene acceso desde la red pública.

Lo único que tenemos que hacer es denegar el acceso desde la red pública al cortafuego para que no se pueda conectar, esto lo haremos mediante una **IPTABLES –A INPUT –S 80.0.0.0/8 –I ENP0S3 –J DROP**, hacemos lo mismo para la salida, tenemos que recordar que esto lo tenemos que hacer para la salida y la entrada de paquetes.



Ahora vamos a comprobar que lo hemos hecho correctamente viendo las iptables que teniamos anteriormente.

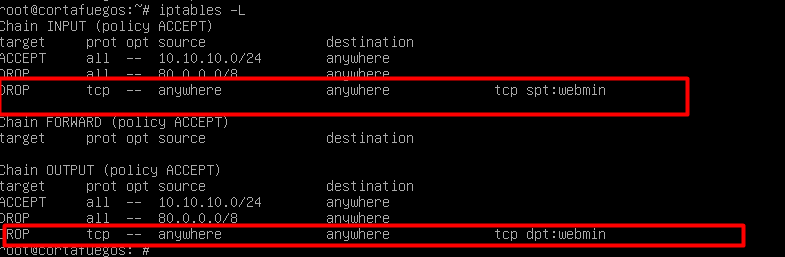


• Se cierra el puerto de gestión webmin (10000).

En esta hacemos lo mismo que hemos hecho anteriormente con otros puertos.

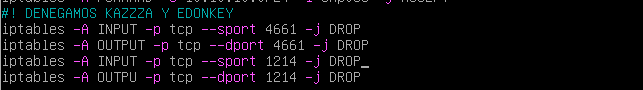


Vemos las iptables para comprobar que se ha ejecutado correctamente.



• Por otro lado, queremos que los trabajadores sólo puedan navegar por internet, pero no accedan, ni a Kazza o Edonkey.

Tenemos que denegar los siguientes puertos, con las siguientes iptables, lo denegamos con **DRO**P.

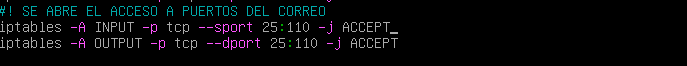


Ahora hacemos un iptables –L, para ver las iptables que hemos hecho.

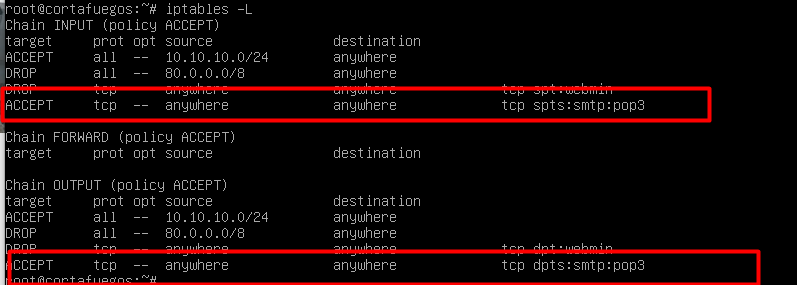


• Se abre el acceso a puertos del correo.

En este lo que tenemos que hacer es saber cuáles son los puertos de correo y en vez que anteriormente le hemos dicho a otros puertos que estén en **DROP**, ósea lo que quiere decir que estén desactivados, lo ponemos en **ACCEPT**.



Ahora comprobamos las iptables que hemos creado, las cuales están señaladas en rojo y dicen que están en accept.

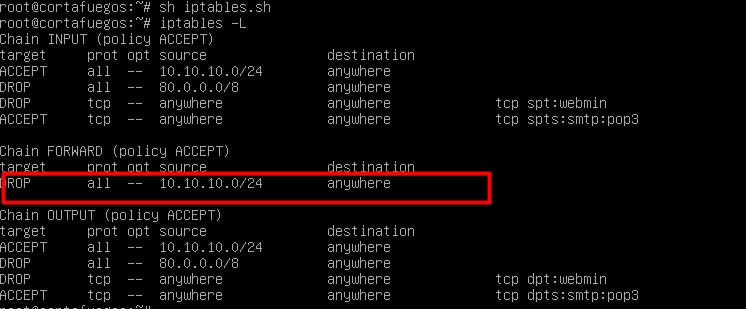


• El resto se deniega.

Que el resto se deniegan lo hacemos con un **FORWARD** –s la red en este caso la de área local –i que es la puerta por la que sale y –j le decimos que estén desactivadas.

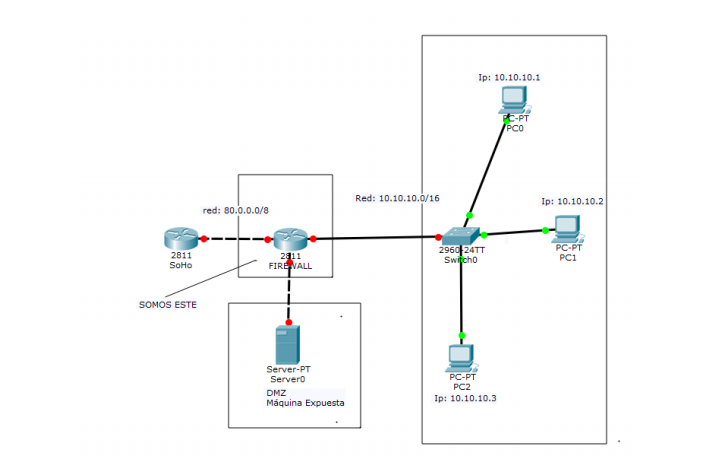


Luego vamos a volver a ver nuestra tabla de iptables, las cuales ya está bien llena de iptables y podemos comprobar que tenemos el **DROP** a las demás a esa red en específico.



ENCENARIO 3:

En un tercer escenario, se agrega al escenario anterior, una DMZ, cómo sigue:



En este tipo de escenarios el cortafuego debe de permitir:

• Acceso de la red local a internet.

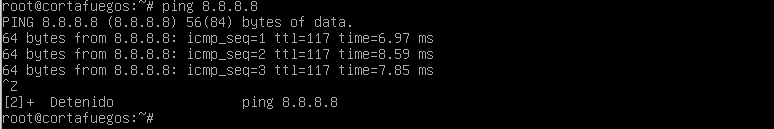
Como hemos hecho anteriormente, con el otro escenario, tenemos que configurar el acceso de red local a internet, para ello tiramos la misma iptable en el router.



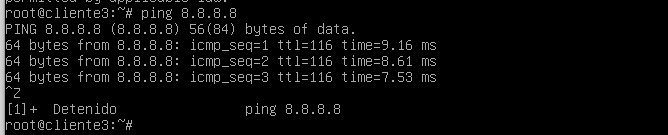
Hacemos lo mismo con el cortafuego.



Ahora comprobamos la conexión en el cortafuego con internet con el siguiente ping.

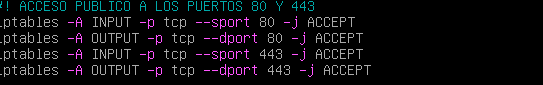


Ahora hacemos lo mismo con el cliente.

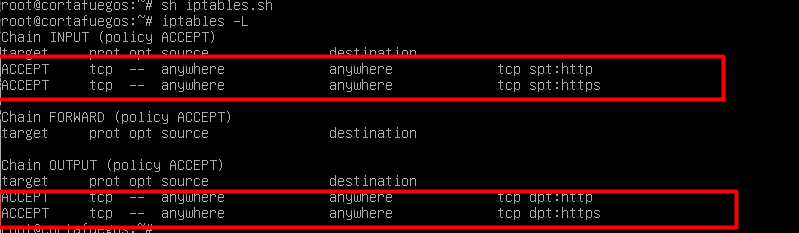


• Acceso público a los puertos 80 y 443.

Para permitir el acceso al puerto 80 y al puerto 443, tiramos las siguientes 4 reglas, que son las mismas que hemos tirado anteriormente en otras reglas, pero la única diferencia es que cambiamos los puertos y si lo queremos denegar o aceptar.

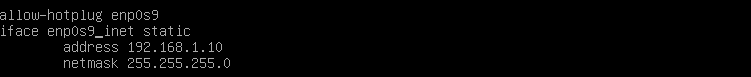
`

Ahora tiramos el **SCRIPT** y luego hacemos una iptables –L, para comprobar que se ha ejecutado correctamente las iptables que hemos creado anteriormente.

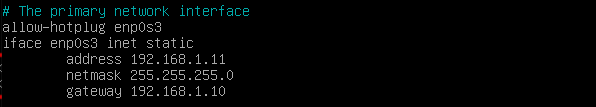


• Acceso del servidor DMZ desde una máquina concreta de la LAN.

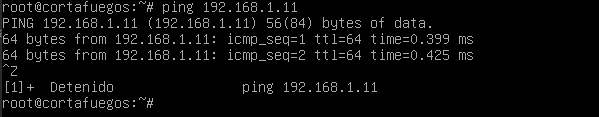
Para hacer este punto tenemos que añadir otra máquina más, la cual va a hacer de **DMZ (ES UNA ZONA DESMILATARIZADA**), lo que también tenemos que hacer es añadir una tercera tarjeta de red en nuestro cortafuego y darle la red que queramos, para que tenga comunicación con nuestro **DMZ**.



Ahora configuramos el **DMZ** con los siguientes parámetros de red, en este caso su puerta de enlace, va ser la **IP** de la tercera tarjeta de red del cortafuego.



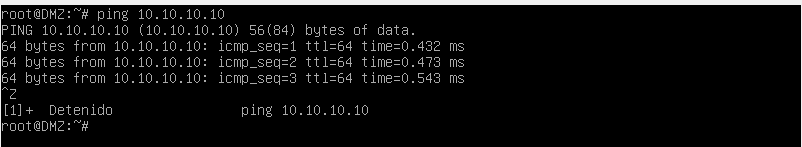
Ahora hacemos un ping del cortafuego al **DMZ** y podemos ver que perfectamente tenemos conexión.



Ahora si queremos que el **DMZ** tenga conexión con la red local, para ello le tenemos que decir que todo lo que entre por la siguiente red, lo acepte.



Ahora hacemos un ping del **DMZ** a la red local y podemos comprobar que tenemos conexión con la red local.



Reglas que debes de definir:

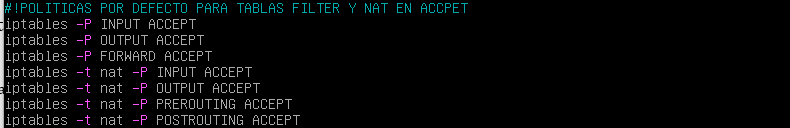
• Elimina cualquier regla que pueda existir.

Primero activamos el bit del forward a 1 y después le tenemos que decir que queremos que todas las reglas de filter y de nat nos las elimine, así podemos tener todo muchísimo más ordenado, cuando volvamos a ejecutar otra vez el **SCRIPT**.



• Políticas por defecto para tablas filter y nat en ACCEPT.

Estas políticas están por defecto, un así nosotros vamos ponerlas, para ello tenemos que poner las 3 que necesitamos en filter y las otras 4 que tenemos para nat.

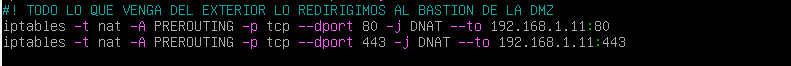


Ahora lo ejecutamos y veremos que se han realizado correctamente, podemos ver las reglas tirados tanto de iptables, como de nat.

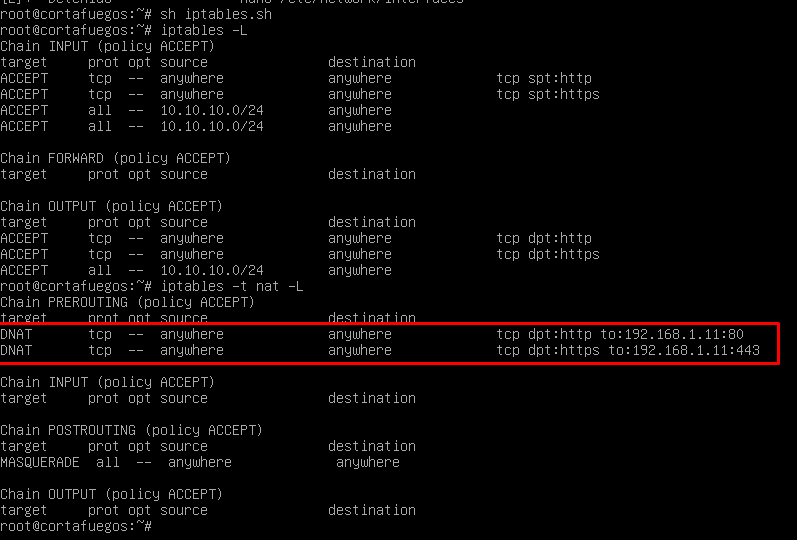


• Todo lo que venga del exterior y vaya al puerto 80 y al puerto 443, lo redirigimos al bastión de la dmz.

Estas son más largas, porque tenemos que dar más parámetros en estos casos, le tenemos que decir que todo lo que entre del puerto 80 y el puerto 443, nos lo redirige al **DMZ**.

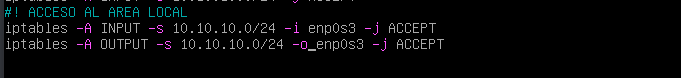


Ahora tenemos que hacer un iptables – t nat –L, para comprobar que las iptables de nat que hemos creado anteriormente se hayan guardado correctamente.



• Al cortafuego se tiene acceso desde la red local.:

Para que el cortafuego tenga acceso a la red local tenemos que tirar dos iptables una de entrada para decirle que todo lo que entre pueda ir y otra de salida para decirle que todo lo que salga pueda salir hacia esa red, esto suele estar por defecto en **ACCEPT**, ponemos la red a la cual quiere llegar y por la pata que está conectada a esa red.



Ejecutamos el **SCRIPT** y después hacemos una **iptables –L**, para ver que se ha hecho correctamente.



• Tanto firewall como red local, tienen acceso al exterior.

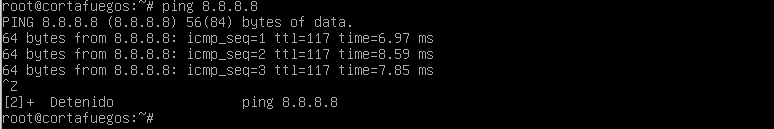
Para poder tener conexión al exterior en el cortafuego y en los clientes, tenemos que tirar las siguientes reglas, la cuales son las mismas que hemos tirado anteriormente.



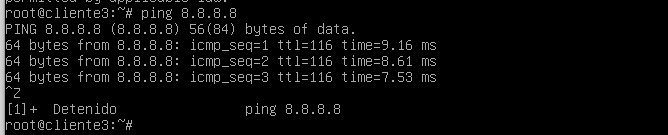
Ahora la tiramos en el cortafuego.



Hacemos ping del cortafuego a internet.



Hacemos un ping del cliente a internet.



• El resto de la LAN se cierra a la DMZ.



