**Dibujo de una persona

Descripción generada automáticamente con confianza baja**

IPTABLES

**CARLOS GONZÁLEZ MARTÍN**

Contenido

[1. Configuración de red 3](#_Toc187909307)

[2. Cambiar nombre a la maquina 3](#_Toc187909308)

[3. Instalación de paquetes 4](#_Toc187909309)

[4. Iptables 4](#_Toc187909310)

[5. Comprobaciones iniciales 4](#_Toc187909311)

[6. Creación del archivo de configuración 6](#_Toc187909312)

[7. Modificación del archivo de configuración 6](#_Toc187909313)

[8. 1ª comprobación 7](#_Toc187909314)

[9. 1ª regla iptables 8](#_Toc187909315)

[10. 2ª regla iptables 9](#_Toc187909316)

[11. 3ª regla iptables 10](#_Toc187909317)

[12. Script finalizado 11](#_Toc187909318)

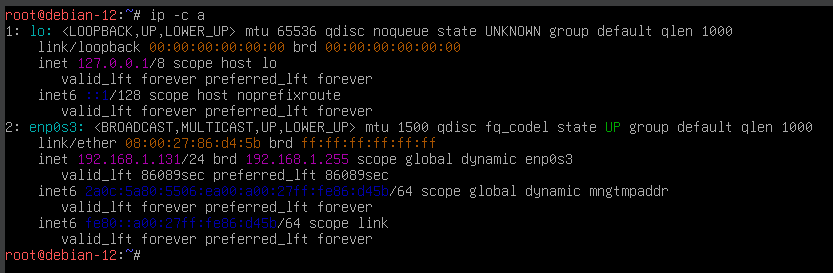
[13. Bastión 12](#_Toc187909319)

[14. Comprobación del cliente 13](#_Toc187909320)

[15. Conclusión 14](#_Toc187909321)

# Configuración de red

Vamos a poner la maquina en adaptador puente para así conectarnos a los diferentes servicios que están en la máquina.

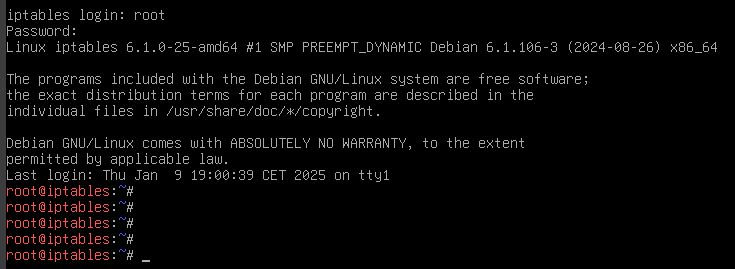


# Cambiar nombre a la maquina

Mediante el siguiente comando cambiamos el nombre a la máquina.

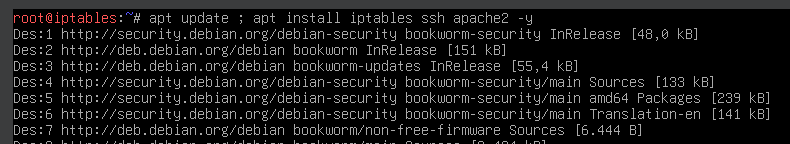


Una vez que le demos a exit e iniciamos sesión veremos que ha cambiado el nombre a la máquina.



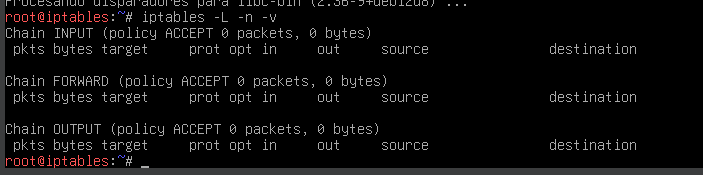
# Instalación de paquetes

Ahora instalaremos el paquete iptables y los servicios como ssh y apache2, ping no lo instalaremos por que viene de serie habilitado en debían.



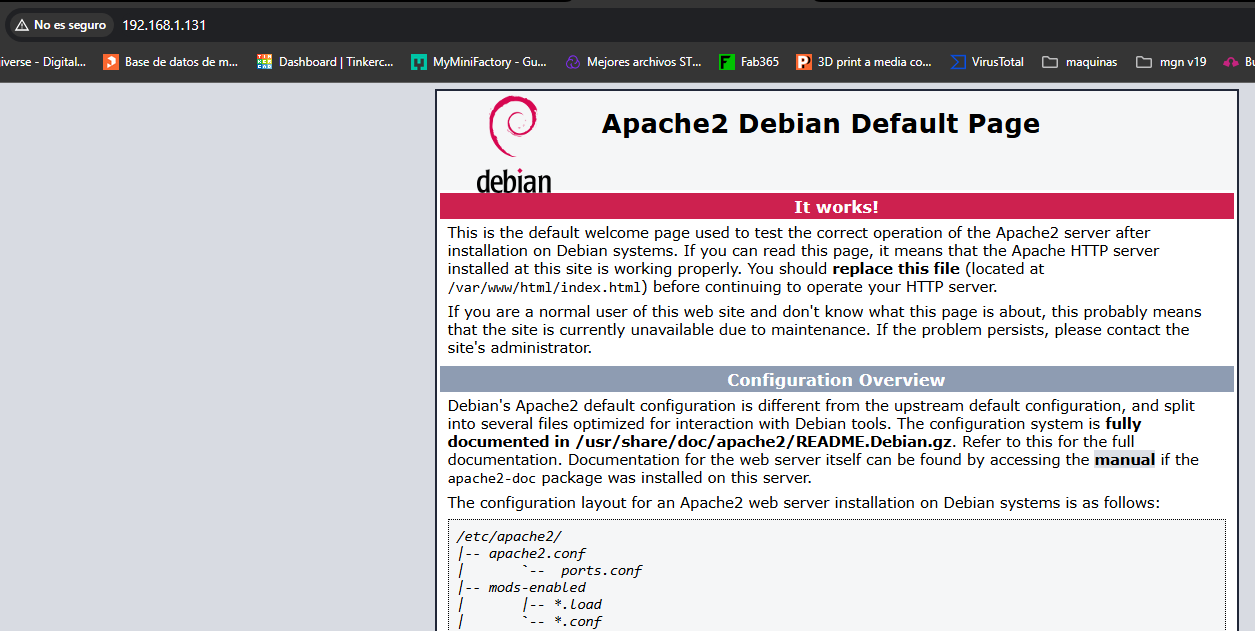
# Iptables

Ahora vamos a comprobar si hay alguna regla de iptables habilitada.

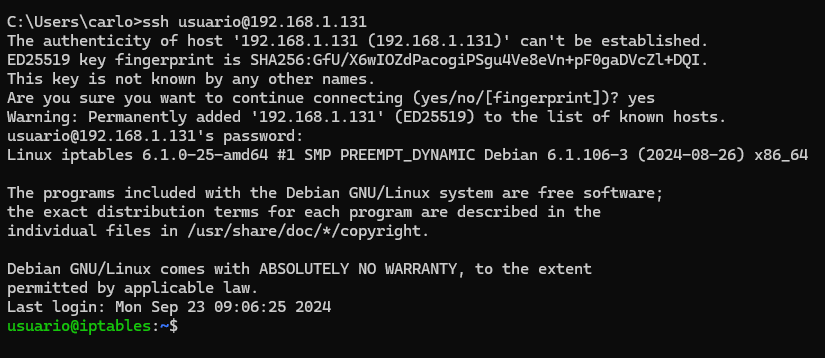


# Comprobaciones iniciales

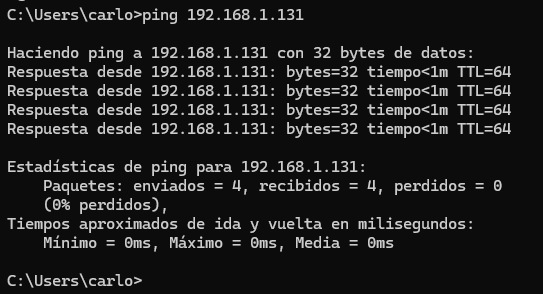
Ahora vamos a conectarnos con los diferentes servicios que tiene el servidor que hemos instalado anteriormente.



Ahora vamos a comprobamos mediante ssh.



Ahora vamos a hacer ping.

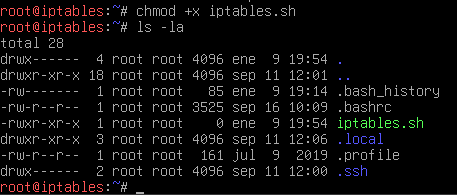


# Creación del archivo de configuración

Ahora crearemos el archivo de configuración de iptables.

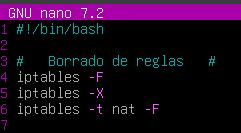


Ahora le daremos permisos de ejecución al archivo creado anteriormente.

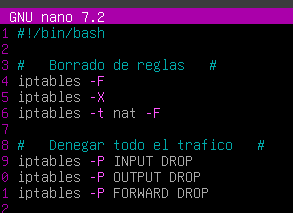


# Modificación del archivo de configuración

Abrimos el archivo de configuración y haremos un borrado de reglas.

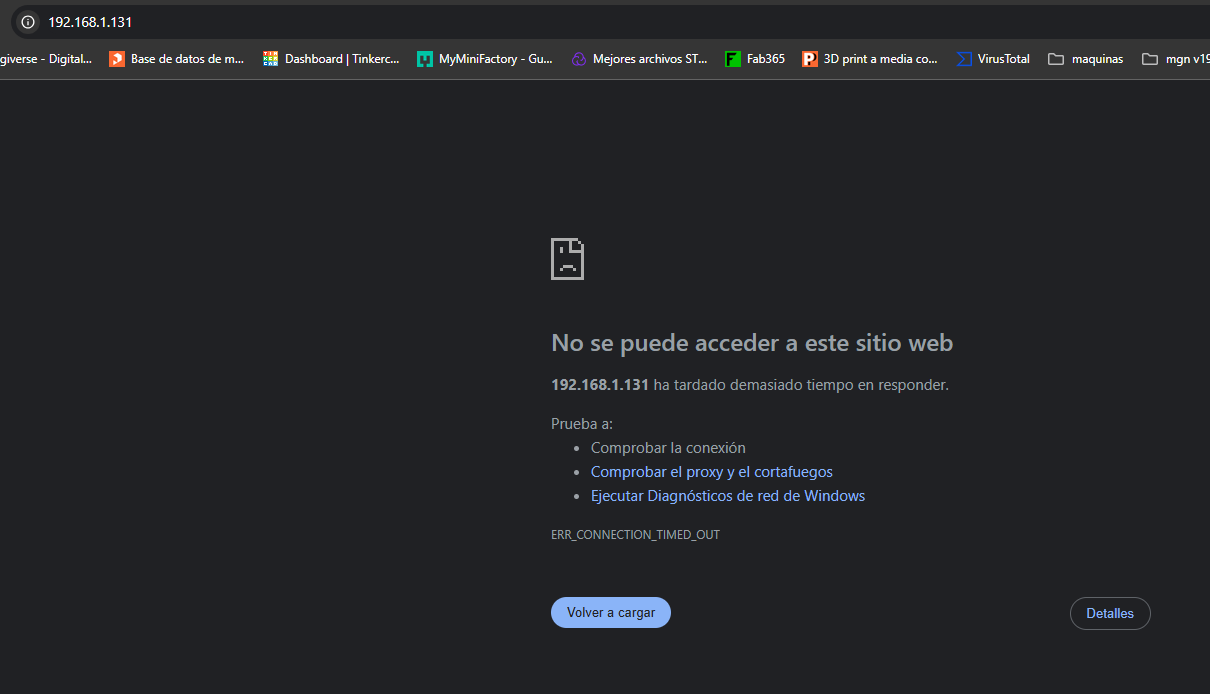


Ahora como vamos a denegar todo el trafico entrante pondremos las siguientes reglas.

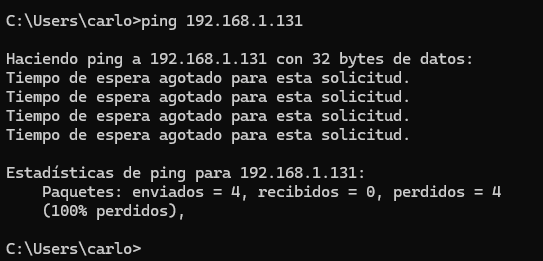


Una vez que ejecutemos el script vamos a comprobar si nos deniega todo.

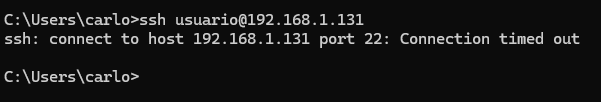
# 1ª comprobación



Ahora vamos a comprobar con un ping.

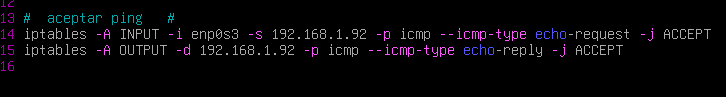


Ahora vamos a conectarnos por ssh.

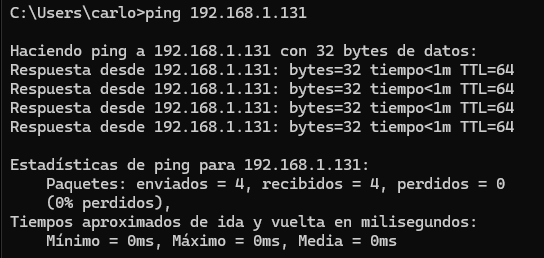


# 1ª regla iptables

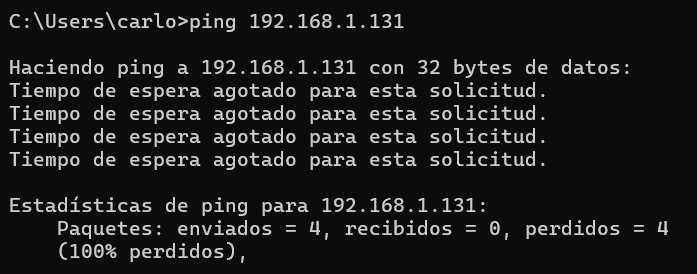
Ahora lo que haremos será crear la primera regla de iptables que acepte el ping de la maquina real.



Ahora haremos la ejecución del script y comprobaremos si funciona en la maquina real.

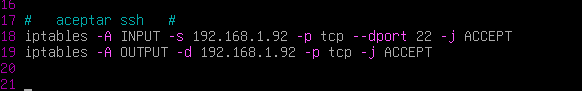


Ahora vamos a comprobar con otro equipo si nos acepta el ping.

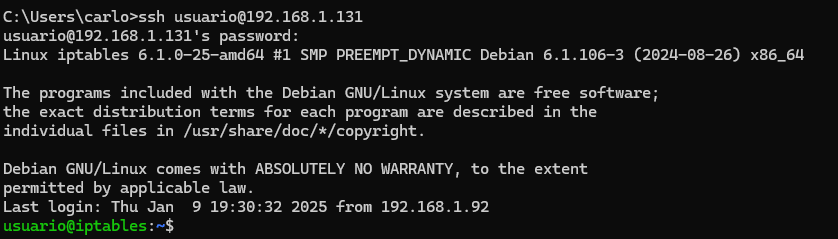


# 2ª regla iptables

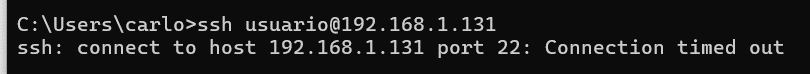
Ahora lo que haremos será permitir solo conexiones por ssh de la maquina real.



Ahora vamos a comprobar con la maquina real.

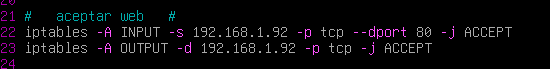


Ahora vamos a comprobar con otro equipo de la red.

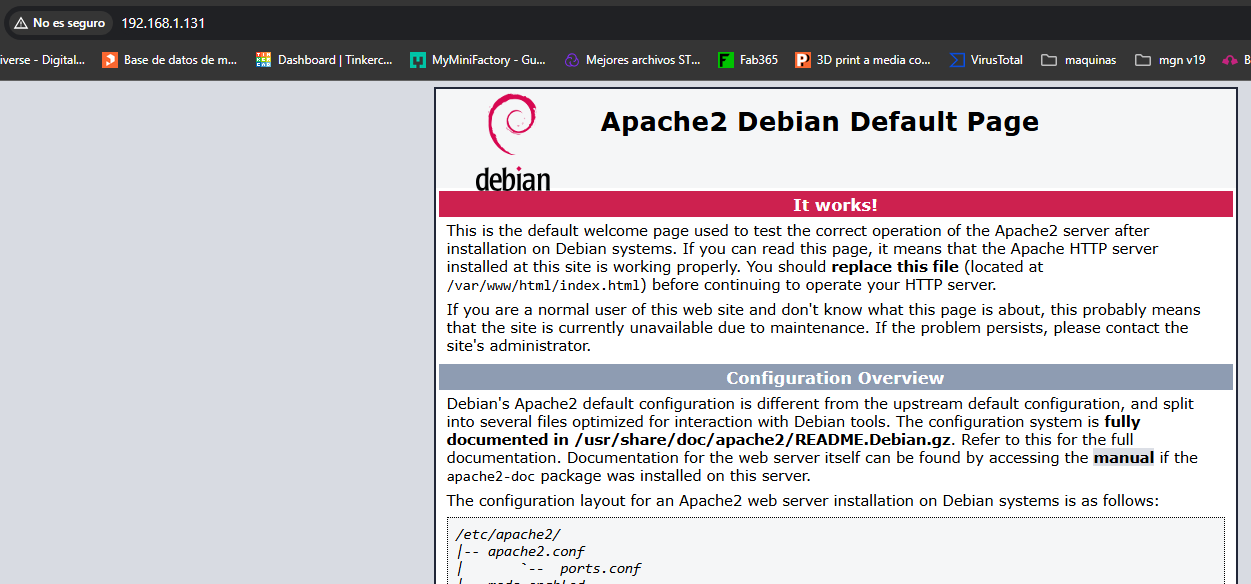


# 3ª regla iptables

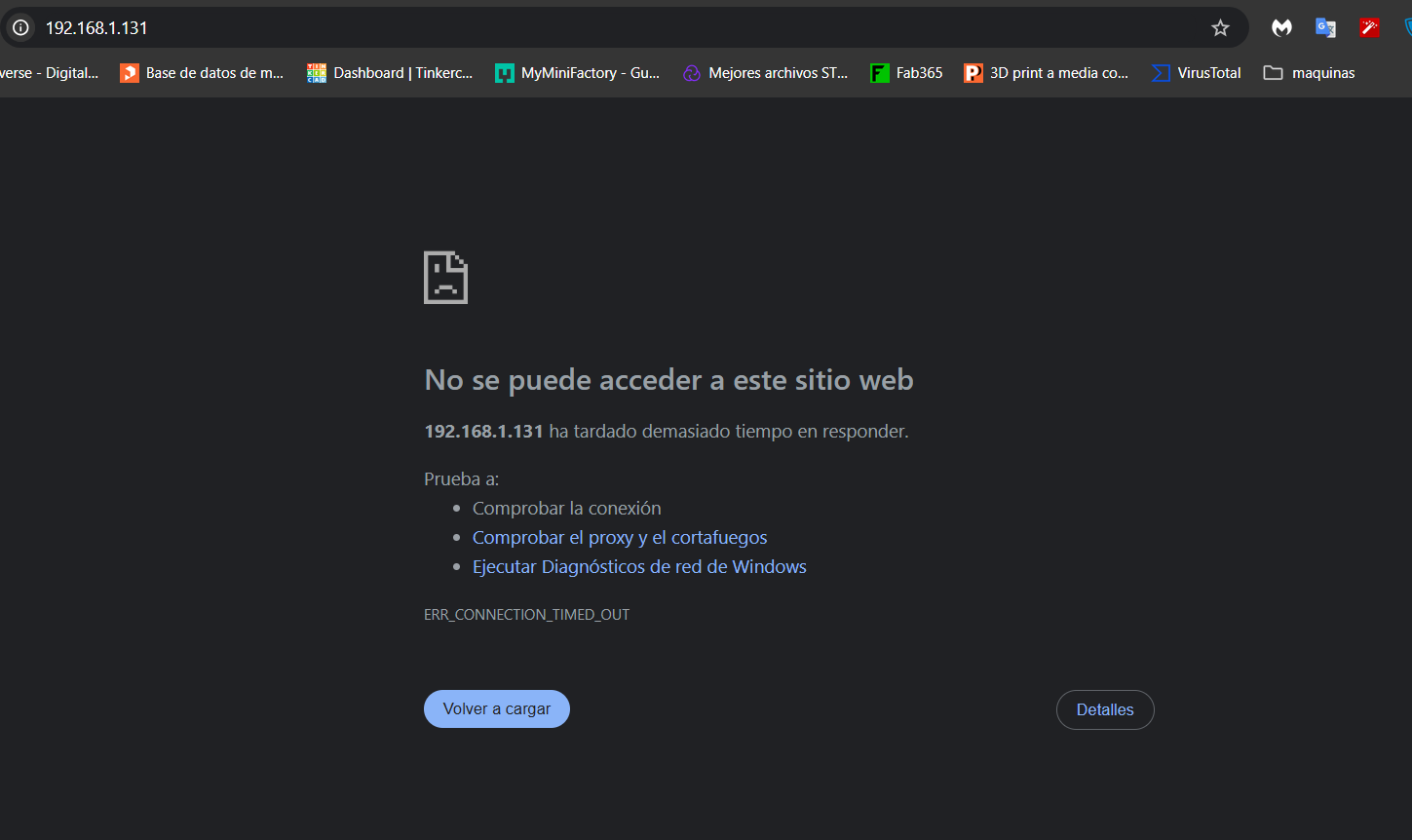
Ahora lo que haremos será aceptar que podamos ver la pagina web en la maquina real.



Ejecutamos el script y comprobaremos la maquina real.

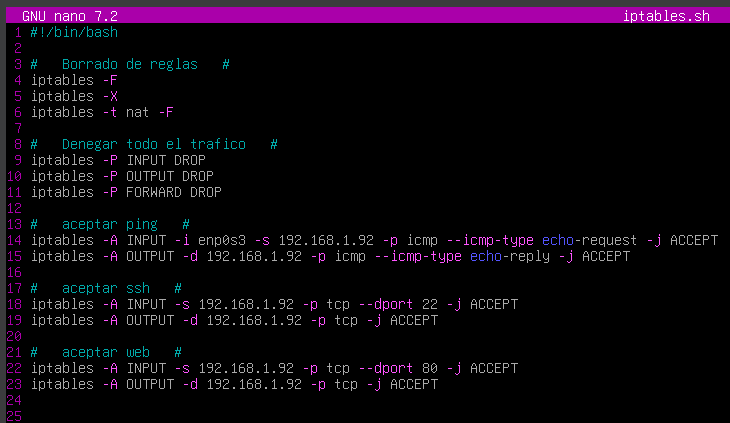


Usando otro equipo comprobaremos.

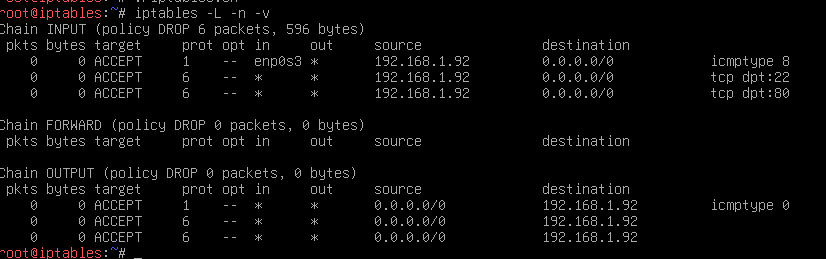


# Script finalizado

Ahora vemos todas las reglas que hemos creado.



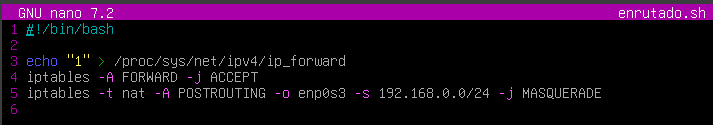
Ahora vamos a hacer un iptables -L -n -v y vemos las reglas creadas.



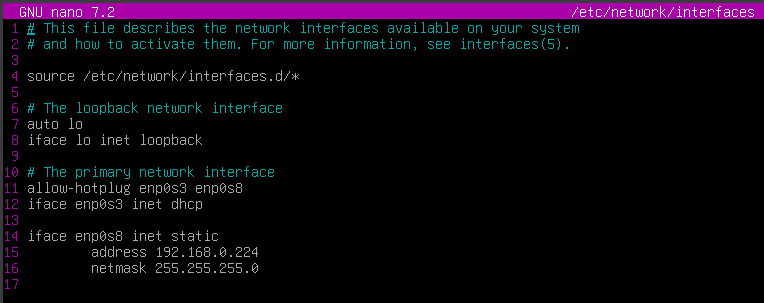
# Bastión

Ahora lo que haremos será usar este equipo como bastión, para que el cliente que esta en una interfaz en modo red interna pueda comunicarse con el exterior.

Este es el archivo de configuración de enrutador.

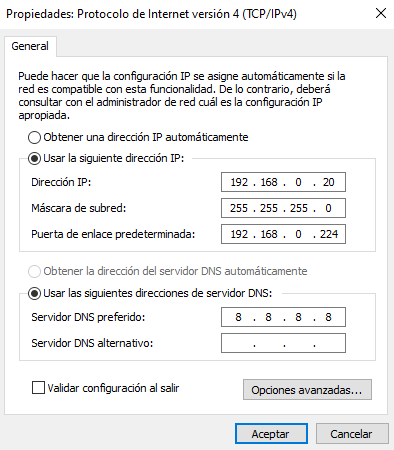


Ahora tenemos que poner la segunda interfaz en red interna y escribir las IPs.

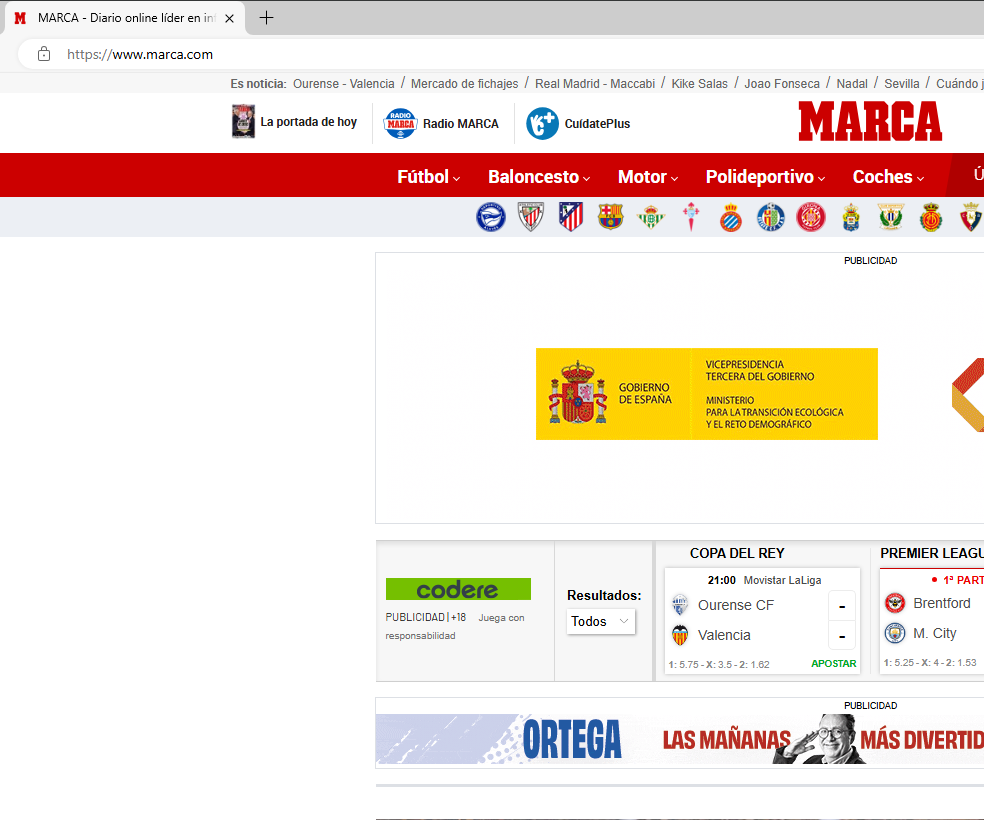


# Comprobación del cliente

Ahora vamos a configurar las IPs en el cliente y probaremos ya que anteriormente ejecutamos el script.



Ahora vamos al navegador y buscamos alguna pagina web, en mi caso es marca.com.



# Conclusión

Al implementar reglas en iptables para denegar el tráfico HTTP, SSH y ICMP, se ha logrado un primer nivel de protección contra ataques comunes.

La creación de una cadena personalizada para permitir el acceso al equipo 192.168.1.92 a través de SSH ha demostrado la potencia de iptables para establecer políticas de acceso granulares. Durante la práctica, se observó la importancia del orden de las reglas y la necesidad de realizar pruebas exhaustivas para evitar bloquear el tráfico legítimo.

Esta experiencia ha consolidado mis conocimientos sobre iptables y me ha permitido comprender la importancia de una configuración precisa y segura del firewall.