UNIVERSIDAD FRANCISCO DE VITORIA

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERÍA INFORMÁTICA

SEGURIDAD

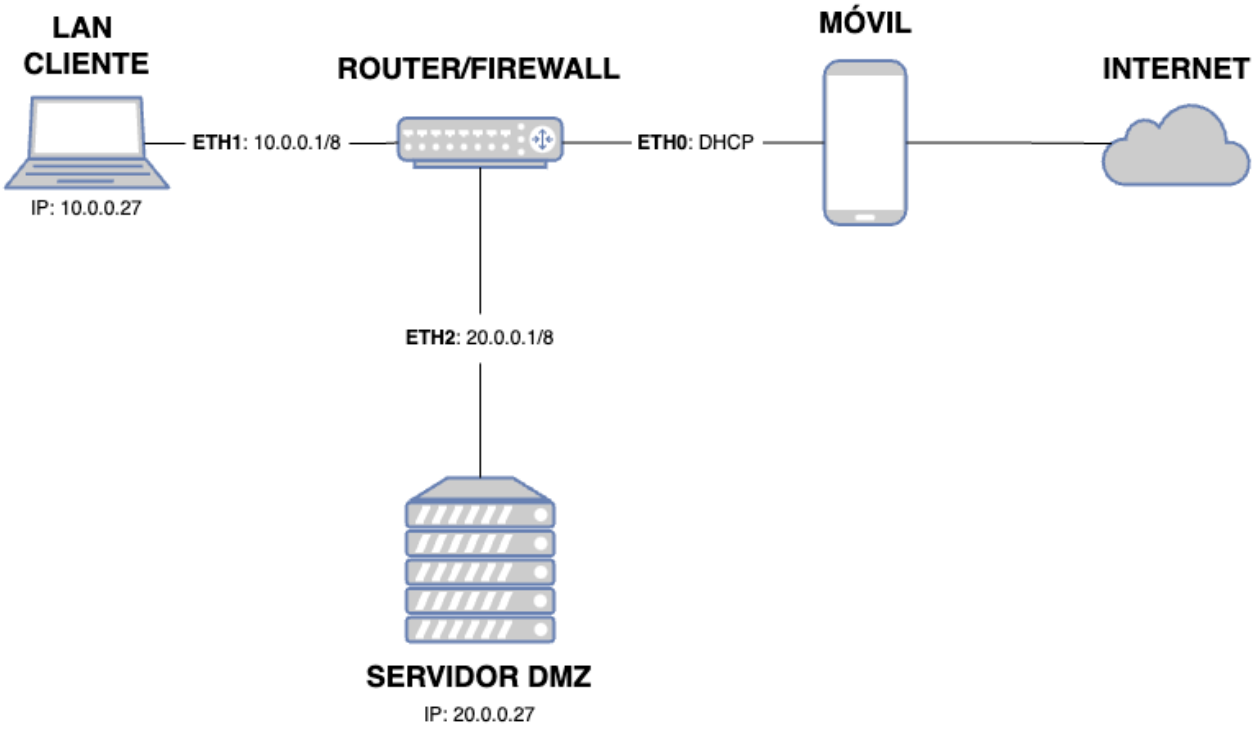
PRÁCTICA 2

Diego Viñals Lage, Javier Garrido Cobo

TABLA DE CONTENIDO

TABLA DE IMÁGENES

1 MAQUETA DE LA INFRAESTRUCTURA RED



Podemos ver en este dibujo como tenemos estructurado la infraestructura red de nuestra práctica, se pueden ver las ips de cada equipo y el Gateway de cada tarjeta de red wifi.

2 PASOS PARA LA ELABORACIÓN

Se detallarán los pasos a seguir para realizar el diseño descrito en la imagen mostrada anteriormente. En primer lugar, se deberá clonar la máquina virtual creada en la práctica 1, la cual contendrá la web configurada con un servidor DNS propio.

2.1 AÑADIR TARJETAS EN EL FIREWALL

Esta máquina ha sido clonada y se le ha modificado el nombre a "Firewall". Podemos verificar el cambio de nombre utilizando el comando "hostname":

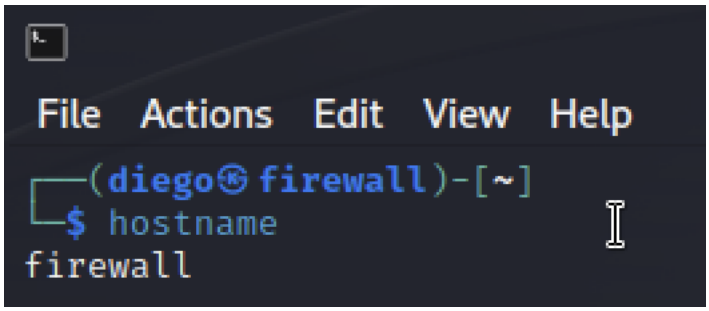


Ilustración 1: Cambio de nombre a máquina Firewall

En esta máquina se han añadido tres tarjetas WiFi, cada una configurada en modo puente. Una de ellas estará en modo dinámico para proporcionar conexión a Internet, mientras que las otras dos tendrán asignados los Gateways para la máquina cliente y la máquina DMZ.

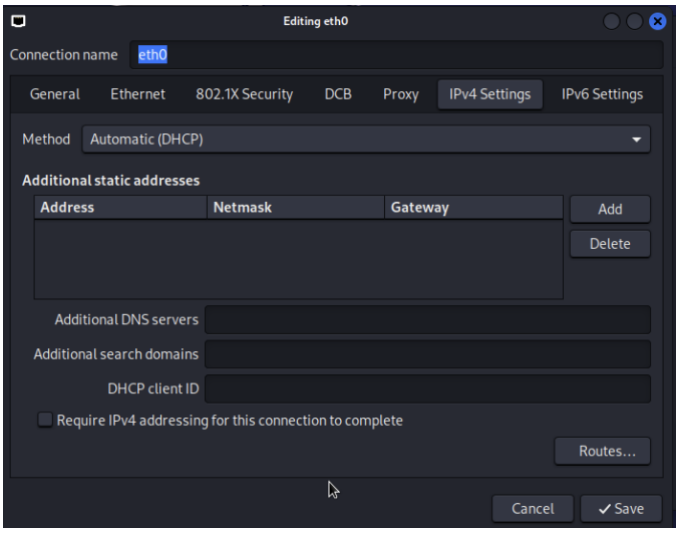


Ilustración 2: Tarjeta eth0 con ip dinámica

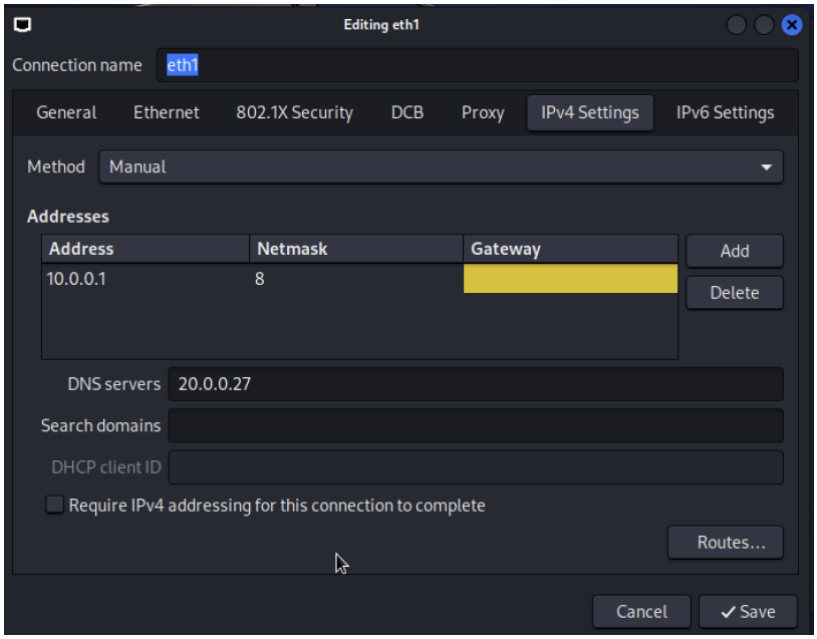


Ilustración 3: Tarjeta eth0 con IP fija

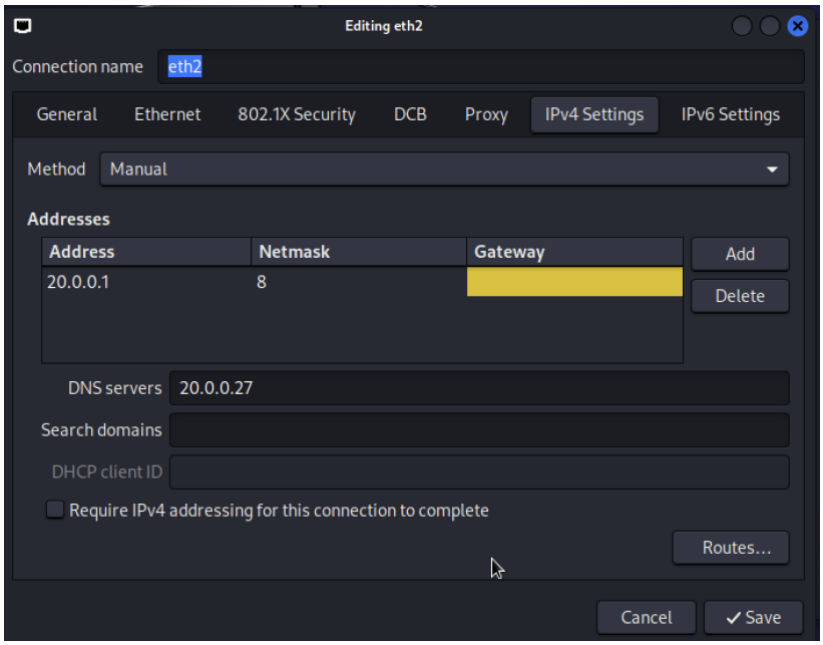


Ilustración 4: Tarjeta eth2 con IP fija

2.2 CAMBIAR IP DEL DMZ

En esta máquina, se ha modificado la dirección IP para establecerla como una dirección IP fija, tanto en el servidor DNS como en el Gateway, utilizando los valores indicados en el esquema del apartado 1.

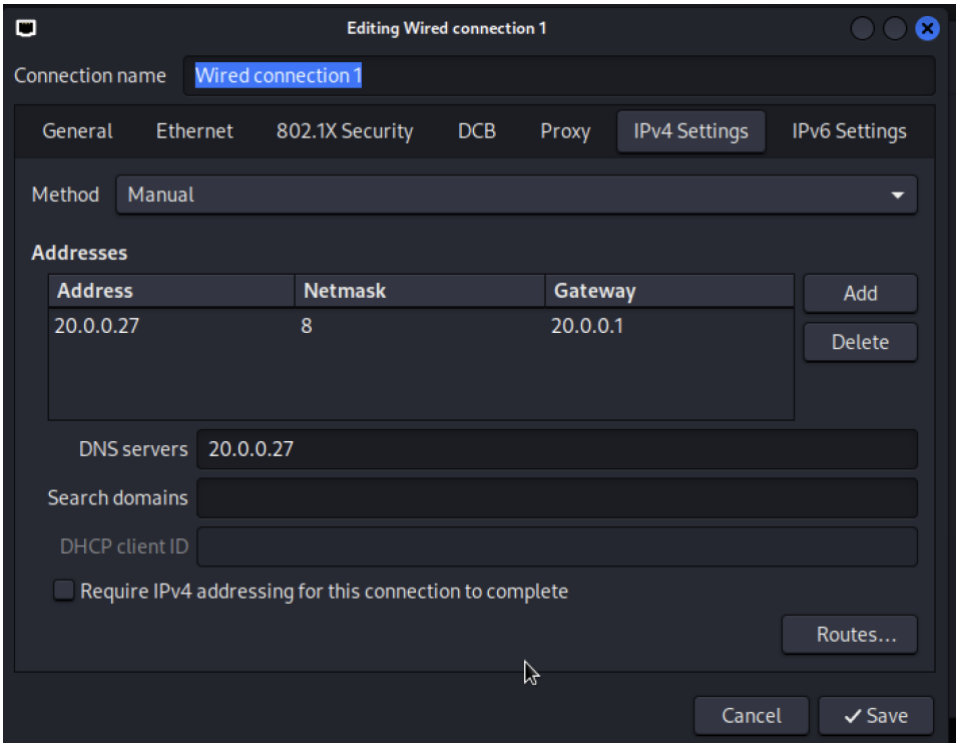


Ilustración 5: IP de la Maquina DMZ

En esta máquina, es recomendable reiniciar los servicios Named y Apache2 para garantizar que la web se muestre correctamente. Para simplificar este proceso, se ha creado un script que ejecuta ambas instrucciones.

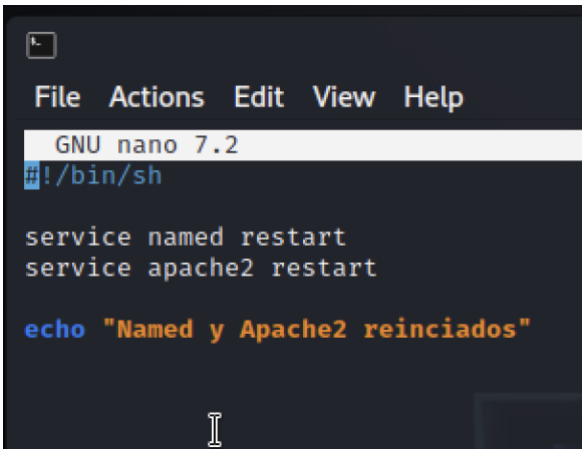


Ilustración 6: Script para reiniciar servicios

2.3 Maquina Cliente (Ubuntu)

En esta máquina, se ha modificado la dirección IP del servidor y se ha añadido el servidor DNS de la máquina DMZ. Dado que estamos utilizando un Mac M1, no fue posible instalar Ubuntu Desktop, por lo que optamos por instalar Ubuntu Server y agregar la interfaz gráfica por separado. Sin embargo, al hacer esto, no se mostraron automáticamente las opciones de configuración de red, lo que nos obligó a realizar los cambios a través del terminal.

Ilustración 7: IP de la maquina LAN (Cliente)

Una vez completado este proceso, las máquinas serán capaces de comunicarse entre sí, y hemos confirmado esta conectividad al realizar pruebas de ping entre todas ellas.

2.4 Creación Reglas del Firewall

Se deberán crear una serie de reglas de firewall que se ejecutarán a través de un script, el cual se adjuntará junto con la presentación de este informe. Las reglas resultantes son las siguientes:

Ilustración 8: Reglas Firewall

Ilustración 9: Reglas Firewall nat

Con estas reglas, se garantiza que solo se tenga acceso a lo deseado en el contexto de la práctica.

3 DEMOSTRACION DE PRUEBAS

3.1 PRUEBA 1 (1.5 PUNTOS)

Pantallazo donde se vea que desde la LAN se accede al servidor SSH de la DMZ.

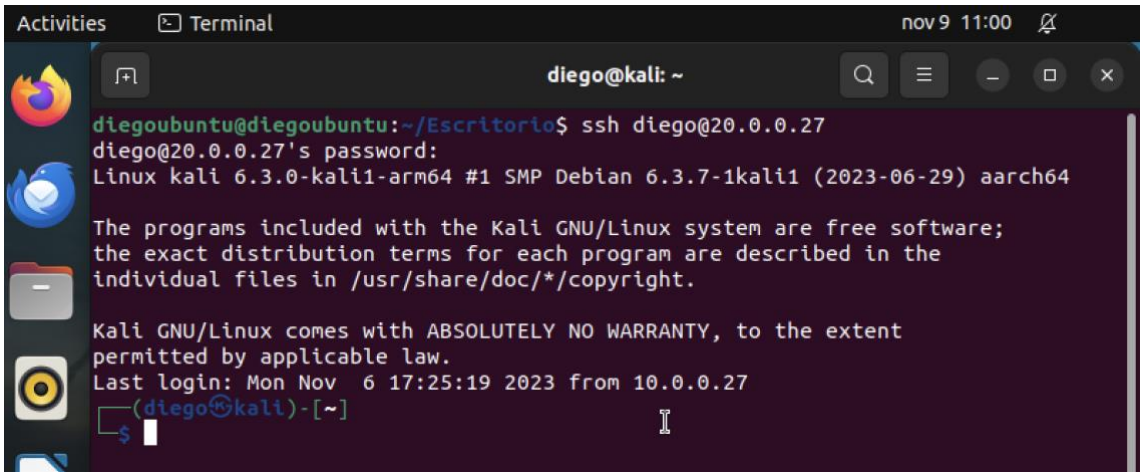


Ilustración 10: Prueba 1: SSH

3.2 PRUEBA 2 (1.5 PUNTOS)

Pantallazo donde se vea que desde la LAN se accede a la página web de la DMZ mediante el nombre DNS creado.

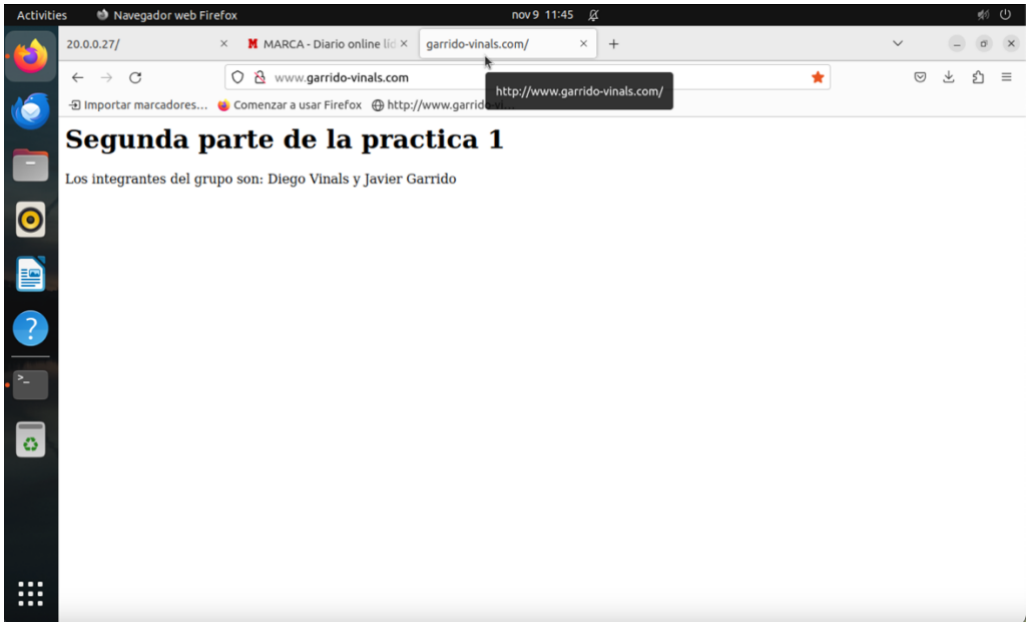


Ilustración 11: Prueba 2: Acceder a web DMZ desde LAN

3.3 PRUEBA 3 (3 PUNTOS)

Pantallazo donde se vea que desde la LAN se accede a Internet.

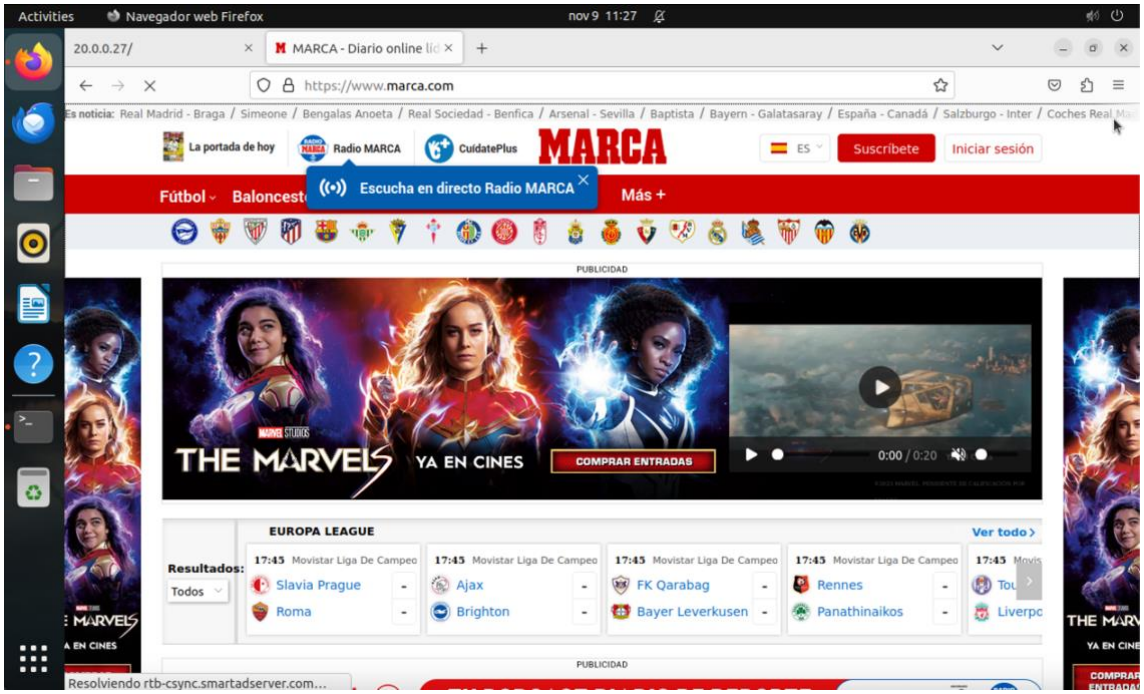


Ilustración 12: Prueba 3: LAN accede a internet

3.4 PRUEBA 4 (3 PUNTOS)

Pantallazo donde se vea que desde un equipo que no tiene una IP de la LAN ni de la DMZ (puede ser el propio móvil) se accede a la página web de la DMZ por la IP del servidor.

Ilustración 13: Prueba 4: Acceder a web desde el Móvil