Universidad Nacional Autónoma de México

Facultad de Ciencias

...

T E S I S

QUE PARA OBTENER EL GRADO DE:

Licenciatura en Ciencias de la Computación

P R E S E N T A :

Pérez Romero Natalia Abigail

TUTOR

Dr. José David Flores Peñaloza

Ciudad Universitaria, Cd. Mx., 2023

Dedicatoria ...

Agradecimientos

Índice general

Prefacio

Contenido de la tesis

Panorama general

Objetivo

Capítulo 1

Introducción

1.1. Protocolo IP

El protocolo IP (Internet Protocol) Junto con el protocolo TCP (Transmission Control Protocol) son los dos protocolos más importantes en el Internet.

IP determinará el formato de los paquetes de datos que se envían y reciben a través de la red. TCP se encargará de la transmisión de los datos.

Existen dos versiones de IP, la versión 4 (IPv4) y la versión 6 (IPv6). La versión 4 es la más utilizada en la actualidad, pero se está migrando a la versión 6 debido a la falta de direcciones IP disponibles en la versión 4.

1.2. Protocolo TCP

El protocolo TCP (Transmission Control Protocol) es un protocolo de transporte orientado a conexión. TCP se encarga de la transmisión de los datos de manera fiable, es decir, garantiza que los datos lleguen a su destino en el orden correcto y sin errores. TCP también se encarga de controlar el flujo de datos, es decir, de evitar que el emisor sature al receptor con datos.

1.3. Protocolo UDP

El protocolo UDP provee un servicio de transporte no orientado a conexión. UDP es más simple que TCP, ya que no tiene control de flujo, control de errores, ni retransmisión de paquetes.

1.4. VPN

Las VPN (Virtual Private Network) son redes privadas virtuales que permiten a los usuarios conectarse a una red privada a través de una red pública, como Internet. Las VPN se utilizan para proteger la privacidad y la seguridad de la información transmitida a través de la red.

1.5. Wireguard

Wireguard es un protocolo de VPN de código abierto y de alto rendimiento. Wireguard es más simple y más rápido que otros protocolos de VPN, como OpenVPN y IPsec.

1.6. NAT

NAT (Network Address Translation) es una técnica que permite a varios dispositivos compartir una única dirección IP pública. Esta técnica ha sido de gran utilidad ante la escasez de direcciones IP en IPv4. NAT traduce las direcciones IP privadas de los dispositivos de una red local a una única dirección IP pública.

1.7. NAT Translation Table

1.8. IP Masquerade

IP Masquerade que permite a una red local compartir una única dirección IP pública, similar a un NAT one-to-many encontado en un router.

Es particularmente útil en un host de Linux que tiene un modem y actua como PPP (Point to Point Protocol) o SLIP server, permitiendo a los clientes de la red local acceder a Internet si estos no tiene direcciones IP públicas.

1.9. IP Forwarding

1.10. Tablas de routeo

1.11. IPTables

IPTables es una herramienta de configuración de firewall en sistemas operativos basados en Linux. Entre sus funciones se encuentran el filtrado de paquetes, redireccionamiento de paquetes, traducción de direcciones de red, etc.

1.12. Relay network

Capítulo 2

Desarrollo

2.1. Casos de uso

2.1.1. Identificación del usuario

En esta primera version no nos preocuparemos de que la información del usuario se transmita de forma segura, por lo que el usuario deberá identificarse con un nombre de usuario, correo electrónico y contraseña. Que será enviada al orquestrador en texto plano para su verificación.

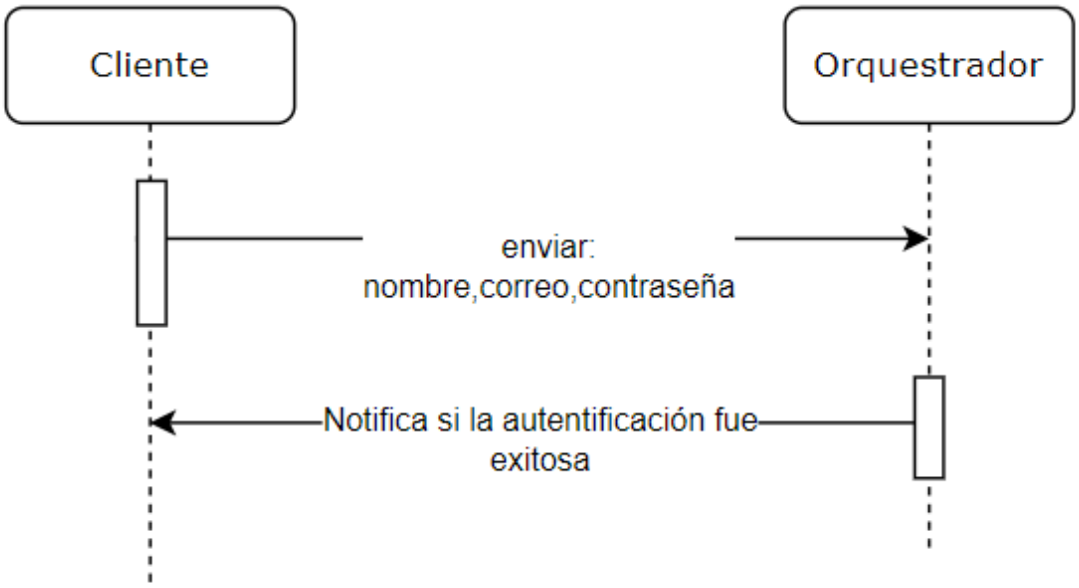

Figura 2.1: Diagrama de caso de uso: identificación del usuario

Registro de usuario

En el registro del usuario se deberá solicitar al usuario su nombre, correo electrónico y contraseña, que será enviada al orquestrador en texto plano para su registro, si es exitoso el orquestrador deberá enviar un mensaje de confirmación al usuario.

2.1.2. Registro de una red privada

Deseamos que el usuario pueda registrar las redes privadas a las que desea conectarse, para ello se deberá implementar un mecanismo de registro de redes privadas. El cliente deberá enviar un mensaje al orquestrador con el nombre de la red privada que desea crear, si la red privada existe el orquestrador deberá notificar al cliente, si la red

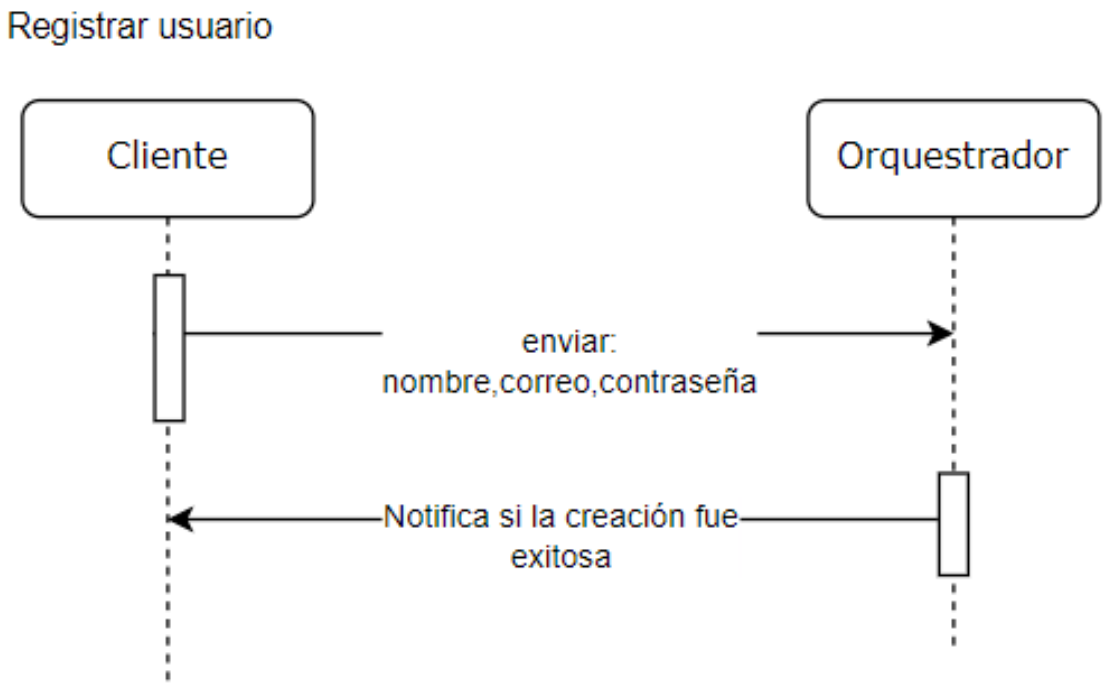

Figura 2.2: Diagrama de caso de uso: registro de usuario

privada no existe, el orquestrador deberá crearla y enviar un mensaje de confirmación con la información siguiente: IP asignada, rango, mascara de la red privada creada.

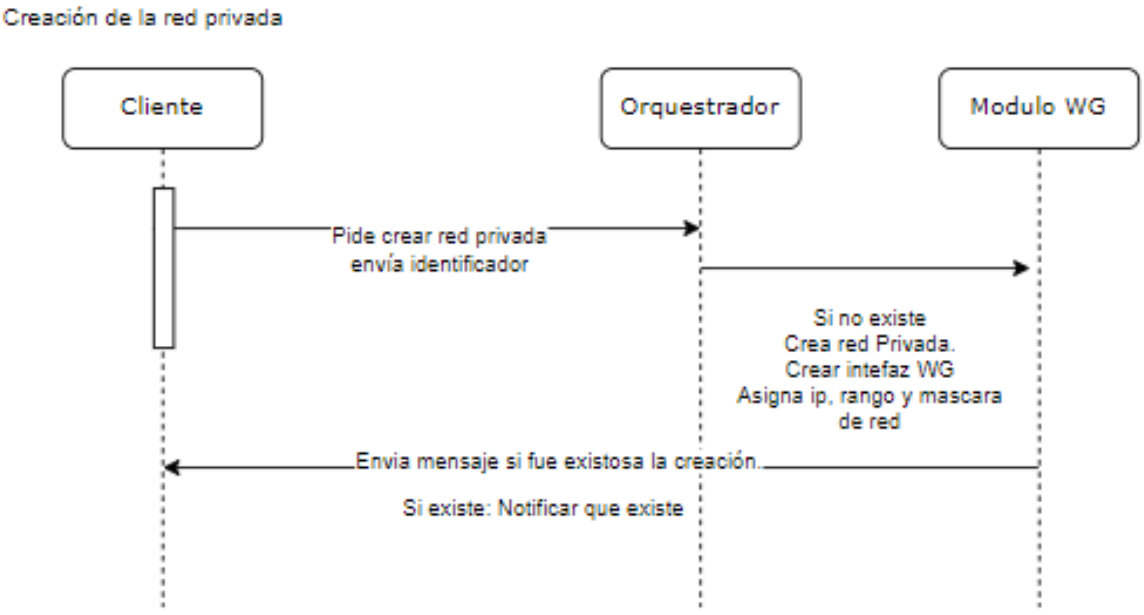

Figura 2.3: Diagrama de caso de uso: registro de red privada

Una red privada desde el punto de vista del orquestrador es un objeto que contiene la siguiente información:

- Identificador
- Nombre de la red privada
- Lista de dispositivos finales
- Lista de conexiones

2.1.3. Registro de un dispositivo final

Uno de los objetivos del orquestrador será registrar los dispositivos finales conectados a la red privada, para ello se deberá implementar un mecanismo de registro de dispositivos.

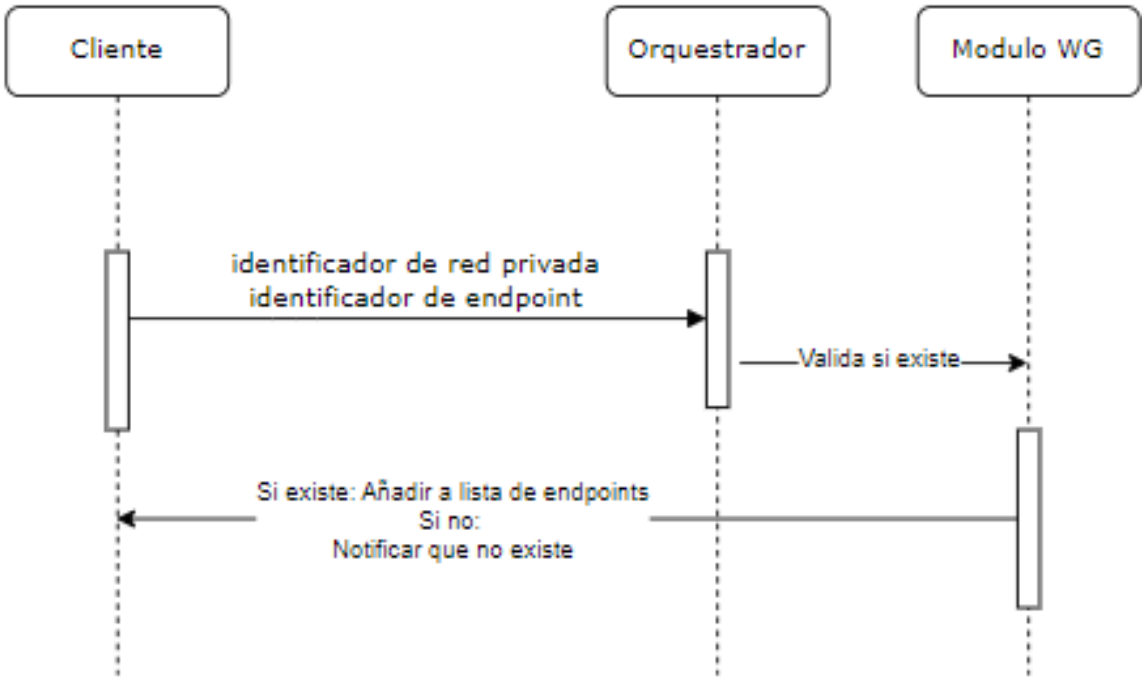

Figura 2.4: Diagrama de caso de uso: registro de dispositivo final

2.1.4. Cliente verifica conectividad con sus endpoint registrados

El cliente deberá informar al orquestrador si es posible que se comunique con los demás dispositivos finales de la red privada, para ello deberá enviar un mensaje al orquestrador para conocer que dispositivos finales supone que están conectados a la red privada. Luego este cliente verificara si alcanza a los demás dispositivos finales de la red privada, mediante un mensaje enviado desde la interfaz Wireguard, es decir, usando las IP asignadas por el orquestrador.

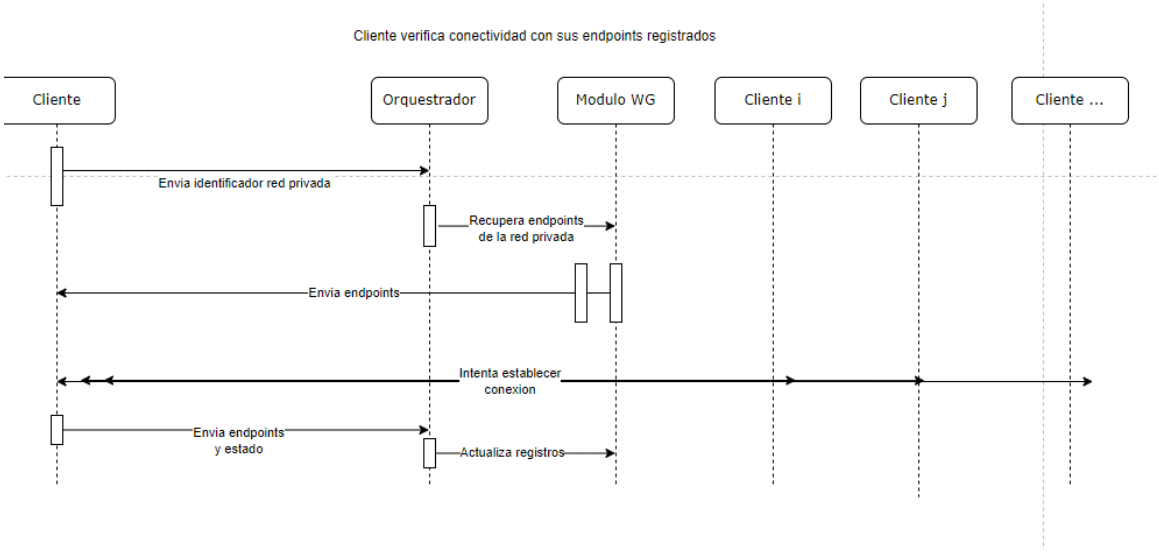

Figura 2.5: Diagrama de caso de uso: cliente verifica conectividad con sus endpoint registrados

2.1.5. Cliente consulta información de red privada al orquestrador

El cliente deberá poder consultar la información de la red privada a la que está conectado, para ello deberá enviar un mensaje al orquestrador con el identificador de la red privada, el orquestrador deberá responder con la información de la red privada.

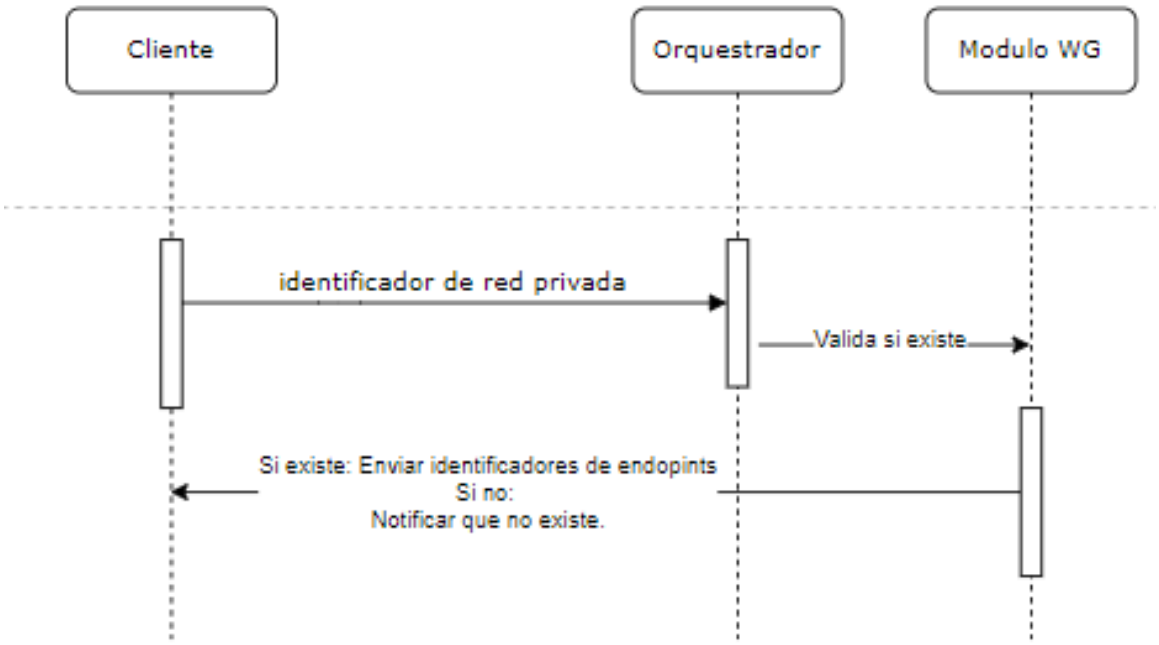

Figura 2.6: Diagrama de caso de uso: cliente consulta información de red privada al orquestrador

2.1.6. Cliente consulta redes privadas disponibles

El cliente deberá poder consultar las redes privadas disponibles, para ello deberá enviar un mensaje al orquestrador, el orquestrador deberá responder con la lista de redes privadas disponibles.

2.1.7. Orquestrador divulga tablero de red privada

Si el cliente envia una solicitud del estado de una red privada al orquestrador, este deberá responder con un tablero de la red privada, que contiene la información de los dispositivos finales conectados a la red privada, las conexiones entre los dispositivos finales y la alcanzabilidad de los dispositivos finales desde el punto de vista del orquestrador.

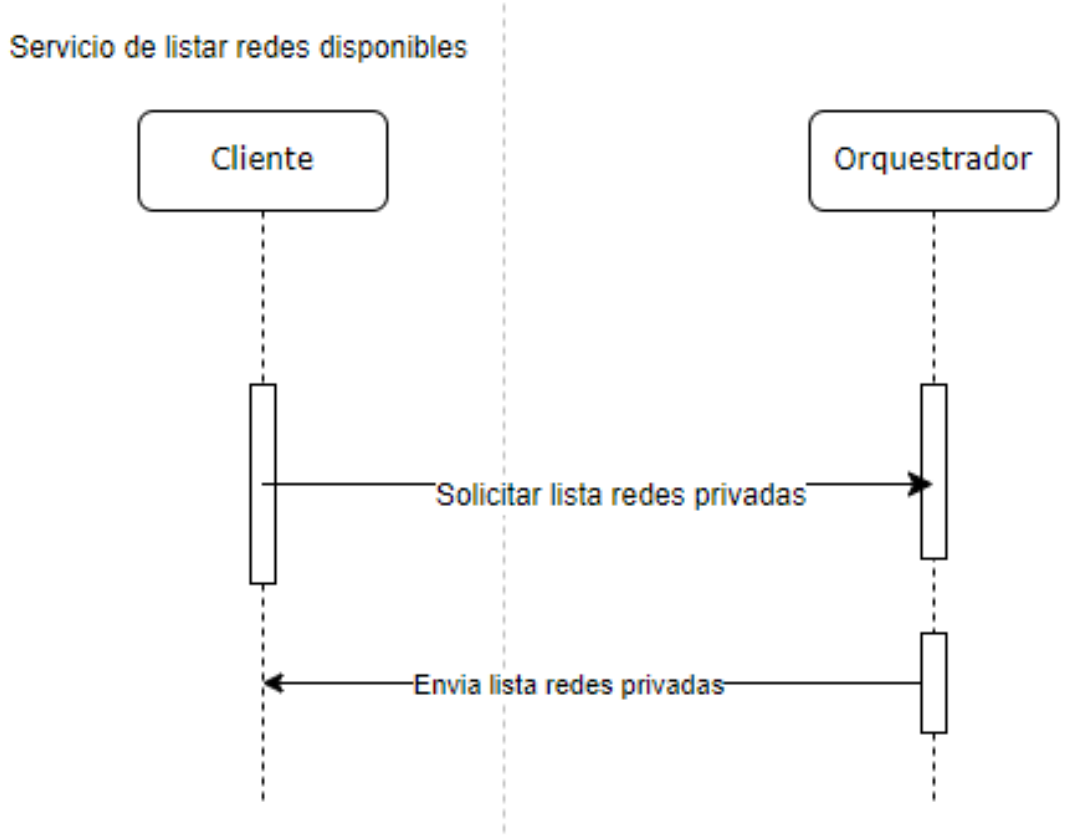

Figura 2.7: Diagrama de caso de uso: cliente consulta redes privadas disponibles

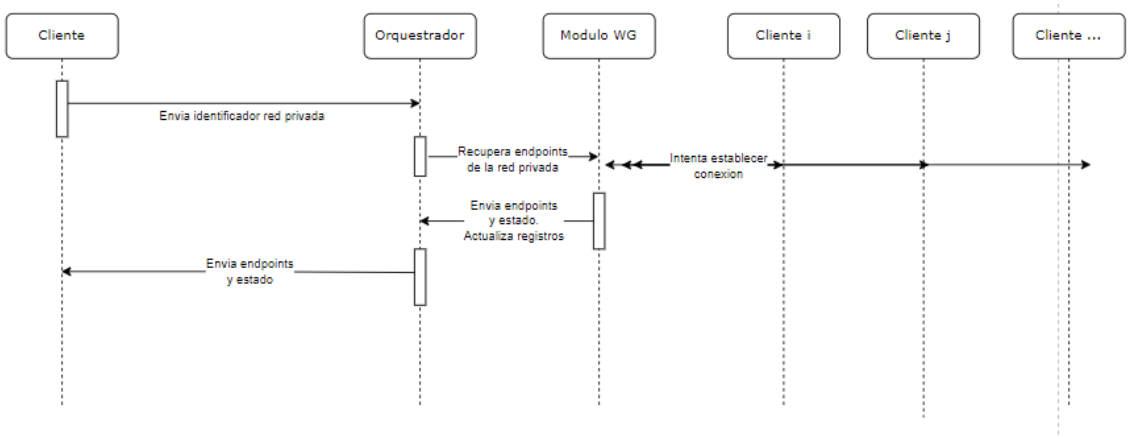

Figura 2.8: Diagrama de caso de uso: orquestrador divulga tablero de red privada

2.2. Sección

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Capítulo 3

Resultados

Capítulo 4

Conclusiones

@sglvgdor

Bibliografía

[1] Kurose, J. F., & Ross, K. W. (2017). *Computer networking: a top-down approach*, Pearson, 7th edition.

[2] WireGuard, *WireGuard: fast, modern, secure VPN tunnel*, `https://www.wireguard.com/`, 2021.

[3] Linux Documentation Project, *Linux Advanced Routing & Traffic Control HOWTO*, `https://tldp.org/HOWTO/Adv-Routing-HOWTO/index.html`, 2021.

[4] Bautts, M., & Dawson, M. (2000). *Linux Network Administrator's Guide*, O'Reilly Media, 3rd edition.

[5] Bautts, M., & Dawson, M. (2000). *Linux IP Masquerade HOWTO*, `https://tldp.org/HOWTO/IP-Masquerade-HOWTO/index.html`, 2021.