Seguridad en Sistemas GNU/Linux a Través de la Implementación de un Firewall Endian

Javier Alexander Molina Monroy
e-mail: aleexandermolina@gmail.com
Jisseth Karina Gonzalez Pinto
e-mail: jkgonzalezsuma@gmail.com
Walter Oswaldo Forero Rangel
e-mail: walter0434@hotmail.com
Juan Esteban Hernández Bonilla
e-mail: bonillajueanes02@gmail.com
Angie Vanesa Pinzón Sandoval
e-mail: ing.vanesapinzon@gmail.com

RESUMEN: *Este artículo presenta la implementación integral de GNU/Linux Endian en VirtualBox, abordando la configuración inicial de la instancia, la asignación de tarjetas de red y la instalación efectiva del sistema. Se establecen las zonas de seguridad VERDE (LAN), ROJA (WAN) y NARANJA (DMZ) para garantizar una segmentación adecuada. Asimismo, se configura NAT para permitir la comunicación desde la LAN y la DMZ hacia la red WAN, validando la creación automática de reglas de traducción de direcciones. Posteriormente, se habilitan servicios HTTP y FTP en la DMZ, mientras se restringe el protocolo ICMP para reforzar la seguridad. Se desarrollan reglas de acceso que permiten o deniegan tráfico entre zonas, verificando su funcionamiento mediante pruebas de conectividad y acceso web. Finalmente, se implementa un proxy HTTP no transparente con autenticación y listas negras, comprobando su efectividad desde la LAN.*

PALABRAS CLAVE: GNU/Linux, Endian Firewall, VirtualBox, segmentación de red, zona verde, zona roja, zona naranja, NAT, DMZ, firewall, reglas de acceso, HTTP, FTP, proxy HTTP, autenticación, lista negra, seguridad perimetral.

1 INTRODUCCIÓN

La seguridad en redes se ha convertido en un componente esencial dentro de cualquier entorno tecnológico, especialmente en aquellos donde múltiples dispositivos conviven y requieren protección frente a amenazas externas e internas. En este contexto, GNU/Linux Endian se presenta como una solución robusta para gestionar y controlar el flujo de información entre distintos segmentos de red. Su implementación en entornos virtualizados, como VirtualBox, permite recrear escenarios reales sin comprometer infraestructuras productivas, ofreciendo un espacio ideal para el aprendizaje y la experimentación.

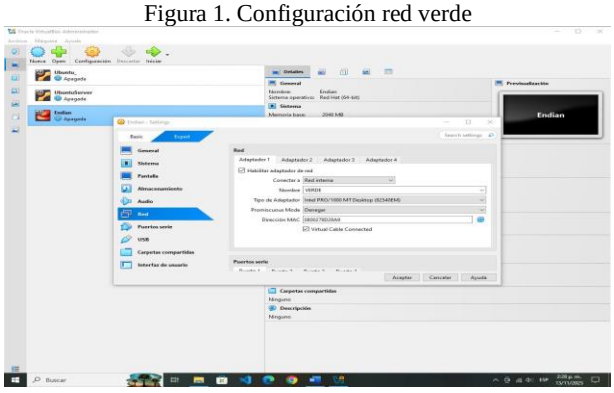
El propósito de este trabajo es documentar el proceso de instalación, configuración y validación de Endian utilizando un esquema dividido en zonas VERDE, ROJA y NARANJA. A partir de esta estructura, se abordan mecanismos esenciales como la traducción de direcciones (NAT), el control de servicios, las reglas de acceso entre segmentos y la implementación de un proxy con políticas de autenticación. Este enfoque permite comprender, desde la práctica, cómo un firewall perimetral puede fortalecer significativamente la seguridad de una red.

2 TEMATICA 1: CONFIGURACION DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUAL BOX (TAREJTAS DE RED) E INSTLACION EFECTIVA DEL MISMO.

2.1 PRIMER ADAPTADOR ZONA VERDE

El primer adaptador se configuró como red interna bajo el nombre VERDE. Esta zona representa la red confiable y servirá como segmento para la máquina Ubuntu Desktop.

Figura 1. Configuración red verde

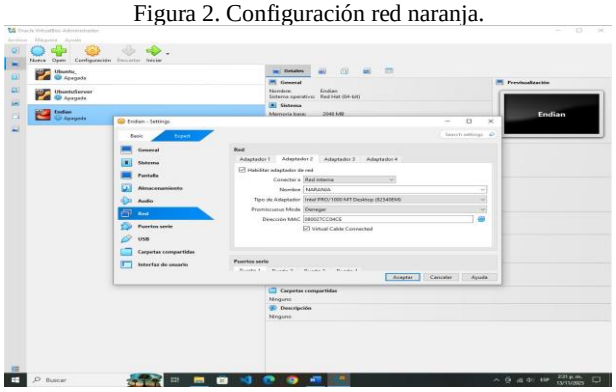


Fuente: Autoría Propia

2.2 SEGUNDO ADAPTADOR ZONA NARANJA

El segundo adaptador se configuró como red interna con el nombre NARANJA, correspondiente a la red semiconfiable o red DMZ que se usara en Ubuntu server.

Figura 2. Configuración red naranja.

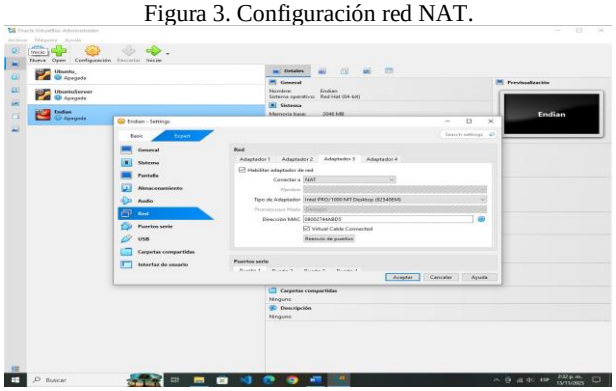


Fuente: Autoría Propia

2.3 TERCER ADAPTADOR ZONA NAT.

El tercer adaptador fue configurado en modo NAT para permitir la comunicación hacia Internet desde Endian cuando fuera necesario para actualizaciones o servicios específicos.

Figura 3. Configuración red NAT.



Fuente: Autoría Propia

2.4 INSTALACION DE ENDIAN FIREWALL

El proceso inicia seleccionando yes y usando la dirección IP 192.168.1.1 para la zona VERDE.

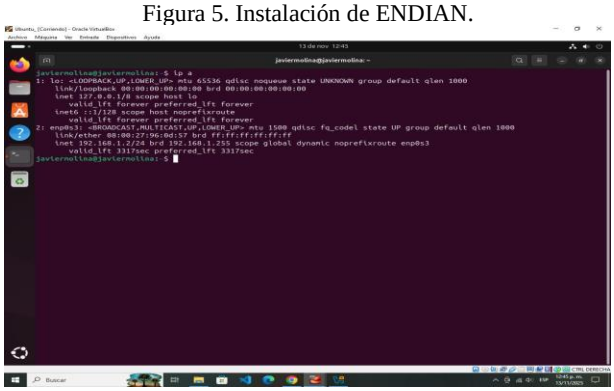
Figura 4. Instalación de ENDIAN.

Fuente: Autoría Propia

2.5 CONFIGURACION INICIAL DESPUES DE LA INSTALACION

Una vez instalado Endian, la máquina Ubuntu Desktop recibe una dirección IP por DHCP, la cual permite verificar la conectividad mediante ping hacia el firewall Endian.

Figura 5. Instalación de ENDIAN.

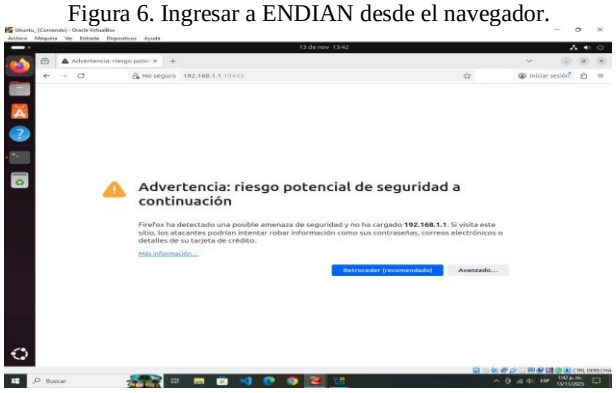


Fuente: Autoría Propia

2.6 ACCESO AL DASHBOARD

Desde Ubuntu Desktop se accede al dashboard mediante el navegador utilizando la IP 192.168.1.1, aceptando las advertencias del navegador. Al ingresar se selecciona idioma, zona horaria y se continúa el proceso sin restaurar backups previos.

Figura 6. Ingresar a ENDIAN desde el navegador.

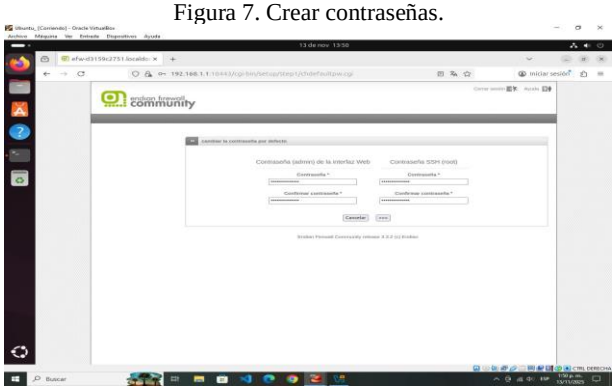


Fuente: Autoría Propia

2.7 CREACION DE CONTRASEÑAS

Se configuran dos contraseñas: una para el usuario admin y otra para acceso SSH como root.

Figura 7. Crear contraseñas.

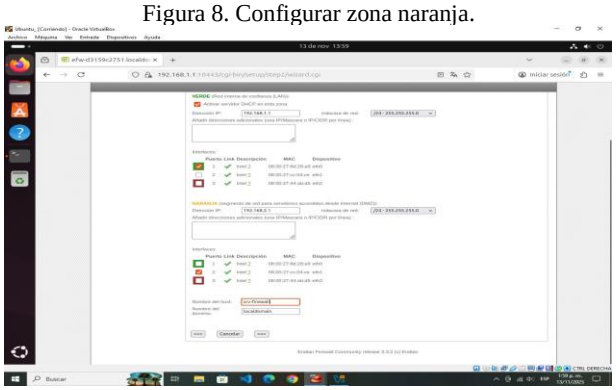


Fuente: Autoría Propia

2.8 CONFIGURACION DE ZONA NARANJA

Se selecciona la zona NARANJA y se asigna la dirección IP 192.168.2.1 para la máquina Ubuntu Server. Se marca la opción correspondiente y se asigna el nombre de host srv-firewall.

Figura 8. Configurar zona naranja.

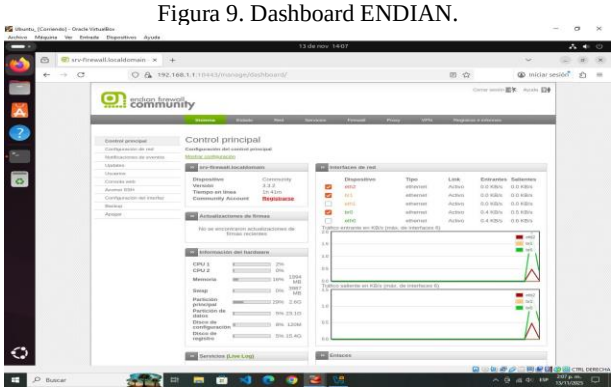


Fuente: Autoría Propia

2.9 APLICACIÓN DE CONFIGURACION

Después de revisar las opciones, se aplica la configuración. Posteriormente, se verifica desde Ubuntu Server que exista conectividad mediante ping hacia Endian. Se ingresa al panel con el usuario admin, se omiten actualizaciones y se carga el dashboard principal de Endian.

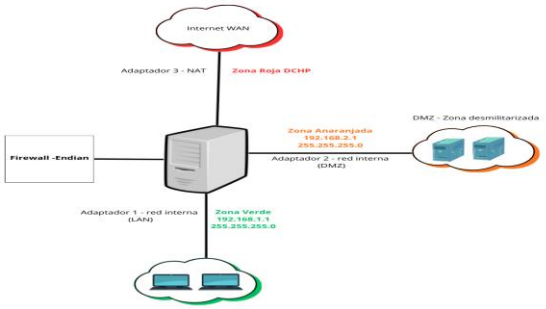
Figura 9. Dashboard ENDIAN.



Fuente: Autoría Propia

2.10 DIAGRAMA DE RED POR ZONAS

Figura 10. Diagrama de red por zonas.



Fuente: Autoría Propia

3 TEMATICA 2: CONFIGURACIÓN NAT Y REENVÍO DE PUERTOS

En esta segunda temática se implementó la traducción de direcciones de red (NAT) y el reenvío de puertos con el fin de permitir la comunicación controlada entre la red interna y la red externa. Dado que la infraestructura utilizada se compuso únicamente de dos máquinas virtuales (Ubuntu Server y Ubuntu Desktop), se diseñó un esquema donde Ubuntu Server asumió el rol de firewall y router, permitiendo la salida hacia Internet mediante su interfaz NAT y gestionando las conexiones provenientes de la máquina de escritorio.

3.1 CONFIGURACIÓN DE REDES EN VIRTUALBOX.

Se establecen dos adaptadores en la máquina Ubuntu Server:

Un adaptador con salida a Internet mediante NAT.

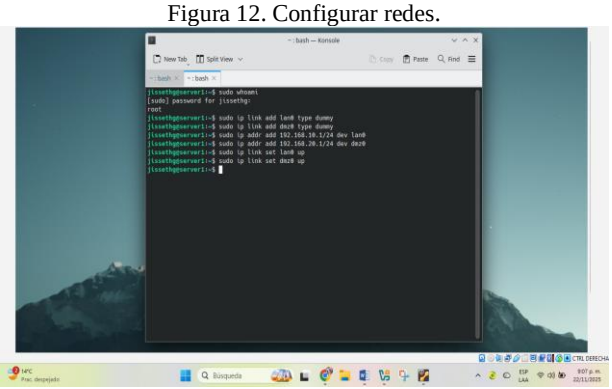
Un segundo adaptador para la red interna donde operará la LAN.

Ubuntu Desktop se conecta únicamente al adaptador interno asignado, simulando un equipo dentro de la LAN.

Figura 11. Configurar redes.

Fuente: Autoría Propia

Figura 12. Configurar redes.



Fuente: Autoría Propia

3.2 CONFIGURACIÓN DE REDES EN VIRTUALBOX.

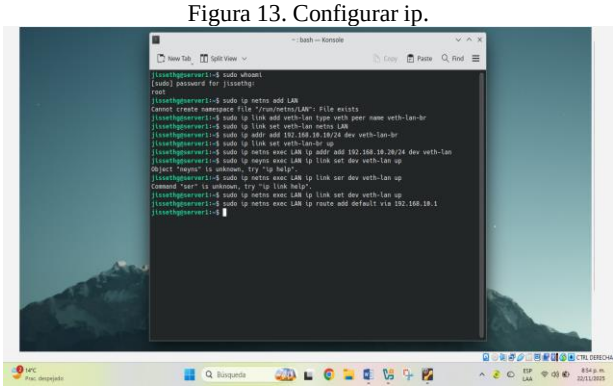
Se asignan direcciones IP estáticas:

Ubuntu Server como gateway de la LAN: 192.168.10.1.

Ubuntu Desktop (LAN): 192.168.10.10, utilizando al servidor como puerta de enlace.

La DMZ y la LAN se simulan mediante namespaces internos, cada uno con su propio rango de direcciones.

Figura 13. Configurar ip.



Fuente: Autoría Propia

Figura 14. Configurar ip.

Fuente: Autoría Propia

3.3 ACTIVACIÓN DE NAT EN UBUNTU SERVER.

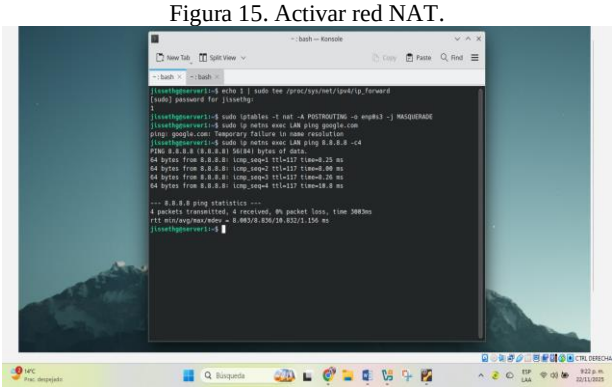
Se habilita el reenvío de paquetes IPv4:

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

Se aplica la regla MASQUERADE, permitiendo que la LAN use la IP pública del servidor:

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

Figura 15. Activar red NAT.



Fuente: Autoría Propia

3.4 VERIFICACIÓN DE CONECTIVIDAD LAN → INTERNET.

Desde la LAN (namespace o Ubuntu Desktop) se realizan pruebas:

Ping a servidores públicos.

Resolución DNS.

Resultados exitosos confirman que el NAT está funcionando y que la LAN sale correctamente a Internet.

Figura 16. Verificar conexión LAN.

Fuente: Autoría Propia

Figura 17. Verificar conexión LAN.

Fuente: Autoría Propia

3.5 REENVÍO DE PUERTOS (DMZ).

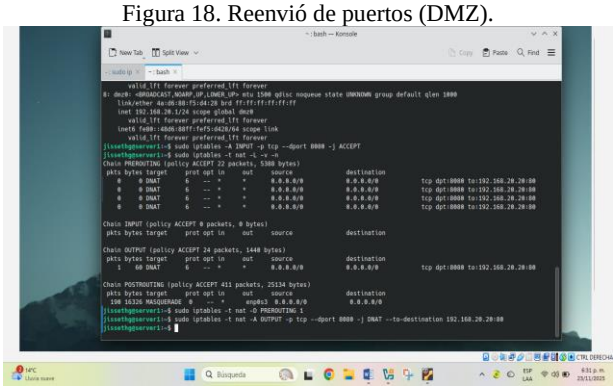
Se instala un servidor Apache para simular un servicio en DMZ.

Luego, se aplica una regla de redirección (DNAT) en Ubuntu Server:

sudo iptables -t nat -A PREROUTING -p tcp --dport 8080 -j DNAT --to-destination 192.168.20.20:80

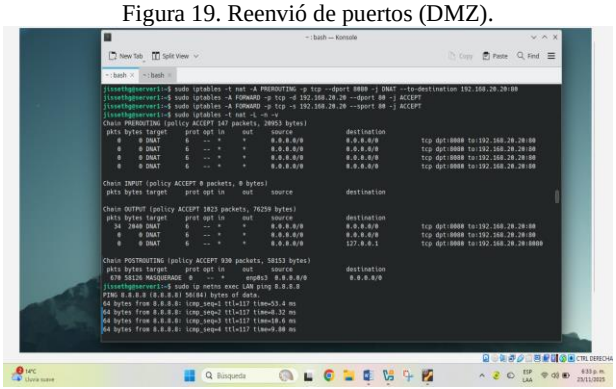
Esto permite que cualquier solicitud al puerto 8080 del servidor llegue al servicio Apache dentro de la DMZ.

Figura 18. Reenvió de puertos (DMZ).



Fuente: Autoría Propia

Figura 19. Reenvió de puertos (DMZ).



Fuente: Autoría Propia

3.6 VALIDACION DE REGLAS ACTIVAS.

Se revisan las reglas implementadas:

sudo iptables -t nat -L -n -v
sudo iptables -L -n -v

Se verifica la presencia de:

Reglas MASQUERADE.

Reglas DNAT hacia la DMZ.

Reglas de reenvío (FORWARD) permitiendo el tráfico.

El correcto funcionamiento de ambas cadenas asegura que se cumplen los productos esperados de la actividad.

Figura 20. Reglas activas.

Fuente: Autoría Propia

Figura 21. Reglas activas.

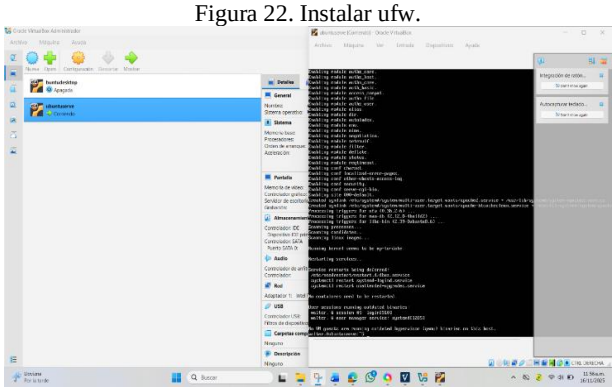
Fuente: Autoría Propia

4 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

4.1 INSTALACIÓN DEL FIREWALL UFW EN UBUNTU SERVER.

La terminal mostrando el comando de instalación del firewall ufw (sudo apt install ufw -y) en un servidor Ubuntu.

Figura 22. Instalar ufw.

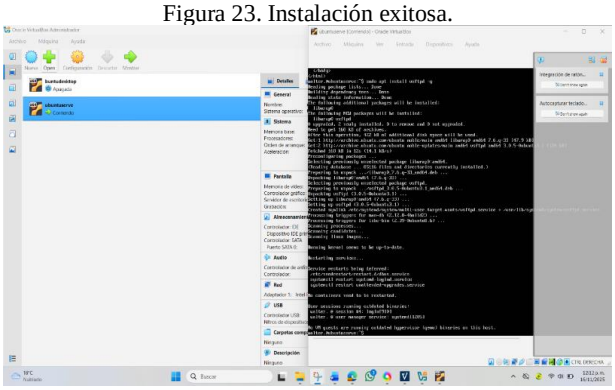


Fuente: Autoría Propia

4.2 EJECUCIÓN EXITOSA DEL COMANDO DE INSTALACIÓN DE UFW.

Terminal mostrando la ejecución exitosa del comando de instalación de UFW, confirmando la descarga e instalación de los paquetes necesarios.

Figura 23. Instalación exitosa.

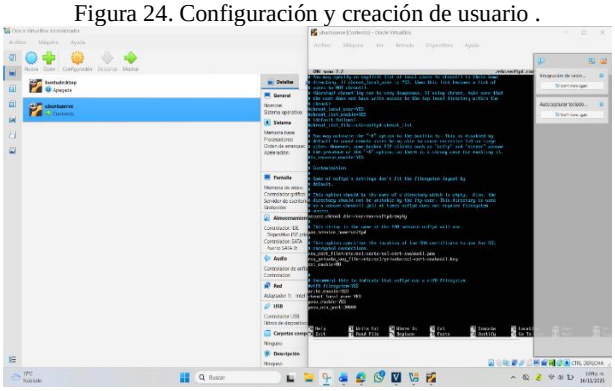


Fuente: Autoría Propia

4.3 PROCESO DE CREACIÓN Y CONFIGURACIÓN DE UN USUARIO EN EL SISTEMA.

Proceso de configuración y creación de un nuevo usuario en el sistema servidor Ubuntu.

Figura 24. Configuración y creación de usuario .

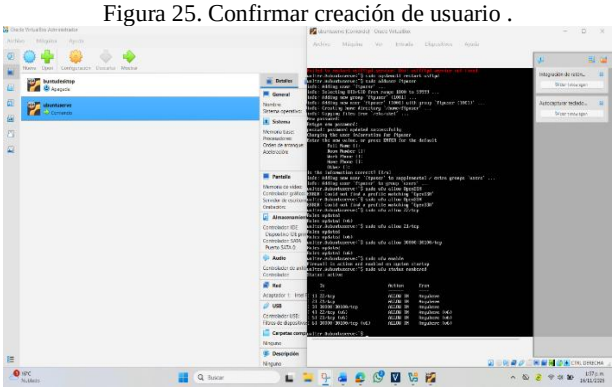


Fuente: Autoría Propia

4.4 CONFIRMACIÓN DE LA CREACIÓN DEL USUARIO EN EL SERVIDOR.

Terminal mostrando la confirmación de la creación del usuario y su adición a grupos necesarios.

Figura 25. Confirmar creación de usuario .

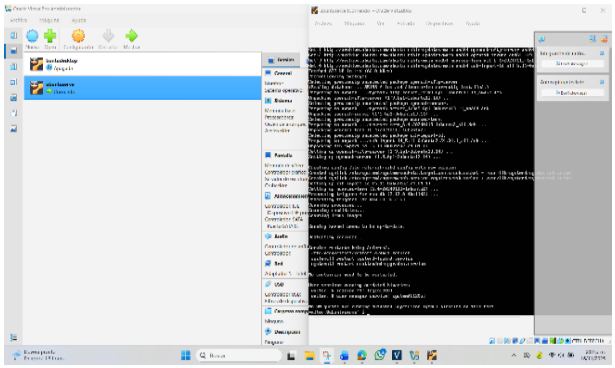


Fuente: Autoría Propia

4.5 PRUEBA DE CONECTIVIDAD EXITOSA AL SERVICIO HTTP (PUERTO 80).

Prueba de conectividad o servicio HTTP, mostrando una respuesta exitosa (código de estado 200 OK) al acceder al puerto 80.

Figura 26. Conexión HTTP puerto 80 .

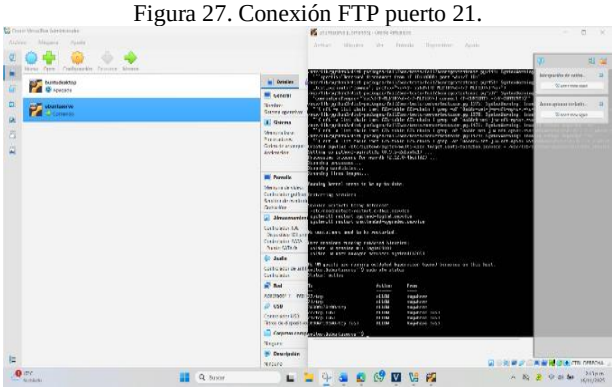


Fuente: Autoría Propia

4.6 PRUEBA DE CONEXIÓN EXITOSA AL SERVICIO FTP (PUERTO 21).

Prueba del servicio FTP, mostrando una conexión exitosa al puerto 21 del servidor.

Figura 27. Conexión FTP puerto 21.



Fuente: Autoría Propia

4.7 VERIFICACIÓN DE LAS REGLAS DE UFW PERMITIENDO TRÁFICO HTTP/HTTPS.

Verificación en la terminal de las reglas del firewall UFW, mostrando que los perfiles de aplicación 'Apache' y 'Apache Full' están configurados para permitir tráfico.

Figura 28. Reglas UFW.

Fuente: Autoría Propia

4.8 IMPLEMENTACIÓN DE LA REGLA IPTABLES PARA BLOQUEAR ICMP TYPE 8.

Implementación de una regla de `iptables` para bloquear el protocolo ICMP Type 8.

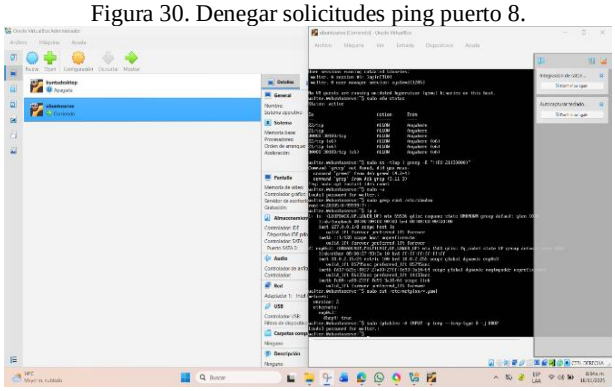
Figura 29. Bloquear ICMP.

Fuente: Autoría Propia

4.9 EJECUCIÓN DEL COMANDO PARA DENEGAR SOLICITUDES DE PING (ICMP TYPE 8).

Terminal mostrando la ejecución del comando para bloquear el ICMP Type 8.

Figura 30. Denegar solicitudes ping puerto 8.

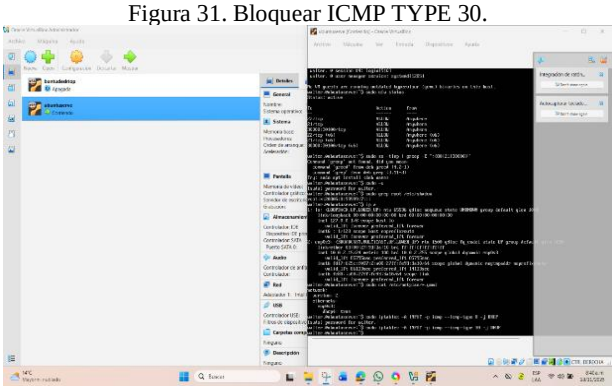


Fuente: Autoría Propia

4.10 IMPLEMENTACIÓN DE LA REGLA `IPTABLES` PARA BLOQUEAR ICMP TYPE 30.

Implementación de una regla de iptables para bloquear el protocolo ICMP Type 30 usando el comando `sudo iptables -A INPUT -p icmp --icmp-type 30 -j DROP`.

Figura 31. Bloquear ICMP TYPE 30.

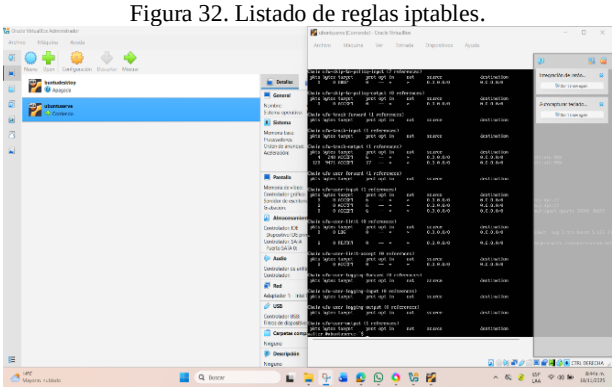


Fuente: Autoría Propia

4.11 LISTADO DE REGLAS `IPTABLES` MOSTRANDO EL BLOQUEO ACTIVO PARA LOS TIPOS ICMP 8 Y 30.

Verificación de las reglas de iptables activas en el sistema usando el comando `sudo iptables -L -n -v`, mostrando las cadenas INPUT, FORWARD y OUTPUT con las reglas de bloqueo ICMP aplicadas.

Figura 32. Listado de reglas iptables.

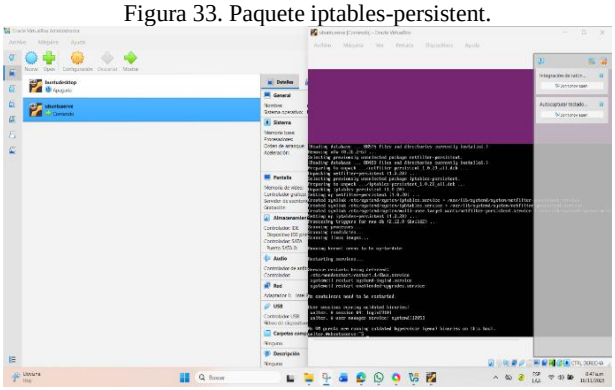


Fuente: Autoría Propia

4.12 INSTALACIÓN DEL PAQUETE IPTABLES-PERSISTENT PARA GUARDAR LAS REGLAS.

Instalación del paquete iptables-persistent (sudo apt install iptables-persistent -y) para guardar las reglas de `iptables` y asegurar su persistencia tras un reinicio del sistema.

Figura 33. Paquete iptables-persistent.

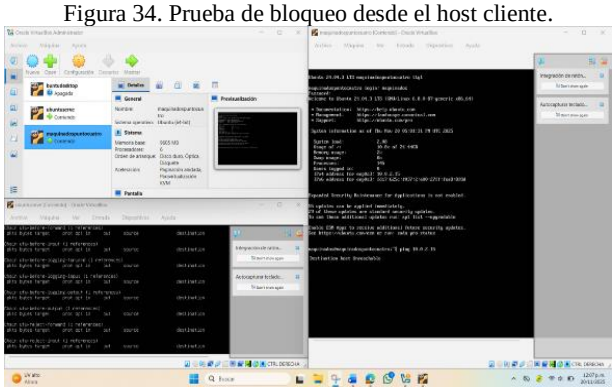


Fuente: Autoría Propia

4.13 PRUEBA DE BLOQUEO DE ICMP: COMANDO `PING` FALLIDO DESDE UN HOST CLIENTE.

Prueba del bloqueo de ICMP: ejecución del comando ping desde una máquina cliente hacia la IP del servidor, mostrando una falla en la recepción de respuestas.

Figura 34. Prueba de bloqueo desde el host cliente.



Fuente: Autoría Propia

5 TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

5.1 EN EL HYPERVISOR (VIRTUALBOX O VMWARE)

5.1.1 Se agregan tres adaptadores:

5.1.2 Adaptador 1 → WAN (Internet)

- Modo: **NAT**
- Nombre: AUTOMÁTICO

5.1.3 Adaptador 2 → Zona Verde / LAN

- Modo: **Red interna**
- Nombre: LAN80

5.1.4 Adaptador 3 → Zona Naranja / DMZ

- Modo: **Red interna**
- Nombre: DMZ80

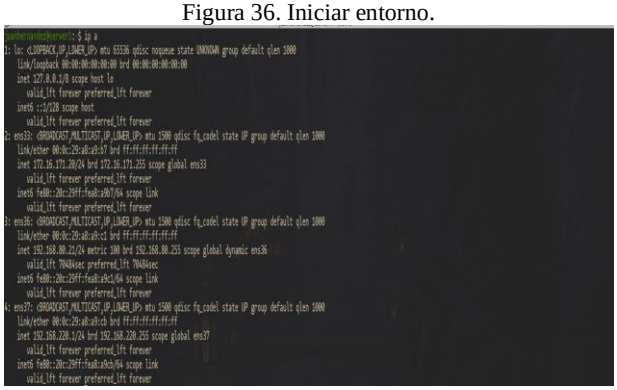
Figura 35. Configuración en VMware.

Fuente: Autoría Propia

5.2 INICIALIZACIÓN DEL ENTORNO

En esta fase se inicia cada máquina virtual, se verifica conectividad básica y se identifican las interfaces disponibles.

Figura 36. Iniciar entorno.

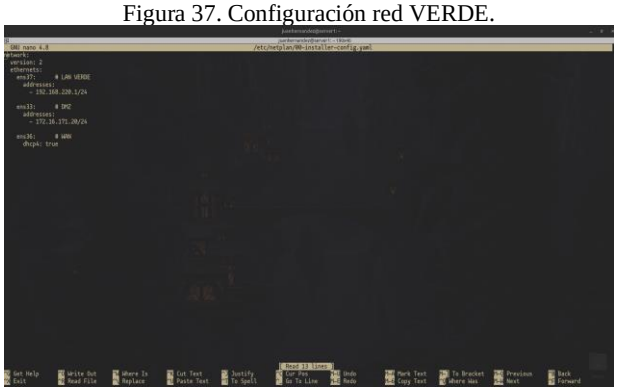


Fuente: Autoría Propia

5.3 CONFIGURACIÓN DE LA INTERFAZ DE RED DEL DESKTOP (LAN VERDE).

Se edita el archivo de configuración de Netplan para asignar una IP estática dentro del segmento 192.168.220.0/24.

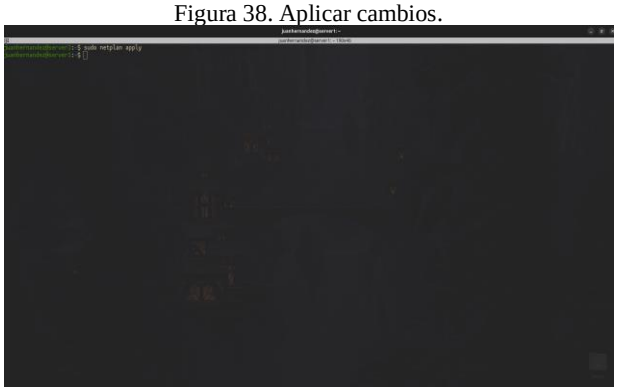
Figura 37. Configuración red VERDE.



Fuente: Autoría Propia

Posteriormente se aplican los cambios:

Figura 38. Aplicar cambios.

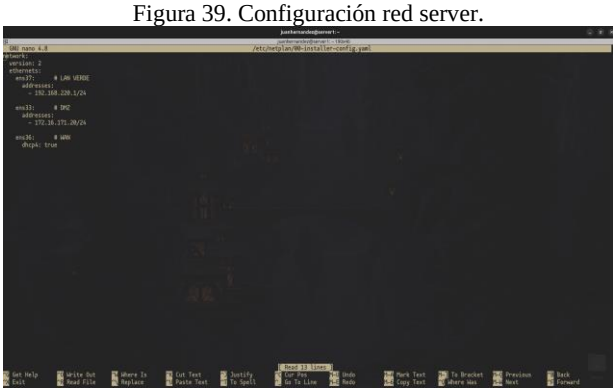


Fuente: Autoría Propia

5.4 CONFIGURACIÓN DE LA INTERFAZ DE RED DEL SERVER (LAN, DMZ Y WAN).

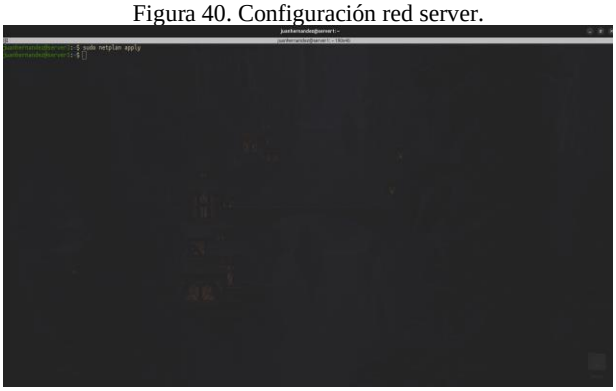
Se configuran las tres interfaces del servidor: LAN (192.168.220.1), DMZ (172.16.171.20) y WAN (DHCP).

Figura 39. Configuración red server.



Fuente: Autoría Propia

Figura 40. Configuración red server.

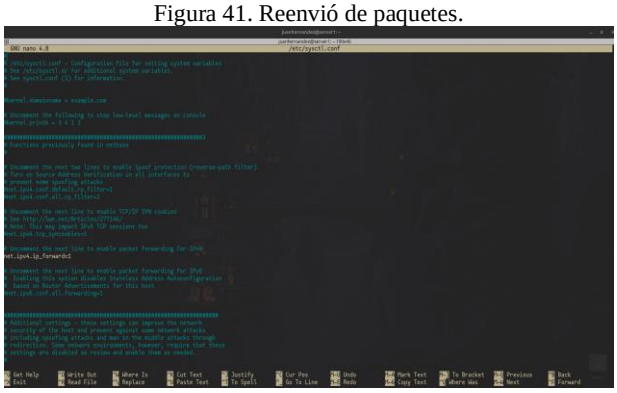


Fuente: Autoría Propia

5.5 ACTIVACIÓN DEL REENVÍO DE PAQUETES (IP FORWARDING).

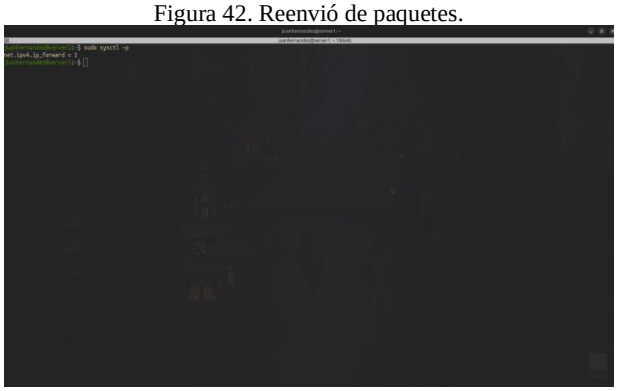
Se habilita el reenvío de tráfico para permitir que el servidor actúe como router.

Figura 41. Reenvió de paquetes.



Fuente: Autoría Propia

Figura 42. Reenvió de paquetes.

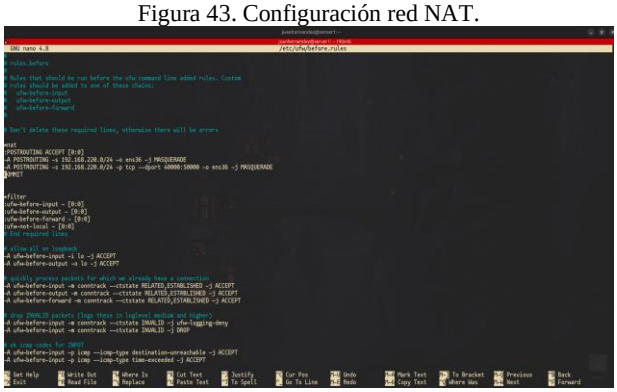


Fuente: Autoría Propia

5.6 CONFIGURACIÓN DEL NAT EN EL SERVIDOR.

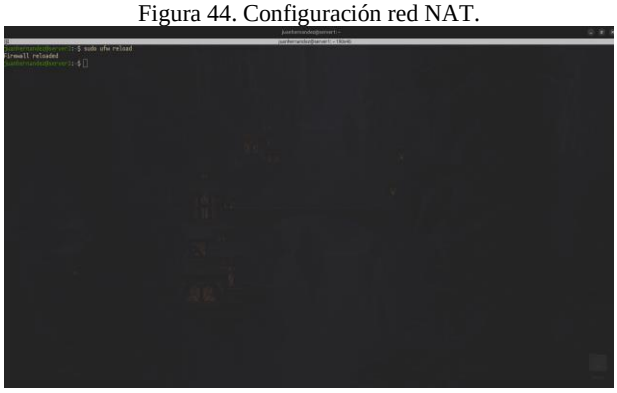
Se agrega la regla MASQUERADE para permitir que la LAN acceda a Internet mediante la interfaz WAN.

Figura 43. Configuración red NAT.



Fuente: Autoría Propia

Figura 44. Configuración red NAT.

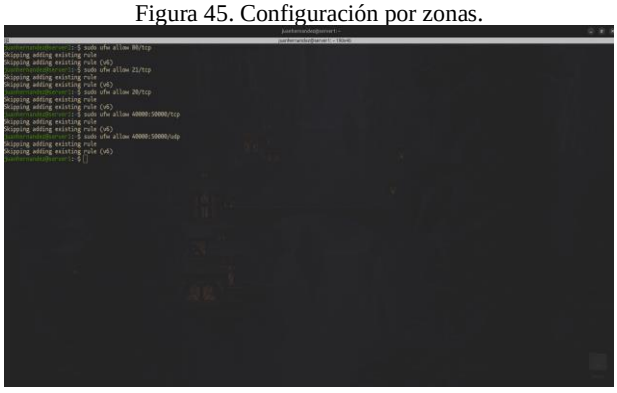


Fuente: Autoría Propia

5.7 CONFIGURACIÓN DEL FIREWALL UFW POR ZONAS.

Se habilitan reglas de acceso entre las zonas LAN, DMZ y WAN.

Figura 45. Configuración por zonas.

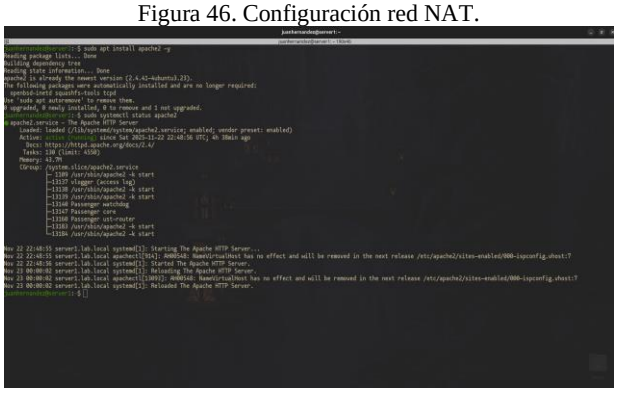


Fuente: Autoría Propia

5.8 INSTALACIÓN Y CONFIGURACIÓN DEL SERVICIO HTTP (APACHE) EN DMZ.

Se instala Apache y se verifica que esté escuchando en el puerto 80.

Figura 46. Configuración red NAT.

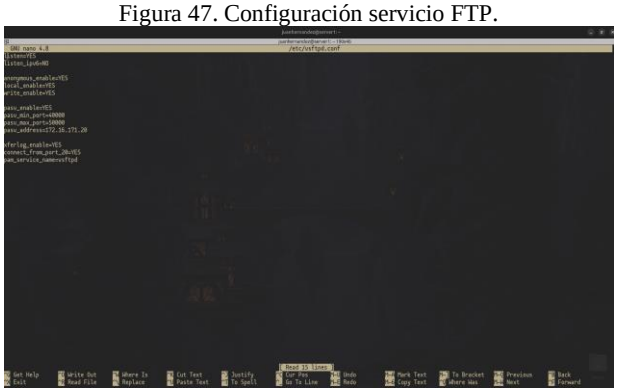


Fuente: Autoría Propia

5.9 CONFIGURACIÓN DEL SERVICIO FTP (VSFTPD) EN DMZ.

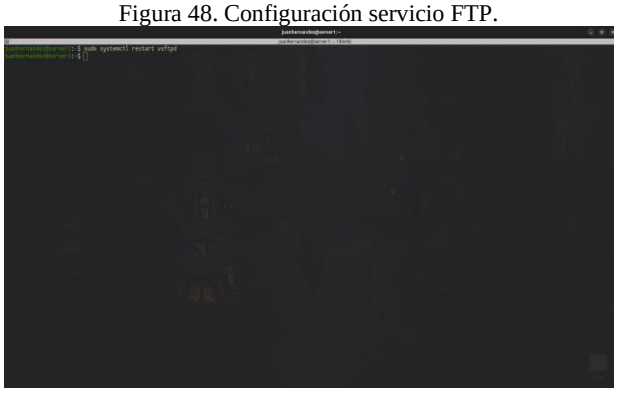
Se instala y configura vsftpd con soporte PASV.

Figura 47. Configuración servicio FTP.



Fuente: Autoría Propia

Figura 48. Configuración servicio FTP.

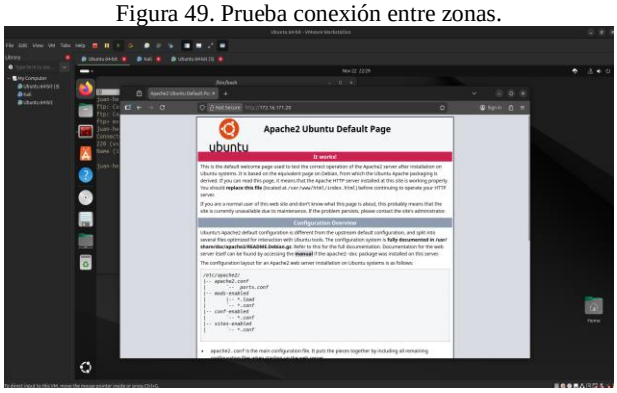


Fuente: Autoría Propia

5.10 PRUEBAS DE CONECTIVIDAD ENTRE ZONAS.

5.10.1 Desde LAN hacia DMZ (HTTP)

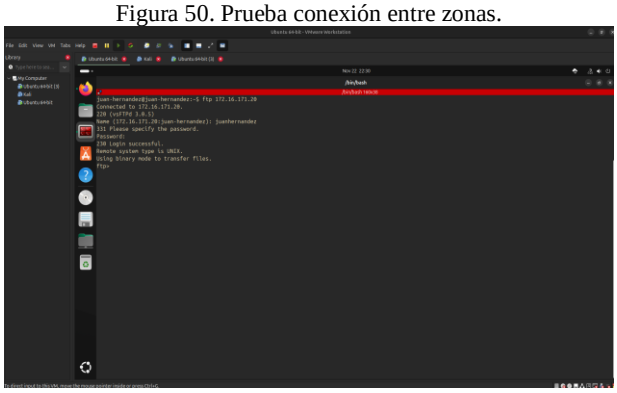
Figura 49. Prueba conexión entre zonas.



Fuente: Autoría Propia

5.10.2 Desde LAN hacia DMZ (FTP)

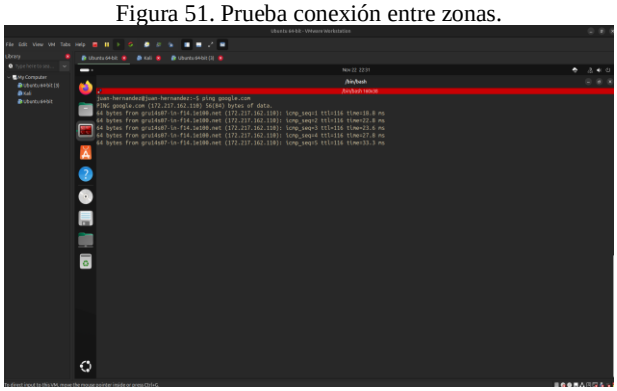
Figura 50. Prueba conexión entre zonas.



Fuente: Autoría Propia

5.10.3 Desde LAN hacia Internet (HTTP)

Figura 51. Prueba conexión entre zonas.



Fuente: Autoría Propia

5.11 VERIFICACIÓN DE REGLAS INTER-ZONA.

Se listan las reglas activas:

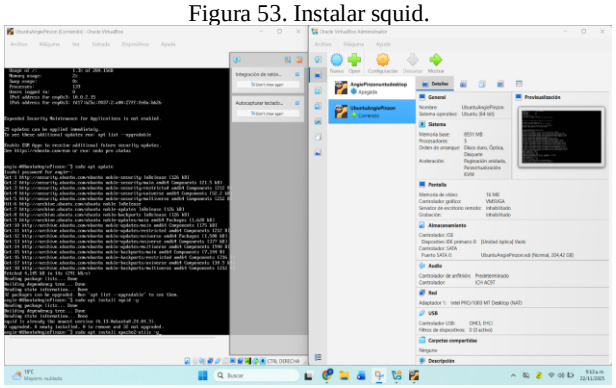
Figura 52. Reglas inter-zona.

Fuente: Autoría Propia

6 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARAENTE) CON POLITICAS DE AUTENTICACION PARA NAVEGACION EN INTERNET.

6.1 INSTALAR SQUID

Figura 53. Instalar squid.

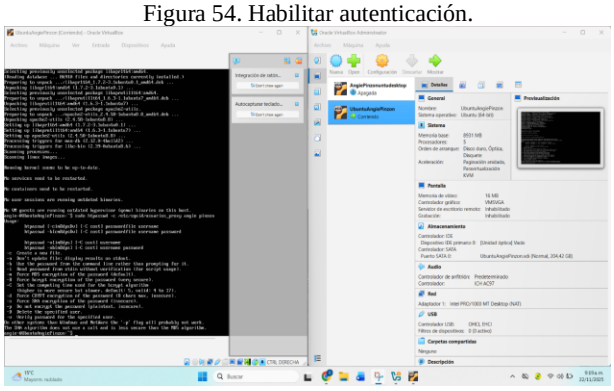


Fuente: Autoría Propia

6.2 HABILITAR LA AUTENTICACION.

apt install apache2- utils -y

Figura 54. Habilitar autenticación.

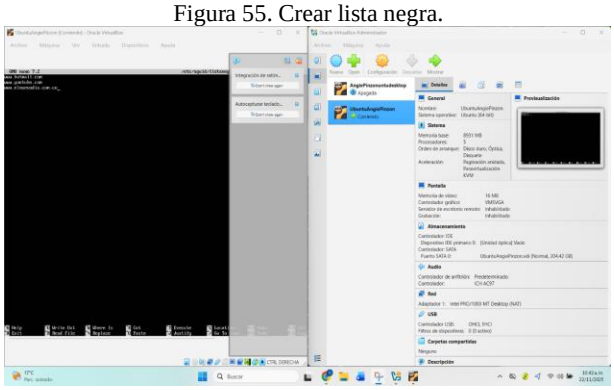


Fuente: Autoría Propia

6.3 CREAR LA LISTA NEGRA.

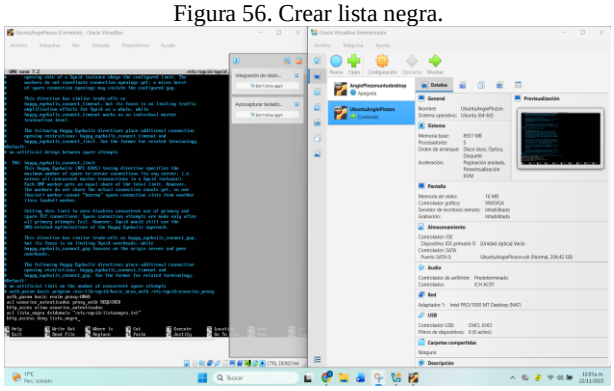
Sudo nano /etc/squid/listanegra.txt

Figura 55. Crear lista negra.



Fuente: Autoría Propia

Figura 56. Crear lista negra.

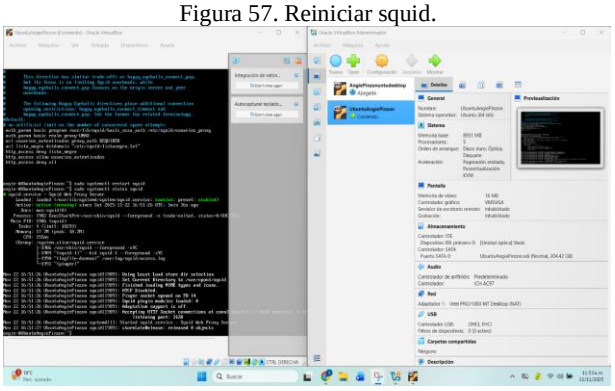


Fuente: Autoría Propia

6.4 REINICIAR SQUID.

Sudo systemctlrestart squid-Sudo systemctl status squid

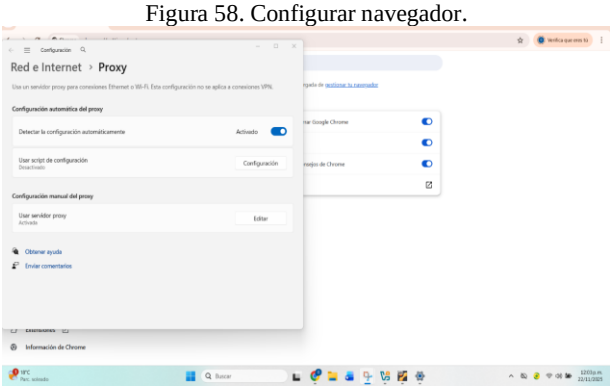
Figura 57. Reiniciar squid.



Fuente: Autoría Propia

6.5 CONFIGURAR EL NAVEGADOR DEL CLIENTE.

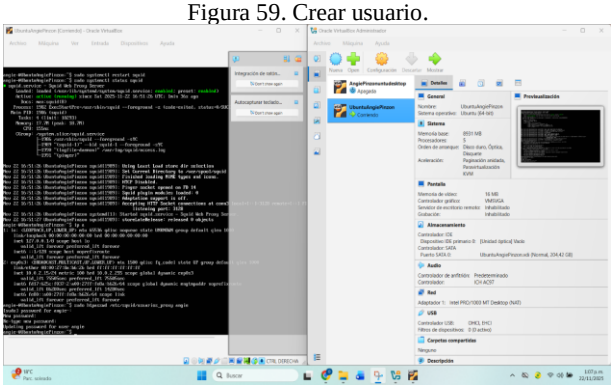
Figura 58. Configurar navegador.



Fuente: Autoría Propia

6.6 CREAR UN USUARIO Y ASOCIARLOS A UN GRUPO SQUID.

Figura 59. Crear usuario.

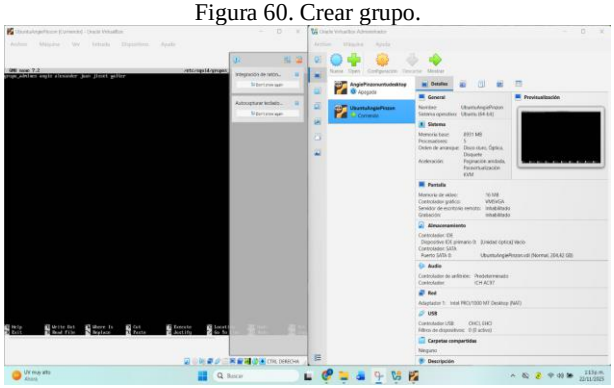


Fuente: Autoría Propia

6.7 CREAR UN GRUPO PARA ESE USUARIO.

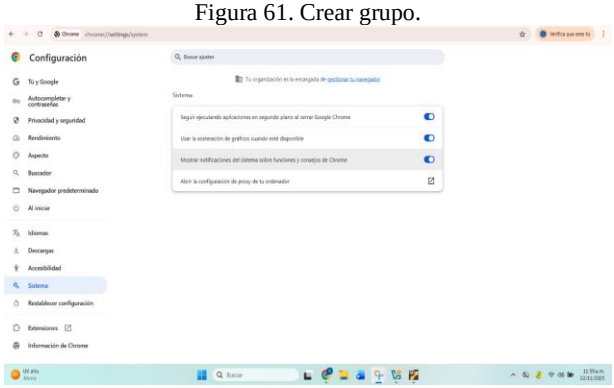
sudo nano /etc/squid/grupos_proxy

Figura 60. Crear grupo.



Fuente: Autoría Propia

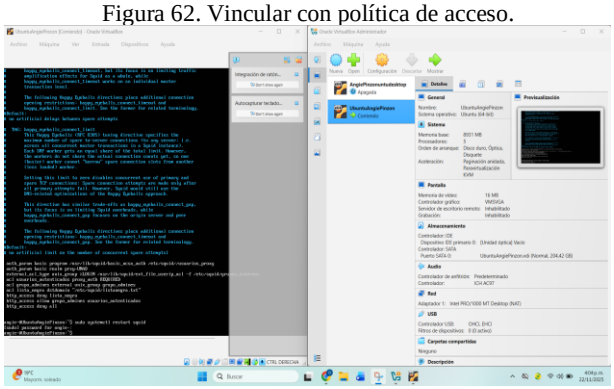
Figura 61. Crear grupo.



Fuente: Autoría Propia

6.8 VINCULAR GRUPO CON POLITICA DE ACCESO Y RELACIONAR LA AUTENTICACION CON EL USUARIO Y EL GRUPO.

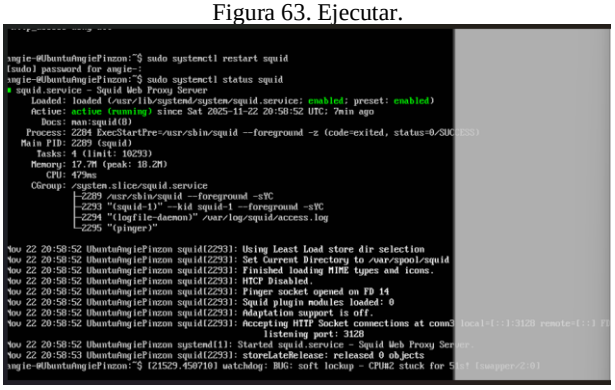
Figura 62. Vincular con política de acceso.



Fuente: Autoría Propia

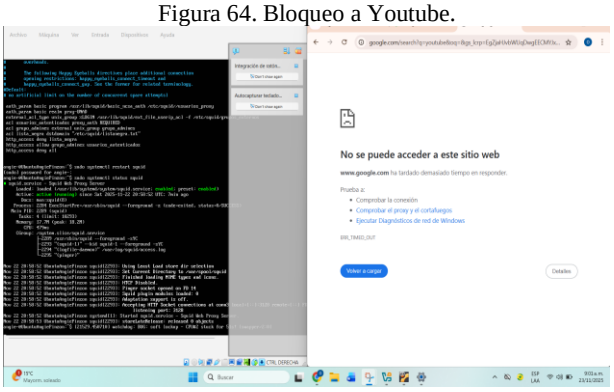
6.9 SE EJECUTA Y SE MUESTRA EL RESULTADO.

Figura 63. Ejecutar.



Fuente: Autoría Propia

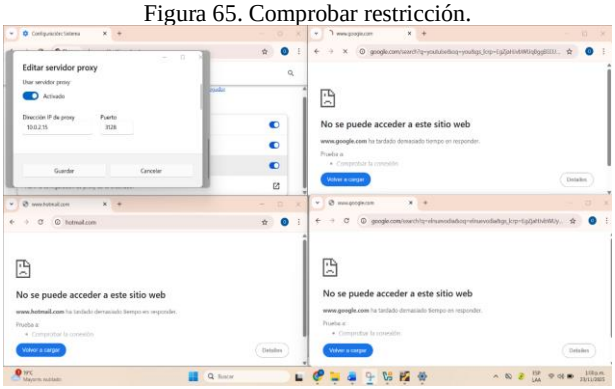
Figura 64. Bloqueo a Youtube.



Fuente: Autoría Propia

6.10 SE COMPRUEBA LA RESTRICCION.

Figura 65. Comprobar restricción.



Fuente: Autoría Propia

7 CONCLUSIONES

La implementación de GNU/Linux Endian en un entorno virtualizado permitió comprender de manera práctica cómo se estructuran y protegen distintos segmentos de red mediante un firewall perimetral. La configuración de las zonas VERDE, ROJA y NARANJA, junto con las reglas de NAT, facilitó la visualización del flujo de tráfico entre la LAN, la DMZ y la WAN. Este proceso evidenció la importancia de definir adecuadamente las interfaces y las políticas de comunicación para mantener un entorno seguro y funcional.

Además, la habilitación y restricción de servicios como HTTP, FTP e ICMP, así como la aplicación de reglas interzonales y la implementación de un proxy con autenticación y listas negras, demostraron el potencial de Endian como herramienta integral para la gestión de la seguridad. Las pruebas realizadas confirmaron que, con una correcta configuración, es posible garantizar control, aislamiento y monitoreo efectivo del tráfico, fortaleciendo así la seguridad en redes educativas y profesionales.

8 REFERENCIAS

[1] Endian. (2016). Manual de referencia Endian UTM 3.2. http://docs.endian.com/3.2/utm/index.html

[2] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Oracle. (220). Manual de usuario VirtualBox. https://www.vrtualbox.org/manual/

[4] Debian. (2023). Manual del administrador de Debian 12.5.0. https://www.debian.org/releases/stable/amd64/index.es.html

[5] Canonical (2024). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu help/index.html

[6] Debian (2024). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/in dex.es.html

[7] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

[8] Debian. (2023). Manual del administrador de Debian 12.5.0. https://www.debian.org/releases/stable/amd64/index.es.html

[9] Ubuntu Server. Packt Publishing. https://research-ebsco com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id= b88 1bf72-20a7-343c 94a8-f12e88b41952 [10] Canonical. (2023). Guía del Ubuntu

[10] Canonical. (2023). Guía del Ubuntu