IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD EN REDES CON GNU/LINUX ENDIAN EN UN ENTORNO VIRTUALIZADO

Andrea Natalia Lagos León
alagosl@unadvirtual.edu.co
Dacne Chirley Monroy Celis
dcmonroyc@unadvirtual.edu.co
Diego Andrés Almanza ortega
Daalmanzao@unadvirtual.edu.co
Stefany Chicue Macias
schicuem@unadvirtual.edu.co
Wendy Yulanny Monroy Celis
wymonroyc@unadvirtual.edu.co

***RESUMEN*:** *Este artículo describe la implementación de una arquitectura de red segmentada en zonas de seguridad utilizando el sistema GNU/Linux Endian Firewall en un entorno virtualizado mediante VirtualBox. Se configuraron tres máquinas virtuales: un cliente (Ubuntu Desktop), un servidor (Ubuntu Server) y un firewall (Endian), estableciendo las zonas verdes (LAN), roja (WAN) y naranja (DMZ). El objetivo principal fue simular un entorno seguro de red con separación lógica del tráfico para prácticas de administración de redes y seguridad informática.*

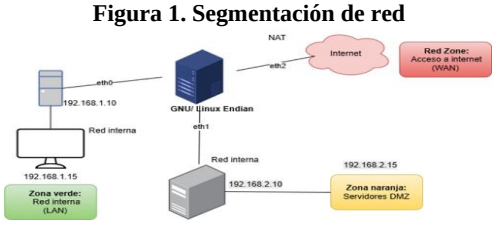
PALABRAS CLAVE: DMZ, Endian, firewall, LAN

1 INTRODUCCIÓN

La seguridad en redes es un componente crítico en la administración de sistemas informáticos. En este contexto, la segmentación de redes mediante zonas es una práctica común en infraestructuras empresariales. Se busca garantizar la protección de los servidores que conforman la intranet (LAN) / extranet (WAN), para lo cual se requiere delimitarlos a través de una zona DMZ y así garantizar la seguridad e integridad de las bases de datos y las aplicaciones bajo plataformas GNU/Linux.

2 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED)

Figura 1. Segmentación de red



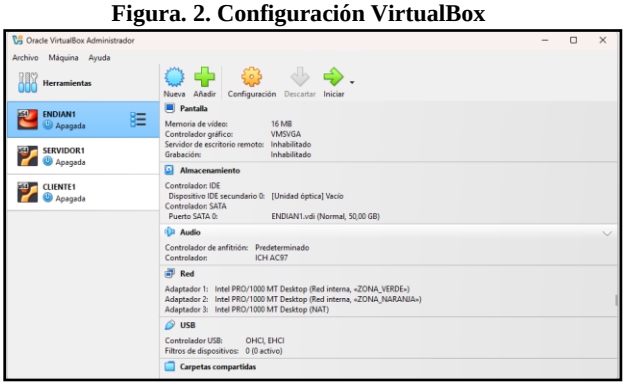
Fuente: Elaboración propia

La figura 1 representa la arquitectura de red implementada con GNU/Linux Endian Firewall Community, configurado con tres zonas de red según el modelo tradicional de seguridad.

Endian es una distribución de GNU/Linux enfocada en la seguridad de redes, que actúa como firewall, router y puerta de enlace entre distintas zonas de red . VirtualBox es una herramienta de virtualización que permite crear entornos de red simulados . Las zonas configuradas fueron:

- Zona Verde (LAN): Red interna segura con acceso total.
- Zona Roja (WAN): Punto de acceso a Internet.
- Zona Naranja (DMZ): Segmento para servidores
- expuestos parcialmente al exterior.

Figura. 2. Configuración VirtualBox



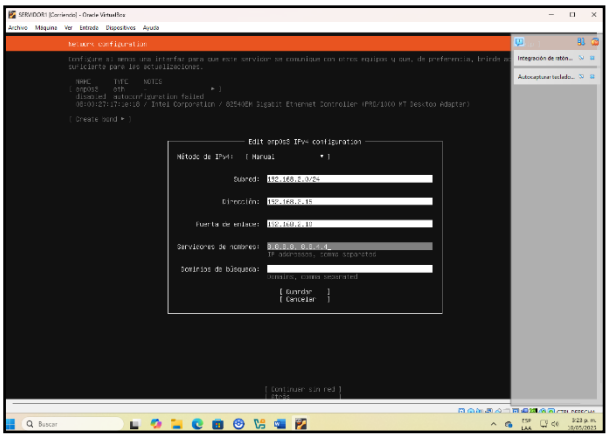
Fuente: Virtual Box elaboración propia

La figura 2 evidencia la configuración de tres máquinas virtuales en Virtual Box; La Zona Verde – Red Interna (LAN) representa a los equipos seguros de la red que están conectadas al firewall Endian, esta red puede acceder a Internet mediante reglas de NAT de salida y, si el firewall lo permite, también comunicarse con los servidores ubicados en la zona naranja (DMZ).

La Zona Naranja – DMZ (Servidores) aloja servidores públicos; esta zona es accesible desde la zona roja (Internet) mediante reglas específicas de reenvío de puertos (NAT de entrada), permitiendo ofrecer servicios públicos sin comprometer la seguridad de la red interna.

La Zona Roja – WAN (Internet) representa la red no confiable, es decir, el acceso a Internet; en esta zona se aplican estrictas reglas de seguridad, permitiendo únicamente el tráfico saliente desde la LAN o la DMZ, o el tráfico entrante hacia la DMZ, siempre y cuando existan reglas explícitas que lo autoricen.

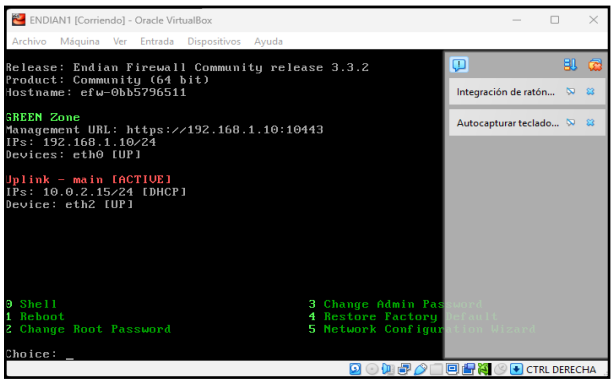
Figura 3. Configuración servidor zona naranja



Fuente: Ubuntu Server elaboración propia

En la figura 3 se evidencia el proceso de configuración manual de red en un servidor Ubuntu, se estableció una dirección IP estática para la interfaz enp0s3, asignando la IP 192.168.2.15 dentro de la subred 192.168.2.0/24, lo cual indica que forma parte de una red local correspondiente a la zona naranja (DMZ) del esquema de red Endian. Como puerta de enlace se definió la dirección 192.168.2.10, que corresponde a la interfaz del firewall Endian en dicha zona, permitiendo así la comunicación hacia otras redes. Además, se configuraron los servidores DNS públicos de Google (8.8.8.8 y 8.8.4.4) para la resolución de nombres.

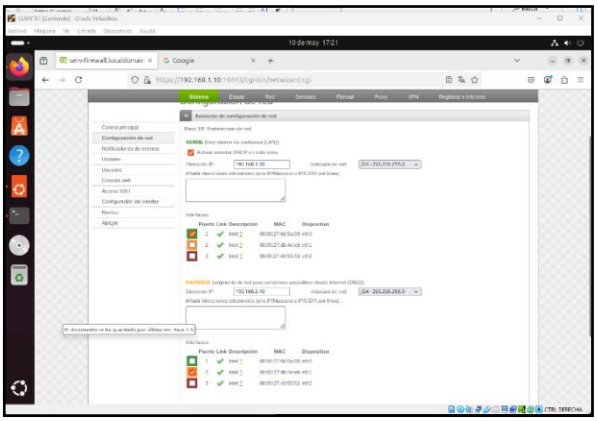
Figura 4. Configuración Endian



Fuente: Ubuntu server elaboración propia

En la figura 4 se presenta la consola de Endian Firewall Community en su versión 3.3.2, donde se evidencia la configuración inicial de las interfaces de red. La zona verde está habilitada en la interfaz eth0, con la dirección IP 192.168.1.10/24, lo que corresponde a la red interna destinada a la comunicación con los dispositivos de la LAN. También se muestra la interfaz eth2 asignada dinámicamente en otra subred, configurada como enlace principal (Uplink) y marcada como activa. Esta configuración indica que el firewall tiene comunicación establecida con una red externa.

Figura 5. Configuración Firewall Endian



Fuente: Firewall Endian elaboración propia

En la figura 5 se aprecia la interfaz web de administración del firewall Endian, específicamente en la sección de configuración de red. Se muestra que la zona **verde** (LAN) tiene asignada la dirección IP 192.168.1.10/24 y que está habilitado el servicio DHCP para esta zona, lo cual permite la asignación automática de direcciones IP a los dispositivos conectados. Asimismo, se evidencia que la zona **naranja** (DMZ) está configurada con la dirección IP 192.168.2.10/24, destinada a alojar servicios accesibles desde Internet de forma segura. Las interfaces físicas están correctamente asignadas a cada zona, y el estado activo de las interfaces está indicado con marcas de verificación verdes.

3 CONFIGURACIÓN NAT.

El uso de NAT (Network Address Translation) es fundamental en redes privadas para permitir que múltiples dispositivos accedan a recursos externos utilizando una única IP pública. En entornos como Endian Firewall, esta funcionalidad es clave para administrar el acceso a Internet desde diferentes zonas de red como LAN (VERDE) y DMZ (NARANJA).

3.1. COMUNICACIÓN DESDE LAN HACIA WAN

La Traducción de Direcciones de Red (NAT) es una técnica utilizada para permitir que dispositivos en una red local (LAN) puedan comunicarse con redes externas (como Internet) a través de una única dirección IP pública. En un entorno virtualizado con tres máquinas (Endian Firewall, Ubuntu Server

y Ubuntu Desktop), es fundamental establecer correctamente una regla de NAT para garantizar dicha comunicación.

En un escenario de red simulado, se utilizan tres zonas de red: una zona verde (LAN interna), una zona naranja (zona DMZ o desmilitarizada) y una zona roja (WAN simulada). La máquina Ubuntu Desktop con dirección IP 192.168.1.10 se ubica en la red verde, representando a los clientes internos. La Ubuntu Server con IP 192.168.2.10 está en la red naranja, simulando servicios expuestos parcialmente al exterior. La red roja representa el acceso a Internet y está gestionada por la interfaz correspondiente del firewall Endian.

El objetivo principal es configurar una regla de NAT en Endian Firewall que permita que la red verde acceda a la red roja, utilizando para ello la función de masquerading que transforma las direcciones IP privadas en la dirección IP pública o de salida.

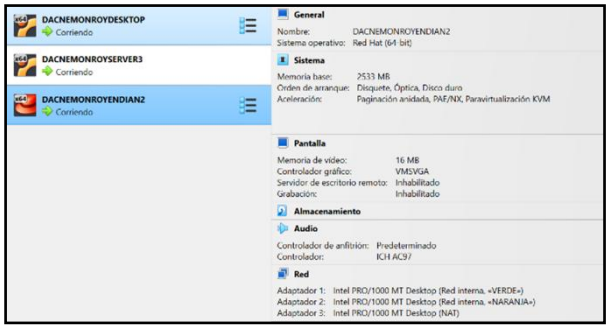
Este proceso permite que múltiples dispositivos internos accedan a Internet utilizando una única IP pública, mientras que el firewall mantiene la tabla de seguimiento de conexiones para asegurar que las respuestas sean reenviadas correctamente al origen.

3.1.1. CONFIGURACIÓN DE INTERFACES DE RED EN ENDIAN

La máquina Endian Firewall debe tener tres interfaces de red:

eth0 (RED): conectada a la red roja (Internet simulado).
eth1 (GREEN): conectada a la red verde 192.168.1.0/24.
eth2 (ORANGE): conectada a la red naranja 192.168.2.0/24.

Figura 6. Configuración máquina virtual

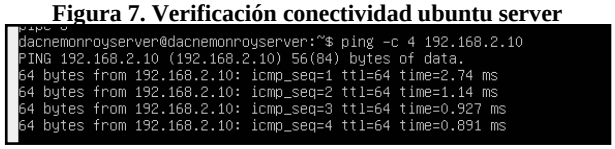


Fuente: Elaboración propia

En la figura 6 se evidencia la configuración de las máquinas virtuales requeridas para realizar el ejercicio práctico.

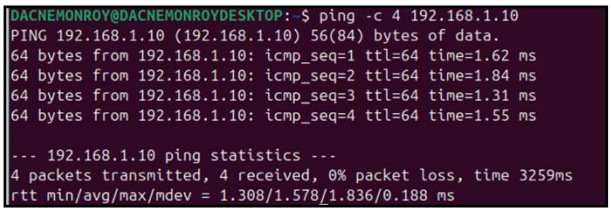
3.1.2. VERIFICAR CONECTIVIDAD ENTRE MÁQUINAS

Figura 7. Verificación conectividad ubuntu server



Fuente: Ubuntu server elaboración propia
Nota: Captura demostrando la verificación de la conectividad ubuntu server

Figura 8. Verificación conectividad Ubunto desktop



Fuente: Ubuntu server elaboración propia
Nota: Captura demostrando la conectividad Ubuntu desktop

En las figuras 7 y 8 se logra evidenciar que las máquinas virtuales tienen comunicación entre ellas.

3.1.3. CONFIGURAR REGLA DE NAT (MASQUERADING) EN ENDIAN

- Ingresar al panel web de Endian.
- Ir a la sección Firewall > NAT > Masquerading.
- Crear una nueva regla:
- Origen: RED VERDE (Green)
- Destino: RED (Red)
- Acción: Masquerading
- Guardar y aplicar la regla.

Figura 9. Creación de regla LAN hacia WAN

Fuente: Firewall Endian Elaboración propia

En la figura 9 se evidencia la creación de la regla LAN hacia WAN mediante la página web endian Firewall

Community con la dirección IP configurada desde la máquina virtual.

3.1.4. VERIFICAR CONECTIVIDAD A LA RED ROJA

Figura 10. Conexión zona roja

```
DACNEMONROY@DACNEMONROYDESKTOP:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=7.58 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=7.76 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=7.40 ms
```

Fuente: Ubuntu server elaboración propia

En la figura 10 se evidencia la conexión al servidor público de Google.

La correcta configuración de NAT no solo permite el acceso a recursos externos, sino que también garantiza un nivel de seguridad al ocultar las direcciones internas detrás de una IP pública o del firewall. Esta práctica es ampliamente utilizada en redes corporativas y domésticas, y su comprensión resulta esencial para administradores de sistemas y redes.

Según , NAT se convierte en una solución efectiva ante la escasez de direcciones IPv4, ya que permite la reutilización de direcciones IP privadas en múltiples redes internas. Asimismo, señalan que, aunque NAT rompe con el principio de extremo a extremo del modelo OSI, su uso sigue siendo práctico y necesario en la mayoría de las implementaciones reales.

3.2. COMUNICACIÓN DE LA ZONA DMZ HACIA LA INTERNET.

En una arquitectura de red segmentada mediante un firewall de tipo Endian, la Zona Desmilitarizada (DMZ) se utiliza para alojar servicios que deben ser accesibles desde Internet. Sin embargo, para permitir que dichos servicios se comuniquen con el exterior, es imprescindible configurar reglas de traducción de direcciones (NAT) y reenviar los puertos necesarios. Esta práctica permite el control seguro del tráfico entre la red interna, la DMZ y la red externa (Internet).

La configuración del reenvío de puertos en el firewall Endian tiene como propósito exponer servicios específicos desde una máquina alojada en la DMZ hacia la red externa (roja), controlando qué puertos están permitidos y asegurando que las solicitudes externas se redirijan al servidor correcto. Este procedimiento se apoya en una regla de DNAT (Destination NAT), que modifica la dirección de destino de los paquetes entrantes hacia el servidor correspondiente.

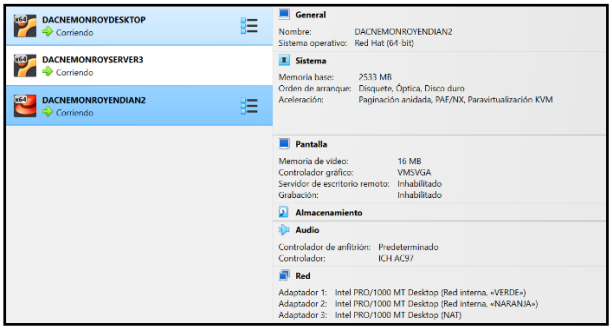
En este caso, la máquina Ubuntu Server con dirección IP 192.168.2.10 está ubicada en la zona naranja (DMZ). Esta red se encuentra entre la red verde (interna) y la red roja (Internet), y es utilizada para servicios como servidores web o FTP. A través del firewall Endian se configurará un reenvío de puerto, por ejemplo, el puerto 80 (HTTP), desde la red roja hacia esta máquina, permitiendo su acceso desde fuera. Al mismo tiempo, se habilitará el acceso saliente desde la DMZ hacia Internet mediante reglas de masquerading .

3.2.1. CONFIGURACIÓN DE RED EN ENDIAN

Endian posee tres interfaces configuradas:

- Red Roja (WAN): conectada a Internet o una red externa simulada.
- Red Naranja (DMZ): 192.168.2.0/24, donde se encuentra la Ubuntu Server con IP 192.168.2.10.
- Red Verde (LAN): 192.168.1.0/24, donde está Ubuntu Desktop con IP 192.168.1.10.

Figura 11. Configuración de interfaces



Fuente: VirtualBox Elaboración propia

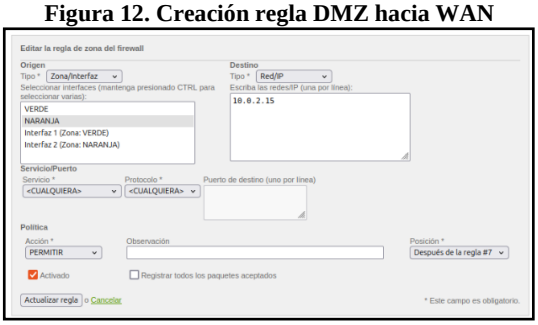
En la figura 11 se evidencia la configuración de las máquinas virtuales requeridas para realizar el ejercicio práctico.

3.2.2. HABILITAR MASQUERADING PARA LA ZONA NARANJA (DMZ)

- Ingresar a Endian vía interfaz web.
- Ir a Firewall > NAT > Masquerading.
- Crear una nueva regla con:
  - Origen: ORANGE (DMZ)
  - Destino: RED (WAN)
  - Acción: Masquerading
- Guardar y aplicar la regla.

Esto permitirá que la Ubuntu Server pueda generar conexiones salientes hacia Internet utilizando la IP pública del firewall.

Figura 12. Creación regla DMZ hacia WAN



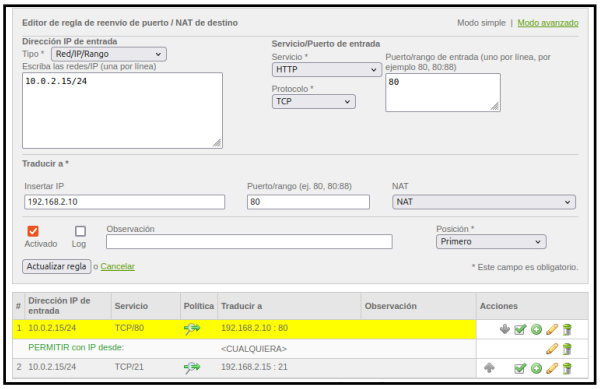
Fuente: firewall Endian Elaboración propia

En la figura 12 se evidencia la creación de la regla DMZ hacia WAN mediante la página web endian Firewall Community con la dirección IP configurada desde la máquina virtual.

3.2.3. CREAR UNA REGLA DE DNAT PARA EXPONER UN SERVICIO AL EXTERIOR

- Desde el panel de Endian, ir a Firewall > Port Forwarding (DNAT).
- Crear una nueva regla con los siguientes parámetros:
  - Origen: RED
  - Destino IP pública: (IP externa de Endian)
  - Puerto externo: 80 (HTTP)
  - Redireccionar a: 192.168.2.10
  - Puerto interno: 80
- Aplicar la regla.

Figura 13. Creación de regla DNAT



Fuente: Firewall Endian Elaboración propia

Esto permite que cualquier solicitud HTTP desde Internet (zona roja) sea reenviada al servidor web alojado en la DMZ. Permitir el tráfico controlado desde y hacia la zona DMZ mediante NAT es una práctica común en entornos empresariales. Según , la DMZ actúa como un "área tampón" entre la red interna y externa, y su propósito es reducir los riesgos de seguridad mientras se mantienen disponibles ciertos servicios públicos en la figura 13 se evidencia la configuración de las reglas. El uso de NAT con DNAT y masquerading permite una separación lógica y segura del tráfico, asegurando que la red interna permanezca aislada de amenazas externas, mientras los servicios en la DMZ operan con visibilidad pública.

En este caso destacan que, a pesar de que el NAT introduce una cierta complejidad en la administración de redes, su uso es casi inevitable cuando se gestionan múltiples zonas de seguridad. La implementación correcta de estas reglas garantiza tanto la funcionalidad como la protección de la red.

Figura 14. Conexión de internet a servidor

Fuente: Edian Elaboración propia

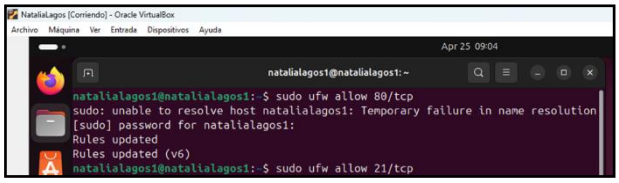
4 PERMITIR A LOS SERVICIOS DE LA ZONA DMZ PARA LA RED

En esta temática del trabajo se configura un servidor Ubuntu en la zona desmilitarizada (DMZ) para permitir únicamente los servicios HTTP y FTP, y se bloquea el protocolo ICMP para evitar la detección del servidor mediante herramientas como ping . La implementación se realiza mediante reglas de firewall iptables, lo que garantiza un entorno más seguro al limitar los vectores de ataque expuestos en la red.

Para ello lo primero es la zona desmilitarizada (DMZ) en una red es una subred perimetral que contiene servicios accesibles desde redes externas, como internet, pero que deben estar separados del resto de la red interna. Este diseño minimiza riesgos al exponer solo los servicios necesarios. En este contexto, es vital permitir únicamente los protocolos requeridos y bloquear otros que puedan ser utilizados para reconocimiento o ataques. En este trabajo se permite el tráfico HTTP (puerto 80) y FTP (puerto 21), mientras se bloquea ICMP (puertos tipo 8 y 30) en un servidor Ubuntu dentro de una DMZ.

Para la configuración el servidor se preparó en primer lugar el servidor Ubuntu en la zona DMZ con los servicios HTTP y FTP instalados, como se puede evidenciar en la figura 15. Configuración del servidor web ubuntu, se muestra la regla de listas donde se puede comprobar el TCP de los puertos 80 y 21 garantizando accesos:

Figura 15. Configuración del servidor web Ubuntu

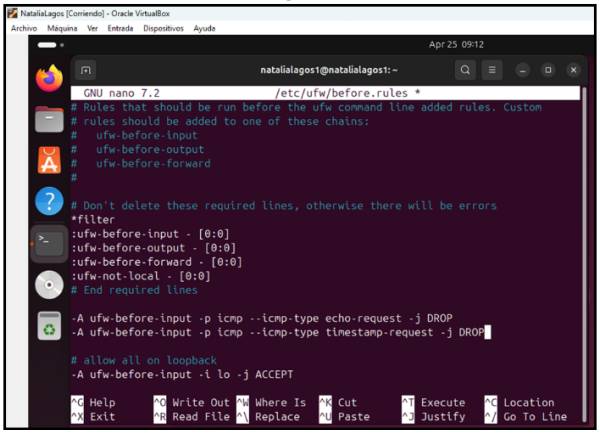


Fuente: Ubuntu server - Elaboración propia

Ahora hay que denegar ICMP en los archivos de configuración “sudo nano /etc/ufw/before.rules”, con el comando “-A ufw-before-input -p icmp --icmp-type echo-request -j DROP” de la siguiente forma:

Debemos guardar y cerrar, para luego recargar el ufw, con el comando “sudo ufw reload”, Verificamos las reglas con el comando “sudo ufw status numbered” en la figura 16 configuración del ICMP en los archivos de configuración porque de esta manera se valida que el servicio FTP se encuentra activo y configurado correctamente permitiendo así las conexiones externas que posteriormente en la figura 17. Bloqueo de los servicios HTTP vamos a cancelar.

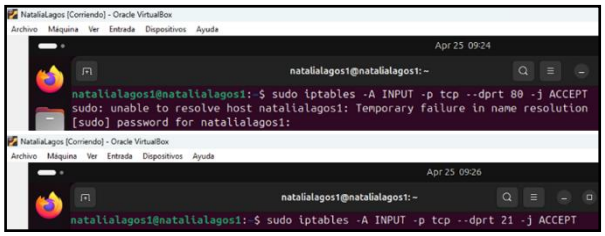
Figura 16. Configuración del CMP en los archivos de configuración.



Fuente: Ubuntu server - Elaboración propia

Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.
Como se evidencia en la figura 17. Bloqueo de los servicios HTTP para poder denegar los servicios HTTP (Puerto 80) y FTP (Puerto 21) y no permitir hacer ping en la red desde el servidor Web bajo Ubuntu Server se implementaron iptables permitiendo HTTP Y FTP bloqueando correctamente los de tipo ICMP 8, lo que es de mucha utilidad a la hora de buscar mejor seguridad y prevenir así mapeos de red, demostrando así en dicha figura que no se recibe ninguna respuesta:

Figura 17. Bloqueo de los servicios HTTP



Fuente: Elaboración propia

Siguiendo con ello, bloqueamos el ICMP de los tipos 80 y de los tipos 21, pasamos a verificar las reglas de tráfico y finalmente probamos el bloqueo del ping, demostrando en la figura 18. Bloqueo del ping que no responde y que dicho intento de conexión o ping es fallido, demostrando así el correcto bloqueo realizado de los puestos tanto 80 como 21 solicitados por el tutor

Figura 18. Bloqueo del ping

Fuente: Elaboración propia

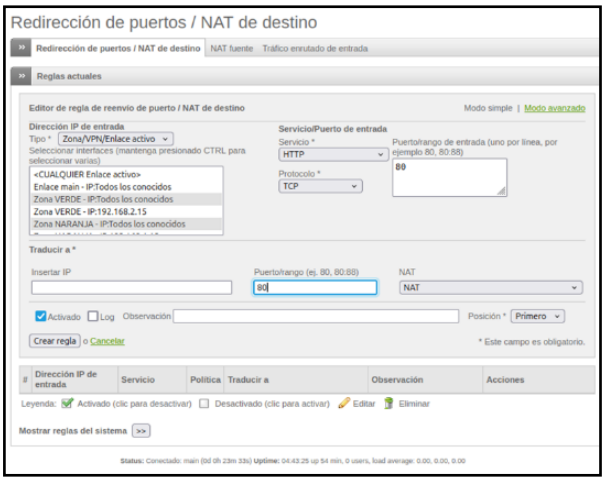
En conclusión, la configuración de servicios HTTP y FTP en la zona mediante los iptables fue exitosa y se logró e implemento una política de acceso controlado en la DMZ permitiendo solo los servicios necesarios (HTTP y FTP) y bloqueando ICMP para reforzar la seguridad del servidor y permitiendo únicamente el tráfico necesario bloqueando ICMP para una mejor seguridad. Esta configuración reduce la superficie de ataque expuesta a redes externas, alineándose con buenas prácticas de seguridad de red. Las pruebas, así como las figuras mencionadas de la 15 a la 18 evidenciaron una correcta operación de los servicios y demostraron la eficacia del bloqueo de pings por medio de las reglas aplicadas mediante iptables.

5 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Como se evidencia en la figura 19, esta configuración asegura que las solicitudes HTTP y FTP provenientes de la Zona Verde lleguen adecuadamente a la Zona Naranja, permitiendo la comunicación entre ambas áreas de la red sin bloquear el tráfico.

Figura 19. Redirección de Puertos /NAT destino

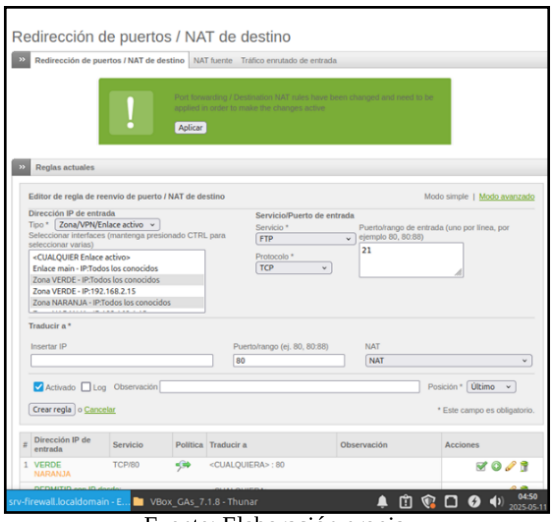


Fuente: Elaboración propia

Comunicando la zona verde con la zona naranja con el protocolo HTTP y FPT con sus respectivos puertos.

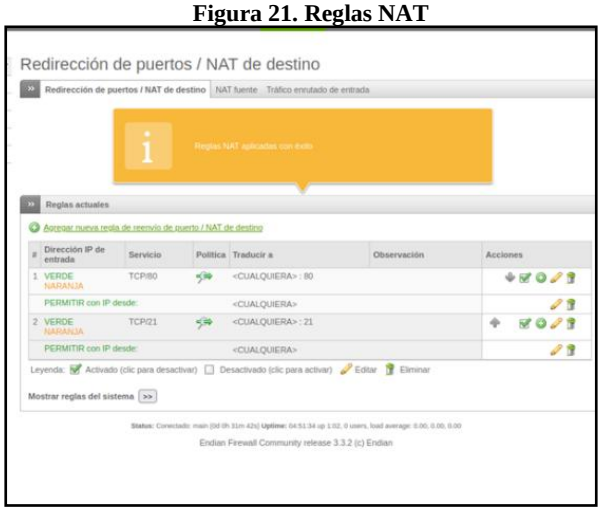
Como se puede evidenciar en las figuras 20 y 21, se realiza la configuración de reglas de acceso en un firewall, con el objetivo de comunicar la Zona Verde con la Zona Naranja utilizando los protocolos HTTP y FTP.

Figura 20. Configurando los parámetros y la ip.



Fuente: Elaboración propia

Figura 21. Reglas NAT

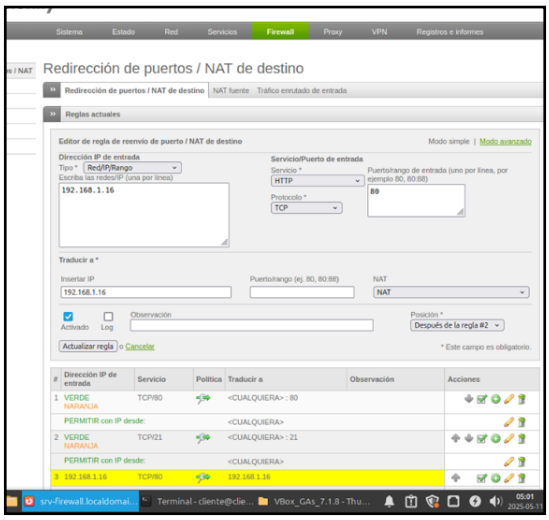


Fuente: Elaboración propia

- HTTP (puerto 80): Permite la transferencia de datos web entre la zona Verde y la zona Naranja. Esto es útil si tienes un servidor web en la DMZ y necesitas que los dispositivos internos accedan a él.
- FTP (puerto 21): Facilita la transferencia de archivos entre ambas zonas. Si tienes un servidor FTP en la DMZ, esta configuración permitirá que los equipos internos lo usen.
- Comunicar la zona Internet con la zona DMZ.

Como se puede evidenciar en las figuras 22 y 23 la configuración permite que dispositivos en la Zona Verde accedan de manera segura a servicios web y FTP alojados en la Zona Naranja, asegurando conectividad sin comprometer la seguridad.

Figura 22. Redirección de puertos



Fuente: Elaboración propia

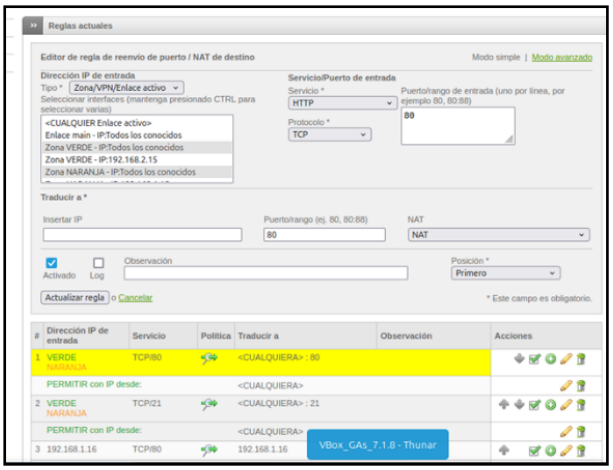
Evidencia de que la configuración se guarda con éxito. La zona Verde representa la red interna segura, donde están los dispositivos de los usuarios. La zona Naranja es la DMZ (Zona Desmilitarizada) según , donde se alojan servidores accesibles desde redes externas. La comunicación entre estas zonas se evidencia en la figura 23. Configuración exitosa y debe ser controlada para garantizar seguridad y funcionalidad.
Verificar en el tráfico Inter - Zona, la creación de las reglas.

Figura 23. Configuración exitosa

Fuente: Elaboración propia

En la figura 24 se evidencia que la configuración se guarda con éxito. Desde un equipo en la Zona Naranja, intenta acceder a un servidor web en la Zona Verde usando un navegador (HTTP en el puerto 80).

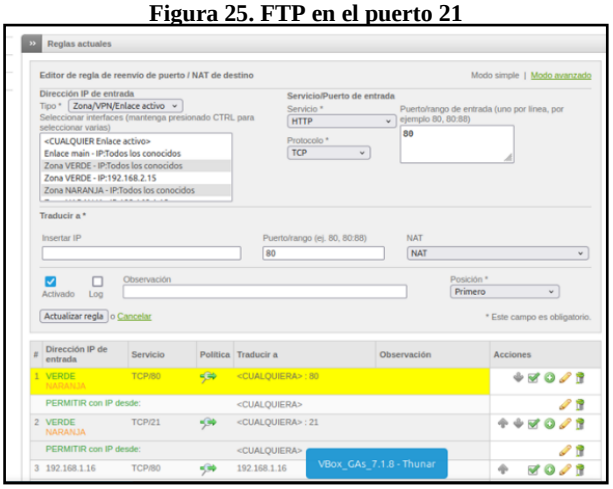
Figura 24. HTTP en el puerto 80



Fuente: Elaboración propia

Desde un equipo en la Zona Naranja, intenta conectarte a un servidor FTP en la Zona Verde usando un cliente FTP (FTP en el puerto 21) como se evidencia en la figura 25.

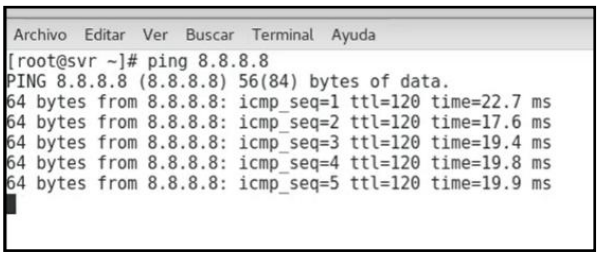
Figura 25. FTP en el puerto 21



Fuente: Elaboración propia

Comunicación de la zona Internet con la zona DMZ, como se puede reconocer en la siguiente ~~figura~~ 26. Internet con la zona DMZ.

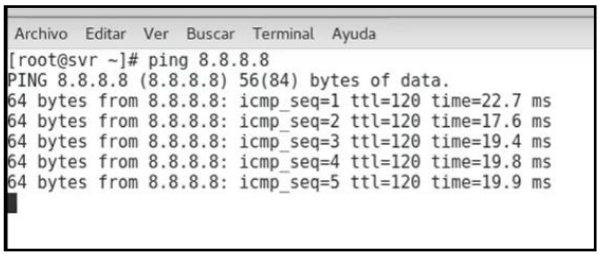
Figura 26. Internet con la Zona DMZ.



Fuente: Elaboración propia

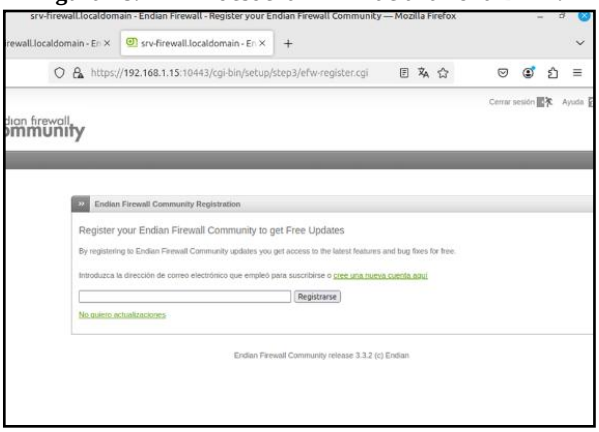
Probar desde un navegador Web, las siguientes directivas: El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. Como se puede evidenciar en las figuras 27 y 28, se permite que los dispositivos en la Zona Verde accedan a los servicios web y FTP alojados en la Zona Naranja, asegurando conectividad sin comprometer la seguridad.

Figura 27. Verifica reglas de tráfico



Fuente: Elaboración propia

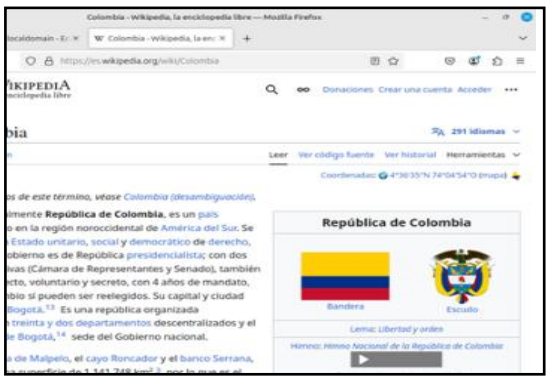
Figura 28. HTTP desde la LAN hacia la zona DMZ.



Fuente: Elaboración propia

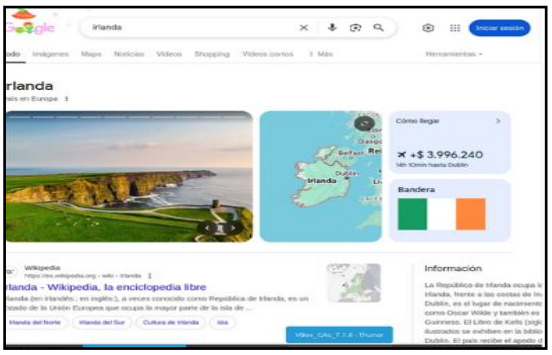
En las figuras 29 y 30 vemos como la red LAN generalmente representa la red interna de usuarios. La DMZ es una zona más segura donde se alojan servidores accesibles desde el exterior. Donde ambas figuras muestran tráfico HTTP saliente desde estas zonas hacia la WAN (internet), lo que indica que las reglas de acceso están funcionando correctamente.

Figura 29. Servicio HTTP desde la LAN hacia la WAN



Fuente: Elaboración propia

Figura 30. Servicio HTTP desde la zona DMZ hacia la WAN



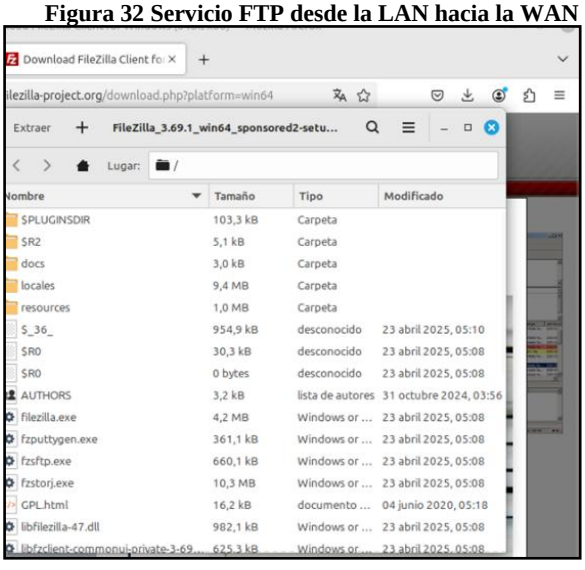
Fuente: Elaboración propia

En la figura 31 se evidencia el ingreso del servicio HTTP desde la WAN hacia la zona DMZ.

Figura 31 Servicio HTTP desde la WAN hacia la zona DMZ

Fuente: Elaboración propia

Figura 32 Servicio FTP desde la LAN hacia la WAN



Fuente: Elaboración propia

En la figura 32 se evidencia el ingreso del servicio FTP desde la WAN hacia la zona DMZ.

Figura 33. Servicio FTP desde la WAN hacia la zona DMZ

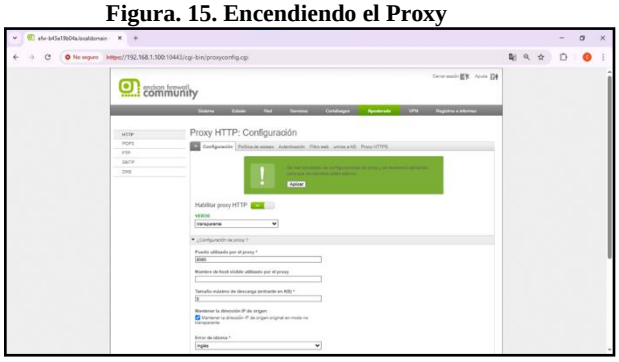
Fuente: Elaboración propia

6 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Para esta temática el objetivo es crear un perfil filtrado web con lista negra: Desde el administrador de endian en la opción Red - editar host se crean los hosts que requerimos bloquear:
www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

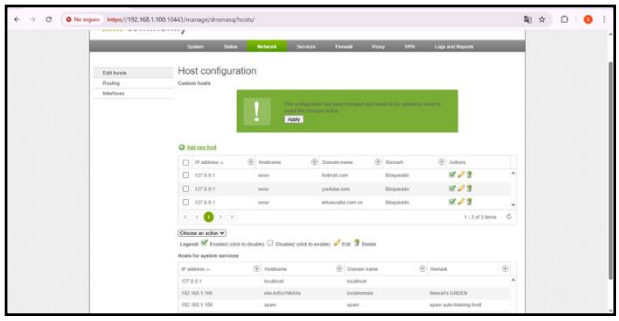
Lo primero que se realizó fue iniciar sesión en el navegador como administrador de Endian, es importante antes de realizar cualquier configuración encender el proxy HTTP y configurarlo como transparente tal como se muestra en la figura 34

Figura. 15. Encendiendo el Proxy



Fuente: Elaboración propia

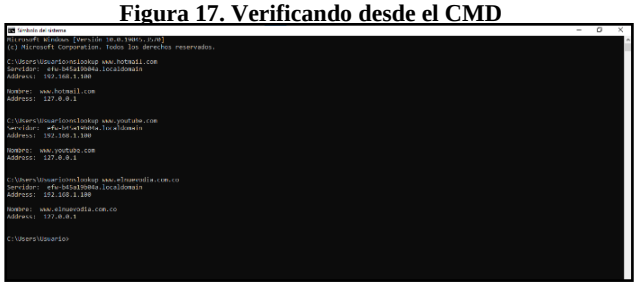
Figura 165. Interfaz web Endian



Fuente: Elaboración propia

En la figura 35 se establecen las políticas de acceso utilizando la IP 127.0.0.1 y asegurándonos que estas reglas tengan prioridad sobre las demás que puedan existir configuradas.

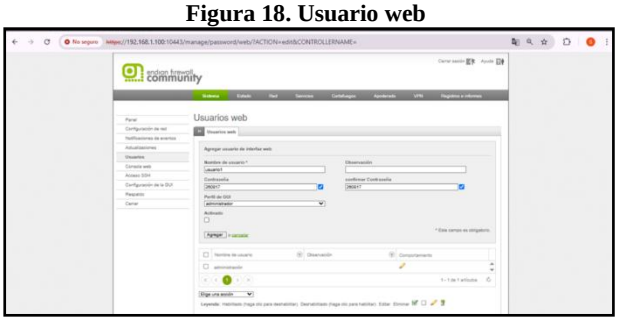
Figura 17. Verificando desde el CMD



Fuente: Elaboración propia

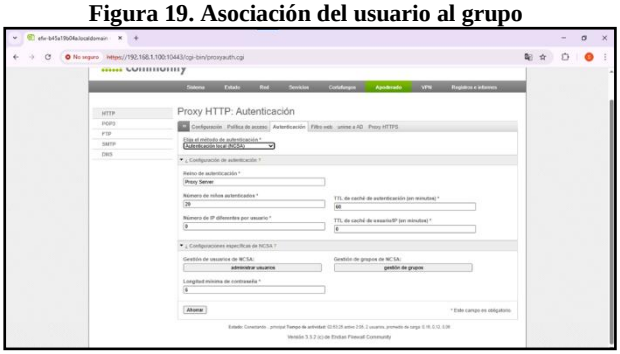
En la figura 36 se verifica desde el CMD utilizando el comando nslookup lo que muestra la página el Address arrojando la IP 127.0.0.1 recordando que esta fue la que se usó para bloquear las páginas

Figura 18. Usuario web



Fuente: Elaboración propia

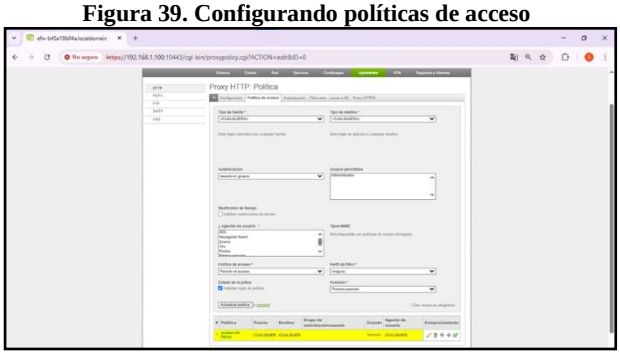
Figura 19. Asociación del usuario al grupo



Fuente: Elaboración propia

En la figura 37 crear un nuevo usuario desde la opción system- users, en la figura 38 en la opción Proxy – HTTP – , se asocia el nuevo usuario a este grupo de administradores para que cuente con todos los permisos

Figura 39. Configurando políticas de acceso



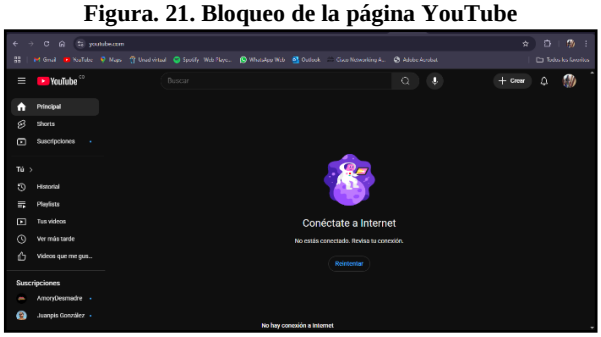
Fuente: Elaboración propia

En la figura 39 configuramos las políticas de acceso del usuario y grupos de usuario, si este cuenta con alguna restricción para acceder a páginas web o algunas carpetas, en este caso se le concedió acceso sin restricciones.

Figura 20. Bloqueo de la página nuevo día

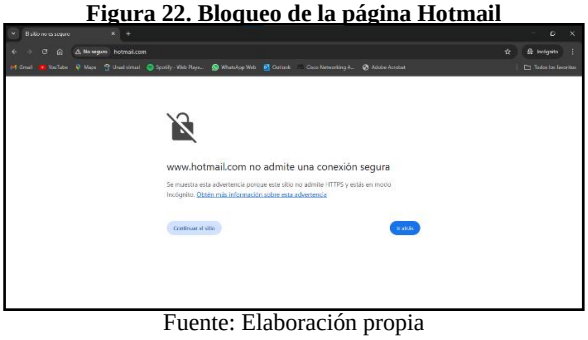
Fuente: Elaboración propia

Figura. 21. Bloqueo de la página YouTube



Fuente: Elaboración propia

Figura 22. Bloqueo de la página Hotmail



Fuente: Elaboración propia

En las figuras 40, 41 y 42 comprobamos el bloqueo de las páginas web configurado anteriormente, en el cual no tenemos acceso a Nuevo día, YouTube y Hotmail

7 CONCLUSIONES

A través de la simulación de un entorno de red segmentado en zonas verde, naranja y roja, y la implementación de una regla de NAT en el firewall Endian, se demostró cómo una máquina en la LAN puede comunicarse con la red externa. Este ejercicio reafirma la importancia de la planificación y correcta configuración de NAT en escenarios de producción y prueba.

La configuración de NAT y reenvío de puertos en un entorno de red segmentado con Endian Firewall demuestra cómo se puede permitir la comunicación de servicios ubicados en la DMZ hacia Internet de forma segura. Este tipo de implementación es crucial en escenarios de servicios web, FTP y correo, donde el control y filtrado del tráfico son fundamentales para la seguridad de la infraestructura de red.

La implementación de GNU/Linux Endian en un entorno virtualizado permite simular eficazmente un entorno seguro y segmentado para prácticas educativas y empresariales. Las reglas NAT, de acceso y el uso del proxy con autenticación fortalecen el control del tráfico y la seguridad perimetral. Endian se presenta como una solución completa y accesible para la gestión integral de redes.

REFERENCIAS

[1] Endian, «Endian Firewall Community,» 2016. [En línea]. Available: https://www.endian.com/community.

[2] Oracle, «VirtualBox Documentation.,» [En línea]. Available: https://www.virtualbox.org .

[3] B. A. Forouzan, Data Communications and Networking (5th ed.), McGraw-Hill Education, 2017.

[4] A. Tanenbaum y D. Wetherall, Computer Networks (5th ed.), Pearson Education., 2011.

[5] Cisco Press, «Cisco Router Firewall Security,» 2004. [En línea]. Available: https://www.ciscopress.com/store/cisco-router-firewall-security-9781587051750.

[6] R. Oppliger, «Internet security: Firewalls and beyond,» *IEEE Security & Privacy*, vol. 1, nº 1, p. 56–62, 2003.

[7] T. Limoncelli, «Securing servers: firewalls and DMZs,» *Commun. ACM*, vol. vol. 52, nº no. 8, p. pp. 28–34, 2009.

[8] U of Linux, «iptables tutorial,» [En línea]. Available: https://linux.die.net/man/8/iptables. [Último acceso: 15 05 2025].

[9] «INGENIERÍA: Ciencia, Tecnología e Innovación.,» vol. 10, nº 1, 2023.

[10] Aquey. (s. f.). ENDIAN, «Cómo bloquear el facebook y otros sitios web https. Scribd.,» [En línea]. Available: https://es.scribd.com/doc/177545589/ENDIAN-Como-bloquear-el-facebook-y-otros|-sitios-web-https. [Último acceso: 20 05 2025].

[11] Getting started, «Endian UTM 3.0 Reference Manual.,» [En línea]. Available: https://docs.endian.com/3.0/utm/first.html.