IMPLEMENTACIÓN Y EVALUACIÓN DE MEDIDAS DE SEGURIDAD EN UN ENTORNO GNU/LINUX CON ENDIAN FIREWALL

Huendy Vanesa Moreno Grajales
e-mail: hvmorenog@unadvirtual.edu.co
Carlos Ardila Romero
e-mail: cardilaro@unadvirtual.edu.co
Andrés Felipe Cardona Bermúdez
e-mail: afcardonab@unadvirtual.edu.co
Francy Katerine Niño López
e-mail: fkninol@unadvirtual.edu.co
Jorge Andrés Cano Cano
e-mail: jacanocan@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de una infraestructura de seguridad perimetral utilizando Endian Firewall en un entorno virtualizado con VirtualBox. Se configuran las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), aplicando reglas de NAT para permitir comunicación controlada entre los segmentos de red. Asimismo, se gestionan servicios en la DMZ, habilitando únicamente protocolos autorizados como HTTP y FTP, y restringiendo ICMP para reforzar la protección. Se establecen políticas de acceso interzonal basadas en principios de aislamiento y mínimos privilegios. Finalmente, se implementa un Proxy HTTP no transparente con autenticación y listas negras para el filtrado de contenido desde la LAN. La experiencia demuestra la efectividad de Endian Firewall como herramienta pedagógica y práctica para comprender la administración y seguridad de redes basadas en tecnologías open source.*

PALABRAS CLAVE: Seguridad Perimetral, Endian Firewall, Administración de Redes, Autenticación, Cliente, Servidor, LAN. DMZ, NAT.

1 INTRODUCCIÓN

La seguridad perimetral constituye un componente esencial en la protección de los sistemas de información, al permitir el control del flujo de tráfico entre redes con diferentes niveles de confianza. En este contexto, los firewalls basados en GNU/Linux se han consolidado como soluciones robustas y flexibles para la administración de accesos, segmentación de redes y disponibilidad segura de servicios. Endian Firewall, una de estas plataformas, integra funcionalidades de filtrado, NAT, proxis y gestión de zonas de seguridad, lo que lo convierte en una herramienta idónea tanto para entornos educativos como productivos.

La virtualización mediante herramientas como VirtualBox facilita la experimentación con arquitecturas de red que incluyen zonas de seguridad diferenciadas, como la LAN (Zona Verde), la WAN (Zona Roja) y la DMZ (Zona Naranja). Este enfoque permite reproducir escenarios reales de administración y control del tráfico sin comprometer infraestructuras físicas.

Este artículo presenta el despliegue e implementación de Endian Firewall en un entorno virtualizado, abordando la configuración de reglas de NAT, políticas interzonales, habilitación de servicios en la DMZ y la integración de un Proxy HTTP no transparente con autenticación. El objetivo es evidenciar el proceso de construcción de un entorno de seguridad perimetral y fortalecer las competencias en administración de redes y filtrado de contenido.

2 ENDIAN FIREWALL

2.1 CARACTERÍSTICAS GENERALES

Endian Firewall es una distribución GNU/Linux orientada a la implementación de soluciones de seguridad perimetral y de gestión unificada de amenazas (Unified Threat Management, UTM). Entre sus características más destacadas se encuentran:

- Sistema de segmentación mediante zonas de seguridad (Verde, Roja, Naranja, Azul).
- Proxy HTTP/HTTPS con autenticación y filtrado de contenido.
- Soporte para NAT, reenvío de puertos y políticas basadas en estados de conexión.
- Servicios integrados como VPN (OpenVPN, IPsec), IDS/IPS (Snort), antivirus y antispam.
- Panel de administración web intuitivo, orientado tanto a usuarios experimentados como a procesos de formación.

Estas características convierten a Endian en una herramienta robusta para implementar políticas de seguridad perimetral en entornos heterogéneos.

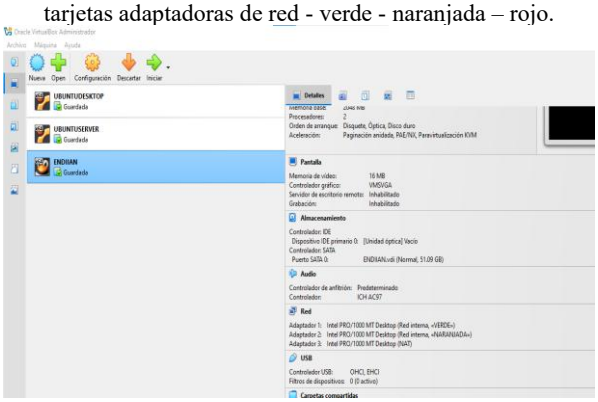
El sistema opera como un cortafuegos de inspección de estado, permitiendo establecer reglas dinámicas basadas en el contexto de las conexiones. Además, incorpora módulos de proxy, servicios de traducción de direcciones y monitoreo del tráfico, lo que facilita la administración centralizada y mejora la visibilidad del comportamiento de la red.

3 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

La instalación del firewall Endian dentro de un entorno virtualizado se convierte en un paso fundamental para establecer una arquitectura de red segura y segmentada. Para esta etapa del proyecto se realizó la creación de la máquina virtual en VirtualBox, seguida por la asignación de los recursos necesarios y la definición de las interfaces de red que permitirían la separación lógica entre LAN, DMZ y WAN. Esta configuración inicial tiene como propósito construir un entorno controlado donde cada zona opere de manera independiente, pero administrada desde un único punto centralizado: el firewall.

Durante el proceso de instalación se definieron los parámetros básicos del sistema, como el reconocimiento de las tarjetas de red, la identificación de cada interfaz física dentro del instalador y la asignación preliminar de direcciones IP según el rol que desempeñaría cada zona. Posteriormente, se accedió al panel de administración vía navegador desde el cliente para completar la configuración y verificar el correcto funcionamiento del enrutamiento. Este conjunto de pasos permitió asegurar que Endian quedara completamente operativo como dispositivo de seguridad capaz de gestionar tráfico, segmentar redes y servir como base para las capas de seguridad que se implementarán en fases posteriores.

Figura 1. Evidencia de la configuración de ENDIAN con las 3 tarjetas adaptadoras de red - verde - naranjada – rojo.



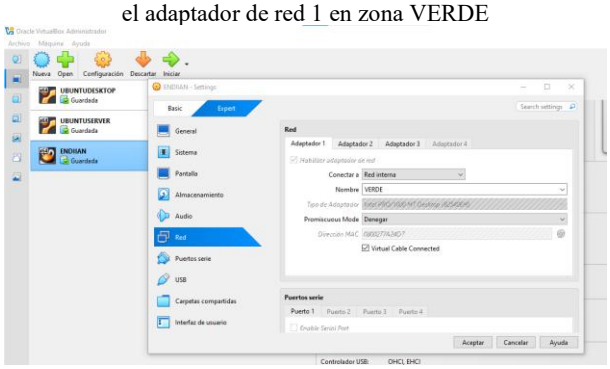
Fuente: autoría propia

3.1 CONFIGURACIÓN DE TARJETAS DE RED EN VIRTUALBOX PARA ENDIAN

Para lograr una separación efectiva entre las distintas zonas de red, fue necesario configurar correctamente las tarjetas virtuales asignadas a la máquina de Endian. Cada una de ellas fue vinculada a un modo de conexión diferente, de acuerdo con la función que debía cumplir dentro del laboratorio. El Adaptador 1 se estableció como Red Interna bajo el nombre “VERDE”, pensado para alojar la conexión del cliente y simular la red local interna. El Adaptador 2 también se configuró como Red Interna, pero bajo el nombre “NARANJADA”, destinada exclusivamente a la DMZ donde se ubica el Ubuntu Server. Finalmente, el Adaptador 3 se configuró en modo NAT, permitiendo que Endian cuente con acceso a Internet a través de la red física del host, cumpliendo así con el rol de Zona Roja.

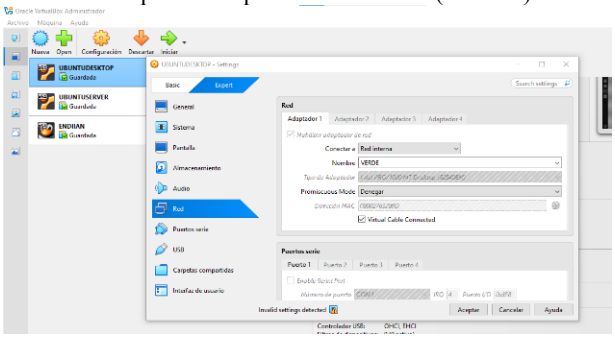
Cada adaptador fue verificado para asegurar que estuviera habilitado, con el cable virtual conectado y con el modelo de red compatible con Endian para evitar fallos en la detección. Esta estructura garantiza que Endian actúe como intermediario entre todas las máquinas del entorno virtual, sin que exista comunicación directa entre ellas que no pase previamente por el firewall. De esta manera, la topología queda correctamente definida desde el plano virtual, permitiendo avanzar a configuraciones más profundas de filtrado, servicios o monitoreo.

Figura 2. Evidencia de configuración de la red del ENDIAN en el adaptador de red 1 en zona VERDE



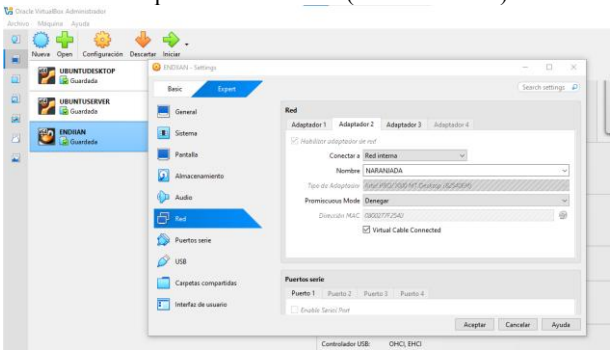
Fuente: autoría propia

Figura 3. Evidencia de configuración de la red del UBUNTU desktop en el adaptador de red 1 con (VERDE).



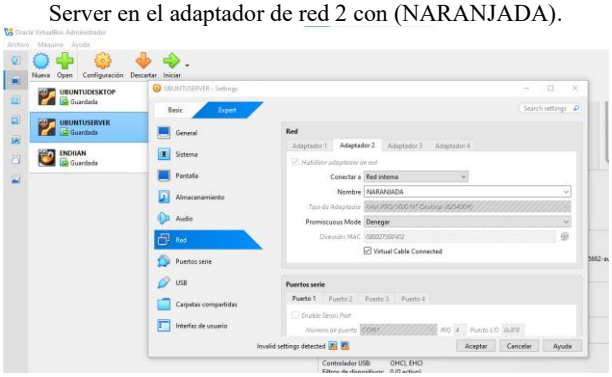
Fuente: autoría propia

Figura 4. Evidencia de configuración de la red del ENDIAN en el adaptador de red 2 con (NARANJADA).



Fuente: autoría propia

Figura 5. Evidencia de configuración de la red del UBUNTU Server en el adaptador de red 2 con (NARANJADA).



Fuente: autoría propia

3.2 ASIGNACIÓN DE DIRECCIONES IP Y VERIFICACIÓN DE CONECTIVIDAD

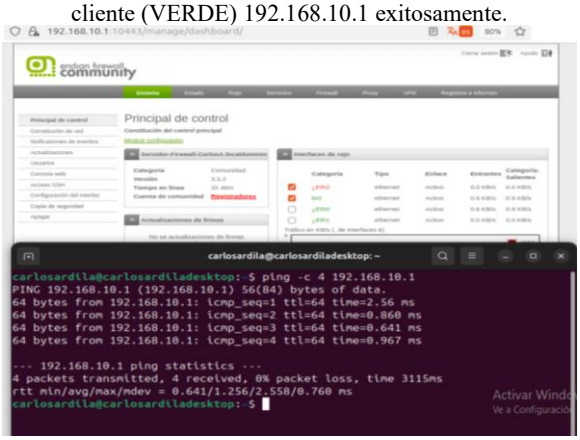
Tras la configuración de los adaptadores, se procedió a la asignación de los segmentos de red para cada zona. En la zona Verde se definió la subred 192.168.10.0/24, otorgando a Endian la dirección 192.168.10.1, destinada a servir como puerta de enlace del equipo cliente conectado a esta red. En la zona Naranja se configuró la subred 192.168.20.0/24, asignándole al firewall la dirección 192.168.20.1, la cual sería posteriormente utilizada como gateway por el Ubuntu Server. La zona Roja quedó administrada automáticamente por VirtualBox a través del adaptador NAT, lo que permitió el acceso a Internet sin necesidad de configuraciones adicionales.

Para verificar el correcto funcionamiento del enrutamiento, se realizaron pruebas de conectividad desde cada máquina virtual. El Ubuntu Desktop fue configurado con la IP 192.168.10.2, logrando conectarse al panel web de Endian mediante la dirección 192.168.10.1. Por su parte, el Ubuntu Server recibió la IP 192.168.20.2, desde donde se comprobó la conectividad hacia el firewall y la funcionalidad de la DMZ. Estas pruebas permitieron asegurar que la comunicación entre las zonas respondía según lo esperado y que las rutas internas estaban correctamente gestionadas por el firewall. Con ello, la base del entorno quedó lista para las siguientes actividades, como la implementación de servicios y reglas de seguridad.

Figura 6. Evidencia de iniciar el ENDIAN, donde muestra los dos adaptadores configurados, el 1 para el cliente desktop (VERDE), el otro en (ROJO) configurado y el adaptador NAT para la navegación a internet automática DHCP.

Fuente: autoría propia

Figura 7. Evidencia que muestra que desde la terminal de Desktop se hace ping con la dirección IP configurada para el cliente (VERDE) 192.168.10.1 exitosamente.



Fuente: autoría propia

Figura 8. Evidencia que muestra que con el UBUNTU SERVER también se hace ping con la dirección IP asignada en el portal de ENDIAN desde el navegador de desktop, evidenciado anteriormente con 192.168.20.1 y se visualiza el ping exitosamente.

Fuente: autoría propia

4 CONFIGURACIÓN NAT

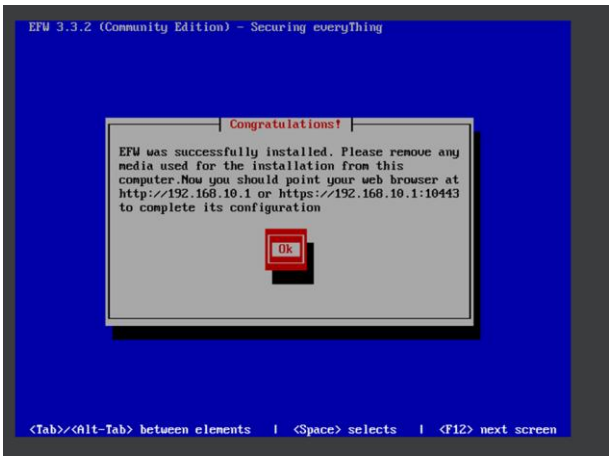
La configuración de Network Address Translation (NAT) constituye uno de los mecanismos esenciales en la administración y aseguramiento del tráfico dentro de redes segmentadas. Su funcionalidad principal se basa en traducir direcciones IP privadas a direcciones públicas o direccionamientos válidos para redes externas, permitiendo la comunicación entre diferentes zonas sin comprometer la seguridad interna. En arquitecturas perimetrales basadas en firewall, como Endian Firewall, NAT cumple un papel estratégico al encapsular los paquetes provenientes de segmentos internos y exponer únicamente la dirección IP asignada a la interfaz WAN.

En el entorno desarrollado, la traducción de direcciones fue crucial para permitir que los equipos ubicados en la zona DMZ (ORANGE) y LAN (GREEN) accedieran a la red WAN sin revelar su estructura interna. La aplicación de la técnica MASQUERADE fue determinante, pues al utilizar una interfaz WAN configurada mediante DHCP, permitió que todos los paquetes salientes adoptaran la dirección pública asignada al firewall en tiempo real. Este enfoque aseguró la continuidad del servicio, la adecuada circulación del tráfico y la preservación de la integridad de la topología interna.

Figura 9. Interfaces de red Adaptador 3 – NAT Cable conectado –Tipo de adaptador consistente.

Fuente: Autoría Propia

Figura 10. Configuración de la interfaz perteneciente a la zona verde (LAN) en el firewall Endian, donde se establece la dirección privada 192.168.10.1/24 que sirve como puerta de enlace para los equipos internos. Esta configuración constituye la base de la infraestructura previa a la aplicación de reglas NAT.



Fuente: Autoría Propia

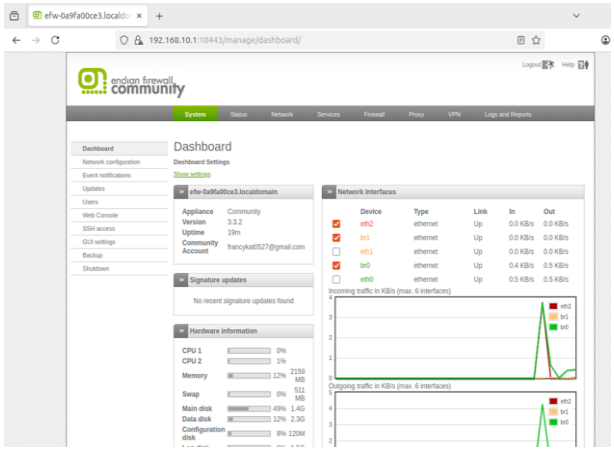
4.1 IMPORTANCIA DE LA TRADUCCIÓN DE DIRECCIONES EN AMBIENTES SEGMENTADOS

En una infraestructura donde la seguridad se construye mediante segmentación por zonas, como Verde (LAN), Naranja (DMZ) y Roja (WAN), la traducción de direcciones representa uno de los componentes más relevantes para garantizar la comunicación controlada entre redes de distinto nivel de exposición. En particular, la zona DMZ aloja servicios que requieren interacción con redes externas, pero sin exponer sus direcciones reales ni permitir accesos directos desde la LAN o la WAN.

La implementación de NAT de salida desde la DMZ permite que los servidores web, de base de datos o de aplicación utilicen la dirección pública del firewall como punto de enlace hacia Internet. De esta manera, se reduce significativamente la superficie de ataque, se mitigan riesgos derivados del reconocimiento activo (como escaneo de puertos o rastreo de topologías internas) y se garantiza la preservación de la arquitectura perimetral.

Este mecanismo no solo actúa como un puente de conectividad, sino también como una barrera protectora que impide que el tráfico externo identifique la estructura interna de los servicios, cumpliendo así con principios fundamentales de seguridad en capas.

Figura 11. Configuración de red del servidor ubicado en la zona DMZ, empleando la dirección privada 192.168.20.50/24. Esta evidencia muestra por qué las direcciones internas requieren traducción (NAT) para comunicarse con redes externas sin ser expuestas directamente.



Fuente: Autoría Propia.

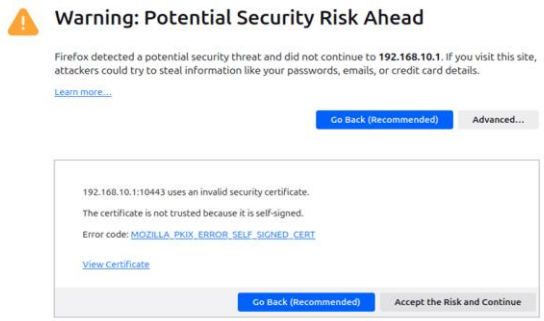
4.2 IMPLEMENTACIÓN PRÁCTICA DE NAT EN EL FIREWALL ENDIAN

La implementación práctica de NAT dentro del firewall Endian se desarrolló mediante la configuración de reglas de Outgoing NAT. Este tipo de regla se utiliza para permitir que el tráfico interno salga hacia Internet utilizando la IP pública asociada a la interfaz WAN (RED). Para este proyecto, la traducción se aplicó tanto a la zona Naranja (DMZ) como a la zona Verde (LAN), con el fin de validar el funcionamiento integral de la infraestructura.

El procedimiento consistió en acceder al panel administrativo del firewall y crear una regla de MASQUERADE indicando como origen la red 192.168.20.0/24 (DMZ) y como destino la interfaz RED (WAN). La misma configuración se replicó para la red 192.168.10.0/24 (LAN). Esta traducción garantiza que todo el tráfico proveniente de estas zonas sea encapsulado y enviado hacia Internet con una dirección válida.

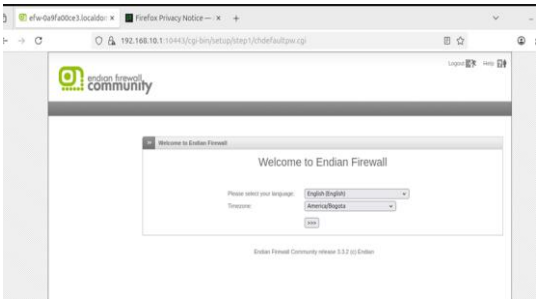
A nivel operativo, la traducción de direcciones se validó mediante pruebas de conectividad (ping hacia 8.8.8.8 y consultas DNS). Adicionalmente, se inspeccionaron las tablas de iptables para confirmar la presencia de reglas NAT aplicadas automáticamente por Endian.

Figura 12. Acceso inicial a la interfaz administrativa del firewall Endian a través del navegador web. Desde este panel se gestionan las reglas de filtrado, traducción de direcciones (NAT) y configuración perimetral del sistema.



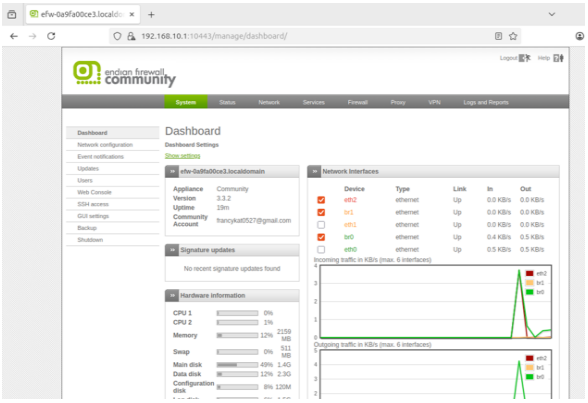
Fuente: Autoría Propia

Figura 13. Pantalla de configuración inicial del entorno gráfico del firewall Endian, donde se selecciona el idioma y la zona horaria para la administración del sistema. Este paso precede a la implementación de reglas de NAT.



Fuente: Autoría Propia

Figura 14. Archivo de configuración del servidor en la DMZ, donde se especifican la dirección IP, puerta de enlace y DNS utilizados. Este direccionamiento es el origen del tráfico que será posteriormente traducido mediante la regla MASQUERADE del firewall.



Fuente: Autoría Propia

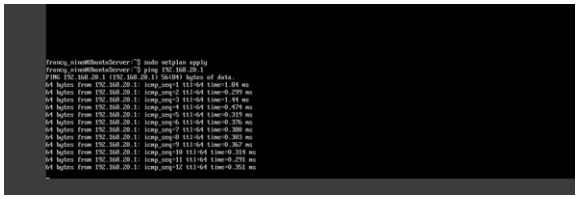
Figura 15. Archivo Netplan del servidor Ubuntu en la DMZ, mostrando la declaración explícita de los parámetros de red (IP, máscara, puerta de enlace y DNS). Esta configuración garantiza que el tráfico de la DMZ sea enrutable a través del firewall.

Fuente: Autoría Propia

Figura 16. Resultado de la validación y aplicación del archivo de configuración netplan, asegurando que los valores asignados al servidor DMZ se carguen correctamente antes de realizar pruebas de NAT.

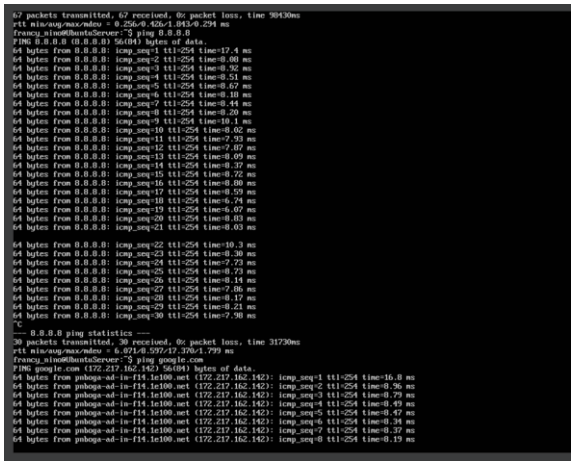
Fuente: Autoría Propia

Figura 17. Prueba de conectividad desde el servidor Ubuntu en la DMZ hacia Internet mediante ping al servidor 8.8.8.8. La respuesta exitosa verifica el funcionamiento del mecanismo NAT aplicado en el firewall Endian.



Fuente: Autoría Propia

Figura 18. Validación de resolución DNS desde la DMZ mediante consulta hacia dominios externos. Esta prueba confirma no solo la conectividad WAN, sino también la correcta traducción y manejo del tráfico saliente a través de NAT.



Fuente: Autoría Propia

5 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

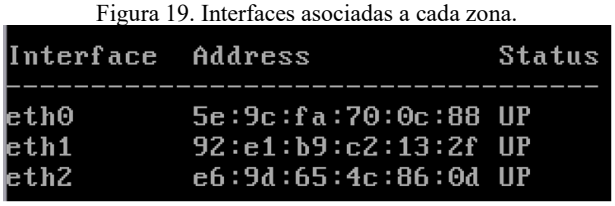
En el diseño de redes seguras es fundamental segmentar los servicios y establecer controles estrictos sobre el tráfico entre zonas como la red interna (LAN), la DMZ y la red externa. La DMZ es utilizada para alojar servicios que requieren acceso controlado desde otras zonas, reduciendo así la exposición directa de los recursos internos.

El objetivo de esta práctica fue implementar políticas de seguridad en Endian Firewall para gestionar el tráfico entre la zona GREEN (192.168.10.0/24) y la zona ORANGE (192.168.20.0/24), donde se encuentra un servidor Ubuntu con servicios web y FTP. Además, se configuraron reglas de bloqueo del protocolo ICMP para evitar la utilización del comando ping, lo que contribuye a disminuir acciones de reconocimiento no autorizado dentro de la red.

Configuración de zonas en ENDIAN NGFW

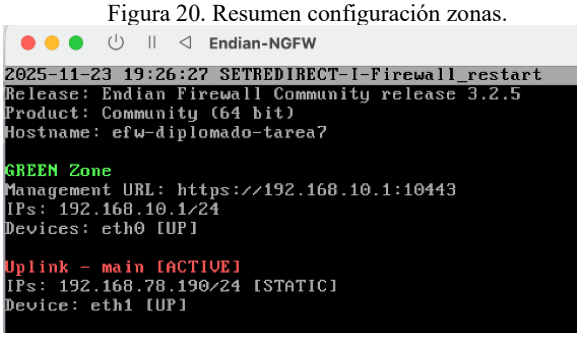
- **Zona Green** - 192.168.10.1/24
- **Zona Red** - 192.168.78.190/24
- **Zona Orange -** 192.168.20.1/24

Figura 19. Interfaces asociadas a cada zona.



Fuente: Autoría Propia

Figura 20. Resumen configuración zonas.



Fuente: Autoría Propia

5.1 METODOLOGIA

La metodología empleada en esta práctica consistió en la implementación progresiva de reglas de seguridad dentro de un entorno segmentado administrado por Endian Firewall. Para ello, primero se definió una arquitectura de red conformada por dos zonas internas: la zona GREEN, correspondiente a la red LAN, y la zona ORANGE, designada como la DMZ donde se alojó un servidor Ubuntu con servicios web y FTP. Esta topología permitió simular un escenario real de control de tráfico entre redes con niveles de seguridad diferenciados.

Una vez establecida la estructura de red, se procedió a la habilitación de los servicios necesarios en la DMZ. Este proceso requirió la creación de reglas específicas en el módulo de Inter-Zone Traffic del firewall, permitiendo el acceso desde la zona GREEN hacia los puertos 80 (HTTP) y 21 (FTP) del servidor Ubuntu ubicado en la zona ORANGE. Dichas reglas fueron configuradas de manera que únicamente autorizaran el tráfico indispensable para el funcionamiento del servidor, asegurando la restricción de cualquier otro tipo de conexión no requerida.

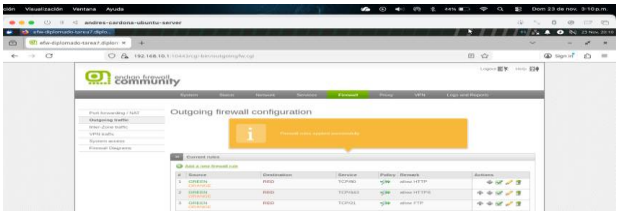
Posteriormente, se implementó una política de bloqueo para el protocolo ICMP con el objetivo de impedir el uso del comando ping entre las zonas GREEN y ORANGE. Esta acción se llevó a cabo mediante la creación de una regla de tipo deny aplicada al tráfico ICMP, abarcando tanto los paquetes de solicitud (echo-request) como los de respuesta (echo-reply). La medida buscó reducir la capacidad de reconocimiento de red por parte de hosts internos o potenciales actores maliciosos.

Finalmente, se desarrolló un proceso de validación para comprobar el correcto funcionamiento de las reglas aplicadas. Esta etapa incluyó pruebas funcionales desde la red GREEN, utilizando comandos como curl, ftp y ping en dirección a la DMZ. Además, se revisaron los registros generados por el firewall en el módulo de Logs & Reports, lo cual permitió confirmar que el tráfico permitido y el tráfico denegado coincidían con las políticas configuradas. Este análisis sirvió para asegurar la efectividad de las reglas implementadas y su impacto en el comportamiento de la red.

5.2 RESULTADOS

Los resultados obtenidos durante la práctica permitieron comprobar el funcionamiento adecuado de las políticas de seguridad configuradas en Endian Firewall. En primer lugar, la habilitación de los servicios HTTP y FTP en la zona DMZ se validó correctamente mediante pruebas de conectividad desde la zona GREEN. El servidor Ubuntu, ubicado en la red ORANGE, respondió de forma satisfactoria a las solicitudes realizadas tanto en el puerto 80 como en el puerto 21, lo cual confirmó que las reglas de permiso aplicadas en el módulo Inter-Zone Traffic fueron procesadas de manera correcta por el firewall.

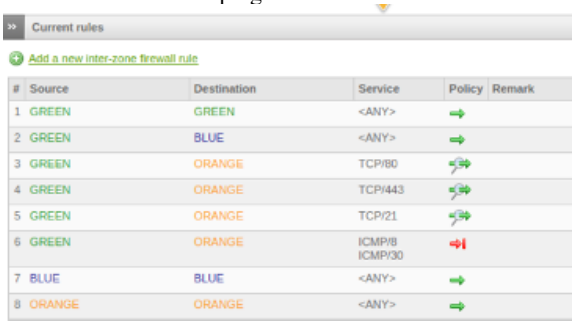
Figura 21. Creación y configuración de reglas que permite el tráfico HTTP (80), HTTPS (443) y FTP (21) entre zona verde y zona naranja (DMZ) en 'Outgoint traffic' y 'Inter-Zone traffic'.



Fuente: Autoría Propia

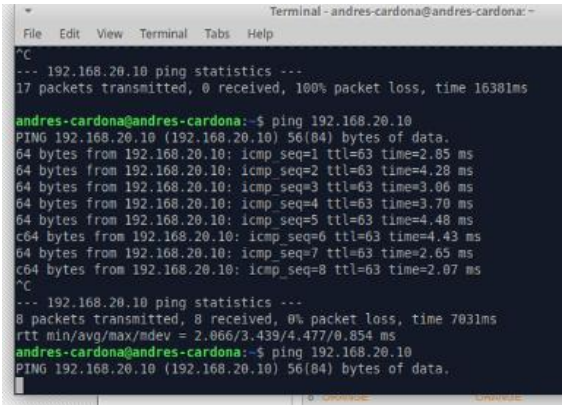
Asimismo, la aplicación de la política de bloqueo del protocolo ICMP mostró resultados consistentes con los objetivos planteados. Al ejecutar el comando ping desde la zona GREEN hacia la zona ORANGE, no se obtuvo respuesta alguna por parte del servidor ubicado en la DMZ. Esto evidenció que las solicitudes echo-request y sus correspondientes echo-reply estaban siendo filtradas de acuerdo con la regla de denegación configurada. La ausencia de respuesta confirmó que el firewall estaba bloqueando correctamente el tráfico ICMP entre ambas zonas.

Figura 22. Configuración de reglas de ICMP para denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.



Fuente: Autoría Propia

Figura 23. Pruebas de denegación ICMP. Antes y Después de la creación de regla.



Fuente: Autoría Propia

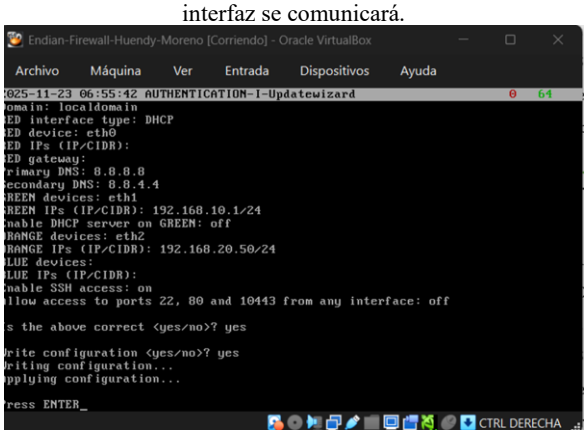
Durante la revisión de los logs generados por Endian Firewall, se identificaron registros correspondientes tanto a conexiones permitidas como a conexiones denegadas. Los eventos relacionados con los servicios HTTP y FTP aparecieron marcados como tráfico autorizado, mientras que las solicitudes ICMP fueron clasificadas como tráfico bloqueado. Esta evidencia corroboró el funcionamiento adecuado del firewall y permitió validar la correcta aplicación de las reglas configuradas.

Finalmente, el análisis conjunto de las pruebas funcionales y los registros del firewall permitió verificar que las políticas implementadas impactaron directamente en el comportamiento del tráfico interzonal. El acceso controlado a los servicios de la DMZ y el bloqueo del protocolo ICMP demostraron la efectividad de la segmentación y el filtrado aplicado mediante Endian Firewall, cumpliendo con los requisitos establecidos en la práctica.

6 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En un firewall, las reglas de acceso son el mecanismo que permite controlar el tráfico de red. Su importancia se debe a que son las que definen de forma precisa qué tipos de tráfico pueden ingresar, salir o circular entre las diferentes zonas, esto para garantizar que sean permitidas únicamente comunicaciones autorizadas. Este control selectivo evita que la red interna quede expuesta a accesos no permitidos o a posibles ataques. Al establecer políticas específicas sobre protocolos y puertos como HTTP o FTP, se puede publicar servicios en la DMZ de forma controlada, esto, permitiendo que la red interna sea aislada de riesgos y asegurando un flujo de información que concuerde con los principios de confidencialidad, integridad y disponibilidad. Es válido aclarar que, las reglas de acceso no solo organizan el tráfico, sino que constituyen la base operativa para mantener una infraestructura segura, estable y alineada con las necesidades del entorno.

Figura 24. Configuración de los adaptadores de red en Endian para manejar varias conexiones de red y definir cómo cada interfaz se comunicará.



Fuente: Autoría Propia

6.1 CONFIGURACIÓN DEL FIREWALL Y APLICACIÓN DE LAS REGLAS

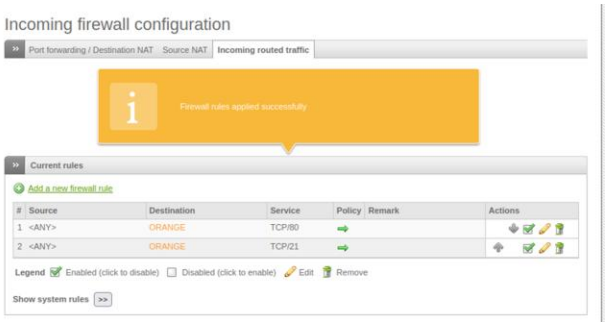
Principalmente, para el desarrollo de la práctica se configuró un firewall en Endian, en este, se establecieron y configuración las zonas e IPs definidas en párrafos anteriores. La zona verde se llevó a cabo mediante un cliente Ubuntu escritorio y para la zona naranja se instaló un servidor Ubuntu Server con los servicios Apache2 y vsftpd.

Una vez establecida la arquitectura, se procedió con la creación de las reglas necesarias en la interfaz de Endian (navegador del cliente). En la sección Inter-Zone, se habilitó el tráfico desde la zona verde hacia la DMZ para los servicios HTTP y FTP y, en la sección Incoming Firewall se configuraron reglas que permiten el acceso desde Internet hacia los servicios de la DMZ (Servidor), asegurando al mismo tiempo que la red interna estuviera protegida.

Para asegurar la correcta aplicación de las políticas a nivel del sistema operativo (SO), se accedió al firewall mediante SSH desde el cliente 192.168.10.50.

Por último, se aplicaron y verificaron las políticas utilizando las herramientas proporcionadas por el mismo firewall y los servicios del servidor.

Figura 25. Configuración del incoming firewall en Endian para controlar y limitar el tráfico que ingresa desde las diferentes interfaces específicas hacia la red interna o el mismo firewall.



Fuente: Autoría Propia

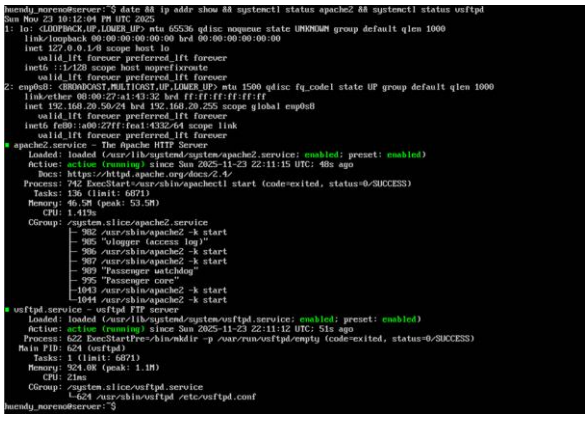
6.2 RESULTADOS DE LAS PRUEBAS DE CONECTIVIDAD

Después de configurar las reglas de acceso, se realizaron varias pruebas para confirmar que todo estuviera funcionando correctamente.

Desde la zona verde fue posible entrar al servidor web y al servicio FTP que están en la DMZ, usando tanto el navegador como la terminal con el comando curl y clientes FTP. Esto permitió comprobar que el firewall estaba filtrando el tráfico y solo dejaba acceder a lo que había sido autorizado. Además, se revisó la conexión a Internet desde la LAN (Cliente - Zona verde) y desde la DMZ (Servidor - Zona naranja), lo que tuvo como resultado que ambas están funcionando correctamente.

Finalmente, para completar las pruebas, se revisó el estado de Apache y vsftpd en el servidor, confirmando que los servicios estaban activos (running) y disponibles solamente por los puertos habilitados, demostrando la correcta segmentación y control de acceso implementado.

Figura 26. Verificación de que los servicios “Apache” y “vsftpd” estén activos para asegurarse de que el sistema esté funcionando correctamente y se eviten fallos futuros.



Fuente: Autoría Propia

Figura 27. Para controlar y regular el tráfico que circula entre las zonas de red (green, orange y red), y definir que zonas pueden conectarse entre sí.

Fuente: Autoría Propia

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

La implementación de un proxy HTTP no transparente permite ejercer un control preciso sobre la navegación web desde la red interna, utilizando autenticación por usuario y filtrado de contenido basado en perfiles. Este mecanismo fortalece la seguridad perimetral al permitir identificar a los usuarios, restringir el acceso a sitios no autorizados y registrar actividad de navegación.

7.1 PROCEDIMIENTO

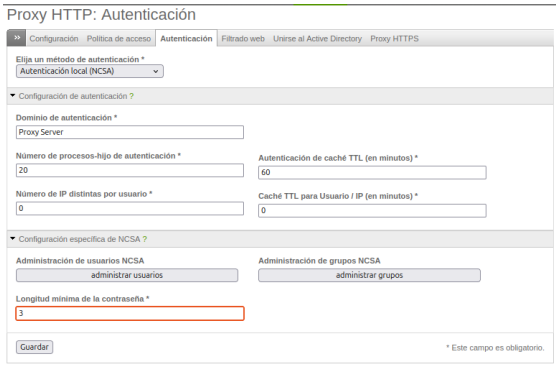
A través del uso de la interfaz de la herramienta Endian, se accede a la opción para configurar el proxy HTTP en modo no transparente, estableciendo un puerto dedicado para el servicio y algunas otras configuraciones opcionales.

Figura 28. Interfaz herramienta Endian Firewall para acceder a las diferentes opciones de configuración, para el caso: proxy.

Fuente: Autoría Propia

En el módulo de autenticación se definen los usuarios y el grupo de control, los cuales serán asociados a las políticas diferenciadas de acceso, definiendo características como el método de autenticación y la longitud de la contraseña para los usuarios.

Figura 29. Módulo de autenticación, para creación de usuarios y grupos y establecimiento de método de autenticación.



Fuente: Autoría Propia

Asimismo, accediendo en la opción “filtrado web”, se generan las opciones de configuración para la creación del perfil de filtrado que incluye una lista negra con los siguientes sitios web: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, a los cuales se registre el acceso por parte de los usuarios desde la red interna.

Figura 30. Módulo Filtrado web, donde se crea el perfil y se incluyen los sitos webs en la lista negra para que restringir su acceso.

Fuente: Autoría Propia

La configuración se culmina con su integración mediante una política de acceso del proxy, en la cual especifica que el tráfico proveniente de la LAN debe autenticarse y ser filtrado a través del perfil configurado.

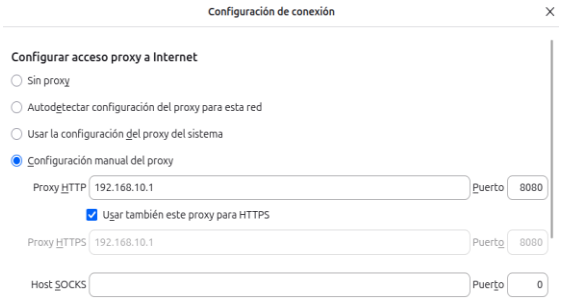
Figura 31. Política de acceso, se realiza la parametrización para la implementación de las configuraciones del perfil creado y de autenticación.

Fuente: Autoría Propia

Esta política garantiza que únicamente usuarios autorizados puedan navegar y que las restricciones definidas se apliquen de manera consistente.

Adicionalmente, para que el proxy no transparente funcione correctamente, es necesario configurar manualmente el proxy en el equipo cliente, estableciendo la dirección IP del firewall y el puerto configurado, lo que permite que el navegador solicite autenticación y aplique las restricciones configuradas en la política.

Figura 32. Configuración en el dispositivo cliente, del servidor que contine el proxy con la parametrización establecida.

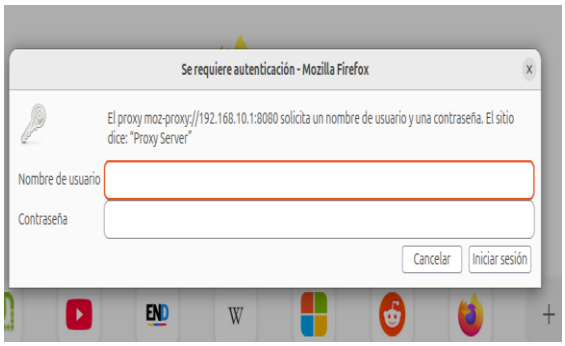


Fuente: Autoría Propia

7.2 RESULTADOS

Una vez aplicada la configuración en el equipo cliente de la LAN y al acceder al navegador web, el sistema solicita credenciales de autenticación antes de permitir cualquier navegación. Tras ingresar el usuario establecido en la configuración del proxy en Endian Firewall, se da ingreso al navegador y se verifica que los tres sitios incluidos en la lista negra fuesen efectivamente bloqueados por el proxy, presentando al usuario un mensaje de denegación.

Figura 33. Evidencia de la solicitud de autenticación en el navegador desde el equipo cliente.

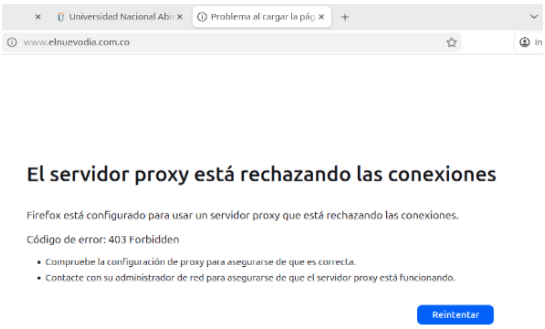


Fuente: Autoría Propia

En la anterior imagen se puede evidenciar la aplicación de las políticas establecidas en el proxy para la autenticación de usuarios al ingreso en el navegador del equipo cliente.

En la siguiente imagen se muestra el mensaje de restricción de acceso a los sitios web establecidos en la lista negra, cuando el usuario intenta ingresar a ellas.

Figura 34. Evidencia de la aplicación de restricción en el acceso al sitio www.elnuevodia.com.co.



Fuente: Autoría Propia

Por otro lado, los sitios no restringidos fueron accesibles sin limitaciones, lo que demuestra el correcto funcionamiento del perfil de filtrado y de la asociación entre usuario, grupo y política de acceso.

Figura 35. Evidencia de acceso a sitios web no incluido en la lista negra.

Fuente: Autoría Propia

Los resultados evidencian que la aplicación del proxy HTTP no transparente, proporciona un control eficiente sobre la navegación, permitiendo identificar al usuario que realiza cada solicitud y ejecutar políticas diferenciadas según grupos u horarios de acuerdo con los objetivos y necesidades planteadas.

La implementación de listas negras asegura el bloqueo efectivo de contenido no autorizado, mientras que el requerimiento de autenticación impide el uso anónimo del servicio de navegación.

Esta configuración mejora significativamente la supervisión del tráfico web en la red LAN y constituye una práctica fundamental en redes corporativas y educativas que buscan aplicar restricciones de acceso alineadas con políticas institucionales.

8 CONCLUSIONES

La configuración inicial del Endian y la segmentación de las zonas verde y naranja me permitió dejar un enrutamiento funcional para que mis compañeros continúen con la siguiente etapa. Logré establecer comunicación entre las máquinas y validar que las direcciones IP y las interfaces quedaran correctamente configuradas. Esta parte del trabajo demuestra lo importante que es organizar bien la red desde el inicio, ya que sobre esta base se montarán los servicios y reglas que siguen en el proyecto.

La implementación de NAT dentro de una arquitectura segmentada demuestra ser un componente indispensable para garantizar tanto la conectividad como la seguridad perimetral. La correcta aplicación del mecanismo MASQUERADE en el firewall Endian permitió que los equipos ubicados en la zona DMZ accedieran a recursos externos sin comprometer la integridad de la red interna. Esta funcionalidad no solo posibilita la optimización del uso de direcciones IP, sino que también ofrece un nivel adicional de protección al ocultar la estructura real de la infraestructura.

La implementación de políticas de seguridad en Endian Firewall permitió reforzar el control de tráfico entre la zona LAN y la DMZ, garantizando que solo los servicios necesarios estuvieran disponibles. La habilitación de HTTP y FTP permitió mantener la funcionalidad requerida por el servidor de la DMZ, mientras que el bloqueo del protocolo ICMP redujo la posibilidad de reconocimiento de red por parte de usuarios no autorizados. El análisis de los registros confirmó la efectividad de las configuraciones aplicadas, evidenciando el papel crítico del firewall como componente de seguridad en arquitecturas de red segmentadas.

La implementación de un proxy permite controlar el uso del servicio de internet con el fin de reducir los riesgos a través de este y generar estadísticas de uso de los usuarios, lo que se traduce en mejores políticas para su utilización.

Por otra parte, la configuración de las reglas de acceso permitió que solo el tráfico autorizado pudiera pasar entre las diferentes zonas (verde, naranja y roja). Las pruebas mostraron que los servicios de la DMZ (servidor) funcionaban correctamente y que la red interna estaba protegida.

9 REFERENCIAS

[1] A. Tanenbaum y D. Wetherall, *Redes de Computadores*. Prentice Hall, 2011.

[2] Canonical, *Netplan Configuration Documentation*. Disponible en: https://netplan.io.

[3] Endian, *Endian UTM 3.2 Reference Manual*. Disponible en: https://docs.endian.com/3.2/utm/index.html.

[4] Endian Firewall, *Community Documentation*. Disponible en: https://www.endian.com/community.

[5] IETF, *RFC 792 – Internet Control Message Protocol (ICMP)*.

[6] InfoRed, "Cómo configurar reglas DNAT en Endian Firewall," 2019. Disponible en: https://www.youtube.com/watch?v=0OEPkMhFrhA.

[7] LPI, *LPIC-1 Exam 101. Tema 102: Comandos GNU y Unix*, 2022. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/.

[8] Squid Project, *Squid: Caching proxy for the web – Official documentation*, 2024. Disponible en: https://www.squid-cache.org/Doc/.

[9] W. Stallings, *Seguridad en Redes*. Pearson, 2017.