SEGMENTACIÓN DE RED Y CONTROL DE TRÁFICO CON ENDIAN: UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL GNU/LINUX EN ENTORNOS VIRTUALES

Cristian Camilo Acero Criales
e-mail: cricaacero01@gmail.com
Hector Alonso Ortiz
e-mail: haortizo@gmail.com
Yefrey Ardila Saldaña
e-mail: yardilasal@unadvirtual.edu.co
Sebastian Vidal Aragón
e-mail: Scvidala@unadvirtual.edu.co
Jhon Alexander Orozco Agudelo
e-mail: dialmi592009@gmail.com

RESUMEN: *Este artículo presenta la implementación de una solución de seguridad perimetral mediante el uso de software libre, específicamente la distribución GNU/Linux Endian Firewall. Utilizando un entorno virtualizado con Oracle VirtualBox, se abordaron cinco temáticas fundamentales para la protección de redes: segmentación mediante zonas LAN, WAN y DMZ, configuración de reglas NAT, permisos de servicios desde la DMZ, filtrado de tráfico interzonas y aplicación de proxy con autenticación. Se diseñó una infraestructura de red con distintas subredes y máscaras, garantizando el aislamiento y control del tráfico entre dispositivos y servicios. El trabajo se desarrolló colaborativamente, permitiendo que cada integrante abordara una temática específica, fortaleciendo el aprendizaje práctico sobre herramientas y conceptos de ciberseguridad en entornos GNU/Linux. Los resultados evidencian una implementación correcta de las políticas de control y segmentación de red en un entorno simulado seguro y funcional.*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, seguridad perimetral, puertos.

1 INTRODUCCIÓN

En el contexto actual de las redes empresariales y académicas, la seguridad perimetral se ha convertido en un componente esencial para la protección de la información y la continuidad del servicio. Las amenazas, tanto externas como internas, obligan a las organizaciones a implementar esquemas de defensa que permitan controlar el flujo de datos y segmentar adecuadamente los entornos de red. En este sentido, el uso de soluciones basadas en software libre, como la distribución GNU/Linux Endian Firewall (EFW), ofrece herramientas robustas y accesibles para construir arquitecturas de seguridad eficientes.

Este trabajo se centra en la configuración inicial de Endian Firewall dentro de un entorno virtualizado con Oracle VirtualBox, abordando especialmente la asignación de tarjetas de red para implementar la zona verde (LAN), la zona roja (WAN) y la zona naranja (DMZ). Esta segmentación permite establecer límites claros entre los equipos de usuarios internos, el acceso externo a Internet y los servidores críticos, mejorando significativamente la capacidad de defensa de la infraestructura. La correcta definición de estas zonas es esencial para garantizar el control del tráfico y la protección de los servicios expuestos, especialmente aquellos que operan en la zona desmilitarizada.

2 IMPLEMENTACIÓN DE LA CONFIGURACIÓN

La solución de seguridad perimetral propuesta fue implementada mediante el uso de la distribución GNU/Linux Endian Firewall (EFW) dentro de un entorno virtualizado con Oracle VirtualBox. Esto permitió configurar una infraestructura de red segmentada, segura y funcional, con zonas bien definidas según los distintos propósitos de la red: usuarios finales, servicios expuestos y conexión a Internet. A continuación, se describen los pasos realizados para configurar el sistema base sobre el cual se desarrollan todas las temáticas del proyecto.

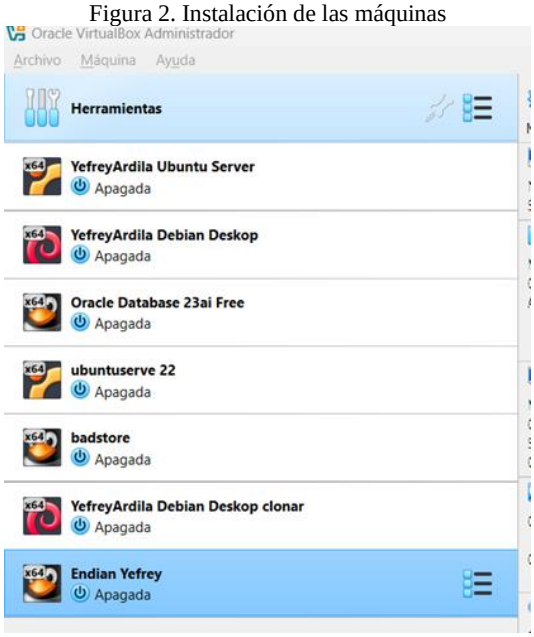
2.1 PREPARACIÓN DEL ENTORNO DE VISUALIZACIÓN

Para iniciar el proceso, se creó una máquina virtual en Oracle VM VirtualBox con las siguientes características:

- Tipo de sistema operativo: Linux
- Versión: Other Linux (64-bits)
- Memoria RAM asignada: 1024 MB
- Disco duro: 8 GB de almacenamiento dinámico
- Adaptadores de red: 3 interfaces (NAT, red interna, adaptador solo-anfitrión)

Endian es una solución de firewall y gateway que facilita la administración segura de redes [2], ofreciendo funcionalidades como filtrado de contenido, VPN, protección contra intrusos y gestión de ancho de banda. En este caso, su función principal es intermediar entre las máquinas Cliente y Servidor, asegurando una comunicación fluida y segura, además de controlar el tráfico entrante y saliente hacia Internet.

Figura 2. Instalación de las máquinas



Fuente: Autoría propia

2.2 CONFIGURACIÓN DE LAS TARJETAS DE RED

Endian requiere tres interfaces para funcionar correctamente bajo el esquema clásico de zonas. Estas fueron configuradas de la siguiente manera en VirtualBox:

- Adaptador 1 – Zona Roja (WAN)
  Modo de conexión: NAT o Adaptador puente
  Función: Simula la conexión a Internet.
  Objetivo: Proveer acceso a la WAN desde la red interna bajo reglas controladas.

- Adaptador 2 – Zona Verde (LAN)
  Modo de conexión: red interna (“verde”)
  Función: Red de estaciones cliente que se comunican entre sí y acceden a servicios.
  Objetivo: Simular una red segura para los usuarios finales.

- Adaptador 3 – Zona Naranja (DMZ)
  Modo de conexión: Red interna (“naranja”)
  Función: Aislar servidores como Web o Bases de Datos accesibles desde la WAN o LAN.
  Objetivo: Crear una red semisegura con acceso limitado desde zonas externas e internas.

Cada adaptador fue habilitado y configurado desde la sección "Configuración > Red" en VirtualBox, seleccionando el nombre del adaptador correspondiente según su propósito.

2.3 CONFIGURACIÓN DE LAS ZONAS ENDIAN

A continuación, se detallan las direcciones IP utilizadas y los propósitos de cada zona:

Figura 3. Configuración IP

Zona	Interfaz VirtualBox	Dirección IP Asignada	Descripción
Verde	Adaptador 1	192.168.2.15	Red LAN interna (estaciones)
Roja	Adaptador 3	DHCP (NAT o Adaptador Puente)	Salida a Internet (WAN)
Naranja	Adaptador 2	192.168.1.15	Servidores Web y BD (DMZ)

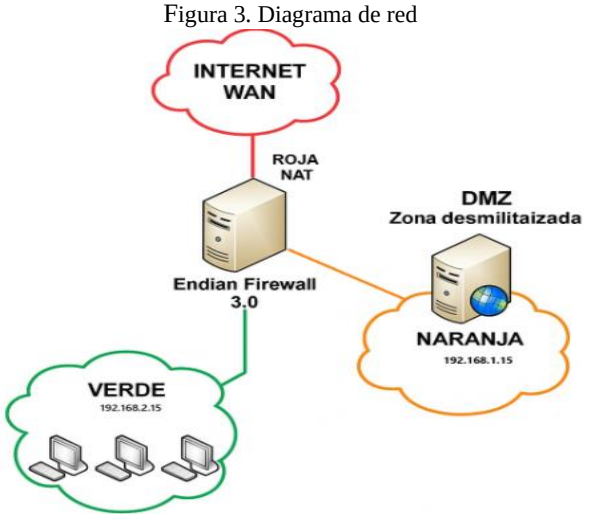
Fuente: Autoría propia

En la interfaz web se asignaron correctamente estas zonas, permitiendo el ruteo interno y la posterior configuración de reglas de seguridad.

2.4 DIAGRAMA DE RED

La arquitectura de red implementada se ilustra en la figura 3, donde se muestra la conexión entre las tres zonas principales: LAN (verde), WAN (roja) y DMZ (naranja). Endian se posiciona como el nodo central que controla el tráfico entre estas zonas, actuando como punto de enlace, inspección y enrutamiento.

Figura 3. Diagrama de red

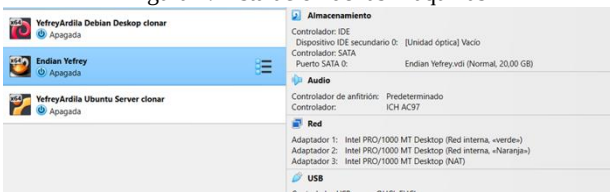


Fuente: Autoría propia.

2.5 INSTALACIÓN DE LAS MÁQUINAS VIRTUALES

Posterior a la configuración inicial de la máquina, se procede a su ejecución. Para ello, fue necesario instalar y configurar las máquinas correspondientes al **Cliente**, al **Servidor** y a **Endian**, esta última actuando como un puente para gestionar las conexiones y permitir el acceso a Internet.

Figura 4. Instalación de las Máquinas



Fuente: Autoría propia

Máquina Cliente.

- Sistema operativo: Ubuntu Desktop / Windows (según el entorno de pruebas). [1]
- Dirección IP asignada de forma estática o dinámica, según la configuración de red.
- Configuración de puerta de enlace apuntando a Endian para gestionar el tráfico.

Máquina Servidor:

- Sistema operativo: Ubuntu Server / Windows Server.
- Servicios habilitados: servidor web (Apache o Nginx), base de datos (MySQL o PostgreSQL), y cualquier aplicación necesaria para las pruebas.
- Configuración de red que permita el enrutamiento a través de Endian.

Máquina Endian:

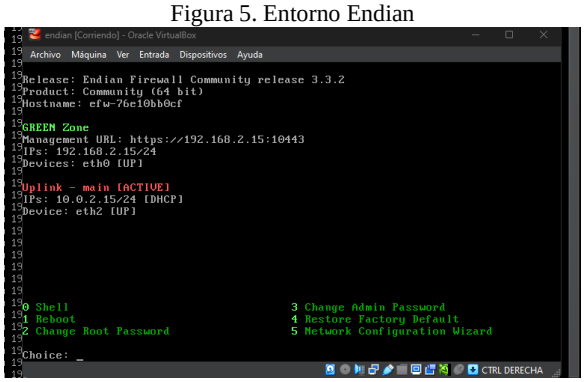
- Endian es configurada para actuar como un firewall y gateway, permitiendo el filtrado de tráfico y el acceso seguro a Internet.
- Se instalan **adaptadores de puente (Bridge Adapters)**, los cuales son necesarios para conectar las interfaces de red de Endian con las máquinas Cliente y Servidor.
- Los adaptadores de puente permiten que Endian gestione el tráfico entrante y saliente, filtrando contenido y aplicando políticas de seguridad.

2.6 INSTALACIÓN DE ENDIAN FIREWALL

La instalación de Endian se realizó seleccionando el disco virtual creado previamente y siguiendo el asistente interactivo [2]:

1. Selección del idioma, zona horaria y diseño de teclado.
2. Configuración de las interfaces de red.
3. Definición de contraseñas y nombre del host.
4. Finalización del proceso e inicio del sistema.

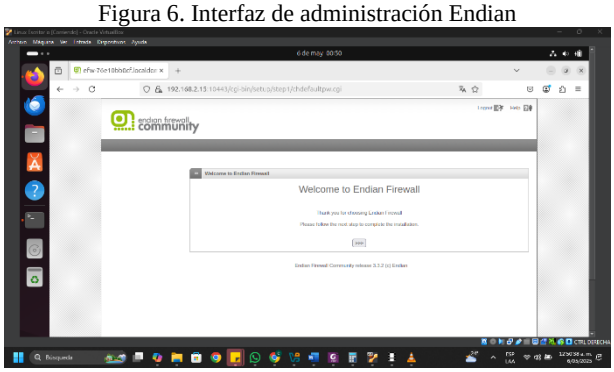
Figura 5. Entorno Endian



Fuente: Autoría propia

Al finalizar la instalación, se accedió a la interfaz web de administración desde una estación conectada a la zona verde mediante la URL: https://192.168.2.15

Figura 6. Interfaz de administración Endian



Fuente: Autoría propia.

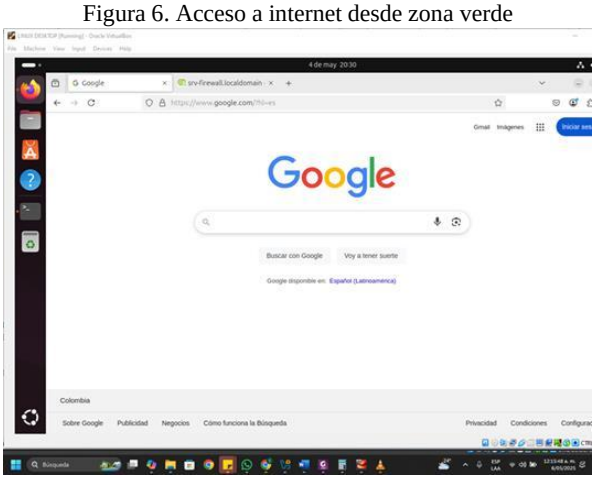
Por medio de esta interfaz realizamos las configuraciones que necesitamos para habilitar la zona naranja para nuestro servidor.

2.7 VERIFICACIÓN DE CONECTIVIDAD ENTRE ZONAS

Se validó la segmentación mediante pruebas de ping y navegación entre estaciones:

Desde el Desktop (zona verde) se accedió exitosamente a la web de administración de Endian y además a una página de internet.

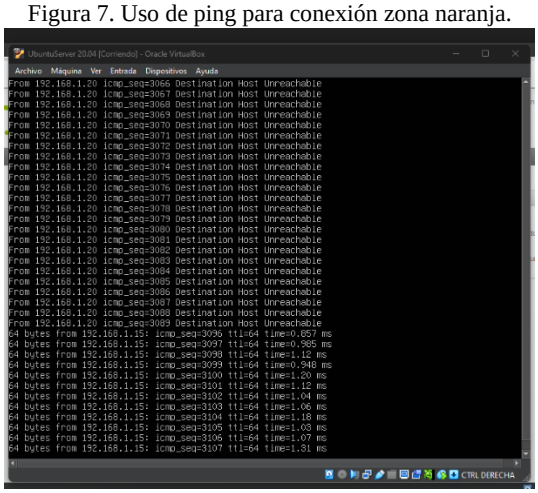
Figura 6. Acceso a internet desde zona verde



Fuente: Autoría propia.

El servidor (zona naranja) respondió a peticiones desde la LAN.

Figura 7. Uso de ping para conexión zona naranja.



Fuente: Autoría propia.

2.8 RESULTADOS

La configuración inicial de GNU/Linux Endian en un entorno virtualizado permitió simular de forma efectiva una arquitectura de red segura compuesta por tres zonas diferenciadas: zona verde (LAN), zona roja (WAN) y zona naranja (DMZ). Esta segmentación facilitó la validación de múltiples escenarios de seguridad perimetral, los cuales servirán como base para las siguientes temáticas del proyecto.

Durante el proceso de implementación, se evidenció que VirtualBox proporciona un entorno flexible para el manejo de múltiples interfaces de red. [4] La asignación de cada adaptador a una zona específica, con direcciones IP independientes y aisladas, permitió establecer límites funcionales entre las áreas de la red y controlar el flujo de tráfico mediante pruebas de conectividad.

Para complementar la infraestructura y validar la segmentación de red, se crearon dos máquinas virtuales adicionales:

- Una estación de trabajo con GNU/Linux Desktop, conectada a la zona verde, para simular el comportamiento de un cliente en la LAN.
- Un servidor con GNU/Linux Server, conectado a la zona naranja [3][4], destinado a alojar servicios (web, base de datos, FTP) en la DMZ.

Los resultados obtenidos demostraron que:

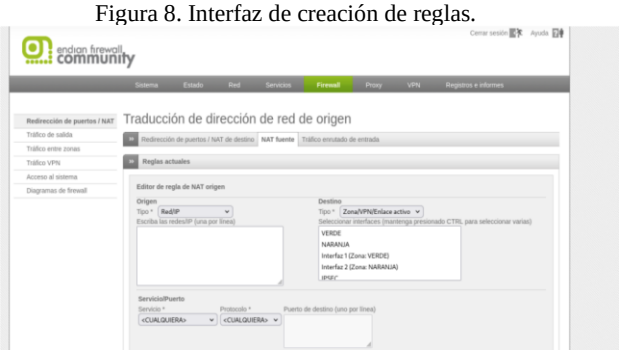
- La zona verde tuvo acceso correcto a la interfaz web de administración de Endian.
- Las direcciones IP asignadas a cada zona fueron reconocidas sin conflictos.
- Fue posible realizar pruebas de conexión (ping, navegador web) entre estaciones de las distintas zonas, validando la segmentación y aislamiento entre redes.

3 CONFIGURACIÓN NAT

Para garantizar el correcto funcionamiento de la red y el acceso seguro a Internet, es necesario proceder con la configuración de reglas de NAT (Network Address Translation) o Traducción de Direcciones de Red. Este proceso permite que las direcciones IP privadas de la red local (LAN) y de la Zona Desmilitarizada (DMZ) se traduzcan en una dirección IP pública, facilitando así la comunicación con la red externa (WAN).

En primer lugar, se configura la regla de NAT para permitir el tráfico desde la LAN hacia la WAN, demostrando de esta forma el establecimiento exitoso de comunicación con Internet. Esta configuración se realiza desde el panel de administración gráfica de Endian, en el módulo correspondiente a reenvío de puertos (Port Forwarding) y NAT. En este espacio, se especifican los puertos de origen, los puertos de destino y la dirección IP interna que se traducirá para interactuar con la red pública.

Figura 8. Interfaz de creación de reglas.



Fuente: Autoría propia.

Simultáneamente, se procede con la configuración de una segunda regla de NAT para permitir el tráfico desde la zona DMZ hacia Internet. La DMZ es un segmento de red que proporciona una capa adicional de seguridad, permitiendo la exposición de servicios hacia el exterior sin comprometer la red interna. En este caso, se configura un reenvío de puertos específico para los servicios que se desean publicar en la red pública, asegurando su accesibilidad desde el exterior.

Para facilitar la gestión y el orden en la configuración, ambas reglas se añaden de manera simultánea en el mismo módulo del entorno gráfico, simplificando el proceso de validación y monitoreo. Finalmente, se procede con la validación de las conexiones y permisos en cada segmento de red:

Figura 9. Configuración de reglas

Fuente: Autoría propia

Una vez configurada la traducción de direcciones (NAT) y verificadas las conexiones básicas hacia Internet y la DMZ, se procede a la activación de las conexiones internas entre el Servidor y el Cliente. Este paso es fundamental para permitir la comunicación fluida y segura dentro de la red local, garantizando que ambos dispositivos puedan intercambiar información de manera efectiva.

Para ello, se añaden reglas específicas en Endian que controlan el tráfico entre las zonas:

- Zona Naranja (DMZ): En esta área se ubica el servidor, expuesto parcialmente para brindar servicios externos, pero con restricciones de seguridad para evitar accesos no autorizados.
- Zona Verde (LAN): Esta área corresponde a los dispositivos de la red interna, como el Cliente, con acceso seguro y controlado.

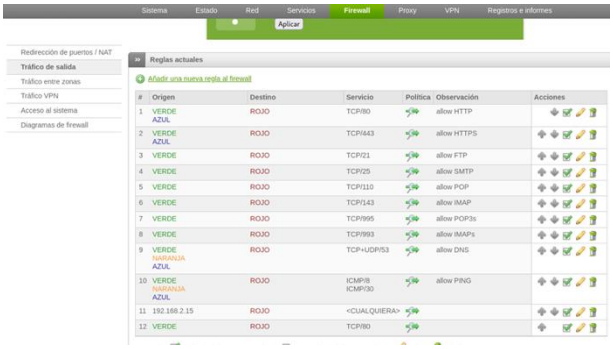
Reglas para la Zona Naranja (DMZ):

- Se configuran reglas que permitan el acceso del Cliente al Servidor utilizando puertos específicos para servicios como HTTP, HTTPS, SSH y otros necesarios para la interacción.
- Se habilita el tráfico saliente del Servidor hacia Internet y hacia la LAN, siempre y cuando esté autorizado por las políticas de seguridad establecidas.

Reglas para la Zona Verde (LAN):

- Se añaden reglas que permitan al Cliente comunicarse de manera directa con el Servidor en la DMZ.
- Se habilitan puertos para pruebas de conectividad (ping, traceroute) y para servicios compartidos como carpetas en red o bases de datos.
- Adicionalmente, se configuran políticas de salida hacia Internet, permitiendo la navegación y el acceso a servicios externos de manera controlada.

Figura 10. Reglas de Salida del Firewall



Fuente: Autoría propia

Una vez finalizada la configuración de las reglas de NAT y la activación de las conexiones internas entre las zonas Naranja (DMZ) y Verde (LAN), se procedió a la validación de la conectividad general de la red. Durante este proceso, se verificó que tanto el Cliente como el Servidor tenían acceso correcto y fluido a Internet, permitiendo realizar pruebas de navegación y acceso a servicios en la red externa (WAN) sin interrupciones.

Figura 11. Prueba de conexión a internet

Fuente: Autoría propia

La configuración de NAT, junto con las reglas de reenvío de puertos y las políticas de seguridad aplicadas en Endian, facilitó el enrutamiento adecuado del tráfico desde las redes internas hacia Internet. Esto permitió que los dispositivos conectados en la red privada pudieran comunicarse con servidores externos, realizar descargas, acceder a servicios en la nube y ejecutar pruebas de conectividad (ping y traceroute) con resultados satisfactorios.

Además, se comprobó que los permisos de salida establecidos en las reglas de firewall estaban funcionando correctamente, garantizando un tráfico controlado y seguro. Las restricciones aplicadas evitaron accesos no autorizados y permitieron únicamente aquellas conexiones que cumplían con los criterios de seguridad definidos. Como resultado, la red se encuentra operativa y con acceso estable a Internet, cumpliendo los objetivos planteados en la configuración inicial.

4 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

En entornos de red donde la seguridad y el control de los servicios son esenciales, implementar una zona desmilitarizada (DMZ) se vuelve una estrategia clave. La DMZ permite alojar servicios accesibles desde el exterior, como servidores web o de correo, sin poner en riesgo directamente la red interna. En este sentido, utilizar Endian Firewall como solución de seguridad ayuda a gestionar de manera efectiva el tráfico entre la red externa, la DMZ y la red interna. Para lograr esto, se utilizan sistemas operativos como Ubuntu Server para desplegar servicios en la DMZ y Ubuntu Desktop como estación de administración o cliente de pruebas. Este tema explora cómo permitir y controlar los servicios dentro de la zona DMZ, asegurando tanto el acceso legítimo como la protección de los recursos internos de la red.

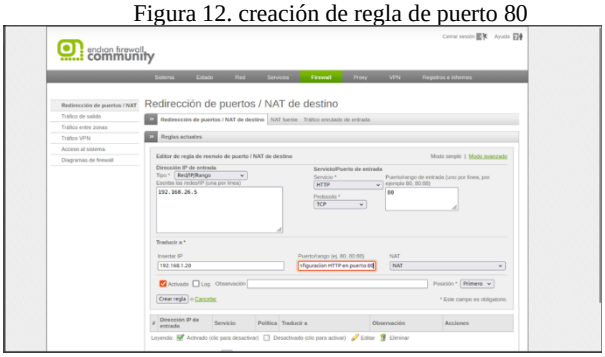
4.1 CONFIGURACIÓN DE PUERTO 80 PARA HTTP Y PUERTO 21 PARA FTP

En esta actividad se configuró la zona DMZ mediante la interfaz web de Endian Firewall, accedida desde un equipo con Ubuntu Desktop. Se permitieron los puertos 80 (HTTP) y 21 (FTP) para habilitar el acceso a servicios web y de transferencia de archivos alojados en un servidor con Ubuntu Server. Esta configuración permitió verificar la correcta publicación de los servicios hacia el exterior, manteniendo protegida la red interna.

- Creación de una regla en Endian para el servicio HTTP en el puerto 80.

Desde el navegador en Ubuntu Desktop, se accedió a la interfaz web de Endian Firewall para configurar el acceso al servicio HTTP. Se creó una regla de firewall que permite el tráfico entrante al puerto 80, que está asignado al servicio web, redirigiéndolo hacia la dirección IP del servidor en la zona DMZ, donde se ejecuta Ubuntu Server. Esta configuración permite que los usuarios externos accedan al sitio web alojado en ese servidor, sin poner en riesgo la seguridad de la red interna.

Figura 12. creación de regla de puerto 80

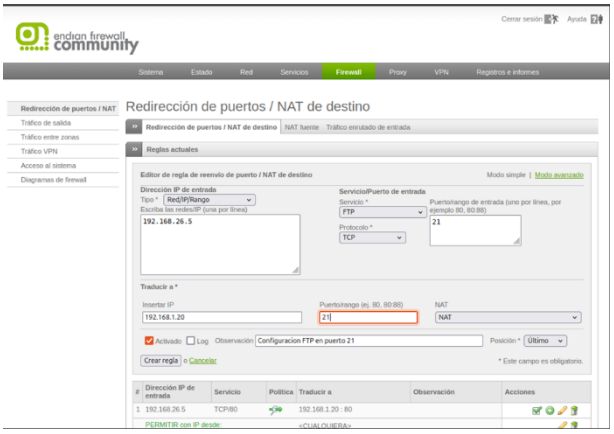


Fuente: Autoría propia

- Creación de una regla en Endian para el servicio FTP en el puerto 21.

La configuración del puerto 21 para el servicio FTP se llevó a cabo a través de la interfaz web de Endian Firewall, utilizando un navegador en Ubuntu Desktop. El objetivo era permitir que usuarios externos accedieran al servidor FTP ubicado en la zona DMZ, sin poner en riesgo la red interna. Para lograr esto, se creó una regla en el firewall de Endian que permite el tráfico entrante al puerto 21 (protocolo TCP), que es el puerto estándar para el servicio FTP. Esta regla redirige el tráfico a la dirección IP interna del servidor con Ubuntu Server, donde se ha instalado y configurado el servicio FTP. Con esta configuración, los clientes externos pueden conectarse al servidor FTP de manera segura, mientras que Endian controla el flujo de datos entre las diferentes zonas de la red.

Figura 13. creación de regla de puerto 21



Fuente: Autoría propia

4.2 DENEGACIÓN DEL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA BLOQUEAR EL USO DE PING EN LA RED.

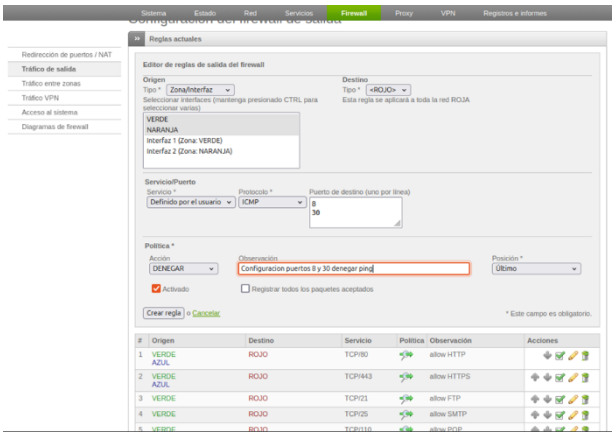
Para mejorar la seguridad de la red, se procedió a denegar el protocolo ICMP en los puertos 8 y 30, con el objetivo de bloquear el uso del comando ping desde redes externas. Esto impide que dispositivos fuera de la red local puedan hacer una consulta de disponibilidad a través de ICMP, dificultando la detección de dispositivos dentro de la red. La configuración de este bloqueo se realizó en el firewall, especificando las reglas para denegar el tráfico ICMP en los puertos mencionados.

Una vez implementada la regla, se probó la no respuesta al comando ping hacia una dirección IP de la red utilizando una consola o terminal. Al realizar el ping, se verificó que no se recibió respuesta, lo que confirmó que la regla estaba funcionando correctamente. Además, se inspeccionó el tráfico de salida para verificar que las reglas de firewall se habían creado correctamente y estaban siendo aplicadas, asegurando que el tráfico ICMP no saliera ni entrara desde la red.

- creación de regla para los puertos 8 y 30 en el firewall

Se procedió a la creación de una regla en el firewall para bloquear el tráfico en los puertos 8 y 30, correspondientes al protocolo ICMP. Esta configuración tiene como objetivo impedir el uso de herramientas como ping en la red, aumentando así la seguridad al evitar la detección de dispositivos internos. La regla fue aplicada correctamente, y se verificó que el tráfico en estos puertos estaba siendo denegado según lo esperado.

Figura 14. creación de regla de puertos 8 y 30

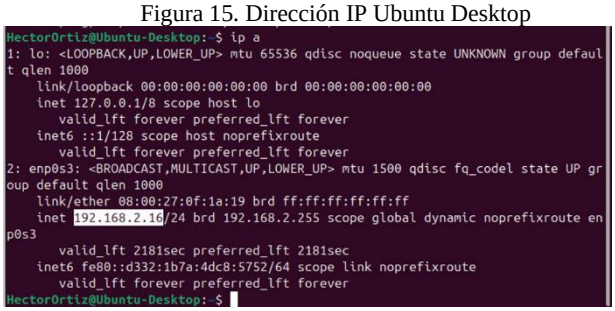


Fuente: Autoría propia

- prueba de negación de ping en la red mediante bloqueo de ICMP

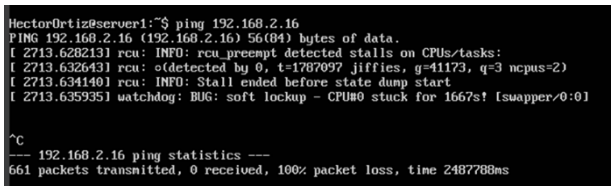
Se llevó a cabo una prueba de negación de ping en la red bloqueando el protocolo ICMP. Para esto, se configuró una regla en el firewall que impide el tráfico en los puertos 8 y 30. La prueba consistió en intentar hacer un ping desde un servidor con Ubuntu Server hacia la dirección IP de un equipo con Ubuntu Desktop. Al ejecutar el comando ping, no se recibió respuesta, lo que confirmó que la regla de bloqueo estaba funcionando como se esperaba. Esto demostró que la configuración del firewall estaba evitando la comunicación ICMP entre los dispositivos en la red.

Figura 15. Dirección IP Ubuntu Desktop



Fuente: Autoría propia

Figura 16. Prueba de ping desde Ubuntu Server



Fuente: Autoría propia

5 CONFIGURACIÓN DE REGLAS DE ACCESO ENTRE ZONAS

La configuración de reglas de acceso entre zonas constituye un pilar fundamental para el aseguramiento del tráfico dentro de una red segmentada. En esta temática se implementaron reglas específicas en el cortafuegos Endian con el objetivo de controlar el tráfico permitido y denegado entre la zona verde (LAN), la zona naranja (DMZ) y la zona roja (WAN).

5.1 ACCESO DE LA ZONA VERDE A LA ZONA NARANJA MEDIANTE HTTP Y FTP

Inicialmente, se accedió a la interfaz de administración web de Endian y se dirigió al módulo "Firewall" > "Inter-Zone Firewall Configuration". Desde allí, se creó una regla que permitiera a la zona verde (estaciones de trabajo LAN) comunicarse con la zona naranja (servidor en la DMZ) a través de los servicios HTTP (puerto 80) y FTP (puerto 21). Para cada protocolo se configuró una regla independiente, especificando el origen, destino, servicio y acción permitida. Esta configuración permitió a los usuarios de la LAN acceder al contenido web y recursos compartidos ubicados en la zona DMZ.

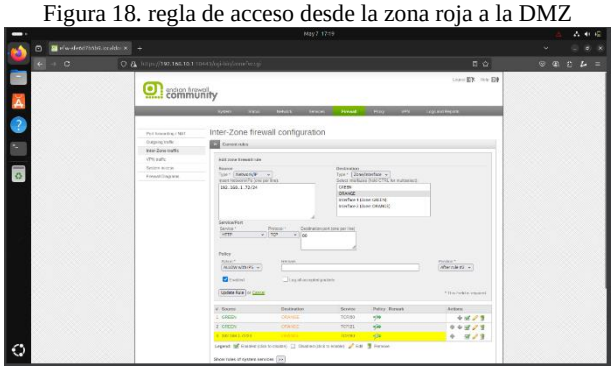
Figura 17. Reglas creadas para HTTP y FTP entre zona verde y naranja

Fuente: Autoría propia

5.2 HABILITACIÓN DEL TRAFICO DESDE LA ZONA WAN HACIA LA ZONA DMZB

Posteriormente, se configuró una regla adicional para permitir que dispositivos ubicados en la zona roja (Internet) pudieran acceder a los servicios publicados en la zona naranja, simulando un escenario real en el que servidores web o FTP se encuentran disponibles al público externo. Esta regla fue esencial para garantizar la exposición controlada de servicios, sin comprometer la integridad de la red interna.

Figura 18. regla de acceso desde la zona roja a la DMZ



Fuente: Autoría propia

5.3 REVISIÓN DE REGLAS EN EL TRAFICO INTER-ZONA.

Una vez creadas las reglas, se revisaron dentro del panel de configuración inter-zonal para confirmar su correcta aplicación. Las reglas aparecieron reflejadas en la interfaz web con su dirección de tráfico, servicio, protocolo, puerto, y estado de activación. Esta revisión permitió asegurar que las políticas estaban en funcionamiento y que los filtros aplicaban según el diseño planeado.

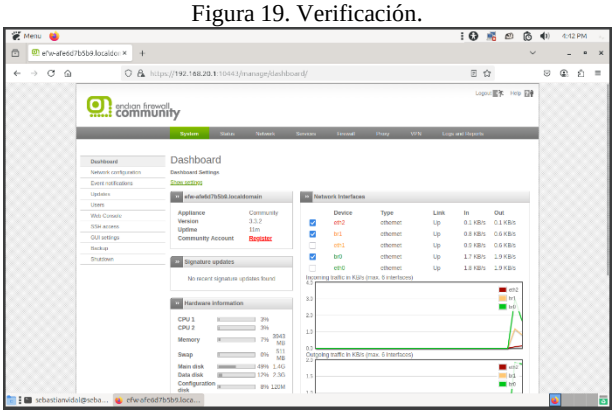
5.4 PRUEBAS FUNCIONALES DESDE CLIENTE Y SERVIDOR

Para validar la implementación, se utilizaron navegadores y herramientas de línea de comandos en las máquinas virtuales de cliente (zona verde), servidor (DMZ) y un host simulado como zona roja. Se ejecutaron las siguientes pruebas de acceso:

- HTTP desde la zona verde a la zona naranja: acceso exitoso al sitio web del servidor DMZ.
- HTTP desde la zona verde a la zona roja: acceso permitido a sitios públicos.
- HTTP desde la zona naranja a la zona roja: navegación hacia internet desde el servidor DMZ.
- HTTP desde la zona roja a la zona naranja: acceso al servidor web publicado.
- FTP desde la zona verde a la zona roja: conexión y transferencia FTP desde clientes LAN hacia un servidor FTP externo.
- FTP desde la zona roja a la zona naranja: prueba de acceso FTP entrante al servidor DMZ desde internet.

Todas las pruebas dieron resultados positivos, confirmando la efectividad de las reglas configuradas.

Figura 19. Verificación.



Fuente: Autoría propia

5.5 RESULTADOS

La implementación de las reglas de acceso entre zonas permitió evidenciar el correcto funcionamiento del sistema de filtrado de tráfico de Endian Firewall en un entorno segmentado. Las reglas fueron diseñadas para controlar con precisión el comportamiento del tráfico entre la zona LAN (verde), la DMZ (naranja) y la red externa (roja), cumpliendo con los requerimientos definidos para esta temática.

En primer lugar, se validó la conectividad entre la zona verde y la zona naranja utilizando los protocolos HTTP y FTP. Desde una estación de trabajo ubicada en la zona LAN, se accedió al servidor DMZ a través de un navegador web, visualizando correctamente el contenido web alojado. De forma paralela, se realizó una conexión FTP utilizando un cliente gráfico y también mediante línea de comandos (ftp), logrando la autenticación y transferencia de archivos. Esto demostró que las reglas configuradas permitieron el paso del tráfico deseado desde LAN hacia DMZ de forma selectiva, sin exponer otros servicios ni protocolos.

En segundo lugar, se configuró una regla de entrada desde la zona roja hacia la zona naranja, permitiendo la exposición pública del servidor DMZ. Desde un navegador ubicado en una máquina configurada como cliente externo (Internet), se accedió correctamente a la dirección IP del servidor en la DMZ. Esto simula un entorno de publicación real de servicios web, en donde los usuarios externos pueden acceder a recursos internos controlados sin comprometer la red local.

Durante la revisión de las reglas interzonales desde la interfaz web de Endian, se constató que todas las políticas creadas estaban activas, correctamente documentadas y reflejadas con sus respectivos servicios, puertos y protocolos. Esta visibilidad facilitó la auditoría del tráfico permitido y la trazabilidad de posibles accesos indebidos. Se confirmó además que las políticas por defecto de Endian bloqueaban cualquier tráfico no autorizado entre zonas, brindando una capa adicional de seguridad.

Posteriormente, se realizaron pruebas combinadas desde distintos puntos de la red. Cada prueba fue validada tanto con herramientas gráficas como mediante comandos (wget, curl, ftp, ping, netstat), lo cual permitió confirmar el funcionamiento del firewall desde distintos niveles. Además, se observó que cualquier intento de acceso no autorizado fuera del rango permitido fue rechazado por la política de denegación implícita.

La correcta segmentación de la red y la creación controlada de reglas evitaron fugas de información, permitieron un monitoreo claro del tráfico y establecieron una base sólida para continuar con políticas más avanzadas de inspección, NAT, o control de contenido.

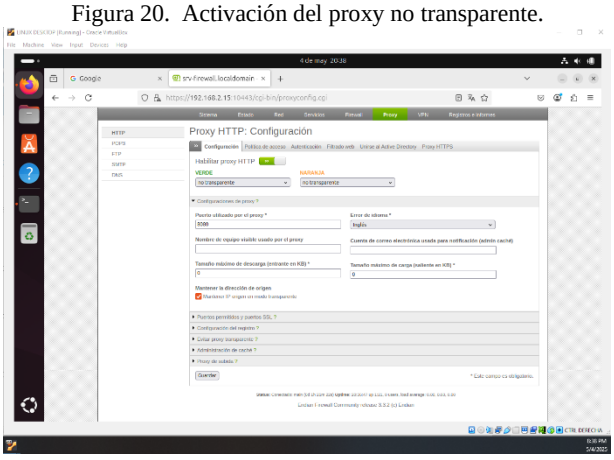
6 IMPLEMENTACIÓN DE UN PROXY HTTP CON AUTENTICACIÓN Y POLÍTICAS DE FILTRADO.

El control del acceso a contenidos web en una red corporativa o educativa es una de las funciones clave en los sistemas de seguridad perimetral. En esta temática se implementó un Proxy HTTP no transparente con políticas de autenticación y filtrado de contenido en la distribución GNU/Linux Endian Firewall, permitiendo regular el acceso a Internet desde la zona verde (LAN).

6.1 ACTIVACIÓN DEL PROXY HTTP NO TRANSPARENTE

Desde la interfaz de administración de Endian, se accedió a la sección Proxy → HTTP. Allí se activó la opción de proxy no transparente, lo cual obliga a los clientes a configurar manualmente el proxy en sus navegadores y autenticarse para acceder a la web. Esta modalidad otorga mayor control y permite aplicar políticas diferenciadas por usuario o grupo.

Figura 20. Activación del proxy no transparente.



Fuente: Autoría propia

6.2 CREACIÓN DEL PERFIL DE FILTRADO CON LISTA NEGRA

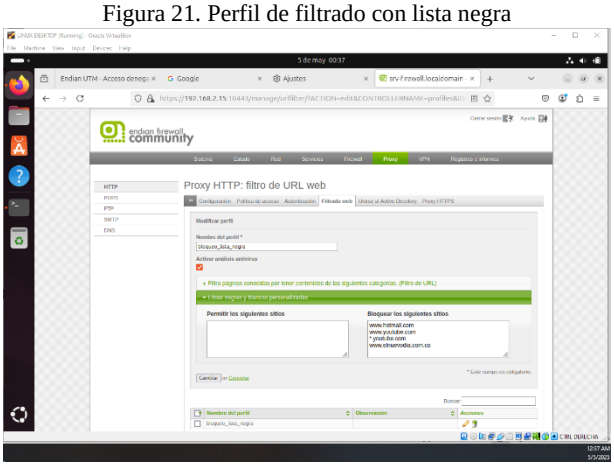
Se creó un nuevo perfil de filtrado mediante la ruta Proxy → HTTP → Filtrado Web → Añadir nuevo perfil. A este perfil se le asignó el nombre bloqueo_lista_negra. En la sección

correspondiente se ingresaron los siguientes dominios para su restricción:

- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co

Este perfil representa una política de denegación explícita de acceso a sitios considerados improductivos o no autorizados para el entorno de red.

Figura 21. Perfil de filtrado con lista negra



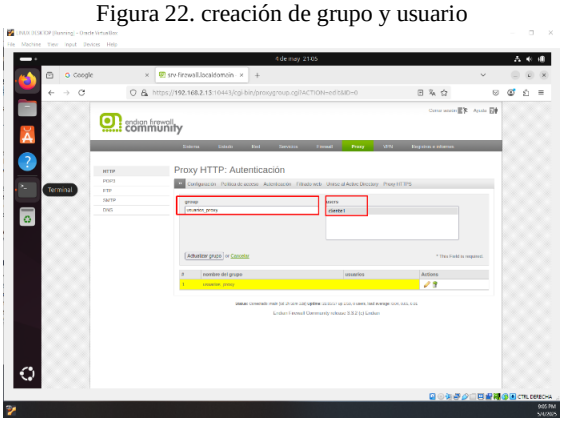
Fuente: Autoría propia

6.3 CONFIGURACIÓN DE AUTENTICACIÓN POR USUARIO

Para aplicar las políticas de filtrado por identidad, se habilitó el módulo de autenticación en el proxy. Se accedió a la ruta Proxy → Autenticación → Administrar grupos, donde se creó un grupo con nombre representativo.

Luego, desde Proxy → Autenticación → Administrar usuarios, se creó un usuario llamado cliente1 con contraseña asignada, y se le asoció al grupo anteriormente creado.

Figura 22. creación de grupo y usuario



Fuente: Autoría propia

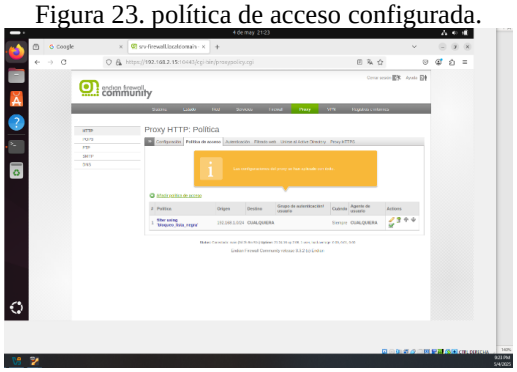
6.4 CREACIÓN DE POLÍTICA DE ACCESO VINCULADA AL PERFIL

Una vez configurado el perfil y creado el usuario, se accedió a Proxy → HTTP → Política de acceso → Añadir política de acceso. Allí se definió una política que vincula:

- El grupo creado.
- El perfil de filtrado bloqueo_lista_negra.
- El mecanismo de autenticación.

Con esta configuración, los usuarios autenticados pertenecientes al grupo quedaron sujetos a las restricciones del perfil.

Figura 23. política de acceso configurada.



Fuente: Autoría propia

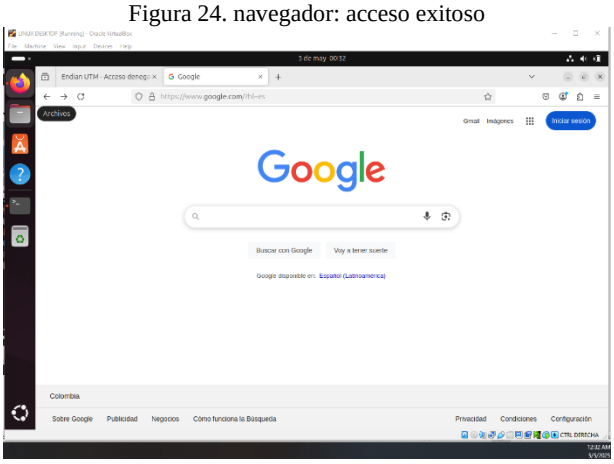
6.5 CONFIGURACIÓN DEL NAVEGADOR CLIENTE Y PRUEBAS

En la estación de trabajo ubicada en la zona verde, se configuró manualmente el proxy en el navegador web con la IP y puerto correspondientes. Al intentar acceder a sitios web, se solicitó credencial de usuario y contraseña.

Se realizó la validación del funcionamiento del proxy:

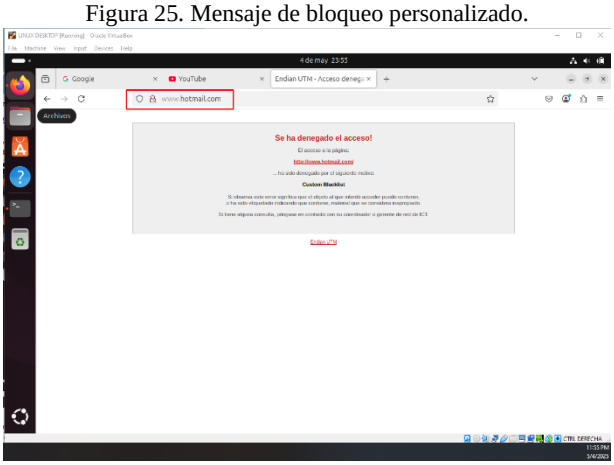
- Las páginas no incluidas en la lista negra se cargaron correctamente tras la autenticación.
- Las páginas bloqueadas mostraron el mensaje de acceso denegado proporcionado por Endian, gracias a la instalación previa del certificado HTTPS en el navegador cliente.

Figura 24. navegador: acceso exitoso



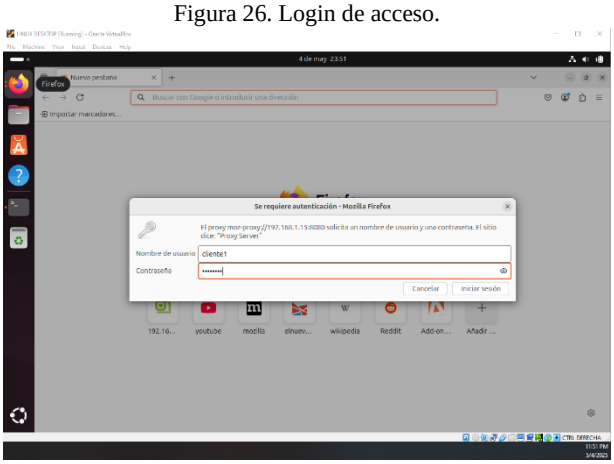
Fuente: Autoría propia

Figura 25. Mensaje de bloqueo personalizado.



Fuente: Autoría propia

Figura 26. Login de acceso.



Fuente: Autoría propia-

6.6 RESULTADOS

La implementación del proxy HTTP no transparente con políticas de autenticación en Endian Firewall permitió controlar eficazmente el acceso a contenidos web desde la zona verde. Esta configuración no solo garantizó la regulación del tráfico saliente, sino que también introdujo un sistema de autenticación por usuario que refuerza las medidas de control y seguimiento de la navegación.

Durante la activación del proxy, se observó que el entorno de Endian permite una configuración precisa y estructurada, desde la definición del modo de operación hasta la aplicación de perfiles personalizados de filtrado. Al optar por el modo no transparente, se exigió a los usuarios realizar ajustes manuales en sus navegadores, incluyendo la configuración del proxy HTTP con la IP de la zona verde y el puerto asignado por el sistema.

El perfil bloqueo_lista_negra, creado específicamente para esta temática, fue eficaz en la denegación de acceso a los dominios definidos. Al intentar ingresar a sitios como YouTube, Hotmail o El Nuevo Día, el sistema arrojó un mensaje de acceso denegado personalizado, confirmando que la política de filtrado funcionaba según lo esperado. Para lograr esta visibilidad, se instaló el certificado HTTPS proporcionado por Endian en el navegador cliente, ya que sin esta acción los navegadores modernos simplemente bloquean la página sin mostrar una explicación detallada.

En cuanto a la autenticación, el sistema exigió credenciales válidas antes de permitir cualquier navegación. Los intentos de conexión sin autenticación fueron inmediatamente rechazados. El usuario cliente1, creado para la prueba, pudo acceder a sitios permitidos, pero fue restringido automáticamente frente a los sitios definidos en la lista negra, lo que verificó el éxito en la aplicación combinada de autenticación y filtrado de contenido.

Otro punto relevante observado fue la capacidad de Endian para asociar múltiples usuarios a grupos, y múltiples grupos a distintas políticas de acceso, lo cual ofrece una escalabilidad significativa para entornos donde se requiere segmentar el tráfico por tipo de usuario, área funcional o niveles de acceso.

En conjunto, las pruebas realizadas demostraron que la solución implementada no solo limita el acceso de los usuarios, sino que también habilita una gestión jerarquizada del tráfico web. Este enfoque no intrusivo, pero efectivo, es especialmente útil en ambientes educativos o corporativos donde se busca balancear el acceso libre a la red con políticas de seguridad claras.

7 RESULTADOS GENERALES

La implementación de una infraestructura de seguridad perimetral bajo entornos GNU/Linux utilizando la distribución Endian Firewall permitió simular, configurar y validar una red segmentada con un enfoque didáctico y técnico. A lo largo de las cinco temáticas, cada una orientada a un

componente esencial de la seguridad de red, se logró establecer una arquitectura funcional y replicable para entornos reales.

En la Temática 1, se configuraron las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), utilizando VirtualBox como plataforma de virtualización. Esta base estructural permitió desplegar servicios, clientes y políticas con segmentación clara de tráfico.

La Temática 2 permitió aplicar reglas de NAT (Network Address Translation), garantizando que tanto los usuarios de la LAN como los servidores en la DMZ tuvieran acceso controlado a internet. Estas reglas facilitaron la traducción de direcciones internas a una interfaz pública, simulando escenarios de producción.

La Temática 3 se enfocó en la exposición controlada de servicios HTTP y FTP desde la DMZ hacia otras zonas, denegando intencionalmente protocolos como ICMP. Esta medida evitó escaneos o pruebas de conectividad externa mediante ping, aumentando la confidencialidad de los servicios internos.

En la Temática 4, se establecieron reglas específicas para permitir o denegar tráfico entre zonas, validando el acceso entre LAN y DMZ, así como entre WAN y DMZ. Las pruebas de tráfico desde distintas zonas confirmaron la efectividad de las políticas implementadas y el principio de mínima exposición.

Finalmente, en la Temática 5, se configuró un proxy HTTP no transparente, con autenticación por usuario y aplicación de una lista negra de sitios. Esta política demostró el control granular del tráfico saliente, diferenciando el acceso según perfiles de usuario y reforzando la seguridad mediante autenticación obligatoria.

8 CONCLUSIONES

- La virtualización con VirtualBox y la distribución Endian Firewall ofrecieron un entorno robusto [4][2], controlado y completamente funcional para la implementación práctica de políticas de seguridad perimetral bajo GNU/Linux.
- La segmentación de red en zonas (LAN, WAN y DMZ) fue la base de todas las políticas aplicadas, permitiendo estructurar controles diferenciados y específicos para cada tipo de tráfico, servicio o usuario.
- La configuración de reglas de NAT, filtrado de puertos, restricciones de servicios y autenticación mediante proxy, permitió simular entornos reales de seguridad de red, replicables en organizaciones educativas y empresariales.
- El uso de herramientas de línea de comandos, tal como lo exige la guía, fortaleció las competencias del equipo en administración avanzada de redes, sin depender de interfaces gráficas.
- Las pruebas realizadas validaron que Endian Firewall es una plataforma efectiva para gestionar políticas de acceso, control de tráfico y protección de recursos internos, siendo aplicable tanto en laboratorios como en escenarios reales.

9 REFERENCIAS

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

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

[3] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting* (3.a ed.). Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[4] Oracle. (2020). *Manual de usuario VirtualBox*. https://www.virtualbox.org/manual/