IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL BASADA EN ENDIAN FIREWALL CON SEGMENTACIÓN DE RED, CONTROL DE ACCESO Y SERVICIOS PROXY EN GNU/LINUX

Brayan Camilo Torres Torres
bctorrest@unadvirtual.edu.co
Dairo Muñoz de La Cruz
dmunozdel@unadvirtual.edu.co
Edwin Yovani Casanova Chachinoy
Edwin@unadvirtual.edu.co
Jesús Celid Gallego Orozco
jcgallegoor@unadvirtual.edu.co
Juan Camilo Alvarado Sierra
Jcalvarados@unadvirtual.edu.co

RESUMEN: *En este artículo se presenta la implementación de un esquema de seguridad perimetral mediante el uso de Endian Firewall en un entorno virtualizado con VirtualBox. El desarrollo se enfoca en la configuración de tres interfaces de red fundamentales: zona verde (LAN), zona roja (WAN) y zona naranja (DMZ), con el propósito de establecer una arquitectura segmentada que fortalezca la protección de la red.*

Asimismo, se implementa la funcionalidad de traducción de direcciones de red (NAT), permitiendo la comunicación desde las zonas internas hacia Internet. En términos de control de seguridad, se definen reglas de firewall para habilitar servicios específicos como HTTP (puerto 80) y FTP (puerto 21) desde la DMZ, al tiempo que se restringe tráfico no deseado, como el generado por el protocolo ICMP, evitando así respuestas a solicitudes de ping.

Finalmente, se establecen políticas de acceso que regulan el tráfico entre las diferentes zonas de red, evidenciando una correcta conectividad entre la LAN, la DMZ y la WAN para los servicios autorizados, garantizando tanto la funcionalidad como la seguridad del entorno implementado.

PALABRAS CLAVE: Endian Firewall, DMZ, NAT, Seguridad Perimetral.

1 INTRODUCCIÓN

En el contexto actual, la seguridad en redes informáticas se ha consolidado como un elemento fundamental dentro de cualquier infraestructura tecnológica. Más que una característica adicional, representa un requisito indispensable para garantizar la protección de la información, la continuidad de los servicios y la integridad de los sistemas frente a múltiples amenazas. En este escenario, los firewalls desempeñan un papel clave al actuar como mecanismos de control que supervisan y regulan el tráfico de red, permitiendo únicamente las comunicaciones autorizadas y bloqueando accesos potencialmente riesgosos [3].

Dentro de las soluciones disponibles, Endian Firewall se posiciona como una alternativa robusta y accesible, especialmente en entornos que requieren optimizar recursos. Al estar basado en GNU/Linux, ofrece estabilidad, flexibilidad y un enfoque de código abierto, lo que facilita su implementación sin necesidad de infraestructura especializada o altos costos [2], [3], siendo especialmente útil en contextos académicos, laboratorios de pruebas y pequeñas organizaciones.

Para el desarrollo de este trabajo, se empleó VirtualBox como plataforma de virtualización, permitiendo simular un entorno de red real sin intervenir la infraestructura física [6]. En este laboratorio se configuró una arquitectura segmentada compuesta por tres zonas principales: la zona verde (LAN), destinada a la red interna; la zona roja (WAN), orientada a la conexión con Internet; y la zona naranja (DMZ), utilizada para la publicación controlada de servicios como servidores web y FTP. Esta segmentación permite establecer diferentes niveles de seguridad según la función de cada red.

Durante la implementación del firewall, se habilitaron funcionalidades esenciales como la traducción de direcciones de red (NAT), facilitando la comunicación de los dispositivos internos hacia redes externas mediante el uso de una dirección IP pública. Asimismo, se definieron políticas de filtrado que permiten únicamente el tráfico necesario, habilitando servicios específicos y restringiendo protocolos como ICMP, con el objetivo de reducir posibles vectores de ataque [3]. De igual manera, se configuraron reglas de acceso para gestionar el flujo de datos entre las distintas zonas, logrando una red organizada, segura y eficiente.

En este artículo se describe de manera práctica el proceso de configuración de este entorno, resaltando la aplicación de buenas prácticas en seguridad perimetral y proporcionando una base sólida para la comprensión de los principios fundamentales en la protección de redes modernas.

2 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

(TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

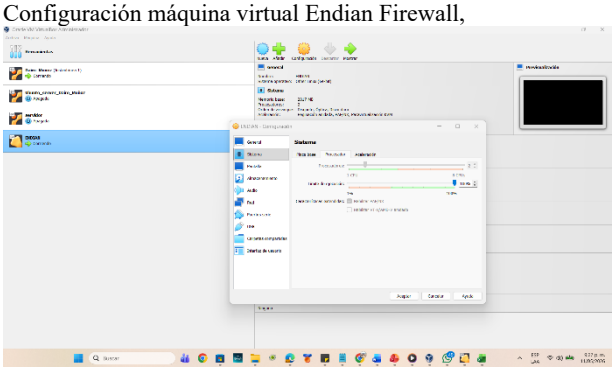
2.1 CONFIGURACIÓN INICIAL DE LA MÁQUINA VIRTUAL EN VIRTUALBOX.

En esta temática se describe el proceso de instalación, configuración y validación del firewall Endian Firewall en un entorno virtualizado, con el objetivo de implementar una arquitectura de red segmentada en diferentes zonas de seguridad.

En esta fase se llevó a cabo la preparación del entorno virtual necesario para la implementación del firewall, utilizando VirtualBox como herramienta de virtualización [6]. Este entorno permitió simular una infraestructura de red sin requerir hardware adicional, facilitando la configuración y validación de los diferentes componentes del sistema.

Inicialmente, se creó una máquina virtual destinada a alojar Endian Firewall, asignándole recursos básicos como memoria RAM, almacenamiento y procesador, acordes a los requerimientos del sistema. Como se muestra en la Figura. 1, se definieron las características generales de la máquina virtual, incluyendo el tipo de sistema operativo y los recursos asignados.

Figura 1.
Configuración máquina virtual Endian Firewall,

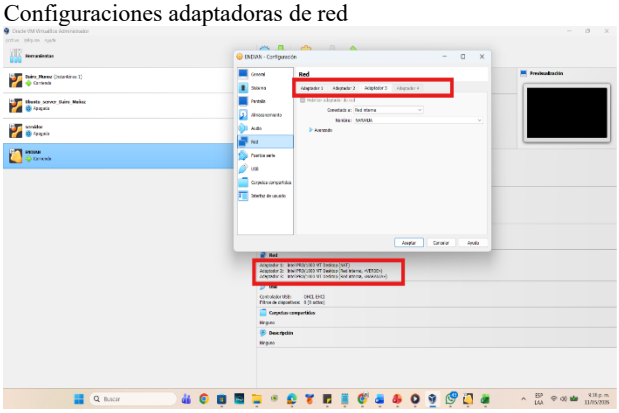


Fuente: Autoría propia

2.2 CONFIGURACIÓN DE ADAPTADORES DE RED PARA LAS ZONAS LAN, WAN Y DMZ.

Se procedió a la configuración de las interfaces de red, las cuales representan los diferentes segmentos de la arquitectura propuesta. Para este propósito, se definieron tres adaptadores de red dentro de la máquina virtual. Como se observa en la Figura. 2, cada adaptador fue configurado de la siguiente manera: el primero en modo NAT para simular la conexión a Internet (zona roja - WAN), el segundo como red interna para la red local (zona verde - LAN) y el tercero como red interna independiente para la zona desmilitarizada (zona naranja - DMZ).

Figura 2
Configuraciones adaptadoras de red

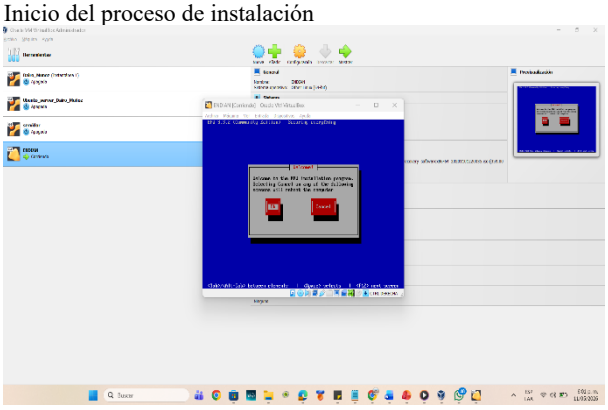


Fuente: Autoría propia

2.3 INSTALACIÓN DE ENDIAN FIREWALL Y ASIGNACIÓN DE ZONAS

Una vez se configura la máquina virtual, se inició el proceso de instalación del sistema [3]. Durante este procedimiento, se seleccionaron las opciones básicas y se aceptaron los términos correspondientes.

Figura 3
Inicio del proceso de instalación



Fuente: Autoría propia

La tabla presenta la configuración de tres interfaces de red, cada una asociada a una zona específica con funciones y niveles de seguridad diferenciados. El adaptador 1 corresponde a la zona roja (WAN), encargada de la conexión hacia Internet; el adaptador 2 se asigna a la zona verde (LAN), destinada a la red interna confiable; y el adaptador 3 se configura para la zona naranja (DMZ), orientada a la publicación de servicios. En conjunto, esta estructura define una arquitectura de firewall de tres segmentos, que permite establecer un control más preciso del tráfico y mejorar la seguridad de la red.

Figura 4
Definición de IP

	Adaptador1	Adaptador2:zona verde	Adaptador3: zona naranja
IP	NAT	192.168.120.0/24	192.168.150.0/24
DHCP	DHCP activado	DHCP desactivado	DHCP desactivado
Puerta de enlace	N/A	192.168.120.1	192.168.150.1
Mascara de red		255.255.255.0	255.255.255.0
Rango de ip		192.168.120.2 - 192.168.120.253	192.168.150.2 - 192.168.150.253

Fuente: Autoría propia

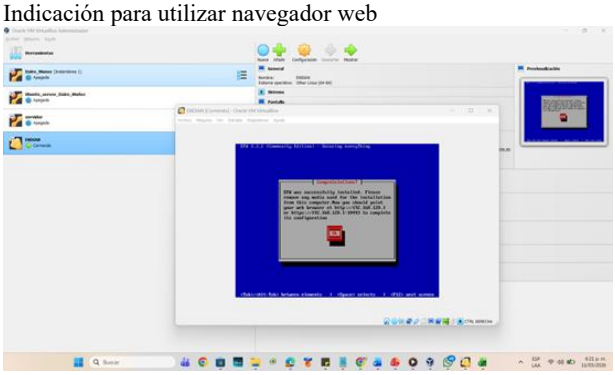
De la configuración de Endian, uno de los puntos fundamentales, es la asignación de la IP a la interfaz verde (GREEN). Este procedimiento establece la puerta de enlace principal del sistema, permitiendo la comunicación y administración de toda la red interna de forma segura. Sin esta definición correcta de la dirección y máscara de subred `255.255.255.0`, sería imposible desplegar posteriormente la zona naranja para la protección de aplicaciones y bases de datos.

Figura 5.
Asignación de IP para la zona verde

Fuente: Autoría propia

Después de terminar las configuraciones el firewall ya está en funcionamiento, y la dirección 192.168.120.1 es la IP de la interfaz de administración.

Figura 6.
Indicación para utilizar navegador web

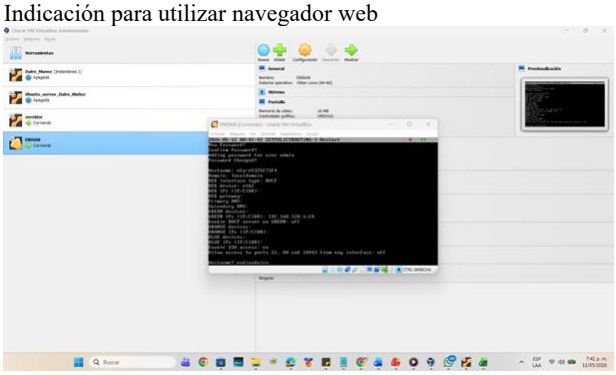


Fuente: Autoría propia

Tras finalizar el proceso de instalación de Endian Firewall, el sistema realizó automáticamente la configuración inicial, incluyendo el cambio de credenciales del administrador y la asignación de parámetros de red. En este punto, la interfaz correspondiente a la zona roja (WAN) fue configurada para obtener dirección IP mediante DHCP, mientras que la zona verde (LAN) se estableció con una dirección IP estática (192.168.120.1) [3].

Posteriormente, se llevó a cabo la asignación del nombre del host y la configuración de las zonas de red, tal como se muestra en la Figura **7**, donde se delimitan las zonas verde, roja y naranja dentro del firewall.

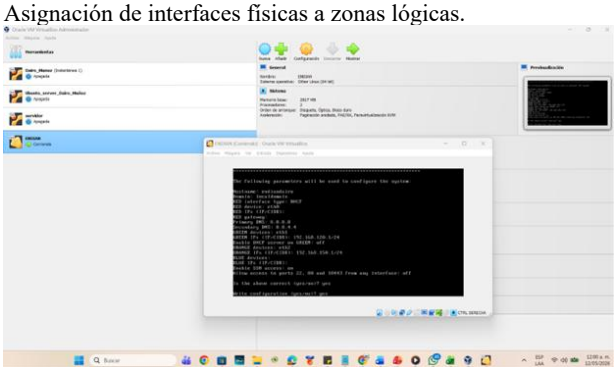
Figura 7
Indicación para utilizar navegador web



Fuente: Autoría propia

Se completó la asignación de las interfaces físicas (eth0, eth1, eth2) a las zonas lógicas correspondientes (roja, verde y naranja), verificando además la correcta configuración de los parámetros de direccionamiento IP y servidores DNS, como se evidencia en la Figura 8.

Figura 8.
Asignación de interfaces físicas a zonas lógicas.



Fuente: Autoría propia

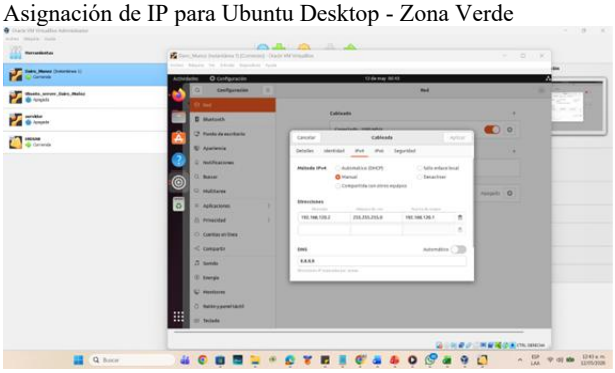
Una vez confirmados los cambios, el firewall aplicó la segmentación de red establecida (eth0 = WAN, eth1 = LAN, eth2 = DMZ), quedando listo para su administración a través de la interfaz web accesible.

2.4 CONFIGURACIÓN Y VALIDACIÓN DE CLIENTES EN LA LAN Y DMZ

Para la integración de los equipos dentro de la arquitectura de red, se realizó la configuración del cliente en la zona verde (LAN) y del servidor en la zona naranja (DMZ), asegurando su correcta comunicación con el firewall Endian Firewall.

En la zona LAN, se configuró el adaptador de red como red interna y se asignó una dirección IP estática junto con su puerta de enlace, permitiendo la conexión con el firewall y la participación dentro de la red local segura [1], como se muestra en la Figura 9.

Figura 9
Asignación de IP para Ubuntu Desktop - Zona Verde

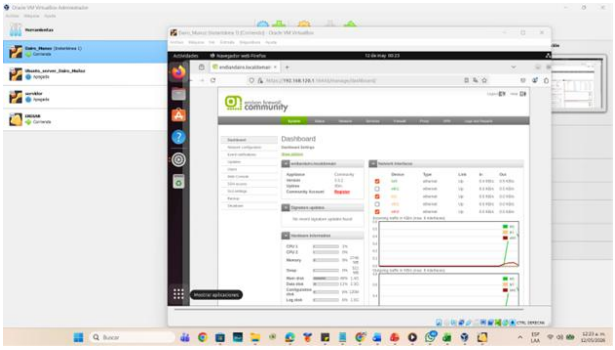


Fuente: Autoría propia

Una vez finalizada la configuración inicial del sistema, se accedió a la interfaz de administración web del firewall Endian Firewall desde un equipo cliente ubicado en la zona verde (LAN). Para ello, se utilizó un navegador web ingresando a la dirección segura https://192.168.120.1:10443, la cual corresponde a la interfaz de gestión del sistema.

Este acceso permitió validar la conectividad entre el cliente y el firewall, así como confirmar que los servicios de administración se encuentran activos y disponibles para la configuración de políticas de seguridad, usuarios y servicios de red.

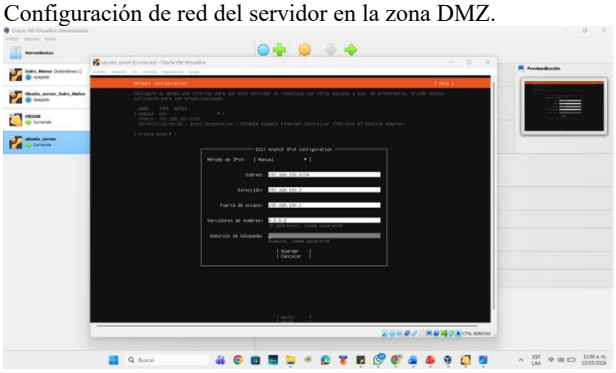
Figura 10.
Acceso a la interfaz web de administración desde la red LAN.



Fuente: Autoría propia

En la zona DMZ, se configuró el servidor basado en Ubuntu Server, asignando su adaptador a una red interna independiente y estableciendo una dirección IP estática junto con la puerta de enlace del firewall, garantizando su ubicación dentro de la arquitectura de seguridad (Figura 11).

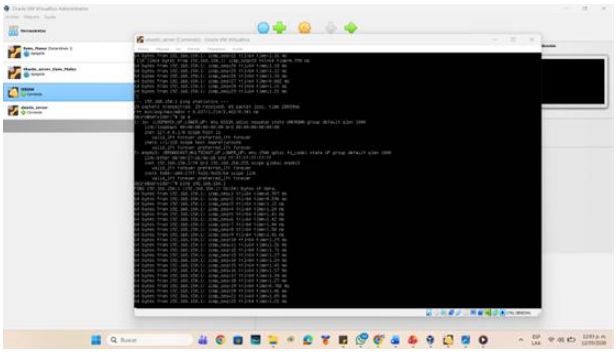
Figura 11.
Configuración de red del servidor en la zona DMZ.



Fuente: Autoría propia

Finalmente, se realizaron pruebas de conectividad desde el servidor hacia el firewall, validando su correcta integración dentro de la zona naranja (Figura 12).

Figura 12
Validación de conectividad en la zona DMZ.



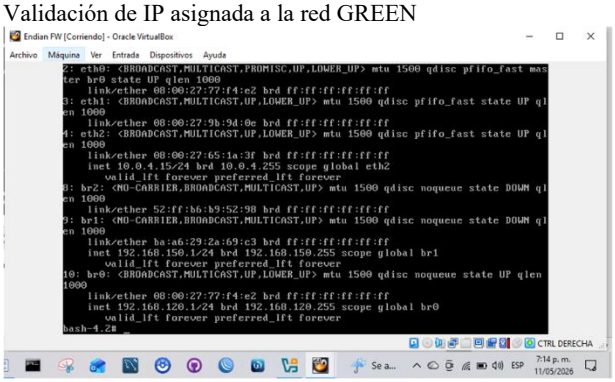
Fuente: Autoría propia

Con lo anterior, se completa la configuración inicial del entorno, logrando la correcta instalación de Endian Firewall y la segmentación de la red en sus respectivas zonas (LAN, WAN y DMZ). Las pruebas realizadas, incluyendo el acceso a la interfaz web de administración, permitieron validar la conectividad y el funcionamiento adecuado del sistema, dejando la infraestructura lista para la aplicación de políticas de seguridad en las siguientes etapas.

3 TEMÁTICA 2: CONFIGURACIÓN NAT.

Posteriormente a la instalación y configuración inicial de Endian Firewall Community, se procedió con la validación de conectividad entre las diferentes zonas de red definidas dentro de la topología propuesta. En primera instancia, se culminó la configuración de la zona GREEN, correspondiente a la red interna segura utilizada para la administración y acceso de los clientes autorizados.

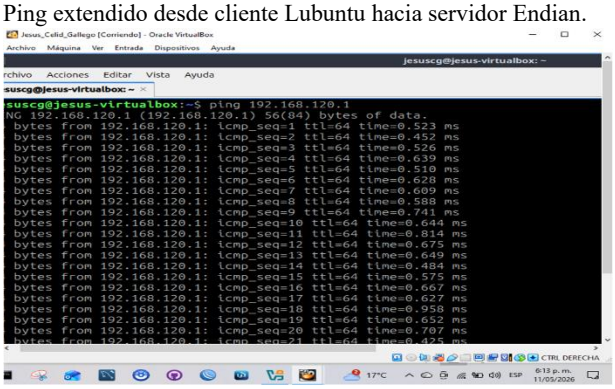
Figura 13.
Validación de IP asignada a la red GREEN



Fuente: Autoría propia

A continuación, se realizó la validación de conectividad desde el cliente Linux hacia el firewall Endian, comprobando la correcta comunicación entre ambos dispositivos dentro del mismo segmento de red

Figura 14.
Ping extendido desde cliente Lubuntu hacia servidor Endian.



Fuente: Autoría propia

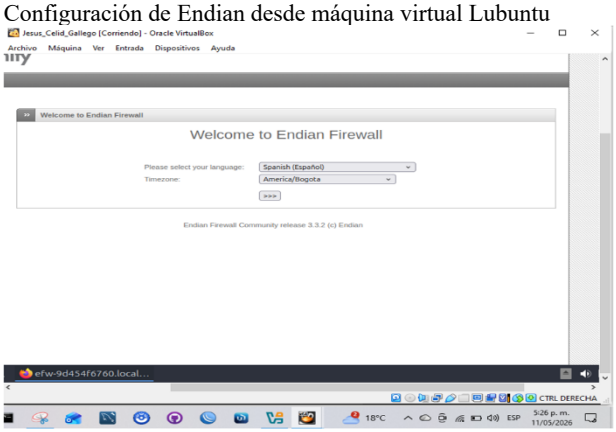
Posteriormente, se verificó la comunicación entre la máquina virtual Lubuntu y el firewall, garantizando que el direccionamiento IP y las interfaces estuvieran configuradas correctamente.

Figura 15.
Comunicación entre Lubuntu y Endian

Fuente: Autoría propia

Una vez validada la conectividad básica, se inició el proceso de administración y configuración del firewall desde la máquina virtual Lubuntu mediante el acceso a la interfaz web de administración de Endian.

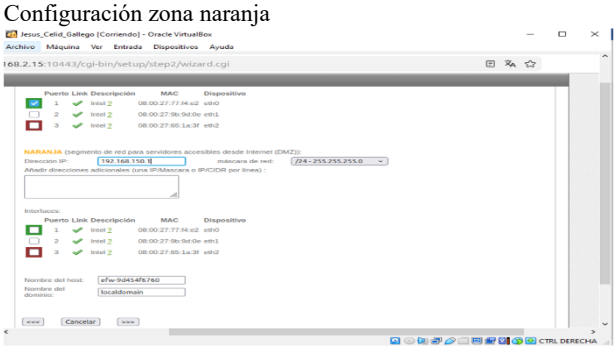
Figura 16
Configuración de Endian desde máquina virtual Lubuntu



Fuente: Autoría propia

Seguidamente, se realizó la configuración de las tarjetas de red de acuerdo con el direccionamiento IP y la segmentación previamente definidos por el compañero encargado de la temática 1, permitiendo la separación adecuada de las zonas GREEN, ORANGE y RED dentro del firewall.

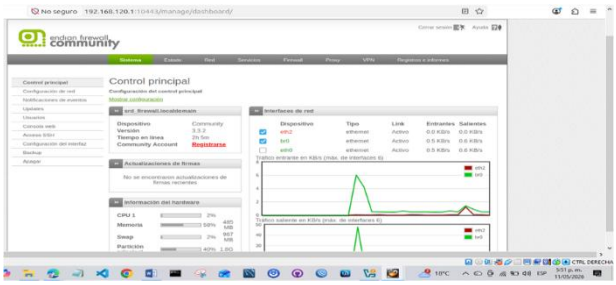
Figura 17
Configuración zona naranja



Fuente: Autoría propia

Después de configurar las interfaces, se accedió al panel principal o Dashboard de Endian para verificar el estado general del sistema, el consumo de recursos y las zonas configuradas.

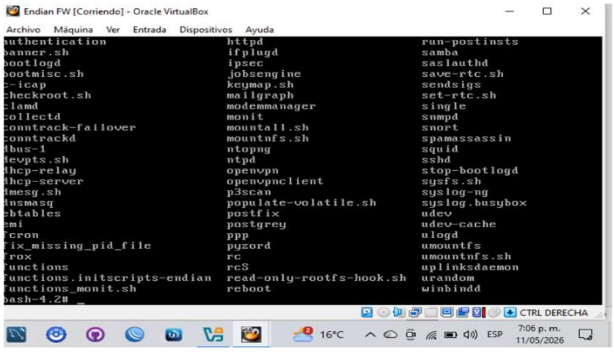
Figura 18
Pantalla de inicio de Endian



Fuente: Autoría propia

Posteriormente, se revisaron los servicios disponibles dentro del sistema, con el objetivo de validar los procesos activos y garantizar el correcto funcionamiento de los servicios esenciales del firewall.

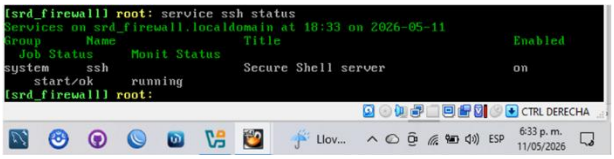
Figura 19.
Servicios activos en Endian



Fuente: Autoría propia

Dentro de las pruebas realizadas, se verificó específicamente el estado del servicio SSH, utilizado para administración remota segura del firewall.

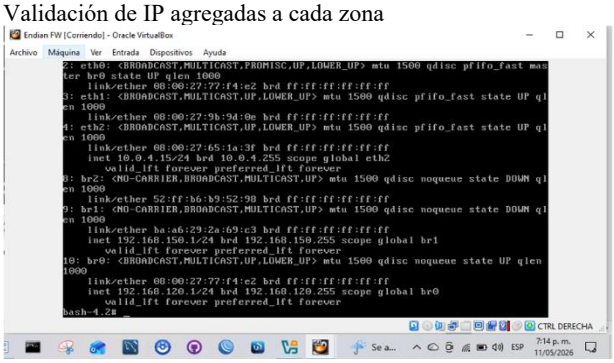
Figura 20.
SSH activo



Fuente: Autoría propia

Antes de iniciar la configuración de las reglas NAT, se realizó nuevamente una validación completa de las interfaces de red configuradas, verificando direccionamiento IP, máscara de subred y asignación correcta de cada zona.

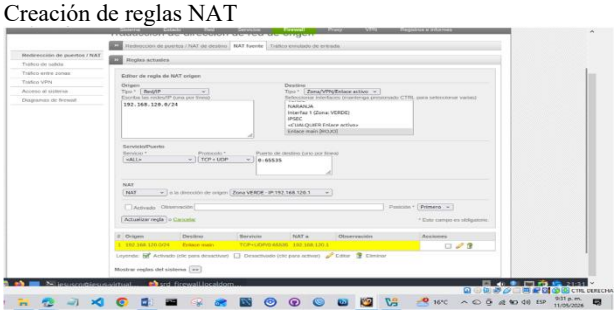
Figura 21
Validación de IP agregadas a cada zona



Fuente: Autoría propia

Se procedió con la creación de las reglas NAT (Network Address Translation), las cuales permiten traducir direcciones IP privadas hacia direcciones públicas para garantizar el acceso a Internet desde las redes internas y DMZ.

Figura 22
Creación de reglas NAT



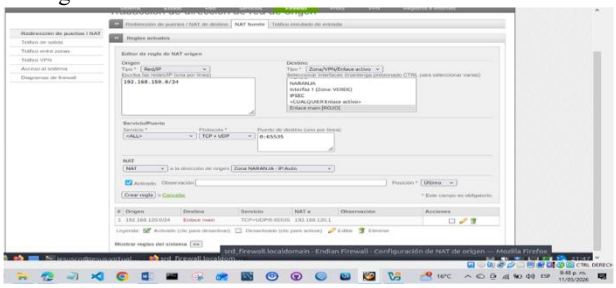
Fuente: Autoría propia

Con el fin de comprobar la salida a Internet desde el firewall, se ejecutó una prueba de conectividad mediante un ping extendido hacia los servidores de Google. Esta validación permitió confirmar que Endian contaba con acceso hacia la red externa

3.1 CONFIGURACIÓN DE LA ZONA DMZ Y PUBLICACIÓN DE SERVICIOS

Para la implementación de la zona desmilitarizada (DMZ), se configuró inicialmente el NAT correspondiente al servidor Linux conectado a la interfaz ORANGE del firewall Endian. Esta configuración permite aislar los servicios públicos del resto de la red interna, incrementando el nivel de seguridad de la infraestructura.

Figura 23
Configuración DMZ



Fuente: Autoría propia

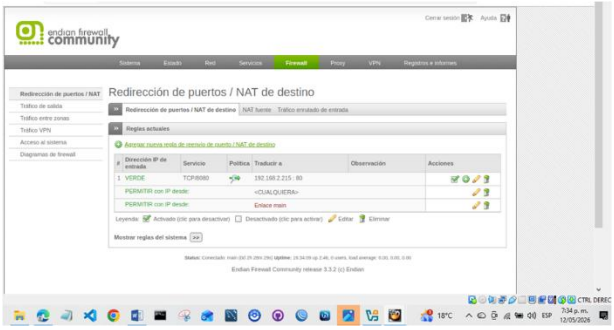
Posteriormente, se verificó la correcta creación y aplicación de las reglas NAT dentro del panel de administración de Endian.

Figura 24
Panel Endian, validación configuración

Fuente: Autoría propia

Luego, se creó específicamente la regla DMZ encargada de permitir el acceso controlado hacia el servidor ubicado en la zona ORANGE, habilitando la publicación segura del servicio web hacia la red interna y externa.

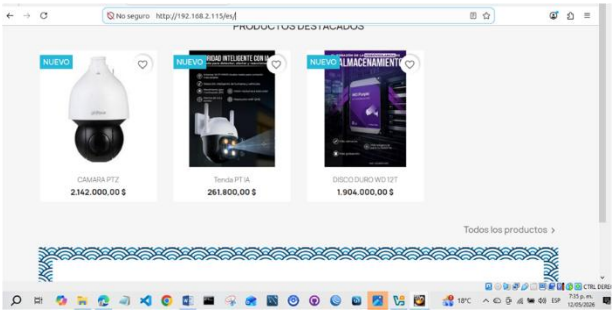
Figura 25.
Regla DMZ



Fuente: Autoría propia

Finalmente, se realizó la validación de acceso al servidor PrestaShop desde el equipo Lubuntu, comprobando que la configuración NAT y DMZ fue implementada correctamente y que el servicio web publicado en la zona ORANGE se encontraba accesible.

Figura 26.
Servidor Web accesible desde la red.



Fuente: Autoría propia

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

En el desarrollo de esta fase se llevó a cabo la implementación de un entorno de red segmentado con el propósito de analizar el comportamiento de los servicios y su control dentro de diferentes zonas de seguridad. Mediante el uso de Endian Firewall en un entorno virtualizado, se estableció una arquitectura que permite gestionar el tráfico entre redes internas y externas de forma controlada.

Se configuraron los servicios necesarios dentro de la zona desmilitarizada (DMZ), con el objetivo de permitir el acceso controlado a recursos específicos desde otras zonas de la red. Utilizando Endian Firewall, se habilitaron servicios como HTTP (puerto 80) y FTP (puerto 21), los cuales fueron desplegados en un servidor ubicado en la DMZ.

4.1 RESTRICCIÓN DE PROTOCOLOS NO AUTORIZADOS

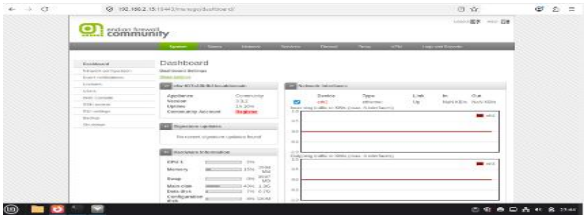
Como parte de las políticas de seguridad, se procedió a restringir protocolos considerados innecesarios o potencialmente riesgosos. En este caso, se bloqueó el protocolo ICMP, evitando la respuesta a solicitudes de ping desde otras zonas de la red.

Esta medida contribuye a reducir la visibilidad de los dispositivos y limita posibles intentos de reconocimiento por parte de usuarios no autorizados [3].

4.2 VALIDACIÓN DE SERVICIOS Y PRUEBAS DE ACCESO

Finalmente, esta práctica permitió comprender la importancia de la segmentación de redes y el uso de firewalls como mecanismo de protección y administración del tráfico, asegurando una comunicación controlada entre usuarios, servicios y zonas de seguridad dentro de un entorno GNU/Linux.

Figura 27
Máquina configurada en LAN.



Fuente: Autoría propia.

Regla 1: HTTP desde DMZ a LAN
Regla 2: FTP desde DMZ a LAN

De igual forma, se comprobó que las restricciones aplicadas funcionaran correctamente, evidenciando la denegación de tráfico no permitido.

Figura 28
Configuración de Firewall de salida.

Fuente: Autoría propia.

4.3 RESULTADOS DE LA TEMÁTICA 3

Los resultados obtenidos evidencian la correcta implementación de servicios en la zona DMZ, garantizando que únicamente los protocolos autorizados se encuentren disponibles. Asimismo, se confirmó que el firewall permite aplicar políticas de control de acceso de manera efectiva, asegurando el aislamiento entre zonas y protegiendo la red interna.

Esta práctica demuestra la importancia de configurar adecuadamente los servicios expuestos y aplicar restricciones que minimicen los riesgos de seguridad, manteniendo un equilibrio entre disponibilidad y protección.

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

Durante el desarrollo de la temática 4 se configuraron reglas de firewall en Endian Firewall Community para permitir y controlar la comunicación entre las diferentes zonas de red implementadas en el entorno virtualizado. Se habilitaron reglas Inter-Zone permitiendo el acceso desde la zona GREEN hacia la zona ORANGE mediante protocolos específicos como HTTP y FTP, garantizando el funcionamiento de los servicios alojados en el servidor Ubuntu Server dentro de la DMZ.

Asimismo, se verificó el correcto funcionamiento de las políticas mediante pruebas de conectividad realizadas desde el cliente Linux Mint utilizando navegador web y servicios de transferencia de archivos. La implementación de estas reglas permitió restringir únicamente el tráfico autorizado, fortaleciendo la seguridad perimetral y evitando accesos no permitidos dentro de la infraestructura de red [3].

A partir de esto, se llevaron a cabo pruebas enfocadas en protocolos como HTTP (puerto 80) y FTP (puerto 21), verificando que la comunicación entre redes internas y externas se realizara de acuerdo con las reglas definidas. Asimismo, se validó el comportamiento del tráfico inter-zona y el acceso a los servicios desde navegadores web, asegurando que las políticas implementadas cumplieran con los criterios de seguridad establecidos.

5.1 CONFIGURACIÓN Y VALIDACIÓN DE REGLAS

Se configuraron reglas en el firewall para permitir la comunicación desde la zona interna (LAN o GREEN) hacia la zona DMZ (ORANGE), habilitando específicamente los servicios HTTP y FTP a través de sus respectivos puertos (80 y 21).

Esta configuración permitió que los equipos de la red interna accedieran a servicios alojados en la DMZ de manera controlada, demostrando cómo se puede habilitar el acceso sin comprometer la seguridad de la red principal.

Figura 29
Regla de acceso para la zona DMZ

Fuente: Autoría propia

5.2 PRUEBAS DE ACCESO DESDE NAVEGADOR Y SERVICIOS

Se realizaron diferentes pruebas prácticas para comprobar el comportamiento del tráfico:

Desde LAN hacia DMZ: Se verificó el acceso a servicios HTTP alojados en la DMZ, confirmando que la comunicación estaba habilitada correctamente.

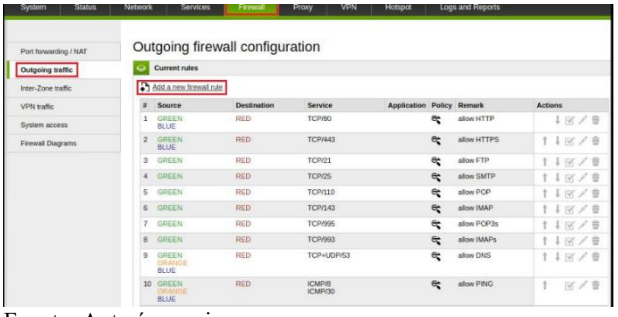
Desde LAN hacia Internet: Se comprobó la salida a la red externa mediante navegación web, evidenciando conectividad con sitios públicos.
Desde DMZ hacia Internet: Se validó que los equipos en la DMZ también pudieran acceder a servicios externos.

Desde Internet hacia DMZ: Se accedió a servicios publicados en la DMZ, demostrando que las reglas permiten conexiones entrantes controladas.

FTP desde LAN hacia Internet: Se comprobó la conexión a servidores FTP externos desde la red interna.

FTP desde Internet hacia DMZ: Se verificó el acceso a un servidor FTP ubicado en la DMZ, mostrando la disponibilidad del servicio.

Figura 30.
Validación de tráfico Inter zona



Fuente: Autoría propia.

6 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

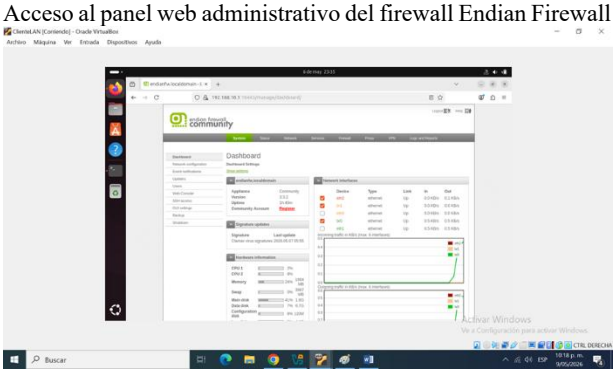
6.1 IMPLEMENTACIÓN DE LA MÁQUINA VIRTUAL ENDIAN FIREWALL COMMUNITY.

Se muestra la implementación y ejecución de la máquina virtual correspondiente al firewall Endian Firewall Community bajo VirtualBox [6]. Durante esta fase se configuraron las tarjetas de red necesarias para permitir la comunicación entre la red LAN y el acceso a Internet. Adicionalmente, se verificó el correcto funcionamiento de la zona GREEN correspondiente a la red interna LAN, permitiendo posteriormente la comunicación entre el cliente Ubuntu y el servidor proxy implementado.

6.2 ACCESO AL PANEL WEB ADMINISTRATIVO DE ENDIAN.

Se muestra el acceso exitoso a la interfaz web administrativa del firewall Endian Firewall Community mediante navegador web desde el cliente Ubuntu perteneciente a la red LAN. El acceso se realizó utilizando la dirección https://192.168.10.1:10443, permitiendo administrar y configurar los diferentes servicios de seguridad implementados dentro del firewall.

Figura 31
Acceso al panel web administrativo del firewall Endian Firewall

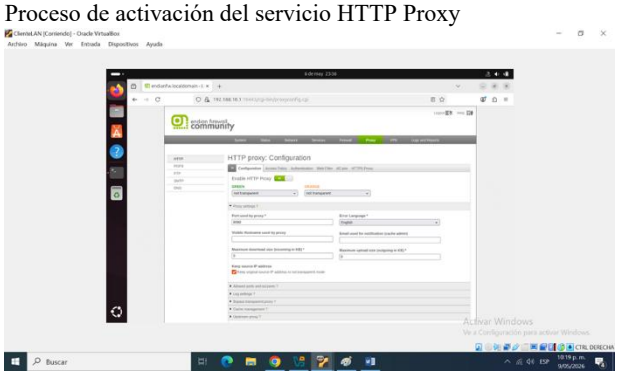


Fuente: Autoría propia.

6.3 ACTIVACIÓN DEL SERVICIO HTTP PROXY.

En esta evidencia se observa el proceso de activación del servicio HTTP Proxy desde la sección Proxy → HTTP → Configuración dentro de Endian Firewall Community. Se habilitó el servicio proxy con el objetivo de controlar y administrar el tráfico de navegación generado desde la red LAN hacia Internet. Esta configuración permite implementar políticas de seguridad, autenticación de usuarios y filtrado de contenido web, fortaleciendo la seguridad perimetral de la infraestructura implementada.

Figura 32.
Proceso de activación del servicio HTTP Proxy

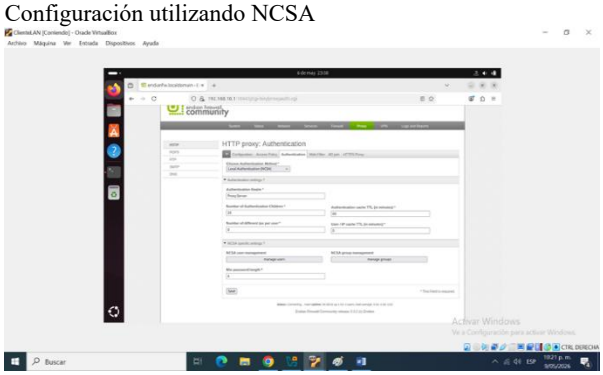


Fuente: Autoría propia.

6.4 CONFIGURACIÓN DE AUTENTICACIÓN DEL PROXY HTTP.

Se configuró la autenticación local del Proxy HTTP utilizando el método NCSA (Local Authentication). Esta configuración permite validar y controlar el acceso de los usuarios a Internet mediante credenciales de autenticación previamente registradas en el sistema. De esta manera, únicamente los usuarios autorizados podrán utilizar el servicio proxy configurado en el firewall.

Figura 33
Configuración utilizando NCSA

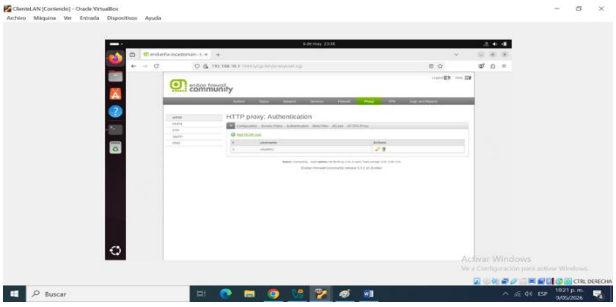


Fuente: Autoría propia.

6.5 CREACIÓN DEL USUARIO DE AUTENTICACIÓN.

Se muestra la creación del usuario local denominado “usuario1”, el cual será utilizado para la autenticación y validación de acceso al servicio Proxy HTTP. Para el usuario se definieron credenciales de acceso que posteriormente serán utilizadas durante la navegación web desde el cliente Ubuntu.

Figura 34.
Creación del usuario

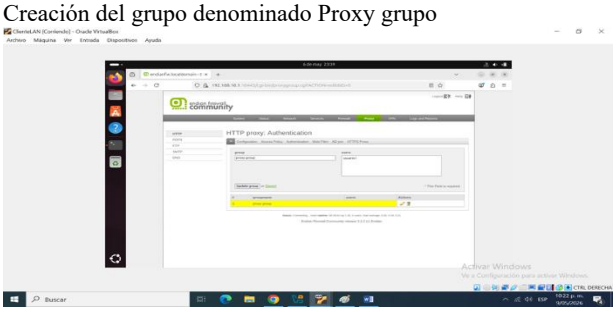


Fuente: Autoría propia.

6.6 CREACIÓN DEL GRUPO DE ACCESO.

Se muestra la creación del grupo denominado "proxygrupo", utilizado para asociar usuarios y aplicar políticas de acceso y filtrado dentro del servicio proxy. Posteriormente el usuario "usuario1" fue asociado a este grupo con el fin de administrar de manera organizada los permisos y restricciones de navegación.

Figura 35.
Creación del grupo denominado Proxy grupo



Fuente: Autoría propia.

6.7 CONFIGURACIÓN DE LA LISTA NEGRA (BLACKLIST)

Se muestra la configuración de la lista negra (Blacklist) dentro del Web Filter del Proxy HTTP en Endian Firewall Community. Se agregaron los dominios www.youtube.com, www.hotmail.com y www.elnuevodia.com.co en la sección "block the following sites", con el propósito de restringir el acceso a estos sitios web desde la red LAN. Esta política de filtrado permite fortalecer la seguridad y el control de navegación de los usuarios autenticados dentro de la infraestructura implementada [3].

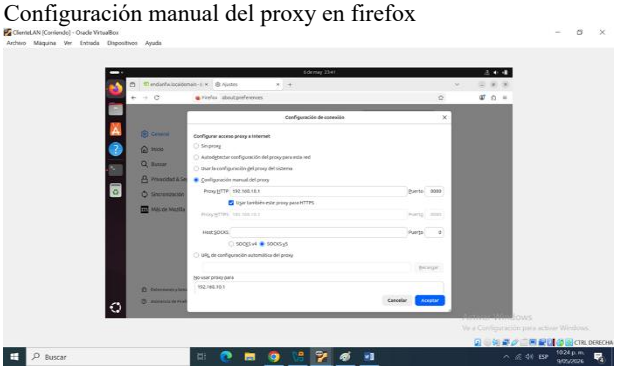
Figura 36.
Configuración de la lista negra

Fuente: Autoría propia.

6.8 CONFIGURACIÓN MANUAL DEL PROXY EN FIREFOX.

Se configura manualmente el navegador Mozilla Firefox del cliente Ubuntu para utilizar el servicio Proxy HTTP no transparente implementado en Endian Firewall Community. La configuración se realizó utilizando la dirección IP 192.168.10.1 y el puerto 8080. Esta configuración confirma que el proxy implementado corresponde a un proxy no transparente, debido a que el navegador requiere ser configurado manualmente para utilizar el servicio.

Figura 37.
Configuración manual del proxy en firefox

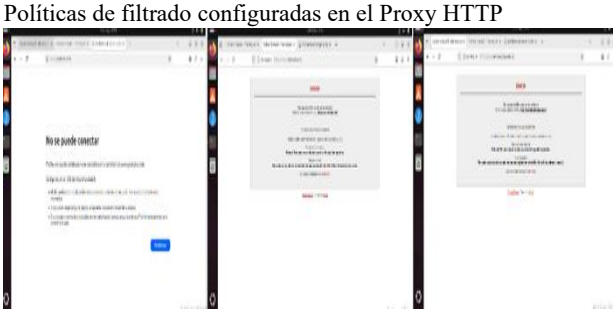


Fuente: Autoría propia.

6.9 VERIFICACIÓN DEL BLOQUEO DE SITIOS WEB.

Se verifica el correcto funcionamiento de las políticas de filtrado configuradas en el Proxy HTTP. Al intentar acceder desde el navegador Firefox a los sitios web incluidos en la Blacklist, el sistema genera mensajes de error como "503 Service Unavailable" y "The request URL could not be retrieved", confirmando que el proxy bloquea exitosamente el acceso a las páginas restringidas según las políticas de seguridad implementadas.

Figura 38
Políticas de filtrado configuradas en el Proxy HTTP



Fuente: Autoría propia.

7 CONCLUSIONES

La implementación de una arquitectura de red segmentada mediante Endian Firewall en un entorno virtualizado permitió verificar la correcta asignación de las interfaces de red tanto a nivel lógico como físico, garantizando una adecuada organización de la infraestructura. Asimismo, la configuración de direcciones IP estáticas y el enrutamiento de los equipos en las zonas LAN y DMZ facilitaron una comunicación controlada entre los diferentes segmentos. Las pruebas de conectividad realizadas confirmaron el correcto funcionamiento del entorno implementado, consolidando una base sólida para la aplicación de políticas de seguridad y el fortalecimiento de la protección perimetral.

La configuración de NAT en Endian permitió comprender la importancia de estructurar adecuadamente la red para garantizar un funcionamiento seguro y estable. La segmentación en zonas LAN, DMZ y WAN proporcionó un mayor control sobre el tráfico, definiendo claramente los accesos y servicios habilitados. Además, el uso de NAT facilitó la conexión de los dispositivos internos a Internet sin exponer sus direcciones IP reales, aportando una capa adicional de protección y evidenciando la importancia de una correcta implementación de SNAT y DNAT para mantener una comunicación eficiente y segura.

La configuración realizada en la zona DMZ permitió habilitar de manera controlada los servicios necesarios, garantizando que únicamente protocolos autorizados como HTTP y FTP estuvieran disponibles. Del mismo modo, la restricción del protocolo ICMP demostró la correcta aplicación de políticas de seguridad al reducir la exposición de la red frente a posibles reconocimientos externos. Las pruebas de conectividad y el análisis del tráfico confirmaron una adecuada segmentación entre la DMZ y la red interna, asegurando tanto la funcionalidad de los servicios como la protección del entorno.

La definición e implementación de reglas de firewall evidenció la importancia de controlar el tráfico entre las diferentes zonas de red mediante políticas claras y específicas. La configuración aplicada permitió garantizar la comunicación necesaria entre servicios autorizados, manteniendo al mismo tiempo la seguridad de la red interna. Los resultados obtenidos reflejan el papel fundamental de la DMZ como zona intermedia de protección dentro de una arquitectura de seguridad perimetral.

La implementación de un Proxy HTTP no transparente con autenticación local permitió controlar el acceso a Internet desde la red LAN mediante políticas de seguridad y filtrado web. Adicionalmente, la creación de una lista negra para restringir sitios web específicos demostró la efectividad de las políticas de control de navegación configuradas. Esta práctica fortaleció los conocimientos relacionados con la administración de servicios en GNU/Linux, la configuración de redes virtuales, la seguridad perimetral y la gestión del acceso a recursos mediante servicios proxy [5].

8 REFERENCIAS

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

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

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

[4] Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server . Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[5] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix https://learning.lpi.org/es/learning-materials/101-500/102

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