CONFIGURACIÓN DE ENDIAN FIREWALL 3.3.2 EN ENTORNO VIRTUALIZADO

Alejandra Moreno Salazar
e-mail: amorenosal@unadvirtual.edu.co
Jhon Fredy Rivera Londoño
e-mail: jfriveralo@unadvirtual.edu.co
Leydi Alejandra Jiménez Rodríguez
e-mail: lajimenezrodr@unadvirtual.edu.co
Leidy Viviana Bernate Roa
e-mail: lvbernatr@outlook.edu.co
Mauricio Baena Zuluaga
e-mail: mbaenaz@unadvirtual.edu.co

RESUMEN: *En este artículo se presenta la implementación de una infraestructura perimetral basada en Endian Firewall Community 3.3.2, desplegada en un entorno virtualizado utilizando VirtualBox. El sistema se configuró bajo un modelo de seguridad de tres zonas: LAN, DMZ y WAN; con el fin de segmentar el tráfico y fortalecer la seguridad de los servicios instalados en servidores GNU/Linux. Cada temática aborda procesos específicos, como preparación del entorno virtual, configuración del firewall, despliegue de servicios, gestión de usuarios, seguridad perimetral y pruebas de conectividad. Las configuraciones se realizaron por consola, siguiendo lineamientos del curso, y se complementaron mediante la interfaz web administrativa de Endian sólo cuando fue estrictamente necesario. Los resultados demostraron que la arquitectura implementada permite un control eficiente del tráfico interno y externo, asegurando la operatividad de los servicios y cumple las buenas prácticas para entornos corporativos.*

PALABRAS CLAVE: DMZ, Endian, Firewall, Virtualización, GNU/Linux.

1. INTRODUCCIÓN

En este trabajo se implementó Endian Firewall Community 3.3.2 como solución perimetral de tres zonas dentro de un entorno virtualizado con VirtualBox. El trabajo se organiza en cuatro temáticas. La Temática 1 aborda la instalación del firewall, la creación de la máquina virtual y la configuración inicial de las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). La Temática 2 domina tanto la NAT de Salida (SNAT/Masquerading) para el acceso a Internet desde redes internas (LAN y DMZ), como la NAT de Entrada (DNAT/Port Forwarding) para exponer servicios de la DMZ al mundo exterior. La temática 3 profundiza como la DMZ es un segmento de red clave para la mitigación de riesgos, aislando servicios públicos de la infraestructura interna [6]. Las políticas de tráfico de salida se diseñaron aplicando el principio de mínimo privilegio [8], restringiendo la comunicación por defecto. Se configuraron las redes del host de la DMZ y se inyectaron reglas en Netfilter/iptables (firewall Endian) para permitir servicios (HTTP/FTP) y fortalecer la seguridad mediante la denegación explícita del tráfico de reconocimiento [7], la Temática 4 detalla las pruebas finales, evidencias de funcionamiento y validación integral del sistema implementado. El proceso se realizó mediante consola, complementado con la interfaz web únicamente.

2. TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

2.1 INFRAESTRUCTURA VIRTUAL.

Para la implementación del firewall perimetral se creó una máquina virtual basada en Endian Firewall Community 3.3.2, siguiendo las recomendaciones establecidas por la documentación oficial del proyecto [1]. La máquina virtual fue configurada con tres tarjetas de red asignadas a las zonas de seguridad: Roja (WAN), Verde (LAN) y Naranja (DMZ). La zona Roja se configuró utilizando un adaptador NAT/Bridge con obtención de dirección IP mediante DHCP, permitiendo el acceso a Internet y actuando como punto de salida de la red. La zona Verde se estableció como una red interna con direccionamiento manual 172.20.10.1/24, mientras que la zona Naranja se configuró también como red interna con el rango 10.100.20.0/24 y gateway 10.100.20.1. Adicionalmente, se integraron dos máquinas complementarias: un cliente Ubuntu Desktop 22.04 dentro de la LAN y un servidor Ubuntu Server 22.04 ubicado en la DMZ. Esta estructura permitió emular un entorno perimetral típico de una organización, segmentando correctamente los dominios de seguridad para proteger servicios críticos alojados en la DMZ.

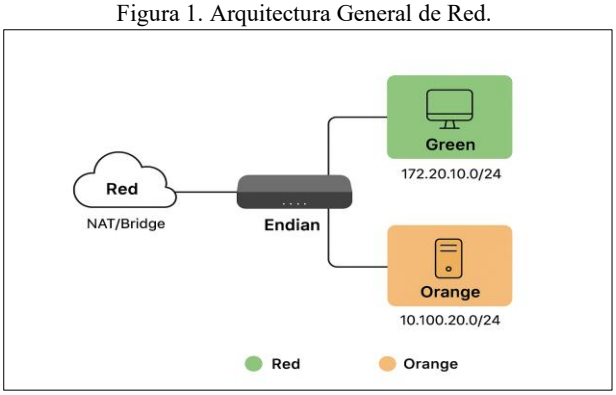
Tabla 1. Esquema de Direccionamiento IP.

Parámetro	Zona Verde (LAN)	Zona Naranja (DMZ)	Zona Roja (WAN)
Identificador de Red	172.20.10.0/24	10.100.20.0/24	N/A
Endian (Puerta de enlace)	172.20.10.1	10.100.20.1	Asignación Automática (DHCP)

Dispositivo	Cliente: 172.20.10.100	Servidor DMZ: 10.100.20.10	N/A
Puerta de enlace para Clientes/Servidor	172.20.10.1	10.100.20.1	N/A
DNS	8.8.8.8	8.8.8.8	N/A
Método de Conexión	Interna	Interna	NAT/Puente

Fuente: Autoría Propia.

Figura 1. Arquitectura General de Red.



Fuente: Autoría Propia

2.2 PREPARACIÓN DE LA MÁQUINA VIRTUAL ENDIAN.

Previo al proceso de instalación, de acuerdo al diagrama de la figura 1, se preparó la máquina virtual asignando recursos adecuados para soportar el funcionamiento del firewall, siguiendo parámetros comunes para soluciones UTM (Unified Threat Management) en entornos educativos [2]. Se definieron 2 GB de memoria RAM, dos procesadores virtuales y un disco de 20 GB, lo cual resulta suficiente para realizar filtrado de tráfico, reglas de firewall, NAT, monitoreo básico y administración web. Además, se configuraron las tres tarjetas de red, cumpliendo las recomendaciones de Endian Firewall, que establece que cada interfaz debe asociarse exclusivamente a una zona de seguridad para evitar conflictos y garantizar aislamiento adecuado del tráfico [1]. La configuración incluyó un adaptador interno para la LAN, otro interno para la DMZ y un tercero en modo NAT para la zona WAN. Esta estructura garantiza que la máquina virtual actúe como punto único de control del tráfico entre los segmentos de red definidos.

2.3 CONFIGURACIÓN DEL CLIENTE LAN Y SERVIDOR DMZ.

El cliente Ubuntu Desktop 22.04 y el servidor Ubuntu Server 22.04 fueron configurados con direcciones IP estáticas asociadas a sus respectivos segmentos de red. En el cliente LAN se asignó la dirección 172.20.10.100 con la puerta de enlace 172.20.10.1 y DNS 8.8.8.8, permitiendo su comunicación con el firewall y acceso a la interfaz web administrativa. En el servidor DMZ, la dirección se configuró mediante el archivo /etc/netplan/01-netcfg.yaml, asignando la IP 10.100.20.10 con gateway 10.100.20.1. Esta configuración corresponde a buenas prácticas de administración de redes en entornos Linux, donde se recomienda que los servidores mantengan direcciones fijas para asegurar la continuidad de los servicios, resolución de rutas y políticas del firewall [3].

Ambos equipos fueron posteriormente validados mediante comandos de red, comprobando que la asignación de direcciones y su integración dentro del esquema de seguridad funcionaban según lo previsto.

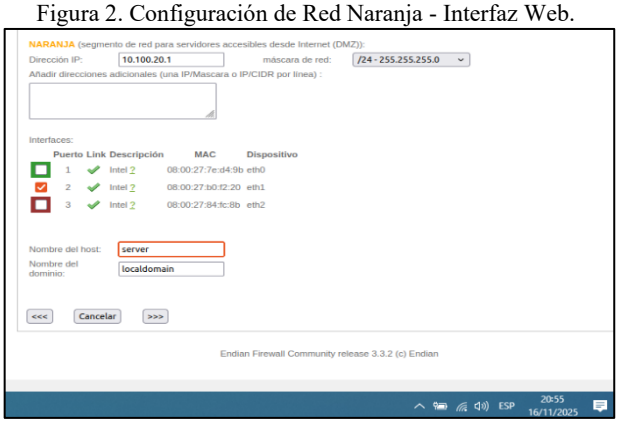
2.4 PROCESO COMPLETO DE INSTALACIÓN DE ENDIAN FIREWALL.

La instalación de Endian Firewall se llevó a cabo cargando la imagen ISO desde VirtualBox, siguiendo el asistente oficial que guía la partición del disco, instalación del sistema base y posterior configuración de la zona Verde. Durante el proceso se asignó la dirección 172.20.10.1/24 como IP principal del firewall en la red LAN, cumpliendo con lo establecido por la documentación oficial, que recomienda iniciar la configuración siempre desde la zona Verde para garantizar acceso seguro al panel administrativo [1]. Una vez finalizado el proceso de instalación, se verificó el estado del sistema mediante comandos como ip a, systemctl status y pruebas básicas de ping, confirmando que los servicios esenciales del firewall habían iniciado correctamente y que la interfaz de la zona Verde estaba operativa.

2.5 CONFIGURACIÓN DESDE LA INTERFAZ WEB.

Tras finalizar la instalación inicial, se accedió a la interfaz web del firewall desde el cliente LAN mediante la URL https://172.20.10.1:10443, procedimiento estándar indicado en la guía de administración de Endian [1]. Desde el panel web se configuró la zona Naranja, asignando la dirección 10.100.20.1/24, habilitando así el segmento DMZ para alojar el servidor Ubuntu como se muestra en la figura 2. También se realizó la actualización de las credenciales de administración, configurando usuarios root y admin con contraseñas seguras, práctica recomendada para cualquier despliegue de firewall. Finalmente, se verificó la correcta asociación de las tarjetas de red y la correspondencia entre adaptadores físicos, zonas lógicas y direcciones IP, asegurando la operación coherente del sistema perimetral.

Figura 2. Configuración de Red Naranja - Interfaz Web.



Fuente: Autoría Propia.

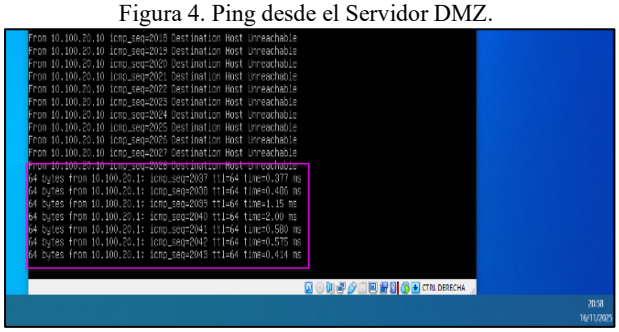
2.6 VERIFICACIÓN DE CONECTIVIDAD ENTRE ZONAS.

Una vez configuradas las tres zonas, se realizaron pruebas de conectividad que permitieron validar el correcto enrutamiento entre segmentos. Desde el cliente LAN se ejecutó la prueba ping 172.20.10.1, de acuerdo con la figura 3, confirmando que la zona Verde se encontraba operativa. Posteriormente, se probó la comunicación desde el servidor DMZ hacia su gateway mediante ping 10.100.20.1, como se puede ver en la figura 4, verificando que el firewall gestionaba adecuadamente la comunicación interna entre zonas. Estas pruebas corresponden a procedimientos estándar de validación en arquitecturas segmentadas, donde se requiere asegurar que cada zona pueda comunicarse únicamente según las políticas definidas [4]. Adicionalmente, se realizaron pruebas hacia Internet para validar que el firewall actuaba como gateway predeterminado de la red y estaba en capacidad de enrutar tráfico externo.

Figura 3. Ping desde el Cliente LAN.

Fuente: Autoría Propia.

Figura 4. Ping desde el Servidor DMZ.



Fuente: Autoría Propia.

3. TEMÁTICA 2. CONFIGURACIÓN NAT.

Para dar cumplimiento a los requerimientos de conectividad descritos en la tabla 1, a continuación se detalla el procedimiento técnico y lógico necesario para configurar la regla de traducción de direcciones de red (NAT) y validar la comunicación desde la Zona Verde (LAN) hacia la Zona Roja (WAN). Este proceso se describe asumiendo el uso del dispositivo Endian Firewall como núcleo de la gestión de red.

3.1 CONFIGURACIÓN DE INTERFACES Y PREPARACIÓN DEL ENTORNO

Antes de abordar la regla de NAT, es imperativo asegurar que las interfaces de red del dispositivo Endian estén configuradas correctamente según los identificadores de red. El proceso inicia con la definición de la Zona Verde, la cual actúa como la red de área local de confianza. Se asigna a la interfaz la dirección IP estática 172.20.10.1 con una máscara de subred de 24 bits (255.255.255.0). Esta dirección funcionará como la puerta de enlace predeterminada (Gateway) para todos los clientes dentro de este segmento.

Simultáneamente, se configura la Zona Roja (WAN). Dado que el método de conexión se describe como "NAT/Puente" y la asignación es automática, la interfaz WAN del firewall se configura en modo cliente DHCP. Esto permite que el dispositivo Endian reciba dinámicamente una dirección IP, una máscara de subred y una puerta de enlace de su proveedor de servicio o de la red simulada de Internet. Sin esta conexión WAN activa y negociada, cualquier intento posterior de enrutamiento hacia el exterior resultará fallido.

Por parte del cliente ubicado en la LAN y del servidor ubicado en la DMZ, se realiza una configuración manual o reservada para el dispositivo desktop con IP 172.20.10.100 y 10.100.20.10 para el servidor. Para que estos equipos puedan participar en la comunicación hacia el exterior, su configuración de red apunta explícitamente a la IP de la interfaz verde y naranja del firewall (172.20.10.1) y (10.100.20.1) respectivamente, como su puerta de enlace y utiliza los servidores DNS especificados (8.8.8.8) para la resolución de nombres de dominio.

3.2 CONFIGURACIÓN DE REGLAS NAT (ORIGEN NAT).

Una vez establecida la conectividad básica a nivel de interfaces, se procede a la configuración lógica de la regla de Traducción de Direcciones de Red. En el contexto de un firewall como Endian, esto se gestiona típicamente bajo el módulo de "Firewall" en la sección de "Tráfico Saliente" o "NAT". El objetivo es permitir que múltiples direcciones privadas de la red 172.20.10.0/24 y 10.100.20.1/24 compartan la única identidad pública (o externa) asignada a la interfaz WAN.

La regla 1 se construyó definiendo el "Origen" (Source) del tráfico como la Zona Verde, subred específica 172.20.10.0/24. El "Destino" se estableció como la interfaz de enlace ascendente o Zona Roja, es decir, cualquier destino en Internet. La acción configurada es NAT o Enmascaramiento (Masquerading). “Enmascaramiento es el término que se usa como referencia a un caso especial de traducción de direcciones de red (NAT, de sus siglas en ingles), NAT se utiliza para lograr que los firewall resulten utilizables”. [5].

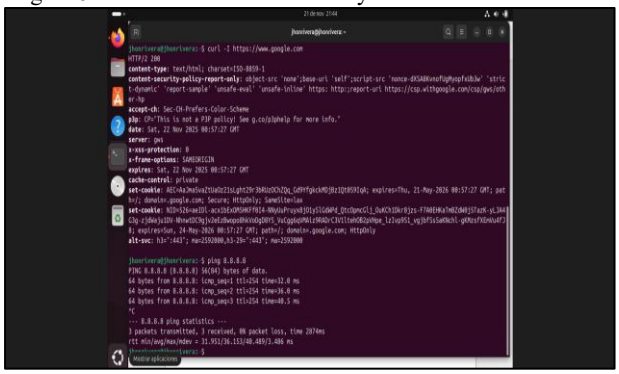
Para la regla 2 (DMZ a WAN) se replicó el procedimiento para el segmento 10.100.20.0/24, permitiendo al servidor descargar actualizaciones y mantener la conectividad externa necesaria.

Al activar el enmascaramiento, el sistema operativo del firewall modifica los encabezados de los paquetes IP que se

originan en el cliente 172.20.10.100. Cuando el paquete llega a la interfaz verde y se determina que su destino está fuera de la red local, el firewall reemplaza la dirección IP de origen privada (172.20.10.100) por su propia dirección IP asignada en la interfaz WAN (Zona Roja). Además, el firewall registra esta traducción en una tabla de estado de conexiones. Esto es crucial porque garantiza que, cuando el servidor en Internet responda, el firewall sepa a qué equipo interno debe entregar el paquete de respuesta, realizando el proceso inverso (Destination NAT automático para el tráfico de retorno).

Posterior al establecimiento de las reglas, se presenta la ejecución de comandos para verificar la conectividad de red y la accesibilidad web. Primero, el comando curl -I https://www.google.com muestra los encabezados HTTP de la respuesta del servidor de Google, indicando una conexión exitosa (HTTP/2 200). Posteriormente, el comando ping 8.8.8.8 (servidor DNS de Google) muestra una exitosa conectividad con tres paquetes transmitidos y recibidos, sin pérdida de paquetes, confirmando la conexión a internet y la resolución de nombres. Fig. 5.

Figura 5. Verificación de Conexión y Acceso Web con Cur -I



Fuente: Autoría Propia.

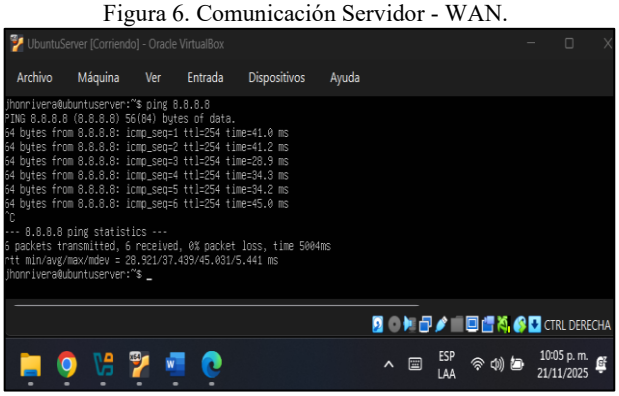
Para demostrar el establecimiento exitoso de la comunicación LAN a WAN, se analiza el flujo de un paquete de datos, como una solicitud ICMP (ping) o una petición HTTP, generado desde el cliente. El cliente (172.20.10.100) intenta acceder a un recurso externo, por ejemplo, el servidor DNS de Google (8.8.8.8).

Al comparar la IP destino con su propia máscara de subred, el cliente determina que el destino no está en su segmento local. En consecuencia, el cliente envía el paquete a su puerta de enlace configurada, que es la interfaz verde del Endian (172.20.10.1). El firewall recibe el paquete, verifica sus reglas de firewall y encuentra que el tráfico desde la Zona Verde hacia la Roja está permitido. Inmediatamente aplica la regla de NAT configurada previamente. La dirección de origen 172.20.10.100 es "enmascarada" y sustituida por la dirección IP pública que el Endian obtuvo por DHCP en su interfaz Roja. El paquete sale hacia la red simulada de Internet. Para el mundo exterior, la solicitud parece provenir exclusivamente del dispositivo Endian, protegiendo la identidad y estructura de la red interna. Cuando el servidor 8.8.8.8 responde, envía el paquete de vuelta a la IP de la interfaz Roja del Endian. El firewall consulta su tabla de conexiones, identifica que esa respuesta corresponde a la solicitud iniciada por 172.20.10.100, restaura la dirección IP privada como destino y entrega el paquete en la interfaz Verde hacia el cliente.

La confirmación final de que todo el sistema opera correctamente se evidencia cuando el cliente recibe respuesta a los comandos ping 8.8.8.8 o puede navegar por sitios web, validando así que la ruta, la resolución DNS y, fundamentalmente, la traducción de direcciones (NAT) están operando armónicamente según los parámetros establecidos.

Para la verificación del establecimiento de la comunicación desde el servidor hacia la WAN, se ejecuta el comando ping 8.8.8.8, utilizado para verificar la conectividad con el servidor DNS público de Google. El comando indica que se transmitieron y recibieron 6 paquetes, con un 0% de pérdida de paquetes, lo que confirma una conexión de red estable y funcional desde el Ubuntu Server hacia el exterior. Los tiempos de respuesta (RTT) también se muestran, proporcionando métricas de latencia. Fig. 6.

Figura 6. Comunicación Servidor - WAN.



Fuente: Autoría Propia.

3.3 PUBLICACIÓN DE SERVICIOS (DESTINO NAT)

Para habilitar el acceso desde Internet hacia el servidor web alojado en la DMZ, se aplican reglas de Destination NAT (DNAT) o reenvío de puertos.

- **Tráfico HTTP:** Redirección del puerto TCP/80 de la interfaz WAN hacia la IP interna 10.100.20.10:80.

- **Tráfico HTTPS:** Redirección del puerto TCP/443 de la interfaz WAN hacia 10.100.20.10:443.

Tras la aplicación de las reglas SNAT, se realizaron pruebas de conectividad desde los clientes internos. En la LAN, mediante el uso de la terminal de Ubuntu, se verificó la resolución de nombres y latencia hacia servidores públicos (DNS de Google 8.8.8.8), obteniendo un 0% de pérdida de paquetes y tiempos de respuesta estables. Además, el comando curl -I confirma la capacidad de establecer sesiones HTTP/2 exitosas con códigos de estado 200.

De manera similar, desde el servidor en la DMZ, se validó la salida a Internet mediante ICMP, registrando una transmisión exitosa de paquetes. Esto confirma que el mecanismo de

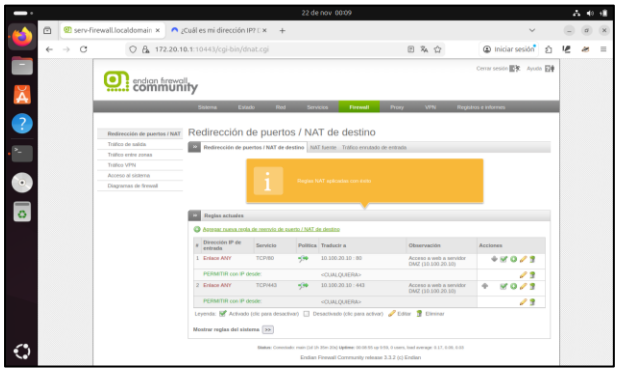
enmascaramiento está operando correctamente para ambas zonas seguras.

3.4 VALIDACIÓN DE REGLAS DE FIREWALL.

La interfaz de administración de Endian reportó la aplicación exitosa de las políticas. Las tablas de NAT evidenciaron la actividad de las reglas de traducción de origen y destino, validando la configuración lógica propuesta en el diseño. La separación de interfaces permite que, aunque la DMZ sea accesible desde el exterior (puertos 80/443), la LAN permanezca aislada de conexiones entrantes no solicitadas.

En la figura 7 se muestra la interfaz de administración web de Endian Firewall Community, específicamente en la sección de "Firewall" y "Redirección de puertos / NAT de destino". Se visualiza la aplicación exitosa de reglas NAT. Se han configurado dos reglas principales: la primera redirige el tráfico TCP/80 (HTTP) de un "Enlace ANY" para 10.100.20.10:80 para acceder a un servidor web en la DMZ. La segunda redirige el tráfico TCP/443 (HTTPS) también desde un "Enlace ANY" a 10.100.20.10:443, permitiendo el acceso seguro al mismo servidor web en la DMZ. Esta configuración ilustra cómo se gestiona la exposición de servicios internos a la red externa.

Figura 7. Redirección de Puertos (DNAT) en Endian Firewall.



Fuente: Autoría Propia.

4. TEMÁTICA 3. DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS DE TRÁFICO DE SALIDA EN LA ZONA DMZ.

El control de acceso para la Zona Naranja (DMZ) fue implementado en el firewall Endian Firewall (EFW), acatando rigurosamente el principio de mínimo privilegio [8]. Este enfoque metodológico, esencial para la seguridad por capas [1], asegura que solo se permita el tráfico estrictamente necesario. Para este propósito, el host de la DMZ (un servidor Ubuntu) se configuró con una dirección IP estática (10.100.20.10), utilizando la interfaz Naranja de EFW (10.100.20.1) como su gateway predeterminado. La Tabla 2 resume el esquema de direccionamiento IP y la asignación de roles a las interfaces del EFW.

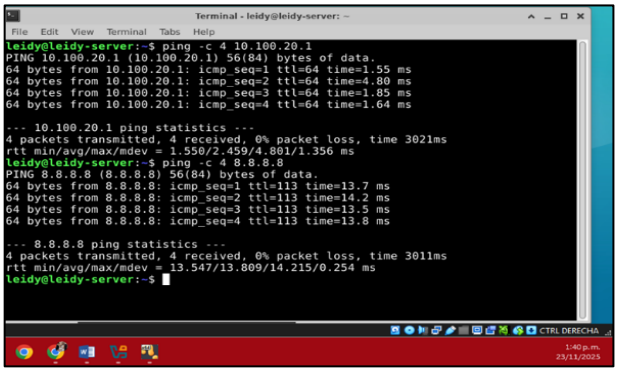
Tabla 2. Direccionamiento IP y Asignación de Roles de Interfaces

Componente	Interfaz	Rol	Dirección IP
Endian EFW (VM 1)	Adaptador 1	(Roja - WAN)	DHCP
Endian EFW (VM 1)	Adaptador 2	(Verde - LAN)	172.20.10.1/24
Endian EFW (VM 1)	Adaptador 3	(Naranja - DMZ)	10.100.20.1/24

Fuente: Autoría Propia.

Para establecer la conectividad y el rol del servidor dentro del segmento de la Zona Naranja, se utilizó la herramienta de configuración de red declarativa Netplan para asignar la dirección IP estática, asegurando su ubicación en el segmento de red (10.100.20.0/24) definido por la interfaz Naranja. La estructura de configuración de Netplan se visualiza en la Figura 8.

Figura 8. Verificación de la Conectividad de la Zona DMZ.



Fuente: Autoría Propia.

Una vez que la configuración estática fue aplicada, se procedió a verificar la conectividad de la zona, una comprobación crítica para asegurar que el servidor pudiera alcanzar el gateway (10.100.20.1) y la red WAN. La verificación inicial se realizó mediante el comando ping dirigido a la dirección del gateway y a un servidor DNS público, como el 8.8.8.8. La Figura 18 muestra el resultado exitoso de estas pruebas, confirmando la comunicación con el gateway Endian. Esta validación inicial sirvió como el primer punto de control para asegurar que la capa de red estaba funcionando correctamente antes de la implementación de las reglas de filtrado de tráfico de la cadena FORWARD.

La implementación (diseño y ejecución) de las políticas de seguridad se ejecutaron directamente en la consola de shell del firewall Endian, enfocándose en la cadena FORWARD de Netfilter.

4.1 HABILITACIÓN DE SERVICIOS CRÍTICOS.

Inicialmente, se definieron las reglas explícitas en iptables que permitieran el tráfico de los servicios críticos (HTTP en el Puerto TCP 80 y FTP en el Puerto TCP 21) desde el host DMZ (10.100.20.10) hacia la WAN. Esta configuración es vital para

asegurar la funcionalidad externa de los servicios del servidor. La Figura 9 detalla la implementación de estas directivas de permiso.

Figura 9. Políticas de Permiso (HTTP/FTP).

Fuente: Autoría Propia.

4.2 DENEGACIÓN DE RECONOCIMIENTO DE RED.

Posteriormente, y para fortificar la seguridad perimetral, fue crucial establecer una regla de denegación absoluta para el protocolo ICMP. Este bloqueo impide que cualquier paquete de sondeo, como el Echo Request (Tipo 8), sea dirigido desde la DMZ hacia la Zona Verde, neutralizando así los intentos de mapeo de la topología interna [7]. La sintaxis utilizada para esta directiva, incluida la orden para asegurar su persistencia, se captura en la Figura 10. El bloqueo del ICMP inter-zona constituye un elemento central en la estrategia de defensa en profundidad.

Figura 10. Denegación ICMP (Ping) de DMZ a LAN.

Fuente: Autoría Propia.

Finalmente, la validación de la configuración base del firewall constituyó un paso previo indispensable para el inicio de las pruebas de funcionalidad. Se verificó el correcto funcionamiento de los tres adaptadores de red configurados en el servidor Endian Firewall (EFW). Este procedimiento aseguró que cada interfaz estuviera correctamente enlazada a su zona (Roja, Verde y Naranja), garantizando que la infraestructura de red subyacente se encontraba completamente operativa antes de la ejecución de las pruebas funcionales.

La implementación de las políticas fue verificada mediante pruebas de conectividad realizadas en la consola del *host* DMZ (10.100.20.10), validando la operatividad de los permisos y la efectividad del bloqueo de tráfico.

4.3 CONECTIVIDAD Y PERMISOS DE SERVICIOS CRÍTICOS.

El tráfico para los servicios críticos fue verificado, confirmando que la regla de ACCEPT configurada en el firewall funcionó correctamente. Las pruebas de conectividad saliente para HTTP y FTP (usando curl y telnet) validaron la apertura de los puertos requeridos hacia la WAN. La Tabla 3 resume la matriz de verificación de estas políticas de tráfico de salida.

Tabla 3. Políticas de Tráfico de Salida de la Zona Dmz.

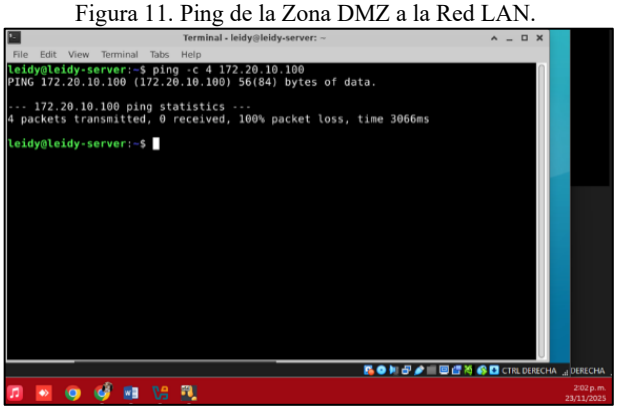
Objetivo de la Política	Protocolo / Tipo	Origen → Destino	Prueba de Verificación	Resultado Esperado
Permitir HTTP	TCP / 80	Naranja → WAN	curl -I http://[IP_WAN]	**Éxito**
Permitir FTP	TCP / 21	Naranja → WAN	telnet [IP_WAN] 21	**Éxito**
Denegar Reconocimiento	**ICMP / Tipo 8**	Naranja → Verde	ping 172.20.10.100	**Denegado**

Fuente: Autoría Propia.

4.4 PRUEBA DE DENEGACIÓN ICMP.

La prueba de la denegación de ICMP se realizó enviando tráfico de sondeo desde la DMZ (10.100.20.10) hacia un host ubicado en la Zona Verde (LAN: 172.20.10.100). La Figura 11 presenta la evidencia de esta prueba. El resultado fue un 100% de pérdida de paquetes (packet loss), lo que confirma que el firewall Endian actuó como DROP. Este éxito valida la estrategia de ocultación de red.

Figura 11. Ping de la Zona DMZ a la Red LAN.



Fuente: Autoría Propia.

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

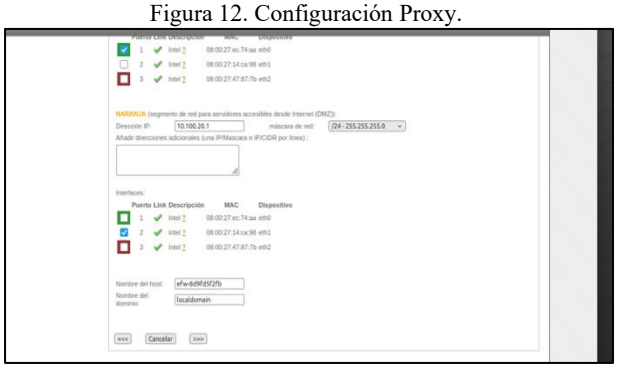
Se llevó a cabo la implementación de Endian Firewall Community 3.3.2 como solución perimetral dentro de un entorno virtualizado en VirtualBox, con el fin de estructurar y

proteger una infraestructura compuesta por tres áreas: LAN, DMZ y WAN. La elección de Endian se justifica por su capacidad para segmentar la red de manera clara y aplicar políticas de seguridad específicas a cada zona, permitiendo así un control preciso del tráfico y un aumento significativo en la seguridad del sistema.

Se inicia la máquina virtual del GNU/Linux Ubuntu Server y se verifica su configuración de red, asegurándose de que esté configurada con Red interna. Una vez iniciado el sistema operativo Ubuntu Server, se abre el navegador y se accede a la IP del servidor Endian, lo que redirigirá a la página en modo seguro.

Se presenta el asistente de configuración que corresponde a las zonas verde y naranja, en el cual se definen los parámetros de red asignados a cada interfaz. Mediante este asistente, se establece la dirección IP, la máscara de red y las configuraciones necesarias para integrar correctamente ambas interfaces, habilitando la opción de proxy para permitir un mejor control y filtrado del tráfico de dichas zonas. Fig. 12.

Figura 12. Configuración Proxy.



Fuente: Autoría Propia.

Para que los servicios HTTP y FTP, nos dirigimos a la opción proxy y habilitamos la configuración HTTP permitiendo a los puertos 80 y 21 para la zona naranja, lo que permite que le tráfico asociado a dichos servicios sea encaminado correctamente hacia los servidores en el DMZ.

Para configurar los servicios HTTP y FTP, se debe dirigir a la opción de proxy y habilitar la configuración HTTP. Esto implica permitir los puertos 80 (HTTP) y 21 (FTP) para la zona naranja, lo que asegura que el tráfico asociado a dichos servicios sea encaminado correctamente hacia los servidores ubicados en la DMZ (Zona Desmilitarizada).

A continuación, se procede a crear una nueva regla en el firewall utilizando el protocolo ICMP. En esta regla se define el servicio correspondiente para el usuario y se establece la acción de DENEGAR el acceso al puerto indicado. Esta configuración permite restringir el tráfico no autorizado y asegurar el flujo adecuado en las comunicaciones dentro de la red.

La imagen 13 muestra la interfaz de configuración de reglas Inter-Zona de un firewall, donde se añadió una nueva política para el tráfico entre zonas. Se estableció que el origen del tráfico es la dirección IP 172.20.10.1 y el destino es una de las interfaces internas (VERDE o NARANJA). El protocolo seleccionado para esta regla es ICMP.

Figura 13. Creación la Regla con la Red Verde.

Fuente: Autoría Propia.

Se configuran las reglas de reenvió de puertos accediendo a la sección Port Forwarding/Destination NAT Rule Editor. Mediante este módulo se define las direcciones necesarias para que el tráfico que proviene de la red externa sea dirigido correctamente hacia los servicios dentro de estructura interna o la zona DMZ.

Para la realizar la configuración correspondiente a la destinación NAT, se accede al módulo de edición de reglas dentro de la sección de Port Forwarding. En este apartado se define las direcciones y puertos de destino al cual se va a redirigir el tráfico. Fig. 14.

Figura 14. Reglas Creadas y Aplicadas.

Fuente: Autoría Propia.

Luego de agregar las reglas, se navega a la opción Zona/VPN y se activa el enlace WAN actual. Se le asigna el servicio FTP y, en la sección Mapear, se elige el tipo IP. Finalmente, se registra la dirección IP de la DMZ para el servicio FTP en su puerto correspondiente, permitiendo así el acceso al servicio web desde cualquier enlace WAN activo.

Posteriormente se procede a la activación del servicio VPN, lo que permite establecer conexiones seguras entre la red externa y la infraestructura interna administrada por Endian. Al habilitar este servicio, se generan los mecanismos necesarios para el cifrado y la autenticación del tráfico, garantizando así el acceso seguro únicamente a los usuarios autorizados.

Para la configuración del tráfico permitido y denegado entre las zonas, el administrador accede al apartado de reglas del firewall dentro de la interfaz de gestión. Desde este módulo, se establecen las políticas que determinan el tipo de comunicación que puede circular entre las áreas LAN, DMZ y WAN. En esta etapa se definen las reglas específicas que permiten el tráfico necesario, como los servicios autorizados de la DMZ, y se bloquea cualquier acceso no requerido o no autorizado. De esta manera, se garantiza un control estricto sobre las comunicaciones interzonal, evitando conexiones indebidas dentro de la red.

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

El desarrollo de la temática 5 se centró en la implementación y configuración de Endian Firewall Community versión 3.3.2. La plataforma fue desplegada en un entorno de máquina virtual para simular una arquitectura de red real.

La base de la infraestructura se estableció mediante un esquema de tres zonas segmentadas:

- Zona Verde (LAN): Designada para albergar a los equipos cliente.
- Zona Naranja (DMZ): Reservada para la ubicación de servidores y servicios públicos.
- Zona Roja (WAN): Interfaz de salida que proporciona la conectividad hacia la red externa (Internet).

Una vez definida la segmentación, se procedió a la configuración de las direcciones IP y se realizaron pruebas exhaustivas de conectividad entre las distintas zonas para asegurar el enrutamiento y la comunicación adecuados.

Finalmente, el núcleo de la implementación se completó con la puesta en marcha de un proxy HTTP en modo no transparente, al cual se le asociaron políticas de acceso y filtrado específicas para lograr el bloqueo selectivo de páginas web y el control granular del tráfico saliente.

6.1 INSTALACIÓN DE ENDIAN EN VIRTUALBOX.

Después del proceso de instalación, en la consola de Endian se ven los datos de red iniciales y la información de acceso, se usan para el ingreso desde la maquina cliente por así llamarle, luego, se configuro las redes de las máquinas virtuales y se ajustaron los adaptadores de red de la máquina virtual del cliente, la máquina virtual del servidor y la máquina virtual de Endian.

6.2 ACCESO A LA INTERFAZ WEB DE ENDIAN.

Tras la instalación exitosa y la configuración de red operativa de Endian Firewall, se procedió al acceso a su interfaz de gestión web (WUI).

El cliente accedió mediante un navegador a la URL HTTPS proporcionada por Endian al finalizar el proceso de instalación. El navegador emitió una advertencia de seguridad debido al uso de un certificado SSL/TLS auto firmado. Dicha advertencia fue aceptada para proceder con la conexión.

La primera interacción mostró la pantalla de bienvenida de Endian, seguida del asistente de configuración inicial online. En este asistente se realizaron los siguientes pasos esenciales:

- Aceptación de la Licencia: Se ratificaron los términos y condiciones de la licencia del software.
- Gestión de Credenciales: Se llevó a cabo la actualización y fortalecimiento de la contraseña para el usuario administrativo por defecto (admin).
- Configuración de Zonas de Red: Se realizó la parametrización de la zona roja (WAN), estableciendo la conectividad externa. Adicionalmente, se verificaron y ajustaron las configuraciones de las demás interfaces y zonas de red, asegurando la correcta segmentación del esquema de red.

Para validar la correcta instalación del firewall y el funcionamiento integral del esquema de red (LAN - DMZ - WAN), se ejecutaron pruebas de conectividad utilizando el protocolo ICMP (ping). La respuesta positiva de estas pruebas confirmó la operatividad del sistema Endian Firewall y la funcionalidad de su arquitectura de red.

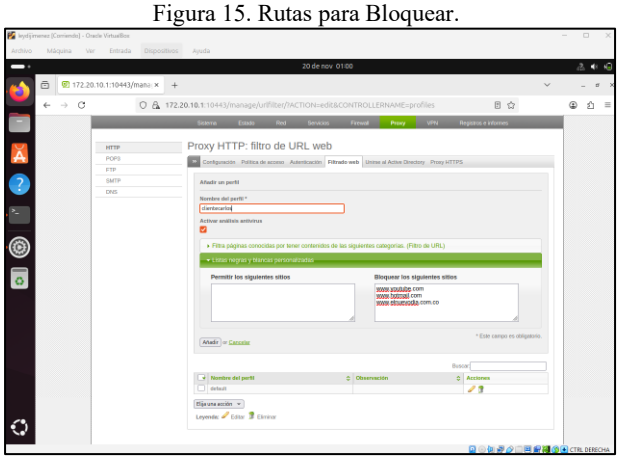
6.3 IMPLEMENTACIÓN DEL PROXY HTTP NO TRANSPARENTE.

En el marco de la temática 5, el objetivo principal fue la configuración del servicio de proxy HTTP en modo no transparente. Para ello, se inició el proceso estableciendo la configuración completa del protocolo de proxy no transparente mediante la creación de perfiles de usuario (clientes) que posteriormente serían vinculados a las reglas de acceso permitidas.

Una vez finalizada la configuración de la estructura de perfiles, se procedió a validar el bloqueo de rutas (URLs o dominios específicos). Esto se logró mediante la implementación de una política de filtrado que exige autenticación previa por parte del usuario y aplica un perfil de lista negra (blacklist).

Específicamente para la temática 5, se definieron las URLs y dominios cuya navegación debía ser restringida. Los dominios seleccionados para el bloqueo incluyeron, a modo de ejemplo, plataformas como Hotmail, YouTube, nuevodia.com, entre otros. Figura 15.

Figura 15. Rutas para Bloquear.



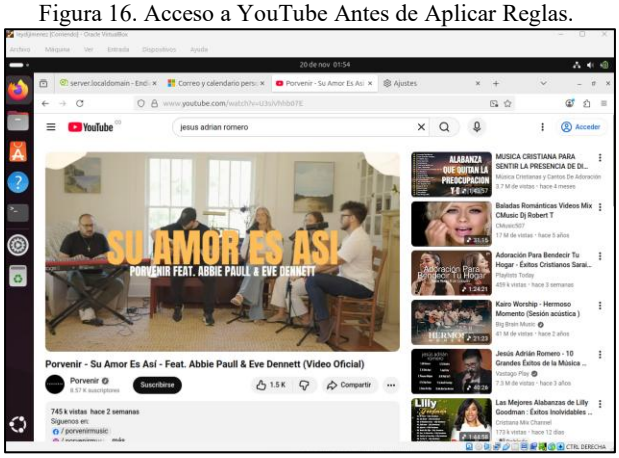
Fuente: Autoría Propia.

Para la implementación del control de acceso, se procedió a la creación de un perfil de cliente específico, el cual fue designado para aplicar la lista negra (blacklist) de dominios previamente definida.

Posteriormente, se configuró una política de acceso que exige autenticación a los usuarios y aplica de manera directa el mencionado perfil de lista negra. Esta metodología de implementación fue fundamental para realizar pruebas exhaustivas del sistema de filtrado.

Las pruebas de funcionalidad se ejecutaron bajo un esquema de verificación pre y post-bloqueo. Inicialmente, se demostró que el recurso YouTube era completamente accesible antes de la activación de las políticas de restricción. (Esta condición inicial puede ser visualizada en la Figura 16). Posteriormente, se aplicaron las políticas para confirmar la efectividad del bloqueo configurado.

Figura 16. Acceso a YouTube Antes de Aplicar Reglas.



Fuente: Autoría propia.

Una vez que el servicio de proxy HTTP no transparente y las políticas de filtrado correspondientes fueron activados, se procedió a la validación funcional desde el equipo cliente.
La prueba consistió en intentar acceder a las páginas web que habían sido incluidas en la lista negra (blacklist). Los resultados confirmaron el bloqueo efectivo de los dominios específicos:

- Se verificó el bloqueo del acceso a hotmail.com (evidenciado en la Figura 17).
- Se constató la restricción de acceso a youtube.com (mostrado en la Figura 18).
- Se observó el bloqueo al dominio nuevodia.com (confirmado en la Figura 19).

Estos resultados demuestran la operatividad integral del proxy HTTP no transparente. La funcionalidad reside en que el tráfico web del cliente es forzado a enrutarse a través del proxy configurado en el navegador, permitiendo al firewall aplicar las reglas de denegación de acceso previamente definidas con total efectividad.

Figura 17. Ruta bloqueada de Hotmail.com

Fuente: Autoría Propia

Figura 18. Ruta bloqueada de YouTube

Fuente: Autoría Propia

Figura 19. Ruta Bloqueada de Nuevodia.com

Fuente: Autoría Propia

El uso de firewalls con arquitectura perimetral por zonas (LAN, DMZ y WAN) y la implementación de proxys HTTP corresponde a los principios fundamentales de la seguridad perimetral en redes, cuyo objetivo es controlar, filtrar y monitorear el tráfico entre segmentos con diferentes niveles de confianza. Según Stallings (2021), un firewall es un sistema diseñado para establecer una barrera entre una red interna confiable y redes externas no confiables, **i**nspeccionando y regulando el tráfico mediante políticas definidas por el administrador. [9].

Dentro de este tipo de sistemas, el proxy no transparente funciona como un intermediario obligatorio entre el cliente y los servicios web, permitiendo aplicar políticas avanzadas como autenticación, control de acceso, filtrado de contenido y registro detallado del tráfico. Este enfoque coincide con lo descrito por Tanenbaum y Wetherall (2013), quienes afirman que los proxys permiten implementar mecanismos adicionales de seguridad al actuar como representantes del cliente, gestionando solicitudes HTTP antes de permitir el acceso al recurso solicitado.[10].

7. CONCLUSIONES.

7.1 CONCLUSIÓN TEMÁTICA UNO.

La configuración de la instancia de Endian Firewall en VirtualBox permitió establecer una arquitectura perimetral funcional basada en las zonas Verde, Naranja y Roja. La asignación adecuada de interfaces, direcciones IP y recursos de la máquina virtual aseguró el funcionamiento estable del firewall. La integración del cliente LAN y el servidor DMZ confirmó la correcta segmentación de la red. Finalmente, las pruebas de conectividad validaron el enrutamiento y la comunicación entre zonas, demostrando que la infraestructura quedó lista para soportar las temáticas posteriores.

7.2 CONCLUSIÓN TEMÁTICA DOS.

La implementación y configuración del dispositivo Endian Firewall validó exitosamente la eficacia de las técnicas de Traducción de Direcciones de Red (NAT) como mecanismo esencial para la gestión perimetral y la seguridad lógica de la infraestructura. A través de una estricta segmentación de zonas (LAN, DMZ y WAN) y el despliegue de políticas de enmascaramiento (SNAT) y reenvío de puertos (DNAT), se logró armonizar la conectividad saliente para los clientes internos con la publicación controlada de servicios web, garantizando tanto la optimización del direccionamiento IP como la ocultación de la topología interna frente a redes públicas.

Asimismo, las pruebas técnicas de conectividad y latencia ratifican la estabilidad operativa del diseño, demostrando que la arquitectura soporta transacciones HTTP/HTTPS y resolución de nombres con métricas de rendimiento óptimas. En conclusión, este despliegue evidencia la capacidad ingenieril para asegurar activos de información bajo el principio de defensa en profundidad, manteniendo la Zona Verde aislada de vectores de ataque externos no solicitados, mientras se asegura la alta disponibilidad y accesibilidad de los servicios alojados en la zona desmilitarizada.

7.3 CONCLUSIÓN TEMÁTICA TRES.

La implementación y verificación exitosa de las reglas de filtrado de tráfico en el firewall Endian demuestran la efectividad de la política de seguridad perimetral aplicada a la DMZ. La denegación absoluta del protocolo ICMP, evidenciada por el 100% de pérdida de paquetes durante las pruebas de sondeo, valida la correcta implementación de una política de seguridad por capas [6]. Este enfoque es fundamental en la administración de firewalls GNU/Linux, ya que previene que herramientas automatizadas de reconocimiento obtengan respuestas directas de los hosts internos de la Zona Verde. Por consiguiente, se logra mitigar activamente la superficie de ataque y se cumple rigurosamente con el principio de mínimo privilegio [8] para el tráfico de salida de la Zona Naranja, fortaleciendo significativamente la postura de seguridad global de la red.

7.4 CONCLUSIÓN TEMÁTICA CUATRO.

La configuración de las reglas para permitir o denegar el tráfico ha sido clave para establecer un control preciso sobre las comunicaciones entre las distintas áreas de la red. Al definir políticas claras sobre qué servicios podían circular entre la LAN, DMZ y WAN, se aseguró que solo el tráfico esencial tuviera autorización, mientras que las conexiones innecesarias o potencialmente peligrosas quedaran bloqueadas. En resumen, las reglas implementadas subrayan la importancia de una gestión adecuada del firewall para mantener la integridad y la seguridad del sistema.

7.5 CONCLUSIÓN TEMÁTICA CINCO.

La implementación y validación del servicio de proxy HTTP en modo no transparente, tal como se detalló en el desarrollo de la temática 5, no solo cumplió con el objetivo de control de acceso, sino que además reafirma los principios fundamentales de la seguridad perimetral de redes.

Los resultados de las pruebas de funcionalidad demostraron que el modelo de proxy no transparente es altamente eficaz para ejercer un control estricto sobre el tráfico saliente. Al forzar el enrutamiento de las peticiones HTTP a través del firewall—una característica inherente de la configuración no transparente—se habilita la aplicación obligatoria de políticas de filtrado específicas, incluyendo la autenticación y la denegación de acceso a dominios definidos en la lista negra (blacklist). La verificación del bloqueo de sitios clave (hotmail.com, youtube.com, nuevodia.com) corrobora la solidez y la operatividad integral del sistema implementado.

En conclusión, la configuración exitosa del proxy HTTP no transparente dentro de una arquitectura zonal robusta valida una metodología eficaz para mitigar riesgos asociados a la navegación web, asegurando que los recursos de red sean accesibles únicamente bajo las políticas y los criterios de seguridad definidos por el administrador. Esta práctica es indispensable para mantener la confidencialidad, integridad y disponibilidad de los activos internos.

8. REFERENCIAS.

[1] Endian. (2024). Endian Firewall Community Documentation. Endian.com. https://www.endian.com/community

[2] Oracle. (2024). VirtualBox User Manual. Oracle Corporation. https://www.virtualbox.org

[3] Canonical. (2024). Ubuntu Server Guide. Canonical Ltd. https://ubuntu.com/server/docs

[4] Stallings, W. (2021). Foundations of Modern Networking: Security, Cloud, and the Internet of Things. Pearson.

[5] Camargo Cruz, A., Eleno Hernández L, C., Palomares Arellano E. (Agosto 2026). Diseño y Restructuración de LAN del IIM, con uso del Firewalls, VLAN's y WIFI. Pp. 99. Tomado de: https://tesiunamdocumentos.dgb.unam.mx/pd2006/0607351/0607351.pdf

[6] Dadheech, K., Choudhary, A., & Bhatia, G. (2018, April). De-militarized zone: A next level to network security. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 595-600). IEEE.

[7] McNab, C. (2007). Network security assessment: know your network. " O'Reilly Media, Inc.".

[8] Enrıquez, E. B., & de la Fraga, L. G. Seguridad y Configuracion de Redes de Computadoras con GNU/Linux.

[9] Stallings, W. (2021). Network security essentials: Applications and standards (7th ed.). Pearson.

[10] Tanenbaum, A. S., & Wetherall, D. J. (2013). Computer networks (5th ed.). Pearson.