Implementación de seguridad y segmentación de redes en GNU/Linux utilizando Endian Firewall

Keidys Mercedes Vanegas Guzmán
kmvanegasgu@unadvirtual.edu.co
Karen Margarita Ayala Segura
kmayalas@unadvirtual.edu.co
Heimy Katrin Acosta Cardenas
hkacostac@unadvirtual.edu.co
Juan José Polo Rivas
jjpolor@unadvirtual.edu.co
Jesús Daniel Bueno Benitez
jdbuenobe@unadvirtual.edu.co

RESUMEN: *este artículo presenta la implementación de un entorno seguro de red basado en GNU/Linux utilizando Endian Firewall Community en un entorno virtualizado mediante Oracle VirtualBox. Durante el desarrollo se configuraron zonas WAN, LAN y DMZ, además de políticas NAT, reglas interzona y servicios HTTP y FTP para controlar el tráfico entre segmentos de red. Asimismo, se realizaron pruebas de conectividad y validación de acceso entre clientes y servidores ubicados en diferentes zonas, permitiendo evidenciar el funcionamiento de las políticas de seguridad implementadas. Los resultados obtenidos demuestran la importancia de la segmentación de redes y del uso de firewalls en entornos Linux para mejorar la administración y protección de la infraestructura tecnológica.*

PALABRAS CLAVES: GNU/Linux, Endian Firewall, NAT, DMZ, VirtualBox, Seguridad de Redes.

ABSTRACT: *This article presents the implementation of a secure network environment based on GNU/Linux using Endian Firewall Community within a virtualized environment via Oracle VirtualBox. Throughout the development, WAN, LAN, and DMZ zones were configured, along with NAT policies, interzona rules, and HTTP and FTP services to control traffic between network segments. Furthermore, connectivity testing and access validation were conducted between clients and servers located in different zones, demonstrating the effectiveness of the implemented security policies. The results obtained highlight the importance of network segmentation and the use of firewalls in Linux environments to improve the administration and protection of technological infrastructure.*

KEYWORDS: GNU/Linux, Endian Firewall, NAT, DMZ, VirtualBox, Network Security.

1. INTRODUCCIÓN

La seguridad informática constituye uno de los pilares fundamentales en la administración de infraestructuras tecnológicas modernas, especialmente en entornos donde es necesario garantizar la protección de la información, la disponibilidad de los servicios y el control del tráfico de red. En este contexto, los sistemas GNU/Linux se destacan por ofrecer estabilidad, flexibilidad y una amplia variedad de herramientas orientadas a la gestión y seguridad de redes empresariales [1].

El presente artículo describe la implementación de un entorno de seguridad utilizando Endian Firewall Community en un laboratorio virtualizado mediante Oracle VirtualBox. Para el desarrollo de la práctica se configuraron zonas de red WAN, LAN y DMZ, permitiendo establecer mecanismos de segmentación, filtrado y control de tráfico entre diferentes segmentos de comunicación [2].

Asimismo, se implementaron políticas NAT, reglas interzona y restricciones de acceso para protocolos específicos, permitiendo controlar la comunicación entre clientes y servidores ubicados en distintas zonas de red. Adicionalmente, se realizaron pruebas de conectividad y validación de servicios HTTP y FTP utilizando Ubuntu Server y Linux Mint, evidenciando el correcto funcionamiento de las políticas de seguridad implementadas [3].

Finalmente, las pruebas desarrolladas permitieron comprender la importancia del uso de firewalls y mecanismos de segmentación dentro de infraestructuras GNU/Linux, fortaleciendo conocimientos relacionados con virtualización, administración de servicios y seguridad informática en entornos controlados.

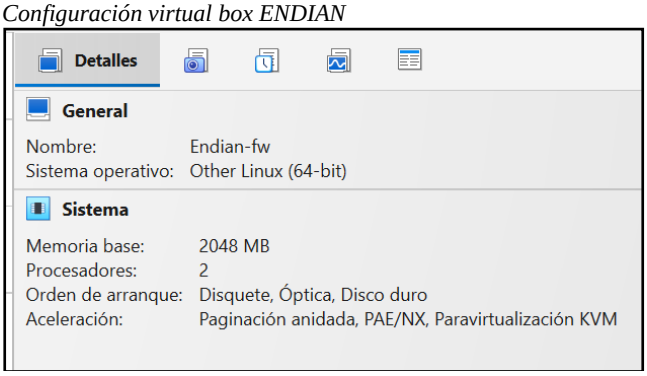
2. TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

La implementación de GNU/Linux Endian sobre Oracle VirtualBox permitió desarrollar un entorno virtualizado orientado a la administración y protección de redes. La máquina

virtual fue configurada utilizando una imagen ISO de Endian Firewall Community como se ilustra en la Fig. 1, asignando 2 GB de memoria RAM y un disco duro virtual de 20 GB [1].

El aspecto más importante de la configuración correspondió a la administración de interfaces de red. Para ello, se configuraron tres adaptadores virtuales: un adaptador en modo puente para la zona WAN (RED) y dos adaptadores de red interna para las zonas LAN (GREEN) y DMZ (ORANGE), permitiendo segmentar el tráfico y controlar la comunicación entre redes [2].

Figura. 1.
Configuración virtual box ENDIAN



Fuente: Autoría propia

2.1. ESQUEMA DE CONFIGURACIÓN INICIAL

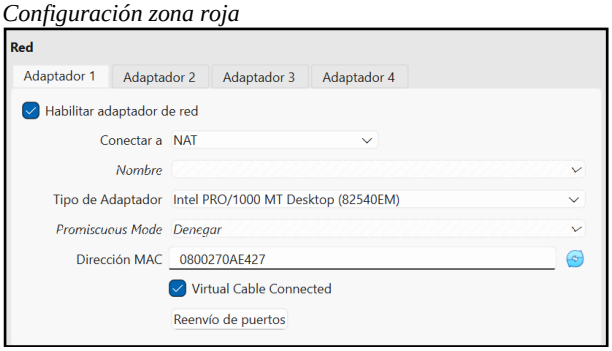
El proceso de instalación se desarrolló desde el arranque de la imagen ISO hasta la configuración inicial del firewall mediante la interfaz web administrativa. Posteriormente, se validó el acceso al portal seguro de administración a través de la dirección https://192.168.0.15:10443.

Durante la implementación de la zona DMZ se presentaron inconvenientes relacionados con el reconocimiento inicial de interfaces virtuales; sin embargo, dichos problemas fueron solucionados mediante la reasignación correcta de adaptadores dentro de VirtualBox, permitiendo establecer conectividad estable con los servidores ubicados en la DMZ [2].

2.2. CONFIGURACIÓN ZONAS DE RED

La configuración del firewall se fundamentó en un modelo de segmentación por zonas, donde cada color representa un nivel de confianza dentro de la infraestructura de red implementada [1].Zona Roja (WAN): Se configura como la interfaz de entrada orientada a la red externa o Internet como se ilustra en la Fig. 2, en el entorno virtualizado previamente configurado, esta se establece mediante un "Adaptador Puente", permitiendo que el firewall obtenga una dirección IP para la salida de datos y la recepción de tráfico externo controlado.

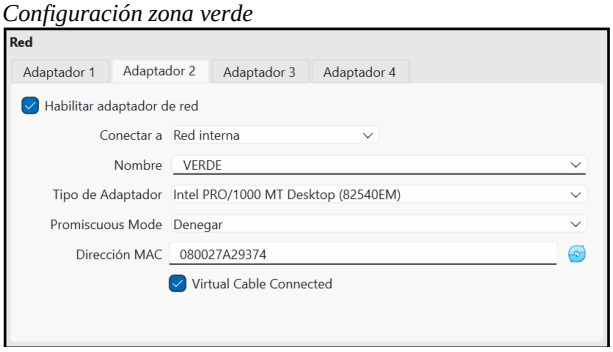
Figura 2.
Configuración zona roja



Fuente: Autoría propia

Zona Verde (LAN): Es el segmento de mayor confianza, destinado a la red interna privada. Se configura con un direccionamiento estático para actuar como puerta de enlace de los clientes locales como se ilustra en la Fig. 3, Es a través de esta zona que se habilita el acceso al portal administrativo.

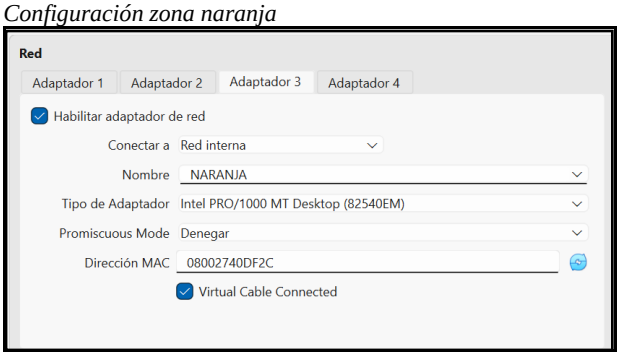
Figura 3.
Configuración zona verde



Fuente: Autoría propia

Zona Naranja (DMZ): Esta zona se reserva para los servidores que deben ser accesibles desde el exterior pero que requieren aislamiento de la red interna. Su configuración técnica implica la habilitación de una red interna dedicada como se ilustra en la Fig. 4, garantizando que, en caso de verse comprometido un servidor en la DMZ, la Zona Verde se mantendrá protegida.

Figura 4.
Configuración zona naranja



Fuente: Autoría propia

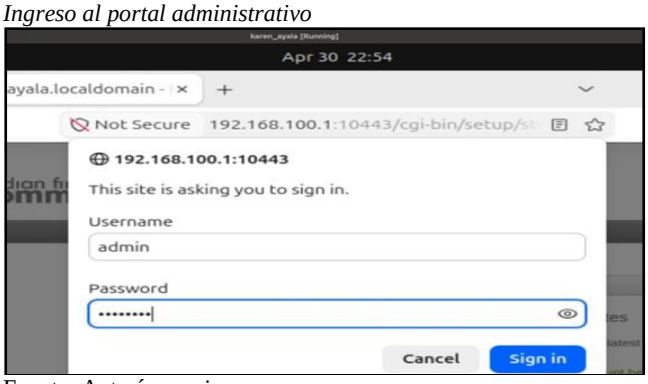
2.3. RESULTADOS

En la actualidad la implementación de la ciberseguridad dentro de un sistema junto a la configuración de firewalls es esencial para mitigar riesgos. El uso de distribuciones Linux especializadas como Endian permitió implementar soluciones de Gestión Unificada de Amenazas (UTM) con alta flexibilidad [6].

Este trabajo se centra en la configuración técnica de una instancia de Endian en un entorno controlado mediante virtualización, analizando la segmentación de tráfico por colores (zonas) y validando la operatividad de cada interfaz. Se validó con éxito la segmentación de red mediante la asignación de tres adaptadores en VirtualBox, logrando la independencia de las zonas Roja (WAN), Verde (LAN) y Naranja (DMZ).

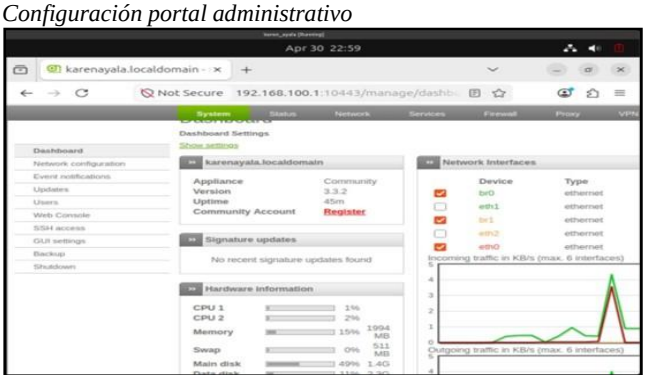
Pruebas de conectividad demostraron un acceso estable al portal administrativo a través de la interfaz segura (192.168.0.15:10443) como se ilustra en la Fig. 5 y Fig. 6, asimismo, se superaron las limitaciones iniciales de reconocimiento de hardware en la DMZ mediante ajustes en el instalador, garantizando el flujo de datos hacia los servidores aislados.

Figura 5.
Ingreso al portal administrativo



Fuente: Autoría propia

Figura 6.
Configuración portal administrativo



Fuente: Autoría propia

3. TEMÁTICA 2: CONFIGURACIÓN NAT

El diseño de una arquitectura de red perimetral segura exige no solo la división física o lógica de los entornos, sino también la gestión estratégica del direccionamiento IP para proteger la infraestructura interna de amenazas externas. En este contexto, la Traducción de Direcciones de Red (NAT, por sus siglas en inglés) se establece como un mecanismo fundamental para ocultar el direccionamiento privado de la organización bajo un conjunto limitado de direcciones públicas, optimizando los recursos y añadiendo una capa esencial de seguridad ofuscada [4], [10].

Para garantizar un control de acceso granular, la implementación de políticas NAT debe complementarse con una segmentación estricta orientada al principio de defensa en profundidad. La distribución del tráfico a través de zonas especializadas, tales como la red de área local (LAN), la red de área amplia (WAN) y una zona desmilitarizada (DMZ), permite aislar los servicios expuestos públicamente de los datos corporativos críticos [5], [9]. A continuación, se detalla el procedimiento técnico llevado a cabo en el cortafuegos perimetral para parametrizar y validar estas directrices de enrutamiento y seguridad.

4. IMPLEMENTACIÓN DE POLÍTICAS NAT

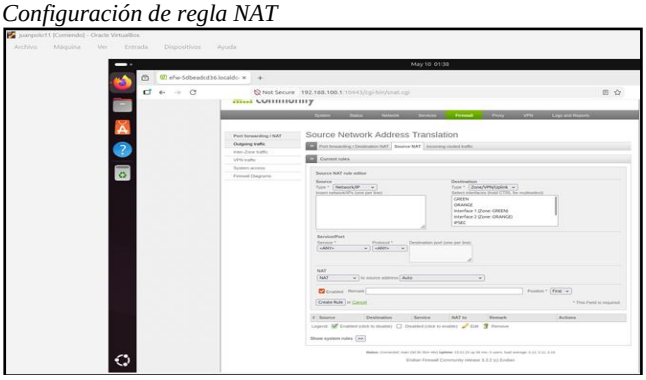
La integración del firewall perimetral Endian [1] permitió validar de manera práctica la segmentación lógica de la infraestructura mediante la parametrización de las zonas WAN (red externa), LAN (red interna) y DMZ (zona desmilitarizada) dentro del entorno virtualizado. Durante esta fase, las pruebas de conectividad interzonal evidenciaron un comportamiento estable y correcto, confirmando tanto la accesibilidad del portal administrativo como la efectiva ejecución de las políticas de filtrado y las directrices de enrutamiento previamente configuradas.

Asimismo, la adopción de esta plataforma basada en GNU/Linux demostró ser una alternativa robusta y eficiente para consolidar mecanismos de Gestión Unificada de Amenazas (UTM). El despliegue de estas reglas no solo optimizó el flujo de paquetes entre los diferentes segmentos, sino que también fortaleció la administración centralizada y los esquemas de seguridad perimetral dentro de la red virtual de pruebas.

5. VALIDACIÓN DE REGLAS NAT

La siguiente Fig. 7, muestra la creación de una regla de traducción de direcciones NAT (Source Network Address Translation) dentro de la plataforma GNU/Linux Endian Firewall. En esta configuración se define el tráfico proveniente de la red interna GREEN con destino hacia la interfaz RED, permitiendo que los equipos de la LAN puedan acceder a redes externas mediante la traducción de direcciones IP privadas a una dirección pública administrada por el firewall.

Figura 7.
Configuración de regla NAT



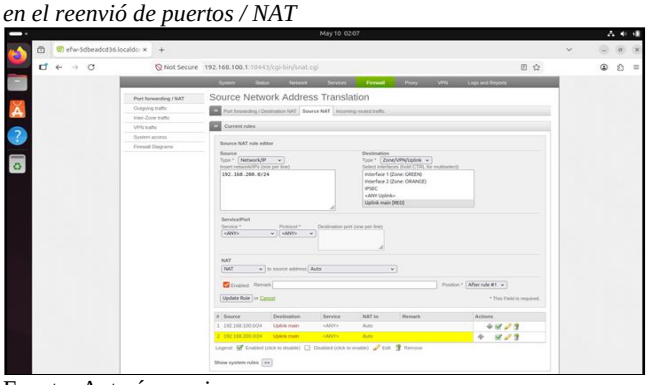
Fuente: Autoría propia

Se muestra en la Fig. 8, la interfaz administrativa de Endian Firewall después de crear correctamente una regla de traducción de direcciones NAT (Source NAT). En la sección "Current rules" se observa la regla habilitada para la red interna 192.168.100.0/24 con salida hacia la interfaz "Uplink main", permitiendo que los dispositivos de la LAN accedan a redes externas mediante la traducción de direcciones IP privadas.

Figura 8.
Aplicación y validación de la regla NAT

Fuente: Autoría propia

Figura 9.
Aplicación de la regla NAT demostrando el establecimiento de la comunicación de la zona DMZ hacia la internet, verificar en el reenvió de puertos / NAT



Fuente: Autoría propia

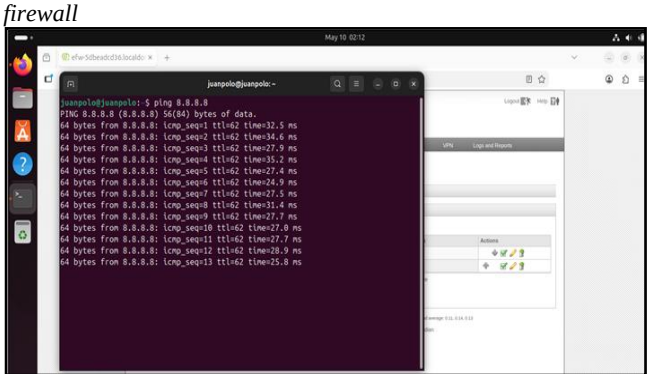
6. PRUEBAS DE CONECTIVIDAD

La Fig. 10, presenta las reglas Source NAT configuradas en GNU/Linux Endian Firewall para permitir la salida de tráfico de las redes internas 192.168.100.0/24 y 192.168.200.0/24 hacia la interfaz WAN. Estas reglas permiten que los dispositivos de la LAN y la DMZ puedan acceder a redes externas mediante traducción de direcciones IP privadas.

Figura 10.
Reglas NAT habilitadas en endian firewall para el acceso de las redes LAN y DMZ hacia la WAN

Fuente: Autoría propia

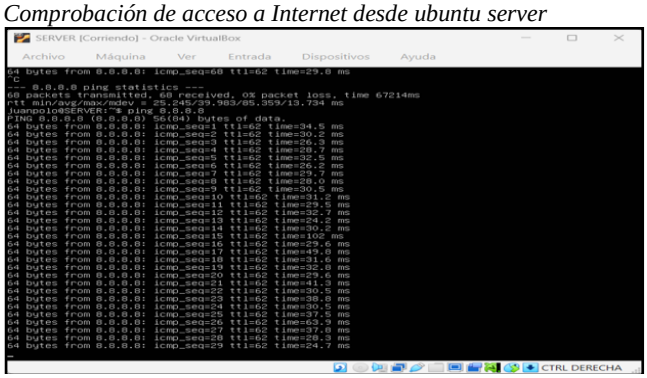
Figura 11.
Validación de conectividad a Internet desde ubuntu desktop mediante pruebas ICMP después de configurar NAT en endian firewall



Fuente: Autoría propia

La Fig. 12, evidencia la validación de conectividad realizada desde Ubuntu Desktop mediante el comando ping hacia la dirección 8.8.8.8. Los resultados exitosos confirman el correcto funcionamiento de las reglas NAT configuradas en Endian Firewall y el acceso de la red interna hacia Internet.

Figura 12.
Comprobación de acceso a Internet desde ubuntu server



Fuente: Autoría propia

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

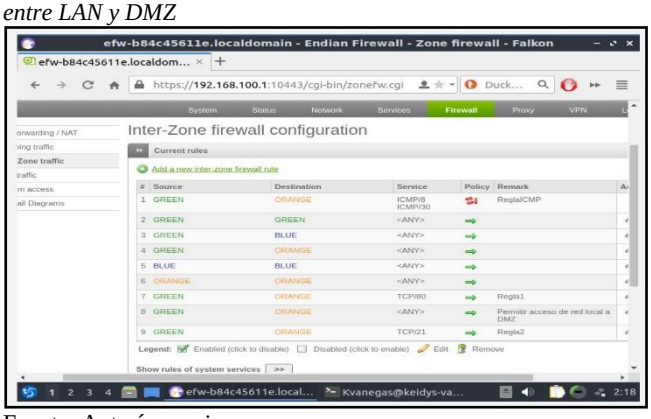
En esta sección se presentan las políticas de seguridad implementadas para controlar la comunicación entre la red LAN y la zona DMZ mediante el uso del firewall Endian. Las configuraciones realizadas permitieron habilitar servicios específicos para la comunicación entre cliente y servidor, así como restringir protocolos no autorizados con el fin de fortalecer la seguridad de la red. La implementación de una DMZ permite aislar los servicios públicos de los recursos críticos de la red interna [4].

7.1. CONFIGURACIÓN DE POLÍTICAS DE ACCESO

La primera fase consistió en la creación de reglas que autorizaran el acceso desde la red LAN hacia los servicios alojados en la DMZ. La configuración de políticas se basó en el modelo de gestión unificada de amenazas (UTM) proporcionado por la distribución Endian [6]. Como se ilustra en la Fig. 13 se habilitó el tráfico correspondiente al protocolo HTTP sobre el puerto 80, permitiendo el acceso a servicios web desde el cliente hacia el servidor. Asimismo, se configuró una política adicional para habilitar el protocolo FTP a través del puerto 21, facilitando la transferencia de archivos entre ambas zonas de red esto siguiendo las recomendaciones de segmentación de red para entornos virtualizados [2].

Se implementó una política de restricción para el protocolo ICMP. Esta medida es una práctica estándar de endurecimiento (hardening), este endurecimiento del sistema sigue las recomendaciones de seguridad para servidores de propósito general [5]. para reducir la visibilidad del servidor y mitigar posibles ataques de reconocimiento de red [1]. Al organizar las reglas como se ilustra en la Fig. 13, se aseguró que las políticas de denegación tuvieran prioridad sobre las de acceso para garantizar la integridad del filtrado

Figura 13.
Reglas configuradas en el firewall para el control de tráfico entre LAN y DMZ



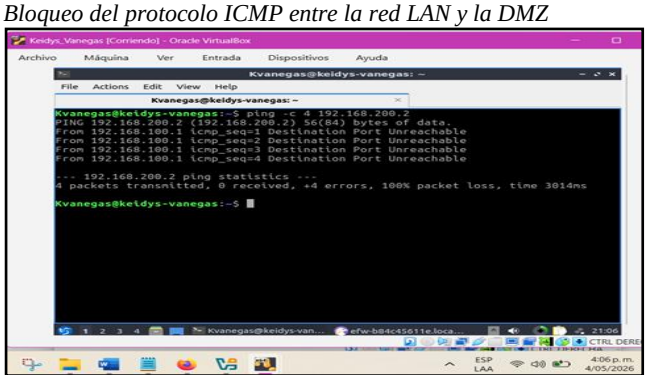
Fuente: Autoría propia

7.2. PRIORIZACIÓN Y APLICACIÓN DE REGLAS

Durante la implementación de las políticas de seguridad, se identificó la importancia del orden de ejecución de las reglas dentro del firewall. Inicialmente, la existencia de una política general de permiso impedía el correcto funcionamiento de la restricción ICMP. Por esta razón, fue necesario reorganizar las reglas, ubicando la política de denegación en una posición prioritaria dentro de la tabla de filtrado.

Esta configuración permitió que el firewall evaluara primero la restricción del protocolo ICMP antes de aplicar las reglas de acceso autorizadas para HTTP y FTP, garantizando así el cumplimiento efectivo de las políticas establecidas como se ilustra en la Fig. 14.

Figura 14.
Bloqueo del protocolo ICMP entre la red LAN y la DMZ



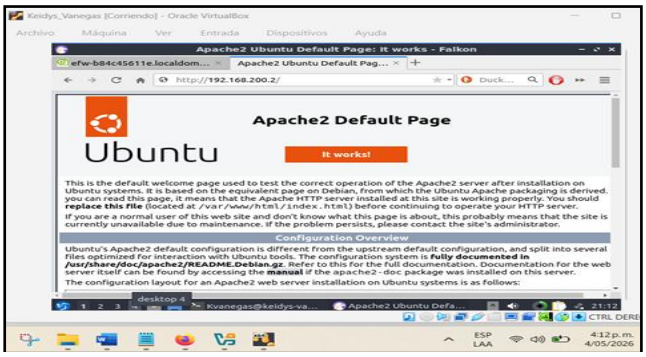
Fuente: Autoría propia

7.3. VALIDACIÓN DE RESULTADOS

Con el fin de verificar el comportamiento de las políticas implementadas, se realizaron pruebas de conectividad desde el cliente hacia el servidor ubicado en la DMZ. Los resultados evidenciaron que las solicitudes ICMP fueron rechazadas correctamente como se ilustra en la Fig. 14, impidiendo el uso del comando ping entre las redes.

De igual forma, se comprobó el acceso exitoso a los servicios HTTP y FTP como se ilustra en la Fig. 15, demostrando que las políticas de acceso configuradas permitieron la comunicación únicamente para los servicios autorizados. Finalmente, mediante el monitoreo de los registros del firewall, fue posible validar el tráfico permitido y bloqueado, confirmando el funcionamiento adecuado de las reglas implementadas.

Figura 15.
Validación del acceso permitido al servicio HTTP desde la red LAN hacia la DMZ



Fuente: Autoría propia

La implementación de reglas de filtrado permitió controlar de manera eficiente el tráfico entre la LAN y la DMZ, garantizando el acceso únicamente a los servicios necesarios y restringiendo protocolos no autorizados. Este ejercicio permitió comprender la importancia de definir políticas de seguridad adecuadas dentro de un firewall, así como el impacto que tiene el orden de prioridad de las reglas en el comportamiento del sistema.

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

La seguridad perimetral se fundamenta en la capacidad de filtrar y controlar el flujo de datos entre segmentos de red con distintos niveles de confianza. En esta sección, se detalla el despliegue de políticas de seguridad aplicadas sobre el firewall Endian para gestionar la interacción entre la red interna y la zona desmilitarizada. El objetivo principal es mitigar riesgos de intrusión mediante la aplicación del principio de menor privilegio, permitiendo únicamente el tráfico estrictamente necesario para la operación de los servicios web y de transferencia de archivos.

8.1. CONFIGURACIÓN DEL ENTORNO VIRTUALIZADO

En esta etapa se implementaron políticas de seguridad utilizando Endian Firewall Community con el objetivo de controlar la comunicación entre la red LAN (GREEN) y la zona DMZ (ORANGE). Para ello, se configuraron reglas interzona que permitieron habilitar el acceso HTTP desde la LAN hacia el servidor Ubuntu ubicado en la DMZ, cumpliendo con los lineamientos establecidos en la guía de aprendizaje del diplomado.

Inicialmente, se configuró el entorno virtualizado utilizando Oracle VirtualBox, implementando tres máquinas virtuales principales:

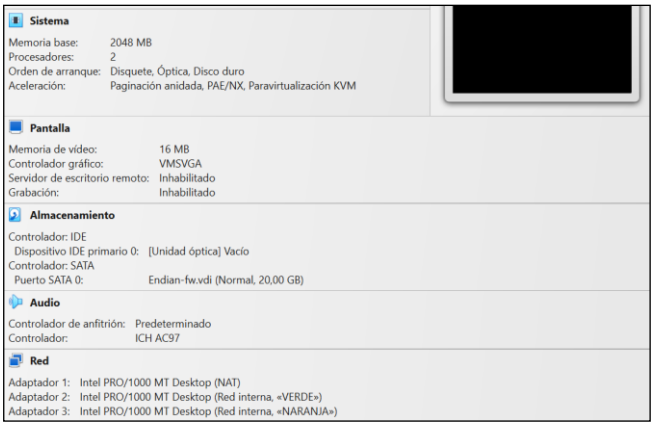
- Endian Firewall Community
- Ubuntu Server
- Linux Mint

El firewall fue configurado con tres interfaces de red virtuales correspondientes a las zonas GREEN, ORANGE y RED. La zona GREEN fue utilizada para representar la red LAN interna con direccionamiento 192.168.100.1/24, mientras que la zona ORANGE fue destinada a la DMZ utilizando el direccionamiento 192.168.200.1/24.

Esta segmentación permitió controlar de forma independiente el tráfico entre usuarios internos y los servicios publicados dentro de la DMZ, aplicando políticas específicas de acceso y filtrado [2].

Además, el uso de VirtualBox permitió simular una infraestructura de red empresarial en un entorno controlado y seguro, facilitando las pruebas de conectividad, segmentación y administración del firewall.

Figura 16.
Configuración del entorno virtualizado y segmentación de redes en virtualBox.



Fuente: autoría propia

8.2. CONFIGURACIÓN DEL SERVIDOR EN LA DMZ

Posteriormente, se implementó un servidor Ubuntu Server dentro de la zona desmilitarizada o ORANGE (DMZ). Este equipo se configuró con el direccionamiento IP estático 192.168.200.2/24, estableciendo como puerta de enlace predeterminada la dirección 192.168.200.1, la cual corresponde a la interfaz ORANGE de Endian Firewall como se ilustra en la Fig. 18.

La adopción de un esquema estático garantizó la estabilidad en la comunicación dentro de la infraestructura de red, lo que a su vez facilitó la administración de las reglas de acceso y la publicación de servicios [3].

En el servidor Ubuntu se desplegó el servicio Apache2 para habilitar un entorno web accesible desde la red LAN mediante el protocolo HTTP. Esta configuración fue fundamental para validar posteriormente el comportamiento de las reglas interzona programadas en el firewall.

Finalmente, se realizaron pruebas de verificación mediante el comando ip a, comprobando la correcta asignación

de las direcciones IP y el estado operativo de la interfaz de red del servidor.

Figura 17.
Configuración del servidor ubuntu y direccionamiento IP en la zona ORANGE (DMZ)

Fuente: Autoría propia

8.3. CREACIÓN DE REGLAS INTERZONA

Con el objetivo de garantizar una comunicación controlada y segura entre la red de área local (LAN) y la zona desmilitarizada (DMZ), se diseñaron e implementaron reglas de acceso interzona dentro de la plataforma Endian Firewall Community [1]. La interconexión de estos segmentos requiere un control estricto de los flujos de tráfico, asegurando que los recursos críticos de la infraestructura no queden expuestos de manera innecesaria y que se mantenga el principio de menor privilegio en el perímetro de la red.

La política configurada fue diseñada específicamente para permitir el tráfico TCP correspondiente al servicio HTTP (puerto 80) originado desde la zona GREEN (LAN) con destino hacia la zona ORANGE (DMZ) como se ilustra en la Fig. 19, esta regla en particular habilita el acceso de los usuarios y clientes internos de la organización hacia el servidor web alojado de forma aislada en la DMZ, impidiendo de forma predeterminada cualquier otro tipo de conexión que no haya sido explícitamente autorizada.

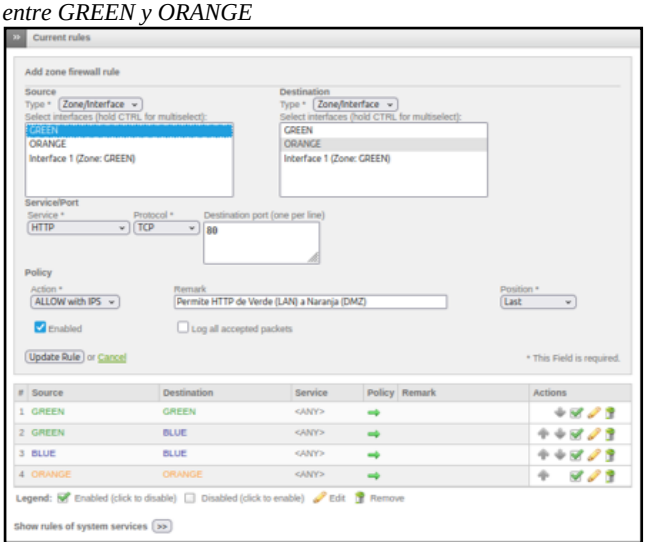
Durante el proceso de despliegue y auditoría de la política en el cortafuegos, se parametrizaron las siguientes variables técnicas dentro de la tabla de reglas de acceso:

- **Source (Origen):** GREEN (Segmento seguro de la LAN interna)
- **Destination (Destino):** ORANGE (Zona desmilitarizada o DMZ donde residen los servicios públicos)
- **Service (Servicio):** HTTP (Protocolo de transferencia de hipertexto)
- **Protocol (Protocolo de Transporte):** TCP (Protocolo de Control de Transmisión)
- **Destination Port (Puerto de Destino):** 80 (Puerto estándar para tráfico web no cifrado)
- **Policy (Acción de la Política):** ALLOW (Permitir el paso del paquete)

La implementación de reglas de acceso sumamente específicas, basadas en criterios de origen, destino y puertos bien definidos, constituye una práctica de ingeniería fundamental en la administración y el endurecimiento (hardening) de firewalls. Como señala Stallings [4], la inspección detallada del tráfico permite limitar y filtrar la comunicación únicamente a los servicios estrictamente esenciales para la operación de la infraestructura, bloqueando vectores de ataque comunes y reduciendo la superficie de vulnerabilidad del sistema.

Asimismo, la estrategia de segmentación por zonas adoptada cumple con las directrices internacionales de seguridad. De acuerdo con la guía de seguridad general para servidores del NIST (SP 800-123) [5], aislar los servidores que prestan servicios a la red en una zona aislada como la ORANGE mitiga significativamente la exposición de los activos internos frente a eventuales compromisos de seguridad. Si un atacante lograse vulnerar el servidor web, la segmentación interzona de Endian evita el movimiento lateral hacia la zona GREEN, facilitando al mismo tiempo el monitoreo, la contención de incidentes y el análisis forense del tráfico de red.

Figura 18.
Configuración de regla interzona para permitir acceso HTTP entre GREEN y ORANGE



Fuente: Autoría propia

8.4. VALIDACIÓN DE ACCESO HTTP

Posteriormente a la configuración e implementación de las políticas de seguridad interzona en el cortafuegos, se procedió a la fase de pruebas y auditoría de conectividad. Esta validación se ejecutó con el propósito de corroborar el correcto enrutamiento y filtrado de paquetes desde un host cliente basado en el sistema operativo Linux Mint (ubicado en el segmento seguro de la red LAN / Zona GREEN) hacia el servidor web Apache2, el cual se encuentra debidamente desplegado e instalado en el sistema operativo Ubuntu Server dentro de la zona perimetral aislada (DMZ / Zona ORANGE).

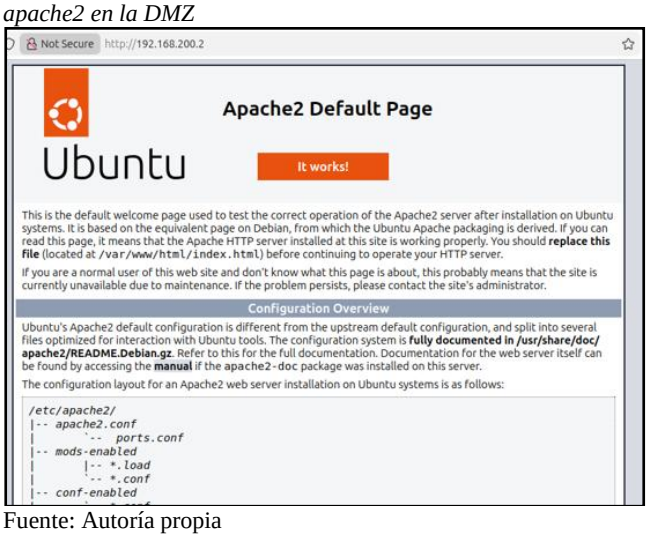
Para llevar a cabo la verificación del servicio en la capa de aplicación, se empleó el navegador web Mozilla Firefox desde la estación de trabajo del cliente. Mediante este entorno gráfico, se realizó una petición HTTP dirigida explícitamente hacia la dirección IP privada del servidor web: http://192.168.200.2

La solicitud se completó de manera exitosa, logrando visualizar en pantalla la interfaz de la página predeterminada de Apache2 (Apache2 Ubuntu Default Page). Este resultado técnico demuestra que el protocolo de enlace de tres vías (three-way handshake) de TCP logró consolidarse de manera transparente a través del firewall sin interrupciones ni bloqueos en el puerto de destino como se ilustra en la Fig. 20.

Los resultados empíricos obtenidos durante esta fase de validación práctica permitieron comprobar de forma concluyente los siguientes hitos de infraestructura:

- Operatividad óptima del firewall: Se demostró la capacidad de la plataforma Endian para procesar, conmutar y validar las tablas de enrutamiento de red bajo condiciones reales de carga de tráfico.
- Aplicación efectiva de las reglas interzona: Se validó que el motor de filtrado del cortafuegos inspecciona y permite de forma selectiva las peticiones que cumplen rigurosamente con los criterios de seguridad previamente establecidos en la matriz de acceso.
- Conectividad bidireccional controlada entre LAN y DMZ: Se constató el establecimiento exitoso de canales de comunicación entre los segmentos GREEN y ORANGE, restringiendo cualquier intento de comunicación no explícita y aislando los dominios de difusión.
- Acceso gobernado a servicios web corporativos: Se ratificó el cumplimiento del diseño de seguridad perimetral, logrando que el servidor exponga sus servicios a los usuarios de la red interna de manera totalmente controlada y dentro de una infraestructura lógicamente segmentada.

Figura 19.
Validación de acceso HTTP desde linux mint hacia el servidor apache2 en la DMZ

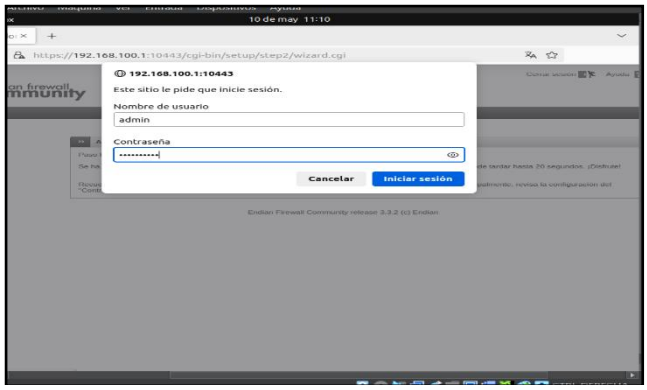


Fuente: Autoría propia

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

Configuramos el acceso al panel administrativo de Endian mediante autenticación web segura. Esta validación confirma el correcto funcionamiento del servicio de administración del firewall y permite continuar con la configuración de políticas de seguridad, filtrado y control de acceso como se ilustra en la Fig. 21.

Figura 20.
Validación de inicio de sesión correctamente a endian



Fuente: Autoría propia

9.1. CREAR PERFIL CON LISTA NEGRA

Se llevó a cabo la parametrización y aplicación de una directriz de filtrado de contenido web a nivel de aplicación (Capa 7). Mediante el módulo de proxy HTTP integrado en Endian, se estructuró un perfil de navegación restrictivo diseñado para denegar el acceso a dominios específicos —tales como Hotmail, YouTube y El Nuevo Día— a través de la implementación de una lista negra personalizada, tal como se ilustra en la Fig. 22, esta regla de filtrado URL se vinculó directamente a una política de autenticación orientada a regular las solicitudes de navegación de los usuarios pertenecientes a la red local (zona GREEN).

La integración de servicios proxy de almacenamiento en caché y filtrado web de código abierto constituye una estrategia crucial en los esquemas modernos de Gestión Unificada de Amenazas (UTM). Este tipo de control granular no solo optimiza el uso del ancho de banda institucional, sino que también complementa las tareas tradicionales de detección y prevención de intrusos a nivel de red, mitigando la exposición de la infraestructura interna a vectores de ataque basados en la web y asegurando el cumplimiento de las políticas de uso aceptable de los recursos de red [1], [6], [9].

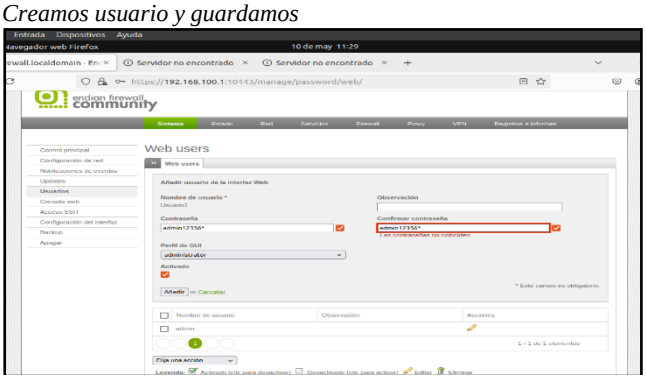
Figura 21.
Creación de listas negras

Fuente: Autoría propia

9.2. AUTENTICACIÓN DE USUARIO

Creamos el usuario dentro del sistema de autenticación de Endian como se ilustra en la Fig. 23, esta configuración nos permite asociar credenciales específicas para controlar el acceso de los usuarios a las políticas de navegación y servicios administrados por el firewall.

Figura 22.
Creamos usuario y guardamos



Fuente: Autoría propia

Para optimizar la estructura de red, se procedió con la creación de grupos de usuarios y la vinculación de cuentas previamente configuradas dentro del ecosistema de Endian UTM. Esta implementación no solo facilita la administración centralizada de políticas de acceso y filtrado, sino que establece una base sólida para la escalabilidad del sistema.

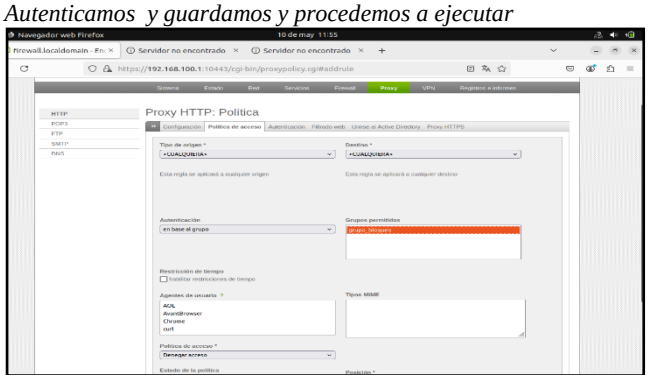
Al agrupar usuarios según su rol o departamento, es posible aplicar restricciones de navegación, priorización de ancho de banda y permisos de seguridad específicos de manera masiva y eficiente. Este nivel de granularidad en la gestión garantiza que las reglas de cumplimiento se ejecuten uniformemente en toda la infraestructura, tal como se detalla visualmente en la Fig. 24.

Figura 23.
Creamos el grupo y asociamos el usuario

Fuente: Autoría propia

Activamos y almacenamos las políticas de autenticación configuradas en Endian como se ilustra en la Fig. 25, este procedimiento permite validar usuarios antes de otorgar acceso a los servicios de navegación, garantizando un mayor control y monitoreo sobre el tráfico generado desde la red LAN.

Figura 24.
Autenticamos y guardamos y procedemos a ejecutar



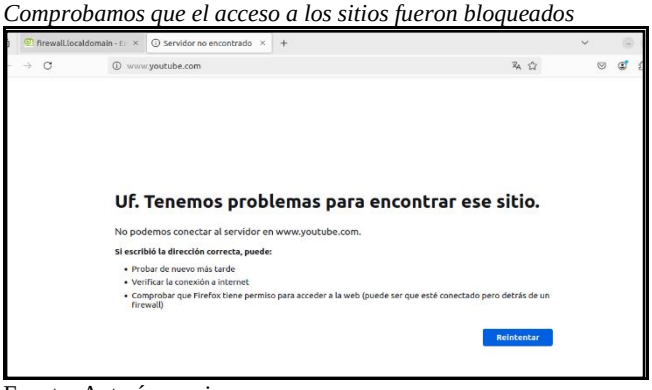
Fuente: Autoría propia

9.3. COMPROBACION DE LAN

Se procedió con la fase de verificación en el entorno de producción, utilizando una estación de trabajo dentro del segmento LAN para testear la robustez del filtrado de contenido. Durante las pruebas, se intentó navegar hacia diversos sitios web restringidos para comprobar la activación de las reglas en el firewall Endian.

La plataforma respondió denegando el tráfico de manera consistente, mostrando la pantalla de bloqueo correspondiente y registrando el evento en los logs del sistema. Este proceso valida satisfactoriamente la jerarquía de permisos y las categorías de filtrado configuradas, cuya arquitectura y confirmación visual se detallan en la Fig. 26.

Figura 25.
Comprobamos que el acceso a los sitios fueron bloqueados



Fuente: Autoría propia

10. CONCLUSIONES

La implementación del entorno virtualizado basado en GNU/Linux permitió comprender el funcionamiento de mecanismos de seguridad y segmentación de redes mediante el uso de Endian Firewall Community. A través de la configuración de zonas WAN, LAN y DMZ fue posible controlar el tráfico de red utilizando políticas NAT, reglas interzona y restricciones de acceso para diferentes protocolos.

Asimismo, la integración de Ubuntu Server y Linux Mint permitió validar el acceso controlado a servicios HTTP y FTP dentro de una arquitectura segmentada, evidenciando la

importancia de aplicar políticas de filtrado y control de tráfico en infraestructuras de red orientadas a la seguridad informática.

Durante el desarrollo de la práctica se implementó y configuró correctamente el servicio de filtrado web mediante el proxy/firewall, permitiendo restringir el acceso a sitios definidos en una lista negra. Posteriormente, se realizaron pruebas desde la red LAN utilizando un navegador web, comprobando que los dominios restringidos no podían ser accedidos, mientras que los sitios permitidos continuaban funcionando normalmente. Con ello se verificó el correcto funcionamiento de las políticas de seguridad y control de navegación implementadas en el sistema.

Finalmente, el uso de Oracle VirtualBox facilitó la implementación de un laboratorio virtual seguro para el desarrollo de prácticas relacionadas con administración de sistemas GNU/Linux, virtualización y configuración de firewalls, fortaleciendo competencias técnicas asociadas a la gestión y protección de redes.

11. REFERENCIAS

[1] Endian srl. (2024). *Endian Firewall Community 3.3.2 Documentation*. Recuperado de https://docs.endian.com/

[2] Oracle. (2024). *Oracle VM VirtualBox User Manual for Release 7.0*. recuperado de https://www.virtualbox.org/manual/UserManual.html

[3] Ubuntu Documentation Team. (2023). *Netplan configuration manager*. Recuperado de https://netplan.io/documentation/

[4] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Upper Saddle River, NJ, USA: Pearson. Recuperado de https://api.pageplace.de/preview/DT0400.9781292154916_A37747529/preview-9781292154916_A37747529.pdf

[5] K. A. Scarfone, W. Jansen & M. Tracy. (2008). *Guide to general server security*. National Institute of Standards and Technology (NIST)

[6] B. Caswell, K. Beale, & J. Baker. (2007). *Snort IDS and IPS Control*. Syngress Publishing.

[7] R. Deal. (2004). *Cisco Router Firewall Security*. Cisco Press.

[8] E. Cole, R. L. Krutz & J. Conley. (2008). *Network Security Bible*. John Wiley & Sons.

[9] Network Security with Open Source Software: Firewall and Intrusion Detection Systems. (s/f-b). *Network Security with Open Source Software: Firewall and Intrusion Detection Systems*.

[10] Tanenbaum, A. S., & Wetherall, D. J. (2021). Pearson Educación. *En Redes de computadoras*.