# DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL SEGMENTADA (LAN/DMZ/WAN) BASADA EN ENDIAN FIREWALL: VALIDACIÓN DE POLÍTICAS DE ACCESO Y CONTROL DE CONTENIDO EN ENTORNOS GNU/LINUX.

Christian Leonel Otálora Coronado
e-mail: clotalorac@unadvirtual.edu.co
David Ricardo Otálora Coronado
e-mail: drotalorac@unadvirtual.edu.co
Jorge Leonardo Martínez Yepez
e-mail: jlmartinezye@unadvirtual.edu.co
Juan David Mayorga Posse
e-mail: jdmayorgap@unadvirtual.edu.co

**RESUMEN:** *Este artículo presenta el diseño, la implementación y la validación de una arquitectura de seguridad perimetral segmentada (WAN, LAN, DMZ) utilizando la distribución Endian Firewall (EFW), una solución basada en software libre en entornos GNU/Linux. El objetivo principal fue evaluar la eficacia de EFW en la aplicación de políticas de seguridad críticas. La metodología incluyó la configuración de Traducción de Direcciones de Red (NAT) para el acceso a Internet, el establecimiento de reglas de filtrado de tráfico entre zonas para mitigar amenazas internas y externas, y la configuración de un Proxy HTTP para el control granular del contenido web. Los resultados demostraron la funcionalidad del modelo propuesto, logrando un control efectivo sobre los protocolos (ej. bloqueo ICMP, permiso HTTP/FTP específico) y la restricción de acceso a recursos web mediante perfiles de usuario. Este estudio valida la viabilidad de utilizar soluciones Open Source para el hardening de redes corporativas.*

**PALABRAS CLAVE:** Endian, Seguridad Perimetral, Segmentación, DMZ, NAT, GNU/Linux, Proxy.

## 1 INTRODUCCIÓN

En el panorama tecnológico actual, la interconexión digital y la masiva transferencia de datos han posicionado a la seguridad perimetral como un pilar fundamental para la continuidad operativa de cualquier organización. La constante evolución de las amenazas cibernéticas exige la implementación de soluciones robustas que no solo bloqueen el tráfico no deseado, sino que también gestionen y segmenten de manera inteligente los flujos de información dentro de la red. Una arquitectura de red plana sin segmentación incrementa exponencialmente la superficie de ataque, permitiendo que una brecha en un solo punto comprometa la integridad de toda la infraestructura.

En respuesta a esta necesidad crítica, el uso de sistemas operativos GNU/Linux como base para la infraestructura de seguridad ha ganado relevancia debido a su flexibilidad, estabilidad y su naturaleza de código abierto. Dentro de este contexto, Endian Firewall (EFW) se presenta como una solución Unified Threat Management (UTM) que permite la configuración de complejas políticas de acceso y la segmentación de red a través de zonas lógicas (WAN, LAN y DMZ). Este trabajo se alinea con los principios de la seguridad en sistemas operativos Open Source, buscando aplicar técnicas de hardening mediante la configuración detallada de reglas de firewall.

Por lo tanto, el objetivo principal de este artículo es diseñar, implementar y validar una arquitectura de seguridad perimetral segmentada y funcional basada en Endian Firewall en un entorno virtualizado. Específicamente, se busca demostrar la eficacia de la solución en tres áreas críticas: 1) la correcta aplicación de la Traducción de Direcciones de Red (NAT), 2) el establecimiento de reglas de filtrado para restringir o permitir protocolos específicos entre las zonas, y 3) la implementación de un Proxy HTTP con control de contenido y autenticación de usuario. Los resultados de esta implementación no solo validan una metodología reproducible para el aseguramiento de redes con software libre, sino que también contribuyen al conocimiento aplicado en la administración de redes y la mitigación de riesgos de seguridad.

## 2 TEMÁTICAS

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

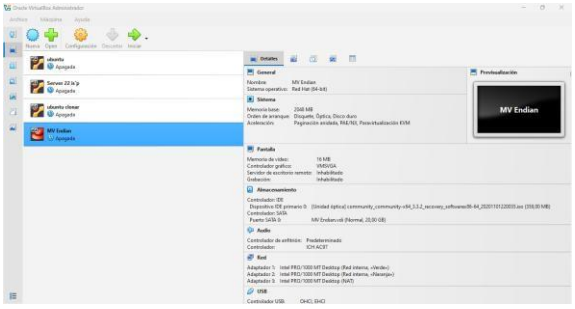
Para el desarrollo de la presente temática, se procedió a realizar el despliegue del firewall Endian 3.3.2 dentro de un entorno virtualizado, siguiendo las directrices establecidas en el diplomado. Como punto de partida, se descargó la imagen ISO oficial de Endian Firewall desde SourceForge [1] y se configuró una máquina virtual en VirtualBox, seleccionando manualmente el tipo de sistema “Linux” y el subtipo “RedHat”, debido a la compatibilidad del sistema con esta familia de distribuciones como se muestra en la figura 1. Aquí es importante aclarar que las especificaciones de hardware se deben dar en base a las necesidades de uso, para este ejemplo práctico mantenemos condiciones mínimas como 512MB de memoria base, y la configuración por defecto sugerida en general, lo cual nos permite tener un funcionamiento para las necesidades estipuladas.

Figura 1 Configuración Maquina virtual Endian


Fuente: Autoría Propia

Una vez creada la máquina virtual, se definieron las interfaces de red necesarias para la segmentación perimetral. En esta etapa se asignaron las tarjetas correspondientes a las zonas roja (WAN), verde (LAN) y naranja (DMZ), con sus respectivos direccionamientos IP, permitiendo la simulación de un entorno perimetral real como se observa en la Figura 2. El desarrollo de esta temática permitió comprender la arquitectura de Endian Firewall y su funcionamiento dentro de entornos virtualizados, estableciendo las bases para la gestión del tráfico y la implementación de reglas de seguridad en las siguientes etapas del trabajo. Con ello, se afianzaron competencias en virtualización, administración perimetral y configuración inicial de firewalls basados en software libre.

Figura 2 Configuración Redes Endian

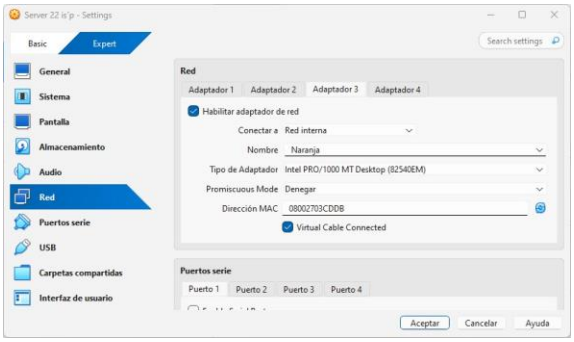



Fuente: Autoría Propia

Posterior a la configuración inicial de las redes en Endian Firewall, se procede a la creación de dos máquinas virtuales adicionales con el fin de simular un entorno empresarial básico. Para este propósito, se despliega una máquina virtual con Ubuntu Desktop, destinada a operar como cliente dentro de la zona Verde (LAN), como se observa en la figura 3 y una máquina virtual con Ubuntu Server, asignada a la zona Naranja (DMZ) como se observa en la figura 4.

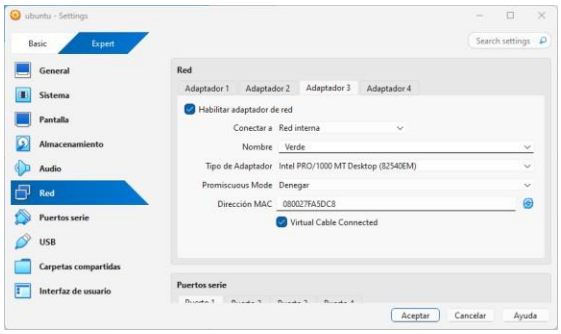
En este punto, resulta fundamental definir la arquitectura de red que será utilizada durante la implementación, ya que la disposición correcta de las zonas y segmentos garantiza el adecuado funcionamiento del firewall perimetral y permite simular un entorno corporativo realista. La distribución adoptada se basa en los principios clásicos de segmentación de redes y defensa en profundidad, ampliamente utilizados en infraestructuras empresariales para reducir riesgos y controlar el flujo de tráfico entre diferentes dominios de seguridad, en nuestro caso manejando las diferentes configuraciones de redes que nos ofrece Virtual Box.

Figura 3 Configuración red interna server




Fuente: Autoría Propia

Figura 4 configuración de red interna cliente




Fuente: Autoría Propia

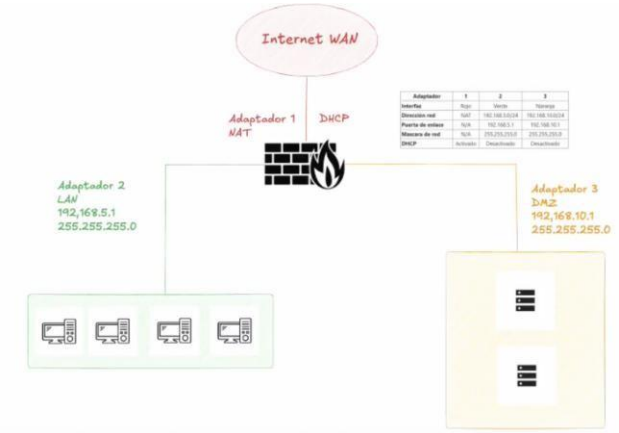
Para esto definimos los diferentes conceptos en donde la zona Verde (LAN) se selecciona como el segmento interno confiable, donde residen los equipos de usuarios y desde el cual se espera un acceso seguro hacia los servicios corporativos. La zona Naranja (DMZ) se implementa como un área intermedia destinada a alojar servidores expuestos parcialmente a redes externas; su propósito es aislar estos servicios, de modo que un compromiso en esta capa no otorgue acceso directo a la red interna. Finalmente, la zona Roja (WAN) representa la red no confiable o externa, comúnmente asociada a Internet, y constituye el punto donde se aplican las políticas de filtrado más estrictas. Esta estructura permite aplicar políticas diferenciadas en función del nivel de confianza asignado a cada zona, facilitando el control del tráfico interzonas, la aplicación de reglas de seguridad y la implementación de mecanismos como NAT, filtrado por puertos y reglas de acceso. La Figura X presenta la distribución seleccionada para el entorno de trabajo [2].

Con esto en mente, podemos observar tanto en la tabla 1, como en la Figura 5 el diseño de red planteado para el presente documento, así como diferentes configuraciones y distribuciones que son importantes al momento de ser aplicadas en la máquina virtual destinada para Endian y también en las descritas previamente. Definido el diseño de red y con los conceptos fundamentales previamente establecidos, se procede a la creación y despliegue de la máquina virtual que alojará Endian Firewall. El proceso de instalación resulta relativamente sencillo y sigue la lógica habitual del entorno VirtualBox; sin embargo, se presentan a continuación los pasos más relevantes con el fin de documentar adecuadamente la metodología empleada.

Tabla 1. Diseño de red.

| Adaptador | 1 | 2 | 3 |
|---|---|---|---|
| **Interfaz** | Rojo | Verde | Naranja |
| **Dirección de red** | NAT | 192.168.5.0/24 | 192.168.10.0/24 |
| **Puerta de enlace** | N/A | 192.168.5.1 | 192.168.10.1 |
| **Mascara de red** | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| **DHCP** | Activado | Desactivado | Desactivado |

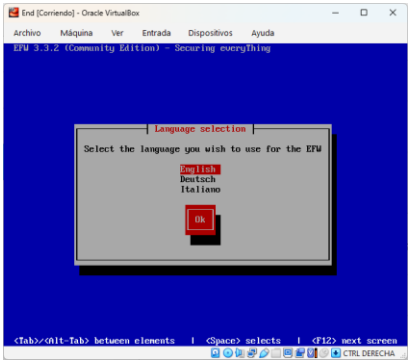
Figura 5. Diseño de red gráfico.




Fuente: Autoría Propia

Durante el proceso de instalación de Endian Firewall, el asistente inicial permite seleccionar el idioma de la interfaz y los parámetros básicos del entorno. La distribución proporciona opciones para definir el esquema de particionado del disco, el manejo de memoria de intercambio y otros ajustes avanzados orientados a la administración del sistema; sin embargo, para efectos de este ejercicio académico, se procedió con las configuraciones predeterminadas, dado que estas garantizan una instalación estable y adecuada para un entorno de pruebas.

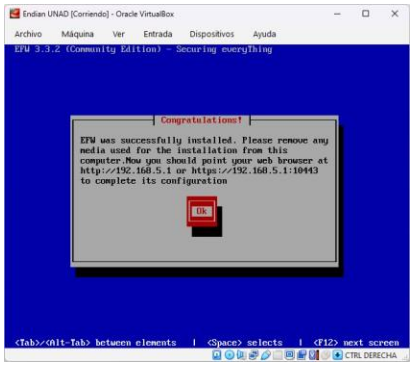
Figura 6 Instalación Endian Idioma




Fuente: Autoría Propia

Tras el primer arranque, Endian presenta un asistente de configuración donde se establecen parámetros esenciales como las interfaces de red, el direccionamiento IP de cada zona, las credenciales administrativas y las opciones básicas de acceso al panel web. Este conjunto de configuraciones iniciales permite dejar operativa la plataforma para la posterior implementación de reglas de seguridad, asignación de zonas y despliegue de los servicios necesarios para el laboratorio.

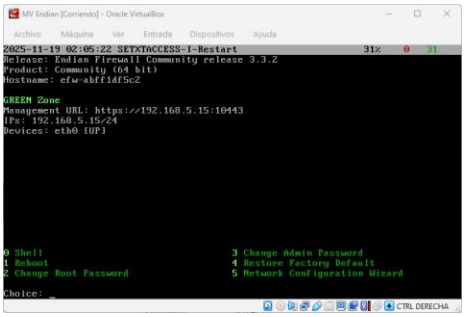
Figura 7 Instalación Endian IP seleccionada




Fuente: Autoría Propia

Con esta información ya tendríamos instalada y montada la imagen de Endian 3.3.2 en nuestra máquina virtual, asociada a la interfaz verde por el puerto 192.168.5.1

Figura 8 Consola Endian

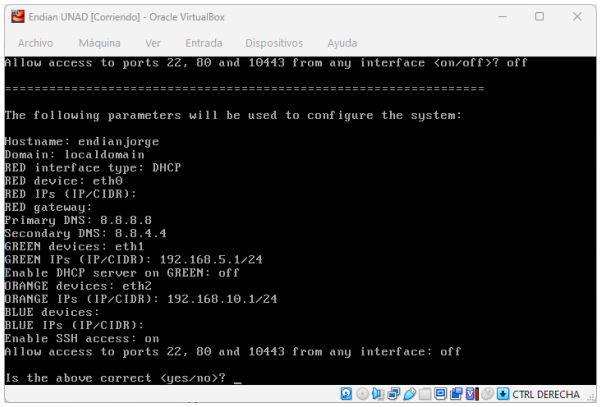



Fuente: Autoría Propia

Posterior a la instalación, la configuración inicial del firewall puede realizarse mediante la interfaz gráfica o a través de la consola; para este ejercicio se utilizó la consola seleccionando la opción 5. Se definieron las zonas y sus parámetros principales de la siguiente manera: la zona Roja, asociada a eth0, quedó configurada con DHCP dinámico, hostname endianjorge, dominio localdomain y los DNS 8.8.8.8 y 8.8.4.4. La zona Verde, asignada a eth1, se configuró con la dirección 192.168.5.1/24 y sin servicio DHCP. La zona Naranja, enlazada a eth2, recibió la dirección 192.168.10.1/24, igualmente con DHCP desactivado. La zona Azul no fue configurada para este entorno.

Una vez finalizada la configuración inicial del firewall, se procede a ajustar los parámetros de red en el cliente. Para ello, se accede a las opciones avanzadas de red del sistema y se ingresan los valores correspondientes a la interfaz asignada.

Figura 9. Configuración zonas Endian




Fuente: Autoría Propia

.En este caso, se establece la dirección IP 192.168.5.2, coherente con el rango de la zona Verde, previamente configurada como segmento interno de la red. Con esta asignación, el cliente queda correctamente integrado a la infraestructura definida para las pruebas y comunicaciones dentro del entorno virtualizado.

Figura 10 Configuración redes Cliente

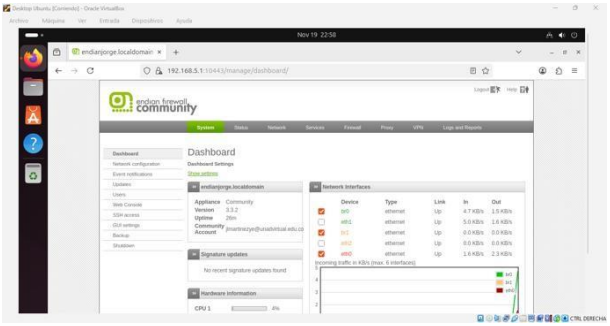
Fuente: Autoría Propia

Tras completar la configuración de red en el cliente, se procede a acceder a la dirección IP indicada al finalizar la instalación de la máquina virtual Endian. Durante este ingreso inicial, es necesario aceptar las advertencias de seguridad asociadas al certificado no confiable generado por defecto y continuar con el registro mediante la dirección de correo solicitada por el sistema.

Posteriormente, la plataforma requiere un usuario administrador, el cual debe haberse creado previamente desde la consola de Endian utilizando la opción 3 del menú de configuración. Una vez superado este proceso de autenticación, se accede a la interfaz gráfica de administración de Endian, donde es posible verificar el estado operativo de las diferentes zonas del firewall, observar el tráfico en tiempo real y acceder a las diversas herramientas de gestión necesarias para las configuraciones posteriores.

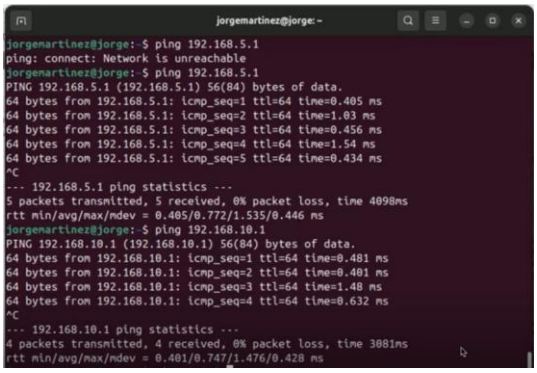
Para verificar el funcionamiento adecuado de las zonas del firewall, se realizaron pruebas de conectividad mediante ping. Los resultados confirmaron el envío exitoso de paquetes hacia cada segmento configurado, siendo todos correctos, como se evidencia en la figura 12, con Ping a zonas verde, naranja y roja.

Figura 11 Interfaz Endian desde cliente




Fuente: Autoría Propia

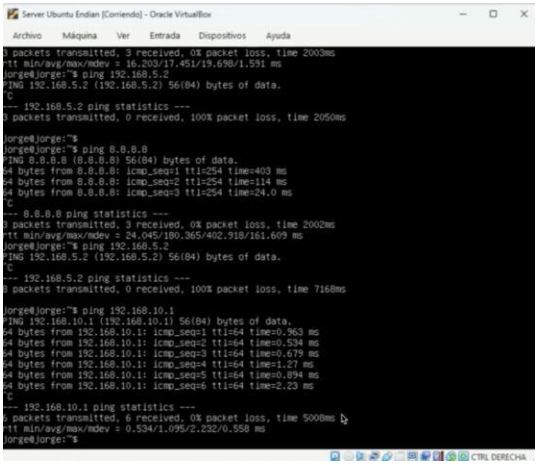
Figura 12 Ping desde cliente




Fuente: Autoría Propia

Finalmente, se configuraron las redes del servidor mediante netplan, asignando las direcciones IP definidas previamente. Para validar, se ejecutaron pruebas de conectividad mediante ping hacia las diferentes zonas del firewall.

Figura 13 Ping desde el servidor.




Fuente: Autoría Propia

Los resultados mostraron comunicación adecuada con la zona verde y la zona roja, evidenciando un tráfico correcto entre estos segmentos. En contraste, la zona naranja no respondió a las solicitudes como se evidencia en la figura 13, lo cual es coherente con las políticas de protección establecidas para este segmento, donde se restringe el tráfico directo como medida de seguridad propia de la DMZ.

# 3. TEMÁTICA 2: CONFIGURACIÓN NAT.

La correcta configuración de Network Address Translation (NAT) es fundamental para garantizar la conectividad segura y controlada entre las zonas de red segmentadas. En esta fase se implementaron y verificaron dos tipos críticos de reglas NAT: NAT Masquerading para permitir el acceso a Internet desde la red interna (LAN), y Port Forwarding para redirigir tráfico específico desde la WAN hacia servidores en la DMZ.

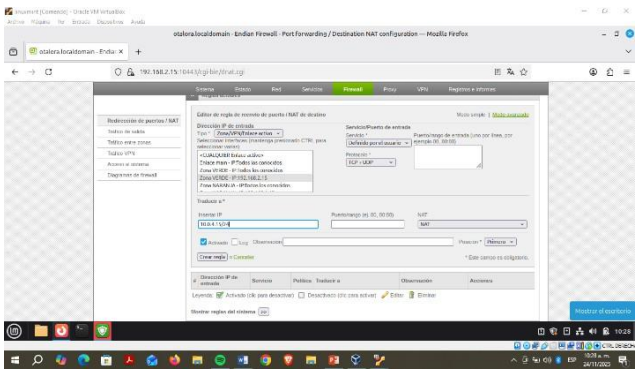
## 3.1 Configuración de NAT Masquerading: Conectividad LAN a WAN

El objetivo principal fue permitir que los hosts de la zona Verde (LAN) accedieran a recursos externos en Internet (WAN) enmascarando sus direcciones IP privadas detrás de la IP pública del firewall. En Endian Firewall, esta funcionalidad se implementa mediante la creación de reglas de salida (Outgoing) en la pestaña Firewall.

- Zona Origen: Verde (LAN)
- Servicio: Cualquiera (para tráfico general) o definido por el usuario (para protocolos específicos como TCP+UDP)
- Destino: IP de la WAN (o cualquier)
- Acción: NAT, activado

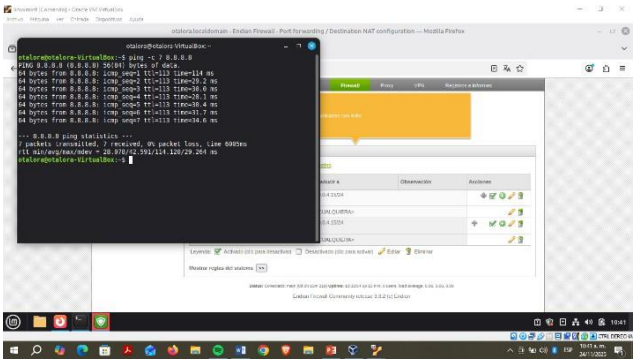
La figura 14 muestra la regla creada en la interfaz de administración de EFW. Tras aplicar la configuración, se verificó la conectividad desde un cliente en la LAN (Linux Mint) ejecutando el comando ping -c 7 8.8.8.8, obteniéndose una respuesta exitosa como se evidencia en la figura 15. Esto confirma que el tráfico de la zona Verde está siendo correctamente enmascarado y enrutado hacia Internet.

Figura 14 Regla de NAT Masquerading configurada para la zona Verde (LAN).



Fuente: Autoría Propia

Figura 15 Prueba de conectividad exitosa desde la LAN (cliente) hacia Internet



Fuente: Autoría Propia

## 3.2 Configuración de Port Forwarding: Conectividad DMZ a WAN y Exposición de Servicios

Para servidores ubicados en la zona desmilitarizada (DMZ), es esencial permitir una salida controlada a Internet (por ejemplo, para actualizaciones de seguridad) y, opcionalmente, redirigir tráfico entrante específico hacia ellos. Se configuró una regla de salida para la DMZ similar a la de la LAN, y se exploró la configuración de reenvío de puertos.

Zona Origen: Naranja (DMZ)

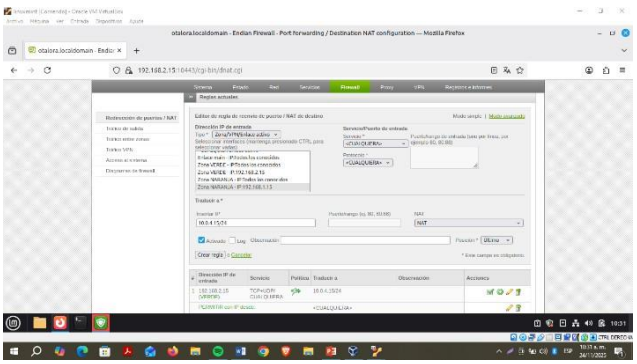
Servicio: Cualquiera

Destino: IP de la WAN

Acción: NAT, activado

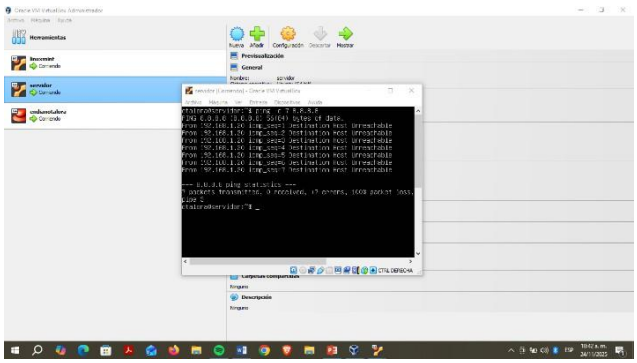
La aplicación de esta regla, ilustrada en la figura 16, permitió verificar la conectividad a Internet desde un servidor en la DMZ, utilizando el comando ping -c 7 8.8.8.8 (Figura 17). Adicionalmente, se configuró una regla de Port Forwarding para redirigir el tráfico HTTP (puerto 80) entrante por la IP de la WAN hacia la IP del servidor web en la DMZ, asegurando así un acceso controlado a servicios internos desde el exterior.

Figura 16 Regla de NAT configurada para la zona Naranja (DMZ)



Fuente: Autoría Propia

Figura 17 Regla de NAT configurada para la zona Naranja (DMZ)



Fuente: Autoría Propia

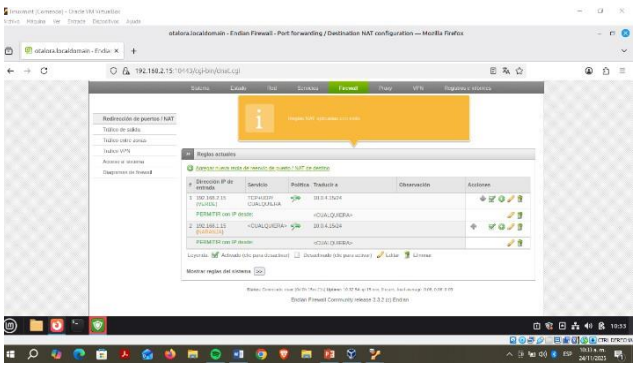
## 3.3 Configuración de Port Forwarding: Conectividad DMZ a WAN y Exposición de Servicios

La efectividad de la configuración NAT se validó exhaustivamente mediante el uso de comandos de diagnóstico en la consola de cada máquina virtual. Las pruebas de conectividad (ping) y el análisis del estado de las reglas desde la interfaz web de EFW confirmaron que:

- Los hosts de la LAN pueden acceder a Internet de forma transparente y segura
- Los servidores en la DMZ tienen salida controlada a Internet
- Las reglas de reenvío de puertos permiten una exposición segura de servicios internos

La Figura 18 muestra el listado final de reglas NAT aplicadas con éxito en el firewall, documentando la configuración realizada.

Figura 18 Listado de reglas NAT aplicadas exitosamente en Endian Firewall



Fuente: Autoría Propia

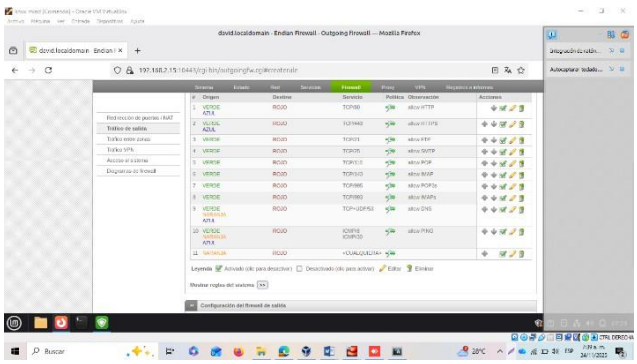
# 4 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

## 4.1 Habilitación de Servicios Esenciales: HTTP y FTP

Para garantizar la funcionalidad del servidor web ubicado en la DMZ, fue necesario permitir explícitamente el tráfico de los protocolos HTTP (puerto 80) y FTP (puerto 21). Esta configuración se realizó mediante reglas de firewall que autorizan el flujo bidireccional de estos servicios específicos.

- Servicio HTTP: Configuración de reglas para permitir tráfico web entrante y saliente
- Servicio FTP: Habilitación de transferencia de archivos para mantenimiento del servidor
- Verificación: Validación mediante navegador web y cliente FTP desde la zona LAN

Figura 19 Servicio Apache2 activo en el servidor Ubuntu de la DMZ



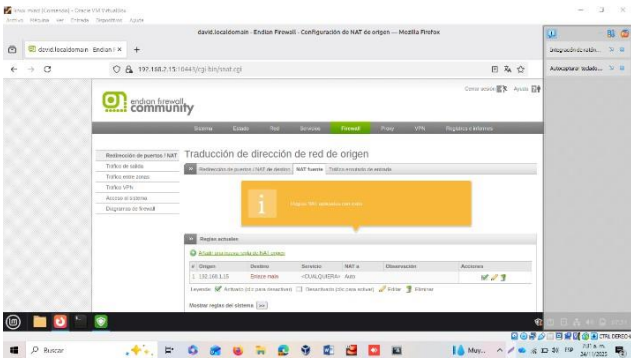
Fuente: Autoría Propia

## 4.2 Configuración de Reglas de Acceso entre Zonas

El acceso controlado entre zonas se implementó mediante reglas específicas en el firewall Endian. Se establecieron políticas que permiten:

- Comunicación desde la LAN hacia la DMZ para servicios HTTP/FTP
- Acceso desde la DMZ hacia Internet para actualizaciones
- Restricción de tráfico no esencial entre zonas

Figura 20 configuración de puente NAT para zona DMZ




Fuente: Autoría Propia

## 4.3 Denegación de Protocolo ICMP como Medida de Seguridad

Como parte de las estrategias de security through obscurity, se implementó la denegación del protocolo ICMP para evitar el descubrimiento de hosts mediante comandos ping.

- Puertos afectados:8 (Echo Request) y 30 (ICMP alternativo)
- Implementación: Reglas de firewall bloqueando tráfico ICMP
- Verificación: Pruebas de conectividad mediante ping desde diferentes zonas

## 4.4 Verificación Integral de la Configuración

La validación final incluyó múltiples pruebas:

- Acceso al servidor web mediante navegador desde la LAN
- Conexión FTP exitosa al servidor en la DMZ
- Pruebas de ping desde LAN hacia DMZ - Sin respuesta
- Verificación de reglas en tabla de firewall

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

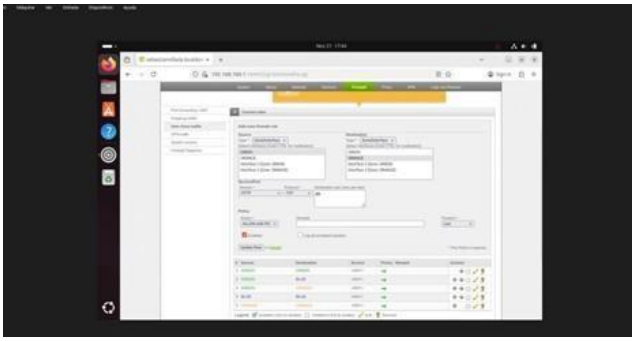
## a. COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

Para lograr esta comunicación se debe de realizar la creación de las siguientes reglas:

- **Regla N°1: HTTP desde la LAN hacia DMZ**
  - From zone: VERDE
  - To Zone: NARANJA
  - Service: HTTP

Una vez que todos los parámetros han sido confirmados, procederemos a presionar el botón de aceptación para que el sistema aplique e integre inmediatamente las configuraciones que hemos especificado en las reglas.

Figura 21 configuración de Regla N°1



Fuente: Autoría Propia

- **Regla N°2: FTP desde la LAN hacia DMZ**
  - From zone: VERDE
  - To Zone: NARANJA
  - Service: FTP (puerto 20 y 21)

Figura 22 configuración de Regla N°2

Fuente: Autoría Propia

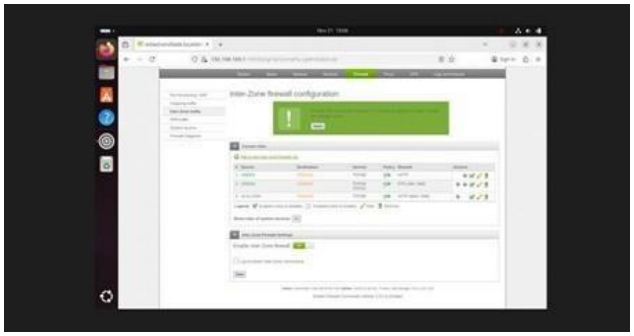
Estas directivas han sido establecidas para conceder el permiso necesario a los dispositivos conectados en la red local (LAN) para que puedan consultar y utilizar el servidor web (HTTP) y el servidor de transferencia de archivos (FTP) que se encuentra alojado en la DMZ.

## b. COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Con el fin de establecer la conectividad desde Internet (la zona RED) hacia los servicios alojados en la DMZ, es imprescindible considerar el siguiente conjunto de directrices:

- **Regla N°3: HTTP desde WAN hacia DMZ**
    - From zone: DHCP
    - To Zone: NARANJA
    - Service: HTTP

Figura 23 configuración de Regla N°3



Fuente: Autoría Propia

- **Regla N°4: FTP desde WAN hacia DMZ**
    - From zone: DHCP
    - To Zone: NARANJA
    - Service: FTP

Figura 24 configuración de Regla N°4

Fuente: Autoría Propia

Mediante estas directivas, se autoriza que el tráfico originado en Internet, o desde cualquier host que pertenezca a la zona RED, pueda acceder y consumir los servicios que han sido desplegados en la Zona DMZ

## c. VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

Tras la correcta inclusión de las directivas de acceso solicitadas, la interfaz de gestión debería reflejar ahora una vista donde se visualiza y confirma la configuración de las reglas recién implementadas

Figura 25 Visualización reglas Configuradas

Fuente: Autoría Propia

Este resultado nos proporciona la evidencia necesaria para ratificar que las directivas de seguridad se han establecido y configurado de forma impecable.

## d. PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS:

## EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ. EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA WAN.

Para verificar la conectividad del servicio HTTP desde la zona GREEN hasta la DMZ, simplemente ingresamos la dirección de destino del servidor en el navegador web. Si la configuración es precisa, la página web alojada en el servidor de la DMZ deberá visualizarse sin errores

Figura 26 Visualización reglas Configuradas


Fuente: Autoría Propia

**EL INGRESO DEL SERVICIO HTTP DESDE LA ZONA DMZ HACIA LA WAN. EL INGRESO DEL SERVICIO HTTP DESDE LA WAN HACIA LA ZONA DMZ. EL INGRESO DEL SERVICIO FTP DESDE LA LAN HACIA LA WAN.**

Para llevar a cabo las verificaciones del servicio HTTP hacia la zona WAN (Internet), simplemente utilizamos el navegador web para acceder a la dirección de destino correspondiente.

Figura 26 Visualización reglas Configuradas

Fuente: Autoría Propia

## 6. CONCLUSIONES

Se fortalecieron las competencias en seguridad perimetral mediante la implementación del firewall Endian y la configuración de servicios esenciales dentro de una arquitectura de red segmentada. La práctica consolidó habilidades en diseño, administración y protección de infraestructuras corporativas en entornos virtualizados

Se logró comprender y aplicar de manera efectiva la estructura de zonas de seguridad (LAN, WAN y DMZ), validando la configuración de interfaces, direccionamientos y servicios base. Esto permitió afianzar los fundamentos operativos del firewall y su papel dentro del perímetro corporativo

Se configuro reglas de NAT para permitir la salida y entrada de tráfico desde las distintas zonas, comprobando adecuadamente el funcionamiento de la traducción de direcciones y la correcta creación automática de reglas en el firewall.

Se implementaron reglas de acceso que habilitaron los servicios HTTP y FTP desde la DMZ, además de la restricción del protocolo ICMP. Estas configuraciones reflejaron la relevancia del control granular del tráfico para mantener la integridad y confidencialidad de la red.

Se verificó la comunicación controlada entre zonas internas y externas, evaluando el comportamiento del tráfico permitido y denegado. Esto evidenció la importancia de las políticas de seguridad bien diseñadas para garantizar un tráfico seguro y acorde con las necesidades del entorno corporativo

## 7 REFERENCIAS


[1] Endian Team. (s.f.). Endian Firewall Community (Versión 3.3.2) [Software de código abierto]. SourceForge. https://sourceforge.net/projects/efw/

[2] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Upper Saddle River, NJ, USA: Pearson, 2020.

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

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

hardware. Linux Professional Institute. Recuperado de https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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