IMPLEMENTANDO SEGURIDAD EN GNU/LINUX ENDIAN

Juan Camilo Cespedes Restrepo.
email: jccespedesr@unadvirtual.edu.co
Paola Vidal Ramírez
email: pvidalr@unadvirtual.edu.co
Sebastian Parias Arias
email: spariasar@unadvirtual.edu.co

RESUMEN: *En el presente artículo se desarrolló la implementación y configuración de un entorno de seguridad de red utilizando Oracle VM VirtualBox y GNU/Linux Endian. Inicialmente, se realizó la configuración de las zonas verde (LAN), roja (WAN) y naranja (DMZ), permitiendo una adecuada segmentación de la red. Posteriormente, se implementaron reglas NAT con el fin de habilitar la comunicación desde la LAN y la DMZ hacia la red de Internet simulada. Asimismo, se configuraron los servicios HTTP y FTP en un servidor Ubuntu Server ubicado en la DMZ, además de restringir el protocolo ICMP para fortalecer la seguridad de la infraestructura. Finalmente, se implementó un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado mediante listas negras para bloquear sitios web específicos. Los resultados obtenidos evidenciaron el correcto funcionamiento de las políticas de seguridad, conectividad y control de acceso, contribuyendo al fortalecimiento de la administración y protección de la red.*

KEYWORDS: DMZ, Endian, GNU/Linux, NAT.

1 INTRODUCCIÓN

La seguridad y administración de redes son aspectos fundamentales en los entornos tecnológicos actuales, debido a la necesidad de proteger la información y controlar el acceso a los servicios de red [1]. En este artículo se presenta la implementación de GNU/Linux Endian en Oracle VM VirtualBox, mediante la configuración de las zonas LAN, WAN y DMZ. Asimismo, se desarrolló la configuración de reglas NAT para permitir la comunicación entre redes, la habilitación de servicios HTTP y FTP en un servidor Ubuntu Server y la restricción del protocolo ICMP como medida de seguridad [8]. Finalmente, se implementó un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado web para controlar el acceso a determinados sitios en Internet.

2 DESARROLLO DE LA TEMÁTICA 1

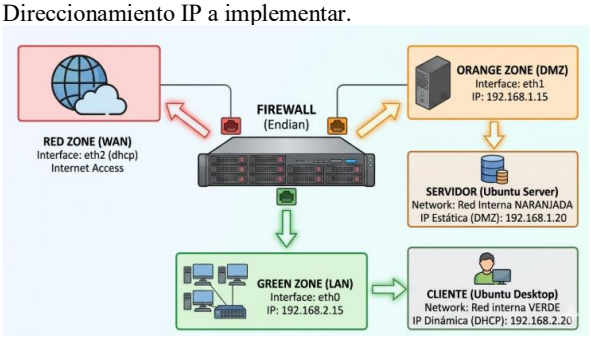
La seguridad en infraestructuras de código abierto demanda la creación de perímetros definidos que aíslen los servicios críticos de las estaciones de trabajo del usuario final [2]. La temática desarrollada en esta etapa se fundamenta en la implementación de un firewall de inspección de estado (SPI) mediante Endian Firewall, configurado en un entorno de red virtualizado. Esta aproximación permite mitigar riesgos asociados a la exposición de servicios en internet, aplicando el principio de defensa en profundidad, donde cada zona de red posee políticas de acceso restrictivas y personalizadas.

2.1 ARQUITECTURA DE RED, Y SEGMENTACIÓN LÓGICA

La implementación utiliza un modelo de seguridad basado en la segmentación por colores, técnica ampliamente documentada para simplificar la administración de políticas de red en sistemas Linux [2]. Se definieron tres niveles de confianza distribuidos en interfaces lógicas:

1. **Zona Verde (Green - ETH0):** Configurada como la red de área local (LAN) de alta confianza. Opera bajo el segmento 192.168.2.0/24. En esta zona reside el cliente Ubuntu Desktop con la IP estática 192.168.2.20. El control de acceso se refuerza mediante el enlace de direcciones MAC en el servidor DHCP del firewall, asegurando que solo dispositivos autorizados reciban parámetros de red correctos, evitando ataques de suplantación internos [3].
2. **Zona Naranja (Orange - ETH1):** Definida como la Zona Desmilitarizada (DMZ) en el segmento 192.168.1.0/24. Alberga el servidor con la IP 192.168.1.20, que ejecuta servicios públicos como ISPConfig. Según las mejores prácticas de seguridad perimetral, esta zona es accesible desde el exterior, pero mantiene restricciones estrictas que prohíben la iniciación de conexiones hacia la red interna [3].
3. **Zona Roja (Red - ETH2):** Actúa como la interfaz de salida hacia redes no confiables (Internet). Es el punto donde se aplican las políticas de NAT y se filtran las peticiones de entrada antes de ser redirigidas a la DMZ [3].

Figura 1.
Direccionamiento IP a implementar.



Fuente: Autoría Propia

El flujo de tráfico y la efectividad de las reglas de firewall se validan a través de las evidencias recolectadas durante la implementación, comparándolas con los estándares de administración de servicios esenciales en Linux. En la configuración de la red en un entorno virtual mediante máquinas virtuales, cada una de ellas se debe configurar en el apartado de red dentro de VirtualBox como se visualiza en la Figura 2, en este caso se utilizan 3 adaptadores para la máquina Endian, el adaptador 1 para la zona verde (LAN), el adaptador 2 para la zona naranja (DMZ) y el adaptador 3 para la zona roja (Internet) [2].

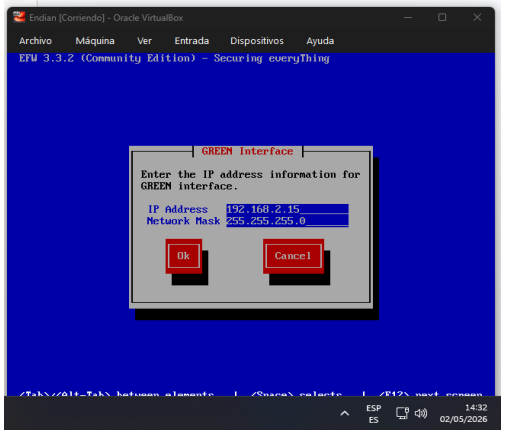
Figura 2.
Configuración de red en la máquina virtual Endian.

Fuente: Autoría Propia

2.2 GESTIÓN, MONITOREO Y ESTADO DEL SISTEMA

Al ser una distribución Open Source [4], Endian se puede descargar gratis desde el portal de SourceForge. Tras configurarlo como una máquina virtual en VirtualBox y ejecutarlo, se observa la interfaz de la Figura 3**.** Luego de terminar esta configuración se podrá ingresar a la interfaz web para finalizar la instalación y configuración de Endian y sus diferentes zonas.

Figura 3.
Ejecución de la máquina virtual con el archivo ISO de Endian.



Fuente: Autoría Propia.

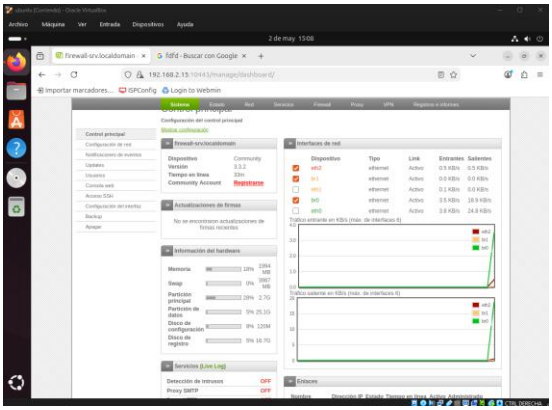
Luego de realizar la configuración de red a través de los diferentes pasos de la interfaz de Endian como se visualiza en la Figura 4**,** se podrá observar el dashboard principal de Endian. La administración centralizada es un pilar fundamental. A través del dashboard de Endian, se supervisa el rendimiento del hardware y el estado de los servicios de protección, asegurando que el sistema operativo base no presente sobrecargas que comprometan la seguridad [2].

Figura 4.
Proceso de configuración de Endian desde la interfaz web.

Fuente: Autoría Propia

Como se aprecia en la Figura 5, el sistema reporta la activación de módulos críticos como el Sistema de Prevención de Intrusiones (IPS) y el Filtrado de Contenido. La correcta visibilidad de las interfaces confirma que el firewall actúa como el nodo central de enrutamiento. De acuerdo con la documentación de Endian, esta vista permite al administrador reaccionar ante anomalías de tráfico de manera proactiva [4].

Figura 5.
Panel de control de Endian Firewall.



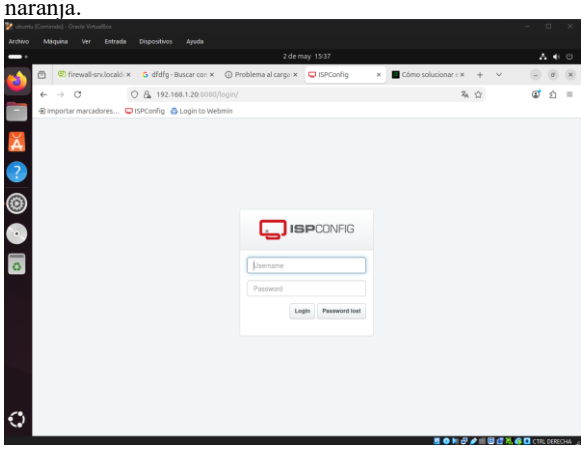
Fuente: Autoría Propia.

2.3 VALIDACIÓN DE POLÍTICAS DE ACCESO Y PRUEBAS DE CONECTIVIDAD

La efectividad de una DMZ radica en su capacidad de aislar problemas [5]. Se realizaron pruebas de conectividad bidireccional para verificar que las reglas de tráfico cumplen

con los requisitos de seguridad de la Etapa 7. En la Figura 6 se documenta la prueba de comunicación. Se confirma el acceso exitoso desde la Zona Verde hacia la Zona Naranja, permitiendo que la administración interna gestione el panel de ISPConfig en el puerto 8080. No obstante, la evidencia técnica más relevante es la falla controlada del comando ping iniciado desde la DMZ hacia la LAN.

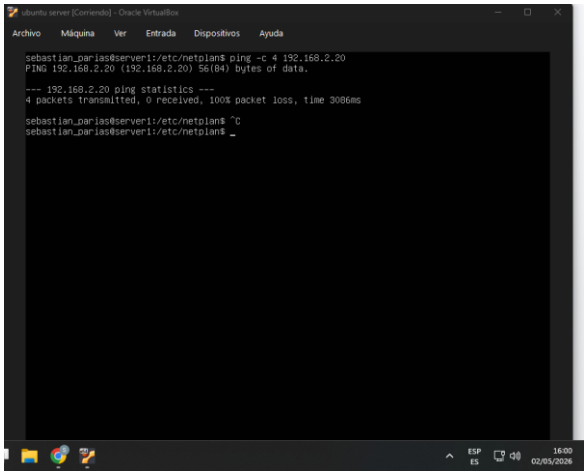
Figura 6.
Verificación de la comunicación entre la zona verde y la zona naranja.



Fuente: Autoría Propia

La pérdida total de paquetes hacia la IP 192.168.2.20 demuestra que las políticas de "Tráfico entre zonas" están correctamente configuradas, impidiendo que un servidor comprometido pueda escalar ataques hacia los equipos locales [2], como se observa en la Figura 7.

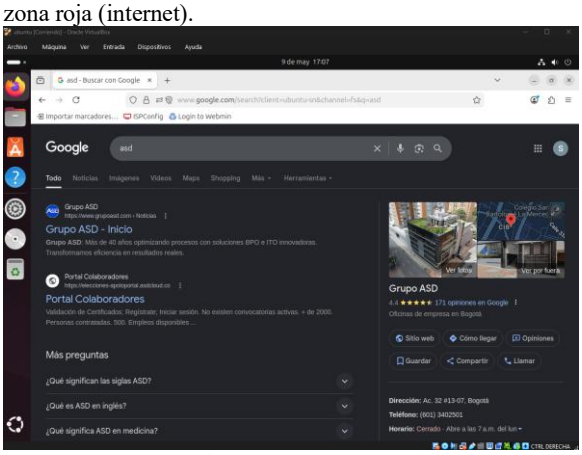
Figura 7.
Bloqueo de comunicaciones iniciadas desde la zona naranja hacia la zona verde.



Fuente: Autoría Propia

Por último, se verifica el acceso desde la zona verde a internet, como se observa en la figura 8. Esta conexión se realiza desde la máquina Ubuntu Desktop.

Figura 8.
Conexión desde Ubuntu Desktop (zona verde o LAN) a la zona roja (internet).



Fuente: Autoría Propia.

La implementación técnica demuestra que la segmentación de red es una barrera lógica esencial en la administración de sistemas operativos Open Source. Endian Firewall proporciona las herramientas necesarias para gestionar la complejidad de estas interconexiones bajo un esquema de "menor privilegio" [4]. Esta configuración reduce drásticamente la superficie de ataque, asegurando que un compromiso en la zona naranja no comprometa los datos sensibles alojados en la zona verde.

3 DESARROLLO DE LA TEMÁTICA 2.

La implementación de reglas NAT (Network Address Translation) en infraestructuras Linux permite controlar el acceso entre redes internas y externas, garantizando conectividad y seguridad dentro de entornos segmentados [3]. Durante la implementación se utilizó Endian Firewall Community como firewall principal dentro de un entorno virtualizado en Oracle VM VirtualBox, permitiendo administrar el tráfico entre una red LAN, una DMZ y la red WAN simulada como Internet [9]. La arquitectura propuesta se fundamenta en el modelo de segmentación por zonas implementado por Endian, donde cada interfaz posee un nivel de confianza diferente. La zona GREEN corresponde a la red local de usuarios, la zona ORANGE representa la DMZ donde se alojan los servicios expuestos y la zona RED funciona como salida hacia redes externas. Este modelo permite aplicar políticas diferenciadas de seguridad y controlar el tráfico mediante reglas NAT y firewall.

3.1 VALIDACIÓN DEL ACCESO A INTERNET DESDE LA ZONA GREEN

Inicialmente se verificó el funcionamiento de las políticas predeterminadas de Endian para la zona GREEN. Esta zona corresponde a la red LAN y posee permisos de salida configurados automáticamente por el firewall, permitiendo que los equipos internos puedan acceder a servicios externos sin necesidad de crear reglas adicionales. Desde el panel de administración de Endian se observó que la zona GREEN tenía habilitadas múltiples reglas de salida,

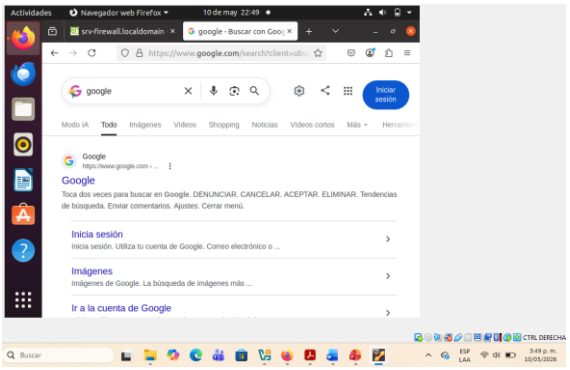
permitiendo navegación web, resolución DNS y acceso a diferentes servicios externos.

Figura 9.
Visualización de políticas activas para la zona GREEN.

Fuente: Autoría propia

Posteriormente, se verificó el acceso a Internet desde el equipo Ubuntu Desktop perteneciente a la LAN. La prueba permitió confirmar que el firewall realizaba correctamente el proceso de traducción NAT para la red GREEN, permitiendo navegación y comunicación hacia redes externas.

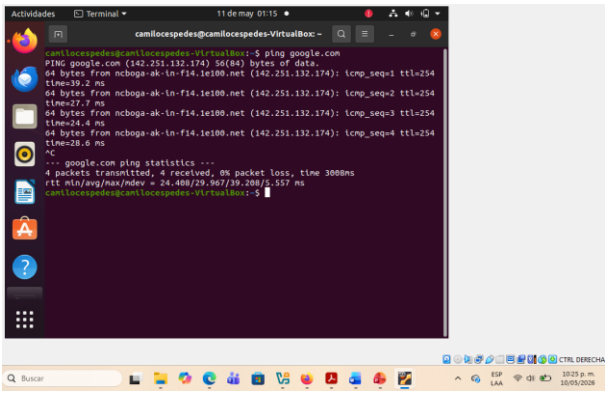
Figura 10.
Acceso exitoso a Internet desde la red GREEN.



Fuente: Autoría propia.

Adicionalmente, se realizaron pruebas utilizando el comando ping google.com, validando tanto la conectividad hacia Internet como el correcto funcionamiento de la resolución DNS dentro de la red local.

Figura 11.
Prueba de conectividad hacia Internet desde la LAN.



Fuente: Autoría propia.

Los resultados obtenidos permitieron evidenciar que la red GREEN posee acceso saliente habilitado por defecto dentro de Endian Firewall, garantizando conectividad hacia la WAN sin necesidad de configuraciones adicionales.

3.2 RESTRICCIÓN DE ACCESO DESDE LA DMZ

Después de validar la conectividad desde la LAN, se realizaron pruebas desde el servidor Ubuntu ubicado en la zona ORANGE (DMZ). Durante esta validación se intentó ejecutar una actualización del sistema operativo, evidenciando que el servidor no contaba con acceso hacia Internet.

Figura 12.
Fallo de conexión hacia Internet desde la DMZ

Fuente: Autoría propia.

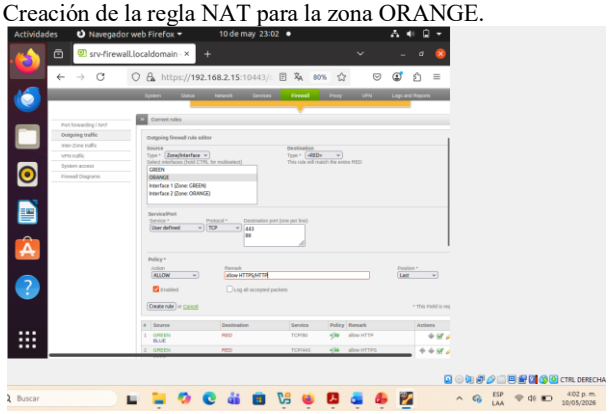
La ausencia de conectividad se debe a que Endian restringe por defecto las conexiones salientes desde la zona ORANGE como medida de seguridad. Este comportamiento busca evitar que servidores expuestos hacia redes externas puedan establecer tráfico no autorizado hacia Internet,

reduciendo riesgos asociados a ataques o compromisos de seguridad

3.3 IMPLEMENTACIÓN DE REGLAS NAT PARA LA DMZ

Con el objetivo de habilitar acceso controlado hacia Internet desde la DMZ, se procedió a crear una nueva regla NAT dentro del firewall Endian. La política fue configurada desde el apartado correspondiente a las reglas de tráfico, permitiendo que la red ORANGE pudiera establecer comunicación hacia la interfaz RED.

Figura 13.
Creación de la regla NAT para la zona ORANGE.



Fuente: Autoría propia.

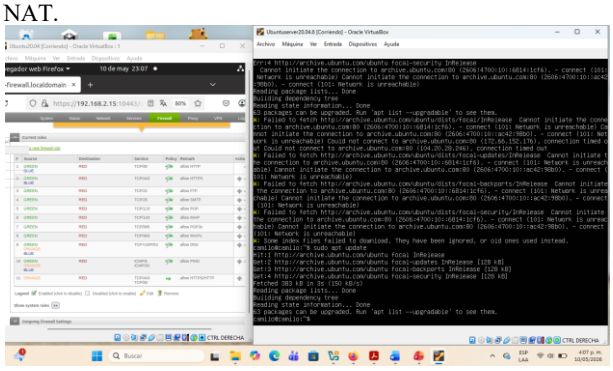
Después de aplicar la configuración, se verificó que la nueva política NAT quedara registrada correctamente dentro de las reglas activas del firewall. La regla creada permitió habilitar el tráfico saliente desde la zona DMZ hacia la WAN, permitiendo que el servidor Ubuntu pudiera acceder a Internet correctamente y establecer conexión con servicios externos.

Figura 14.
Verificación de la regla NAT configurada en Endian.

Fuente: Autoría propia.

Posteriormente, se realizaron nuevamente pruebas desde el servidor Ubuntu ubicado en la DMZ. En esta ocasión, el sistema logró establecer conexión con los repositorios externos y ejecutar correctamente las actualizaciones del sistema operativo [7].

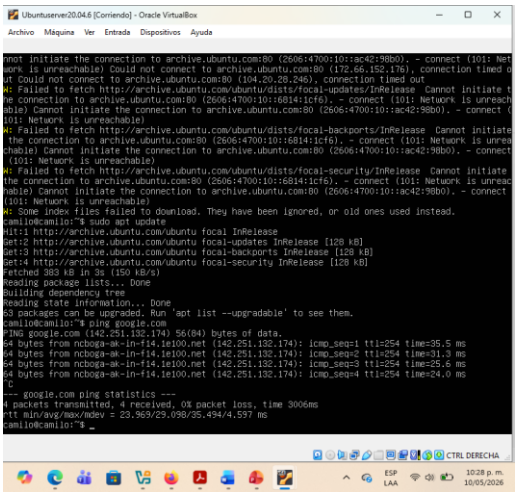
Figura 15.
Actualización exitosa del servidor después de aplicar la regla NAT.



Fuente: Autoría propia.

Adicionalmente, se ejecutaron pruebas mediante el comando ping google.com, obteniendo respuestas satisfactorias desde Internet. Esto confirmó que la política NAT implementada funcionaba correctamente y permitía el acceso controlado desde la zona ORANGE hacia redes externas.

Figura 16.
Prueba de conectividad exitosa desde la DMZ hacia Internet.

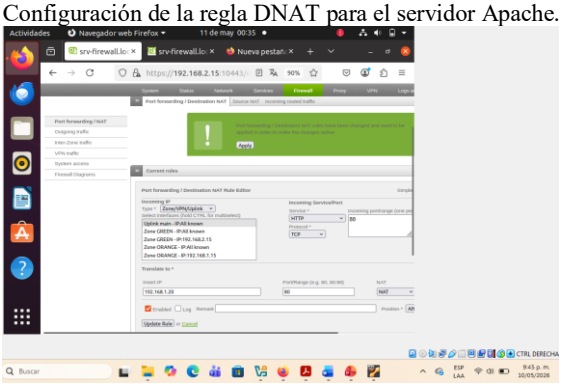


Fuente: Autoría propia.

3.4 CONFIGURACIÓN DE REENVÍO DE PUERTOS MEDIANTE DNAT

Finalmente, se implementó una regla DNAT (Destination NAT) dentro del firewall Endian para permitir el acceso externo hacia el servidor Apache ubicado en la zona ORANGE. La regla fue configurada para redirigir las solicitudes entrantes realizadas al puerto 80 de la interfaz WAN hacia la dirección IP interna 192.168.1.20 correspondiente al servidor Ubuntu.

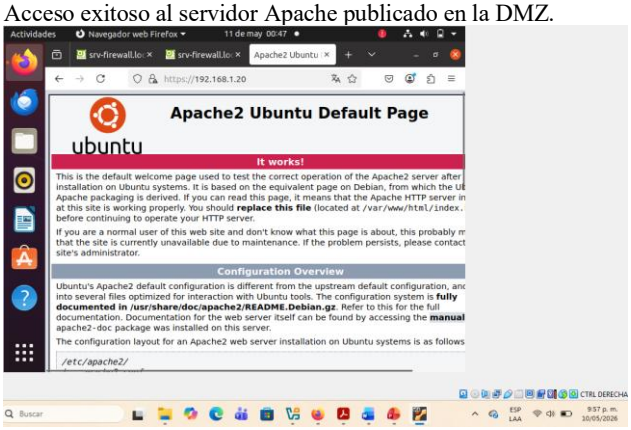
Figura 17.
Configuración de la regla DNAT para el servidor Apache.



Fuente: Autoría propia.

La implementación de esta política permitió publicar el servicio web alojado dentro de la DMZ sin exponer directamente la red interna. Endian procesó las solicitudes provenientes de la WAN y realizó automáticamente el reenvío del tráfico hacia el servidor Apache configurado en la zona ORANGE. Posteriormente, se verificó el correcto funcionamiento de la regla accediendo desde el navegador web al servidor publicado. Como resultado, se visualizó correctamente la página predeterminada de Apache2, confirmando que el reenvío de puertos y la traducción de direcciones funcionaban adecuadamente.

Figura 18.
Acceso exitoso al servidor Apache publicado en la DMZ.



Fuente: Autoría propia.

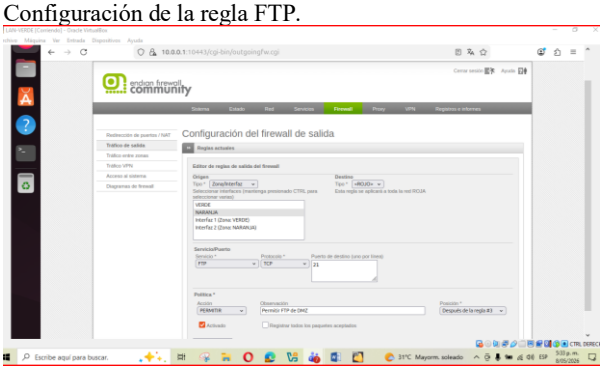
4 DESARROLLO DE LA TEMÁTICA 3

Esta temática aborda la ejecución de reglas de control de tráfico en Endian Firewall orientadas a publicar los servicios HTTP y FTP para su consumo desde Internet mediante la habilitación de los puertos 80 y 21 en un servidor Ubuntu Server [6]. Asimismo, se restringió el protocolo ICMP con el propósito de bloquear pruebas de conectividad mediante el comando ping.

4.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21) DESDE EL SERVIDOR WEB

Se establece la habilitación de los servicios HTTP (puerto 80) y FTP (puerto 21) en el servidor web, mediante la configuración de una regla de redirección de puertos en el firewall. Esta regla permite que el FTP alojado en la zona DMZ sea accesible desde cualquier IP externa, de tal manera que Endian firewall actúa como intermediario, recibiendo las solicitudes entrantes, redirigiéndolas hacia el servidor interno correspondiente y enviando de vuelta la respuesta al cliente que realizó la conexión.

Figura 19.
Configuración de la regla FTP.



Fuente: Autoría propia.

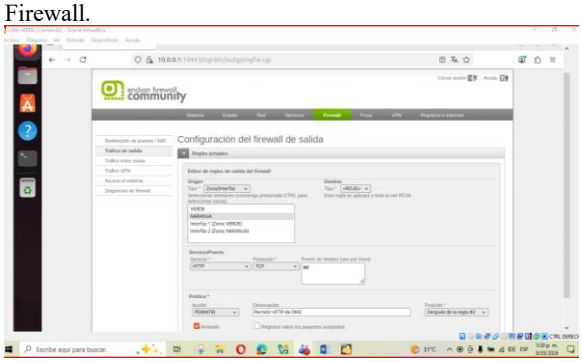
Para configurar que la regla configurada funciona adecuadamente, se realizó una prueba de conexión al FTP publicado en el servidor ubicado en la DMZ con dirección IP 192.168.0.2. Desde la terminal del equipo cliente se realiza el comando FTP hacia dicha dirección, lo que permitió establecer comunicación con el servidor.

Figura 20.
Comprobación de la regla FTP.

Fuente: Autoría propia.

Se realiza el mismo procedimiento utilizado para la configuración de la regla del servicio FTP, pero en este caso enfocado en habilitar el servicio HTTP, ajustando los parámetros correspondientes para permitir el acceso a través del puerto 80.

Figura 21.
Configuración de la regla para el servicio FTP en Endian Firewall.



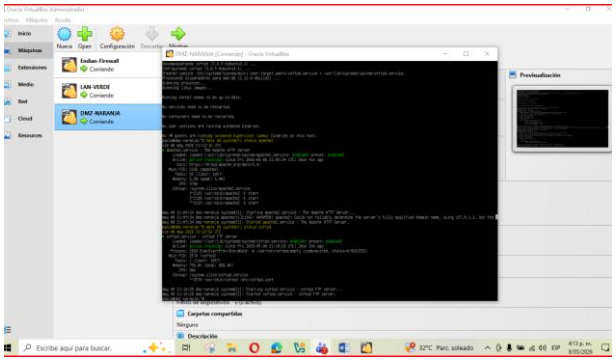
Fuente: Autoría propia.

4.2 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS.

Se configuraron reglas dentro del firewall para permitir o bloquear servicios específicos como HTTP, FTP e ICMP según la zona de red definida [5]. Estas políticas se implementaron con el propósito de controlar el flujo de tráfico entre los diferentes segmentos de la red, garantizando que únicamente los servicios autorizados pudieran establecer comunicación. La configuración incluyó la habilitación del servicio HTTP mediante el puerto 80 y del servicio FTP a través del puerto 21, permitiendo la publicación controlada de dichos servicios desde el servidor ubicado en la zona DMZ.

Asimismo, se aplicaron restricciones al protocolo ICMP para limitar las pruebas de conectividad mediante el comando ping, reduciendo posibles riesgos asociados al reconocimiento de la infraestructura de red. Adicionalmente, se verificó el estado de los servicios Apache y VSFTPD mediante los comandos systemctl status apache2 y systemctl status vsftpd, confirmando que ambos servicios se encontraban activos y funcionando correctamente dentro del servidor Ubuntu. Estas validaciones permitieron comprobar la correcta implementación de las reglas definidas en Endian Firewall y el adecuado funcionamiento de los servicios autorizados.

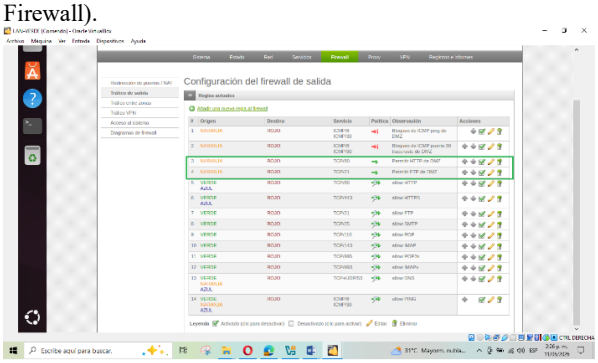
Figura 22.
Verificación del estado de los servicios Apache y VSFTPD en el servidor Ubuntu.



Fuente: Autoría propia.

Las reglas implementadas en el firewall incluyeron una política para permitir el tráfico HTTP desde la zona DMZ hacia la LAN, una segunda regla destinada a habilitar el servicio FTP entre estas zonas y una tercera política orientada al bloqueo del protocolo ICMP (Ping). Estas configuraciones permitieron administrar el tráfico de red de manera controlada, garantizando el acceso a los servicios autorizados y restringiendo las comunicaciones no permitidas.

Figura 23.
Configuración de servicios y reglas en la red LAN (Endian-Firewall).

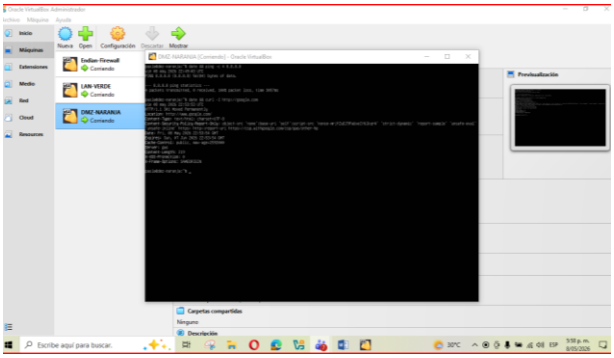


Fuente: Autoría propia.

4.3 PRUEBAS REALIZADAS PARA CADA REGLA

Con el propósito de validar el correcto funcionamiento de las reglas implementadas en Endian Firewall, se realizaron pruebas desde la máquina virtual ubicada en la zona DMZ (Naranja). Inicialmente, se ejecutó el comando ping hacia la dirección IP 8.8.8.8, obteniendo una pérdida total de paquetes (100%), lo que confirmó el correcto bloqueo del protocolo ICMP conforme a las políticas de seguridad establecidas. Posteriormente, se realizó una prueba mediante el comando curl hacia el sitio web Google, obteniendo una respuesta satisfactoria del servidor HTTP. Los resultados permitieron comprobar que las reglas configuradas funcionaban correctamente, permitiendo únicamente el tráfico autorizado y restringiendo las comunicaciones bloqueadas por el firewall.

Figura 24.
Verificación del acceso HTTP y bloqueo del protocolo ICMP desde la zona DMZ.



Fuente: Autoría propia.

5 CONCLUSIONES

Los sistemas GNU/Linux proporcionan herramientas ampliamente utilizadas para la administración de servicios y redes [10]. La implementación de la distribución Endian en Oracle VM VirtualBox permitió validar la correcta configuración de las zonas Green (LAN), Orange (DMZ) y Red (WAN), evidenciando que la segmentación lógica constituye un mecanismo esencial para la administración y protección de infraestructuras de red. La separación de niveles de confianza facilitó la aplicación de políticas diferenciadas de acceso y fortaleció el esquema de defensa en profundidad.

La configuración de reglas NAT permitió establecer comunicación entre las diferentes zonas de red y la WAN simulada, garantizando el acceso controlado a Internet desde la LAN y la DMZ. Las pruebas realizadas confirmaron el correcto funcionamiento de las políticas de traducción y reenvío de tráfico, demostrando la capacidad de Endian Firewall para administrar el flujo de datos entre redes internas y externas de manera segura.

La habilitación de los servicios HTTP y FTP, junto con la restricción del protocolo ICMP mediante reglas de firewall, permitió comprobar la efectividad de los mecanismos de control de acceso implementados. Las pruebas de conectividad evidenciaron que los servicios autorizados permanecieron disponibles para los usuarios, mientras que las comunicaciones restringidas fueron bloqueadas correctamente, fortaleciendo la seguridad de la infraestructura de red.

6 REFERENCIAS

[1] Stallings, W. (2011). *Network security essentials: Applications and standards* (4.ª ed.). Pearson.

[2] Goetz, C. (2004). *What is a network segment? Is a network segment the same as an Ethernet segment?* SearchNetworking. https://www.techtarget.com/searchnetworking/answer/What-is-a-network-segment-Is-a-network-segment-the-same-as-an-Ethernet-segment

[3] Ortiz Lozano, A. F. (2025). *Configuración y verificación del mecanismo NAT en Endian firewall para la comunicación entre LAN, DMZ y WAN*. Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/handle/10596/76974

[4] Endian. (2016). *Endian UTM 3.2 reference manual*. http://docs.endian.com/3.2/utm/index.html

[5] NETWORLD. (2021). *Servicios en DMZ o en LAN | ¿Dónde los pongo?, ¿por qué?* [Video]. YouTube. https://www.youtube.com/watch?v=qpWghjJZIMk

[6] Boucheron, B., & Camisso, J. (2025). *How to set up a firewall with UFW on Ubuntu*. DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu

[7] Canonical. (2026). *Ubuntu desktop documentation*. https://documentation.ubuntu.com/desktop/en/latest/

[8] Canonical Ltd. (2024). *Ubuntu Server 22.04 LTS documentation*. https://ubuntu.com/server/docs

[9] Oracle. (2020). *Oracle VM VirtualBox User Manual*. https://www.virtualbox.org/manual/

[10] Linux Professional Institute. (2022). *LPIC-1 Exam 101: Tema 102: Comandos GNU y Unix*. https://learning.lpi.org/pdfstore/LPI-Learning-Material-010-160-es.pdf