IMPLEMENTACIÓN DE ENDIAN FIREWALL PARA SEGMENTACIÓN DE RED Y REGLAS EN UN ENTORNO VIRTUALIZADO

Brayan Alexander Vargas Arguello
e-mail: ba.vargasar@unadvirtual.edu.co
Cristian Camilo Castañeda Morales
e-mail: cccastanedam@unadvirtual.edu.co
Kevin Franco Guerrero
e-mail: kafrancog@unadvirtual.edu.co

RESUMEN: *Este artículo describe la implementación de un entorno de seguridad utilizando GNU/Linux Endian Firewall en VirtualBox. Se configuró una instancia del sistema con tres zonas diferenciadas: verde para la red interna, roja para el acceso a Internet y naranja para la DMZ, asegurando su correcta comunicación mediante la asignación de interfaces virtuales. Posteriormente, se establecieron reglas de NAT para permitir la salida de tráfico desde la LAN y la DMZ hacia la red externa, validando su funcionamiento a través de pruebas de conectividad y verificación del reenvío de puertos. Finalmente, se habilitaron los servicios HTTP y FTP en la zona DMZ y se implementaron políticas de restricción, como el bloqueo del protocolo ICMP, comprobando la efectividad de dichas reglas mediante pruebas de acceso y monitoreo del tráfico. Los resultados demostraron un control adecuado del flujo entre zonas y el funcionamiento consistente de las políticas configuradas.*

PALABRAS CLAVE: Endian Firewall, NAT, segmentación de red, servicios zona DMZ.

1 INTRODUCCIÓN

La seguridad constituye un elemento fundamental en la protección de infraestructuras de red, especialmente en entornos donde es necesario segmentar el tráfico y controlar el acceso entre diferentes zonas. En este contexto, las soluciones basadas en software libre, como GNU/Linux Endian Firewall, ofrecen mecanismos eficaces para gestionar comunicaciones, aplicar políticas de seguridad y establecer reglas que permitan un funcionamiento confiable del sistema.

El proyecto desarrollado se centró en la implementación de Endian Firewall en un entorno virtualizado mediante VirtualBox, configurando una arquitectura compuesta por tres zonas: verde (LAN), roja (WAN) y naranja (DMZ). A partir de esta estructura, se realizaron procedimientos orientados a la creación de reglas NAT para habilitar la salida de tráfico desde la LAN y la DMZ hacia una red externa simulada, así como pruebas de conectividad que permitieron validar su funcionamiento.

Adicionalmente, se configuraron servicios en la DMZ, habilitando HTTP y FTP, y se establecieron políticas de restricción como el bloqueo del protocolo ICMP, con el fin de fortalecer el aislamiento entre segmentos de red. Los resultados obtenidos evidencian el adecuado control del flujo de información y la efectividad de las reglas aplicadas en cada zona. A continuación, se describen las configuraciones implementadas, los procedimientos realizados y el comportamiento observado durante las pruebas.

2 CONOCIENDO ENDIAN

Endian Firewall Community es una distribución GNU/Linux diseñada específicamente para la seguridad de red, que convierte hardware estándar en un dispositivo UTM (Unified Threat Management) de código abierto [1].

Entre sus características principales se incluyen [2]:

- Un firewall inspección de estado bidireccional, que controla tanto el tráfico entrante como el saliente.
- VPNs (OpenVPN e IPSec), para crear túneles seguros y conectar redes remotas.
- Proxy de aplicación (HTTP, FTP, SMTP, POP3), con capacidad para filtrado de contenido y antivirus para tráfico web.
- Gestión de múltiples zonas de red, como LAN (verde), DMZ (naranja) y WAN (roja), lo que permite segmentar el tráfico con políticas específicas.
- Sistema de detección de intrusos (IDS), registro de tráfico y estadísticas, así como una interfaz de administración web (HTTPS).

Endian ofrece múltiples beneficios que lo convierten en una solución robusta para la seguridad perimetral. Su capacidad de segmentar la red en zonas diferenciadas —green, red y orange— permite aislar niveles de confianza y aplicar políticas específicas como reglas NAT, control de servicios y filtrado de tráfico, favoreciendo una administración más precisa del entorno. Además, su enfoque de gestión unificada de amenazas (UTM) integra funciones esenciales como firewall, proxy, VPN, filtrado de contenido y antivirus, lo que reduce la necesidad de herramientas adicionales y mejora la visibilidad general del tráfico [3].

Su disponibilidad como software libre y en versión comunitaria lo hace flexible y escalable, ideal para laboratorios, entornos educativos o pequeñas infraestructuras, especialmente al ejecutarse fácilmente en máquinas virtuales como VirtualBox. Endian también incorpora mecanismos avanzados

de seguridad, como inspección de estado, IDS y soporte VPN, complementados con capacidades de proxy y filtrado que refuerzan la protección frente a amenazas externas. Finalmente, su interfaz web simplifica la administración diaria y, pese a no incluir soporte comercial en la edición comunitaria, cuenta con una comunidad activa que aporta documentación y asistencia, facilitando su adopción y uso continuo [1][2][3].

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

3.1 CONFIGURACIÓN DE VIRTUAL BOX

Para la implementación de Endian Firewall se utilizó UTM (Universal Turing Machine) como plataforma de virtualización en macOS. Dado que Endian Firewall está compilado para arquitectura x86_84 y el sistema host emplea un procesador Apple Silicon (ARM64), fue necesario configurar UTM en modo emulación x86_64. Los demás integrantes del grupo usaron Oracle Virtual Machine.

Tabla 1. Especificaciones de la Máquina Virtual

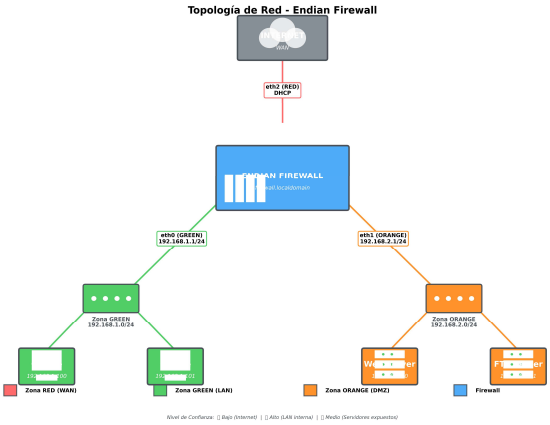
Parámetro	Configuración
Modo de ejecución	Emulación x86_64
Arquitectura	x86_64 (64 bits)
Sistema	Standard PC (i440FX + PIIX, 1996)
Firmware	BIOS Legacy
Memoria RAM	1024 MB
Procesador	2 núcleos virtuales
Almacenamiento	10 GB (VirtIO)
Controlador de disco	VirtIO Block Device

Fuente: Autoría propia

Configuración de Interfaces de Red La configuración de red constituye el elemento más crítico de la implementación, ya que determina la correcta segmentación en zonas de seguridad diferenciadas. Se agregaron tres adaptadores de red virtuales a la máquina virtual del firewall [3].

La arquitectura de red se diseñó con tres segmentos independientes, cada uno asociado a un nivel de confianza diferente. como se muestra en la Fig. 1

Figura 1. Topología de red implementada



Fuente. Autoría propia.

La topología implementada establece el firewall Endian como punto central de control entre Internet y las redes internas. La zona RED proporciona conectividad mediante DHCP, mientras que las zonas GREEN y ORANGE operan con direccionamiento estático, permitiendo un control granular del tráfico entre segmentos de red.

Interfaz 1 - Zona RED (Internet/WAN):

- Nombre en VM: Red (Adaptador 1)
- Dispositivo que será asignado: eth2
- Modo de red: Red compartida (Shared Network)
- Modelo de adaptador: virtio-net-pci
- Propósito: Proporcionar conectividad a Internet
- Tipo de asignación IP: DHCP (obtenida del host)
- Nivel de confianza: Mínimo (tráfico no confiable)

Esta interfaz conecta el firewall al exterior, recibiendo tráfico de Internet. Todo el tráfico proveniente de esta zona debe ser inspeccionado y filtrado rigurosamente.

Interfaz 2 - Zona GREEN (LAN):

- Nombre en VM: Red (Adaptador 2)
- Dispositivo que será asignado: eth0
- Modo de red: Red compartida
- Modelo de adaptador: virtio-net-pci
- Propósito: Red interna de la organización
- Tipo de asignación IP: Estática (192.168.1.1/24)
- Nivel de confianza: Alto (usuarios internos)
- Servidor DHCP: Habilitado (192.168.1.100-200)

Esta interfaz conectará los equipos cliente de la red interna (estaciones de trabajo, laptops). Se configurará un servidor DHCP para asignación automática de direcciones IP.

Interfaz 3 - Zona ORANGE (DMZ):

- Nombre en VM: Red (Adaptador 3)
- Dispositivo que será asignado: eth1
- Modo de red: Red compartida
- Modelo de adaptador: virtio-net-pci
- Propósito: Zona desmilitarizada para servidores públicos

- Tipo de asignación IP: Estática (192.168.2.1/24)
- Nivel de confianza: Medio (servicios expuestos)
- Rango para servidores: 192.168.2.10-50

Esta interfaz será la zona desmilitarizada (DMZ) desde la cual se ejecutará el servidor.

3.2 INSTALACIÓN DE ENDIAN

La instalación de Endian Firewall Community Edition 3.3.2 se realizó mediante un asistente interactivo basado en texto. El proceso inició arrancando la máquina virtual desde la imagen ISO [4].

3.2.1 PROCESO DE INSTALACIÓN

La pantalla de bienvenida del instalador (Fig. 2) presentó una advertencia indicando que cancelar el proceso en cualquier momento reiniciaría el equipo. Se aceptó la licencia GPL y se procedió con la configuración del disco [].

Figura 2. Instalación Endian

Fuente. Autoría propia.

El instalador detectó el disco virtual `/dev/vda` de 10 GB y solicitó confirmación para el particionamiento. Se confirmó la operación, permitiendo al sistema crear automáticamente las particiones necesarias, el sistema de archivos ext4 y configurar el gestor de arranque GRUB2.

Se deshabilitó la consola serial (Fig. 3) ya que la administración se realizaría mediante SSH e interfaz web HTTPS.

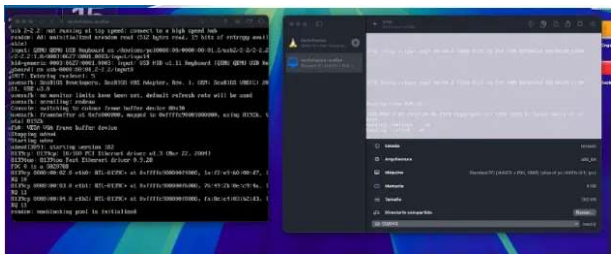
Figura 3. Configuración de consola serial, opción deshabilitada para este entorno virtualizado.

Fuente. Autoría propia.

El instalador copió los archivos del sistema al disco duro, proceso que tomó aproximadamente 10-15 minutos debido a la emulación x86_64 en procesador ARM64. Al finalizar, se removió el ISO del lector virtual y se reinició el sistema.

El sistema arrancó exitosamente desde el disco instalado, presentando el menú de consola de Endian (Fig. 4) que confirmó la instalación correcta y mostró las interfaces de red detectadas listas para configuración.

Figura 4. Menú principal de consola de Endian Firewall tras la instalación exitosa.



Fuente. Autoría propia.

Tabla 2. Duración de la Instalación

Etapa	Tiempo
Configuración inicial	3-5 min
Copia de archivos	10-15 min
Instalación gestor de arranque	1 min
TOTAL	**14-21 min**

Fuente. Autoría propia.

La instalación se completó exitosamente, detectando las tres interfaces de red (eth0, eth1, eth2) necesarias para las zonas de seguridad. El sistema quedó listo para la configuración de red descrita en la siguiente sección.

3.3 CONFIGURACIÓN DE ZONAS

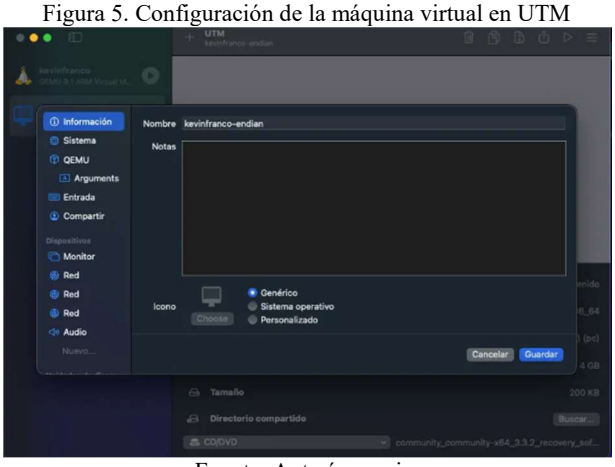
La seguridad perimetral mediante firewall con segmentación de red en zonas DMZ permite establecer niveles diferenciados de seguridad, aislando recursos críticos de la organización [1]. Este trabajo documenta la implementación de Endian Firewall Community Edition 3.3.2 con tres zonas de seguridad: RED (Internet/WAN), GREEN (LAN) y ORANGE (DMZ), ejecutado sobre UTM en Mac con procesador Apple Silicon M4.

Tabla 3. Asignación de Interfaces

Interfaz	Zona	Tipo	IP	Función
eth2	RED	DHCP	192.168.64.10/24	Internet/WAN
eth0	GREEN	Estática	192.168.1.1/24	LAN
eth1	ORANGE	Estática	192.168.2.1/24	DMZ

Fuente: Autoria Propia

Figura 5. Configuración de la máquina virtual en UTM



Fuente. Autoría propia.

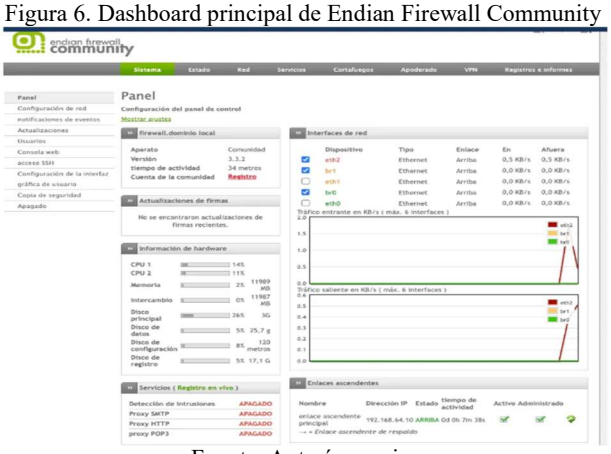
Configuración aplicada:

- GREEN: 192.168.1.1/24, DHCP Server habilitado.
- ORANGE: 192.168.2.1/24.
- RED: DHCP, device eth2. SSH y puertos 22, 80, 10443: Habilitados.
- Hostname: firewall.localdomain

3.4 CONFIRMACIÓN DEL RESULTADO

Se accede al dashboard por medio de un equipo configurado en zona verde para confirmar la conexión y la configuración realizada: Fig. 6, Fig. 7 y Fig.8.

Figura 6. Dashboard principal de Endian Firewall Community



Fuente. Autoría propia.

Endian Firewall Community 3.3.2 instalado exitosamente. Dashboard muestra:

- Uso CPU: 14% (CPU1), 11% (CPU2)
- Memoria: 2% (11989 MB disponibles)
- Disco: 26% (3G de 12 GB)
- Tiempo actividad: 34 minutos

Figura 7. Tabla de enrutamiento IP del kernel

Fuente. Autoría propia.

Panel "Estado de la red" confirmó: Tres interfaces ethernet (eth0, eth1, eth2) en estado UP. Tarjetas NIC: Realtek Semiconductor [Enlace OK] (x3). Bridges br0 (GREEN) y br1 (ORANGE) operativos.

Servicios activos: SSH (puerto 22): Administración remota. Interfaz web (puerto 10443): Gestión HTTPS. Servidor DHCP: Zona GREEN.

Servicios disponibles (deshabilitados por defecto): IDS, Proxy SMTP, HTTP, POP3.

Figura 8. Panel de estado de la red mostrando las interfaces

Fuente. Autoría propia.

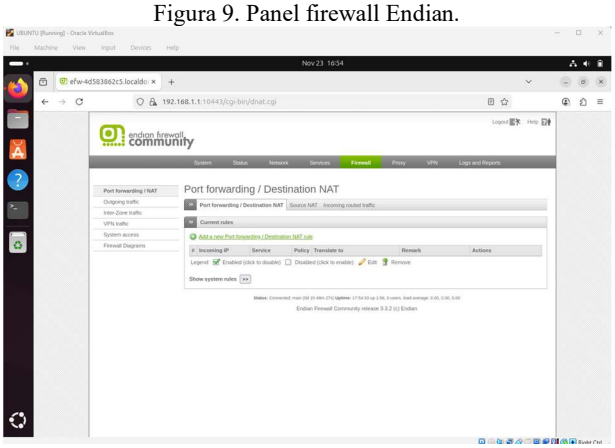
Esquema de direccionamiento unificado: Firewall: firewall.localdomain. GREEN (LAN): Red: 192.168.1.0/24, Gateway: 192.168.1.1, DHCP: 192.168.1.100-200. ORANGE (DMZ): Red: 192.168.2.0/24, Gateway: 192.168.2.1, Servidores: 192.168.2.10-50.

Acceso: Usuario: admin. URL: https://192.168.1.1:10443 (desde GREEN). Alternativa: https://192.168.64.10:10443 (desde host).

4 TEMÁTICA 2: CONFIGURACIÓN NAT

Una vez configuradas las zonas, verde y naranja en Endian, se procede a crear las reglas NAT, en el menú firewall [4]: Fig. 9.

Figura 9. Panel firewall Endian.



Fuente. Autoría propia.

4.1 Conexión red LAN hacia la WAN

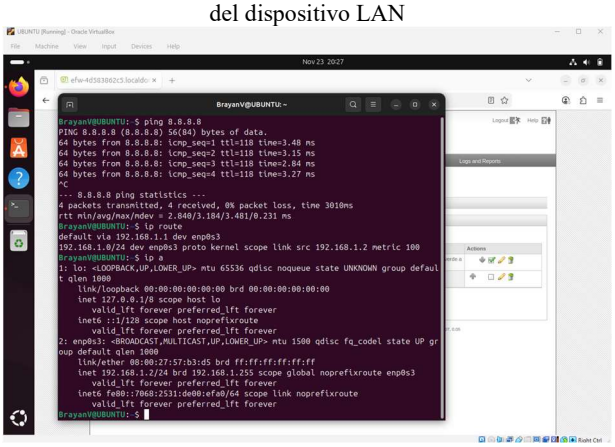
El propósito de esta configuración es permitir que los equipos de la LAN interna (Ubuntu Desktop) accedan a recursos de la WAN (zona roja) mediante la traducción de direcciones privadas a una dirección pública, garantizando conectividad a Internet y manteniendo la seguridad de la red [5][6]. Para esto se realizó en el firewall la creación de reglas de masquerading para la interfaz WAN: Fig. 10.

Figura 10. Creación regla conexión red LAN a WAN

Fuente. Autoría propia.

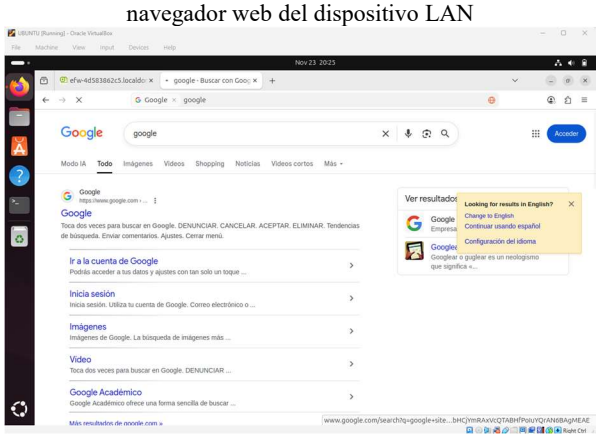
Una vez creada la regla aplicamos los cambios y verificamos que desde nuestro desktop tengamos conexión a internet haciendo ping hacia el DNS de Google (8.8.8.8): Fig. 11. Igualmente podemos verificar la conexión utilizando el navegador web del desktop: Fig. 12.

Figura 11. Comprobación conexión a internet desde la terminal del dispositivo LAN



Fuente. Autoría propia.

Figura 12. Comprobación conexión a internet desde el navegador web del dispositivo LAN

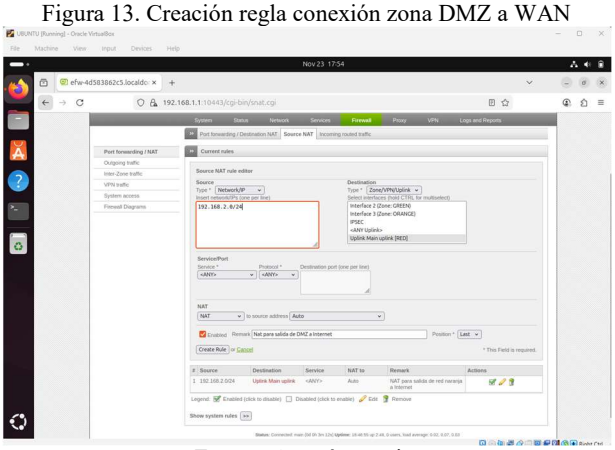


Fuente. Autoría propia.

4.2 *Conexión zona DMZ hacia la WAN*

El objetivo de esta configuración es permitir que los servicios ubicados en la zona DMZ (servidores expuestos, como web o correo) tengan acceso controlado hacia la WAN (zona roja), garantizando conectividad externa sin comprometer la seguridad de la LAN interna [6]. Para esto se realizó la configuración mediante reglas de Source NAT (SNAT) y masquerading para la interfaz WAN, con el fin de traducir las direcciones privadas de la DMZ a la dirección pública de salida: Fig. 13.

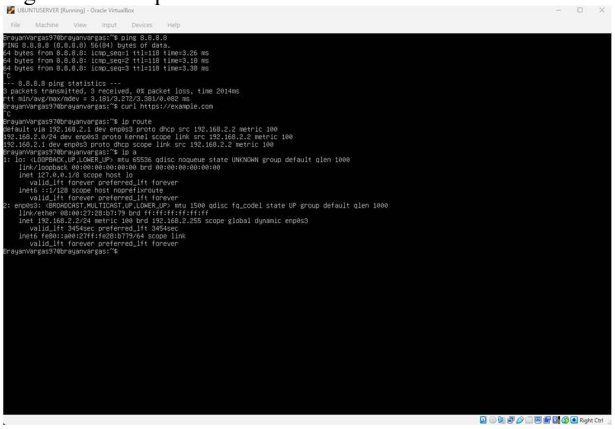
Figura 13. Creación regla conexión zona DMZ a WAN



Fuente. Autoría propia.

Una vez creada la regla aplicamos los cambios y verificamos que desde nuestro servidor tengamos conexión a internet haciendo ping hacia el DNS de Google (8.8.8.8): Fig. 14. Evidenciando que el tráfico saliente es correctamente enrutado y enmascarado por el firewall.

Figura 14. Comprobación conexión a internet desde el servidor



Fuente. Autoría propia.

Esta validación garantiza que Endian puede actuar como intermediario entre las zonas internas (verde y naranja) y la red externa (roja), permitiendo la salida controlada de tráfico hacia Internet.

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

La tercera parte del proyecto se enfocó en la administración de servicios y políticas de acceso desde la Zona Desmilitarizada (DMZ), con el objetivo de controlar de manera precisa la interacción entre los servidores expuestos y el resto de la infraestructura. En esta etapa se configuraron los servicios esenciales de la DMZ, permitiendo el acceso a HTTP y FTP desde el servidor ubicado en Ubuntu Server, con el fin de asegurar su disponibilidad para la red interna. Paralelamente, se definieron reglas orientadas al fortalecimiento de la seguridad perimetral, entre ellas la restricción del protocolo ICMP, con el propósito de impedir la ejecución de pruebas de eco (ping) hacia direcciones internas y evitar la exposición innecesaria de información sobre la red.

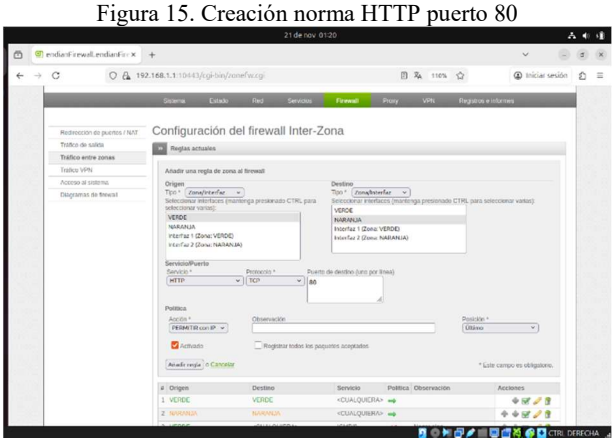
Para completar este objetivo se crearon nuevas normas en el firewall, la creación de las mismas se realiza desde el dashboard, accediendo a la pestaña Firewall y luego a la opción Trafico entre zonas [7].

Damos clic en la opción Añadir una nueva regla de firewall Inter-Zona, aquí crearemos la norma seleccionando origen, destino, servicio, protocolo, si es necesario configuramos los puertos, y en el apartado política seleccionamos si queremos permitir con IP, permitir, denegar o rechazar, debemos recordar que la posición define la prioridad con la que la norma será aplicada, por ejemplo la norma 3 tiene prioridad sobre la norma 8 [#] esto será importante para el punto 2 de ping, por tal motivo también debemos elegir su posición en el panel de creación. Luego de terminar la configuración debemos dar clic en Añadir regla, aparecerá un modal en verde con el botón aplicar los cambios damos clic en ese botón para aplicar los cambios en las normas [8].

5.1 PERMITIR HTTP POR PUERTO 80

Se crea la norma como se muestra en al Fig. 15, teniendo en cuenta los parámetros de configuración, como la selección del origen y destino, el servicio en la opción HTTP, proceso TCP y puerto 80, seleccionamos permitir con IP, damos clic en Añadir regla y aplicamos la norma.

Figura 15. Creación norma HTTP puerto 80

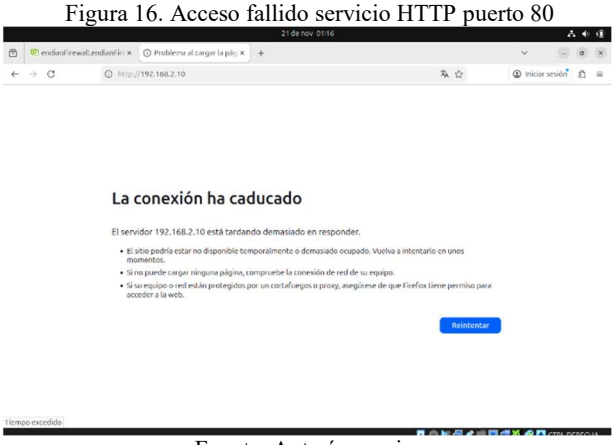


Fuente. Autoría propia.

Se comprueba la efectividad de la norma intentando acceder a la IP del servidor 192.168.2.10 desde el navegador, si existe un servicio web como apache, este se redireccionará desde el navegador con la IP al puerto 80 [9].

Se realiza un intento de acceso previo a su activación Fig. 16. Que resulta fallido, y un acceso exitoso al servicio posterior a la activación de la misma Fig. 17.

Figura 16. Acceso fallido servicio HTTP puerto 80



Fuente. Autoría propia.

Figura 17. Acceso exitoso servicio HTTP puerto 80

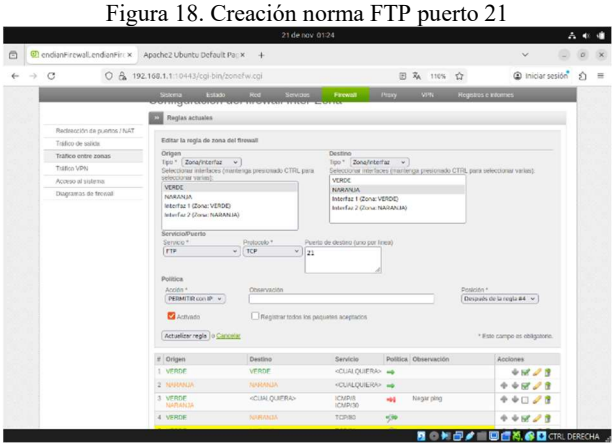
Fuente. Autoría propia.

5.2 PERMITIR FTP PUERTO 21

Con la finalidad de llevar a cabo es te proceso previo a la creación de las normas se realiza instalación del paquete vsftpd, en el servidor para permitir conexión FTP [10].

Igual que en el punto anterior al crear la regla de zona se elige la opción zona/interfaz en origen y destino, luego se selecciona origen la zona verde y destino la zona naranja, en servicio se elige la opción FTP, proceso TCP y puerto 21, seleccionamos la acción Permitir con IP, damos clic en Añadir regla y aplicamos la norma. Se puede ver la creación de la mima en la Fig. 18.

Figura 18. Creación norma FTP puerto 21



Fuente. Autoría propia.

Se comprueba la efectividad de la norma intentando realizar por consola desde nuestro cliente un acceso al servicio FTP del servidor con el comando (ftp 192.168.2.10), se realiza un intento de acceso previo a su activación. Que resulta fallido y debe ser cancelado, y un acceso exitoso al servicio posterior a la activación de la misma Fig. 19. Donde vemos que se solicitan los datos de acceso y se inicia la conexión.

Figura 19. Acceso fallido servicio FTP puerto 21

Fuente. Autoría propia.

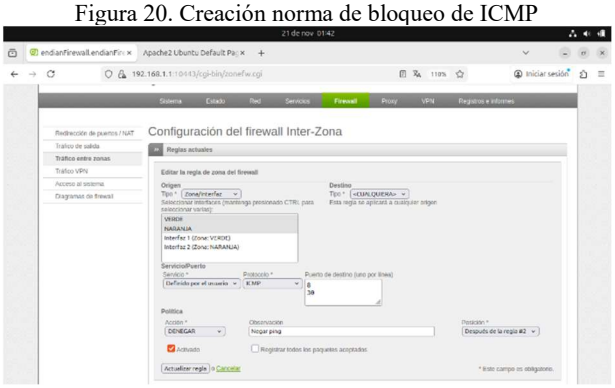
5.3 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR HACER PING EN LA RED

Para completar este punto activamos primero una norma que ya estaba por defecto que permite el acceso de cualquier servicio desde nuestra zona verde a nuestra zona naranja, clonamos la norma y la editamos para que ahora sea de zona naranja a verde, de esta forma ya podremos hacer ping desde nuestro equipo servidor (192.168.2.10), a nuestro cliente (192.168.1.5) y viceversa, y confirmar que el bloqueo funciona.

Se crea la regla como se ve en la Fig. 20, seleccionando en origen nuestras dos zonas y en destino <cualquiera>, aunque si se quisiera solo bloqueo de server a cliente origen seria zona naranja y destino zona verde, por fines académicos se dejaran las dos zonas para mostrar la efectividad bidireccional, seleccionamos el protocolo y el servicio se pondrá automático, escribimos los puertos 8 y 30, y la acción damos en Denegar,

dejaremos la regla en un puesto alto para que tenga prioridad sobre las reglas que se crearon al inicio de este punto para permitir cualquier interacción, luego la creamos y aplicamos los cambios.

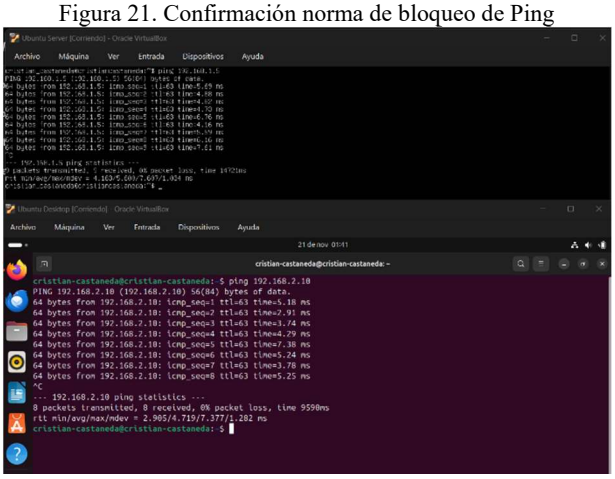
Figura 20. Creación norma de bloqueo de ICMP



Fuente. Autoría propia.

Previo a la activación de la norma, realizamos ping del cliente al servidor y del servidor al cliente, y este resuelve de forma exitosa, enviando los paquetes, se procede a activar la norma y se ejecuta nuevamente el ping, obteniendo que ahora las maquinas ya no obtienen resultados, se termina el comando con CTRL+c, podemos ver que se enviaron paquetes, pero ninguno fue recibido y se perdió el 100%, por lo tanto, la creación de la norma fue exitosa, como se evidencia en la Fig. 21.

Figura 21. Confirmación norma de bloqueo de Ping



Fuente. Autoría propia.

6 CONCLUSIONES

La implementación de Endian Firewall permitió construir una arquitectura de seguridad perimetral completamente funcional, basada en un modelo de segmentación por zonas que facilitó la definición de distintos niveles de confianza dentro de la red. La correcta configuración de las interfaces virtuales asignadas a las zonas GREEN, RED y ORANGE permitió establecer un aislamiento claro entre la LAN, la DMZ y la salida hacia Internet, consolidando una estructura escalable y coherente con prácticas profesionales de seguridad en redes. La interfaz web de administración de Endian demostró ser una herramienta altamente intuitiva, reduciendo la complejidad asociada a la configuración manual y permitiendo gestionar reglas, servicios y monitoreo de tráfico de manera eficiente.

En la segunda fase, la configuración de reglas NAT garantizó la comunicación controlada desde la LAN y la DMZ hacia la red externa. El uso de técnicas como masquerading aseguró que los equipos internos pudieran acceder a Internet sin exponer sus direcciones privadas, preservando la integridad de los segmentos internos y permitiendo validar el funcionamiento del firewall como punto central de salida.

Finalmente, la administración de servicios en la zona DMZ permitió evidenciar la capacidad de Endian para controlar el acceso a servidores expuestos mediante reglas específicas. La habilitación de HTTP y FTP demostró la correcta disponibilidad de servicios desde la red interna, mientras que la restricción del protocolo ICMP fortaleció la superficie de seguridad al impedir respuestas de diagnóstico que podrían ser utilizadas para reconocimiento de red. Estas configuraciones, junto con las pruebas realizadas, confirman que Endian Firewall es una solución eficaz para gestionar servicios críticos, aplicar políticas de acceso y mantener un equilibrio adecuado entre funcionalidad y protección.

En conjunto, las tres temáticas desarrolladas permitieron construir un entorno seguro, segmentado y completamente administrable, reafirmando el valor de Endian Firewall como alternativa sólida para el aprendizaje y la implementación de infraestructuras perimetrales en entornos virtualizados.

7 REFERENCIAS

[1] Endian. (2025). Endian Community Firewall. https://www.endian.com/en/community/

[2] ITM. (n.f.) Endian Firewall. https://www.i-t-m.com/productos-servicios/seguridad/endian-firewall

[3] Geier, E. (2010). Endian Firewall, Router & Server Set Up. ServerWatch. https://www.serverwatch.com/guides/setting-up-an-open-source-server-firewall-and-router-on-endian-part-1/

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

[5] IBM i. (2025). Documentación Crear Reglas NAT https://www.ibm.com/docs/es/i/7.6.0?topic=rules-creating-nat

[6] Walton, A. (2018). Configuración de la NAT: Ejemplos y Comandos. CCNA Desde Cero. https://ccnadesdecero.es/configuracion-nat-estatica-dinamica-pat/

[7] Araque, D., Gonzalez, C. y Deossa, A. (2009). Servidor firewall Endian [Trabajo académico, SENA – Regional Antioquia, Programa de Administración de Redes de Computadores]. https://es.slideshare.net/slideshow/manual-endian/1360390

[8] Endian (2019). Endian UTM 6.6 Reference Manual. Firewall. https://docs.endian.com/6.6/utm/firewall.html

[9] Apache Software Foundation. (2025). Mapeo de direcciones y puertos. Servidor HTTP Apache Versión 2.5. https://httpd.apache.org/docs/trunk/es/bind.html

[10] Pozo Martin, J. (2024). Instalación y administración de un servidor FTP utilizando vsFTPd en un entorno de máquinas virtuales con Ubuntu y Windows. Scribd. https://es.scribd.com/document/875490332/Pozo-Martin-Jessica-Sri04-Tarea04-v1