Estrategias de Seguridad en Infraestructuras Linux: Análisis Práctico de Firewall, LAN, DMZ y WAN

Luis Fernando Ochoa Silva
lfochoa@unadvirtual.edu.co
Jhoan Styven Chamorro Diaz
jschamorrod@unadvirtual.edu.co
Gloria Stella Calderón Torres
gscalderont@unadvirtual.edu.co
Daira Carolina Rojas Rivera
dcrojasriv@unadvirtual.edu.co

RESUMEN: *Este artículo técnico documenta la metodología de diseño e implementación de una arquitectura de seguridad perimetral robusta utilizando el firewall de código abierto Endian Firewall (EFW), desplegado en un entorno virtualizado sobre Oracle VirtualBox. El objetivo principal fue establecer un modelo de red segmentada, funcional y seguro, ideal para la experimentación académica. La implementación se centró en la configuración crítica de tres zonas de seguridad diferenciadas: la zona Verde (LAN), la zona Roja (WAN) y la zona Naranja (DMZ), mediante la asignación y gestión de interfaces de red virtuales. Se detalló el proceso de configuración de traducción de direcciones de red (NAT) para asegurar la conectividad a Internet desde las redes internas de forma controlada.*

PALABRAS CLAVE: DMZ, Endian, Firewall, LAN, NAT, Proxy, Segmentación, Seguridad Perimetral, WAN, Zonas.

1 INTRODUCCIÓN

En el panorama actual de la ciberseguridad, la protección de los recursos informáticos internos frente a las amenazas externas es una necesidad imperativa para cualquier organización, incluyendo entornos académicos y empresariales. El rápido crecimiento del tráfico de red y la complejidad de los ataques exigen la implementación de una seguridad perimetral robusta que actúe como primera línea de defensa. Es en este contexto que los firewalls de nueva generación se han consolidado como herramientas esenciales para inspeccionar, controlar y gestionar el flujo de datos. Este trabajo aborda la implementación práctica de estas defensas en un ambiente controlado y simulado, utilizando una herramienta de código abierto para demostrar su eficacia y configuración.

La base de esta estrategia de seguridad reside en la segmentación de la red, un principio arquitectónico fundamental. Para ello, se seleccionó e implementó Endian Firewall (EFW) en un entorno virtualizado, lo cual permitió la creación y gestión precisa de las zonas de seguridad clave: la Zona Verde (LAN), la Zona Roja (WAN) y la Zona Naranja (DMZ). La Temática 1 se centra en detallar esta configuración inicial, desde el hardware virtual hasta la asignación de interfaces, estableciendo la estructura física y lógica necesaria para aislar los distintos segmentos de la red, asegurando que cada host opere bajo un nivel de confianza y acceso predefinido.

Una vez definida la arquitectura física, el foco se trasladó a la gestión del tráfico de red en las capas inferiores. La Temática 2 y 3 abordan cómo se logró la conectividad externa mediante la configuración de la Traducción de Direcciones de Red (NAT), esencial para que los hosts internos puedan acceder a Internet de forma controlada. Posteriormente, se establecieron las Reglas de Acceso del firewall para regular el flujo entre zonas. Esto implicó la aplicación rigurosa del principio de mínimo privilegio, configurando políticas específicas para permitir servicios necesarios (como HTTP y FTP desde la DMZ) y, de forma crítica, bloquear tráfico de control (como ICMP) en segmentos vulnerables, validando la efectividad de cada regla directamente desde la línea de comandos (CLI) de los sistemas operativos host.

Finalmente, la Temática 4 (o 5) escaló el control de la red a la capa de aplicación mediante la implementación de un servicio Proxy HTTP. Esta funcionalidad permitió la aplicación de políticas de seguridad más sofisticadas, como el filtrado web a través de listas negras personalizadas y la exigencia de autenticación de usuarios. Este nivel de control demuestra cómo un firewall perimetral puede ir más allá de la gestión básica de puertos y protocolos para convertirse en una herramienta integral de gestión de contenidos y comportamiento del usuario. El resultado final es un ambiente de laboratorio que sirve como una prueba de concepto exhaustiva para el fortalecimiento de la seguridad perimetral.

2 TEMÁTICAS

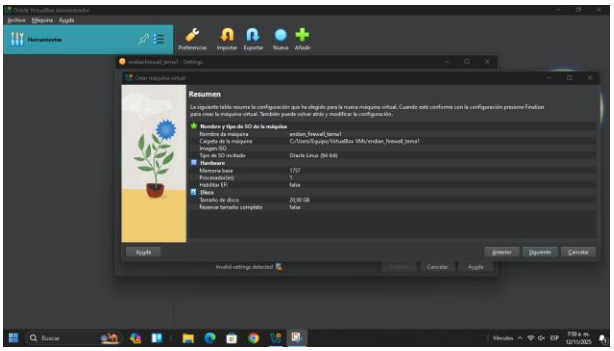
2.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

La implementación de la seguridad perimetral comenzó con el aprovisionamiento del entorno virtualizado, que es esencial para simular la red corporativa. El proceso se desarrolló en tres fases críticas: configuración de la máquina virtual (MV), segmentación de red a través de interfaces virtuales y la instalación del sistema operativo firewall con sus validaciones iniciales.

2.1.1 CONFIGURACIÓN DEL ENTORNO VIRTUALIZADO Y ASIGNACIÓN DE RECURSOS

El software seleccionado para la virtualización fue Oracle VirtualBox, sobre el cual se creó la MV destinada a alojar el Endian Firewall Community (EFW). Para garantizar un rendimiento óptimo en el entorno de laboratorio, se asignaron recursos de hardware virtual que incluyen 1757 MB de memoria RAM y un núcleo de CPU [1]. Esta asignación preliminar es crucial para el desempeño del sistema operativo y sus servicios internos.

Ilustración 1 Asignación de Recursos de Memoria y CPU en la MV de Endian



Fuente: autoría propia

2.1.2 SEGMENTACIÓN LÓGICA Y CONFIGURACIÓN DE INTERFACES DE RED

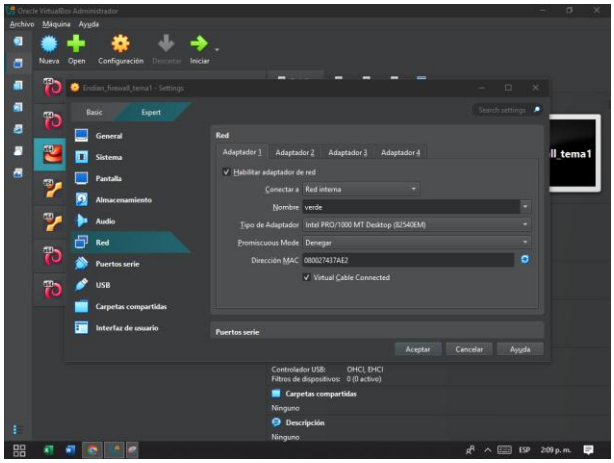
El paso fundamental para el establecimiento de la seguridad perimetral fue la segmentación de la red mediante la configuración de las interfaces virtuales. Se asignaron tres adaptadores de red a la MV de EFW, cada uno mapeado a una zona de seguridad distinta conforme a las buenas prácticas de firewalling.

Tabla 1 Segmentación que se utilizara

zona	Interfaz VirtualBox	Tipo de red VirtualBox	Rango IP
Verde (LAN)	Adaptador 1	Red Interna	192.168.10.1
Naranja (DMZ)	Adaptador 2	Red Interna	192.168.20.1
Roja (WAN)	Adaptador 3	NAT	Asignada por VirtualBox

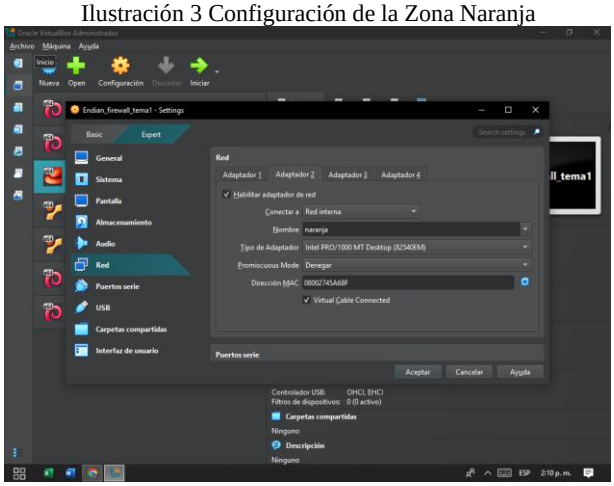
Fuente: autoría propia

Ilustración 2 Configuración de la Zona Verde



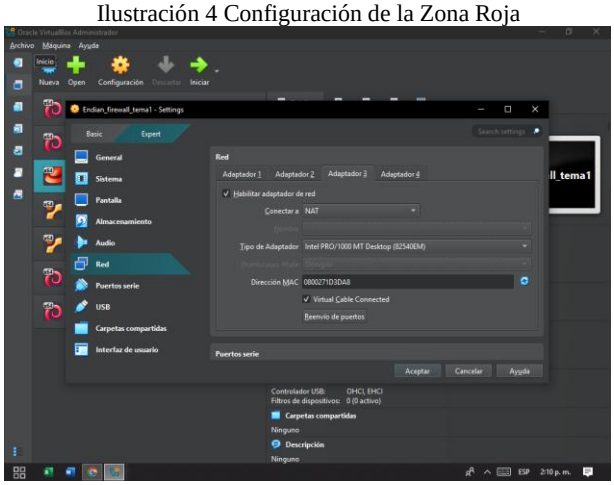
Fuente: autoría propia

Ilustración 3 Configuración de la Zona Naranja



Fuente: autoría propia

Ilustración 4 Configuración de la Zona Roja



Fuente: autoría propia

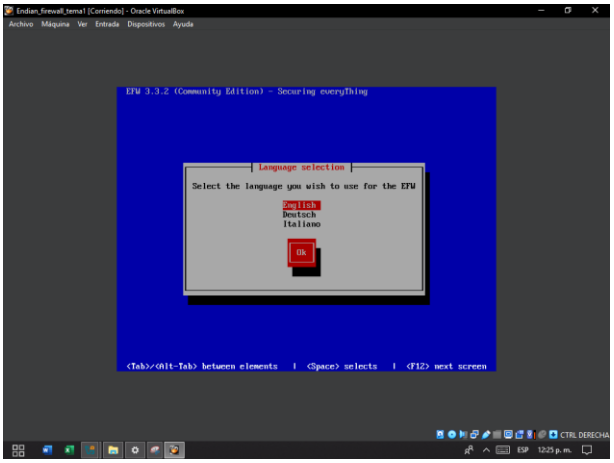
2.1.3 INSTALACIÓN EFECTIVA DE ENDIAN Y CONFIGURACIÓN DE LAS ZONAS DE RED

La instalación de EFW se llevó a cabo utilizando la imagen ISO mediante el proceso asistido. Durante esta etapa,

se seleccionaron los parámetros fundamentales, incluyendo el idioma, el uso de la totalidad del disco duro virtual para la instalación y la habilitación del puerto serial para posibles tareas [1].

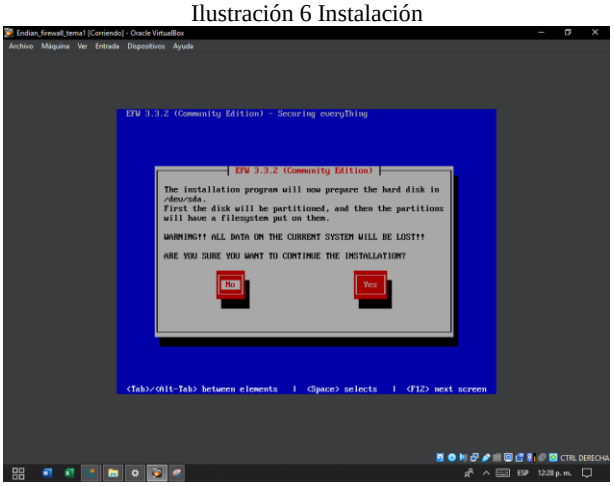
Al finalizar la instalación y reiniciar el sistema, el firewall se inicializó en su consola administrativa. En este punto, se confirmó que el sistema había asignado automáticamente la dirección IP 192.168.10.1 a la interfaz de la Zona Verde. Esta dirección sirve como Gateway y punto de acceso inicial para la configuración web posterior. A pesar de esta asignación automática, la configuración de otras zonas críticas se realizó por medio de la Línea de Comandos (CLI). Específicamente, la IP estática para la Zona Naranja (DMZ) se configuró directamente en la consola de Endian antes de acceder al entorno gráfico, seleccionando la opción 5 (Configuración de red) del menú principal para establecer su Gateway en $192.168.20.1$.

Ilustración 5 selección de idioma



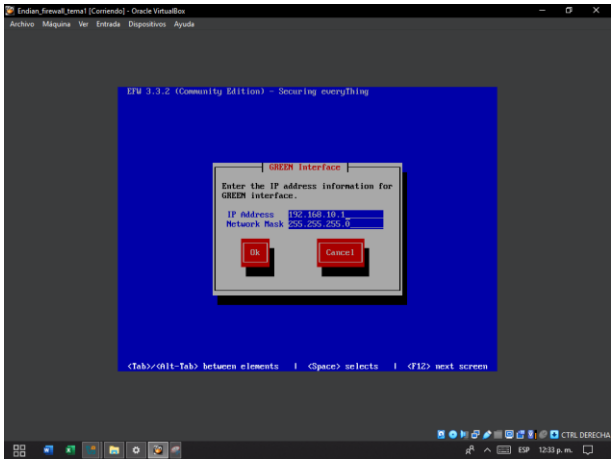
Fuente: autoría propia

Ilustración 6 Instalación



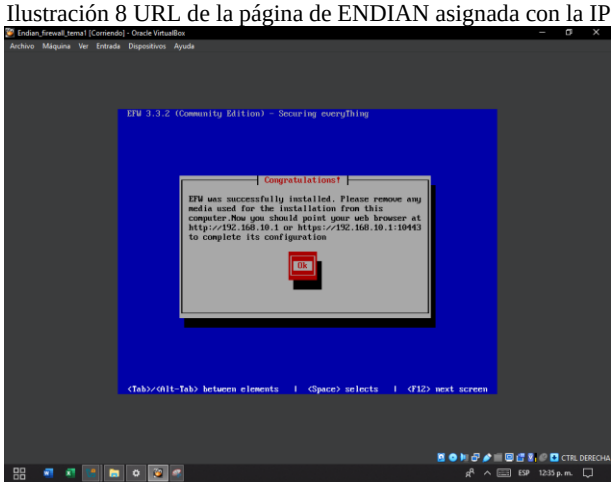
Fuente: autoría propia

Ilustración 7 IP seleccionada para el trabajo



Fuente: autoría propia

Ilustración 8 URL de la página de ENDIAN asignada con la IP



Fuente: autoría propia

2.1.4 FINALIZACIÓN DE LA CONFIGURACIÓN Y MAPEO LÓGICO DE ZONAS

3 TEMÁTICA 2 Configuración NAT.

El NAT (Network Address Translation) es una técnica que permite la traducción de direcciones IP privadas a direcciones públicas, facilitando la comunicación entre redes internas y externas. En entornos de seguridad, como los gestionados por Endian Firewall, NAT es esencial para habilitar el acceso de clientes internos a Internet y para publicar servicios alojados en la zona DMZ (Demilitarized Zone).

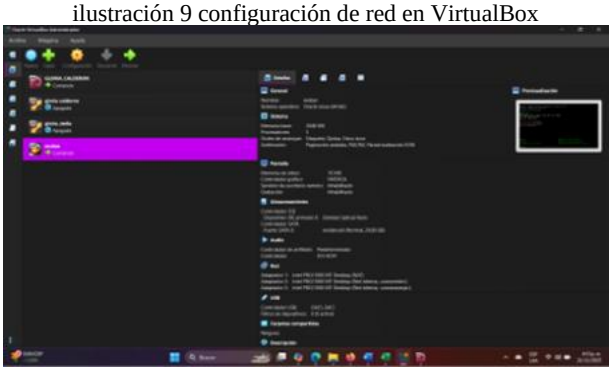
3.1.1 ARQUITECTURA DE RED

Tabla 1

Zona	Tipo de red	Adaptador	Rango IP
Red WAN	Red NAT	1	10.0.2.15/24
Red LAN(zonaverde)	Red interna	2	192.168.10.0/23
Red DMZ(Zonanaranja)	Red interna	3	192.168.20.0/24

Fuente: autoría propia

ilustración 9 configuración de red en VirtualBox



Fuente: autoría propia

3.2 FUNDAMENTOS DE NAT Y REENVIOS DE PUERTO

3.2.1 SNAT (Source NAT / Masquerading)

Traduce la IP origen de los paquetes salientes es usado para que los equipos de la LAN accedan a Internet.
Ejemplo: un cliente 192.168.10.2 se traduce a la IP pública 200.50.60.70 al salir hacia la WAN.

3.2.2 DMZ (Demilitarized Zone)

Zona intermedia entre LAN e Internet que aloja servidores que deben ser accesibles desde fuera (web, correo, FTP) se protege con reglas de DNAT y políticas de firewall para aislarla de la LAN.

3.2.3 DNAT (Destination NAT / Port Forwarding)

Traduce la IP destino de los paquetes entrantes es usado para publicar servicios de la DMZ hacia Internet.
Ejemplo: tráfico entrante a 200.50.60.70:80 se redirige al servidor web 10.0.0.10:80 en la DMZ.

3.3 CONFIGURAR LA REGLA DE NAT, DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN (RED SIMULADA DE INTERNET)

Para permitir que los clientes internos naveguen en Internet, se configura una regla de Source NAT (SNAT) o Masquerading.
Procedimiento:

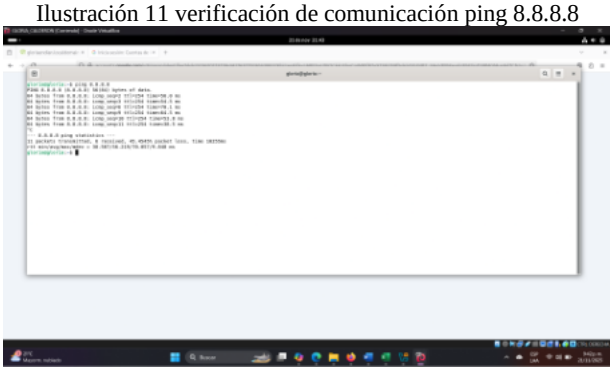
- Acceder a la interfaz web de Endian: https://192.168.10.1:10443
- Ir a Firewall → NAT → Source NAT.
  Crear regla:
- **Origen**: red LAN (ej. 192.168.1.0/24).
- Destino: Any (Internet).
- Acción: *Masquerade* (usar la IP pública de la interfaz WAN).

Guardar y aplicar cambios.

Ilustración 10 Configuración de la regla Source NAT (SNAT)

Fuente: autoría propia

Ilustración 11 verificación de comunicación ping 8.8.8.8



Fuente: autoría propia

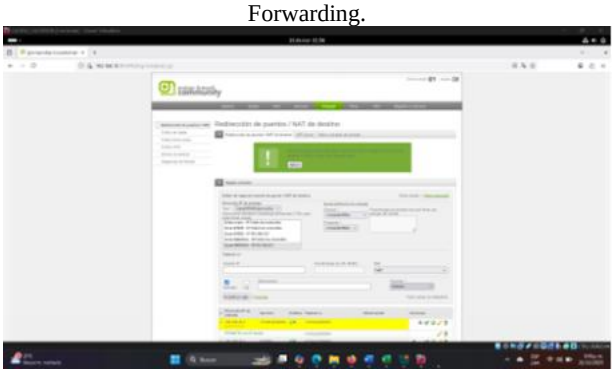
Ilustración 12 navegación en internet IP cliente

Fuente: autoría propia

Para publicar servicios de la DMZ hacia Internet, se configura una regla de **Destination NAT (DNAT)** o *Port Forwarding*.
Procedimiento:

- Ir a **Firewall → NAT → Destination NAT / Port Forwarding**.
  Crear regla:
- **Interfaz de entrada**: WAN.
- **Destino público**: IP de la interfaz WAN.
- **Puerto**: servicio requerido (ej. HTTP → 80, HTTPS → 443).
- **Redirección**: IP privada del servidor en la DMZ (ej. 192.168.20.10).
  Guardar y aplicar cambios.

Ilustración 13 Destination NAT (DNAT) o Port Forwarding.



Fuente: autoría propia

Ilustración 14 Ping desde el servidor hacia internet a través de ssh desde Debian escritorio

Fuente: autoría propia

Ilustración 15 Verificación de las IP verde y roja en ENDIAN

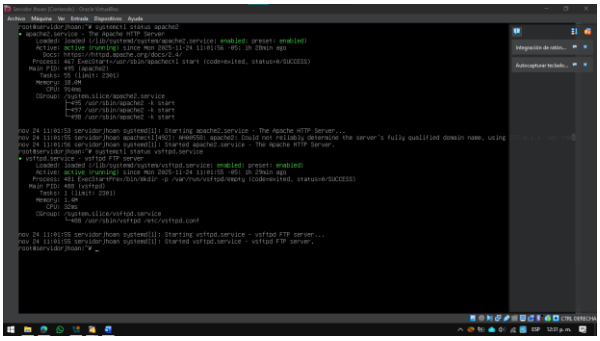
Fuente: autoría propia

4 TEMÁTICA 3 - PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

La configuración de la Zona DMZ requiere un equilibrio estratégico entre accesibilidad y seguridad. En esta temática implementaremos reglas de firewall que autoricen únicamente el tráfico indispensable para los servicios corporativos, mientras bloqueamos protocolos de diagnóstico que pueden ser explotados para reconocimiento de red. El enfoque sigue el principio de mínimo privilegio, garantizando que solo los puertos estrictamente necesarios permanezcan accesibles.

Verificamos que nuestro servidor Debian tenga los servicios Apache2 y vsftpd en ejecución, garantizando su disponibilidad cuando los clientes soliciten conectarse a ellos.

Ilustración 16 Verificación de los servicios Apache y FTP

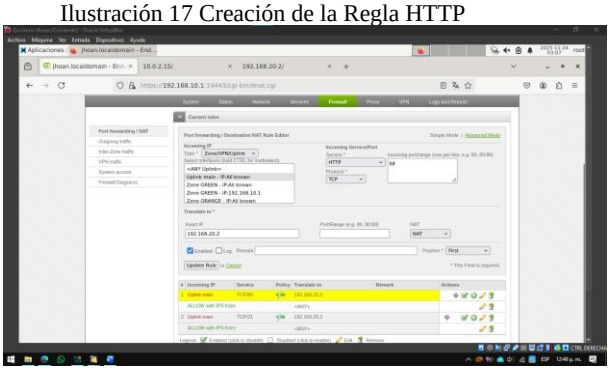


Fuente: autoría propia

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

Utilizamos el apartado de redireccionamiento de puertos para establecer la regla que permite la comunicación entre la red y nuestro servidor. Esta configuración se aplica en la uplink principal para tráfico entrante, seleccionando el servicio HTTP y redirigiendo las conexiones hacia la IP asignada a nuestro servidor.

Ilustración 17 Creación de la Regla HTTP



Fuente: autoría propia

Realizamos la misma configuración de redireccionamiento de puertos, pero ahora aplicamos la regla para el servicio FTP, dirigiendo el tráfico hacia la IP de nuestro servidor.

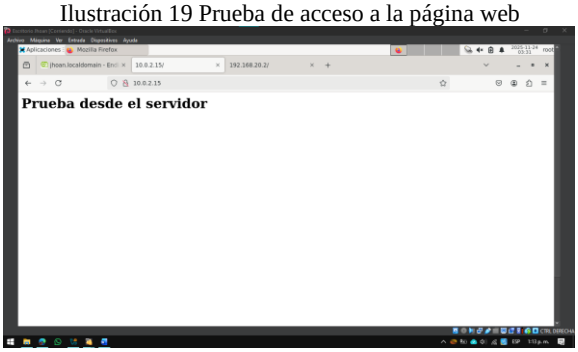
Ilustración 18 Creación de la regla FTP

Fuente: autoría propia

Para comprobar que estén funcionado correctamente las reglas vamos a realizar unas pruebas desde el cliente.

Realizamos la primera prueba desde el navegador del cliente, accediendo a la página web mediante la IP pública del Endian. Este método simula una conexión externa a través de Internet para validar la correcta configuración del servicio.

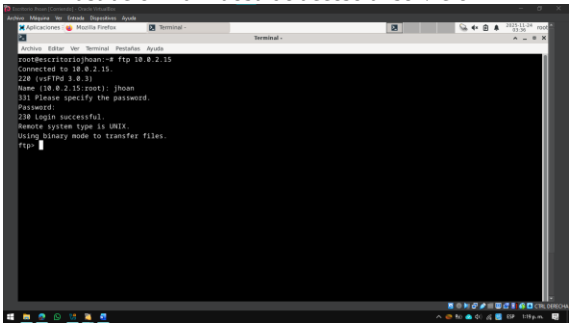
Ilustración 19 Prueba de acceso a la página web



Fuente: autoría propia

Ahora realizamos la prueba para el servidor FTP, está la hacemos desde la terminal y volvemos a utilizar la IP publica de Endian.

Ilustración 20 Prueba de acceso al servicio FTP

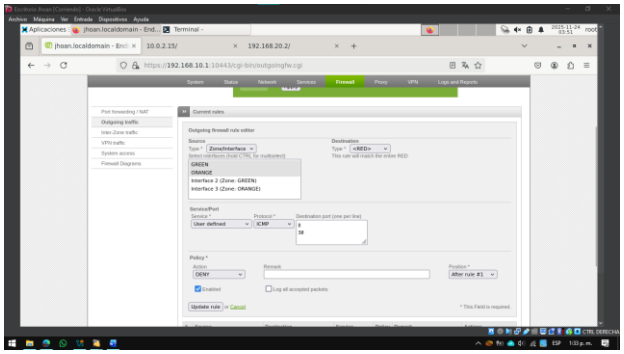


Fuente: autoría propia

4.1.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR HACER PING EN LA RED. PROBAR A TRAVÉS DE UNA CONSOLA O TERMINAL LA NO RESPUESTA DEL COMANDO PING HACIA UNA IP DE LA RED. VERIFICAR EN EL TRÁFICO DE SALIDA, LA CREACIÓN DE LAS REGLAS.

Para esta regla, trabajamos en el apartado de tráfico de salida donde negamos el protocolo ICMP en los puertos 8 y 30. En la configuración, seleccionamos como origen las zonas verde y naranja, y como salida la zona roja, lo que bloquea toda comunicación de este protocolo.

Ilustración 21 Regla para bloquear ICMP



Fuente: autoría propia

Para validar la efectividad de la regla, ejecutamos el comando ping desde la terminal del cliente hacia un dominio externo como google.com. Este comando utiliza el protocolo ICMP para enviar paquetes de solicitud y, como se puede observar en los resultados, la configuración aplicada bloquea exitosamente toda comunicación ICMP, impidiendo cualquier respuesta hacia destinos externos.

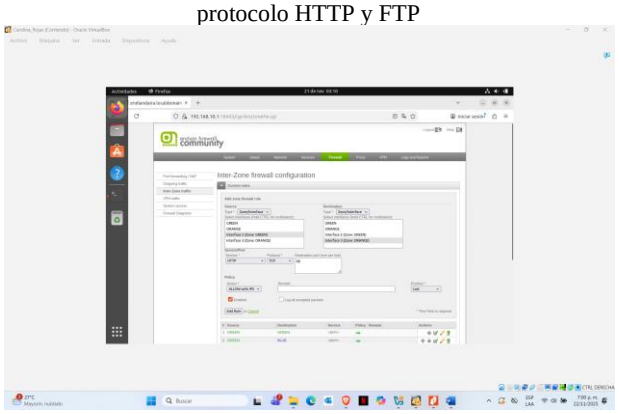
Ilustración 22 Comprobación de la regla ICMP

Fuente: autoría propia

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

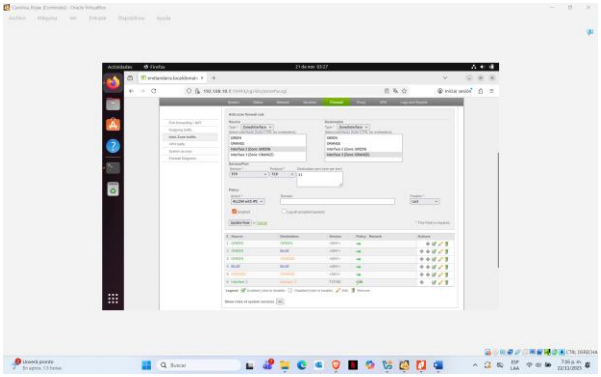
Para estas reglas es necesario que las zonas estén definidas y comunicadas en el server en ENDIAN y desktop, de esta manera las reglas solicitadas como la comunicación, el acceso y la delimitación podrán crearse correctamente según lo requerido con los diferentes protocolos nombrados (HTTP, FTP) en las zonas DMZ

Ilustración 23 comunicación de zona verde a zona naranja protocolo HTTP y FTP



Fuente: autoría propia

Ilustración 24 comunicación entre la zona Internet a la DMZ



Fuente: autoría propia

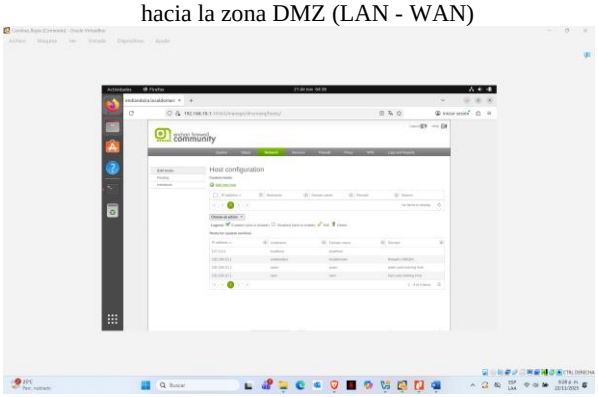
Ilustración 25 verificación del tráfico Inter – Zona

Fuente: autoría propia

5.1 INGRESO DEL SERVICIO DESDE LAS ZONAS

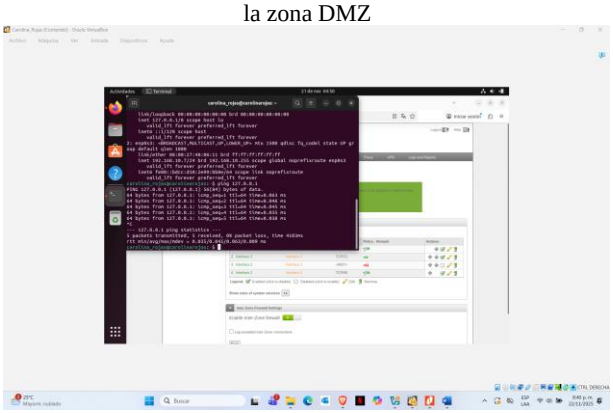
La implementación y verificación de las reglas de firewall confirman el correcto flujo de tráfico según los requisitos de seguridad establecidos. Se validó el acceso HTTP desde DMZ hacia WAN para actualizaciones y comunicaciones externas, se restringió adecuadamente el ingreso HTTP desde WAN hacia DMZ para proteger servicios internos, y se garantizó la conectividad FTP desde LAN hacia WAN para transferencias seguras. Estas configuraciones refuerzan el modelo de defensa en profundidad y cumplen con los principios de menor privilegio y segmentación de red.

Ilustración 26 Ingreso a los servidores HTTP desde la LAN hacia la zona DMZ (LAN - WAN)



Fuente: autoría propia

Ilustración 25 El ingreso del servicio FTP desde la WAN hacia la zona DMZ



Fuente: autoría propia

6 CONCLUSIONES

6.1 TEMATICA 1

De esta forma, la Temática 1 consolidó una plataforma base completamente funcional y técnicamente verificada. La correcta asignación de las direcciones IP y la operatividad de los gateways en cada segmento fueron confirmadas mediante pruebas funcionales ejecutadas por comandos ping desde los hosts complementarios. Este resultado no solo demostró la capacidad de interconexión del firewall con la LAN y la DMZ, sino que también estableció un entorno de laboratorio estable, aislado lógicamente, y listo para avanzar hacia la siguiente fase del proyecto: la definición, aplicación y prueba exhaustiva de las políticas de tráfico y el endurecimiento (hardening) del perímetro.

6.2 TEMARICA 2

La configuración de NAT en Endian Firewall permite una gestión segura y eficiente de la comunicación entre redes internas y externas. El uso de SNAT garantiza la navegación de clientes internos, mientras que DNAT facilita la publicación de servicios en la DMZ, manteniendo el aislamiento de la LAN.

6.3 TEMATICA 3

La implementación exitosa de la configuración de la Zona DMZ representa un avance crucial en nuestro diseño de red, logrando un equilibrio estratégico entre dos necesidades fundamentales: permitir el acceso público a servicios corporativos esenciales y proteger la infraestructura interna de potenciales amenazas. Al aplicar rigurosamente el principio de mínimo privilegio, configuramos reglas de firewall que funcionan como guardias de seguridad inteligentes, autorizando únicamente el tráfico indispensable para los servicios web y FTP mediante redireccionamiento de puertos hacia nuestro servidor Debian, mientras bloqueamos proactivamente protocolos de diagnóstico como ICMP que podrían ser explotados para mapear y estudiar nuestra red. Las exhaustivas pruebas de conectividad realizadas no solo validaron técnicamente la funcionalidad de cada regla confirmando tanto el correcto acceso a los servicios como la efectividad del bloqueo de ping sino que demostraron en la práctica cómo podemos construir puentes seguros hacia el exterior sin comprometer la integridad de nuestra red interna. Este enfoque metódico transforma conceptos abstractos de seguridad en una protección operativa tangible, creando una defensa perimetral que es tanto robusta como inteligentemente selectiva.

6.4 TEMATICA 4

La correcta configuración de reglas de firewall y el testing de conectividad entre zonas (LAN, DMZ y WAN) son esenciales para garantizar la seguridad sin sacrificar la funcionalidad de los servicios. Las pruebas realizadas validan que el tráfico HTTP esté permitido únicamente según los requisitos de negocio, reforzando el principio de mínimo privilegio y asegurando una infraestructura confiable y auditada

7 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/

Canonical (2023). Guía del Ubuntu desktop 20.04 LTS . [2] Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

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

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

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

[6] Jay LaCroix. (2020). Packt Publishing.https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[7] Descarga de Endian EFW 3.3.2 https://sourceforge.net/projects/efw/

[8] García, M., & Lee, K. (2019). Protocol security: Risks and mitigation of ICMP in corporate networks. Journal of Network Security, 28(3), 45-62. https://doi.org/10.1016/j.jns.2019.04.003

[9] Endian Ltd. (2023). Endian Firewall documentation: Traffic rules and port forwarding. Endian Network Security. Recuperado de https://docs.endian.com/firewall/traffic-rules

[10] Zimmerman, J. (2020). Firewall policies and network defense: Implementing DMZ architectures. Cisco Press.