CONFIGURACIÓN Y VERIFICACIÓN DE POLÍTICAS DE SEGURIDAD PERIMETRAL EN GNU/LINUX USANDO ENDIAN FIREWALL

Luis F. Rojas González
lfrojasgo@unadvirtual.edu.co
Josué D. Pedraza Triana
jdmanosalvapa@unadvirtual.edu.co
Luis S. Díaz Oviedo
lsdiazo@unadvirtual.edu.co
Emiliano A. Poloche Sánchez
eapoloches@unadvirtual.edu.co
Jorge A. Ayala Castro
jaayalaca@unadvirtual.edu.co

RESUMEN: *La seguridad perimetral en redes corporativas y académicas es esencial para proteger servidores y aplicaciones críticas en GNU/Linux. Este trabajo presenta la implementación colaborativa de una infraestructura con Endian Firewall, que delimita una zona desmilitarizada entre LAN y WAN para garantizar la integridad de bases de datos y servicios web. Cada integrante del grupo instala y configura EFW, validando el estado de los servicios mediante comandos de consola y registrando evidencia de ejecución. Los resultados muestran la viabilidad de establecer políticas homogéneas de seguridad y la importancia de la verificación sistemática de servicios, ofreciendo un marco práctico y replicable para entornos académicos y profesionales.*

PALABRAS CLAVE: DMZ, Endian Firewall (EFW), GNU/Linux, seguridad perimetral.

1 INTRODUCCIÓN

La creciente interconexión de sistemas informáticos en entornos corporativos y académicos ha incrementado la necesidad de implementar mecanismos de seguridad perimetral robustos y colaborativos. En particular, la protección de servidores que conforman la intranet (LAN) y la extranet (WAN) se ha convertido en una prioridad estratégica, dado que estos sistemas alojan bases de datos y aplicaciones críticas bajo plataformas GNU/Linux. Para mitigar riesgos asociados a accesos no autorizados y garantizar la integridad de la información, resulta indispensable la delimitación de una zona desmilitarizada (DMZ), que actúe como capa intermedia entre los servicios internos y externos.

Diversos estudios han demostrado que la incorporación de firewall de código abierto, como Endian Firewall (EFW), ofrece una solución flexible y escalable para la gestión del tráfico entre LAN, WAN y DMZ. Sin embargo, aún persisten desafíos relacionados con la correcta configuración de servicios, la verificación de su estado operativo y la coordinación entre equipos de trabajo en entornos colaborativos. En este contexto, se propone un enfoque práctico en el que cada integrante del grupo realiza la instalación, configuración y validación de EFW, abordando temáticas específicas de seguridad perimetral y consolidando posteriormente los resultados en un entorno de aprendizaje compartido.

La infraestructura planteada contempla estaciones de trabajo GNU/Linux para la red LAN, un servidor GNU/Linux en la DMZ destinado a aplicaciones web y bases de datos, y un firewall Endian como punto de control entre LAN y WAN. Este diseño permite establecer políticas de seguridad homogéneas, garantizar la trazabilidad de las configuraciones y facilitar la replicación de escenarios en entornos académicos y profesionales.

2 METODOLOGIA

El desarrollo del presente proyecto se realizó bajo un enfoque práctico experimental, de tipo aplicado, orientado a la implementación dentro de una verificación de políticas de seguridad perimetral controlado bajo uso de software de virtualización y herramientas de código abierto de plataformas Linux

2.1 Fase de análisis y planeación

Se identificaron necesidades de seguridad de la infraestructura en la red, determinando así todos los requerimientos técnicos definiendo así zonas de seguridad (LAN, WAN, DMZ), servicios habilitados (HTTP, FTP y Proxy), protocolos a restringir (ICMP) se utiliza herramientas como lo es VirtualBox, Endian Firewall la cual es la solución de seguridad perimetral, Desktop y Ubuntu server como el servidor de servicios en la DMZ.

2.2 Fase de diseño de la arquitectura de red

Se diseño una topología de red dividida en tres zonas que son Zona Verde (LAN), Zona Naranja (DMZ) y la Zona Roja (WAN) de acuerdo a esto se establecen direcciones IP posterior a ello asignación de interfases de red con el proyecto se permite simular un entorno real diferenciando así la confianza, garantizando el aislamiento. Control y monitoreo del tráfico entre las redes.

2.3 Fase de implementación

Se lleva a cabo la instalación y configuración del Endian Firewall asignándoles la configuración de los adaptadores, posterior a ello se implementaron reglas NAT para permitir la comunicación entra LAN, WAN y DMZ configurando así las políticas de filtrado necesarias para permitir solo los servicios autorizados (HTTP y FTP) hacia y desde la DMZ, también se establecen reglas para el bloqueo del protocolo ICMP para evitar la detección del servidor mediante comandos generando así un ping verificando su estado de conectividad

2.4 Fase de Verificación

Una vez implementadas todas las configuraciones se realizaron pruebas de verificación desde las diferentes zonas de red mediante consola como ping, curl, navegadores web y clientes FTP verificando así la correcta aplicación de reglas de Firewall
Esta metodología permite validad de manera practica el cumplimiento de los objetivos propuestos estableciendo creación de un entorno seguro, segmentado y controlado alineado con principios de seguridad perimetral de Linux

3 TEMÁTICA 1.

El producto esperado para esta temática fue la implementación exitosa de la distribución GNU/Linux Endian Firewall (EFW) como el componente central de seguridad perimetral. Esto incluyó la configuración de una instancia en VirtualBox con tres interfaces de red aisladas, correspondientes a las zonas de seguridad definidas: Zona Verde (Red Interna o LAN), Zona Roja (Acceso a Internet o WAN) y Zona Naranja (Servidores o DMZ).

3.1 DESARROLLO TEMÁTICA

La implementación de la infraestructura base de seguridad se realizó siguiendo una metodología estructurada para garantizar la segregación del tráfico de red desde su concepción.

3.1.1 Configuración de la Máquina Virtual

Se creó una nueva máquina virtual en Oracle VM VirtualBox, asignando recursos de sistema adecuados para el funcionamiento de EFW. La configuración crítica involucró la habilitación de tres adaptadores de red, cada uno vinculado a una red interna específica para simular el entorno de zonas desmilitarizadas. La Tabla 1 detalla esta configuración.

Tabla 1. Configuración de adaptadores de red en Virtualbox.

Adaptador	Nombre de Red	Zona Asignada	Conectado a
Adaptador 1	Red Verde	Verde (LAN)	Conexión a red interna
Adaptador 2	Red Naranja	Naranja (DMZ)	Conexión a servidores
Adaptador 3	Red Roja	Roja (WAN)	Simulación de acceso a Internet

3.1.2. Instalación del Sistema

Se inicializó la máquina virtual desde la imagen de instalación de Endian UTM 3.2. Se procedió con una instalación estándar, utilizando el particionamiento automático del disco y estableciendo credenciales de administrador seguras. Tras la finalización del proceso, el sistema se reinició y se accedió a la consola de administración para la configuración inicial.

3.1.3. Configuración de Zonas de Red

El firewall Endian detecta automáticamente las interfaces de red físicas disponibles (eth0 eth1, eth2). A través de la interfaz web de administración, se asignó cada interfaz a su zona de seguridad correspondiente y se configuraron direcciones IP estáticas, de acuerdo con el esquema de direccionamiento preestablecido por el grupo colaborativo. La Tabla 2 presenta la configuración final de las zonas.

Tabla 2. Configuración IP de zonas de seguridad.

Zona	Dirección IP	Máscara de Red
Verde (LAN)	192.168.1.1	255.255.255.0
Naranja (DMZ)	192.168.2.1	255.255.255.0
Roja (WAN)	Zona Roja (DHCP)	255.255.255.0

3.1.4 Verificación de la Implementación

La verificación del correcto funcionamiento se realizó en dos niveles. Primero, desde la línea de comandos del sistema EFW, se utilizaron utilidades como ip addr y **systemctl status** firewall para confirmar el estado de las interfaces de red y los servicios críticos del cortafuegos. Posteriormente, se emplearon las herramientas de diagnóstico integradas en la interfaz web administrativa para validar la conectividad básica de cada zona. Este proceso confirmó que todas las interfaces estaban operativas y que el servicio de firewall se ejecutaba correctamente, estableciendo una base sólida para la implementación de reglas de filtrado y políticas de seguridad en las siguientes fases del proyecto.

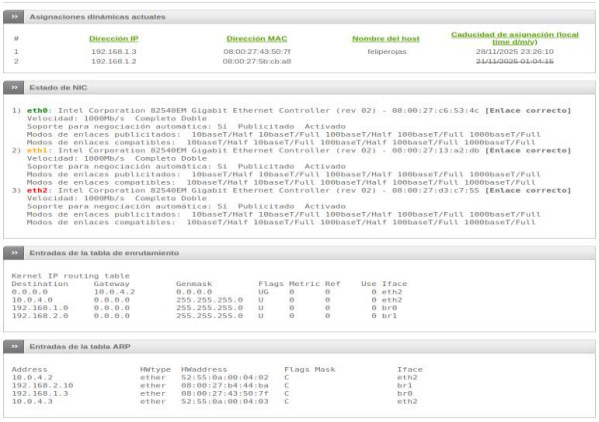

Fig. 1. Estado operativo red del Firewall Endian

3. TEMÁTICA 2.

Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el reenvió de puertos / NAT, la creación de las reglas.

4.1 DESARROLLO TEMÁTICA

4.1.1. Configuración de NAT

La configuración de las reglas de traducción de direcciones de red (NAT, Network Address Translation) constituye un paso fundamental para garantizar la comunicación entre las distintas zonas de la infraestructura de seguridad perimetral. En este escenario, se habilitó la salida a Internet desde la zona desmilitarizada (DMZ) y se verificó el acceso desde la red local (LAN) hacia la red externa (WAN).

Inicialmente se evidenció que el servidor ubicado en la Zona Naranja (DMZ) no disponía de conectividad hacia internet para la actualización de paquetes.

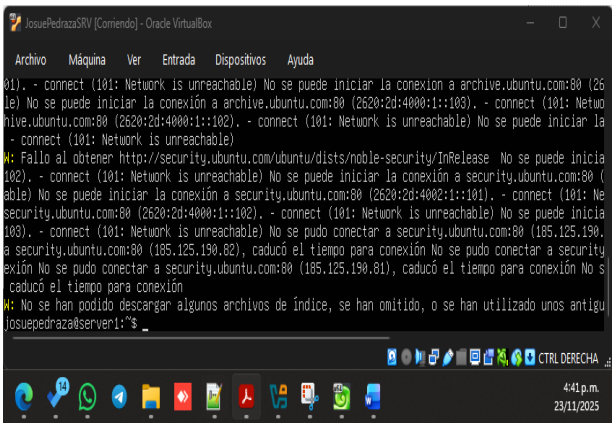

Fig. 2. Evidencia no conectividad.

Para solucionar esta limitación, NAT fue habilitado en la interfaz Roja, permitiendo el tráfico saliente desde la DMZ hacia la WAN mediante los protocolos TCP en los puertos 80 y 443.
El acceso a la puerta de enlace se realizó desde la terminal de la Zona Verde mediante la URL
https://192.168.1.1:10443

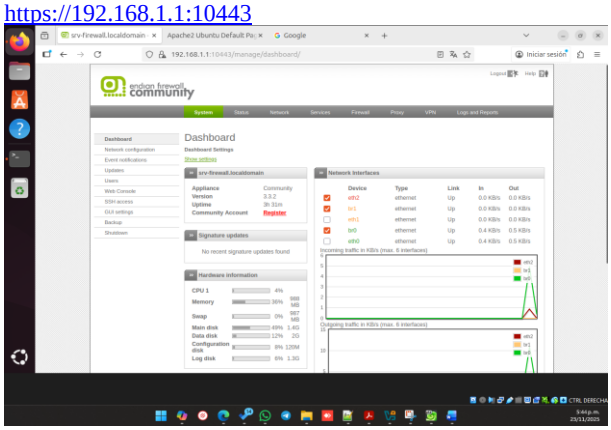

Fig. 3. Menú principal Endian.

La opción de *masquerading* (NAT) fue activada para salida a Internet en los puertos TCP 80 y 443.

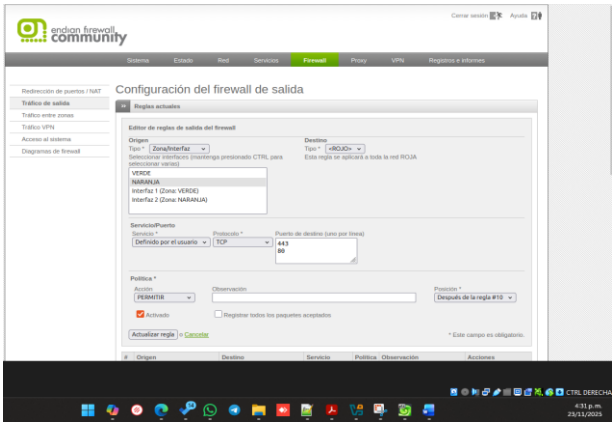

Fig. 4. Menú endian – Trafico de Salida.

La actualización de paquetes desde el servidor 192.168.2.10 en la DMZ confirmó la conectividad hacia internet.

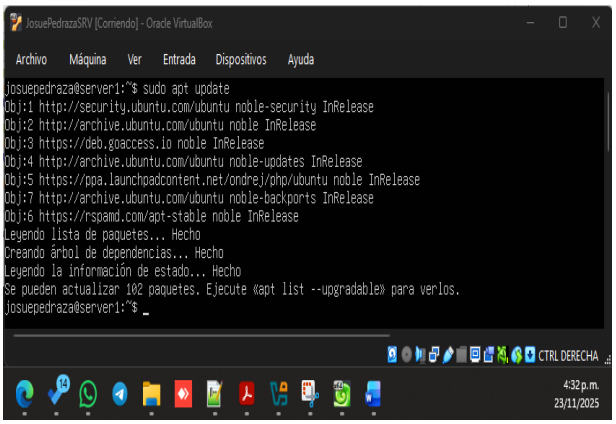

Fig. 5. Evidencia conexión servidor en DMZ.

La navegación desde un equipo en la Zona Verde corroboró la comunicación establecida.

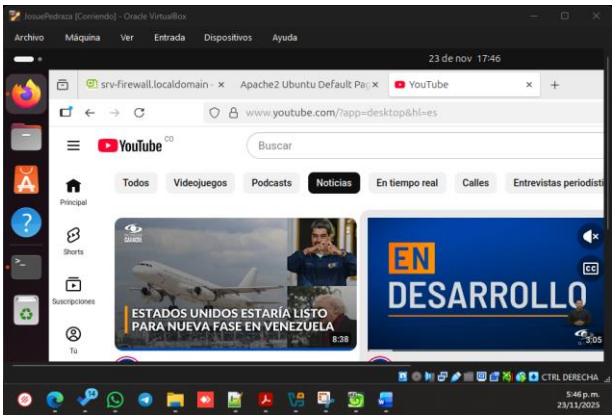

Fig. 6. Pantalla acceso internet zona verde.

4.1.2 Reenvío de Puertos (DNAT)

El reenvío de los puertos (Destination NAT) permite redirigir solicitudes externas hacia servicios específicos alojados en la DMZ. Para este caso, se configuró el acceso al servidor Apache y PHPMyAdmin ubicado en la dirección 192.168.2.10
El ingreso a la interfaz web de Endian Firewall se efectuó en la sección *Firewall → Port Forwarding / NAT*.

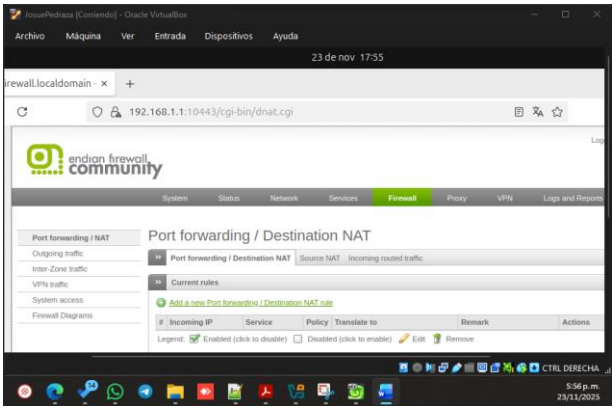

Fig. 7. Interfaz endian Firewall.

La regla correspondiente fue creada en la pestaña Port Forwarding / Destination NAT

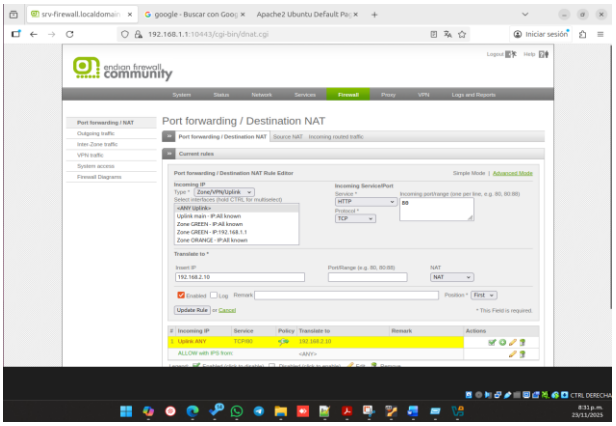

Fig. 8. Interfaz endian Port forwarding.

El acceso al servidor Apache desde un equipo en la Zona Roja con dirección IP 192.168.0.108 confirmó la correcta aplicación de la regla de DNAT

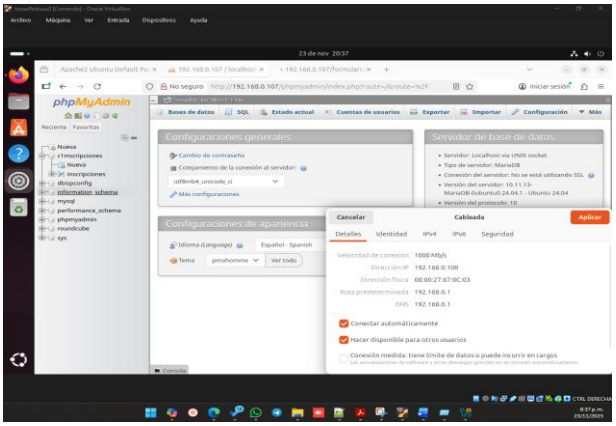

Fig. 9. Evidencia acceso desde internet al servidor.

5 TEMÁTICA 3.

Permitir servicios de la Zona DMZ para la red. Producto esperado:

Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

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 cumplir con los requisitos de seguridad en la Zona DMZ, se implementaron reglas específicas en el firewall Endian, y en el servidor GNU/Linux previa su instalación y configuración

5.1 DESARROLLO TEMÁTICA

La tercera temática se centró en la definición de reglas de seguridad orientadas a la zona naranja (DMZ).
El objetivo garantizar la disponibilidad de servicios.

se busca limitar la exposición del servidor a protocolos necesarios.

5.1.1 Permitir servicios HTTP y FTP

Se configuraron reglas de acceso en la interfaz Naranja (DMZ) con lo cual se habilita el tráfico entrante hacia el servidor web en los puertos TCP 80 (HTTP) y 21 (FTP) las pruebas realizadas sección *Firewall – Port Forwarding / Access Policy* de Endian Firewall desde equipos en la LAN y la WAN confirmaron la disponibilidad de los servicios web y transferencia de archivos. El servidor Ubuntu respondió de manera estable a las solicitudes, validando la disponibilidad de aplicaciones críticas en un entorno controlado

Fuente Elaboración Propia

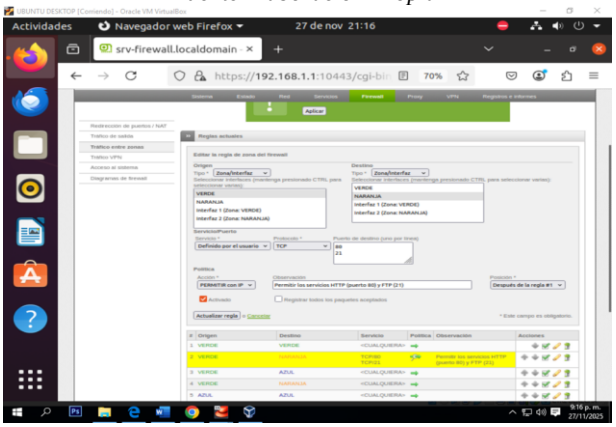

Fig. 10. Configuración Regla para puertos TCP 80 (HTTP) y 21 (FTP).

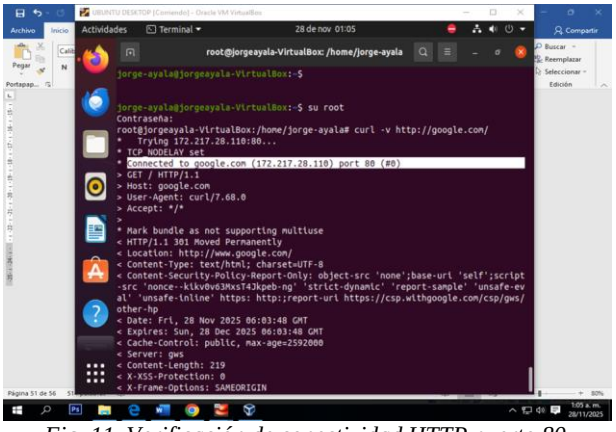

Fig. 11. Verificación de conectividad HTTP puerto 80 mediante comando curl –v http: google.com/.

Tabla 3. Reglas de acceso aplicadas en la DMZ para servicios permitidos y bloqueo de ICMP.

Origen	Destino	Protocolo	Puerto	Acción
LAN	DMZ	TCP	80	ACCEPT
WAN	DMZ	TCP	21	ACCEPT
Cualquiera	DMZ	ICMP	-	DROP

5.1.2 Denegar/Bloqueo Protocolo ICMP

Con el fin de reducir la superficie de ataque y evitar la detención del servidor mediante herramientas de escaneo, se configuró mediante una regla explicita para denegar o bloquear el tráfico ICMP desde y hacia la DMZ, Esta política impidió la respuesta a los comandos ping ejecutados desde diferentes zonas de la red hacia el servidor en la DMZ, se verificó la ausencia de respuesta, validando la correcta aplicación de la política ya que las pruebas realizadas desde la consola de equipos LAN y la WAN mostraron la ausencia de respuesta, lo que confirmo la efectividad de la regla y la coherencia con las prácticas de seguridad recomendadas en entornos corporativos y académicos

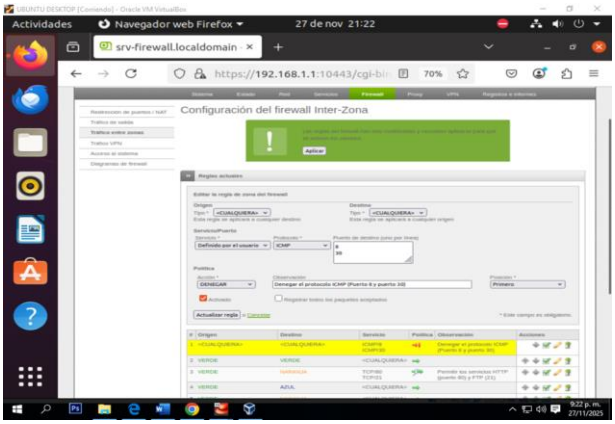

Fig. 12. Configuración regla puertos 8 y Puerto 30.

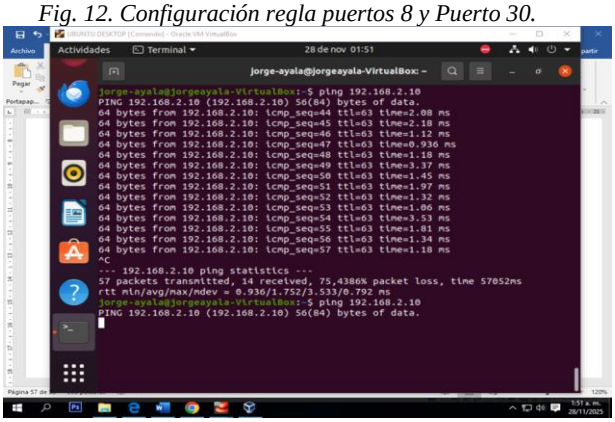

Fig. 13. Se configura regla para bloquear mensajes ICMP (Puerto 8 y 30) con el fin de impedir ejecución de comandos ping hacia el servidor.

5.1.2 Verificación de tráfico de salida

La revisión de los registros de firewall mostró entradas de ACCEPT para los servicios HTTP y FTP, mientras que las solicitudes ICMP aparecieron como DROP esto confirmo que las reglas se aplicaron correctamente y que la política de seguridad definida se encuentra activa

La implementación de estas políticas fortalece la seguridad DMZ permitiendo únicamente los servicios necesarios para la operación bloqueando así protocolos que podrían ser utilizados para reconocimiento o ataques de red de esta manera se consolida un entorno confiable para la publicación de aplicaciones web y servicios de transferencia de archivos, alineado con las mejores prácticas de seguridad perimetral

6 TEMÁTICA 4.

Reglas de acceso para permitir o denegar el tráfico. Producto esperado:

Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Comunicar la zona Internet con la zona DMZ.

Verificar en el tráfico Inter - Zona, la creación de las reglas.

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.
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.
El ingreso del servicio FTP desde la WAN hacia la zona DMZ.

6.1 DESARROLLO TEMÁTICA

Para cumplir con los requisitos de seguridad y conectividad de la red, se diseñó e implementó un conjunto de reglas de acceso (ACL) en el firewall. La configuración involucró la definición de políticas para permitir el tráfico específico entre las distintas zonas de seguridad, mientras se mantiene el principio de "denegar por defecto". A continuación, se detallan las reglas implementadas.

6.1.1 Comunicación entre la Zona Verde (LAN) y la Zona Naranja

Se creó una regla para permitir la comunicación bidireccional entre la Zona Verde (red interna de confianza) y la Zona Naranja (red de administración) para los protocolos HTTP y FTP. La regla especifica los puertos de servicio estándar: TCP 80 para HTTP y TCP 21 para FTP.

6.1.2 Comunicación entre la Zona Internet y la Zona DMZ

Se implementaron reglas para gestionar el tráfico entre la Zona Internet (WAN) y la Zona DMZ (Zona Desmilitarizada). Se permitió el acceso desde Internet (WAN) hacia los servidores públicos ubicados en la DMZ para los servicios HTTP (TCP 80) y FTP (TCP 21). Como práctica de seguridad, el tráfico de retorno asociado a estas conexiones establecidas también fue permitido.

6.1.3 Verificación de las Reglas de Acceso Inter-Zona

Posteriormente a la implementación, se verificó la correcta creación y aplicación de las reglas Inter-Zona. Se utilizó la utilidad de línea de comandos del firewall y su interfaz gráfica para confirmar que las políticas estuvieran activas, en el orden correcto y asignadas a las interfaces y zonas correspondientes. La verificación confirmó que las reglas estaban operativas.

6.1.4 Pruebas de Conectividad y Validación de Directivas

Para validar el funcionamiento de las directivas de seguridad, se realizaron una serie de pruebas desde un navegador web y un cliente FTP.

Las pruebas demostraron que la configuración del firewall fue exitosa. Todos los escenarios de tráfico definidos en los requisitos se cumplieron satisfactoriamente. Se pudo constatar el acceso HTTP desde la LAN hacia la DMZ y la WAN, así como el acceso HTTP desde la WAN hacia los servidores en la DMZ. De igual manera, las sesiones FTP desde la LAN hacia la WAN y desde la WAN hacia la DMZ se establecieron sin inconvenientes. Se concluye que las reglas de acceso implementadas controlan efectivamente el flujo de tráfico interzonal de acuerdo con la política de seguridad definida.

Fuente Elaboración Propia

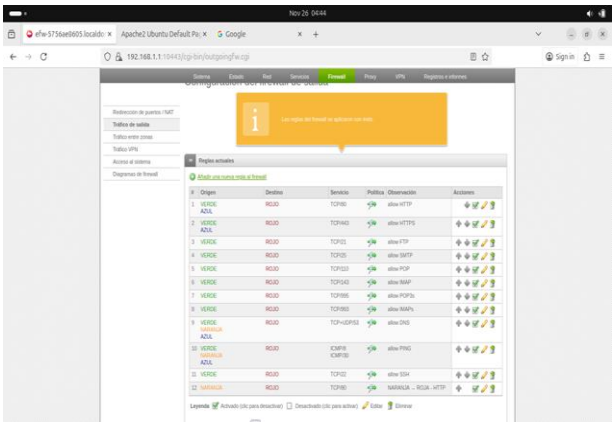

Fig. 14. Configuración reglas de tráfico saliente.

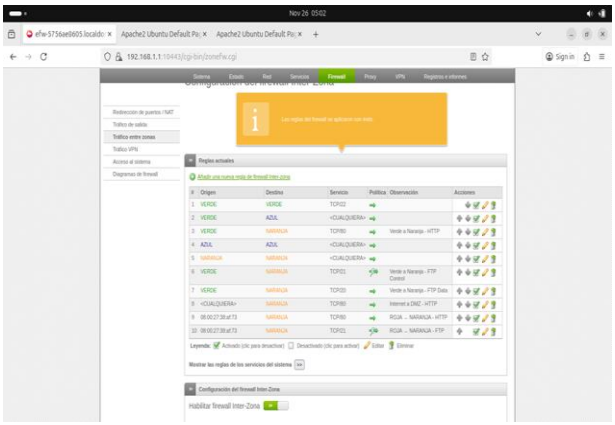

Fig. 15. Configuración de reglas interzonal. Se especifican las combinaciones de origen, destino y servicio permitidas o restringidas entre las diferentes zonas de red.

7 TEMÁTICA 5.

Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Producto esperado:

1. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:

www.hotmail.com

www.youtube.com

www.elnuevodia.com.co

2. Autenticación por usuario: A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.

3. Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

Configuración del Proxy y Filtro Web Se accede a la interfaz de Endian Firewall en la pestaña Proxy y se habilita el servicio mediante el botón Enable HTTP Proxy, manteniendo la configuración predeterminada. A continuación, en la pestaña Web Filter, se crea un nuevo perfil haciendo clic en la opción Add new Profile y se aplica la configuración al perfil denominado Temática5.

Posteriormente, se dirige a la pestaña Access Policy y se agrega una nueva política de acceso mediante el botón Add access policy, la cual se asocia al perfil Temática5 creado anteriormente.

Configuración de la Autenticación Se ingresa a la pestaña Authentication para proceder con la creación del usuario autenticador.

Verificación de la Política de Filtrado Para validar la efectividad de las políticas, se procede a eliminar las reglas creadas en las listas negras. Seguidamente, se verifica el acceso a los sitios web que inicialmente habían sido bloqueados, confirmando que el filtro ya no restringe su visualización.

7.1 DESARROLLO TEMÁTICA

Se ingresa a la interfaz de Endian Firewall en la pestaña Proxy, Se procede a habilitar el proxy en el botón Enable HTTP Proxy se deja por defecto la configuración que tiene.

Luego se ingresa en la pestaña Web Filter, Luego se procede a realizar el perfil dándole clic en la opción Add new Perfile / Perfil, Se le da clic en aplicar la configuración al perfil creado Temática5.

Fuente Elaboración Propia

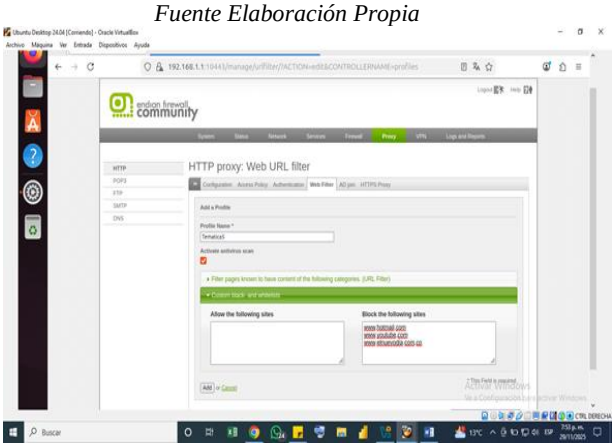

Fig. 16. Creación de Perfil y Agregar páginas en listas negras.

Luego se ingresa a la pestaña Access Policy y se agrega una nueva política dándole clic en el botón Add access policy, Luego se procede a crear la nueva política.

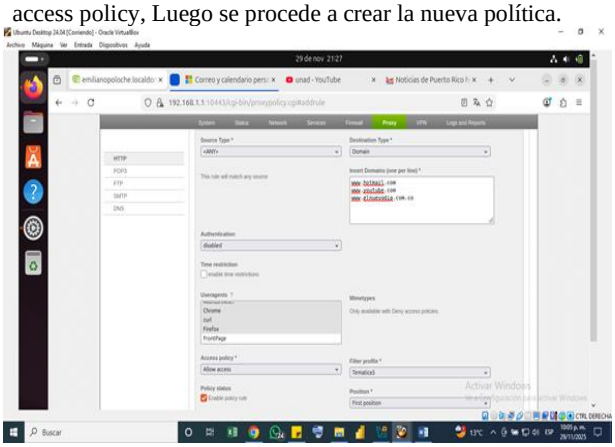

Fig. 17. Creación de políticas para aplicarlo de Temática 5.

Se ingresa a la pestaña Autenticación

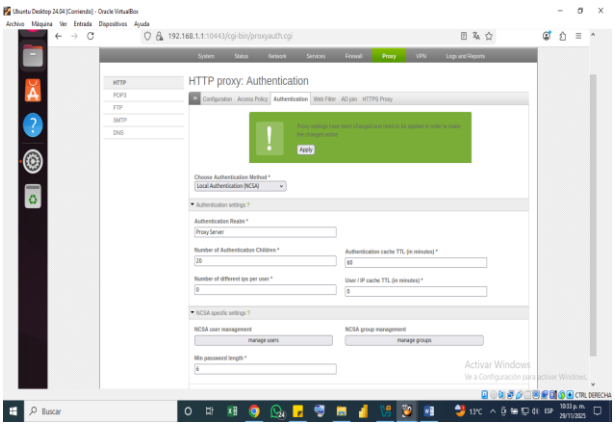

Fig. 18. Creación de Usuario Autenticador.

Se procede a realizar la eliminación de las policitas creadas en las listas negras y se verifica que puedan ingresar a las páginas que inicialmente se en listaron en las páginas negras.

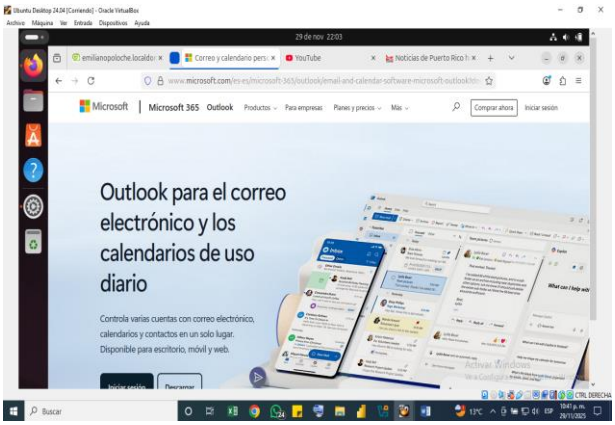

Fig. 19. Validación de ingreso a Hotmail.

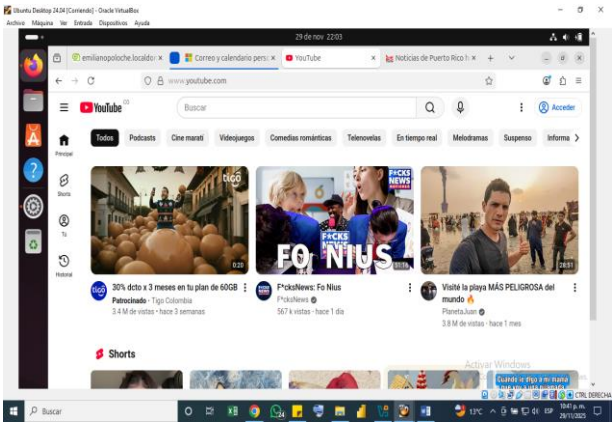

Fig. 20. Validación de ingreso a YouTube.

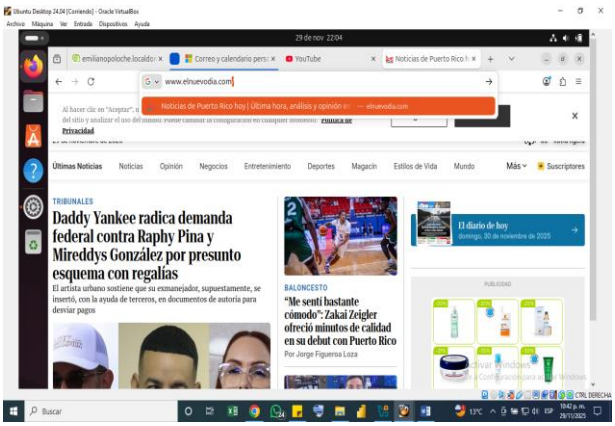

Fig. 21. Fuente Elaboración Propia.

8 CONCLUSIONES.

Temática 1- Implementación de Endian Firewall
La instalación y configuración de Endian Firewall permitió establecer una infraestructura perimetral funcional, garantizando la segmentación de las zonas LAN, WAN y DMZ.

Temática 2- configuración de NAT y DNAT
Con la correcta configuración de las reglas NAT y DNAT se aseguró la conectividad controlada entre las zonas internas y externas, validando la disponibilidad de servicios internos como el servidor web y el aislamiento de la DMZ.

Temática 3- Reglas de acceso en la DMZ
Se definen reglas de filtrado para la habilitación de servicios HTTP y FTP, denegando así protocolos innecesarios o riesgosos junto con el bloqueo del protocolo ICMP, fortaleció la seguridad de la DMZ al limitar la exposición del servicio únicamente a protocolos necesarios reduciendo así riesgos de ataque.

Temática 4- Reglas de acceso interzonales
La definición de políticas de acceso entre LAN, DMZ y WAN permitió un flujo de tráfico seguro y controlado, permitiendo cumplir así con el principio de denegar por defecto y habilitar solo lo indispensable garantizando un servicio interno controlado.

Temática 5- implementación de Proxy HTTP0
El uso de un proxy con listas negras y autenticación de usuarios proporciono un mecanismo adicional de control de acceso fomentando practicas seguras en la navegación y responsabilidad en el uso de reuniones integrando así el funcionamiento del sistema.

Para concluir el desarrollo integral de esta actividad permitió la consolidación de un entorno de seguridad perimetral robusto y funcional mediante la implementación sucesiva de zonas, reglas de filtrado, políticas de NAT y servicios proxy, se demostró la efectividad de un enfoque para la defensa de la red mediante la configuración metódica de Endian Firewall y los servidores Ubuntu, ajustado estrictamente al principio de denegar por defecto y permitir solo lo necesario, como resultado obteniendo una arquitectura que garantiza tanto la disponibilidad de los servicios esenciales como la integridad de la infraestructura interna, este proyecto demuestra la correcta aplicación de fundamentos de seguridad en GNU/Linux.

9 REFERENCIAS

[1] Linux Professional Institute, “Linux Essentials - Tema 5: Seguridad y sistema de permisos de archivos,” 2022. [Online]. Available: https://learning.lpi.org/es/learningmaterials/010-160/5/ . Accessed: Dic. 2025.

[2] Linux Professional Institute, “LPIC-1 Exam 101 - Tema 101: Determinar y configurar los ajustes de hardware,” 2022. [Online]. Available: https://learning.lpi.org/es/learningmaterials/101-500/101/101.1/. Accessed: Dic. 2025.

[3] Canonical Ltd., “Guía del Ubuntu desktop 20.04 LTS,” 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html . Accessed: Dic. 2025.

[4] Debian Project, “Guía Debian GNU/Linux de instalación 12.5.0, “ 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html . Accessed: Dic. 2025.

[5] Oracle Corporation, *Manual de usuario VirtualBox*, 2020. [Online]. Available: https://www.virtualbox.org/manual/ . Accessed: Dic. 2025.

[6] Endian Technologies, *Endian UTM 3.2 Manual referencia*, 2016. [Online]. Available: http://docs.endian.com/3.2/utm/index.html . Accessed: Dic. 2025.

[7] YouTube, “Configuración de firewall Endian,” 2025. [Online]. Available: https://www.youtube.com/watch?v=gavzDYz8FkE . Accessed: Dic. 2025.

[8] YouTube, “Implementación de seguridad en GNU/Linux,” 2025. [Online]. Available: https://www.youtube.com/watch?v=Dvht5wCPIrI . Accessed: Dic. 2025.

[9] Endian Firewall Community, “Endian Firewall Documentación,” 2025. [Online]. Available: https://www.endian.com/en/community/ . Accessed: Dic. 2025.

[10] Dialnet, “Implementación de un sistema de control y seguridad Endian Firewall,” 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=9236278 . Accessed: Dic. 2025.