DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL BASADA EN ZONAS MEDIANTE ENDIAN FIREWALL EN ENTORNOS GNU/LINUX

Brayan Manuel Granados Navarro
bmgranadosn@unadvirtual.edu.co
Cesar Fernando Silva Maldonado
cfsilvam@unadvirtual.edu.co
Diego Alejandro Garavito Feliciano
dagaravitof@unadvirtual.edu.co
Jhon Anderson Rodriguez Martin
sagarafree17@gmail.com
Juan Sebastián Reyes Hernández
jsreyesh@unadvirtual.edu.co

RESUMEN: *Se describe la implementación de un esquema de seguridad perimetral utilizando Endian Firewall Community en un entorno virtualizado mediante VirtualBox. El proceso incluyó la creación y configuración inicial de la instancia, la definición de las zonas Roja, Verde y Naranja, y el establecimiento del direccionamiento fijo para garantizar un entorno estable; la configuración de reglas NAT para permitir la comunicación controlada entre la LAN, la DMZ y la red externa; la habilitación y restricción de servicios desde la DMZ, incluyendo HTTP, FTP e ICMP; la aplicación de reglas de acceso entre zonas para gestionar el tráfico interno y externo; y la implementación de un proxy HTTP no transparente con autenticación y listas de bloqueo. Los resultados obtenidos demostraron la correcta segmentación de la red, el funcionamiento de las políticas de acceso y la eficacia del control de navegación, consolidando un entorno seguro y funcional para prácticas de seguridad perimetral.*

PALABRAS CLAVE: Endian Firewall, DMZ, NAT, Proxy HTTP.

1 INTRODUCCIÓN

El montaje de un firewall perimetral es una tarea fundamental cuando se trabaja en laboratorios de redes, ya que permite organizar el flujo de información y separar los distintos segmentos de la red. En este proyecto se inició dejando configurada la instancia base de Endian Firewall Community, la cual sirve como punto de partida para el desarrollo de las actividades posteriores y garantiza un entorno seguro y estable para las pruebas en un laboratorio de redes.

Inicialmente se realizó la creación, instalación y configuración de Endian Firewall Community dentro de VirtualBox, estableciendo las bases para el trabajo colaborativo del grupo. La configuración detallada de las zonas Roja, Verde y Naranja, junto con el direccionamiento fijo asignado, permite evitar conflictos en las siguientes configuraciones. Esta preparación es esencial para implementar posteriormente las reglas de traducción de direcciones (NAT), la habilitación y restricción de servicios desde la DMZ, la creación de reglas de acceso entre zonas y la configuración de un proxy HTTP con autenticación. Todo ello forma parte de un proceso integral orientado a fortalecer la seguridad perimetral en entornos GNU/Linux mediante el uso de Endian Firewall. Adicionalmente, este trabajo aborda la configuración de reglas de acceso inter-zona, la verificación del tráfico y la prueba de servicios desde distintas zonas de la red, demostrando la funcionalidad y seguridad de la infraestructura configurada.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar un esquema de seguridad perimetral en GNU/Linux mediante Endian Firewall, configurando sus zonas de red y aplicando políticas de control de tráfico, NAT, servicios y proxy, utilizando protocolos HTTP y FTP, para garantizar la correcta comunicación y seguridad de los servicios implementados.

2.2 OBJETIVOS ESPECÍFICOS

- Crear la máquina virtual de Endian en VirtualBox con los recursos adecuados para su funcionamiento.
- Montar la imagen ISO correspondiente e instalar el sistema operativo del firewall.
- Configurar las tres interfaces de red requeridas (Roja, Verde y Naranja), asignando un direccionamiento fijo que permita el trabajo coordinado con los demás integrantes del grupo.
- Verificar el correcto funcionamiento de las zonas mediante pruebas de conectividad desde consola.
- Validar el funcionamiento mediante pruebas básicas de conectividad.
- Habilitar el acceso desde navegador para su administración.
- Implementar reglas de traducción de direcciones (NAT) para permitir la comunicación controlada entre LAN, DMZ y WAN.

- Probar la conectividad y funcionalidad de los servicios HTTP y FTP desde las distintas zonas mediante navegadores web y comandos de prueba.

- Verificar el tráfico inter-zona para asegurar que las reglas de acceso se apliquen correctamente y que la comunicación cumpla con los criterios de seguridad establecidos.

- Verificar el correcto funcionamiento de los servicios mediante pruebas de conectividad y monitoreo del tráfico de salida en Endian Firewall.

3 METODOLOGÍA

La metodología empleada en este trabajo se basa en un enfoque práctico y secuencial orientado a la implementación y validación de un esquema de seguridad perimetral en un entorno virtualizado. El proceso se estructuró en diferentes etapas, iniciando con la configuración de la instancia de Endian Firewall Community y la definición de las zonas de red, seguido de la aplicación de mecanismos de traducción de direcciones (NAT), la habilitación y control de servicios en la zona DMZ, la implementación de reglas de acceso inter-zona y, finalmente, la configuración de un proxy HTTP con autenticación. Cada temática se desarrolló de manera progresiva, permitiendo verificar el correcto funcionamiento de la infraestructura y garantizar la coherencia de las políticas de seguridad establecidas.

3.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED)

3.1.1 CREACIÓN DE MÁQUINA VIRTUAL

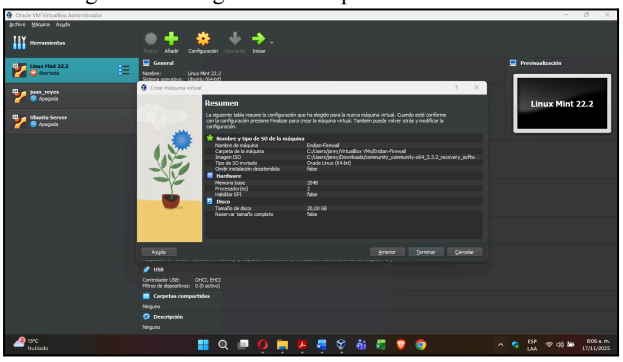
La máquina fue creada en VirtualBox bajo el nombre Endian-Firewall, con la siguiente configuración:

- TIPO: Linux
- VERSIÓN: Other Linux (64-bit)
- RAM: 2048 MB
- CPU: 2 núcleos
- DISCO: 20 GB en formato VDI

Estos recursos resultan adecuados para el funcionamiento estable de Endian Firewall Community y permiten el manejo del tráfico entre las diferentes zonas de red definidas [2]. La asignación de memoria y capacidad de procesamiento garantiza la correcta operación del sistema durante las pruebas de conectividad y validación de las políticas de seguridad implementadas, evitando cuellos de botella en el procesamiento del tráfico.

La siguiente imagen muestra la configuración general de la máquina virtual utilizada para la implementación del firewall perimetral. En la Figura 1 se observa el resumen de parámetros definidos durante la creación de la instancia en VirtualBox, incluyendo el tipo de sistema operativo, la asignación de memoria, la capacidad de procesamiento y el tamaño del disco virtual. Esta configuración inicial constituye la base sobre la cual se implementaron posteriormente las interfaces de red y las políticas de seguridad del firewall.

Figura 1. Configuración Máquina Virtual Endian.



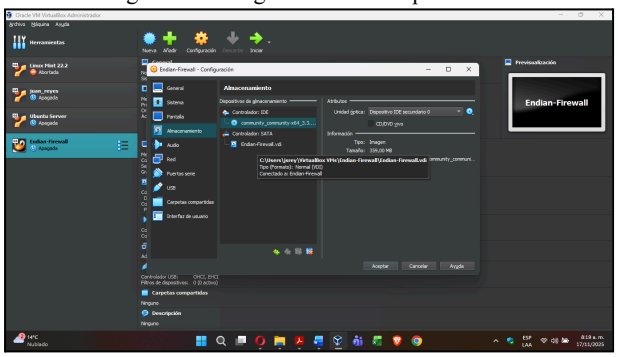
Fuente: Autoría Propia

3.1.2 MONTAJE DE LA ISO

Para iniciar el proceso de instalación del firewall, se montó la imagen endian-community-x86_64-3.3.2.iso en el controlador IDE de la máquina virtual. Esta acción permitió que el sistema cargará correctamente el instalador de Endian Firewall durante el arranque inicial, garantizando una instalación limpia y controlada del sistema [1].

En la siguiente imagen se observa la asignación de la imagen ISO dentro de la configuración de VirtualBox.

Figura 2. Configuración de Adaptadores.



Fuente: Autoría Propia

3.1.3 CONFIGURACIÓN DE INTERFACES DE RED

Con el fin de segmentar adecuadamente la red y aplicar un esquema de seguridad perimetral basado en zonas, se configuraron tres adaptadores de red en la máquina virtual:

· Zona Roja (WAN): Adaptador en modo NAT

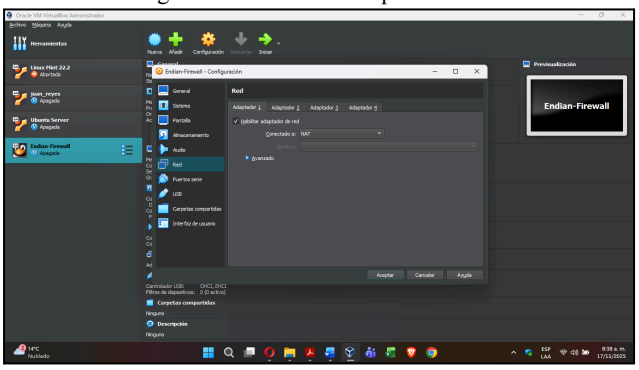
· Zona Verde (LAN): Red interna denominada LAN

· Zona Naranja (DMZ): Red interna denominada DMZ

Esta separación permite aislar la red interna, los servicios expuestos y la conexión hacia Internet, siguiendo las buenas prácticas de seguridad perimetral [1].

En la siguiente imagen se evidencia la activación y asignación de los adaptadores de red correspondientes a cada zona.

Figura 3. Activación Adaptadores.



Fuente: Autoría Propia

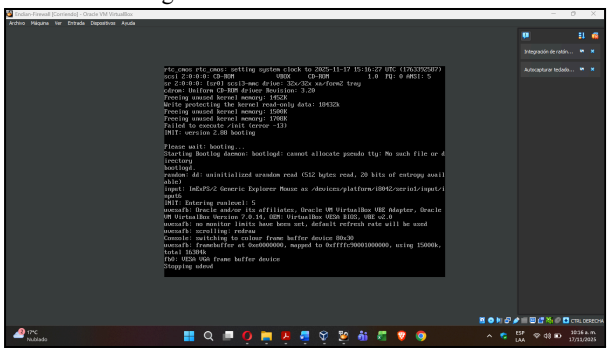
Se definieron estos nombres (“LAN” y “DMZ”) con el fin de facilitar la interconexión de los equipos utilizados en las demás temáticas del laboratorio, garantizando coherencia en el uso de las redes virtuales.

3.1.4 INSTALACIÓN DEL SISTEMA

Durante la instalación de Endian Firewall Community se seleccionaron las opciones predeterminadas del asistente, incluyendo la instalación completa del sistema, el uso total del disco y la configuración de la contraseña del usuario administrador (root). Al finalizar el proceso, la máquina virtual fue reiniciada retirando la imagen ISO para permitir el arranque normal del sistema instalado.

La siguiente imagen muestra el proceso de instalación del sistema operativo Endian Firewall.

Figura 4. Instalación ISO Endian.



Fuente: Autoría Propia

3.1.5 DIRECCIONAMIENTO IP

Con el objetivo de unificar los parámetros de red y facilitar el trabajo colaborativo, se definió un esquema de direccionamiento IP fijo para las zonas LAN y DMZ, mientras que la zona WAN obtuvo dirección IP de forma automática mediante NAT.

Este direccionamiento garantiza la correcta comunicación entre los distintos segmentos de red y evita conflictos durante las configuraciones posteriores.

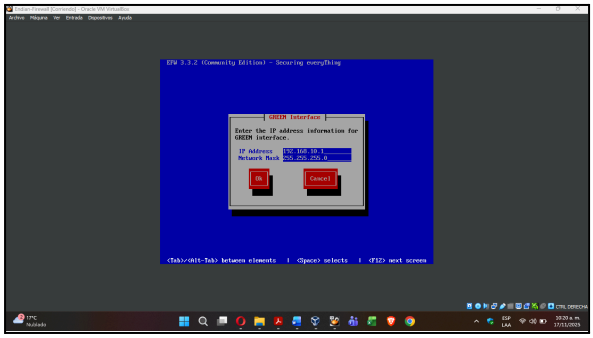
Tabla 1. Direccionamiento IP de cada zona.

Zona	Interfaz	Dirección IP	Máscara
Verde (LAN)	eth1	192.168.10.1	255.255.255.0
Naranja (DMZ)	eth2	192.168.20.1	255.255.255.0
Roja (WAN)	eth0	DHCP NAT	Automática

Fuente: Autoría Propia

La siguiente imagen presenta la configuración correspondiente a la zona Verde (LAN).

Figura 5. Instalación Zona Verde.



Fuente: Autoría Propia

3.1.6 INSTALACIÓN DEL SISTEMA

Una vez finalizada la instalación y configuración inicial del sistema, se realizó la verificación de las interfaces de red mediante comandos de diagnóstico, lo que permitió confirmar la correcta asignación de direcciones IP a cada zona. Posteriormente, se ejecutaron pruebas de conectividad hacia un host externo utilizando mensajes ICMP, con el fin de validar la salida a Internet a través de la zona WAN y comprobar el correcto funcionamiento del enrutamiento y la traducción de direcciones.

Finalmente, se accedió a la interfaz web de administración de Endian Firewall mediante el navegador, lo que confirmó que el servicio de gestión se encontraba operativo y disponible para la configuración de reglas y políticas de seguridad.

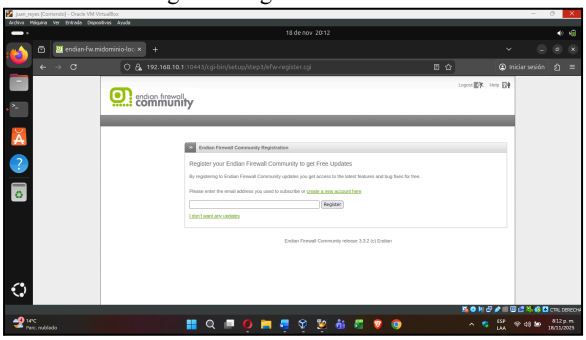
Se verificaron las interfaces con: ip addr show

También se probó la salida a Internet con: ping -c 4 8.8.8.8

Por último, se ingresó a la interfaz web: https://192.168.10.1:10443

La siguiente imagen muestra el acceso exitoso a la interfaz web del firewall.

Figura 6. Ingreso a Interfaz Web.



Fuente: Autoría Propia

Este acceso permitirá gestionar las reglas y configuraciones necesarias para las demás temáticas.

3.2 CONFIGURACIÓN NAT

Una vez configurada la instancia de Endian Firewall en VirtualBox y establecidas las zonas de red necesarias para garantizar una segmentación adecuada (LAN, DMZ y WAN), se procedió a aplicar las reglas de traducción de direcciones de red (Network Address Translation – NAT) las cuales constituyen un mecanismo fundamental en arquitecturas de seguridad perimetral, ya que permite el acceso controlado de redes privadas hacia redes externas sin exponer directamente el direccionamiento interno.

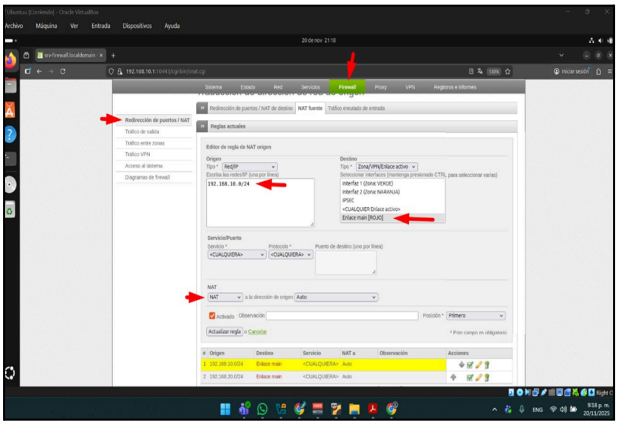
En entornos segmentados mediante zonas, como LAN, DMZ y WAN, el uso de NAT facilita la comunicación hacia Internet manteniendo el principio de ocultamiento de la topología interna y reduciendo la superficie de ataque. Como se menciona en el RFC 3022, la configuración de NAT requiere la modificación de las direcciones de origen de los paquetes para permitir la conectividad entre redes privadas y la red externa, mientras se conserva el estado de las conexiones activas [6].

En el escenario implementado, el firewall Endian actúa como punto de interconexión entre las zonas LAN, DMZ y WAN. Dado que las redes internas utilizan direccionamiento privado, se aplicaron reglas de traducción de direcciones de origen (SNAT) para permitir la salida controlada del tráfico hacia la red externa.

3.2.1 CONFIGURACIÓN NAT PARA LA RED LAN (VERDE)

Para la red LAN, identificada por el segmento 192.168.10.0/24, se configuró una regla de traducción de direcciones de origen (SNAT) asociada a la interfaz ROJA del firewall. Esta regla permite que todo el tráfico originado desde la zona VERDE sea traducido dinámicamente al momento de salir hacia la WAN, garantizando que las direcciones privadas no sean expuestas directamente a la red externa. En la Figura 7 se evidencia la regla SNAT configurada en Endian Firewall para la red LAN, donde se observa la asociación del segmento interno con la interfaz de salida hacia la WAN.

Figura 7. Configuración de la regla NAT para la red LAN.



Fuente: Autoría Propia

La correcta aplicación de esta regla se evidenció mediante pruebas de conectividad desde un equipo cliente ubicado en la LAN, las cuales incluyeron comunicación local con la interfaz del firewall y acceso a destinos externos. La recepción de respuestas exitosas confirmó que la traducción de direcciones y el enrutamiento se estaban realizando de manera adecuada, demostrando que la red LAN cuenta con salida controlada hacia Internet sin exposición directa de su direccionamiento interno.

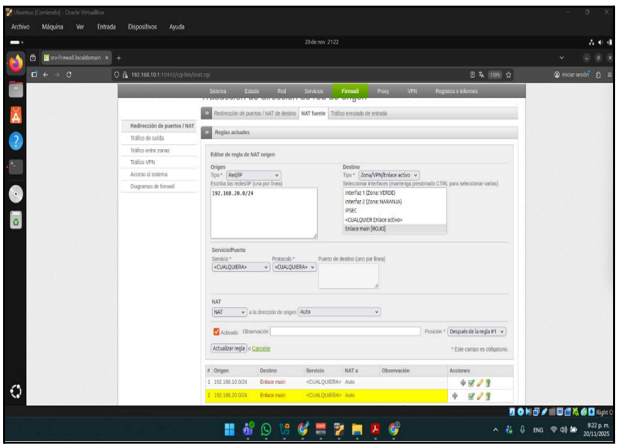
3.2.2 CONFIGURACIÓN NAT PARA LA ZONA DMZ (NARANJA)

De igual forma, se implementó una regla de traducción de direcciones de origen para la red DMZ, correspondiente al segmento 192.168.20.0/24. Esta configuración resulta especialmente relevante, ya que la DMZ alberga servicios que requieren conectividad externa controlada, como actualizaciones del sistema o acceso a recursos externos específicos. En la Figura 8 se muestra la regla SNAT aplicada a la red DMZ, donde se aprecia la traducción del tráfico proveniente de la zona NARANJA hacia la interfaz ROJA del firewall.

Adicionalmente, fue necesario habilitar explícitamente el tráfico de salida desde la zona NARANJA hacia la zona ROJA, dado que las políticas de seguridad por defecto del firewall restringen este tipo de comunicación. Esta combinación de reglas asegura que los servidores ubicados en la DMZ puedan establecer conexiones hacia la WAN sin comprometer la segmentación ni permitir flujos no autorizados.

La validación de esta configuración se realizó verificando la tabla de ruteo del servidor ubicado en la DMZ y ejecutando pruebas de conectividad hacia destinos externos. Los resultados obtenidos confirmaron que el firewall procesó correctamente el tráfico proveniente de la zona NARANJA, aplicando la traducción de direcciones conforme a la política definida y manteniendo la coherencia con la arquitectura de seguridad establecida.

Figura 8. Configuración de la regla NAT para la DMZ.



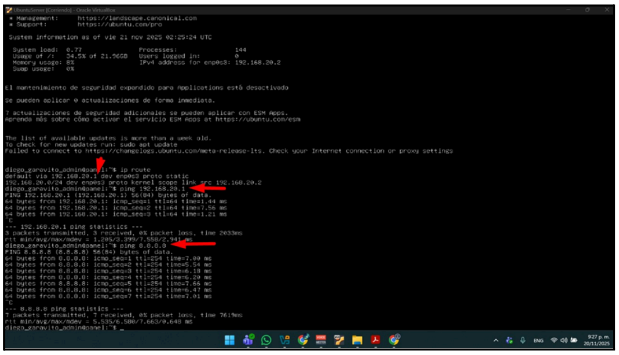
Fuente: Autoría Propia

3.2.3 VALIDACIÓN DE LA CONECTIVIDAD HACIA LA WAN

La validación del funcionamiento de NAT se realizó mediante pruebas de conectividad desde las zonas LAN y DMZ hacia la red WAN. Estas pruebas permitieron confirmar que ambos segmentos internos podían establecer comunicación externa utilizando la interfaz WAN del firewall como punto de salida, cumpliendo con los principios de ocultamiento de direcciones y control del tráfico. En la Figura 9 se presentan los resultados de las pruebas de ruteo y conectividad desde la DMZ hacia la WAN, donde se evidencia la correcta salida del tráfico a través del firewall perimetral.

El comportamiento observado demuestra que la correcta configuración de NAT, en conjunto con las reglas de tráfico inter-zona, permite una salida segura y controlada hacia Internet, sin comprometer la segmentación de la red ni la exposición de servicios internos. Este enfoque es consistente con las buenas prácticas de seguridad perimetral y con los lineamientos propuestos para firewalls basados en zonas.

Figura 9. Verificación de conectividad y ruteo desde la DMZ.



Fuente: Autoría Propia

Las reglas SNAT aplicadas permitieron el establecimiento exitoso de la comunicación tanto desde la red LAN como desde la zona DMZ hacia la WAN. Las pruebas ejecutadas confirmaron que el firewall gestionó adecuadamente la traducción de direcciones en ambos segmentos, garantizando un flujo seguro y controlado hacia la red externa. A partir de esta base, se avanzó hacia la habilitación de servicios en la zona DMZ bajo criterios de seguridad perimetral.

3.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Una vez validada la conectividad controlada entre las zonas internas y la red externa mediante la configuración de NAT, se procedió a habilitar de forma selectiva los servicios ubicados en la zona DMZ. Esta etapa tuvo como objetivo permitir el acceso a servicios específicos desde otras zonas de la red, manteniendo los principios de segmentación, mínima exposición y control estricto del tráfico característicos de una arquitectura de seguridad perimetral.

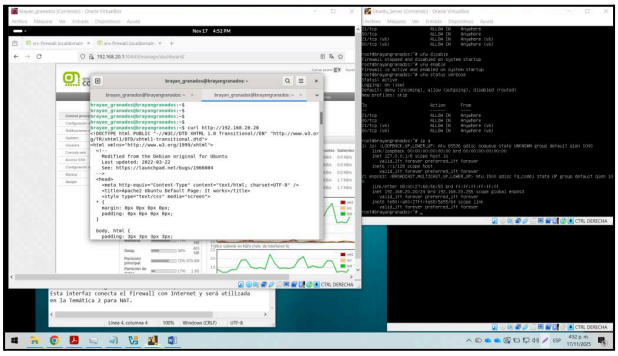
3.3.1. HABILITACIÓN DE SERVICIOS (HTTP y FTP)

Para permitir el acceso controlado a los servicios ubicados en la zona DMZ, se habilitaron los servicios HTTP y FTP en un servidor Ubuntu Server desplegado en dicho segmento. El servicio HTTP se utilizó para la publicación de contenidos web [3], mientras que el servicio FTP permitió la transferencia controlada de archivos entre la red LAN y la DMZ, conforme a la especificación del protocolo [4]. El control del tráfico hacia estos servicios se realizó mediante reglas de filtrado locales utilizando UFW, permitiendo únicamente los puertos necesarios y reforzando el esquema de seguridad bajo un enfoque de defensa en profundidad.

Este esquema responde al principio de mínima exposición, en el cual solo los servicios estrictamente necesarios son accesibles desde otras zonas de la red, reduciendo la superficie de ataque del servidor ubicado en la DMZ y complementando las políticas de control inter-zona definidas en el firewall perimetral.

En la Figura 10 se evidencia la configuración de las reglas UFW aplicadas en el servidor Ubuntu Server de la zona DMZ, donde se habilitan los puertos correspondientes a los servicios HTTP (puerto 80) y FTP (puerto 21). Esta configuración garantiza que únicamente el tráfico asociado a dichos servicios sea aceptado por el servidor, mientras que el resto de las conexiones son descartadas.

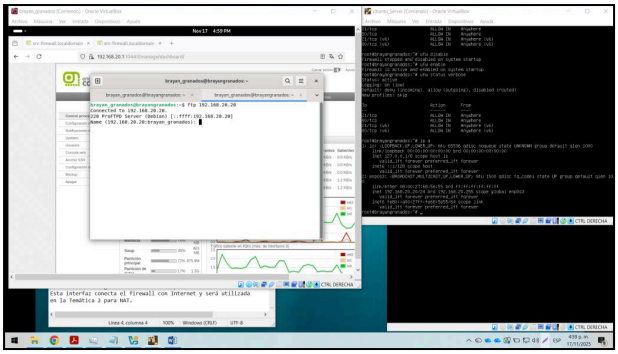
Figura 10. Aplicación de reglas UFW y acceso al servicio FTP en el servidor de la DMZ.



Fuente: Autoría Propia

La correcta operación del servicio FTP fue validada mediante una conexión autenticada desde un equipo cliente ubicado en la red interna. En la Figura 11 se muestra el establecimiento exitoso de la conexión al servidor FTP alojado en la DMZ, lo que confirma que el servicio se encuentra operativo y accesible conforme a las políticas de seguridad definidas.

Figura 11. Validación del acceso al servicio FTP desde un equipo cliente hacia el servidor de la DMZ.



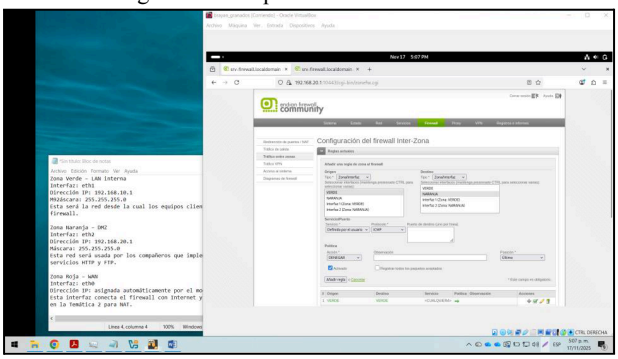
Fuente: Autoría Propia

3.3.2. CONFIGURACIÓN DEL FIREWALL PARA DENEGAR ICMP (BLOQUEAR PING)

Como medida adicional de seguridad, se configuraron reglas en el firewall perimetral Endian para denegar el tráfico ICMP desde la zona VERDE hacia la zona NARANJA. Esta restricción tiene como finalidad reducir la superficie de ataque de los servidores ubicados en la DMZ, impidiendo tareas de reconocimiento y exploración de red desde otros segmentos internos.

En la Figura 12 se evidencia la regla configurada en Endian Firewall para bloquear el tráfico ICMP entre las zonas mencionadas, donde se observa la definición explícita de la política de denegación aplicada al protocolo ICMP.

Figura 12. Bloqueo ICMP entre zonas.

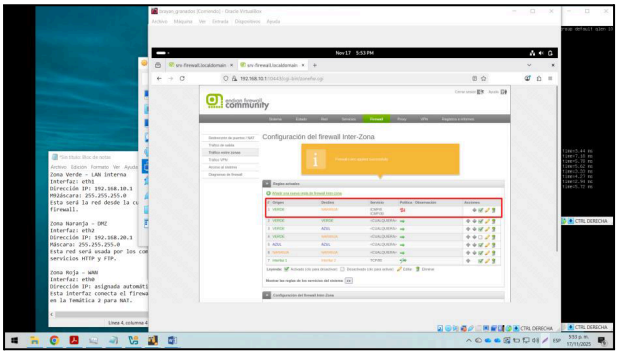


Fuente: Autoría Propia

Con el fin de garantizar la correcta aplicación de la política de seguridad definida, se verificó que la regla de bloqueo ICMP se encontrara ubicada en la primera posición dentro del conjunto de políticas del firewall, evitando que otras reglas pudieran precederla y permitir el tráfico no autorizado.

En la Figura 13 se observa la priorización de la regla de bloqueo ICMP dentro del conjunto de reglas del firewall Endian, lo que asegura su ejecución antes de otras políticas de tráfico configuradas.

Figura 13. Ubicación prioritaria de la regla de bloqueo ICMP en la configuración inter-zona del firewall Endian.

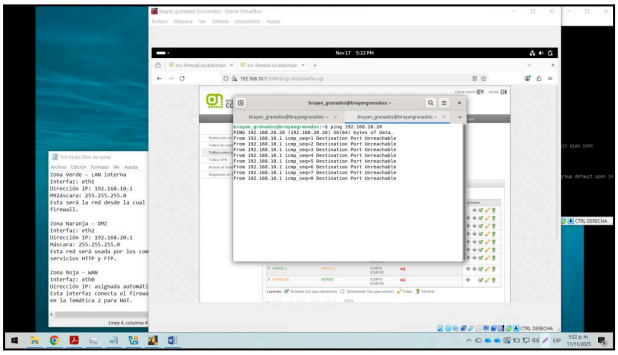


Fuente: Autoría Propia

La efectividad de la configuración implementada fue validada mediante pruebas de conectividad realizadas desde un equipo cliente ubicado en la red LAN, las cuales permitieron comprobar el comportamiento del firewall ante solicitudes ICMP dirigidas hacia la DMZ.

En la Figura 14 se evidencia que las solicitudes ICMP enviadas desde la red LAN hacia el servidor ubicado en la DMZ no reciben respuesta, confirmando el correcto funcionamiento de la regla de bloqueo implementada.

Figura 14. Prueba de conectividad ICMP fallida desde la red LAN hacia el servidor ubicado en la DMZ.



Fuente: Autoría Propia

La correcta habilitación y restricción de servicios en la zona DMZ permitió validar el funcionamiento de los mecanismos de control perimetral y local implementados en la infraestructura. A partir de estos resultados, se procedió a definir y evaluar reglas de acceso más específicas entre las zonas LAN, DMZ y WAN, con el fin de controlar de manera granular el flujo de tráfico autorizado y reforzar las políticas de seguridad establecidas en el firewall.

3.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La validación de las reglas de acceso entre zonas LAN, DMZ y WAN se llevó a cabo mediante pruebas controladas de

comunicación, utilizando herramientas de diagnóstico como curl, registros del firewall Endian, y trazabilidad de tráfico en tiempo real.

Estas pruebas permitieron determinar si las reglas diseñadas en el firewall cumplían con los objetivos de seguridad planteados, es decir, permitir únicamente el tráfico explícitamente autorizado y bloquear todo el tráfico no solicitado.

3.4.1. FUNCIONAMIENTO DEL ACCESO HTTP LAN HACIA LA DMZ

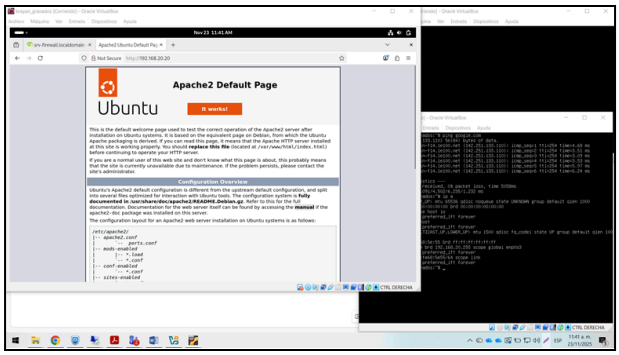
Para validar el funcionamiento de la regla que permite el acceso desde la red LAN hacia los servicios ubicados en la DMZ, se efectuó una solicitud HTTP [3] desde la máquina Desktop utilizando el comando curl http://192.168.20.20.

El servidor web ubicado en la DMZ respondió con la página por defecto de Apache, lo que confirmó que:

- El firewall permitió correctamente el tráfico HTTP (puerto 80).
- La DMZ recibió y procesó la petición sin restricciones.
- No existían bloqueos por parte del UFW del servidor en DMZ.
- Las interfaces del firewall estaban enroutando correctamente el tráfico entre zonas.

En la Figura 15 se evidencia que la zona DMZ es accesible únicamente desde la red LAN, conforme a las políticas de acceso definidas. Este comportamiento confirma que la segmentación de la red y las reglas implementadas permiten el acceso controlado a la DMZ, reforzando la postura de seguridad basada en aislamiento y control del tráfico entre zonas.

Figura 15. Ingreso del servicio HTTP desde la LAN hacia la zona DMZ.



Fuente: Autoría Propia

3.4.2. CONSUMO DE SERVICIOS HTTP HACIA LA WAN

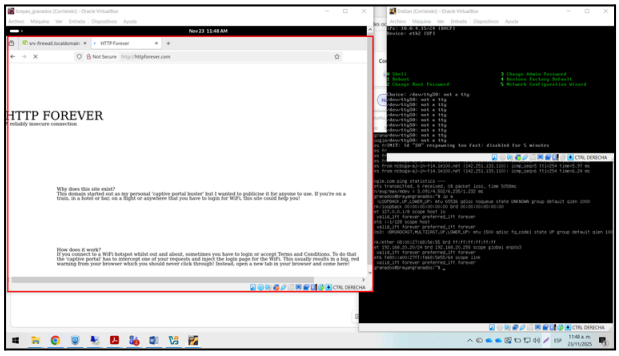
Para validar el tráfico de salida hacia Internet, se realizó una solicitud HTTP [3] desde la LAN y la DMZ hacia un sitio web público externo http://httpforever.com.

Los resultados mostraron:

- Las solicitudes fueron enviadas exitosamente hacia la WAN.
- El firewall Endian permitió las conexiones salientes según las reglas LAN → WAN y DMZ → WAN.
- Se recibieron respuestas HTTP válidas, demostrando conectividad total hacia Internet.
- No existieron bloqueos imprevistos por parte del Firewall o políticas internas.

En la Figura 16 se evidencia el acceso exitoso al servicio HTTP desde la red LAN hacia la zona WAN, lo que confirma que el firewall Endian realiza correctamente la traducción de direcciones (NAT) para el tráfico originado en la red interna. Este comportamiento demuestra que las reglas de salida configuradas permiten la comunicación externa sin exponer el direccionamiento interno, cumpliendo con los principios de seguridad perimetral establecidos.

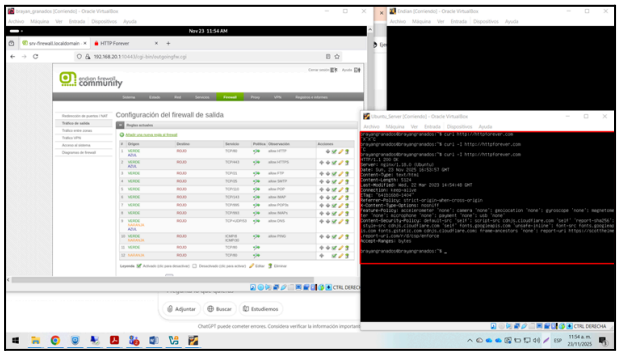
Figura 16. Ingreso del servicio HTTP desde la LAN hacia la zona WAN



Fuente: Autoría Propia

En la Figura 17 se observa el acceso al servicio HTTP desde la zona DMZ hacia la zona WAN, validando que la traducción de direcciones (NAT) se aplica de manera adecuada también para este segmento. Este resultado confirma que el tráfico generado desde la DMZ puede salir hacia la red externa de forma controlada, manteniendo la segmentación de la red y las políticas de seguridad definidas en el firewall perimetral.

Figura 17. Ingreso del servicio HTTP desde la DMZ hacia la zona WAN



Fuente: Autoría Propia

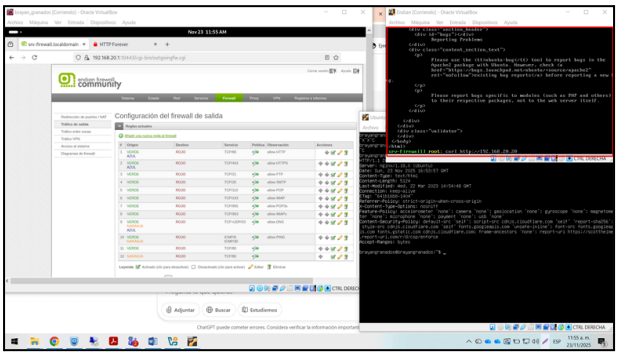
3.4.3 ACCESO HTTP DESDE LA WAN HACIA LA DMZ

Con el fin de simular tráfico entrante desde Internet, se utilizó la terminal de la interfaz WAN de Endian para ejecutar el comando curl http://192.168.20.20, donde el servidor de la DMZ respondió exitosamente. Este resultado comprobó que:

- La DMZ estaba correctamente expuesta de manera controlada a la WAN.
- La regla WAN → DMZ estaba permitiendo únicamente tráfico HTTP autorizado.
- No existía exposición no deseada de puertos adicionales.
- El firewall cumplía su función como primera línea de defensa.

En la Figura 18 se evidencia el acceso al servicio HTTP desde la zona WAN hacia la zona DMZ, lo que valida el principio de publicación segura de servicios en una arquitectura de seguridad perimetral. Este comportamiento confirma que la DMZ funciona como una zona intermedia entre la red externa y la red LAN, permitiendo la exposición controlada de servicios sin comprometer el aislamiento de la red interna.

Figura 18. Ingreso del servicio HTTP desde la WAN hacia la zona DMZ



Fuente: Autoría Propia

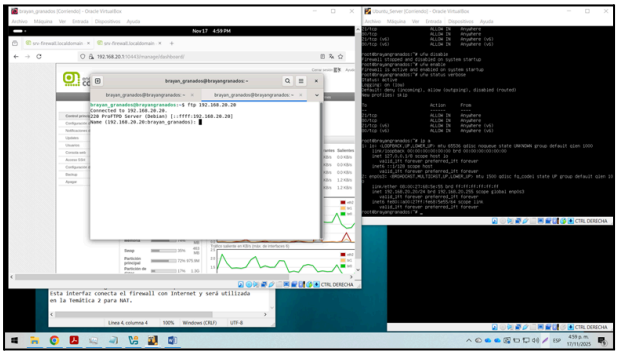
3.4.4. FUNCIONAMIENTO DEL SERVICIO FTP

Para evaluar las reglas asociadas al servicio FTP, se implementó un servidor FTP dentro de la DMZ y se ejecutaron pruebas desde la LAN por consola donde demostraron que:

- El puerto 21 estaba correctamente habilitado en Endian y UFW.
- El servidor FTP respondió inmediatamente solicitando credenciales.
- Las transferencias de archivos se completaron sin interrupciones.
- No se identificaron problemas de modo pasivo o activo.
- Las carpetas de usuario en la DMZ respetaron permisos y propietarios definidos.

En la Figura 19 se evidencia el acceso al servicio FTP desde la red LAN hacia la zona DMZ, lo que permitió verificar la correcta operación del servicio y la aplicación de las reglas de acceso definidas. Este resultado confirma que el acceso al servicio FTP se realiza de forma segura y controlada, considerando las particularidades propias de este protocolo, el cual utiliza canales separados para control y transferencia de datos, lo que requiere configuraciones específicas para su correcto funcionamiento [4].

Figura 19. Ingreso del servicio FTP desde la LAN hacia la zona DMZ



Fuente: Autoría Propia

3.4.5. VALIDACIÓN VISUAL DEL TRÁFICO EN ENDIAN

Una vez ejecutadas las pruebas prácticas, se realizó una inspección detallada del módulo Inter-Zone Traffic del firewall Endian, lo que permitió observar en tiempo real:

- Registros generados por cada solicitud HTTP y FTP.
- Correspondencia exacta entre reglas definidas y tráfico permitido.
- Ausencia de paquetes bloqueados que pudieran interferir con la operación.
- Información detallada de IP origen, IP destino, protocolo y puerto.
- Flujo consistente con el modelo de segmentación planeado (LAN ↔ DMZ ↔ WAN).

La validación visual cumplió un papel fundamental, ya que permitió verificar que la política de seguridad aplicada no solo funcionaba correctamente, sino que además se mantenía alineada con los principios de seguridad perimetral, reforzando la arquitectura basada en zonas.

La correcta aplicación de reglas demostró que el firewall actuaba de forma efectiva como un mecanismo de control de acceso, garantizando que cada zona se comunicará únicamente bajo criterios definidos.

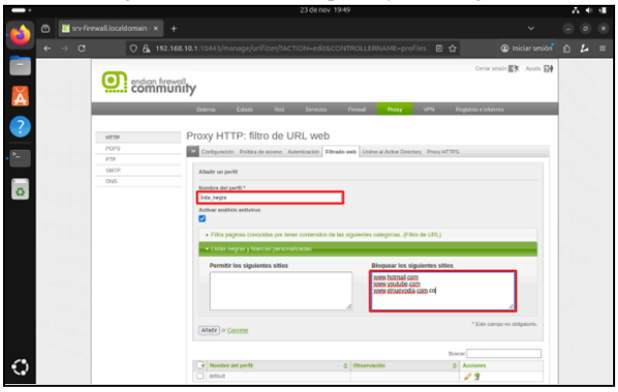
3.5 IMPLEMENTACIÓN DEL PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

Para complementar las configuraciones anteriores, se implementó un Proxy HTTP no transparente utilizando el módulo de proxy de Endian Firewall. La primera etapa consistió en habilitar el proxy en la zona VERDE y configurar el puerto 8080 como canal de comunicación. Posteriormente, se creó un perfil de filtrado denominado lista_negra, donde se agregaron los sitios www.hotmail.com, www.youtube.com y

www.elnuevodia.com.co, con el fin de limitar el acceso a estos portales desde la red LAN.

En la Figura 20 se evidencia la definición del perfil de filtrado y la creación de la lista negra dentro del módulo de proxy HTTP de Endian Firewall. Esta configuración permite establecer restricciones centralizadas sobre los contenidos accesibles desde la red LAN, constituyendo la base del control de navegación y garantizando que las políticas de filtrado se apliquen de forma consistente a los usuarios que utilicen el servicio proxy.

Figura 20. Creación de perfil y lista negra

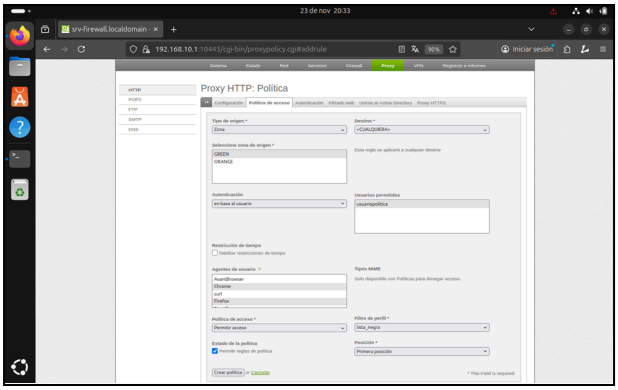


Fuente: Autoría Propia

A continuación, se habilitó el método de autenticación local (NCSA) y se creó el usuario usuariopolitica, quien fue vinculado a un grupo específico para la aplicación de políticas personalizadas. Una vez configurados el perfil y el usuario, se generó una política de acceso asociando el perfil de lista negra con la autenticación del usuario, de manera que solo se permitiera la navegación después de ingresar credenciales válidas.

En la Figura 21 se observa la asociación del perfil de filtrado con el mecanismo de autenticación local, así como la creación de una política de acceso basada en usuario. Este enfoque permite aplicar restricciones de navegación de manera individualizada, reforzando el control de acceso y asegurando que el uso del servicio proxy esté condicionado a la validación previa de credenciales.

Figura 21. Creación de política con autenticación de usuario

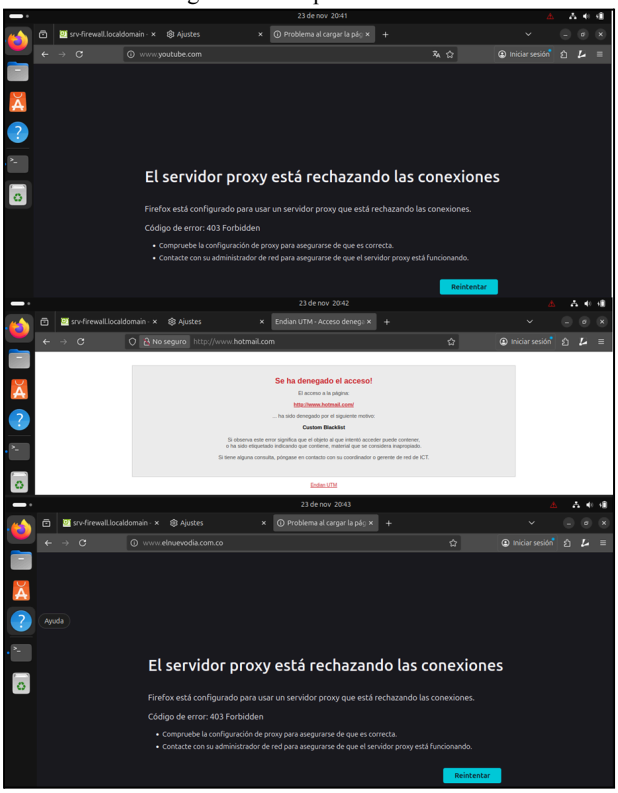


Fuente: Autoría Propia

Finalmente, desde un equipo en la zona VERDE se configuró manualmente el proxy en el navegador utilizando la IP 192.168.10.1 y el puerto 8080. Durante las pruebas, el navegador solicita las credenciales del usuario creado y, tras autenticarse, permite navegar por sitios generales. Los portales incluidos en la lista negra fueron bloqueados correctamente, mostrando la página de denegación de acceso del firewall. Estas pruebas confirmaron la correcta implementación del proxy, la autenticación obligatoria y el filtrado basado en políticas definidas.

En la Figura 22 se evidencia el comportamiento del proxy HTTP durante las pruebas de navegación, donde los sitios incluidos en la lista negra son bloqueados correctamente tras la autenticación del usuario. Este resultado confirma la correcta integración entre el filtrado de contenido y el mecanismo de autenticación, validando la efectividad de las políticas definidas para el control de acceso web desde la red LAN.

Figura 22. Bloqueo de sitios



Fuente: Autoría Propia

Con la ejecución de las actividades definidas se dio por finalizada la implementación del esquema de seguridad perimetral propuesto, logrando la correcta integración de los mecanismos de segmentación de red, control de tráfico, publicación segura de servicios y filtrado de acceso. A partir de esta infraestructura funcional, en la siguiente sección se presentan las pruebas de evaluación y el análisis de los resultados obtenidos, orientados a verificar el comportamiento y la efectividad de las políticas de seguridad configuradas.

4 RESULTADOS

En esta sección se presentan los resultados obtenidos a partir de la implementación del esquema de seguridad perimetral propuesto. Los resultados se organizan de acuerdo con cada una de las configuraciones realizadas, permitiendo evidenciar el comportamiento de la infraestructura, la efectividad de las políticas aplicadas y el cumplimiento de los objetivos de seguridad establecidos, de esta manera se facilita la evaluación individual de cada componente antes de su análisis e interpretación en la sección de discusión.

4.1 RESULTADOS DE LA CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED)

Los resultados obtenidos evidenciaron que la configuración inicial de la instancia de Endian Firewall Community en el entorno virtualizado proporcionó una base estable para la implementación del esquema de seguridad perimetral. La correcta asignación de recursos de hardware virtual y la definición de múltiples interfaces de red permitieron el funcionamiento adecuado del firewall y la segmentación lógica de la red, lo cual es coherente con las buenas prácticas para entornos virtualizados de laboratorio descritas en la documentación de VirtualBox [2].

Asimismo, la correcta identificación y activación de las zonas VERDE, NARANJA y ROJA permitió establecer un entorno controlado para la aplicación de políticas de seguridad diferenciadas, garantizando la separación funcional entre la red interna, la DMZ y la red externa.

4.2 RESULTADOS DE LA CONFIGURACIÓN NAT

Los resultados obtenidos permitieron verificar que la traducción de direcciones de red permitió la salida controlada del tráfico desde las zonas internas hacia la red externa sin exponer el direccionamiento privado. Las pruebas de conectividad realizadas desde la red LAN y la DMZ confirmaron que el firewall aplicó correctamente la traducción de direcciones de origen, permitiendo el acceso a servicios externos y recibiendo respuestas válidas.

Este comportamiento confirma que el mecanismo de NAT implementado cumple con el principio de ocultamiento del direccionamiento interno, característica fundamental de los traductores de direcciones tradicionales descritos en el estándar correspondiente [6], y valida su correcta integración dentro del esquema de seguridad perimetral configurado.

4.3 RESULTADOS DE LA HABILITACIÓN DE SERVICIOS EN LA ZONA DMZ

Se evidenció que los servicios HTTP y FTP alojados en la zona DMZ se encontraban operativos y accesibles únicamente desde las zonas autorizadas. El servicio HTTP permitió la publicación controlada de contenido web, mientras que el servicio FTP facilitó la transferencia de archivos entre la red LAN y la DMZ de forma autenticada, conforme al funcionamiento esperado del protocolo FTP [4].

Adicionalmente, los resultados confirmaron que el uso de reglas de filtrado locales en el servidor de la DMZ permitió restringir el acceso únicamente a los puertos necesarios, reduciendo la superficie de ataque del sistema y reforzando el control de acceso a los servicios expuestos. Este resultado validó que el principio de mínima exposición fue correctamente implementado en la publicación de servicios.

4.4 RESULTADOS DE LAS REGLAS DE ACCESO Y CONTROL INTER-ZONA

Las pruebas realizadas permitieron verificar que las reglas de acceso configuradas entre las zonas LAN, DMZ y WAN se aplicaron de manera coherente con las políticas de seguridad definidas. En particular, se evidenció que el tráfico ICMP desde la red LAN hacia la DMZ fue correctamente bloqueado, impidiendo la realización de pruebas de conectividad y reconocimiento hacia los servidores ubicados en la zona intermedia.

Este comportamiento validó que el firewall perimetral gestionó adecuadamente el tráfico entre zonas, restringiendo protocolos de diagnóstico como ICMP, los cuales, aunque útiles para pruebas, pueden ser utilizados con fines de exploración de red según lo descrito para este protocolo [5]. La priorización de las reglas garantizó que las políticas de denegación se aplicaran antes que otras reglas permisivas.

4.5 RESULTADOS DE LA IMPLEMENTACIÓN DEL PROXY HTTP AUTENTICADO

Los resultados de las pruebas de navegación demostraron que el proxy HTTP no transparente implementado en Endian Firewall funcionó de manera adecuada, exigiendo autenticación previa para permitir el acceso a recursos web desde la red LAN. Una vez autenticado el usuario, se comprobó que la navegación hacia sitios permitidos se realizaba sin inconvenientes.

Adicionalmente, se evidenció que los sitios incluidos en la lista negra fueron bloqueados correctamente, mostrando la página de denegación del firewall. Este comportamiento confirmó la correcta integración entre el mecanismo de autenticación, las políticas de filtrado y el control de navegación, consolidando un esquema de control de acceso web efectivo y alineado con las funcionalidades del proxy HTTP de Endian Firewall [1].

5 DISCUSIÓN

En esta sección se analizan e interpretan los resultados obtenidos a partir de la implementación del esquema de seguridad perimetral propuesto. La discusión se organiza de acuerdo con cada uno de los componentes configurados, con el propósito de evaluar su impacto en la seguridad de la infraestructura, su coherencia con los principios teóricos de la seguridad perimetral y su contribución al cumplimiento de los objetivos planteados. Este análisis permite contextualizar los

resultados dentro de buenas prácticas y estándares reconocidos, facilitando una comprensión integral del comportamiento observado del sistema.

5.1 DISCUSIÓN DE LA CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED)

La correcta configuración de las zonas de red en el entorno virtualizado utilizando VirtualBox y Endian Firewall Community evidenció que la segmentación y asignación fija de direcciones son fundamentales para garantizar un trabajo sin interferencias. La virtualización permitió simular un entorno de red real, donde las configuraciones de NAT, DMZ y LAN no solo son posibles, sino fáciles de gestionar, lo que refuerza la flexibilidad y adaptabilidad del laboratorio educativo [2]. Esta infraestructura también demostró ser eficaz para realizar pruebas sin comprometer el entorno real, una característica clave para entornos educativos y de laboratorio donde se necesita replicar situaciones de red complejas sin riesgo para las redes físicas.

5.2 DISCUSIÓN DE LA CONFIGURACIÓN NAT

La implementación de NAT en Endian Firewall cumplió un papel esencial en el proceso de conexión entre redes internas y externas. La segmentación de redes mediante NAT no solo permite la conexión controlada a la red externa, sino que refuerza el principio de ocultamiento del direccionamiento interno, lo que reduce el riesgo de exposición del sistema a posibles ataques. Las reglas de SNAT diferenciadas para la LAN y la DMZ validaron que la arquitectura de seguridad perimetral es capaz de controlar el flujo de tráfico sin comprometer la conectividad, algo que se alinea con las recomendaciones de RFC 3022, que especifican la importancia de un NAT bien implementado para entornos de seguridad [6]. La implementación correcta de NAT en Endian Firewall demostró ser eficaz para ocultar la topología interna y permitir un control granular sobre el tráfico saliente.

5.3 DISCUSIÓN DE LA HABILITACIÓN DE SERVICIOS EN LA ZONA DMZ

La habilitación controlada de los servicios HTTP y FTP en la zona DMZ demostró cómo se puede permitir el acceso a servicios críticos sin comprometer la seguridad de la red interna. La filtración de tráfico mediante iptables y la aplicación de políticas de seguridad estratificadas garantizaron que solo el tráfico legítimo pueda alcanzar los servicios expuestos, lo cual es un ejemplo de defensa en profundidad. La configuración de la DMZ mostró que se puede ofrecer acceso externo limitado a ciertos servicios, asegurando la protección de la infraestructura interna al mismo tiempo. La combinación de este enfoque con políticas de filtrado permitió comprobar que la seguridad perimetral no solo depende de la segmentación, sino también de la correcta implementación de controles de acceso que refuercen esa segmentación.

5.4 DISCUSIÓN DE LAS REGLAS DE ACCESO Y CONTROL INTER-ZONA

Las reglas de acceso inter-zona implementadas demostraron que la correcta gestión del tráfico entre la LAN, la DMZ y la WAN es esencial para asegurar una arquitectura de seguridad sólida. Bloquear ICMP desde la LAN hacia la DMZ resultó ser una medida efectiva para mitigar el riesgo de ataques de reconocimiento de red. RFC 792 explica que ICMP puede ser utilizado para realizar tareas de escaneo de red, lo que hace que su restricción sea esencial en entornos donde la exposición de servicios debe ser minimizada [5]. El control granular de acceso entre zonas refuerza la postura de seguridad al garantizar que solo el tráfico explícitamente autorizado pueda pasar entre las redes, cumpliendo con los principios de segmentación y control de tráfico.

5.5 DISCUSIÓN DE LA IMPLEMENTACIÓN DEL PROXY HTTP AUTENTICADO

La implementación de un proxy HTTP no transparente con autenticación local demostró ser un mecanismo eficaz para monitorear y controlar el tráfico web generado desde la LAN. Al exigir autenticación previa, se introdujo un nivel adicional de control, lo que permite rastrear y regular el acceso a recursos web. Esta funcionalidad es fundamental en entornos educativos, donde se requiere supervisar el uso de Internet. La lista negra utilizada para bloquear sitios como YouTube y Hotmail refuerza el control de acceso a recursos web específicos, demostrando que la combinación de filtrado de contenidos y autenticación permite cumplir con las políticas de navegación definidas. El uso de Endian Firewall como proxy confirma que los sistemas de filtrado y trazabilidad de tráfico son componentes críticos en la seguridad perimetral, permitiendo un control exhaustivo de los servicios accesibles desde la red interna [1].

El trabajo desarrollado se enfocó en la validación de un esquema de seguridad perimetral en un entorno virtualizado de laboratorio. Aspectos como alta disponibilidad, escalabilidad o integración con sistemas avanzados de detección de intrusos no fueron abordados, dado que exceden los objetivos y el contexto académico definidos para esta implementación. No obstante, el alcance planteado permitió verificar de manera efectiva el funcionamiento de los principales mecanismos de seguridad perimetral, cumpliendo con los objetivos propuestos y proporcionando un entorno adecuado para el análisis y comprensión de políticas de control de acceso en redes segmentadas.

6 CONCLUSIONES

La configuración inicial de la instancia de Endian Firewall Community permitió establecer un entorno virtualizado estable y uniforme para el desarrollo del laboratorio. La correcta definición de las zonas VERDE, NARANJA y ROJA, junto con un esquema de direccionamiento fijo, facilitó el trabajo colaborativo y sentó las bases técnicas necesarias para la implementación progresiva de políticas de seguridad perimetral.

La implementación de reglas NAT para las redes LAN y DMZ permitió validar que el firewall Endian gestiona de manera adecuada la traducción de direcciones y el enrutamiento del tráfico hacia la WAN. Las pruebas realizadas confirmaron que la conectividad externa puede habilitarse de forma controlada, manteniendo el ocultamiento del direccionamiento interno y reforzando la segmentación de la arquitectura perimetral.

La habilitación controlada de los servicios HTTP y FTP en la zona DMZ demostró que es posible ofrecer servicios a otras zonas de la red sin comprometer la seguridad de la infraestructura interna. La combinación entre segmentación de red y reglas de filtrado específicas permitió garantizar la disponibilidad de los servicios, al tiempo que se restringió el acceso únicamente a los protocolos autorizados.

La configuración y validación de reglas de acceso inter-zona evidenció la importancia de aplicar políticas estrictas de control del tráfico en entornos segmentados. El bloqueo del tráfico ICMP y la correcta priorización de las reglas permitieron reducir la exposición de la DMZ frente a tareas de reconocimiento, fortaleciendo la postura de seguridad del firewall perimetral.

La implementación del proxy HTTP no transparente con autenticación permitió comprobar la efectividad del control de navegación basado en usuarios y políticas. El uso de perfiles y listas de bloqueo facilitó la restricción de contenidos específicos, demostrando que el proxy de Endian Firewall constituye un mecanismo eficaz para reforzar el control de acceso web y la trazabilidad del tráfico generado desde la red LAN.

En conjunto, las configuraciones realizadas permitieron validar la efectividad de un esquema de seguridad perimetral basado en zonas, apoyado en mecanismos de segmentación, traducción de direcciones, control de servicios y filtrado de tráfico. Los resultados obtenidos confirman que el uso de Endian Firewall en entornos GNU/Linux permite implementar políticas de seguridad coherentes y funcionales, orientadas al control del acceso, la protección de servicios y la gestión segura del tráfico entre redes segmentadas.

7 REFERENCIAS

[1] Endian Firewall Community Documentation. Disponible en: https://www.endian.com/community/

[2] Oracle VirtualBox User Manual. Disponible en: https://www.virtualbox.org/manual/

[3] The Apache Software Foundation, "*The Apache HTTP Server Project,*" 2024. [Online]. Available: https://httpd.apache.org/

[4] Internet Engineering Task Force (IETF), *"RFC 959: File Transfer Protocol (FTP),"* 1985. [Online]. Available: https://www.rfc-editor.org/rfc/rfc959

[5] IETF, "*RFC 792: Internet Control Message Protocol*," 1981. [Online]. Available: https://www.rfc-editor.org/rfc/rfc792

[6] Internet Engineering Task Force, "*RFC 3022: Traditional IP Network Address Translator (Traditional NAT),*" Jan. 2001. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3022