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

Johana Carolina Quevedo Perez
jcquevedop@unadvirtual.edu.co

RESUMEN: *En este trabajo se presenta el diseño e implementación de una arquitectura de seguridad perimetral basada en zonas mediante el uso de Endian Firewall Community en un entorno virtualizado. La solución se desarrolló empleando Oracle VM VirtualBox, permitiendo la segmentación de la red en tres zonas fundamentales: WAN (Red), LAN (Green) y DMZ (Orange). Se implementaron mecanismos de traducción de direcciones de red (NAT) con el fin de garantizar la comunicación controlada entre segmentos, preservando el ocultamiento del direccionamiento interno. Asimismo, se configuraron políticas de acceso y filtrado para habilitar servicios específicos como HTTP y FTP en la DMZ, así como restricciones de tráfico mediante reglas de firewall, incluyendo la denegación del protocolo ICMP para mitigar actividades de reconocimiento. Adicionalmente, se implementó un proxy HTTP no transparente con autenticación de usuarios y filtrado de contenido, lo que permitió controlar la navegación web y aplicar políticas de acceso basadas en perfiles. Los resultados obtenidos evidencian que la arquitectura propuesta permite una adecuada segmentación de la red, un control eficiente del tráfico y una reducción significativa de la superficie de ataque, consolidando a Endian Firewall como una solución viable y eficaz para la implementación de seguridad perimetral en entornos GNU/Linux.*

PALABRAS CLAVE: Endian Firewall; VirtualBox; segmentación de red; NAT; DMZ; proxy HTTP

1 INTRODUCCIÓN

La seguridad de redes constituye un componente fundamental dentro de la infraestructura tecnológica de organizaciones y entornos académicos. El incremento de amenazas informáticas ha generado la necesidad de implementar mecanismos de protección que permitan controlar el acceso, segmentar los recursos y garantizar la integridad de la información.

En este contexto, los firewalls perimetrales desempeñan un papel clave, ya que permiten establecer políticas de control sobre el tráfico de red, gestionar la comunicación entre diferentes segmentos y reducir la exposición de los sistemas internos frente a posibles ataques.

El presente trabajo tiene como objetivo el diseño e implementación de un esquema de seguridad perimetral basado en zonas, utilizando la distribución GNU/Linux Endian Firewall Community en un entorno virtualizado. La arquitectura propuesta se fundamenta en la segmentación de la red en tres zonas: LAN, DMZ y WAN, lo que permite aplicar políticas diferenciadas de acceso y control de tráfico.

A partir de esta estructura, se implementan mecanismos de traducción de direcciones (NAT), reglas de firewall para la habilitación y restricción de servicios, y un proxy HTTP con autenticación, con el fin de fortalecer la seguridad de la infraestructura.

Por último, se realizan pruebas de conectividad y validación del tráfico que permiten evaluar el comportamiento del sistema y verificar la efectividad de las políticas de seguridad implementadas.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar e implementar una solución de seguridad perimetral en GNU/Linux utilizando Endian Firewall Community, integrando segmentación de red, políticas de control de tráfico, NAT y servicios proxy, con el objetivo de fortalecer la seguridad, gestionar el acceso a la red y garantizar el funcionamiento controlado de los servicios HTTP y FTP.

2.2 OBJETIVOS ESPECÍFICOS

- Configurar un entorno virtualizado en VirtualBox mediante la creación de una máquina virtual con Endian Firewall, asignando los recursos necesarios para su correcto funcionamiento.
- Instalar el sistema operativo del firewall a partir de la imagen ISO, garantizando su adecuada implementación en el entorno virtual.
- Establecer la segmentación de la red mediante la configuración de las interfaces correspondientes a las zonas WAN (Roja), LAN (Verde) y DMZ (Naranja), asignando direcciones IP estáticas.
- Verificar la conectividad inicial entre las diferentes zonas de red mediante pruebas desde consola, asegurando la correcta comunicación entre los segmentos.
- Implementar mecanismos de traducción de direcciones de red (NAT) que permitan la comunicación controlada entre las zonas LAN, DMZ y WAN.
- Configurar y habilitar servicios de red basados en los protocolos HTTP y FTP dentro de la arquitectura definida, garantizando su accesibilidad bajo políticas de seguridad.
- Realizar pruebas de acceso y conectividad a los servicios implementados desde las diferentes zonas de la red, utilizando herramientas de verificación como navegador web y comandos de red.

3 METODOLOGÍA

La metodología empleada se fundamenta en la implementación de un entorno virtualizado mediante Oracle VM VirtualBox, en el cual se configuró una máquina virtual con

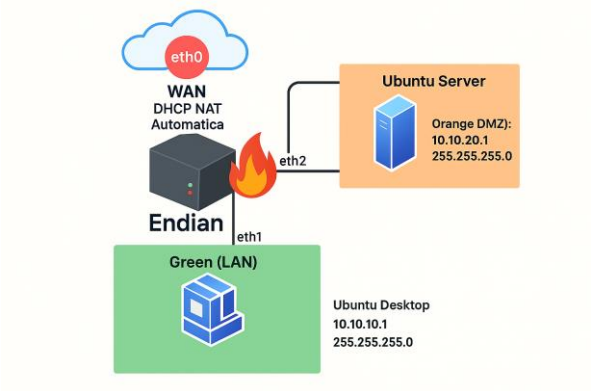
Endian Firewall Community como elemento central de la arquitectura de seguridad.

Inicialmente, se definió la estructura de red basada en segmentación por zonas, estableciendo tres interfaces correspondientes a WAN, LAN y DMZ. A partir de esta configuración, se procedió a la asignación de direcciones IP, utilizando un esquema de direccionamiento estático para las zonas internas y dinámico para la conexión externa.

Con el propósito de estandarizar los parámetros de red durante la implementación, se definió un esquema de direccionamiento IP basado en asignación estática para las zonas LAN y DMZ, mientras que la zona WAN fue configurada para obtener su dirección IP de forma automática mediante el protocolo Dynamic Host Configuration Protocol (DHCP), apoyado por un mecanismo de traducción de direcciones de red (NAT).

Este enfoque permite mantener un control preciso sobre las direcciones internas, facilitando la administración de la red y la aplicación de políticas de seguridad, mientras que la asignación dinámica en la WAN simplifica la integración con redes externas. Asimismo, este esquema reduce la probabilidad de conflictos de direccionamiento y garantiza la correcta comunicación entre los diferentes segmentos de la infraestructura.

Figura 1. Direccionamiento IP por zona.



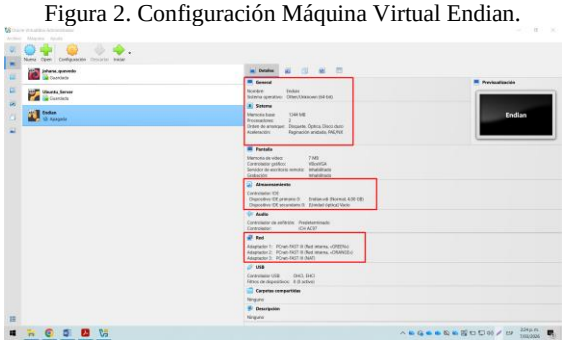
Fuente: Autoría Propia

4. CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

Se implementó una máquina virtual en Oracle VM VirtualBox con el nombre Endian, destinada a la instalación del sistema de seguridad perimetral. Durante su configuración, se definieron los siguientes parámetros: tipo de sistema operativo Linux, versión Other Linux (64-bit), asignación de 1344 MB de memoria RAM, dos núcleos de CPU y un disco duro virtual de 4 GB en formato VDI.

La asignación de estos recursos resulta adecuada para el funcionamiento estable de Endian Firewall Community, ya que permite gestionar el tráfico de red entre las diferentes zonas definidas dentro de la arquitectura propuesta. En particular, la cantidad de memoria y la capacidad de procesamiento asignadas garantizan un desempeño eficiente durante la ejecución de pruebas de conectividad, la aplicación de reglas de firewall y la validación de políticas de seguridad, evitando cuellos de botella en el procesamiento de paquetes.

Figura 2. Configuración Máquina Virtual Endian.



Fuente: Autoría Propia

La Figura 2 presenta la configuración general de la máquina virtual utilizada en la implementación del firewall perimetral. En esta se observa el resumen de los parámetros definidos durante la creación de la instancia en VirtualBox, incluyendo el tipo de sistema operativo, la memoria asignada, la cantidad de núcleos de procesamiento y la capacidad del disco virtual.

Esta configuración inicial constituye la base de la infraestructura sobre la cual se implementaron posteriormente las interfaces de red, la segmentación por zonas y las políticas de seguridad, permitiendo un entorno controlado y adecuado para la evaluación del comportamiento del sistema.

Para dar inicio al proceso de instalación del firewall, se montó la imagen ISO community_community-x64_3.3.2_recovery_softwarex86-64_20201101220035.iso en el controlador IDE de la máquina virtual configurada en Oracle VM VirtualBox.

Esta configuración permitió que, durante el arranque inicial, el sistema reconociera el medio de instalación y ejecutara automáticamente el asistente de instalación de Endian Firewall Community. De esta manera, se garantizó un proceso de instalación controlado, evitando conflictos con otros dispositivos de arranque y asegurando la correcta carga del sistema operativo [1].

Adicionalmente, el uso de una imagen ISO montada como unidad óptica virtual facilita la replicabilidad del entorno, permitiendo reinstalaciones o pruebas adicionales sin necesidad de medios físicos, lo cual resulta especialmente útil en entornos virtualizados.

Figura 3. Configuración de la imagen

Fuente: Autoría Propia

La Figura 3 muestra la configuración de almacenamiento de la máquina virtual en VirtualBox, donde se evidencia la asignación de la imagen ISO al controlador IDE. Esta disposición permite que el sistema arranque directamente desde el medio de instalación, iniciando el proceso de configuración del firewall de manera automática.

Dicha configuración constituye un paso fundamental dentro de la implementación, ya que establece el punto de partida para la instalación del sistema y la posterior configuración de las interfaces de red y políticas de seguridad.

Con el propósito de implementar un esquema de seguridad perimetral basado en segmentación por zonas, se configuraron tres adaptadores de red en la máquina virtual definida en Oracle VM VirtualBox, asignando cada uno a un segmento específico de la infraestructura.

Las configuraciones establecidas fueron las siguientes:

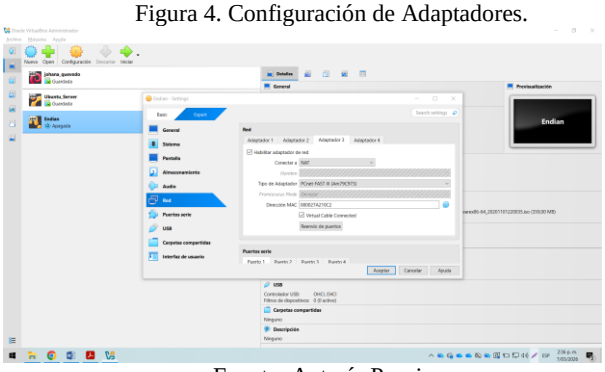
- Zona Red (WAN): Adaptador configurado en modo NAT, permitiendo la conexión hacia la red externa.
- Zona Green (LAN): Adaptador configurado como red interna denominada LAN, destinada a los equipos de la red local.
- Zona Orange (DMZ): Adaptador configurado como red interna denominada DMZ, destinada a la exposición controlada de servicios.

Esta segmentación responde a un modelo clásico de seguridad perimetral, en el cual se separan los recursos internos, los servicios públicos y la conexión a redes externas. De esta manera, se logra aislar cada zona, reduciendo la superficie de ataque y permitiendo aplicar políticas de seguridad diferenciadas para cada segmento [1].

En particular, la zona LAN se protege frente a accesos directos desde el exterior, mientras que la DMZ actúa como una zona intermedia donde se ubican servicios que requieren ser accesibles, pero bajo restricciones controladas. Por su parte, la zona WAN representa el entorno externo, desde el cual pueden originarse conexiones no confiables.

La Figura 4 presenta la configuración de los adaptadores de red en VirtualBox, donde se observa la asignación de cada interfaz a las zonas Roja, Verde y Naranja. Esta configuración constituye un elemento fundamental dentro de la arquitectura implementada, ya que permite establecer la base para la aplicación de reglas de firewall, políticas de acceso y mecanismos de control de tráfico entre las diferentes zonas.

Figura 4. Configuración de Adaptadores.



Fuente: Autoría Propia

Con el fin de garantizar la coherencia en la configuración de la infraestructura de red virtual, se definieron las denominaciones LAN y DMZ para los segmentos internos implementados en Oracle VM VirtualBox.

Esta nomenclatura permite identificar de manera clara y consistente cada zona de la arquitectura, facilitando la interconexión de los equipos utilizados durante el desarrollo del laboratorio. Asimismo, contribuye a la correcta asociación de las interfaces de red de las máquinas virtuales con los segmentos correspondientes, evitando errores de configuración y asegurando la integridad del esquema de segmentación.

Adicionalmente, el uso de nombres estandarizados como LAN y DMZ favorece la comprensión de la topología de red y simplifica la integración de nuevas máquinas virtuales en etapas posteriores, permitiendo mantener una estructura organizada y escalable dentro del entorno virtualizado.

Durante el proceso de instalación de Endian Firewall Community, se emplearon las configuraciones predeterminadas proporcionadas por el asistente de instalación del sistema. Entre las opciones seleccionadas se incluyeron la instalación completa del sistema, la asignación total del disco duro virtual para el sistema operativo y la definición de la contraseña del usuario administrador (root).

La utilización de parámetros predeterminados permitió garantizar una instalación estable y compatible con la arquitectura propuesta, evitando configuraciones manuales que pudieran comprometer el correcto funcionamiento del sistema en etapas posteriores. Asimismo, la asignación completa del disco virtual aseguró la disponibilidad de espacio suficiente para la operación del firewall, el almacenamiento de registros y la ejecución de servicios asociados.

Una vez finalizado el proceso de instalación, se procedió al reinicio de la máquina virtual y a la eliminación de la imagen ISO previamente montada como medio de instalación. Esta acción permitió que el sistema iniciara correctamente desde el disco duro virtual, asegurando la carga normal del sistema operativo ya instalado.

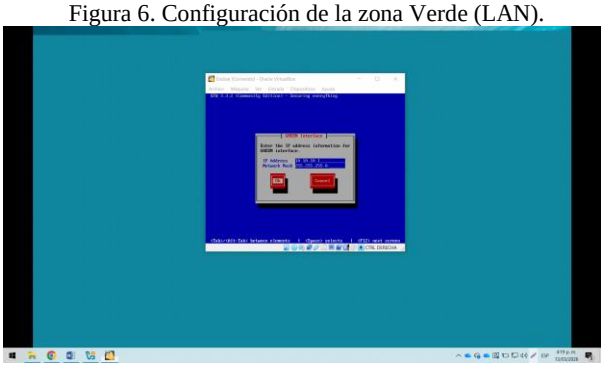
Figura 5. Instalación ISO Endian.

Fuente: Autoría Propia

La Figura 5 ilustra el proceso de instalación del sistema operativo, evidenciando las etapas ejecutadas durante la configuración inicial del firewall. Este proceso constituye un paso fundamental dentro de la implementación, ya que establece la base sobre la cual se configuran posteriormente las interfaces de red, las políticas de seguridad y los servicios del sistema.

La Figura 6 presenta la configuración correspondiente a la zona Verde (LAN) dentro del sistema Endian Firewall Community, en la cual se define la interfaz asociada a la red interna y se asigna la dirección IP correspondiente al segmento local.

Figura 6. Configuración de la zona Verde (LAN).



Fuente: Autoría Propia

Una vez finalizada la instalación y configuración inicial del sistema Endian Firewall Community, se procedió a verificar el estado y la configuración de las interfaces de red mediante herramientas de diagnóstico del sistema operativo. Esta verificación tuvo como propósito confirmar la correcta asignación de direcciones IP en cada una de las zonas configuradas, así como validar el estado operativo de las interfaces.

Para ello, se empleó el siguiente comando: ip addr show, este comando permitió identificar las interfaces disponibles, sus direcciones IP asociadas y su estado, facilitando la comprobación de la configuración de red establecida.

Posteriormente, se realizaron pruebas de conectividad hacia un host externo mediante el envío de paquetes utilizando el protocolo Internet Control Message Protocol (ICMP). Estas pruebas tuvieron como finalidad validar la conectividad hacia Internet a través de la zona WAN, así como comprobar el correcto funcionamiento del enrutamiento y del mecanismo de traducción de direcciones de red (NAT).

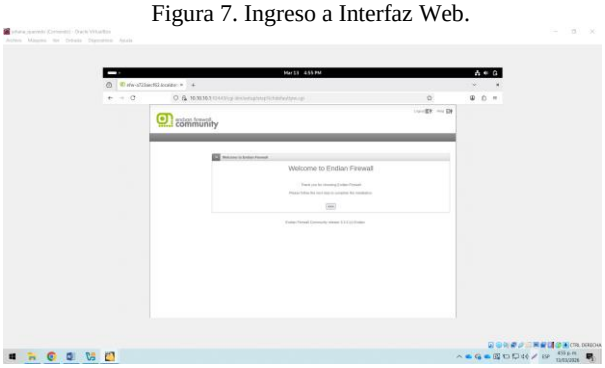
Para esta validación se utilizó el siguiente comando: ping -c 4 8.8.8.8.

Los resultados obtenidos evidenciaron respuestas satisfactorias por parte del servidor externo, lo cual confirma que el sistema permite la salida de tráfico desde la red interna hacia la WAN mediante el proceso de NAT, garantizando la comunicación externa sin exponer las direcciones IP privadas.

Finalmente, se accedió a la interfaz web de administración del sistema Endian Firewall Community a través de un navegador web, utilizando la dirección segura: https://10.10.10.1:10443

La Figura 7 muestra el acceso exitoso a esta interfaz permitió verificar que el servicio de gestión del firewall se encuentra operativo y disponible para la configuración de reglas de acceso, políticas de seguridad y monitoreo del tráfico, constituyendo un componente fundamental para la administración centralizada del sistema.

Figura 7. Ingreso a Interfaz Web.



Fuente: Autoría Propia

5. CONFIGURACIÓN NAT

Una vez configurada la instancia de Endian Firewall Community en Oracle VM VirtualBox y establecida la segmentación de la red en las zonas LAN, DMZ y WAN, se implementaron mecanismos de traducción de direcciones de red (Network Address Translation, NAT).

Este mecanismo permite que las redes internas, con direccionamiento IP privado, accedan a redes externas sin exponer su estructura interna, contribuyendo a la seguridad del sistema. En este contexto, Endian Firewall actúa como punto central de interconexión entre las zonas, gestionando el tráfico de red.

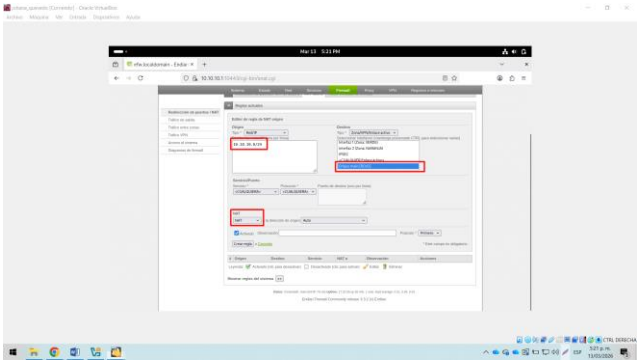
Para ello, se configuraron reglas de traducción de direcciones de origen (Source NAT, SNAT), las cuales permiten la salida controlada del tráfico hacia Internet, garantizando la conectividad y preservando la confidencialidad del direccionamiento interno.

Para la red LAN (10.10.10.0/24), se configuró una regla de traducción de direcciones de origen (Source NAT, SNAT) en Endian Firewall Community, asociada a la interfaz ROJA

(WAN), con el fin de permitir la salida del tráfico desde la zona VERDE (LAN) hacia la red externa.

Este mecanismo posibilita que los dispositivos con direcciones IP privadas accedan a Internet utilizando una dirección pública, evitando la exposición directa del direccionamiento interno y fortaleciendo la seguridad perimetral.

Figura 8. Configuración de la regla NAT para la red LAN.



Fuente: Autoría Propia

La Figura 8 muestra la configuración de la regla NAT dentro de la interfaz de administración, evidenciando la asociación del segmento interno con la interfaz de salida hacia la WAN.

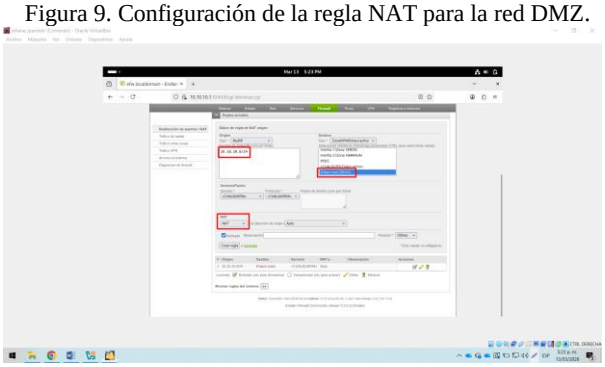
La correcta implementación de esta regla fue validada mediante pruebas de conectividad desde un equipo en la red LAN, confirmando el funcionamiento adecuado del proceso de traducción de direcciones y el acceso controlado a recursos externos.

De manera similar, se implementó una regla de traducción de direcciones de origen (Source NAT, SNAT) para la red DMZ (10.10.20.0/24) en Endian Firewall Community, asociada a la interfaz ROJA (WAN), con el fin de permitir la salida controlada del tráfico hacia la red externa.

Esta configuración es especialmente relevante, ya que la zona DMZ aloja servicios que requieren conectividad externa, como actualizaciones o acceso a recursos remotos, sin comprometer la seguridad de la red interna.

Adicionalmente, fue necesario habilitar explícitamente el tráfico desde la zona NARANJA (DMZ) hacia la zona ROJA, debido a las políticas restrictivas predeterminadas del firewall. Esto garantiza que únicamente el tráfico autorizado pueda salir hacia la WAN, manteniendo el principio de segmentación de red.

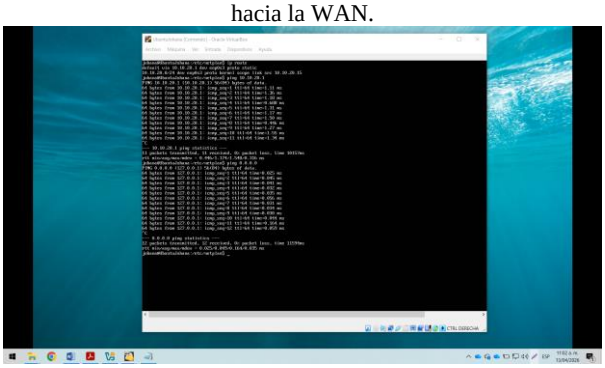
Figura 9. Configuración de la regla NAT para la red DMZ.



Fuente: Autoría Propia

La validación del funcionamiento de los mecanismos de traducción de direcciones de red (NAT) se realizó mediante pruebas de conectividad desde las zonas LAN y DMZ hacia la red WAN. Los resultados confirmaron que ambos segmentos pueden establecer comunicación externa a través del firewall, garantizando el ocultamiento del direccionamiento interno y el control del tráfico saliente.

Figura10. Verificación de conectividad y ruteo desde la DMZ hacia la WAN.



Fuente: Autoría Propia

La Figura 10 presenta los resultados de las pruebas de conectividad y ruteo desde la zona DMZ, evidenciando la correcta salida del tráfico hacia la red externa a través del firewall perimetral.

El comportamiento observado confirma que una adecuada configuración de NAT, en conjunto con las reglas de tráfico entre zonas, permite una comunicación segura y controlada hacia Internet, sin afectar la segmentación de la red ni exponer los servicios internos.

Las reglas de Source NAT (SNAT) implementadas garantizaron el funcionamiento correcto del proceso de traducción de direcciones, permitiendo el flujo de tráfico desde las redes internas hacia la WAN de manera segura. Con base en estos resultados, se procedió a la habilitación de servicios en la zona DMZ bajo criterios de seguridad perimetral.

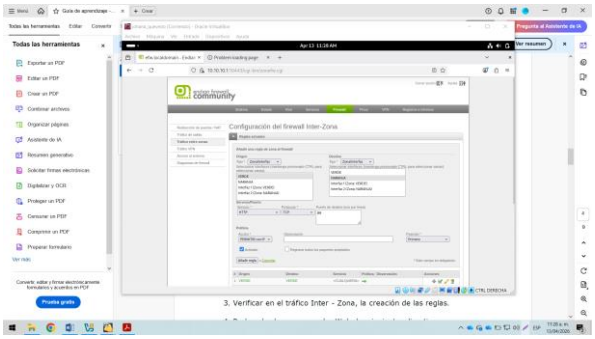
Esta etapa tuvo como objetivo permitir el acceso a servicios específicos desde otras zonas de la red, manteniendo los principios de segmentación, mínima exposición y control del tráfico, propios de una arquitectura de seguridad perimetral.

6. REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Con el propósito de habilitar el acceso controlado a los servicios ubicados en la zona DMZ, se implementaron 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 de archivos entre la red LAN y la DMZ [4].

Para reforzar la seguridad del servidor, se aplicaron reglas de filtrado locales mediante Uncomplicated Firewall (UFW), permitiendo únicamente los puertos necesarios (80 para HTTP y 21 para FTP). Esta configuración se integra dentro de un enfoque de defensa en profundidad, complementando las políticas establecidas en el firewall perimetral.

Figura 11. Aplicación de reglas UFW y acceso al servicio FTP en el servidor de la DMZ.



Fuente: Autoría Propia

En la Figura 11 se presenta la configuración de las reglas UFW aplicadas en el servidor, donde se habilitan exclusivamente los puertos correspondientes a los servicios implementados. De esta manera, se garantiza que únicamente el tráfico autorizado sea aceptado, mientras que el resto de las conexiones son bloqueadas.

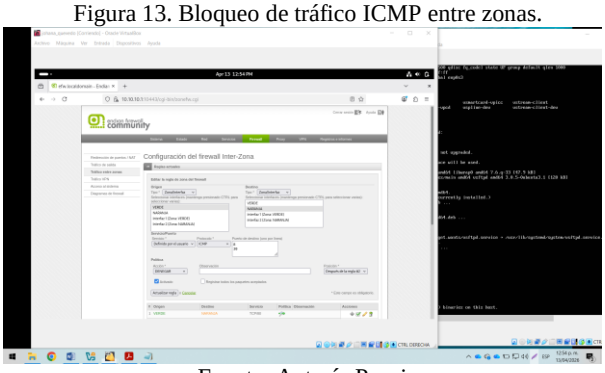
Como parte del proceso de validación, se realizó una prueba de acceso al servicio FTP mediante una conexión autenticada desde un equipo cliente ubicado en la red LAN. Los resultados obtenidos evidenciaron el establecimiento exitoso de la conexión, confirmando la correcta operación del servicio bajo las políticas de seguridad definidas.

Figura 12. Validación del acceso al servicio FTP desde la red LAN hacia la DMZ.

Fuente: Autoría Propia

Con el objetivo de fortalecer la seguridad del sistema, se implementaron reglas en el firewall perimetral Endian Firewall Community para denegar el tráfico ICMP desde la zona VERDE (LAN) hacia la zona NARANJA (DMZ). Esta restricción reduce la superficie de ataque de los servidores ubicados en la DMZ, evitando actividades de reconocimiento y exploración de red desde otros segmentos internos.

Figura 13. Bloqueo de tráfico ICMP entre zonas.

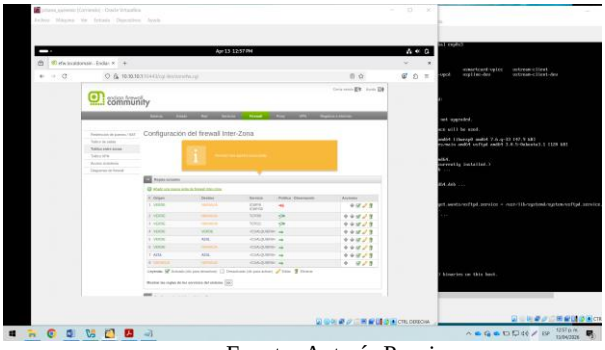


Fuente: Autoría Propia

En la Figura 13 se presenta la configuración de la regla de denegación aplicada al protocolo ICMP, donde se establece de forma explícita la política de bloqueo entre las zonas mencionadas.

Para garantizar la correcta aplicación de esta política, se verificó que la regla estuviera ubicada en la primera posición dentro del conjunto de reglas del firewall, asegurando su ejecución prioritaria frente a otras configuraciones que pudieran permitir el tráfico.

Figura 14. Prioridad de la regla de bloqueo ICMP en el firewall.

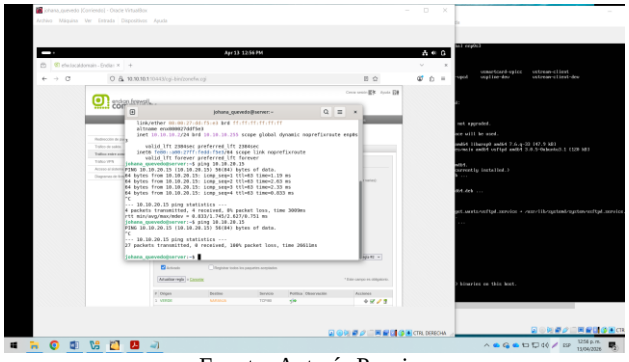


Fuente: Autoría Propia

Tal como se observa en la Figura 14, la regla se encuentra correctamente posicionada dentro de la configuración interzona, lo que garantiza su aplicación antes de cualquier otra política de tráfico.

Como parte del proceso de validación, se realizaron pruebas de conectividad desde un equipo cliente en la red LAN, evaluando el comportamiento del firewall ante solicitudes ICMP dirigidas hacia la DMZ.

Figura 15. Prueba de conectividad ICMP desde LAN hacia la DMZ.



Fuente: Autoría Propia

Los resultados obtenidos evidenciaron la ausencia de respuesta a dichas solicitudes, confirmando el correcto funcionamiento de la regla de bloqueo implementada.

En conjunto, la aplicación de estas políticas permitió validar la efectividad de los mecanismos de control perimetral y local, sentando las bases para la definición de reglas de acceso más específicas entre las zonas LAN, DMZ y WAN, con el fin de gestionar de manera granular el tráfico autorizado y reforzar la seguridad de la infraestructura.

Para verificar la correcta aplicación de las reglas de acceso entre las zonas LAN, DMZ y WAN, se realizaron pruebas controladas de comunicación utilizando herramientas de diagnóstico como curl, registros del firewall Endian y mecanismos de monitoreo de tráfico en tiempo real.

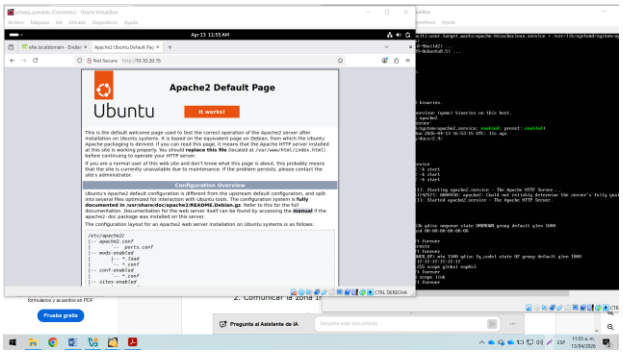
A partir de estas pruebas, fue posible confirmar que las reglas implementadas cumplen con los objetivos de seguridad establecidos, permitiendo únicamente el tráfico explícitamente autorizado y bloqueando cualquier intento de comunicación no definido previamente.

Con el fin de validar la regla que permite el acceso desde la red LAN hacia los servicios ubicados en la DMZ, se realizó una solicitud HTTP [3] desde una máquina cliente mediante el comando curl hacia la dirección del servidor.

Como resultado, el servidor web ubicado en la DMZ respondió con la página por defecto de Apache, lo cual permitió confirmar que el firewall autorizó correctamente el tráfico HTTP (puerto 80). Asimismo, se evidenció que la solicitud fue procesada sin restricciones en la DMZ y que no existían bloqueos por parte del firewall local (UFW) del servidor.

Adicionalmente, se verificó el correcto enrutamiento del tráfico entre las interfaces del firewall, garantizando la comunicación entre las zonas involucradas.

Figura 16. Acceso al servicio HTTP desde la red LAN hacia la zona DMZ.



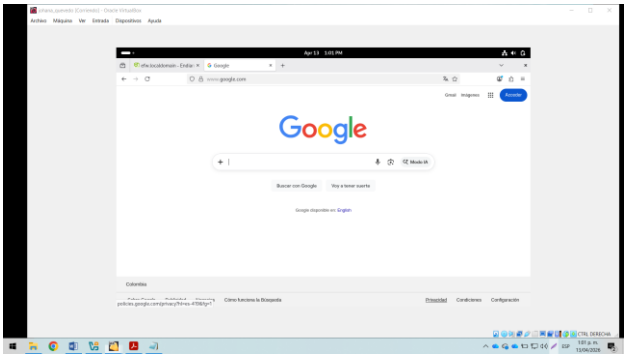
Fuente: Autoría Propia

En la Figura 16 se evidencia que la zona DMZ es accesible 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 un acceso controlado a los servicios, reforzando la seguridad mediante el aislamiento y el control del tráfico interzona.

Con el propósito de validar el tráfico de salida hacia Internet, se realizaron solicitudes HTTP [3] desde las zonas LAN y DMZ hacia un servidor web público externo.

Los resultados obtenidos evidenciaron que las solicitudes fueron enviadas correctamente hacia la WAN y que el firewall Endian permitió las conexiones salientes conforme a las reglas definidas para el tráfico LAN → WAN y DMZ → WAN. Asimismo, se recibieron respuestas HTTP válidas, confirmando la existencia de conectividad funcional hacia Internet sin bloqueos imprevistos.

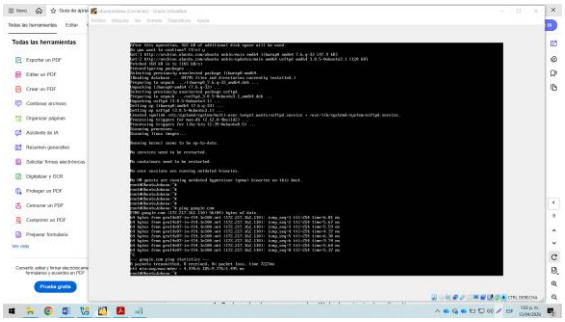
Figura 17. Acceso a google.com desde la red LAN hacia la WAN.



Fuente: Autoría Propia

En la Figura 17 se observa el acceso exitoso a google.com desde la red LAN, lo cual confirma que el firewall realiza correctamente la traducción de direcciones (NAT) para el tráfico originado en la red interna. Este comportamiento evidencia que las reglas de salida permiten la comunicación externa sin exponer el direccionamiento IP privado.

Figura 18. Acceso a google.com desde la red DMZ hacia la WAN.



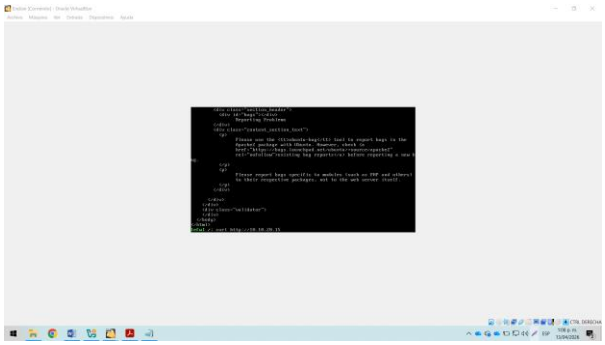
Fuente: Autoría Propia

Por su parte, la Figura 18 presenta la validación de conectividad desde la zona DMZ hacia la WAN, evidenciando que la traducción de direcciones (NAT) también se aplica correctamente en este segmento. Este resultado confirma que el tráfico generado desde la DMZ puede acceder a la red externa de manera controlada, manteniendo la segmentación de la red y las políticas de seguridad definidas en el firewall perimetral.

Con el objetivo de validar el tráfico entrante desde la red externa, se simuló una solicitud HTTP desde la interfaz WAN del firewall Endian hacia el servidor ubicado en la zona DMZ. Como resultado, el servidor respondió de manera exitosa, lo que permitió confirmar la correcta configuración de las reglas de acceso definidas.

Este comportamiento evidencia que la DMZ se encuentra expuesta de forma controlada hacia la WAN, permitiendo únicamente el tráfico HTTP autorizado. Asimismo, se verificó que no existe exposición de puertos adicionales y que el firewall actúa efectivamente como primera línea de defensa frente a accesos externos.

Figura 19. Acceso al servicio HTTP desde la WAN hacia la zona DMZ

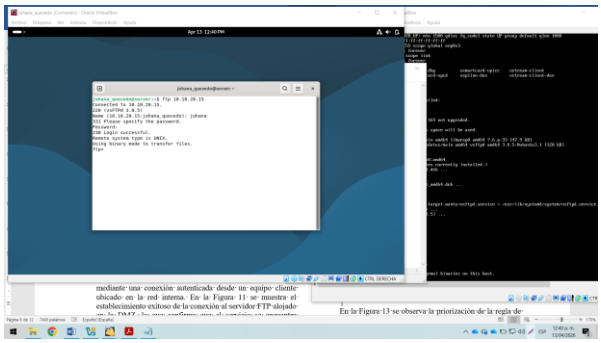


Fuente: Autoría Propia

En la Figura 19 se observa el acceso al servicio HTTP desde la zona WAN hacia la DMZ, validando el principio de publicación segura de servicios en una arquitectura de seguridad perimetral. Este resultado 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.

Los resultados evidenciaron que el puerto 21 se encontraba correctamente habilitado tanto en el firewall Endian como en el firewall local UFW. Asimismo, el servidor respondió adecuadamente solicitando credenciales de autenticación, y las transferencias de archivos se realizaron sin interrupciones. También se verificó el correcto funcionamiento de los modos activo y pasivo del protocolo, así como el cumplimiento de los permisos y propietarios definidos en las carpetas del servidor.

Figura 20. Acceso al servicio FTP desde la LAN hacia la zona DMZ



Fuente: Autoría Propia

En la Figura 20 se observa el acceso exitoso al servicio FTP desde la red LAN, lo que permitió validar tanto la correcta operación del servicio como la aplicación de las reglas de acceso configuradas. Este resultado confirma que el acceso se realiza de manera segura y controlada, considerando las características propias del protocolo FTP, el cual utiliza canales separados para el control y la transferencia de datos, requiriendo configuraciones específicas para su correcto funcionamiento [4].

Como parte del proceso de validación final, se realizó una inspección del módulo Inter-Zone Traffic del firewall Endian, lo que permitió observar en tiempo real los registros generados por solicitudes HTTP y FTP, así como la correspondencia entre las reglas definidas y el tráfico permitido.

Durante este análisis, se verificó la ausencia de paquetes bloqueados que pudieran afectar la operación, junto con información detallada sobre direcciones IP de origen y destino, protocolos y puertos utilizados. Los resultados evidenciaron un flujo de tráfico coherente con el modelo de segmentación implementado entre las zonas LAN, DMZ y WAN.

A partir de esta validación, se confirmó que la política de seguridad aplicada no solo opera correctamente, sino que también se encuentra alineada con los principios de seguridad perimetral, reforzando la arquitectura basada en zonas.

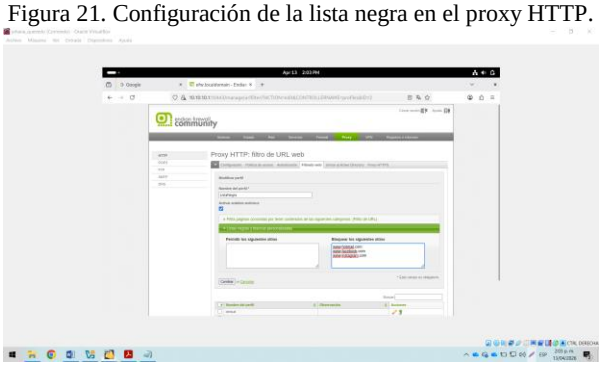
En consecuencia, se determinó que el firewall actúa de manera efectiva como mecanismo de control de acceso, garantizando que la comunicación entre las zonas se realice únicamente bajo las políticas previamente definidas.

7. IMPLEMENTACIÓN DEL PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

Como complemento a las configuraciones de seguridad implementadas, se habilitó un proxy HTTP no transparente

mediante el módulo correspondiente del firewall Endian. Inicialmente, el servicio se activó en la zona VERDE, configurando el puerto 8080 como canal de comunicación. Posteriormente, se definió un perfil de filtrado denominado ListaNegra, en el cual se incluyeron los sitios www.hotmail.com, www.facebook.com y www.instagram.com, con el objetivo de restringir el acceso a estos portales desde la red LAN.

Figura 21. Configuración de la lista negra en el proxy HTTP.



Fuente: Autoría Propia

En la Figura 21 se presenta la configuración de la lista negra dentro del módulo de proxy HTTP, permitiendo establecer restricciones centralizadas sobre el contenido accesible y garantizando la aplicación uniforme de políticas de filtrado.

Con el fin de reforzar el control de acceso, se habilitó el método de autenticación local (NCSA) y se creó el usuario johana, el cual fue asignado a un grupo específico para la aplicación de políticas personalizadas. A partir de esta configuración, se estableció una política que asocia el perfil de filtrado con la autenticación de grupo.

Figura 22. Asociación del perfil de filtrado con autenticación de grupo.

Fuente: Autoría Propia

Tal como se observa en la Figura 22, esta configuración permite aplicar restricciones de navegación de manera individualizada, asegurando que el uso del proxy esté condicionado a la autenticación previa del usuario.

Para validar el funcionamiento del proxy, se configuró manualmente en un equipo de la zona VERDE la dirección IP 10.10.10.1 y el puerto 8080 en el navegador. Durante las pruebas, el sistema solicitó credenciales de acceso y, tras la autenticación, permitió la navegación hacia sitios permitidos, mientras que los dominios incluidos en la lista negra fueron bloqueados correctamente.

Figura 23. Bloqueo de sitios web mediante el proxy HTTP.

Fuente: Autoría Propia

En la Figura 23 se evidencia el comportamiento del proxy durante las pruebas de navegación, donde los sitios restringidos muestran la página de denegación de acceso. 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.

En conjunto, la implementación del proxy HTTP complementa el esquema de seguridad perimetral desarrollado, integrando mecanismos de segmentación de red, control de tráfico, publicación segura de servicios y filtrado de acceso. A partir de esta infraestructura, se procede a la evaluación de resultados con el fin de analizar el comportamiento y la efectividad de las políticas de seguridad configuradas.

8. RESULTADOS

En esta sección se presentan los resultados obtenidos a partir de la implementación del esquema de seguridad perimetral propuesto. Estos se organizan conforme a las configuraciones realizadas, con el fin de 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 de cada componente del sistema, sirviendo como base para su posterior análisis e interpretación.

En primera instancia, la configuración de Endian Firewall Community en el entorno virtualizado mediante Oracle VM VirtualBox proporcionó una base estable para la implementación del esquema de seguridad. La asignación adecuada de recursos y la configuración de múltiples interfaces de red permitieron el funcionamiento correcto del firewall, así como la segmentación lógica de la red. Asimismo, la activación de las zonas VERDE, NARANJA y ROJA facilitó la aplicación de políticas diferenciadas, garantizando la separación entre la red interna, la DMZ y la red externa.

En relación con la conectividad, se comprobó que la implementación de NAT permitió la salida controlada del tráfico desde las zonas internas hacia la WAN sin exponer el direccionamiento privado. Las pruebas realizadas desde las redes LAN y DMZ evidenciaron que el firewall aplicó

correctamente la traducción de direcciones de origen, permitiendo el acceso a servicios externos y la recepción de respuestas válidas. Este resultado confirma el cumplimiento del principio de ocultamiento del direccionamiento interno y la correcta integración de NAT dentro del esquema de seguridad.

Respecto a los servicios desplegados en la DMZ, se verificó que los servicios HTTP y FTP se encuentran operativos y accesibles únicamente desde las zonas autorizadas. El servicio HTTP permitió la publicación controlada de contenido, mientras que el servicio FTP facilitó la transferencia de archivos de forma autenticada. Adicionalmente, la aplicación de reglas de filtrado locales mediante UFW restringió el acceso a los puertos necesarios, reduciendo la superficie de ataque y validando el principio de mínima exposición.

En cuanto a las políticas de acceso entre zonas, se evidenció que las reglas configuradas fueron aplicadas de manera coherente. En particular, el tráfico ICMP desde la red LAN hacia la DMZ fue bloqueado correctamente, impidiendo actividades de reconocimiento. Este comportamiento demuestra que el firewall gestionó adecuadamente el tráfico interzona, y que la priorización de reglas garantizó la ejecución efectiva de las políticas de denegación sobre las permisivas.

Finalmente, las pruebas de navegación confirmaron el correcto funcionamiento del proxy HTTP no transparente. Se evidenció que el sistema requiere autenticación previa para permitir el acceso a recursos web, y que los sitios incluidos en la lista negra fueron bloqueados de manera efectiva. Este resultado valida la integración entre autenticación, filtrado de contenido y control de acceso, consolidando un mecanismo adicional de seguridad dentro de la infraestructura implementada.

9. DISCUSIÓN

El análisis de los resultados obtenidos a partir de la implementación del esquema de seguridad perimetral permite evaluar el impacto de las configuraciones realizadas sobre la seguridad de la infraestructura. Este análisis se organiza en función de los componentes implementados, con el fin de examinar su coherencia con los principios teóricos de la seguridad perimetral y su contribución al cumplimiento de los objetivos planteados.

En primer lugar, la configuración de las zonas de red en el entorno virtualizado mediante Oracle VM VirtualBox y Endian Firewall Community evidenció que la segmentación de la red y la asignación estática de direcciones constituyen elementos fundamentales para garantizar un entorno estable y controlado. La virtualización permitió emular una infraestructura real, facilitando la implementación de servicios como NAT, LAN y DMZ sin afectar entornos productivos, lo cual resulta especialmente relevante en contextos académicos.

En relación con la conectividad, la implementación de NAT desempeñó un papel clave en la interconexión entre redes internas y externas. Este mecanismo no solo permitió el acceso a la WAN, sino que también reforzó el principio de ocultamiento del direccionamiento interno, reduciendo la exposición de la infraestructura. Las reglas SNAT aplicadas a la LAN y la DMZ evidenciaron un control diferenciado del tráfico, en concordancia con las recomendaciones del RFC 3022 [6], validando la capacidad del firewall para abstraer la topología interna y gestionar adecuadamente el tráfico saliente.

Por otra parte, la habilitación controlada de servicios HTTP y FTP en la zona DMZ demostró la viabilidad de exponer servicios hacia redes externas sin comprometer la seguridad de la red interna. La combinación de segmentación, reglas de acceso y filtrado local permitió restringir el tráfico a los puertos estrictamente necesarios, alineándose con el principio de defensa en profundidad. Esto confirma que la seguridad perimetral no depende únicamente de la segmentación, sino también de la correcta implementación de mecanismos de control de acceso.

En cuanto a las políticas de filtrado entre zonas, se evidenció que las reglas implementadas permiten un control granular del tráfico. El bloqueo del protocolo ICMP desde la LAN hacia la DMZ demostró la capacidad del firewall para mitigar actividades de reconocimiento de red. De acuerdo con el RFC 792 [5], este protocolo puede ser utilizado tanto para diagnóstico como para exploración, por lo que su restricción en entornos segmentados constituye una práctica recomendada.

Finalmente, la implementación del proxy HTTP no transparente con autenticación local evidenció un control efectivo sobre el acceso a recursos web desde la red LAN. La autenticación previa permitió identificar a los usuarios, mientras que el uso de listas negras reforzó el filtrado de contenido. Esta combinación de mecanismos demuestra que es posible aplicar políticas de uso de Internet de manera centralizada, consolidando al firewall como una herramienta integral para la gestión de seguridad en entornos segmentados [1].

10. CONCLUSIONES

La implementación de Endian Firewall Community en un entorno virtualizado permitió establecer una infraestructura estable y controlada para el desarrollo del esquema de seguridad perimetral. La adecuada definición de las zonas VERDE, NARANJA y ROJA, junto con un esquema de direccionamiento IP estático, facilitó la segmentación funcional de la red y la aplicación progresiva de políticas de seguridad.

La configuración de reglas de Network Address Translation (NAT) en las redes LAN y DMZ permitió evidenciar un manejo adecuado de la traducción de direcciones y del 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 fortaleciendo la seguridad de la arquitectura perimetral.

La habilitación de servicios HTTP y FTP en la zona DMZ demostró que es posible exponer recursos hacia otras zonas de la red sin comprometer la seguridad de la infraestructura interna. La combinación de segmentación de red y reglas de filtrado específicas permitió garantizar la disponibilidad de los servicios, restringiendo el acceso únicamente a los protocolos autorizados y reduciendo la superficie de ataque.

El análisis de las reglas de acceso interzona evidenció la importancia de aplicar políticas estrictas de control del tráfico.

En particular, el bloqueo del protocolo ICMP y la correcta priorización de las reglas contribuyeron a mitigar actividades de reconocimiento, fortaleciendo la postura de seguridad del firewall perimetral.

La implementación del proxy HTTP no transparente con autenticación permitió validar un control efectivo de la navegación web basado en usuarios y políticas. El uso de perfiles de filtrado y listas de bloqueo facilitó la restricción de contenidos específicos, evidenciando que este mecanismo complementa las funciones del firewall al proporcionar control y trazabilidad del tráfico generado desde la red LAN.

En conjunto, los resultados obtenidos permiten concluir que un esquema de seguridad perimetral basado en segmentación de red, traducción de direcciones, control de servicios y filtrado de tráfico constituye una solución efectiva para la protección de infraestructuras en entornos GNU/Linux. La implementación realizada demuestra que Endian Firewall proporciona las herramientas necesarias para aplicar políticas de seguridad coherentes, garantizando el control de acceso, la protección de servicios y la gestión segura del tráfico en redes segmentadas.

11. REFERENCIAS

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

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

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

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

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

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

[7] NIST, "Guide to Firewalls and Firewall Policy (SP 800-41 Rev. 1)," National Institute of Standards and Technology, 2009. https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

[8] Cisco Systems, Firewall Fundamentals – Security Zones and Policy Enforcement. https://www.cisco.com/