Implementación de un Entorno Seguro de Red utilizando Endian Firewall Community en VirtualBox

Brandon Mauricio Ramirez Cortes
bmramirezco@unadvirtual.edu.co
Jeyson Andres Sanchez Correa
jasanchezcorr@unadvirtual.edu.co
Leidy Johanna Amezquita Chiguasuque
ljamezquitac@unadvirtual.edu.co
Luisa Fernanda Anacona Taque
lfanaconat@unadvirtual.edu.co
Yeison Mayken Martinez Cuenca
ymmartinezcu@unadvirtual.edu.co

RESUMEN: *En este trabajo se implementó un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall Community (EFW) en VirtualBox. La infraestructura fue segmentada en tres zonas: GREEN para la red LAN, RED para la conexión WAN y ORANGE para la DMZ. Se realizó la instalación y configuración de Endian, incluyendo la asignación de interfaces de red, reglas NAT para permitir la comunicación hacia Internet y políticas de firewall para controlar el tráfico entre zonas. Además, se habilitaron servicios en la DMZ y se implementó un Proxy HTTP no transparente con autenticación para gestionar la navegación web. La validación se efectuó mediante pruebas de conectividad y comandos de administración en GNU/Linux. Los resultados demostraron el correcto funcionamiento de la segmentación de red y de los mecanismos de control implementados, evidenciando la importancia de la seguridad perimetral y del uso de firewalls para proteger infraestructuras de red en entornos GNU/Linux.*

PALABRAS CLAVE: Endian Firewall Community, DMZ, Firewall, GNU/Linux, NAT, Proxy HTTP, Seguridad Perimetral, VirtualBox.

ABSTRACT: *In this work, a perimeter security environment was implemented using GNU/Linux Endian Firewall Community (EFW) within VirtualBox. The infrastructure was segmented into three zones: green for the LAN network, red for the WAN connection, and orange for the DMZ. The installation and configuration of Endian were carried out, including the assignment of network interfaces, NAT rules to allow internet communication, and firewall policies to control traffic between zones. Additionally, services were enabled in the DMZ, and a non-transparent HTTP Proxy with authentication was implemented to manage web browsing. Validation was performed through connectivity tests and administration commands in GNU/Linux. The results demonstrated the correct functioning of the network segmentation and the implemented control mechanisms, highlighting the importance of perimeter security and the use of firewalls to protect network infrastructures in GNU/Linux environments.*

KEYWORDS: Endian Firewall Community, DMZ, Firewall, GNU/Linux, NAT, HTTP Proxy, Perimeter Security, VirtualBox.

1 INTRODUCCIÓN

En la actualidad, la seguridad informática representa un desafío fundamental para las organizaciones que administran infraestructuras basadas en GNU/Linux, debido al incremento constante de amenazas y vulnerabilidades en los entornos de red. Frente a este panorama, la implementación de estrategias de defensa en profundidad se convierte en un elemento esencial para garantizar la protección de los servicios, la integridad de la información y la continuidad operativa. Dentro de estas estrategias, la seguridad perimetral y la segmentación de redes desempeñan un papel clave al permitir el aislamiento de recursos y el control detallado del tráfico entre diferentes niveles de confianza.

El presente artículo expone el diseño e implementación de una arquitectura de seguridad utilizando Endian Firewall Community Edition, basada en un modelo estructurado en cinco componentes principales. En primer lugar, se describe la instalación y configuración inicial del firewall mediante una topología segmentada por zonas de seguridad (GREEN, ORANGE y RED), las cuales permiten diferenciar la red interna, los servicios públicos y la conexión externa a Internet. Posteriormente, se aborda la administración del sistema GNU/Linux y la gestión eficiente de las interfaces y recursos de red, garantizando el correcto funcionamiento y la estabilidad del entorno.

Como tercer eje, se desarrolla la configuración de una Zona Desmilitarizada (DMZ), destinada a alojar servicios públicos de manera aislada para minimizar riesgos de acceso no autorizado hacia la red interna. Seguidamente, se profundiza en la implementación de políticas de firewall y mecanismos de control de acceso, estableciendo reglas específicas para permitir protocolos como HTTP y FTP, mientras se restringe el tráfico ICMP con el propósito de fortalecer la seguridad entre los distintos segmentos de la red.

Finalmente, se analiza la implementación de un proxy HTTP no transparente con autenticación, herramienta fundamental para el monitoreo, filtrado y control de la navegación web de los usuarios. A través de este enfoque integral, se evidencia cómo la integración de técnicas de segmentación, filtrado y control de tráfico permite construir una

infraestructura de red robusta, resiliente y alineada con los principios de seguridad basados en software de código abierto.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall Community (EFW) en una plataforma virtualizada mediante VirtualBox, con el fin de aplicar principios de seguridad informática, segmentación de redes y administración de servicios en un entorno práctico y funcional.

2.2 OBJETIVOS ESPECÍFICOS

- Configurar las interfaces de red e instalar Endian Firewall para establecer la zona verde (LAN), roja (WAN) y naranja (DMZ).
- Implementar reglas NAT para habilitar la comunicación hacia Internet y configurar los servicios en la zona DMZ para su acceso controlado desde la red.
- Desarrollar reglas de acceso para permitir o denegar el tráfico según las políticas definidas, con el fin de fortalecer el control de seguridad sobre las comunicaciones.
- Implementar un servidor Proxy HTTP no transparente con autenticación que permita gestionar y controlar la navegación de los usuarios en Internet.

3 PREPARACIÓN DEL ENTORNO

3.1 INSTALACIÓN Y CONFIGURACIÓN MÁQUINAS VIRTUALES

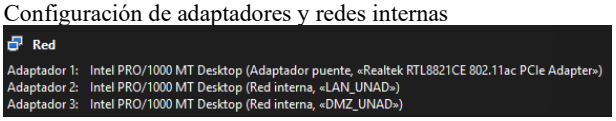
Se procedió con la creación y configuración de tres máquinas virtuales independientes en el hipervisor Oracle VM VirtualBox, asegurando un entorno técnico controlado para cada función específica: el nodo de administración Ubuntu Desktop, el servidor de servicios Debian Server DMZ y la unidad de control perimetral Endian Firewall. Como se evidencia en la Fig. 1, a cada máquina se le asignaron recursos de hardware proporcionales a su carga de trabajo, tales como memoria RAM y procesadores, para garantizar la estabilidad operativa de los sistemas operativos antes de su despliegue en la red.

Figura 1.
Listado de máquinas virtuales configuradas

Fuente: Autoría Propia

Se establecieron los parámetros de conectividad para el Endian Firewall mediante la habilitación de tres adaptadores de red, como se detalla en la Fig. 2, permitiendo la comunicación entre las distintas zonas. El primer adaptador se vinculó en modo Puente para obtener salida a redes externas, mientras que los adaptadores restantes se asociaron a redes internas personalizadas, denominadas «LAN_UNAD» y «DMZ_UNAD», con el fin de garantizar el aislamiento de tráfico requerido para la administración y los servicios del servidor.

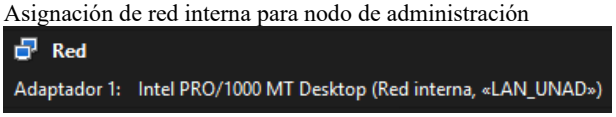
Figura 2.
Configuración de adaptadores y redes internas



Fuente: Autoría Propia

Se realizó la vinculación del adaptador de red para el nodo cliente, asociando de manera exclusiva a la red interna denominada «LAN_UNAD». Como se observa en la Fig. 3, esta configuración permite que la máquina virtual se integre al segmento de administración controlado por el firewall, garantizando que el tráfico generado permanezca dentro del entorno privado.

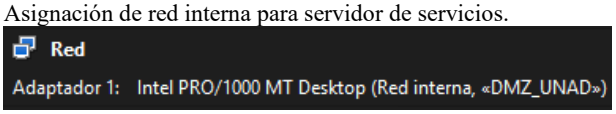
Figura 3.
Asignación de red interna para nodo de administración



Fuente: Autoría Propia

Se configuró el adaptador de red del servidor Debian Server DMZ, direccionando hacia la red interna «DMZ_UNAD». Como se ilustra en la Fig. 4, esta asignación es fundamental para la segmentación lógica, ya que sitúa al servidor en una zona aislada del segmento de administración, permitiendo la implementación de políticas de seguridad restrictivas para los servicios que serán expuestos.

Figura 4.
Asignación de red interna para servidor de servicios.



Fuente: Autoría Propia

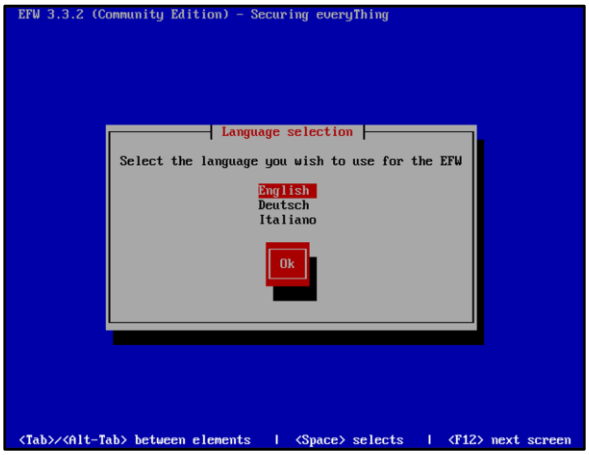
La arquitectura de red se fundamenta en la interconexión de las tres máquinas virtuales a través del Endian Firewall, el cual actúa como el nodo central de enrutamiento y seguridad. Como se ha detallado en las figuras anteriores, la conectividad se establece vinculando el nodo de administración a la red interna «LAN_UNAD» y el servidor a la red «DMZ_UNAD», permitiendo que el firewall gestione el flujo de datos entre ambos segmentos de forma aislada. Esta estructura asegura que la comunicación entre el administrador y el servidor de servicios siempre sea supervisada por las reglas de filtrado definidas en el firewall perimetral.

4 DESARROLLO DE TEMÁTICAS

4.1 TEMÁTICA 1: SEGMENTACIÓN LÓGICA Y DIRECCIONAMIENTO IP POR ZONAS DE RED

Para iniciar con el despliegue del software de seguridad, se procedió con la ejecución del instalador de Endian Firewall Community Edition, como se muestra en la Fig. 5. En esta fase inicial, se seleccionó el idioma de interfaz y se preparó el entorno para la configuración de los parámetros del núcleo de red, asegurando que la distribución esté lista para reconocer los adaptadores previamente asignados en el hipervisor.

Figura 5.
Selección de idioma en el instalador de Endian Firewall



Fuente: Autoría Propia

Continuando con el despliegue, el instalador solicita la confirmación para la preparación del disco duro virtual en la ruta /dev/sda, como se observa en la Fig. 6. En este paso, se autoriza el particionamiento y la creación del sistema de archivos necesario para alojar el sistema operativo, garantizando que el almacenamiento esté optimizado para las funciones de registro y control de tráfico del firewall.

Figura 6.
Confirmación de particionamiento y formato de disco duro

Fuente: Autoría Propia

Posteriormente, el asistente de instalación consulta sobre la activación de la consola a través de puerto serial, como se aprecia en la Fig. 7. Para los fines de este laboratorio virtual, se selecciona la opción negativa, ya que la administración se realizará directamente mediante la interfaz de terminal del hipervisor y, posteriormente, vía interfaz web, prescindiendo de conexiones físicas por puerto serie.

Figura 7.
Configuración de acceso por consola serial

Fuente: Autoría Propia

Una vez finalizada la instalación base, se procede con la configuración de la interfaz GREEN, la cual representa la red local segura y de confianza. Como se detalla en la Fig. 8, se asignó la dirección IP 192.168.10.1 con una máscara de subred 255.255.255.0, estableciendo así la puerta de enlace predeterminada para que el nodo de administración pueda comunicarse con el firewall y acceder a la gestión del sistema.

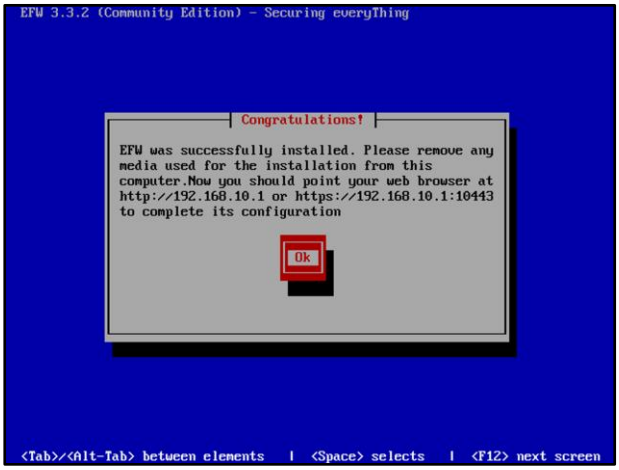
Figura 8.
Configuración de direccionamiento IP para la interfaz GREEN

Fuente: Autoría Propia

Tras confirmar los parámetros de red, el instalador notifica la finalización exitosa del despliegue, como se muestra en la Fig. 9. En esta ventana de cierre, el sistema indica que el acceso para la configuración avanzada debe realizarse vía navegador web a través de la dirección 192.168.10.1, utilizando

el puerto seguro 10443, lo que marca el paso de la instalación local a la gestión remota del firewall.

Figura 9.
Notificación de finalización de instalación y parámetros de acceso web



Fuente: Autoría Propia

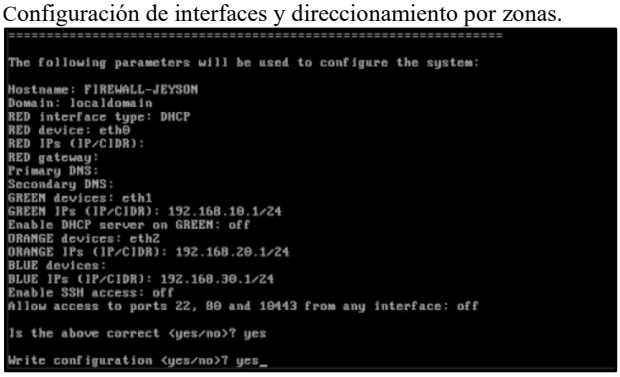
Una vez reiniciado el sistema, se visualiza la consola de administración local del Endian Firewall, como se muestra en la Fig. 10. En esta interfaz se confirma que el servicio está activo, detallando la URL de gestión y el estado de la interfaz eth0 asociada a la zona GREEN. Asimismo, la consola proporciona un menú de opciones rápidas para la gestión del sistema, permitiendo verificar de forma inmediata que la configuración de red inicial es correcta antes de proceder con el acceso vía entorno web.

Figura 10.
Consola de administración local y estado de la zona GREEN

Fuente: Autoría Propia

En esta etapa, se visualiza el resumen detallado de la configuración del sistema, donde se definen las tres zonas de red esenciales para el proyecto. Como se observa en la Fig. 11, la zona RED se establece vía DHCP para la salida a internet, mientras que la zona GREEN (administración) se configura con el segmento 192.168.10.1/24 y la zona ORANGE (DMZ) con el segmento 192.168.20.1/24. Esta asignación de interfaces (eth0, eth1 y eth2) consolida la estructura de seguridad lógica necesaria para el aislamiento de servicios y el control de tráfico perimetral.

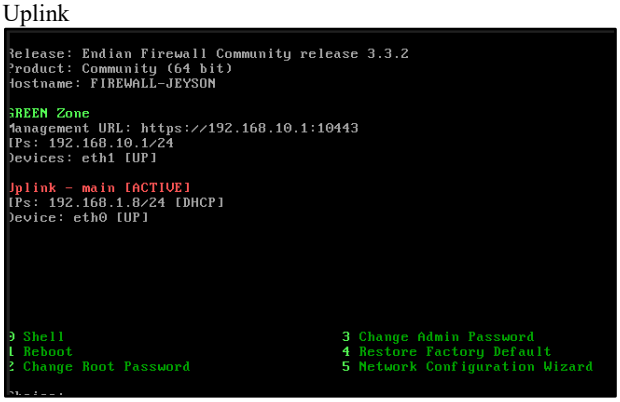
Figura 11.
Configuración de interfaces y direccionamiento por zonas.



Fuente: Autoría Propia

Tras la aplicación de los cambios, se confirma la operatividad del sistema bajo el nombre de host personalizado FIREWALL-JEYSON, tal como se evidencia en la Fig. 12. En esta pantalla de estado, se observa que la zona GREEN se encuentra activa en el segmento 192.168.10.1/24 a través de la interfaz eth1, mientras que el enlace de salida (Uplink) en la zona RED ha obtenido exitosamente una dirección IP por DHCP (192.168.1.8) mediante el dispositivo eth0. Con esta verificación visual, se da por terminada la configuración por consola, dejando el firewall listo para la gestión avanzada desde el entorno gráfico.

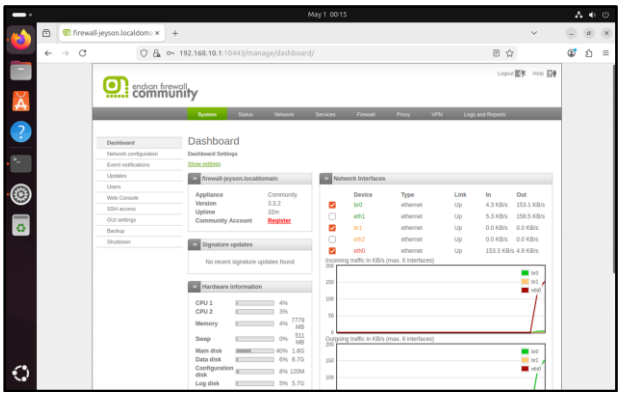
Figura 12.
Consola de administración con host personalizado y estado de Uplink



Fuente: Autoría Propia

Se realizó el acceso exitoso a la interfaz web de administración utilizando el navegador Firefox desde la estación Ubuntu, como se muestra en la Fig. 13. En el panel principal o Dashboard, se valida la salud del sistema, observando el uso de recursos de hardware y el tráfico en tiempo real de las interfaces de red configuradas (br0, br1 y eth0). Este entorno gráfico permite una gestión centralizada y profesional de todas las directivas de seguridad, confirmando que la conectividad entre el nodo de administración y el firewall se ha establecido correctamente bajo el protocolo HTTPS por el puerto 10443.

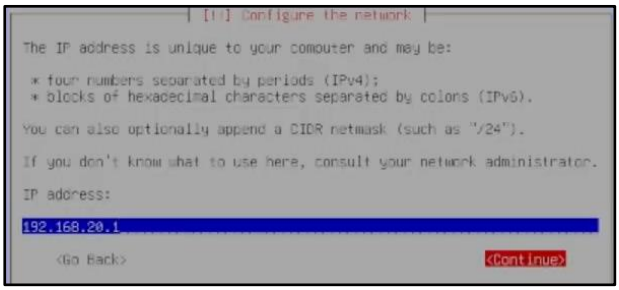
Figura 13.
Panel de control (Dashboard) de Endian Firewall desde el cliente Ubuntu



Fuente: Autoría Propia

Como parte de la configuración de red del servidor, se procedió a ingresar la dirección IP 192.168.20.2, como se observa en la Fig. 14. Este parámetro establece la comunicación directa con la interfaz del firewall correspondiente a la zona naranja (DMZ), asegurando que el servidor tenga una ruta de salida y entrada definida para el tráfico de datos supervisado por el sistema de seguridad perimetral.

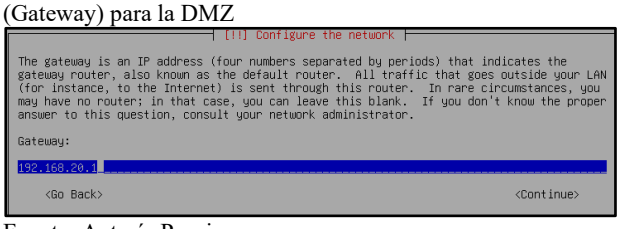
Figura 14.
Asignación de dirección IP para la puerta de enlace en el servidor



Fuente: Autoría Propia

En esta fase del despliegue del servidor Debian, se definió la dirección 192.168.20.1 como la puerta de enlace predeterminada o Gateway, tal como se muestra en la Fig. 15. Este parámetro es fundamental para la arquitectura de red, ya que indica al nodo que todo el tráfico destinado a redes externas o a Internet debe ser canalizado a través de la interfaz del firewall. De esta manera, se garantiza que el flujo de datos de la zona naranja permanezca bajo la inspección y el control de las políticas de seguridad perimetral establecidas.

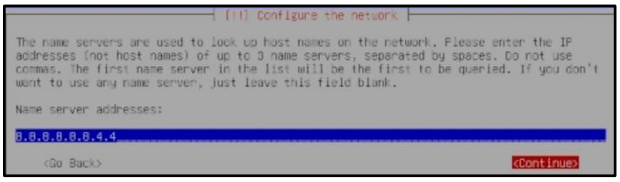
Figura 15.
Configuración de la puerta de enlace predeterminada (Gateway) para la DMZ



Fuente: Autoría Propia

Para asegurar que el servidor de la zona naranja pueda resolver nombres de dominio en internet, se configuraron los servidores DNS públicos de Google, 8.8.8.8 y 8.8.4.4, como se observa en la Fig. 16. Esta configuración proporciona una capa de redundancia para la resolución de nombres, permitiendo que el servidor Debian realice actualizaciones de software y acceda a repositorios externos de manera eficiente a través de la conexión gestionada por el firewall.

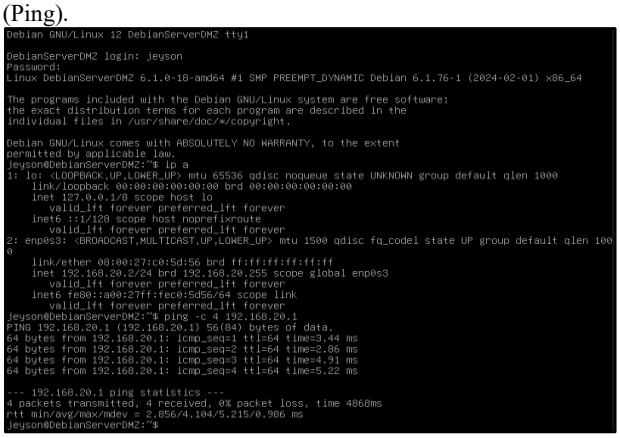
Figura 16.
Configuración de servidores DNS públicos en el servidor de la DMZ



Fuente: Autoría Propia

Tras finalizar la instalación, se validó la configuración interna del servidor Debian mediante el comando ip a, confirmando la asignación exitosa de la dirección 192.168.20.2 en la interfaz de red, como se muestra en la Fig. 17. Acto seguido, se realizó una prueba de conectividad hacia la puerta de enlace (192.168.20.1) utilizando el comando ping, obteniendo una respuesta exitosa con 0% de pérdida de paquetes. Este resultado certifica que el canal de comunicación entre el servidor de la zona naranja y el firewall está plenamente operativo y correctamente segmentado.

Figura 17.
Verificación de direccionamiento IP y prueba de conectividad (Ping).



Fuente: Autoría Propia

4.2 TEMÁTICA 2: CONFIGURACIÓN NAT

Se realizó la configuración de NAT en un firewall Endian, con el objetivo de permitir la comunicación desde la red LAN y la zona DMZ hacia Internet, garantizando seguridad perimetral mediante la traducción de direcciones IP.

Tabla 1. Información IP de cada Zona

ZONA	IP	FUNCION
Roja	192.168.1.8	WAN (internet)
Naranja	192.168.20.1	DMZ (servidores)
Verde	192.168.10.1	LAN (red interna o cliente)

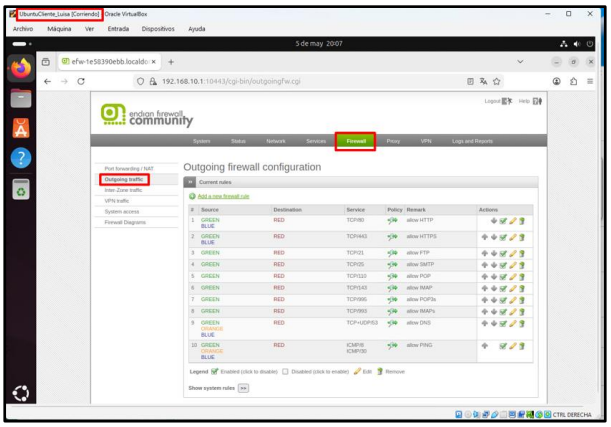
Nota. Se presenta la información correspondiente de cada Zona con su respectiva IP y su función

4.2.1 CONFIGURACIÓN DE LA REGLA NAT DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN

La configuración de NAT (Network Address Translation) es un mecanismo fundamental dentro de la seguridad perimetral, ya que esta permite que los dispositivos de una red privada puedan comunicarse con redes externas como Internet mediante la traducción de direcciones IP.

Durante el proceso de instalación y configuración de Endian, se realizó la configuración de diferentes zonas de red con el objetivo de segmentar el tráfico y mejorar la seguridad perimetral de la infraestructura. Ingresando a la interfaz de Endian Firewall mediante la dirección IP correspondiente a la zona verde, se establece una regla NAT estableciendo como origen la red verde y como interfaz de salida la zona RED, correspondiente a la conexión WAN.

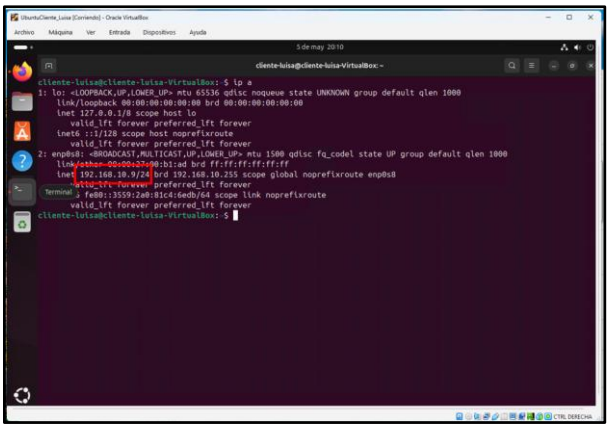
Figura 18.
Verificación NAT activo



Fuente: Autoría Propia

Dentro de las verificaciones adicionales que se realizan para que se valide la configuración de la LAN y con el propósito de conocer las direcciones IP a las cuales se puede obtener la conexión y que coincidan con el rango de la IP de la zona verde, se ejecuta el comando ip a.

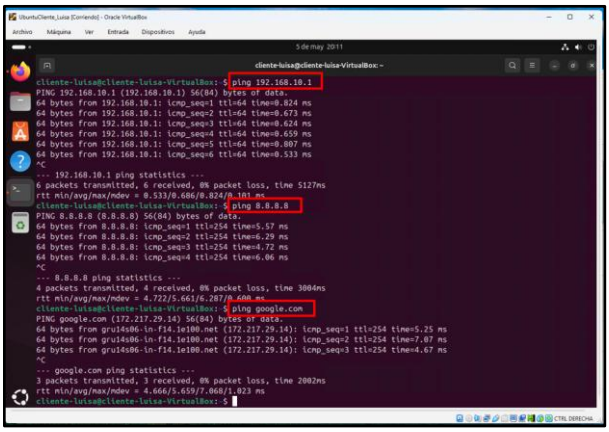
Figura 19.
Verificación configuración de la LAN



Fuente: Autoría Propia

Para probar la conectividad en la máquina, desde la terminal se van a probar la conexión al firewall realizando un ping a la zona verde (192.168.10.1), también se va a probar la salida a internet por IP, realizando un ping a la IP de Google (8.8.8.8) y finalmente se prueba la navegación por DNS realizando un ping a Google (google.com). Estas pruebas permiten confirmar que la máquina cliente tiene una salida correcta a Firewall por IP y por DNS.

Figura 20.
Prueba de conectividad en la LAN



Fuente: Autoría Propia

La regla implementada permitió que todo el tráfico proveniente de la red LAN fuera traducido y encaminado hacia la red externa, garantizando conectividad hacia Internet y ocultando las direcciones privadas de los equipos internos.

4.2.2 CONFIGURACIÓN LA REGLA DE NAT, DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DE LA ZONA DMZ HACIA LA INTERNET

La implementación de reglas NAT en la zona DMZ, permite establecer una comunicación controlada y segura entre los servidores ubicados en esta red y la Internet. La DMZ o zona desmilitarizada se utiliza para alojar servicios y aplicaciones

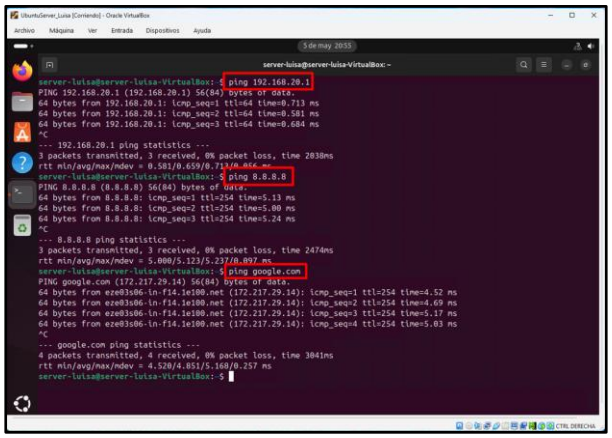
que requieren cierto nivel de acceso externo, manteniendo aislada y protegida la red interna de la organización.

No existe conectividad desde la DMZ, por lo cual se debe realizar una configuración previa a la configuración de la regla. Esta configuración consiste en agregar la puerta de enlace correspondiente a la DMZ para que se pueda realizar las salidas hacia internet. Por lo cual se debe editar el archivo /etc/netplan/*.yaml para que el servidor tenga conexión a firewall adicionando al archivo la siguiente información:

```
version: 2
  ethernets:
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.20.10/24
      gateway4: 192.168.20.1
      nameservers:
        addresses:
          - 8.8.8.8
```

Al finalizar este proceso, desde la DMZ se realiza un ping al firewall (192.168.20.1), a la IP de Google (8.8.8.8) y al DNS de Google (google.com) para así poder comprobar las conexiones correctas desde esta máquina.

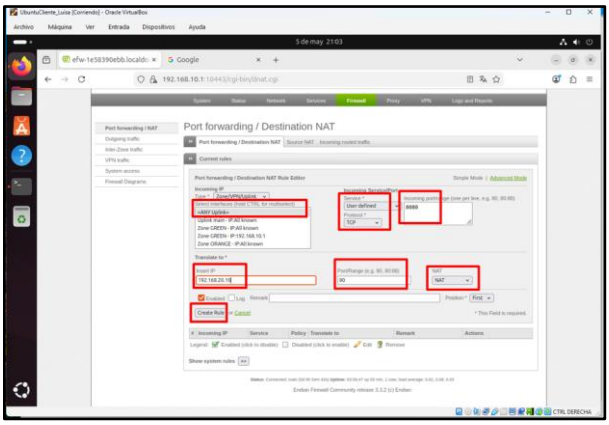
Figura 21.
Prueba de conectividad desde la DMZ



Fuente: Autoría Propia

Para iniciar con la creación de la regla, desde la interfaz de Endian, se debe seleccionar la interfaz, el protocolo, el puerto y se inserta la IP de la zona verde. La configuración de esta regla de reenvío de puertos (Port Forwarding) en el firewall Endian Firewall Community, permite redirigir solicitudes externas desde el puerto 8080 hacia el puerto 80 de un servidor web ubicado en la zona DMZ. Esto permite el acceso controlado desde Internet a servicios internos sin comprometer la seguridad de la red LAN.

Figura 22.
Configuración de parámetros para la creación de la regla en Endian



Fuente: Autoría Propia

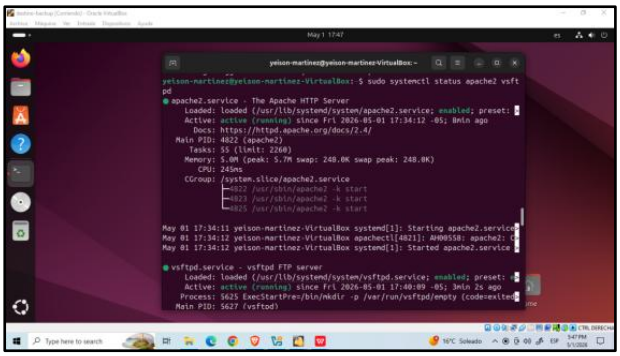
La configuración de una regla NAT en GNU/Linux Endian Firewall Community para permitir la salida de tráfico desde la zona naranja (DMZ) hacia la WAN (Internet). Esta configuración posibilita que los servidores puedan acceder a recursos externos, realizar actualizaciones o establecer conexiones necesarias para su funcionamiento, utilizando la dirección pública del firewall.

4.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Una vez validada la segmentación de red y el direccionamiento IP por zonas (Temática 1), se procede a la fase de exposición de servicios en la zona desmilitarizada (DMZ). El objetivo de esta etapa es configurar los servicios HTTP y FTP en el servidor Debian y aplicar las reglas de firewall correspondientes para autorizar o denegar el tráfico entre la zona interna (GREEN) y la zona de servicios (ORANGE).

Se procedió con la instalación de los servicios apache2 y vsftpd en la máquina virtual correspondiente a la zona DMZ. Tras la instalación, se verificó mediante el comando systemctl status que ambos servicios se encontraran en estado activo y operativos, asegurando que los puertos 80 y 21 estuvieran a la escucha antes de aplicar las políticas de seguridad. Como se observa en la Fig. 23, el servidor web y el servicio de transferencia de archivos están habilitados para su ejecución en la red interna.

Figura 23.
Verificación del estado activo de los servicios HTTP y FTP.

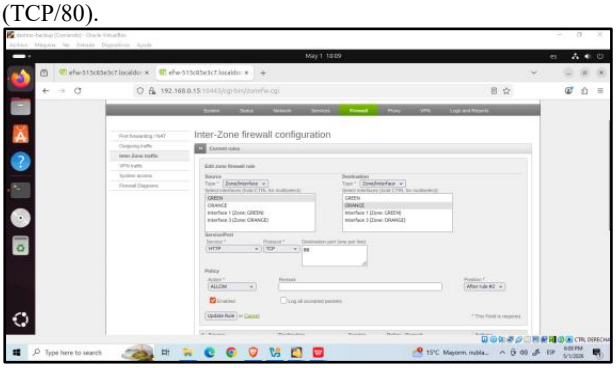


Fuente: Autoría Propia

Desde la interfaz web de administración de Endian Firewall, se accedió al módulo Inter-Zone traffic para definir las políticas de filtrado. Se establecieron tres reglas críticas que garantizan la disponibilidad de los servicios y el endurecimiento de la seguridad perimetral.

Primero, se creó la regla para habilitar el tráfico web. Como se detalla en la Fig. 24, se configuró el servicio HTTP (TCP/80) con una política de acción ALLOW, permitiendo que los nodos de la zona GREEN accedan a la página alojada en el servidor de la zona ORANGE.

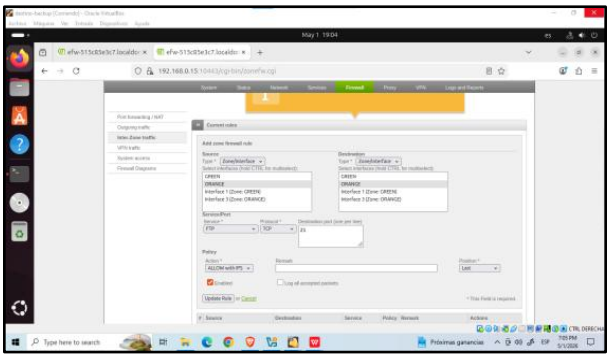
Figura 24.
Configuración de regla de permiso para servicio HTTP (TCP/80).



Fuente: Autoría Propia

Posteriormente, se definió la regla para el servicio de transferencia de archivos. En la Fig. 20 se observa la configuración del protocolo FTP (TCP/21) con una política ALLOW with IPS, lo que autoriza la transferencia de datos aplicando además inspección de paquetes para prevenir vulnerabilidades.

Figura 25.
Configuración de regla de permiso para servicio FTP.



Fuente: Autoría Propia

Finalmente, para reducir la superficie de ataque, se implementó una restricción contra el protocolo ICMP. Como se ilustra en la Fig. 21, se creó una regla con política DENY para el tráfico ICMP (ping), impidiendo que se puedan diagnosticar o enumerar los hosts de la zona DMZ desde la red interna.

Figura 26.
Configuración de regla de denegación para protocolo ICMP.

Fuente: Autoría Propia

La tabla final de reglas activas se presenta en la Fig. 22, donde se confirma la correcta aplicación de las directivas: HTTP y FTP permitidos, y ICMP bloqueado, validando así el cumplimiento de los objetivos de seguridad planteados para la temática.

Figura 27.
Tabla final de reglas inter-zona aplicadas en el firewall.

Fuente: Autoría Propia

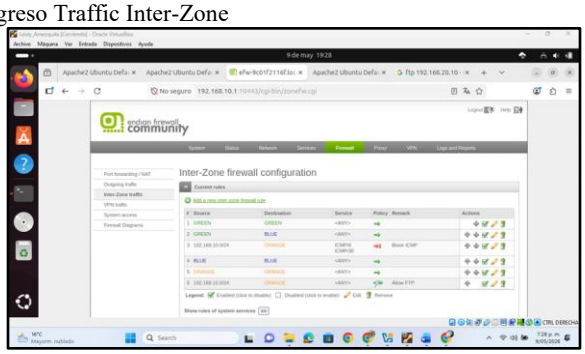
4.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Este apartado detalla la configuración técnica de políticas de seguridad en el firewall perimetral para segmentar y controlar el flujo de datos entre las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN).

4.4.1 CONFIGURACIÓN DE POLÍTICAS INTER-ZONA

Se establecieron reglas específicas para gestionar el tráfico que atraviesa el firewall, asegurando que solo los servicios autorizados operen entre los distintos segmentos de la red:

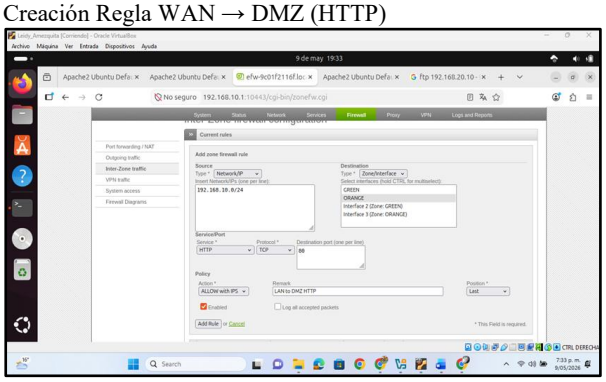
Figura 28.
Ingreso Traffic Inter-Zone



Fuente: Autoría Propia

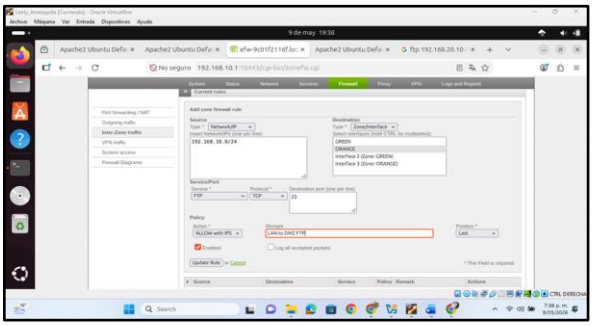
Segmentación LAN → DMZ: Se crearon reglas para permitir el tráfico HTTP y FTP desde la red interna hacia los servidores ubicados en la zona desmilitarizada.

Figura 29.
Creación Regla WAN → DMZ (HTTP)



Fuente: Autoría Propia

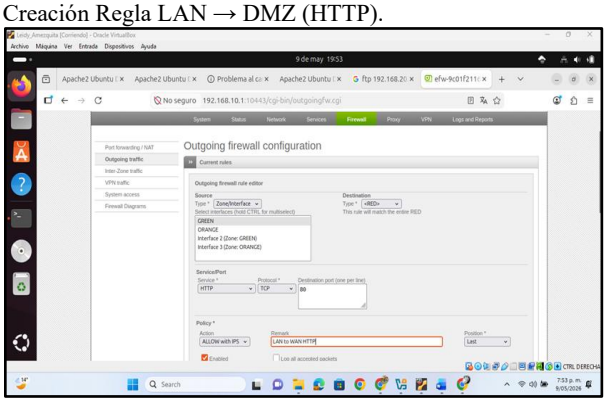
Figura 30.
Creación Regla LAN → DMZ (FTP).



Fuente: Autoría Propia

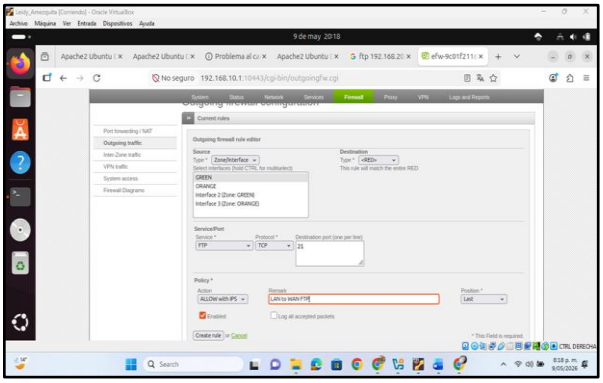
Control Internet ↔ DMZ: Se definieron políticas de acceso bidireccional para servicios web y de transferencia de archivos, facilitando la publicación controlada de servicios hacia la WAN.

Figura 31.
Creación Regla LAN → DMZ (HTTP).



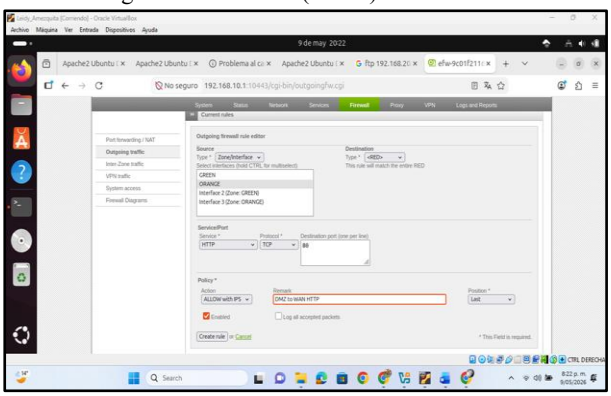
Fuente: Autoría Propia

Figura 32.
Creación Regla LAN → WAN (FTP).



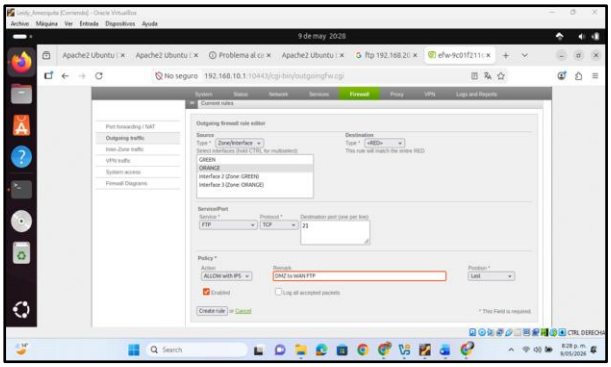
Fuente: Autoría Propia

Figura 33.
Creación Regla DMZ → LAN (HTTP)



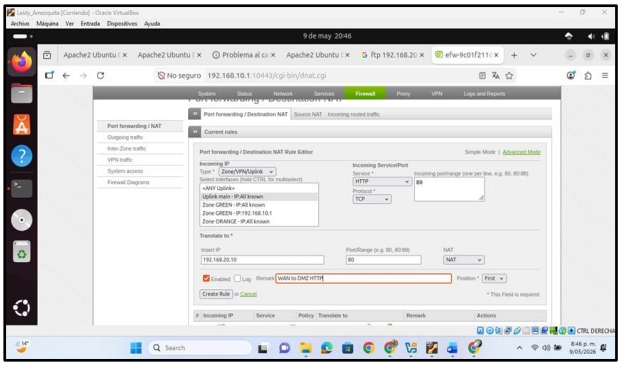
Fuente: Autoría Propia

Figura 34.
Creación Regla DMZ → LAN (FTP)



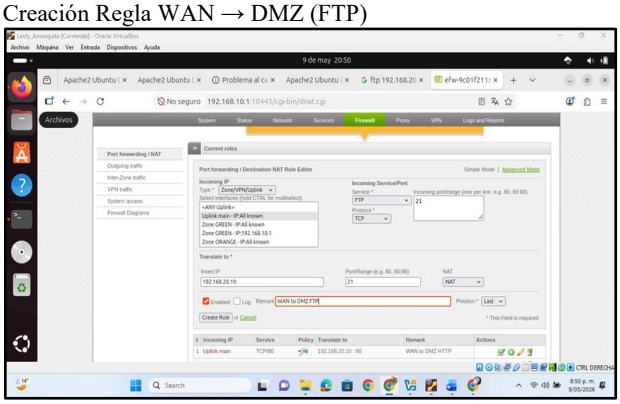
Fuente: Autoría Propia

Figura 35.
Creación Regla WAN → DMZ (HTTP)



Fuente: Autoría Propia

Figura 36.
Creación Regla WAN → DMZ (FTP)



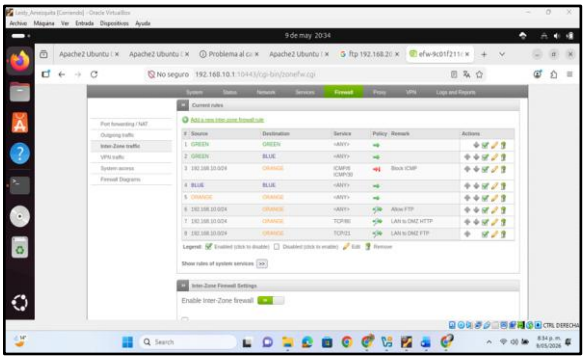
Fuente: Autoría Propia

Políticas de Salida (Outgoing): Configuración de reglas para permitir que los equipos internos y los servidores en la DMZ realicen consultas externas bajo protocolos específicos.

Figura 37.
Resumen Reglas Endian Outgoing traffic

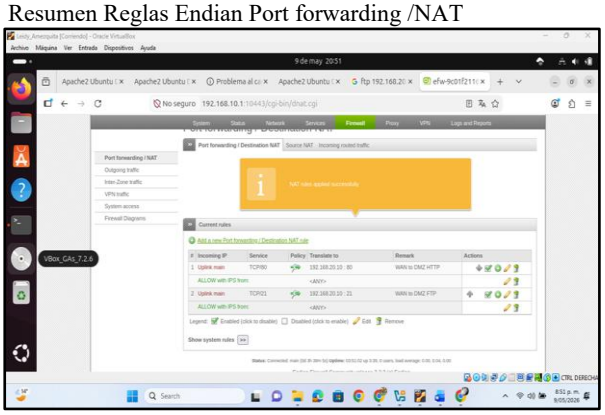
Fuente: Autoría Propia

Figura 38.
Resumen Reglas Endian Inter Zone Traffic



Fuente: Autoría Propia

Figura 39.
Resumen Reglas Endian Port forwarding /NAT



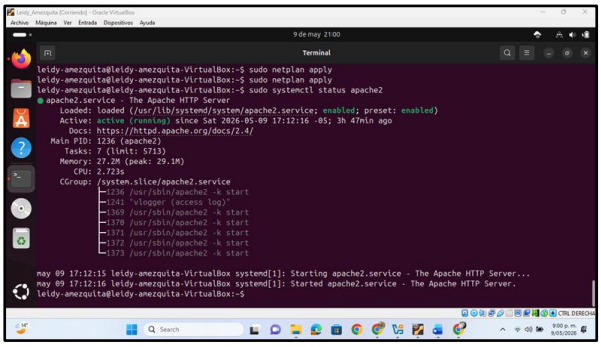
Fuente: Autoría Propia

4.4.2 VALIDACIÓN Y PRUEBAS DE CONECTIVIDAD

Para garantizar la integridad de las reglas aplicadas, se ejecutaron protocolos de verificación técnica:

Verificación de Servicios: Comprobación del estado activo de los servidores Apache y VSFTPD en la zona DMZ mediante comandos de sistema (systemctl status).

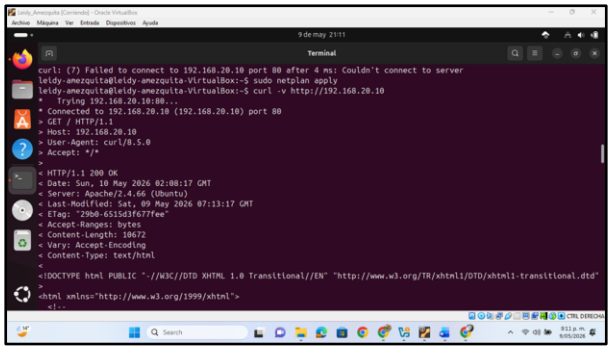
Figura 40.
Validar apache



Fuente: Autoría Propia

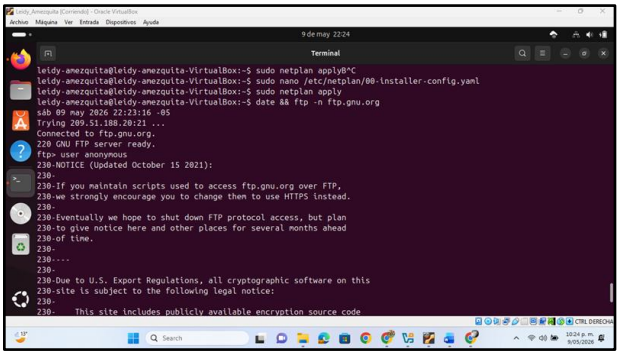
Pruebas de Acceso Web: Uso de herramientas como curl y navegadores web para validar la respuesta HTTP (código 200) desde la LAN y redes externas hacia la DMZ.

Figura 41.
Verificación desde TerminalFuente: Autoría Propia



Pruebas de Transferencia FTP: Instalación de clientes FTP para confirmar la conexión y el listado de directorios a través de las reglas de NAT y firewall.

Figura 42.
Conectar FTP externo



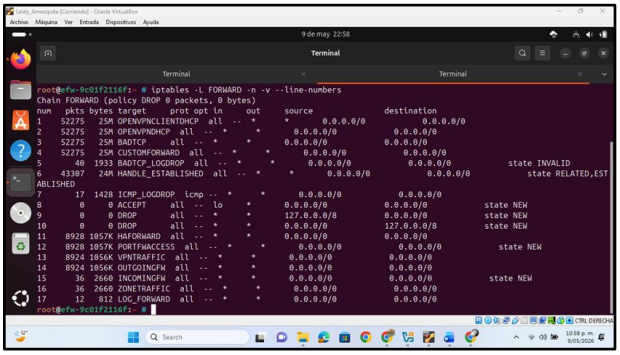
Fuente: Autoría Propia

4.4.3. MONITOREO Y AUDITORÍA DEL FIREWALL

La fase final consistió en la supervisión en tiempo real de la infraestructura de seguridad:

Inspección de Iptables: Ejecución de comandos de diagnóstico (iptables -L FORWARD) con contadores de paquetes para visualizar el tráfico que impacta cada regla.

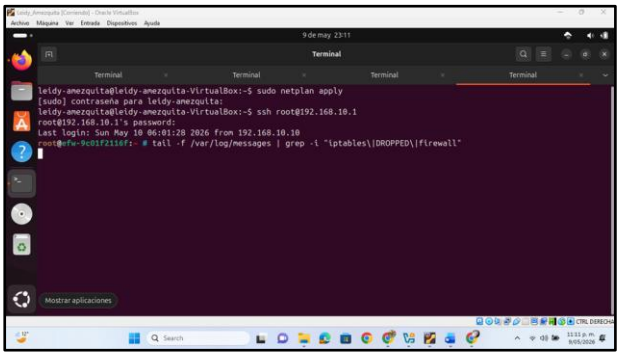
Figura 43.
Ver todas las reglas del firewall con contadores



Fuente: Autoría Propia

Análisis de Logs: Monitoreo activo de los registros del sistema (tail -f /var/log/messages) para identificar y analizar intentos de acceso denegados o paquetes descartados (DROPPED).

Figura 44.
Logs del firewall para ver qué está siendo bloqueado



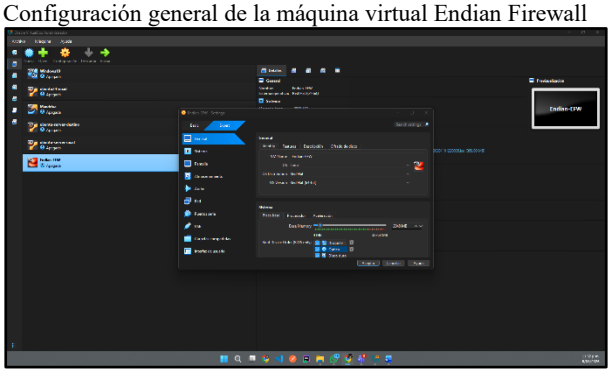
Fuente: Autoría Propia

Este proceso permitió consolidar un entorno de red robusto donde la segmentación garantiza que cada flujo de datos cumpla estrictamente con las políticas de seguridad institucional.

4.5 TEMÁTICA 5: IMPLEMENTACIÓN DE PROXY HTTP CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Se implementó un proxy HTTP en modo no transparente sobre Endian Firewall Community 3.3.2 en un entorno virtualizado con VirtualBox, integrando autenticación local mediante el protocolo NCSA y un perfil de lista negra para el control de acceso web. Este modo de operación requiere que cada equipo cliente configure manualmente el servidor proxy en su navegador, garantizando que solo los usuarios autenticados y autorizados puedan navegar bajo las restricciones definidas por el administrador de red. A continuación, se describe el proceso de configuración y validación realizado.

Figura 45.
Configuración general de la máquina virtual Endian Firewall



Fuente: Autoría Propia

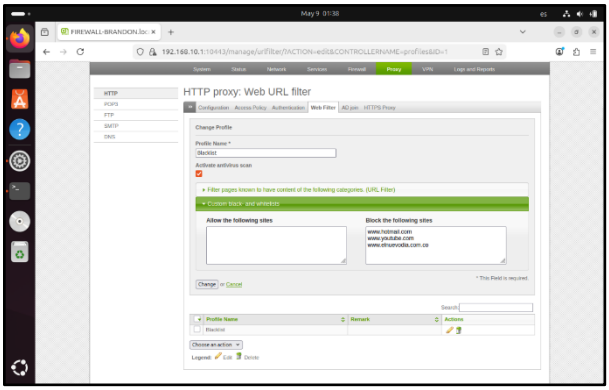
Se creó la máquina virtual para Endian Firewall Community en VirtualBox, asignando los recursos de hardware necesarios: memoria RAM, procesador y almacenamiento en disco para garantizar el correcto funcionamiento del firewall en el entorno de laboratorio.

Figura 46.
Habilitación del proxy HTTP no transparente en puerto 8080

Fuente: Autoría Propia

En el módulo Proxy → HTTP → Configuration se habilitó el proxy HTTP en modo no transparente, configurando el puerto 8080 como puerto de escucha. Este modo requiere que los equipos clientes configuren manualmente el proxy en su navegador para que el tráfico sea interceptado y filtrado.

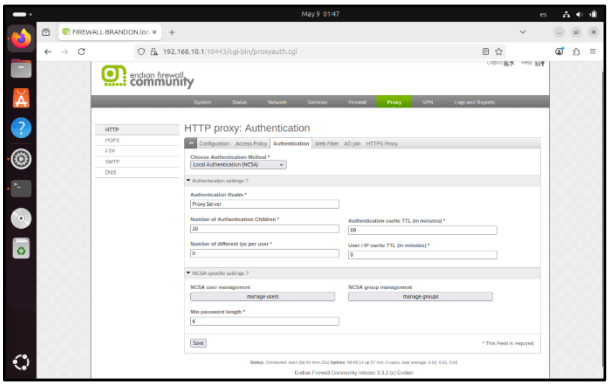
Figura 47.
Perfil Blacklist con lista de sitios bloqueados



Fuente: Autoría Propia

En el módulo Web Filter se configuró el perfil Blacklist, estableciendo en la sección de listas personalizadas los dominios a bloquear: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, los cuales quedan registrados en el campo "Block the following sites".

Figura 48.
Configuración del método de autenticación Local NCSA



Fuente: Autoría Propia

En la pestaña Authentication del módulo HTTP Proxy se seleccionó el método Local Authentication (NCSA), el cual permite gestionar usuarios y grupos de forma local directamente desde el panel de administración del firewall, sin depender de servicios externos de directorio.

Figura 49.
Usuario brandon_proxy asociado al grupo grupo_lan

Fuente: Autoría Propia

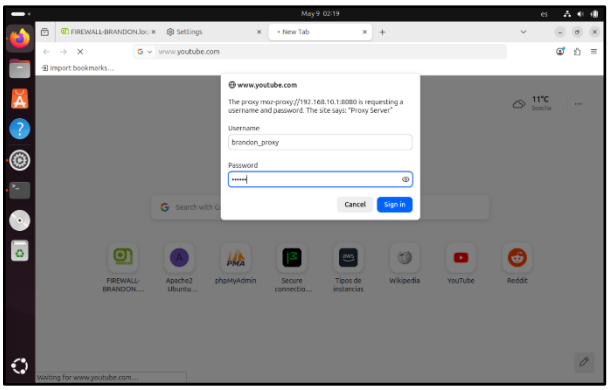
Se creó el usuario brandon_proxy desde la opción NCSA User Management y se asoció al grupo grupo_lan, previamente creado desde NCSA Group Management. Este usuario es el encargado de autenticar las solicitudes de navegación provenientes de la red LAN.

Figura 50.
Política de acceso aplicada exitosamente

Fuente: Autoría Propia

En la pestaña Access Policy se configuró la política con origen GREEN, autenticación por grupo grupo_lan, perfil Blacklist y acción Allow Access. El sistema confirmó su aplicación con el mensaje "Proxy settings have been applied successfully".

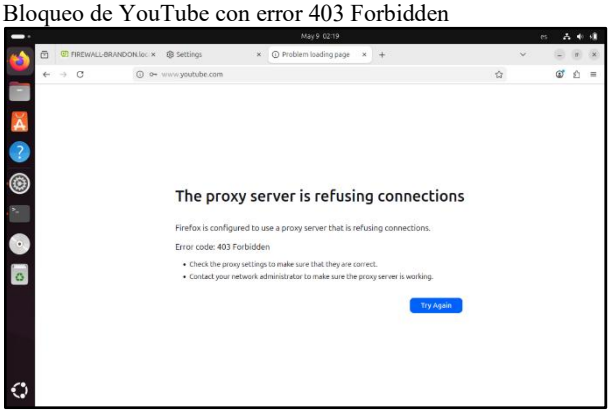
Figura 51.
Ventana de autenticación al intentar acceder a los sitios web bloqueados



Fuente: Autoría Propia

Desde el equipo cliente Ubuntu con el proxy configurado manualmente en Firefox (192.168.10.1:8080), al intentar acceder a www.hotmail.com el proxy interceptó la solicitud y presentó una ventana de autenticación, confirmando el correcto funcionamiento del proxy no transparente.

Figura 52.
Bloqueo de YouTube con error 403 Forbidden



Fuente: Autoría Propia

Al autenticar con el usuario brandon_proxy e intentar acceder a www.youtube.com, el proxy retornó el error 403 Forbidden, bloqueando el acceso al sitio definido en la lista negra del perfil Blacklist y confirmando que la política de acceso está siendo aplicada correctamente sobre el tráfico de la red LAN.

Figura 53.
Bloqueo de www.hotmail.com con mensaje Access Denied

Fuente: Autoría Propia

Al intentar acceder a www.hotmail.com desde el equipo cliente con el proxy configurado, Endian Firewall retornó la página de error del motor Squid con el mensaje "Access Denied", confirmando que el proxy HTTP interceptó la solicitud y aplicó la política de bloqueo definida en el perfil Blacklist para este dominio.

5 CONCLUSIONES

La implementación de Endian Firewall Community permitió establecer una arquitectura de red segmentada y segura mediante la correcta configuración de las zonas GREEN, ORANGE y RED, garantizando el aislamiento efectivo de la red interna y la DMZ, así como la protección de los servicios frente a amenazas provenientes de la red externa. La gestión de la zona RED como interfaz hacia Internet posibilitó la aplicación de políticas estrictas de filtrado y control de tráfico, mientras que el uso de direccionamiento estático en los nodos Ubuntu y Debian aseguró una administración organizada de la conectividad y la integridad de los datos dentro de la infraestructura.

Asimismo, la segmentación de la red permitió implementar de manera efectiva el principio de defensa en profundidad, fortaleciendo la seguridad perimetral mediante la habilitación controlada de servicios HTTP (puerto 80) y FTP (puerto 21) hacia la DMZ sin comprometer la red interna. De igual forma, el bloqueo explícito del protocolo ICMP contribuyó a reducir la superficie de ataque al dificultar la identificación de hosts activos y limitar posibles procesos de reconocimiento por parte de usuarios no autorizados.

Por otra parte, la implementación del proxy HTTP no transparente en Endian Firewall Community demostró ser una solución eficiente para el control de acceso web en entornos corporativos. La integración de autenticación NCSA permitió asociar las políticas de navegación con la identidad de los usuarios, garantizando que únicamente los miembros autorizados pudieran acceder a Internet bajo las restricciones definidas. Además, el uso de perfiles Blacklist validó la correcta aplicación de las políticas de seguridad al bloquear exitosamente los dominios configurados mediante respuestas 403 Forbidden y Access Denied generadas por el motor Squid.

Finalmente, se evidenció que el tráfico HTTPS requiere mecanismos adicionales de inspección SSL para aplicar controles equivalentes sobre conexiones cifradas. En conjunto, el desarrollo de estas prácticas permitió consolidar competencias en administración de firewalls, segmentación de redes, gestión de políticas de acceso y seguridad perimetral, habilidades fundamentales en la formación y desempeño profesional de un administrador de sistemas y seguridad informática.

6. REFERENCIAS

[1] Canonical. (2023). *Guía del Ubuntu Desktop 20.04 LTS*. Help Ubuntu. https://help.ubuntu.com/

[2] Cisco. (2026). *Preguntas frecuentes sobre la traducción de direcciones de red (NAT)*. Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

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

[4] Endian S.r.l. (2007). *The Proxy Menu — Endian Firewall Reference Manual r. 2.2*. Endian Documentation. https://docs.endian.com/archive/2.2/efw.proxy.html

[5] Fortinet. (2025). *What Is a DMZ Network and Why Would You Use It?* Fortinet Cyberglossary. https://www.fortinet.com/resources/cyberglossary/what-is-dmz

[6] Mozilla Developer Network. (2025). *Autenticación HTTP*. MDN Web Docs. https://developer.mozilla.org/es/docs/Web/HTTP/Guides/Authentication

[7] Netskope. (2026). *¿Qué es un servidor proxy? Tipos y casos de uso*. Netskope Security. https://www.netskope.com/es/security-defined/what-is-a-proxy-server

[8] Oracle. (2023). *Oracle VM VirtualBox User Manual*. Oracle VirtualBox. https://www.virtualbox.org/manual/UserManual.html

[9] RedesZone. (2024). *Vsftpd servidor FTP para Linux: Instalación y configuración*. RedesZone. https://www.redeszone.net/tutoriales/servidores/vsftpd-configuracion-servidor-ftp/

[10] Universidad de Quintana Roo. (2014). *Seguridad perimetral*. Risisbi UQROO. http://risisbi.uqroo.mx/bitstream/handle/20.500.12249/3102/QA76.9.OS57.2014-378.pdf

[11] Universidad de San Carlos de Guatemala. (2008). *Diseño de aseguramiento de redes utilizando DMZ* [Tesis de grado, Universidad de San Carlos de Guatemala]. Biblioteca USAC. http://biblioteca.usac.edu.gt/tesis/08/08_0236_EO.pdf