DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL MEDIANTE ENDIAN FIREWALL EN SISTEMAS GNU/LINUX

Cristopher Ochoa Ramos
e-mail: cochoar@unadvirtual.edu.co
Fanor Losada Garay
e-mail: flosadaga@unadvirtual.edu.co
Oscar Alejandro Betancour García
oabetancourg@unadvirtual.edu.co
Samara Hernández Yasnó
e-mail: shernandezya@unadvirtual.edu.co
Zuleidy Dayana Silva Rubio
e-mail: zdsilvar@unadvirtual.edu.co

RESUMEN: *La creciente necesidad de proteger infraestructuras de red frente a accesos no autorizados y amenazas externas ha impulsado la adopción de mecanismos de seguridad basados en software libre. En este contexto, el presente artículo presenta una solución de seguridad perimetral basada en Endian Firewall para entornos virtualizados, orientada al control y administración del tráfico entre las zonas LAN, WAN y DMZ. La implementación incluyó la configuración de interfaces de red y segmentación de zonas, reglas de traducción de direcciones de red (NAT) y políticas de acceso para regular la comunicación entre los distintos segmentos de la infraestructura.*

Asimismo, se habilitaron servicios HTTP y FTP en un servidor ubicado en la zona DMZ, complementados con restricciones sobre protocolos ICMP para fortalecer la protección de la red. Finalmente, se implementó un proxy HTTP no transparente con autenticación de usuarios y listas negras para el control de navegación web. Los resultados obtenidos evidencian la efectividad de Endian Firewall para la administración, monitoreo y protección de infraestructuras basadas en GNU/Linux.

PALABRAS CLAVE: Endian, Firewall, GNU/Linux, Seguridad.

1 INTRODUCCIÓN

En la actualidad, la seguridad de las infraestructuras de red se ha convertido en un aspecto fundamental debido al crecimiento constante de amenazas informáticas, accesos no autorizados y vulnerabilidades presentes en entornos conectados a Internet. Las organizaciones requieren mecanismos que permitan controlar el tráfico de red, proteger la información crítica y garantizar la disponibilidad de los servicios alojados en sus servidores. En este contexto, la implementación de soluciones de seguridad basadas en software libre representa una alternativa eficiente y accesible para fortalecer la protección de redes empresariales y académicas [1].

Una de las estrategias más utilizadas para mejorar la protección de los servicios expuestos consiste en la segmentación de la red mediante zonas de seguridad, permitiendo separar la red interna de los servicios accesibles desde redes externas. La implementación de una Zona Desmilitarizada (DMZ) facilita el aislamiento de servidores web y aplicaciones, reduciendo el riesgo de acceso directo a la infraestructura interna y permitiendo un mayor control sobre las comunicaciones entre segmentos de red [2].

Con el propósito de analizar este modelo de protección, se desarrolló un entorno virtualizado utilizando Oracle VM VirtualBox [3], en el cual se implementó Endian Firewall como plataforma principal para la administración y control del tráfico de red. La arquitectura propuesta permitió establecer diferentes zonas de comunicación y definir políticas de acceso entre ellas mediante mecanismos como NAT, filtrado de tráfico y control de servicios. Asimismo, se integró un servidor GNU/Linux en la zona DMZ para la habilitación de servicios de red y la validación del acceso controlado entre los distintos segmentos de la infraestructura.

Adicionalmente, se incorporaron mecanismos de restricción y monitoreo orientados al fortalecimiento de la seguridad de la red, incluyendo limitaciones sobre protocolos ICMP y la configuración de un proxy HTTP no transparente con autenticación de usuarios y filtrado de navegación mediante listas negras. Las pruebas realizadas permitieron validar el funcionamiento de las políticas implementadas y evidenciar la importancia de la segmentación y el control de tráfico como elementos fundamentales para la protección de infraestructuras de red.

2 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

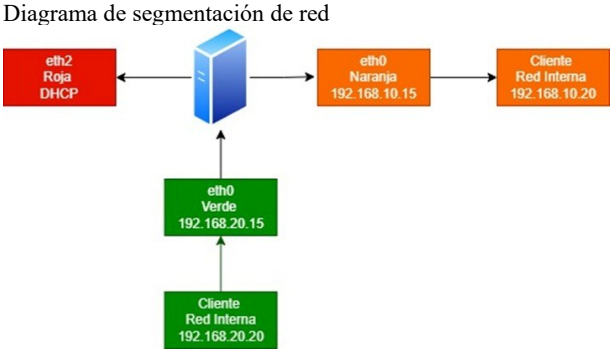
Para la creación del firewall Endian, se define un almacenamiento de 50 GB, la memoria base de 2048 MB y 2 procesadores virtuales. Con la finalidad de permitir la correcta segmentación de red, se configura los tres adaptadores de red en el firewall Endian de la siguiente forma [4]:

- Adaptador 1 (Zona verde): Red Interna, usada para red local, es la zona protegida, que nadie de la zona roja puede ingresar.
- Adaptador 2 (Zona naranja): Red Interna, es la zona desmilitarizada, esta zona alberga los servidores. Esta es la única zona a la que se puede acceder a la zona roja.
- Adaptador 3(Zona Roja): NAT, es el segmento no confiable, permite la conexiona a internet. Esta zona no es gestionable.

Además, se vincularon las máquinas virtuales con su zona correspondiente:

- Ubuntu Desktop: Red Interna, configurada para la zona verde
- Ubuntu Server: Red Interna, configurada para la zona naranja

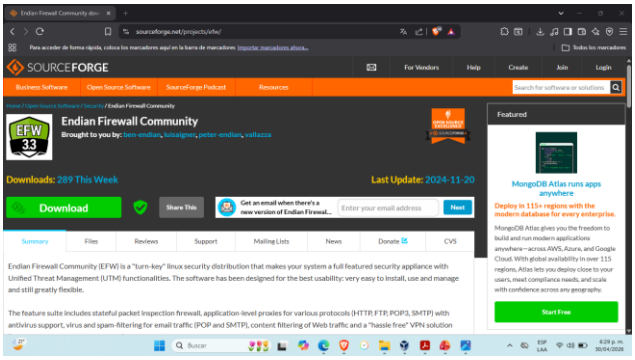
Figura 1.
Diagrama de segmentación de red



Fuente: Autoría propia

Se realiza la segmentación de la red asignando la dirección IP 192.168.20.20 para la zona VERDE y 192.168.10.20 para la zona NARANJA, ambas configuradas mediante adaptadores de red interna. Esta configuración permite separar los diferentes segmentos de red y controlar la comunicación entre ellos. Además, la zona ROJA se configura en modo NAT utilizando el protocolo DHCP para permitir la conexión a Internet y la comunicación con redes externas.

Figura 2.
Instalación del Endian



Fuente. Autoría propia

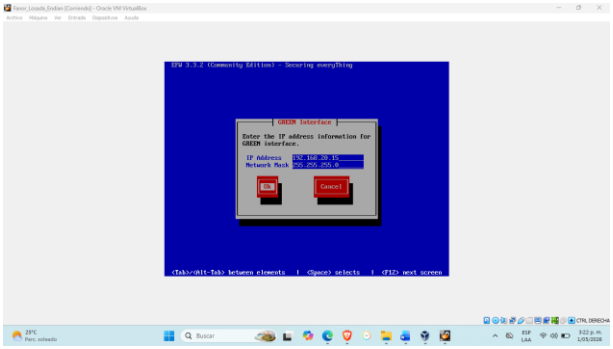
La descarga de la imagen ISO se realiza desde la página oficial de Endian Firewall Community, permitiendo obtener el archivo necesario para llevar a cabo la instalación del firewall dentro del entorno virtualizado. Este proceso garantiza el uso de una versión oficial y compatible para la implementación de la solución de seguridad. Además, permite asegurar la estabilidad y el correcto funcionamiento del sistema durante su configuración en VirtualBox.

Figura 3.
Configuración de la máquina virtual

Fuente: Autoría propia

Para la creación de la máquina virtual se indican diversos parámetros importantes para la configuración de la misma. Se asigna un nombre identificador y la ruta donde se almacenarán los archivos asociados al sistema. Además, se selecciona el tipo y la versión del sistema operativo compatible con Endian Firewall. También se definen recursos de hardware como la memoria RAM, el almacenamiento y la cantidad de procesadores virtuales. Esta configuración inicial permite garantizar el correcto funcionamiento del firewall dentro del entorno virtualizado.

Figura 4.
Instalación máquina virtual Endian y asignación de red zona verde



Fuente: Autoría propia

Se realiza la configuración de la interfaz VERDE, asignando la dirección IP estática 192.168.20.15 con máscara de subred 255.255.255.0. Esta interfaz corresponde a la red local interna y representa la zona protegida de la infraestructura. La dirección IP configurada funciona como puerta de enlace y administración del firewall dentro de la red LAN. Además, esta configuración permite controlar el acceso y la comunicación de los dispositivos internos de forma segura.

Figura 5.
Configuración zona roja

Fuente: Autoría propia

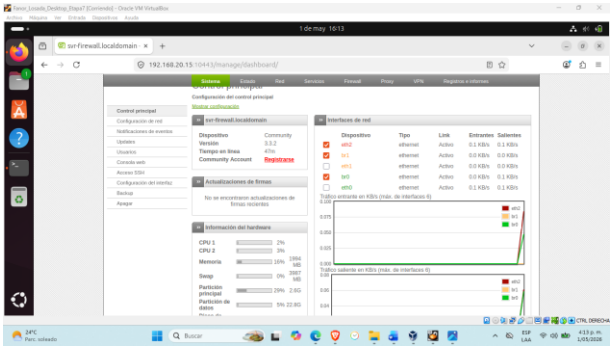
Para la zona ROJA se habilita el enrutamiento y el protocolo DHCP para la asignación dinámica de direcciones IP. Esta zona representa el segmento no confiable de la red, ya que corresponde a la conexión hacia Internet. Su configuración permite gestionar el tráfico externo y controlar las conexiones entrantes y salientes mediante el firewall. De esta manera, se protege la comunicación entre las diferentes zonas definidas en la arquitectura de red.

Figura 6.
Configuración zona naranja

Fuente: Autoría propia

En la zona NARANJA se asigna la dirección IP 192.168.10.15 con máscara de red 255.255.255.0. Esta zona corresponde a la DMZ, utilizada para alojar servicios y servidores accesibles desde otras redes. Además, se realiza la vinculación de las interfaces de red y la asignación del nombre del host para facilitar la administración del sistema. La implementación de esta zona permite mantener aislados los servicios expuestos respecto a la red interna protegida.

Figura 7.
Dashboard de Endian Firewall



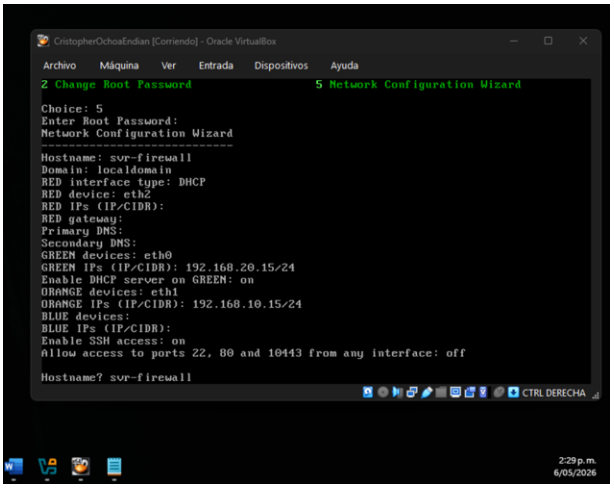
Fuente: Autoría propia

El dashboard de Endian Firewall permite visualizar el estado general del sistema y supervisar el funcionamiento de las interfaces de red. Desde este panel es posible monitorear el tráfico, verificar el estado de las zonas configuradas y observar el consumo de recursos en tiempo real. Además, proporciona información relacionada con conexiones activas y servicios habilitados en el firewall. Esto facilita las tareas de administración y validación del correcto funcionamiento de la infraestructura implementada.

3 TEMÁTICA 2: CONFIGURACIÓN NAT

Para realizar la configuración de NAT, técnica utilizada para traducir direcciones IP privadas en direcciones IP públicas y permitir la comunicación entre redes internas y externas [5], se usó Endian Firewall, donde se configuraron 3 interfaces de red. Esta configuración permitió la segmentación de la red en distintas zonas y la aplicación de reglas NAT para permitir la correcta salida del tráfico hacia internet desde LAN y DMZ.

Figura 8.
Validación zonas en Endian



Fuente: Autoría propia

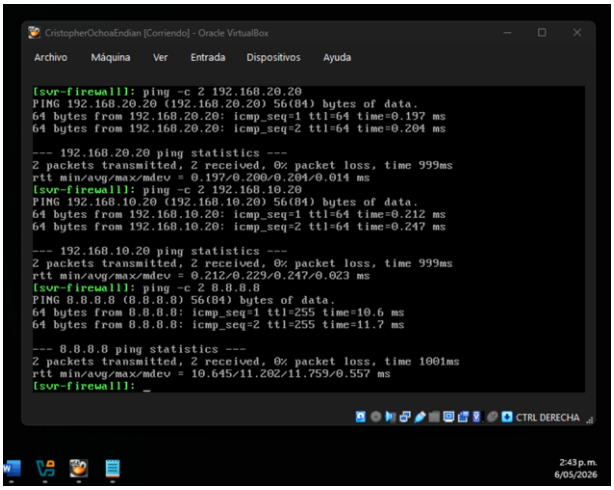
Se realiza la validación de la configuración de las zonas del firewall Endian las cuales corresponden a las siguientes.

- Eeth0: se configuro con la dirección IP estática 192.168.20.15/24, la cual se encuentra conectada a la red interna LAN (VERDE) donde esta Ubuntu Desktop quien tiene la dirección IP 192.168.20.20.

- Eeth1: se configuro con la dirección IP estática 192.168.10.15/24, la cual se encuentra conectada a la red interna DMZ (NARANJA) donde esta Ubuntu Server quien tiene la dirección IP 192.168.10.20.

- Eht2: se configuro con DHCP quien tiene una dirección IP dinámica 10.0.4.15/24, la cual proporciona el acceso a internet mediante el adaptador NAT.

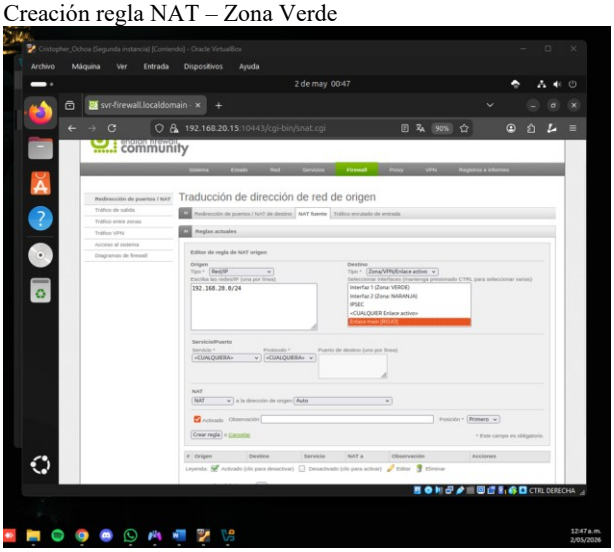
Figura 9.
Validación de conexión desde Endian



Fuente: Autoría propia

Se realizó la validación de la conectividad desde el firewall Endian con el comando ping hacia LAN (Verde) con IP 192.168.20.20, DMZ (Naranja) con IP 192.168.10.20 hacia la dirección IP 8.8.8.8 mediante la interfaz WAN (Roja) donde se obtiene una respuesta exitosa en todos los casos validando así el correcto funcionamiento de todas las interfaces.

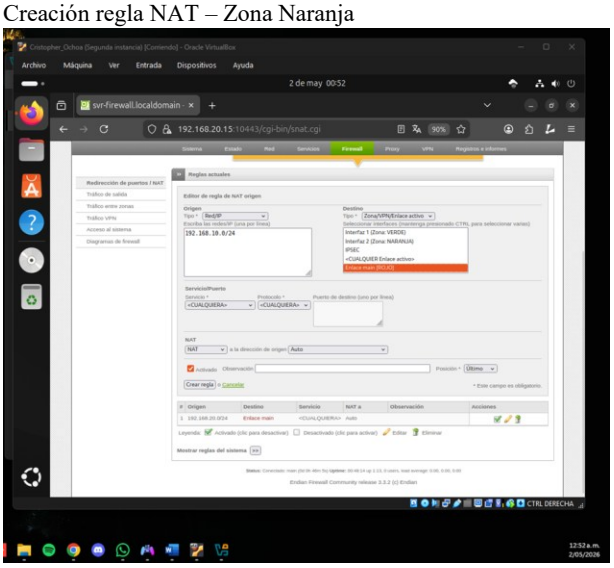
Figura 10.
Creación regla NAT – Zona Verde



Fuente: Autoría propia

Una vez instalado y configurado Endian, se ingresa desde el explorador de Ubuntu Desktop mediante la URL https://192.168.20.15:10443 donde una vez colocadas las credenciales dará accedo a la interfaz de Endian, una vez allí, se dirige a Firewall – NAT Fuente donde se realiza la creación de una regla de NAT de origen en Endian así como se muestra en la captura de pantalla, lo que permitiría a los equipos de la red 192.168.20.0/24 LAN (zona Verde) poder acceder a la red externa (zona roja).

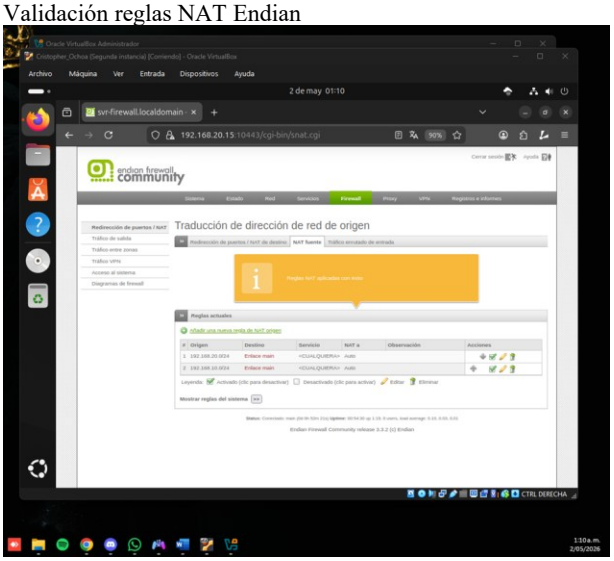
Figura 11.
Creación regla NAT – Zona Naranja



Fuente: Autoría propia

Se realiza la creación de una regla de NAT de origen en Endian, así como se muestra en la captura de pantalla, lo que permite a los equipos de la red 192.168.10.0/24 DMZ (zona Naranja) acceder a la red externa (WAN) mediante masquerade. Esta configuración posibilita la traducción de las direcciones IP privadas de la DMZ hacia una dirección pública para permitir la comunicación con Internet. Además, la regla garantiza que el tráfico proveniente de los servidores ubicados en la zona desmilitarizada pueda salir de manera controlada a través del firewall Endian, manteniendo la segmentación y seguridad de la red.

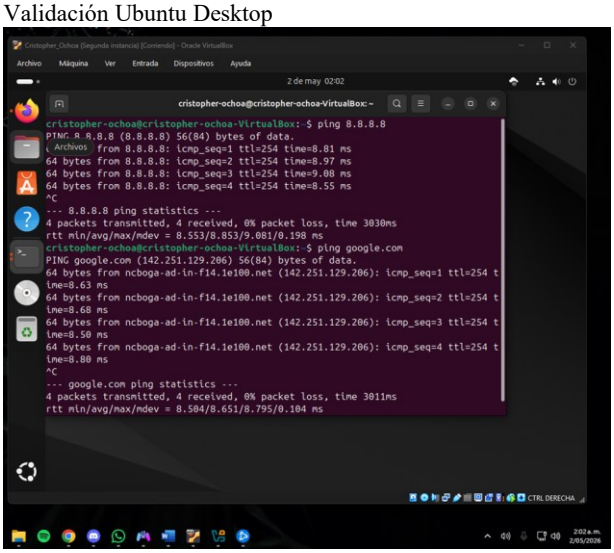
Figura 12.
Validación reglas NAT Endian



Fuente: Autoría propia

Se verifica la correcta creación de las reglas de traducción de dirección de origen configuradas para las redes 192.168.20.0/24 correspondiente a la zona VERDE y 192.168.10.0/24 correspondiente a la zona NARANJA. Ambas reglas tienen como destino el enlace MAIN, permiten cualquier servicio y utilizan NAT automático para realizar la traducción de direcciones IP privadas hacia la red externa.

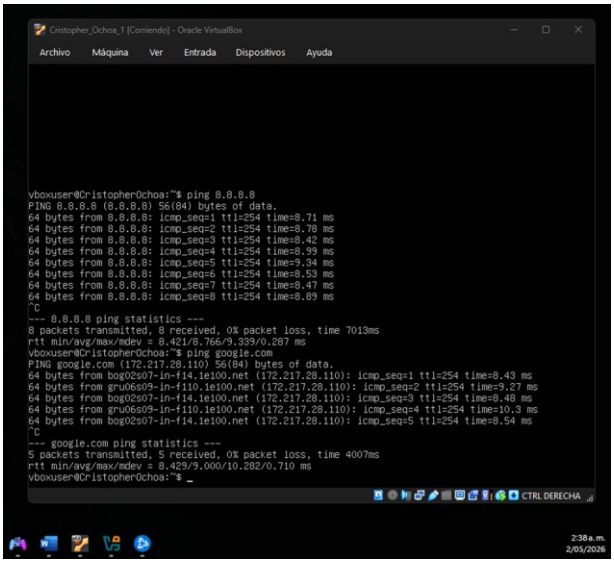
Figura 13.
Validación Ubuntu Desktop



Fuente: Autoría propia

Se realiza la prueba de conectividad desde el equipo Ubuntu Desktop con dirección IP 192.168.20.20 (LAN) hacia Internet, utilizando los comandos ping a las direcciones 8.8.8.8 y google.com. Con esta prueba se verifica la correcta salida del tráfico a través del firewall Endian, confirmando el funcionamiento de las reglas de NAT configuradas.

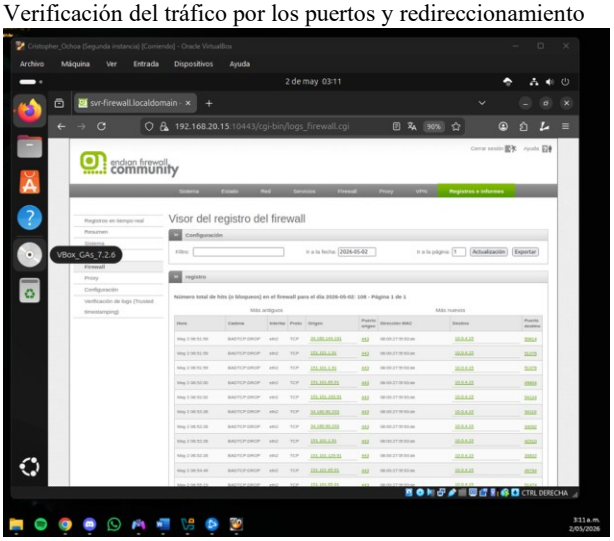
Figura 14.
Validación Ubuntu Server



Fuente: Autoría propia

Se realiza la prueba de conectividad desde el servidor Ubuntu Server con dirección IP 192.168.10.20 (DMZ) hacia Internet, mediante los comandos ping a 8.8.8.8 y google.com. Esta validación permite comprobar que el tráfico de la zona DMZ es correctamente traducido y gestionado por el firewall Endian, evidenciando el correcto funcionamiento de la configuración de NAT.

Figura 15.
Verificación del tráfico por los puertos y redireccionamiento



Fuente: Autoría propia

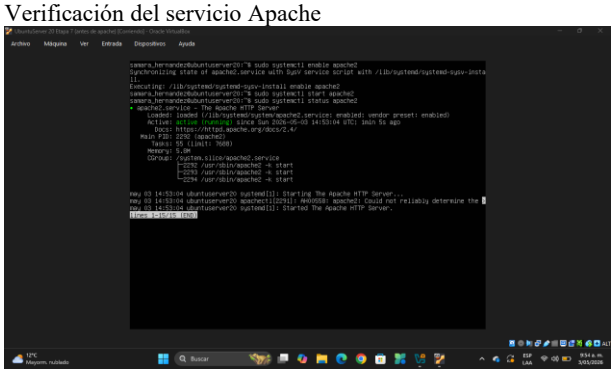
Se realiza la verificación del funcionamiento del firewall mediante el visor de registros de Endian, donde se evidencia el bloqueo de tráfico entrante no autorizado desde direcciones externas hacia la red interna. Esto confirma que el firewall no solo permite la salida controlada mediante NAT, sino que también protege la infraestructura frente a intentos de conexión no permitidos.

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

Con el propósito de implementar una arquitectura de red segmentada y con control estricto del tráfico, se definieron políticas de filtrado entre la zona interna (verde) y la zona desmilitarizada (DMZ o zona naranja), orientadas a habilitar únicamente servicios esenciales y limitar protocolos no necesarios. En este contexto, se permitió el acceso a los servicios HTTP (puerto 80) y FTP (puerto 21) sobre un servidor Ubuntu ubicado en la DMZ, mientras que se restringió el protocolo ICMP como medida de mitigación frente a actividades de reconocimiento. Esta configuración garantiza la disponibilidad de servicios críticos bajo un esquema de acceso controlado, reduciendo la exposición de la infraestructura ante accesos no autorizados.

Como etapa previa a la aplicación de las reglas, fue importante verificar que los servicios Apache y FTP se encontraran activos y correctamente configurados en el servidor. Asimismo, se creó un conjunto de credenciales para validar la conectividad al servicio FTP, confirmando la disponibilidad operativa de los servicios dentro de la red.

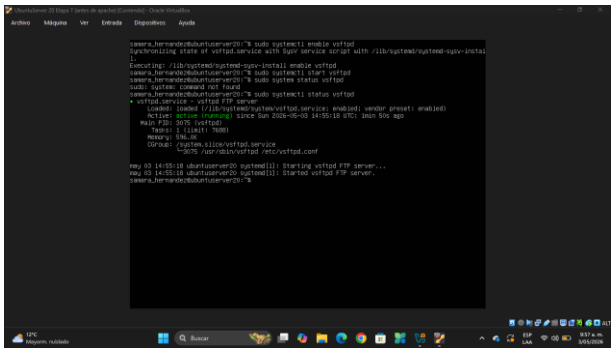
Figura 16.
Verificación del servicio Apache



Fuente: Autoría Propia

Se realiza la verificación del estado del servicio Apache en el servidor Ubuntu ubicado en la zona DMZ, con el fin de confirmar su correcto funcionamiento antes de aplicar las reglas de acceso desde la red interna. Esta validación permite comprobar que el servicio web se encuentra activo y disponible para atender solicitudes HTTP mediante el puerto 80.

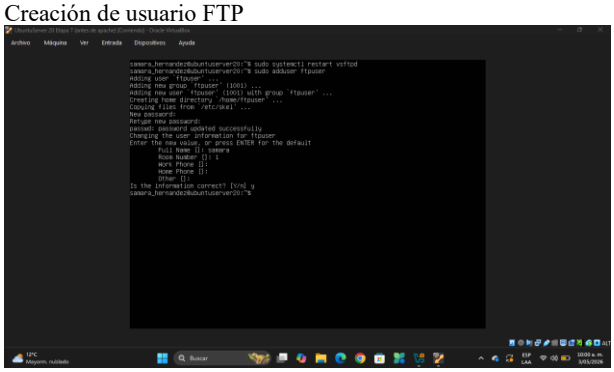
Figura 17.
Verificación del servicio FTP



Fuente: Autoría Propia

Se verifica también el funcionamiento del servicio FTP en el servidor Ubuntu de la zona DMZ, comprobando que el servicio se encuentre activo y preparado para aceptar conexiones remotas. Esta validación resulta necesaria para garantizar posteriormente el acceso controlado desde la red interna mediante el puerto 21.

Figura 18.
Creación de usuario FTP



Fuente: Autoría Propia

Igualmente es importante realizar la creación de un usuario y contraseña para el servicio FTP con el propósito de validar más adelante la autenticación y el acceso remoto al servidor ubicado en la DMZ. Estas credenciales permitirán realizar pruebas de conexión y transferencia de archivos, verificando el correcto funcionamiento del servicio configurado en el entorno virtualizado.

En este marco, se definieron políticas orientadas a habilitar únicamente los servicios requeridos, en concordancia con el principio de mínimo privilegio. El uso de HTTP responde a la necesidad de proporcionar acceso a interfaces web alojadas en la DMZ [6], mientras que FTP facilita la gestión remota de archivos en el servidor [7]. No obstante, ambos servicios representan posibles vectores de ataque si no son adecuadamente controlados, lo que justifica su habilitación mediante reglas específicas y limitadas.

Figura 19.
Regla de firewall para permitir HTTP y FTP en Endian

Fuente: Autoría Propia

A partir de lo anterior, la configuración de las reglas se llevó a cabo mediante la interfaz de administración del firewall Endian, donde se definieron políticas específicas de acceso entre zonas. Se estableció una regla que permite el tráfico TCP desde la zona verde hacia la zona naranja, restringiendo la comunicación exclusivamente a los puertos 80 y 21. Dicha regla fue establecida con protocolo TCP, acción de permitir (Allow) y registro de eventos activado (Logging). Esta configuración permite exponer servicios esenciales de forma controlada, garantizando su disponibilidad y evitando la apertura innecesaria de otros puertos que puedan ampliar la superficie de exposición del sistema

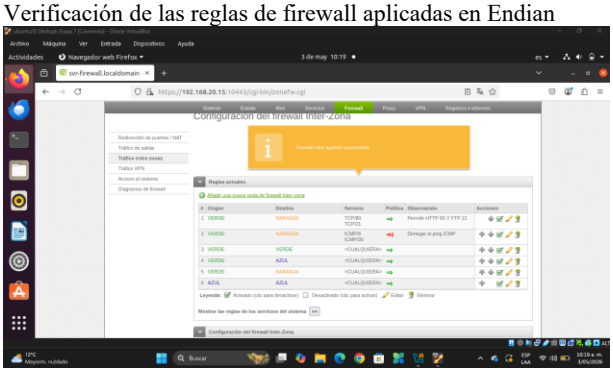
De forma complementaria, se implementó una política orientada a restringir el protocolo ICMP. En particular, se configuró una regla de denegación para los tipos 8 y 30, definiendo como origen la zona verde y como destino la zona naranja correspondiente al servidor, con acción de denegar (Deny) y registro de eventos activado. Esta decisión se fundamenta en la reducción de capacidades de descubrimiento de red, ya que la habilitación de ICMP puede facilitar la identificación de dispositivos activos y la inferencia de la topología de red [8].

Figura 20.
Regla de firewall para bloqueo de ICMP

Fuente: Autoría Propia

En la interfaz de administración de Endian se observa la configuración de la política de filtrado aplicada para el protocolo ICMP, donde se especifican las zonas involucradas, la acción de denegación y el registro de eventos asociado a la regla implementada. Esta configuración permite controlar las solicitudes de ping entre segmentos de red y fortalecer la seguridad del entorno implementado.

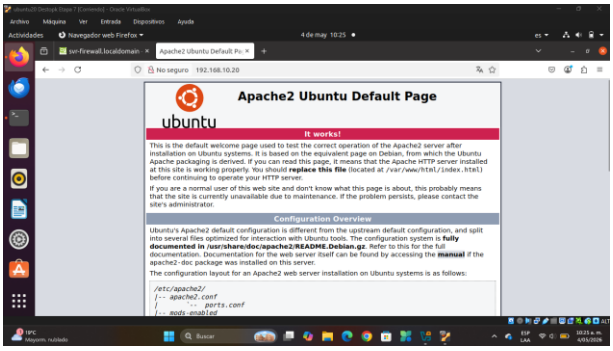
Figura 21.
Verificación de las reglas de firewall aplicadas en Endian



Fuente: Autoría Propia

En la interfaz de administración de Endian se observa que las reglas de firewall aparecen creadas y aplicadas correctamente dentro del listado de políticas configuradas. Además, se visualizan las acciones, servicios y zonas asociadas a cada regla, permitiendo verificar su correcta implementación dentro de la infraestructura de red.

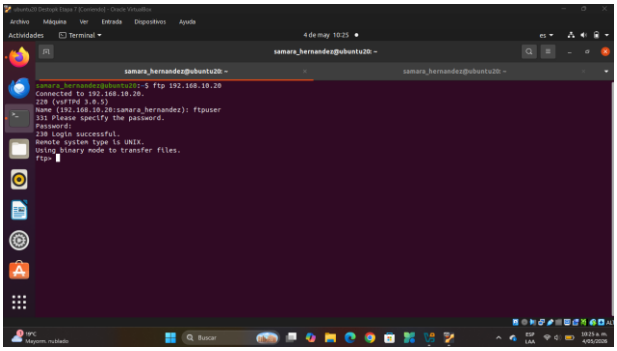
Figura 22.
Acceso HTTP exitoso desde el cliente



Fuente: Autoría Propia

Una vez aplicadas las reglas, se realizaron pruebas de validación desde un cliente ubicado en la zona verde. Se verificó el acceso al servicio HTTP mediante un navegador web, evidenciando así la correcta carga de la página predeterminada del servidor Apache. Esta validación permitió confirmar el correcto funcionamiento de las políticas configuradas en el firewall.

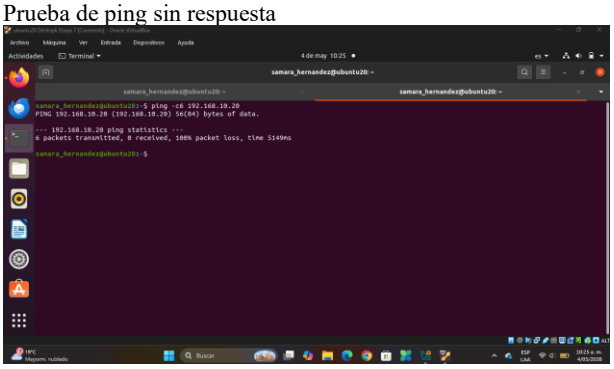
Figura 23.
Conexión FTP exitosa



Fuente: Autoría Propia

De igual forma, se estableció una conexión FTP utilizando credenciales previamente configuradas, confirmando la funcionalidad del servicio. Además, se verificó que el acceso a los servicios habilitados en la DMZ se realiza de manera controlada a través de las reglas implementadas en Endian.

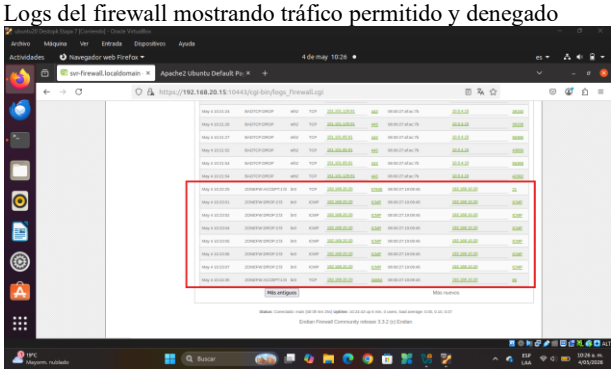
Figura 24.
Prueba de ping sin respuesta



Fuente: Autoría Propia

En contraste, al ejecutar pruebas de conectividad mediante el comando ping hacia la dirección IP del servidor en la DMZ, no se obtuvo respuesta, lo que confirma la correcta aplicación del bloqueo del protocolo ICMP. Esto permite evidenciar que las políticas de restricción configuradas en el firewall están funcionando correctamente dentro de la infraestructura de red implementada.

Figura 25.
Logs del firewall mostrando tráfico permitido y denegado



Fuente: Autoría Propia

Adicionalmente, se realizó un análisis de los registros generados por el firewall, donde se evidenció tráfico permitido (ACCEPT) para los servicios HTTP y FTP, así como tráfico denegado (DROP) asociado a paquetes ICMP. Este monitoreo permite validar el comportamiento del sistema y aporta capacidades de auditoría para la identificación de eventos relevantes.

En síntesis, la configuración implementada adquiere especial relevancia en entornos empresariales, donde la disponibilidad de servicios debe integrarse con mecanismos sólidos de protección. El uso de segmentación de red junto con un control granular del tráfico permite que cada zona opere bajo políticas claramente definidas, limitando los servicios accesibles y reduciendo puntos de exposición del sistema. Bajo este enfoque, la habilitación controlada de servicios como HTTP y FTP garantiza la operación de funciones críticas en condiciones seguras, mientras que la restricción del protocolo ICMP contribuye a disminuir la exposición frente a procesos de exploración y análisis de red. Asimismo, esta arquitectura puede evolucionar hacia implementaciones más avanzadas que integren sistemas de monitoreo continuo, detección de intrusiones (IDS/IPS) o políticas de seguridad automatizadas, constituyendo una base sólida para el desarrollo de infraestructuras resilientes y seguras en contextos organizacionales.

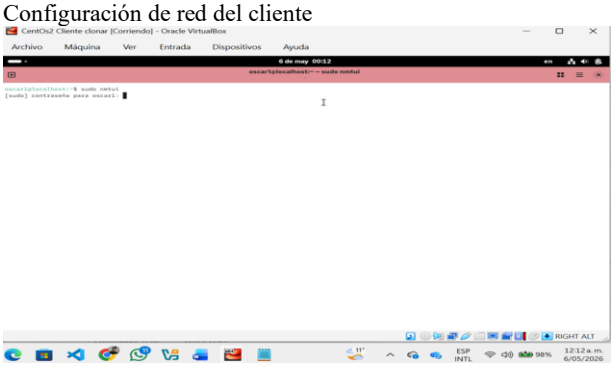
5 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La implementación de reglas de acceso y control de tráfico en GNU/Linux Endian permite administrar de manera segura la comunicación entre las diferentes zonas de red definidas dentro de la infraestructura virtualizada. En esta práctica se configuraron políticas de acceso entre las zonas LAN (VERDE), WAN (ROJA) y DMZ (NARANJA), permitiendo únicamente el tráfico autorizado mediante los protocolos HTTP y FTP.

Inicialmente se realizó la configuración de direccionamiento IP tanto en la máquina cliente como en el servidor GNU/Linux utilizando herramientas de administración de red en Ubuntu y CentOS. Posteriormente se verificó la conectividad entre las diferentes zonas mediante

pruebas de comunicación utilizando comandos de red hacia el firewall Endian.

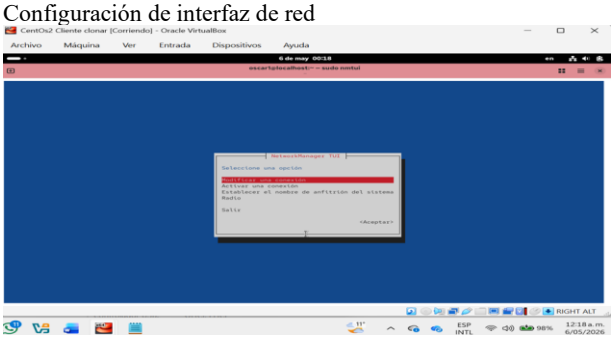
Figura 26.
Configuración de red del cliente



Fuente: Autoría propia

Para la configuración de red se utilizó la herramienta de administración de conexiones de red del sistema GNU/Linux, permitiendo establecer direcciones IP estáticas y parámetros de conectividad necesarios para la comunicación entre las diferentes zonas administradas por la herramienta Endian.

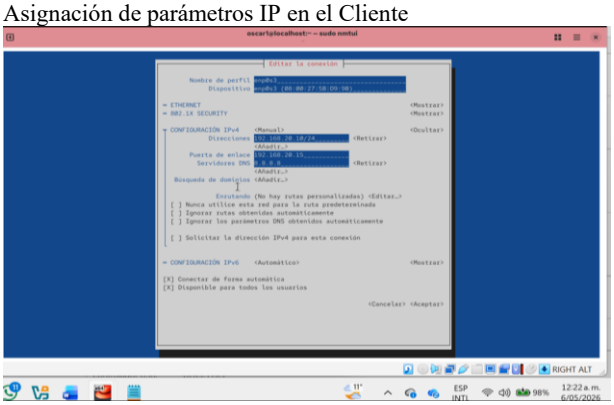
Figura 27.
Configuración de interfaz de red



Fuente: Autoría propia

Se verificó la interfaz de red configurada en la máquina virtual y posteriormente se asignaron los parámetros de conectividad correspondientes. Esta validación permitió comprobar que la interfaz estuviera correctamente vinculada al segmento de red asignado dentro de VirtualBox y preparada para establecer comunicación con el firewall Endian.

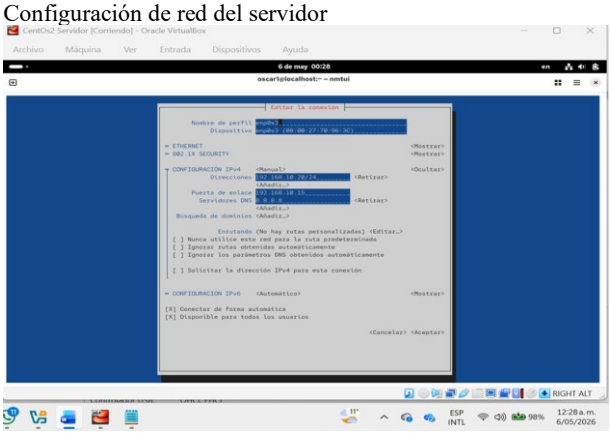
Figura 28.
Asignación de parámetros IP en el Cliente



Fuente: Autoría propia

Se estableció la dirección IP estática y la máscara de red necesarias para la comunicación dentro de la zona LAN. Asimismo, se configuró la puerta de enlace correspondiente al firewall Endian para permitir el acceso a otras redes y servicios autorizados. Esta configuración garantiza una correcta comunicación entre el cliente y los demás dispositivos de la infraestructura.

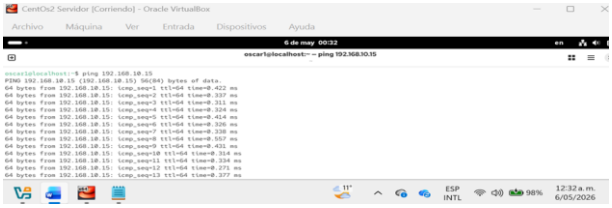
Figura 29.
Configuración de red del servidor



Fuente: Autoría propia

Se realizó la configuración de red en la máquina servidor ubicada en la zona DMZ para permitir la comunicación con el firewall. Durante este proceso se asignaron los parámetros de direccionamiento IP correspondientes al segmento de red de la zona ORANGE. Esta configuración permite mantener una correcta identificación y administración del servidor dentro de la infraestructura virtualizada.

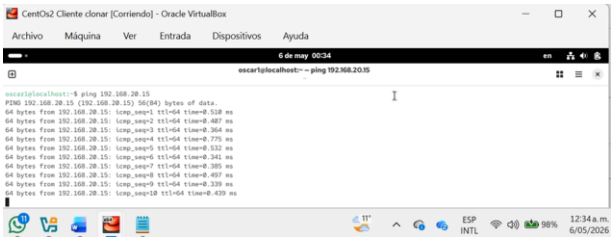
Figura 30.
Prueba de conectividad desde el servidor hacia Endian



Fuente: Autoría propia

Se verificó la conectividad entre el servidor y el firewall Endian mediante pruebas de comunicación utilizando comandos de red. Estas pruebas permitieron comprobar que la configuración de red aplicada en la zona DMZ funciona correctamente. Además, se validó que el servidor puede establecer comunicación con el firewall sin inconvenientes de conectividad.

Figura 31.
Prueba de conectividad desde el cliente hacia Endian

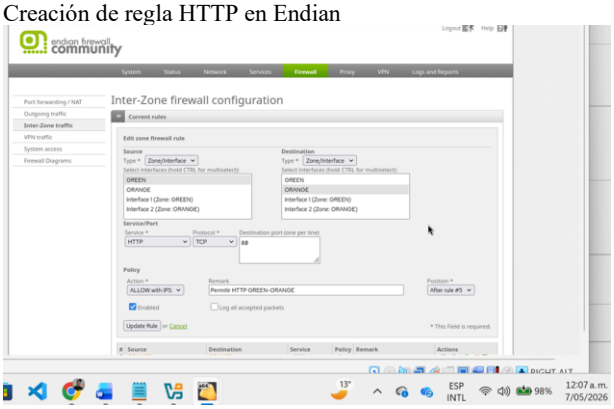


Fuente: Autoría propia

Se validó la comunicación entre la máquina cliente y el firewall comprobando la correcta respuesta de conectividad. Esta prueba permitió confirmar que la configuración de direccionamiento IP en la zona VERDE fue realizada correctamente. Asimismo, se verificó que el cliente puede comunicarse adecuadamente con la infraestructura administrada por Endian.

Una vez validada la conectividad entre las zonas de red, se ingresó a la interfaz administrativa de Endian Community para realizar la creación de reglas Inter-Zona. Se habilitaron políticas de firewall permitiendo tráfico HTTP y FTP desde la zona VERDE hacia la zona NARANJA, autorizando el acceso controlado a los servicios publicados en la DMZ.

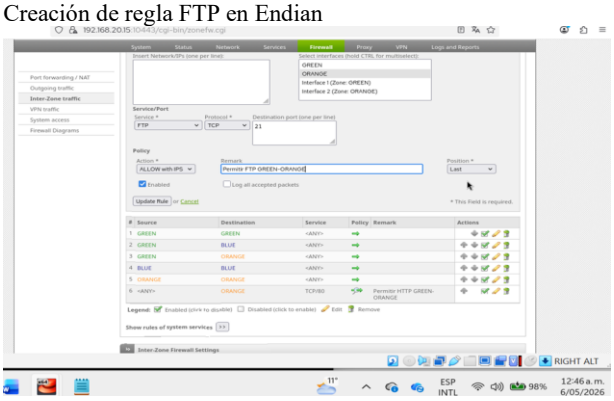
Figura 32.
Creación de regla HTTP en Endian



Fuente: Autoría Propia

Se configuró una regla de firewall permitiendo tráfico HTTP desde la zona VERDE hacia la zona NARANJA. Esta política permite el acceso al servicio web alojado en el servidor de la DMZ mediante el puerto 80 utilizando el protocolo TCP. Además, la regla facilita el acceso controlado al contenido publicado en el servidor sin habilitar otros servicios no autorizados.

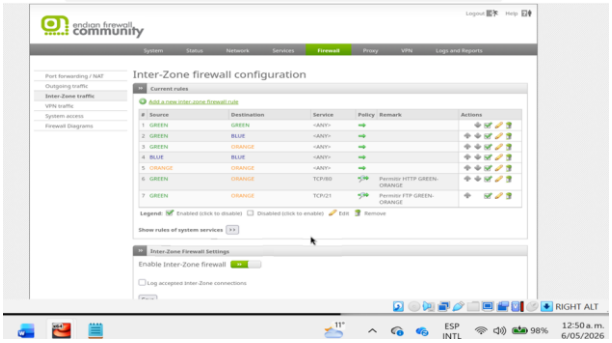
Figura 33.
Creación de regla FTP en Endian



Fuente: Autoría propia

Se habilitó el protocolo FTP mediante reglas Inter-Zona para permitir transferencia de archivos entre redes autorizadas. La configuración realizada permite el acceso desde la zona VERDE hacia el servidor ubicado en la zona NARANJA mediante el puerto 21. Asimismo, esta política facilita la comunicación controlada con el servicio FTP manteniendo el filtrado y administración del tráfico desde el firewall Endian.

Figura 34.
Verificación de reglas configuradas en Endian

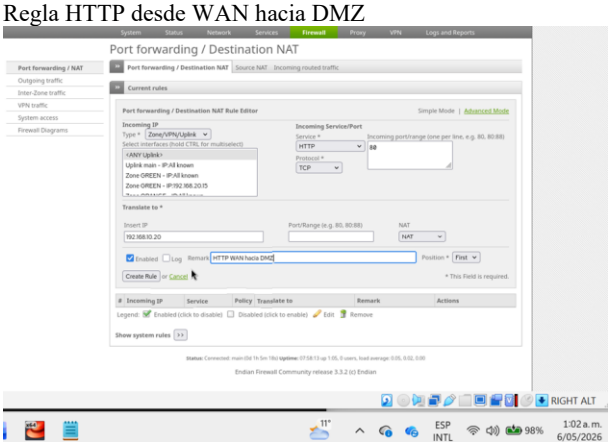


Fuente: Autoría propia

En la interfaz administrativa de Endian se visualizan las reglas de firewall configuradas para el control del tráfico entre las diferentes zonas de red. En esta sección se verifica que las políticas correspondientes a los servicios HTTP y FTP se encuentran creadas y habilitadas correctamente, permitiendo validar su correcta aplicación dentro de la infraestructura implementada.

Posteriormente se configuró la comunicación entre la zona WAN y la zona DMZ mediante reglas específicas de acceso HTTP, permitiendo el ingreso controlado desde Internet hacia los servicios alojados en el servidor de la zona desmilitarizada.

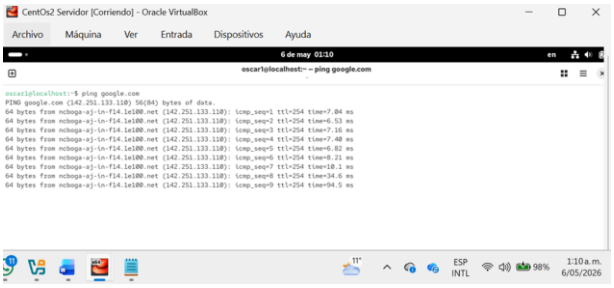
Figura 35.
Regla HTTP desde WAN hacia DMZ



Fuente: Autoría propia

Se creó una política de acceso HTTP permitiendo la comunicación desde la zona WAN hacia la DMZ. Esta configuración permite el acceso controlado desde redes externas hacia el servidor web ubicado en la zona desmilitarizada mediante el puerto 80.

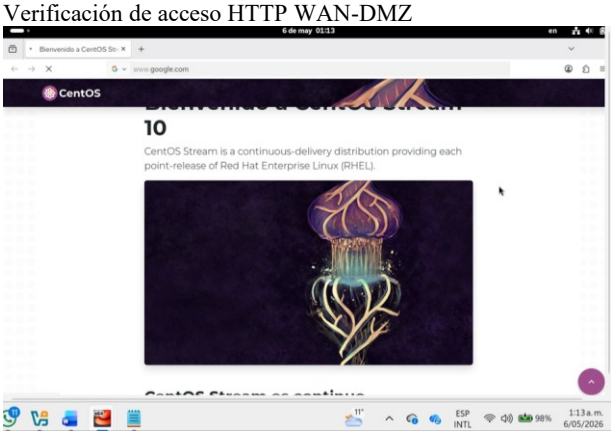
Figura 36.
Validación de conectividad WAN hacia DMZ



Fuente: Autoría propia

Se verificó la correcta comunicación entre la red WAN y el servidor ubicado en la zona desmilitarizada. Esta validación permitió comprobar que las reglas de firewall configuradas permiten el tráfico autorizado desde redes externas hacia los servicios publicados en la DMZ.

Figura 37.
Verificación de acceso HTTP WAN-DMZ



Fuente: Autoría propia

Se comprobó el funcionamiento de la regla HTTP configurada para el acceso desde Internet hacia la DMZ. Mediante esta prueba se verificó que el servicio web alojado en el servidor responde correctamente a solicitudes provenientes de la zona WAN. Esto permitió validar la correcta publicación del servicio HTTP a través del firewall Endian.

Figura 38.
Verificación de reglas Inter-Zona

Fuente: Autoría propia

Se validó la existencia de las reglas de tráfico configuradas entre las diferentes zonas administradas por Endian. En esta sección se visualizan las políticas creadas para controlar la comunicación entre las zonas VERDE y NARANJA. Además, se comprobó que las reglas se encuentren habilitadas y funcionando correctamente dentro del firewall.

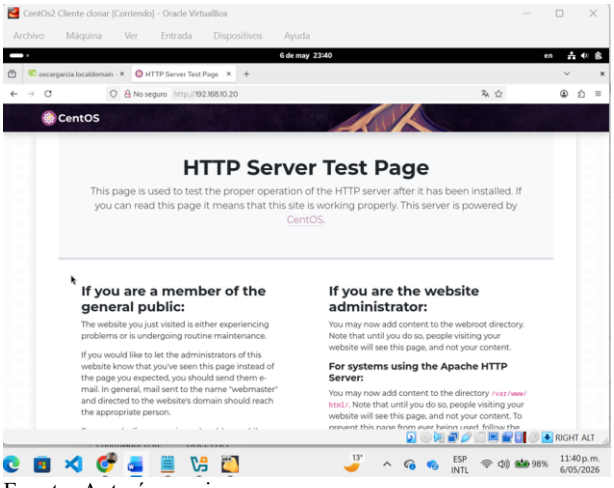
Figura 39.
Listado de reglas activas en Endian

Fuente: Autoría propia

Se visualizaron las políticas de acceso habilitadas dentro del firewall verificando su estado activo. La interfaz de administración permite identificar las reglas configuradas, los servicios autorizados y las zonas involucradas en cada política de tráfico. Esto facilita la validación y supervisión de las configuraciones aplicadas en Endian Firewall.

Finalmente, se realizan pruebas de acceso HTTP y FTP entre las diferentes zonas de red utilizando navegador web y terminal GNU/Linux, verificando el correcto funcionamiento de las reglas configuradas para permitir o denegar tráfico según las políticas establecidas.

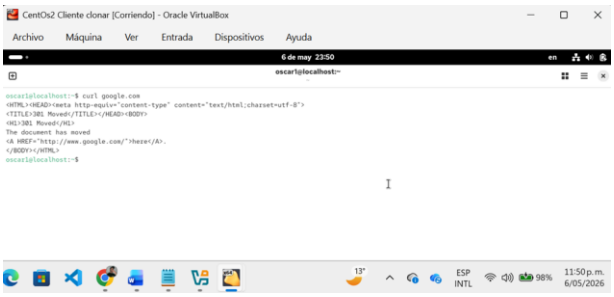
Figura 40.
Acceso HTTP desde LAN hacia DMZ



Fuente: Autoría propia

Se verificó la validación del acceso HTTP desde la red LAN hacia el servidor ubicado en la zona DMZ. La prueba se realizó mediante un navegador web desde el cliente de la zona VERDE, permitiendo comprobar que las reglas configuradas en Endian autorizan correctamente la comunicación hacia el servicio web publicado en el servidor.

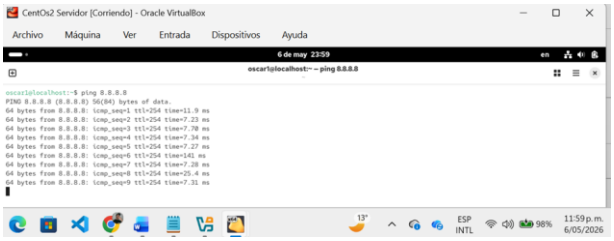
Figura 41.
Acceso HTTP desde LAN hacia WAN



Fuente: Autoría propia

Se comprobó la salida de tráfico HTTP desde la red LAN hacia Internet mediante el firewall Endian. Esta validación permitió verificar que las políticas de acceso configuradas autorizan correctamente la navegación y comunicación hacia servicios externos. Además, se confirmó el funcionamiento adecuado de las reglas de salida de tráfico.

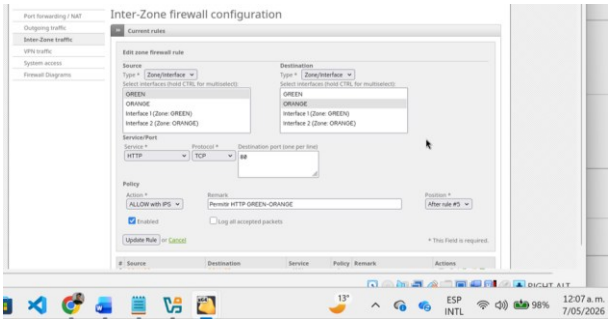
Figura 42.
Acceso HTTP desde DMZ hacia WAN



Fuente: Autoría propia

Se validó la comunicación del servidor de la DMZ hacia servicios externos en Internet. Esta prueba permitió comprobar que el servidor ubicado en la zona ORANGE puede establecer conexiones HTTP hacia redes externas mediante las reglas configuradas en Endian. Asimismo, se verificó el correcto funcionamiento de la conectividad desde la DMZ hacia la WAN.

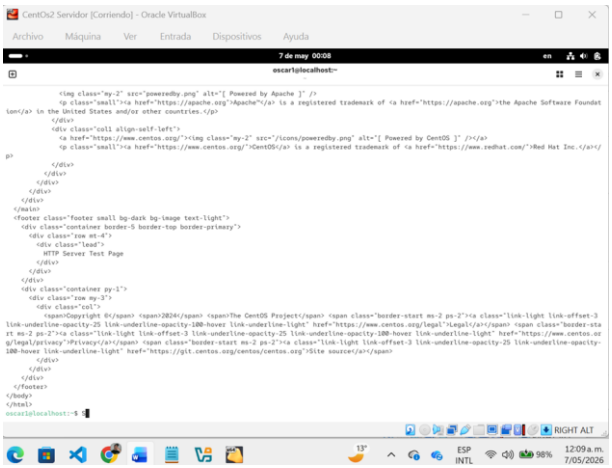
Figura 43.
Acceso HTTP desde WAN hacia DMZ



Fuente: Autoría propia

Se verificó el acceso desde la red WAN hacia los servicios HTTP configurados en la zona DMZ. La prueba permitió comprobar que el tráfico externo puede acceder de manera controlada al servidor web publicado mediante las reglas configuradas en el firewall. Además, se validó la correcta comunicación entre ambas zonas de red.

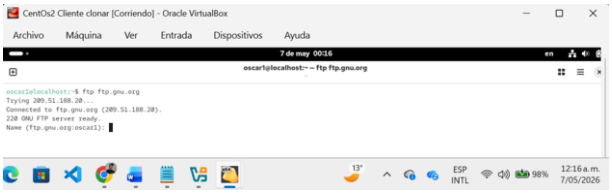
Figura 44.
Validación de servicio HTTP WAN-DMZ



Fuente: Autoría propia

Se comprobó el correcto funcionamiento del servicio web publicado mediante las reglas de firewall configuradas. Esta validación permitió evidenciar que las solicitudes HTTP provenientes de la zona WAN son procesadas correctamente por el servidor ubicado en la DMZ. Asimismo, se confirmó la disponibilidad del servicio a través del firewall Endian.

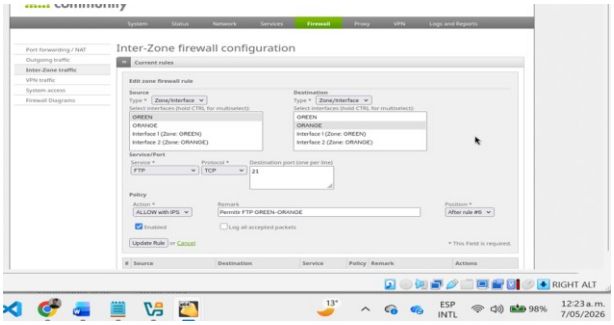
Figura 45.
Prueba FTP desde LAN hacia WAN



Fuente: Autoría propia

Se realizaron pruebas de conectividad FTP desde la red interna hacia servicios externos autorizados. Esta validación permitió comprobar el correcto funcionamiento de las políticas de tráfico configuradas para el protocolo FTP. Además, se verificó la capacidad de transferencia y comunicación entre la red LAN y servicios externos.

Figura 46.
Prueba FTP desde WAN hacia DMZ



Fuente: Autoría propia

Por último, se validó el funcionamiento de las políticas FTP permitiendo acceso desde la red WAN hacia la zona DMZ. La prueba permitió comprobar que las reglas configuradas en el firewall autorizan correctamente la comunicación hacia el servidor FTP publicado en la infraestructura. Asimismo, se verificó la disponibilidad y acceso controlado al servicio desde redes externas.

Los resultados obtenidos permitieron comprobar el correcto funcionamiento de las reglas de acceso implementadas en Endian Firewall Community, validando la comunicación autorizada entre las diferentes zonas de red mediante los protocolos HTTP y FTP. Asimismo, se evidenció la importancia de la segmentación de red y del control de tráfico como mecanismos fundamentales para fortalecer la seguridad perimetral en entornos GNU/Linux virtualizados.

6 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE)

La gestión del tráfico de red en entornos corporativos y académicos es un pilar fundamental de la ciberseguridad y la administración de recursos. La Temática 5 se centra en la implementación de un servidor Proxy HTTP en modo No Transparente utilizando la plataforma Endian Firewall Community Edition.

A diferencia de un proxy transparente, el modo no transparente requiere una configuración explícita en el cliente y permite un control más riguroso mediante desafíos de autenticación [9]. Este laboratorio integra tres componentes críticos:

Filtrado de contenido: El despliegue de perfiles de seguridad mediante Blacklists para restringir el acceso a dominios específicos.

Gestión de identidades: La configuración de un servicio de autenticación local bajo el estándar NCSA, garantizando que solo usuarios autorizados puedan establecer conexiones externas.

Políticas de acceso: La orquestación de reglas que vinculan identidades de usuario con perfiles de filtrado.

A continuación, se detalla el proceso técnico de configuración, desde la definición de las listas de bloqueo hasta la validación de la arquitectura desde una estación de trabajo Ubuntu Desktop, demostrando la eficacia del sistema para interceptar y validar peticiones de red en tiempo real.

Figura 47.
Implementación y parametrización del servicio Proxy HTTP

Fuente: Autoría propia

Se procedió con la activación del servicio de Proxy HTTP para las zonas VERDE y NARANJA. Se estableció el modo de operación 'not transparent', configurando el puerto 8080 como puerto de escucha. Esta parametrización garantiza que el tráfico web sea canalizado de forma explícita hacia el servidor de seguridad, permitiendo la ejecución de los mecanismos de filtrado de contenido y auditoría de red.

Figura 48.
Configuración de perfiles de filtrado de contenido

Fuente: Autoría propia

Se accedió al módulo Web Filter para la configuración del perfil de navegación denominado 'Filtro_Restringido'. En esta etapa se parametrizó la Blacklist (lista negra), definiendo los dominios específicos sujetos a restricciones de acceso. Este perfil actúa como el conjunto de reglas de filtrado que será vinculado posteriormente a las políticas de acceso del servidor.

Figura 49.
Configuración de listas de control de acceso (Blacklist)

Fuente: Autoría propia

Se realizó la configuración de la Blacklist (Lista Negra) bajo el perfil 'Filtro_Restringido', donde se definieron los dominios de destino sujetos a restricción. El proceso concluyó con la persistencia de los cambios y la ejecución del comando 'Apply', garantizando la actualización inmediata de las políticas de filtrado en el motor del firewall y la entrada en vigor de las restricciones sobre el tráfico saliente.

Figura 50.
Definición y estructura de grupos

Fuente: Autoría propia

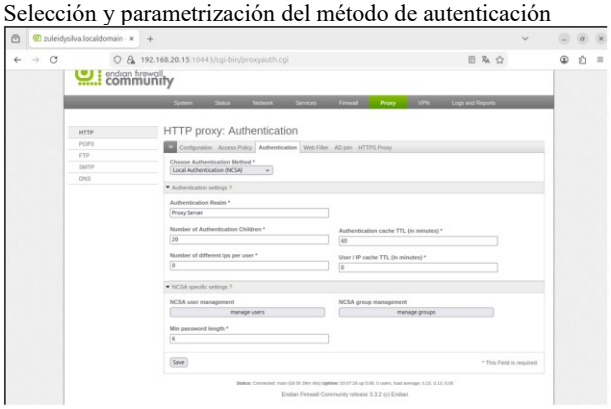
Se realizó la creación del contenedor lógico denominado 'Grupo_Internet'. Esta unidad organizativa se estableció con el propósito de centralizar la administración de las políticas de navegación, permitiendo una gestión escalable y organizada mediante la aplicación de perfiles de seguridad colectivos.

Figura 51.
Aprovisionamiento de usuarios y credenciales

Fuente: Autoría propia

Posteriormente, se procedió con el registro del usuario 'zuleidysilva_user', efectuando su vinculación inmediata al grupo previamente definido. Durante esta etapa, se parametrizó una credencial de acceso segura para la autenticación NCSA, garantizando la integridad del proceso de validación de identidad en el servidor Proxy.

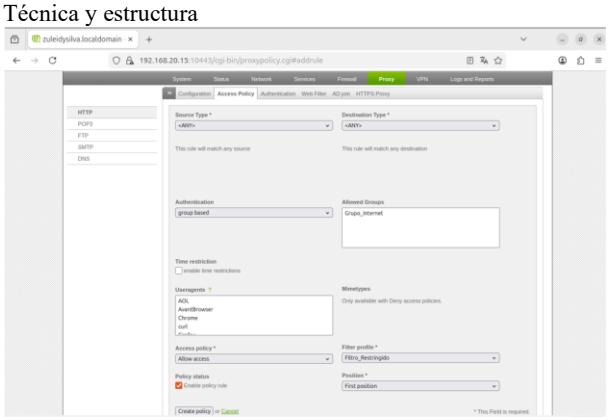
Figura 52.
Selección y parametrización del método de autenticación



Fuente: Autoría propia

Se estableció el esquema de autenticación en modo Local (NCSA), procediendo con la persistencia de la configuración en el sistema. Esta parametrización faculta al firewall para realizar la validación de credenciales de usuario mediante una compulsa contra su base de datos interna. De este modo, se garantiza un control de acceso granular al servicio de proxy, supeditando la navegación a la autenticación exitosa de los sujetos de red previamente registrados.

Figura 53.
Técnica y estructura



Fuente: Autoría propia

Se procedió con la configuración de la Access Policy para la consolidación de los servicios de seguridad. Se implementó una directiva de tipo 'group based' asociada al 'Grupo_Internet', vinculándola de forma unívoca con el perfil de filtrado 'Filtro_Restringido'. Al asignar a esta regla la prioridad máxima en el orden jerárquico, se garantiza que el firewall intercepte las peticiones de manera preferente, forzando la autenticación de usuarios y la aplicación de las restricciones de la Blacklist sobre todo el tráfico originado en la red local.

Figura 54.
Validación de resultados y comportamiento del sistema

Fuente: Autoría propia

La fase de validación funcional se ejecutó mediante pruebas de acceso desde la estación de trabajo perteneciente a la zona LAN (VERDE). Como se evidencia en la captura de pantalla, al iniciar una solicitud de navegación, el agente de usuario despliega un desafío de autenticación para la captura de credenciales. Este comportamiento confirma que la Access Policy intercepta el tráfico de forma efectiva, supeditando la conectividad a una validación de identidad obligatoria antes de autorizar el tránsito de datos hacia la red externa.

Figura 55.
Evaluación de denegación de acceso a dominios restringidos

Fuente: Autoría propia

Se ejecutó la validación de conectividad hacia el dominio www.hotmail.com desde el nodo cliente. Tras la resolución del desafío de identidad, el motor de Endian Firewall interceptó la trama de datos y generó una respuesta de error del tipo 'Access Denied'. Esta evidencia empírica confirma la operatividad del servidor Proxy en la aplicación de políticas de restricción; validando que el sistema deniega el tránsito de paquetes de forma explícita hacia los dominios indexados en la Blacklist del perfil de filtrado.

7 CONCLUSIONES

En primer lugar, la correcta configuración del Endian Firewall permitió generar un entorno capaz de gestionar de manera efectiva las interfaces de red, aspecto fundamental para disponer de una infraestructura segura y funcional. Asimismo, el equilibrio alcanzado entre las tres zonas (verde, roja y naranja) contribuyó a garantizar seguridad y confiabilidad tanto para el entorno de los usuarios como para el tráfico de la red. De igual manera, fue posible establecer una conexión estable a internet y brindar mayor seguridad durante la navegación, además de implementar servicios que permitieron disponer de un servidor multifacético y confiable.

En segundo lugar, el establecimiento de las dos reglas NAT en Endian Firewall permitió una correcta comunicación entre la LAN (Verde), representada mediante Ubuntu Desktop, y la DMZ (Naranja), representada con Ubuntu Server, ambas con acceso a internet. Todo esto fue realizado en un entorno virtualizado, donde Endian también ejecutó un adecuado control del tráfico. Asimismo, se pudo comprender la importancia que tiene NAT en la administración de redes, ya que contribuye a la seguridad de la infraestructura al controlar los accesos y denegar el paso a usuarios no autorizados, además de monitorear todas las conexiones existentes. De esta manera, se evidenció cómo el uso de herramientas de seguridad y control resulta fundamental para el correcto funcionamiento y protección de una red.

Por otra parte, la configuración de la zona DMZ mediante reglas de filtrado específicas permitió habilitar de forma controlada los servicios HTTP y FTP, garantizando su disponibilidad sin comprometer la seguridad del entorno. Asimismo, la restricción del protocolo ICMP demostró ser efectiva para limitar la exposición de información sobre la red. Los resultados obtenidos, validados mediante pruebas de conectividad y análisis de registros, evidencian la correcta implementación de las políticas definidas. En este sentido, la aplicación de principios como el mínimo privilegio y la

segmentación de red contribuye a fortalecer el control del tráfico entre zonas y a reducir riesgos operativos. Adicionalmente, el uso de soluciones basadas en software de código abierto confirma su viabilidad como alternativa eficiente y flexible para la implementación de mecanismos de seguridad en entornos empresariales.

De igual manera, la implementación de reglas de acceso y control de tráfico mediante Endian Firewall permitió validar el correcto funcionamiento de la comunicación entre las zonas LAN, WAN y DMZ dentro de la infraestructura virtualizada. A través de la configuración de políticas Inter-Zona para los protocolos HTTP y FTP, se logró establecer un control seguro sobre el tráfico de red, permitiendo únicamente las conexiones autorizadas entre los diferentes segmentos. Las pruebas realizadas desde cliente, servidor y red externa confirmaron la efectividad de las reglas implementadas y el adecuado funcionamiento de los servicios configurados. Asimismo, los resultados evidencian la importancia de la segmentación de red y de las políticas de filtrado como mecanismos fundamentales para fortalecer la seguridad perimetral y proteger los servicios publicados en entornos GNU/Linux virtualizados.

Finalmente, la integración del servidor Proxy HTTP no transparente mediante Endian Firewall permitió validar la eficacia de la arquitectura de seguridad perimetral en la gestión del tráfico saliente. Mediante la integración del método de autenticación NCSA y la configuración de perfiles de filtrado basados en Blacklists, se logró establecer un control granular sobre el acceso a la red, donde la correcta jerarquización de las Access Policies garantizó que las restricciones se aplicaran de forma prioritaria y obligatoria. Los resultados obtenidos en la fase de pruebas confirman que el sistema no solo mitiga el acceso a dominios no autorizados, sino que asegura la trazabilidad y la autenticación unívoca de los usuarios, cumpliendo satisfactoriamente con los objetivos de administración y seguridad propuestos para esta infraestructura de red.

8 REFERENCIAS

[1] M. Rash, *Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort*, O'Reilly Media, pp. 47–80, 2007.

[2] W. Cheswick, S. Bellovin and A. Rubin, *Firewalls and Internet Security*, 2nd ed., Addison-Wesley, pp. 12–15, 2003.

[3] Oracle Corporation, *Oracle VM VirtualBox User Manual*, pp. 59–141, 2024. [En línea]. Disponible en: Oracle VM VirtualBox User Guide for Release 7.0

[4] Endian, *Endian UTM 3.2 Reference Manual*, ver. 3.2, pp. 87–126, 2016. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/index.html

[5] P. Srisuresh and M. Holdrege. (1999, agosto). *IP Network Address Translator (NAT) Terminology and Considerations* (RFC 2663), pp. 1–16 [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc2663

[6] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach et al. (1999, junio). *Hypertext Transfer Protocol -- HTTP/1.1* (RFC 2616), pp. 11–20 [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc2616

[7] J. Postel and J. Reynolds (1985, octubre). *File Transfer Protocol (FTP)* (RFC 959), pp. 1–8 [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc959

[8] J. Postel (1981, septiembre). *Internet Control Message Protocol* (RFC 792), pp. 1–6 [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc792

[9] D. Gourley, B. Totty, M. Sayer, A. Aggarwal and S. Reddy, *HTTP: The Definitive Guide*, O'Reilly Media, pp. 129–160, 2002.