IMPLEMENTACIÓN COLABORATIVA DE SEGURIDAD PERIMETRAL EN ENTORNOS GNU/LINUX MEDIANTE ENDIAN FIREWALL

Andrés Jesús Padilla López
e-mail: ajpadillal@unadvirtual.edu.co
Jesús Antonio Bolaño Guerrero
e-mail: jbolanog@unadvirtual.edu.co
Juan Sebastián Arrieta Pineda
e-mail: jsarrietap@unadvirtual.edu.co
Leonardo Moreno Soto
e-mail: lmorenoso@unadvirtual.edu.co
Robertson José Ortega Peña
e-mail: rdortegap@unadvirtual.edu.co

RESUMEN: *Este artículo describe la implementación colaborativa de un esquema de seguridad perimetral en redes LAN, WAN y DMZ utilizando la distribución GNU/Linux Endian Firewall (EFW). La práctica se desarrolló en entornos virtualizados con VirtualBox, integrando servidores Ubuntu/Debian, Ubuntu 24 y aplicando configuraciones de NAT, reglas de acceso inter-zonas, servicios HTTP/FTP y un proxy HTTP con autenticación. Los resultados evidencian la correcta segmentación de la red y la protección de servidores críticos, garantizando la integridad de bases de datos y aplicaciones. El trabajo se complementa con ejercicios del LPI 101 [1], fortaleciendo competencias en administración de sistemas operativos y seguridad informática*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, Seguridad Perimetral

ABSTRACT: This article describes the collaborative implementation of a perimeter security scheme in LAN, WAN, and DMZ networks using the GNU/Linux Endian Firewall (EFW) distribution. The practice was carried out in virtualized environments with VirtualBox, integrating Ubuntu/Debian and Ubuntu 24 servers, as well as NAT configurations, inter-zone access rules, HTTP/FTP services, and an authenticated HTTP proxy. The results demonstrated proper network segmentation and the protection of critical servers, ensuring the integrity of databases and applications. The work was complemented with LPI 101 exercises *[1]*, strengthening skills in operating systems administration and computer security

KEYWORDS: DMZ, Endian Firewall, GNU/Linux, perimeter security

1 INTRODUCCIÓN

En esta sustentación se implementa la seguridad perimetral que es un componente esencial en la administración de sistemas informáticos. En entornos corporativos, la necesidad de proteger servidores y aplicaciones críticas exige la implementación de arquitecturas que segmenten el tráfico y reduzcan riesgos de intrusión. La creación de una zona desmilitarizada (DMZ) permite aislar servicios expuestos a Internet, garantizando la integridad de las bases de datos y aplicaciones internas [5].

Este proyecto académico se centra en la instalación y configuración de Endian Firewall, una distribución GNU/Linux orientada a la seguridad perimetral [5]. La práctica se realizó en VirtualBox [4], con tres zonas diferenciadas: LAN (verde), WAN (roja) y DMZ (naranja). El trabajo se desarrolló de forma colaborativa, con cada integrante abordando una temática específica, y se complementó con ejercicios del LPI 101 para reforzar conocimientos de hardware y configuración básica. *[1]*

2 OBJETIVO GENERAL

Implementar un esquema de seguridad perimetral en entornos GNU/Linux mediante la instalación y configuración de Endian Firewall, garantizando la protección de servidores y aplicaciones críticas en redes LAN, WAN y DMZ, bajo un enfoque colaborativo y con fundamentos técnicos.

2.1 OBJETIVOS ESPECIFICOS

Configurar la infraestructura virtualizada en VirtualBox, estableciendo las zonas LAN, WAN y DMZ con direccionamientos IP coherentes, para simular un entorno seguro y controlado.

Aplicar reglas de seguridad perimetral en Endian Firewall [3], incluyendo NAT, control de servicios (HTTP, FTP, ICMP) y políticas de acceso inter-zonas, verificando su funcionamiento mediante pruebas de conectividad y evidencias en consola.

Implementar un proxy HTTP con autenticación y políticas de restricción de acceso, evaluando su impacto en la navegación de usuarios internos y documentando los resultados con capturas y análisis comparativo.

Evidenciar la ejecución de comandos en consola mostrando fecha y hora, para garantizar trazabilidad y reproducibilidad de la práctica en un entorno colaborativo.

Fortalecer competencias académicas y técnicas en administración de sistemas GNU/Linux, integrando los conocimientos obtenidos en actividades anteriores y adaptándolos con la práctica de seguridad perimetral, y consolidando un documento en formato IEEE con las temáticas desarrolladas.

3 TEMATICA # 1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Se instaló Endian Firewall versión 3.3.2 en VirtualBox [4], configurando tres tarjetas de red para las zonas verde, roja y naranja según las recomendaciones de Endian [5]. Se definieron direccionamientos IP coherentes para garantizar la interoperabilidad entre los integrantes del grupo.

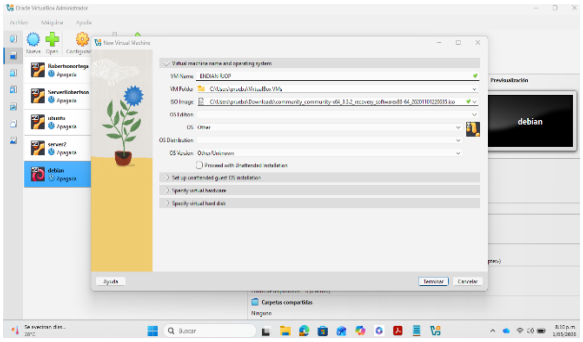
3.1 ENLACE DE LA DESCARGA

https://sourceforge.net/projects/efw/

3.2 PROCESO DE INSTALACION ENDIAN

Se descarga el archivo ISO del sistema Endian Firewall desde la plataforma oficial [5], luego que el archivo este en el equipo se creó una nueva máquina virtual y se configuran las tres tarjetas con cada zona especificada con las cuales vamos a trabajar e implementar según indicaciones de la guía de actividades.

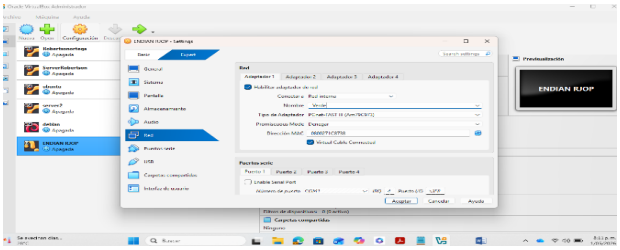
Figura 1.
Creación MV con ISO ENDIAN



Fuente: Autoría Propia

Creación de la máquina virtual en Oracle VM VirtualBox utilizando la imagen ISO de Endian Firewall para la implementación de las zonas LAN, WAN y DMZ.

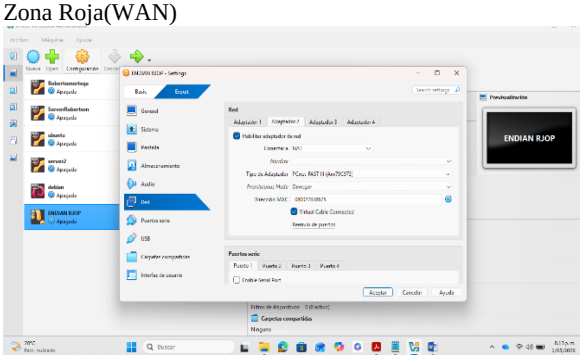
Figura 2.
Zona Verde



Fuente: Autoría Propia

Configuración de la interfaz de red correspondiente a la zona verde (LAN), utilizada para la comunicación interna entre los equipos cliente y el firewall Endian.

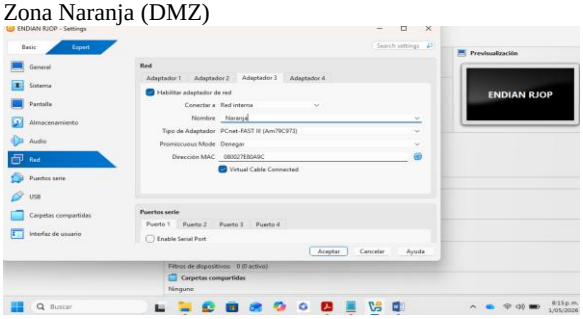
Figura 3.
Zona Roja(WAN)



Fuente: Autoría Propia

Configuración de la interfaz de red asociada a la zona roja (WAN), destinada a simular la conexión externa hacia Internet dentro del entorno virtualizado.

Figura 4.
Zona Naranja (DMZ)

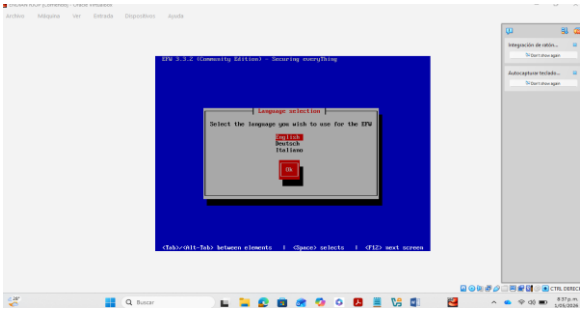


Fuente: Autoría Propia

Después de haber configurado las tarjetas se procede a realizar la instalación de ENDIAN en este paso seguimos las indicaciones del asistente de instalación [3].

Se escoge el idioma de configuración del asistente de instalación.

Figura 5.
Selección Idioma de la Instalación



Fuente: Autoría Propia

Preparación del disco para la instalación, particionando el disco, para luego instalar el sistema de archivos en las particiones, se nos advierte que los datos se pueden perder, pero como es una instalación nueva escogemos la opción yes.

Figura 6.
Preparación sistema de Archivos

Fuente: Autoría Propia

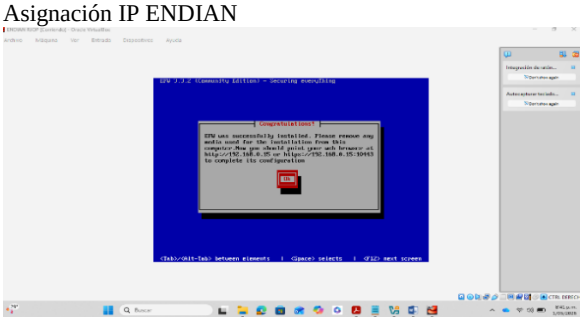
En el proceso de la instalación y configuración el segmento de red el cual previamente se estableció para este paso.

Figura 7.
Asignación segmento de Red Zona Verde

Fuente: Autoría Propia

Luego que se establece la ip donde apuntar a ENDIAN para terminar de configurar los parámetros desde la Web iniciando en la IP que se le asigna.

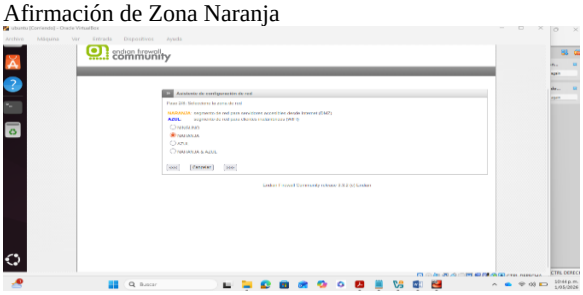
Figura 8
Asignación IP ENDIAN



Fuente: Autoría Propia

Aquí se procede a configurar el idioma, la zona naranja, zona roja afirmar la asignación a cada tarjeta y asignarles los rangos de IPS y agregarle contraseña a ENDIAN Firewall para mantener un ingreso seguro a su configuración y administración de nuestras redes [10].

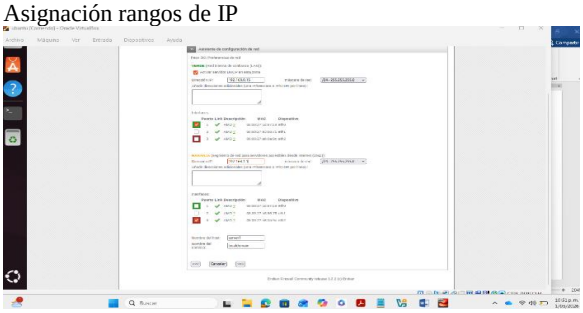
Figura 9.
Afirmación de Zona Naranja



Fuente: Autoría Propia

En este paso se realizó la configuración de los rangos de direcciones IP correspondientes a las zonas verde (LAN) y naranja (DMZ), garantizando la correcta segmentación y comunicación de la red.

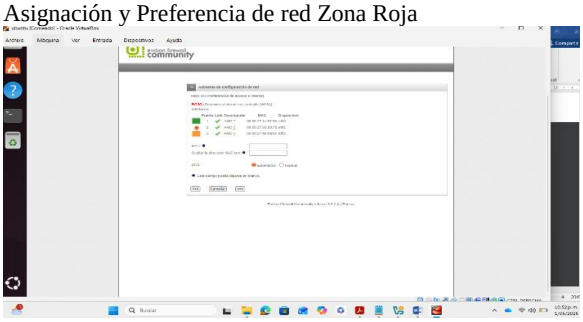
Figura 10.
Asignación rangos de IP



Fuente: Autoría Propia

Se Escoge la tarjeta número dos, para el tráfico de internet como indicaba la solicitud de la guía de actividades para WAN zona roja e indicamos en siguiente para que sea aplicada la configuración que tomamos.

Figura 11.
Asignación y Preferencia de red Zona Roja



Fuente: Autoría Propia

Después de estos pasos se ingresa al panel de configuración de ENDIAN y ahí se monitorea la configuración que se realiza de las tarjetas y zonas [6], su tráfico entrante y saliente y funcionamiento por medio de un gráfico de ENDIAN. En este panel podemos añadir reglas, crear protocolos, permitir

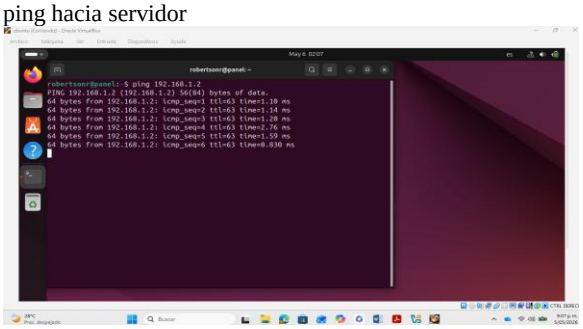
o negar accesos controlados al internet y así se evita que los usuarios entren a paginas perjudiciales para el sistema y la red corporativa.

Figura 12.
Panel de Configuración y Monitoreo

Fuente: Autoría Propia

Luego de configurar se ingresa a las maquinas Ubuntu cliente y Ubuntu servidor para verificar las IPS asignadas y revisar conexión entre ellas.

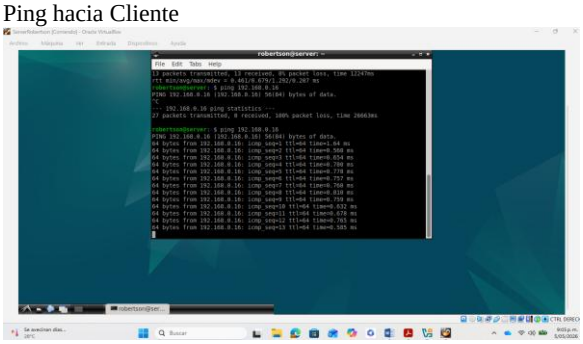
Figura 13.
ping hacia servidor



Fuente: Autoría Propia

Con el fin de verificar la conectividad entre los equipos de la red, se realizó una prueba de comunicación mediante el comando ping desde el servidor hacia el cliente ubicado en la zona LAN.

Figura 14.
Ping hacia Cliente



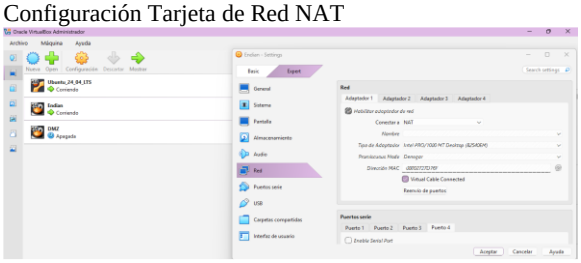
Fuente: Autoría Propia

Prueba de conectividad mediante el comando ping desde el cliente hacia el servidor configurado en la red LAN, validando la comunicación entre los equipos y el correcto funcionamiento de las reglas establecidas.

4 TEMATICA #2 CONFIGURACION NAT

Inicialmente, se realizó la configuración de las tarjetas de red necesarias para la implementación de la temática propuesta, estableciendo los parámetros correspondientes para la comunicación entre las zonas LAN, WAN y DMZ dentro del entorno virtualizado.

Figura 15.
Configuración Tarjeta de Red NAT



Fuente: Autoría Propia

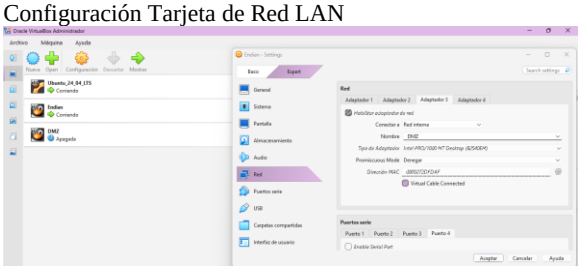
Posteriormente, se configuró la tarjeta de red correspondiente a la zona LAN con el fin de permitir la comunicación interna entre los equipos cliente y el firewall Endian dentro del entorno virtualizado.

Figura 16.
Configuración Tarjeta de Red LAN

Fuente Autoría Propia

A continuación, se realizó la configuración adicional de la tarjeta de red LAN para garantizar la correcta comunicación entre los equipos de la red interna y los servicios administrados por ENDIAN Firewall.

Figura 17.
Configuración Tarjeta de Red LAN

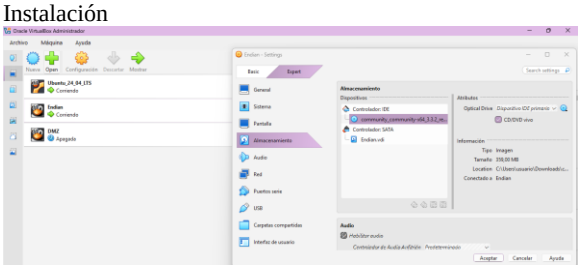


Fuente: Autoría Propia

Una vez configuradas las interfaces de red, se procedió a montar la imagen ISO de Endian Firewall en la

máquina virtual para iniciar el proceso de instalación y configuración del sistema de seguridad perimetral.

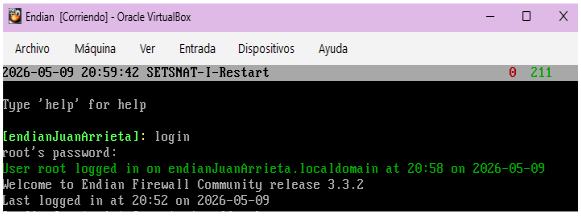
Figura 18.
Instalación



Fuente: Autoría Propia

Una vez finalizada la instalación de Endian Firewall, se inició sesión con el usuario administrador root con el fin de verificar el correcto funcionamiento del sistema y acceder a las opciones de configuración y administración de la red.

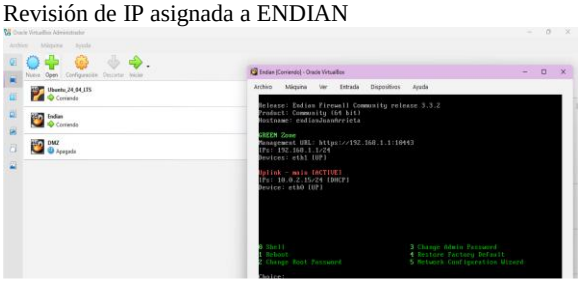
Figura 19.
Inicio de sesión en ENDIAN



Fuente: Autoría Propia

Verificación de la IP de ENDIAN y que esté funcionando para luego entrar al panel y realizar las configuraciones correspondientes.

Figura 20.
Revisión de IP asignada a ENDIAN

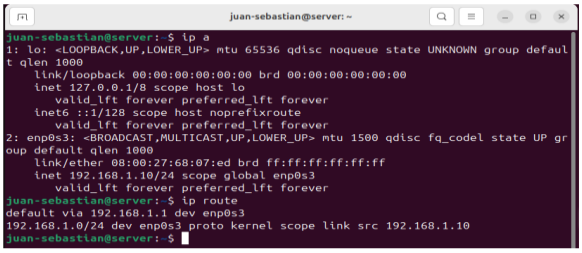


Fuente: Autoría Propia

Posteriormente, se accedió al equipo cliente ubicado en la zona verde (LAN interna) con el fin de verificar la dirección IP asignada y comprobar la correcta conectividad hacia Endian Firewall a través de la red interna previamente configurada. Este procedimiento permitió confirmar que la asignación de parámetros de red se encontraba en concordancia con la configuración establecida en el firewall, garantizando la comunicación segura entre los clientes internos y el sistema de gestión perimetral.

.

Figura 21.
Verificación IP



Fuente: Autoría Propia

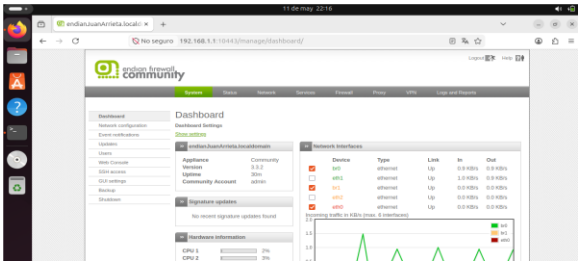
Posteriormente, se accedió desde el navegador web del equipo Ubuntu ubicado en la zona LAN a la interfaz de administración de Endian Firewall mediante la dirección IP asignada y el puerto seguro correspondiente, con el fin de continuar con la configuración de los servicios y políticas de seguridad.

Figura 22.
Ingreso al Panel de ENDIAN

Fuente: Autoría Propia

Una vez autenticado el acceso al sistema, se visualizó la interfaz principal de Endian Firewall, donde se encuentran los paneles de monitoreo y administración correspondiente a las zonas RED (WAN), GREEN (LAN) y ORANGE (DMZ), permitiendo supervisar el estado y funcionamiento de la red.

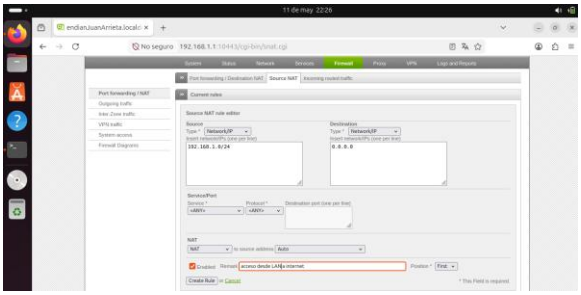
Figura 23.
Verificación Interfaz ENDIAN



Fuente: Autoría Propia

Posteriormente, se ingresó al módulo de Firewall de Endian con el propósito de verificar la existencia y el estado de las reglas de seguridad necesarias para la implementación de la temática, comprobando si estas se encontraban activas o requerían ser creadas manualmente.

Figura 24.
Verificación de las Reglas



Fuente: Autoría Propia

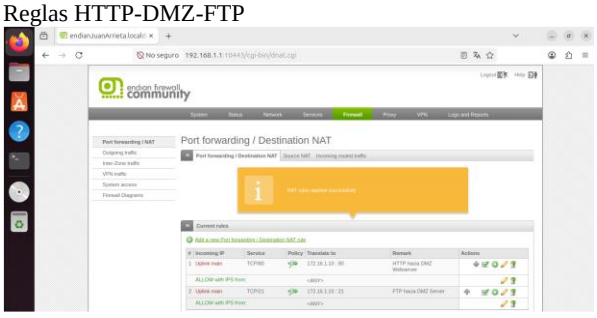
El mismo procedimiento fue aplicado para cada una de las reglas de firewall configuradas, verificando su correcta creación, activación y funcionamiento dentro de las políticas de seguridad establecidas en Endian Firewall.

Figura 25.
Verificación de las reglas

Fuente: Autoría Propia

Para poder permitir que el exterior acceda al servidor web en la DMZ, se implementa el reenvió de puertos donde se crearon las reglas HTTP (puerto 80) - servidor DMZ y FTP (puerto 21) – servidor DMZ, verificamos que se creen correctamente y aplicamos los cambios.

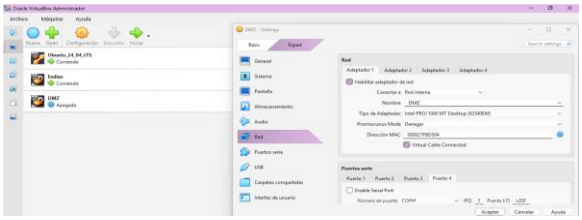
Figura 26.
Reglas HTTP-DMZ-FTP



Fuente: Autoría Propia

El servidor Ubuntu ubicado en la zona DMZ fue configurado con el propósito de realizar pruebas de conectividad, administración y verificación de las configuraciones implementadas en Endian Firewall, garantizando el correcto funcionamiento de los servicios y la segmentación de la red.

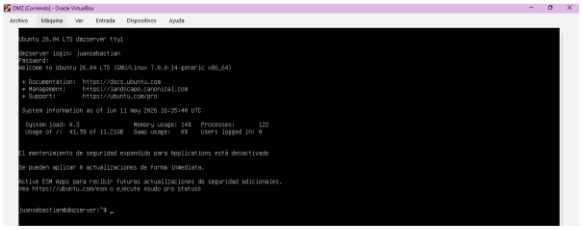
Figura 27.
Red DMZ



Fuente: Autoría Propia

Una vez finalizada la instalación y configuración inicial del sistema, se accedió al servidor Ubuntu ubicado en la zona DMZ con el propósito de verificar el funcionamiento del entorno, administrar los servicios configurados y realizar pruebas de conectividad.

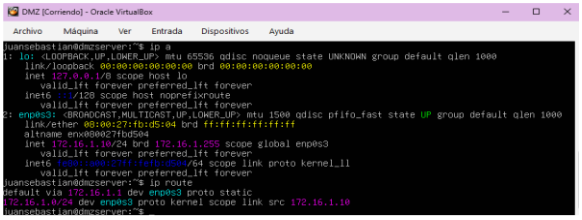
Figura 28.
Ubuntu Server



Fuente: Autoría Propia

Lo primero que se debe realizar al tener acceso a la maquina DMZ es verificar nuestra “ip” y “route” en modo consola con los comandos que se ilustran en la imagen.

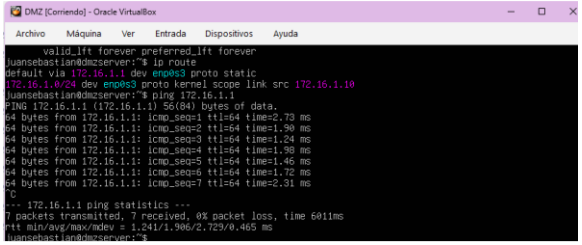
Figura 29.
Verificación IP Servidor



Fuente: Autoría Propia

En esta etapa se verificó el correcto funcionamiento de la conectividad entre el servidor y el firewall Endian mediante el comando ping hacia la dirección IP 172.16.1.1, comprobando la comunicación y estabilidad de la red configurada.

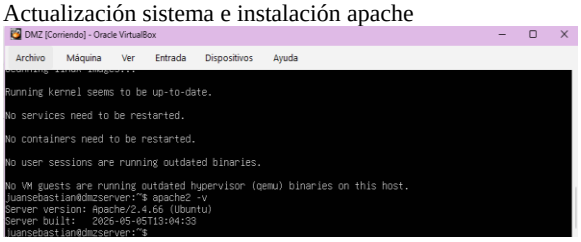
Figura 30.
Verificación de Funcionamiento



Fuente: Autoría Propia

Posteriormente, se realizó la actualización del sistema operativo Ubuntu Server y la instalación del servicio Apache2, siguiendo lineamientos de administración y configuración de sistemas GNU/Linux con el fin de habilitar los servicios web requeridos en la zona DMZ [2], [8].

Figura 31.
Actualización sistema e instalación apache



Fuente: Autoría Propia

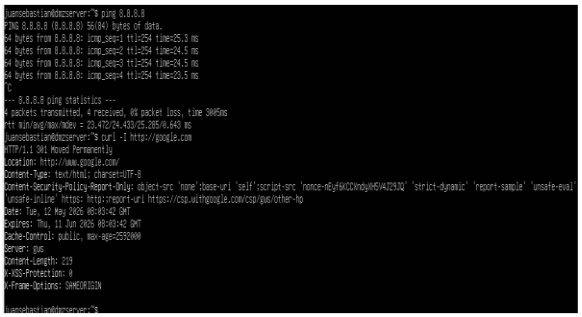
Ahora verificamos que verificar si nuestra maquina LAN tiene Internet (HTTP), necesitamos saber si existe resolución DNS y si la conectividad (HTTP) se encuentra funcionando

Figura 32.
Resolución DNS y HTTP

Fuente: Autoría Propia

Con el propósito de validar la conectividad externa del servidor ubicado en la zona DMZ, se realizó una prueba de acceso a Internet para comprobar el correcto funcionamiento de las reglas de red y la comunicación establecida a través de Endian Firewall.

Figura 33.
Verificación Internet Servidor



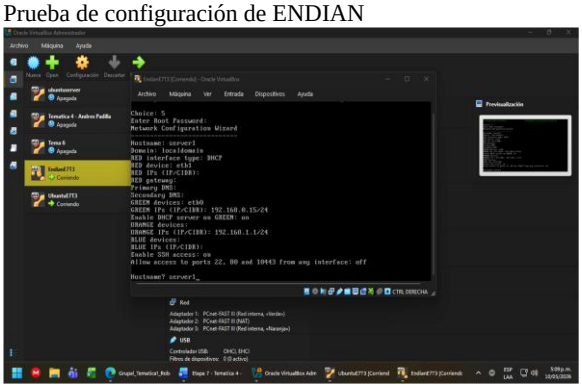
Fuente: Autoría Propia

Se observa que la conexión es estable y que “curl -I http://google.com” funciona gracias a las reglas establecidas para DMZ [5].

5 TEMATICA # 3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Una vez realizada la configuración inicial de las tarjetas de red conforme a lo establecido en la temática 1 y con Endian Firewall correctamente instalado, se procedió a definir las reglas de acceso para los servicios requeridos. Este paso permitió establecer políticas de comunicación entrantes y salientes, regulando el tráfico en función de los puertos y protocolos habilitados. La configuración de reglas constituye un mecanismo esencial para garantizar que los servicios críticos puedan operar de manera controlada, asegurando la protección de la infraestructura interna y la correcta segmentación de las zonas de red. De esta manera, se refuerza la seguridad perimetral y se consolida la administración de políticas de firewall como práctica fundamental en entornos corporativos y académicos.

Figura 34.
Prueba de configuración de ENDIAN



Fuente: Autoría Propia

Para garantizar la comunicación entre la zona DMZ y la red externa, fue necesario verificar y habilitar las reglas NAT configuradas en Endian Firewall, permitiendo la traducción de direcciones y el acceso controlado a Internet desde el servidor.

Figura 35.
Verificación y Habilitación Reglas NAT

Fuente: Autoría Propia

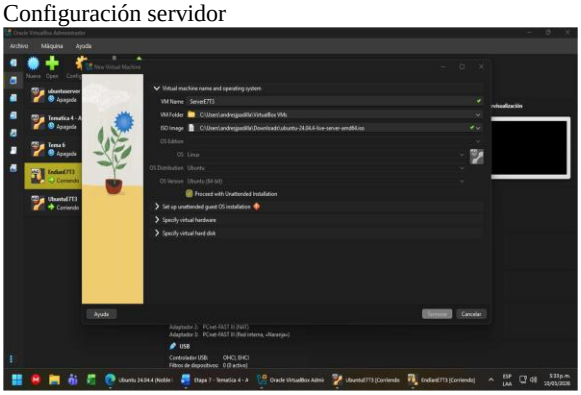
Posteriormente, se efectuó una nueva verificación de las reglas NAT configuradas en Endian Firewall con el propósito de confirmar su correcto funcionamiento y garantizar la comunicación segura entre la zona DMZ y la red externa. Este procedimiento permitió comprobar que los servicios alojados en la DMZ podían establecer conexión hacia la WAN bajo un control estricto de las políticas de traducción de direcciones, asegurando que únicamente el tráfico autorizado atravesara el perímetro de seguridad. La validación de las reglas evidenció la coherencia entre la configuración aplicada y el comportamiento real del sistema.

Figura 36.
Verificación y Habilitación Reglas NAT

Fuente: Autoría Propia

El servidor ubicado en la zona DMZ fue configurado mediante una máquina virtual creada con Ubuntu Live Server, permitiendo implementar y administrar los servicios para las pruebas de conectividad y seguridad de la red [2], [8].

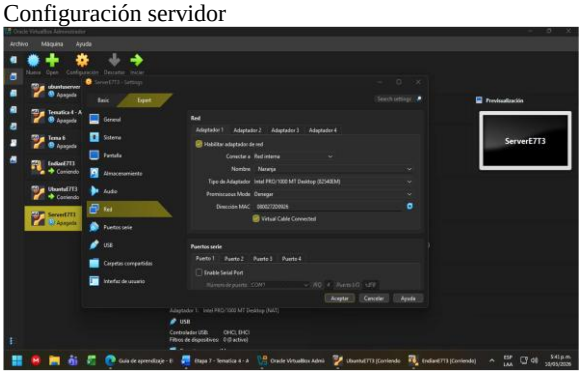
Figura 37.
Configuración servidor



Fuente: Autoría Propia

Posteriormente, se configuró la tarjeta de red del servidor en modo de red interna, verificando que el nombre asignado correspondiera a la zona naranja (DMZ), con el fin de garantizar la correcta comunicación y segmentación de la red dentro del entorno virtualizado.

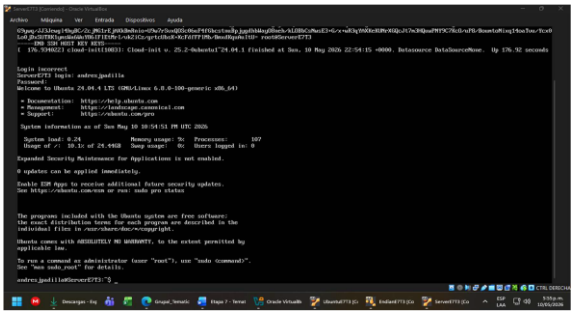
Figura 38.
Configuración servidor



Fuente: Autoría Propia

Posteriormente, se realizó una conexión local al servidor mediante el protocolo FTP utilizando la herramienta FileZilla, con el propósito de verificar el correcto funcionamiento del servicio y la transferencia de archivos dentro de la red configurada [7].

Figura 39.
Inicio de Servidor



Fuente Autoría Propia

Posteriormente, la dirección IP del servidor fue configurada manualmente para coincidir con el rango de direcciones asignado a la VLAN de la zona DMZ, garantizando la correcta segmentación de la red y la comunicación con Endian Firewall. Después de realizar la configuración, se ejecutó una prueba de conectividad para verificar el acceso y funcionamiento de la red.

Figura 40.
Asignación Manual IP Servidor

Fuente: Autoría Propia

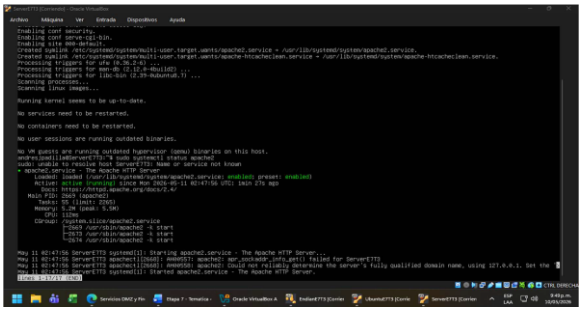
Finalmente, se realizó una prueba de conexión entre el servidor configurado en la zona DMZ y Endian Firewall con el propósito de verificar la correcta comunicación entre los dispositivos y validar el funcionamiento de la configuración de red implementada.

Figura 41.
Prueba de Conexión con ENDIAN

Fuente: Autoría Propia

Posteriormente, se verificó el estado de los servicios configurados en el servidor, comprobando que permanecieran activos y funcionando correctamente para garantizar la disponibilidad y operación adecuada de los servicios implementados en la zona DMZ.

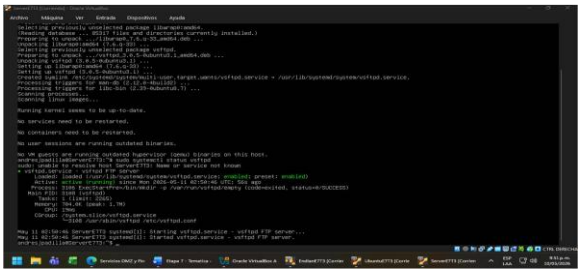
Figura 42.
Verificación de Servicios



Fuente: Autoría Propia

Posteriormente, se realizó la instalación y verificación del servicio FTP en el servidor ubicado en la zona DMZ, comprobando que el servicio permaneciera activo y funcionando correctamente para permitir la transferencia de archivos dentro de la red configurada [7].

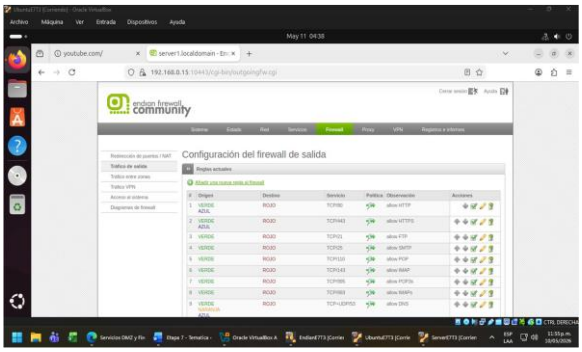
Figura 43.
Verificación de Servicio FTP



Fuente: Autoría Propia

Con los servicios en ejecución, se procedió a ingresar al panel de administración de Endian Firewall para configurar las reglas entrantes y salientes correspondientes a los puertos HTTP (80) y FTP (21). Esta acción permitió establecer políticas de acceso específicas que regulan la comunicación entre clientes internos y servicios externos, garantizando que únicamente el tráfico autorizado pueda atravesar el perímetro de seguridad. La definición de estas reglas constituye un mecanismo esencial para controlar el flujo de información, proteger los recursos alojados en la DMZ y asegurar la disponibilidad de servicios críticos como la transferencia de archivos y la navegación web. De esta manera, se refuerza la segmentación de la red y se consolidan las prácticas de administración de firewalls en entornos corporativos.

Figura 44.
Panel de ENDIAN

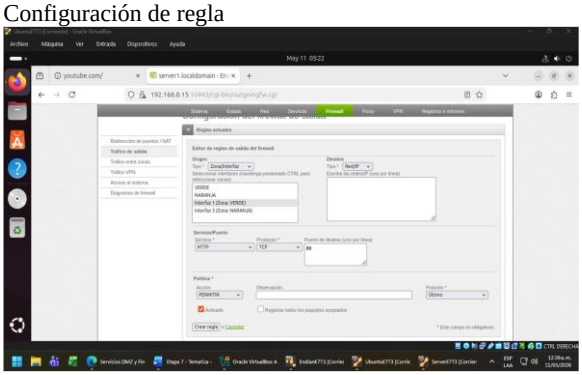


Fuente: Autoría Propia

Estando en la sección de trafico de salida se configura la primera regla NAT de la siguiente Nueva regla 1.

Quedará configurada como:
Origen: Interfaz 1 (Zona: VERDE)
Destino: Red/IP
Servicio: HTTP
Protocolo: TCP
Puerto de destino: 80
Acción: Permitir

Figura 45
Configuración de regla

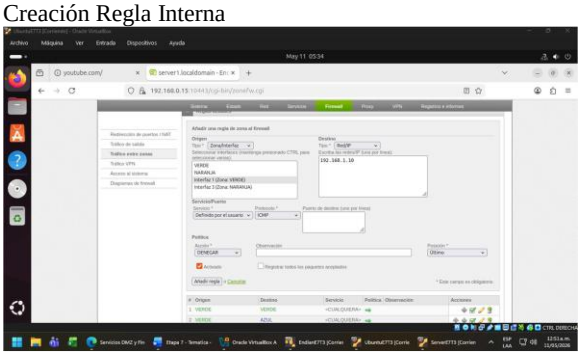


Fuente: Autoría Propia

Después de haber creado estas dos reglas se crea la tercera regla para el tráfico de ICMP (puerto 8 y puerto 30), esta regla es creada para no permitir hacer ping en la red.

Destino: Red/IP
Red IP: 192.168.1.10
Servicio: definido por el usuario
Protocolo: ICMP
Acción: Denegar

Figura 46.
Creación Regla Interna



Fuente: Autoría Propia

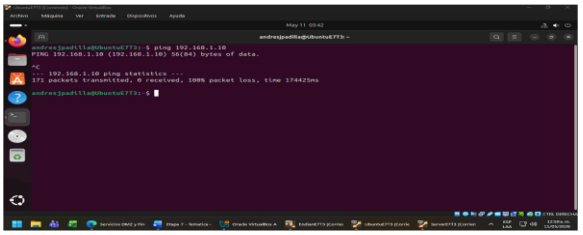
Con la regla creada, se coloca en el índice de la leyenda como la numero #1 por encima de las demás para que se ejecute en primera instancia.

Figura 47.
Orden de Reglas Creadas

Fuente: Autoría Propia

Luego de crear las reglas se realiza la prueba de conectividad mediante el comando ping desde el cliente hacia el servidor en la DMZ (192.168.1.10), obteniendo como resultado un 100% de pérdida de paquetes, lo que evidencia el bloqueo efectivo del protocolo ICMP según la regla configurada en el firewall.

Figura 48.
Prueba de Conectividad



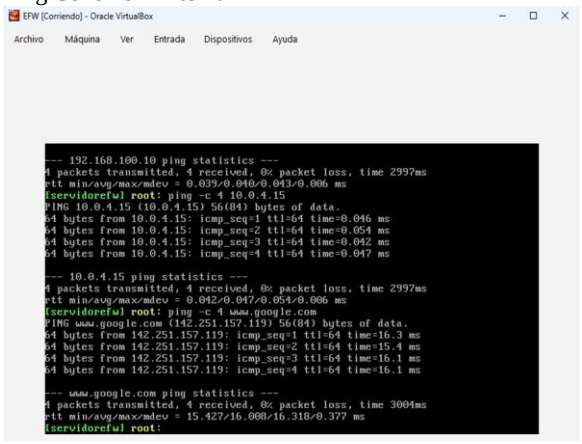
Fuente: Autoría Propia

6 TEMATICA #4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Realizada la configuración como lo indica la temática 1,2,3 la configuración de las tarjetas previamente instalado ENDIAN, creación de las reglas se procede a verificar conexión de las maquinas.

Se realizó una verificación de conectividad hacia la red externa mediante la ejecución del comando ping, lo que permitió comprobar la correcta salida de tráfico desde la infraestructura interna hacia Internet. El resultado obtenido evidenció que las reglas de firewall y las políticas de NAT configuradas en Endian Firewall estaban funcionando adecuadamente, garantizando la comunicación estable y segura entre la LAN y la WAN.

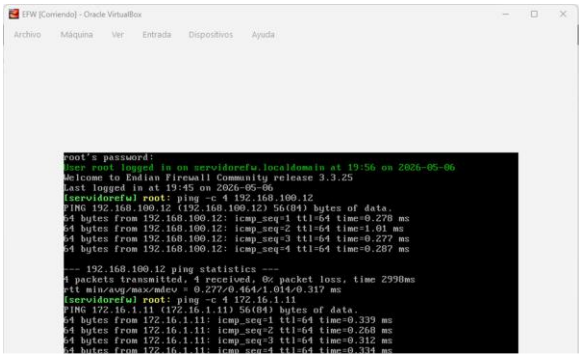
Figura 49.
Ping Conexión Externa



Fuente: Autoría Propia

Se efectúa la prueba de conexión hacia la zona naranja y verde. Se realiza esta prueba de conexión entre la zona naranja (DMZ) y la zona verde (LAN interna) con el propósito de validar la comunicación controlada entre segmentos de red diferenciados. Este procedimiento permitió comprobar que los servicios alojados en la DMZ podían interactuar con los clientes internos de manera segura, sin comprometer la integridad de la LAN. La verificación de conectividad entre ambas zonas evidenció la correcta aplicación de las reglas de acceso configuradas en Endian Firewall, demostrando que el tráfico autorizado fluye de forma confiable mientras se mantienen bloqueados los intentos de acceso no permitidos. Este resultado refuerza la importancia de la segmentación de redes como estrategia fundamental para garantizar seguridad perimetral y protección de recursos críticos.

Figura 50.
Conexión Zona naranja-Verde



Fuente: Autoría Propia

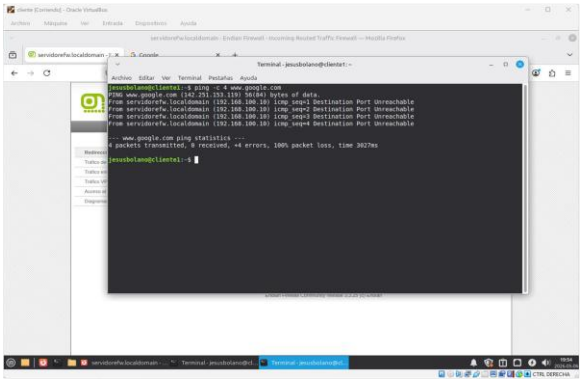
También se realiza prueba de conectividad hacia la zona Roja. Se efectuó una prueba de conectividad hacia la zona roja (WAN), con el fin de validar que las reglas de acceso configuradas en el firewall permiten la comunicación controlada entre la red interna y el exterior. Este procedimiento es vital para comprobar que el tráfico hacia Internet este regulado, garantizando que únicamente los servicios autorizados puedan establecer conexión. La verificación hacia la zona roja confirma la correcta segmentación de la red y evidencia que Endian Firewall actúa como punto central de decisión en la gestión del tráfico, reforzando la seguridad perimetral y la protección de los recursos internos.

Figura 51.
Conexión Hacia Zona Roja

Fuente: Autoría Propia

Se procede a realizar prueba de conectividad desde la Zona verde hacia red externa. Se efectuó esta prueba de conectividad desde la zona verde (LAN interna) hacia la red externa con el objetivo de validar que los clientes internos pudieran acceder a Internet bajo las políticas de seguridad previamente configuradas en el firewall. Este procedimiento permitió comprobar que el tráfico saliente se encontraba regulado, garantizando que únicamente los servicios autorizados fueran capaces de establecer comunicación con la WAN. La verificación de conectividad hacia la red externa evidenció la correcta aplicación de las reglas de acceso y demostró que Endian Firewall cumple su función como punto central de control, asegurando la protección de la LAN frente a accesos no deseados y reforzando la seguridad perimetral.

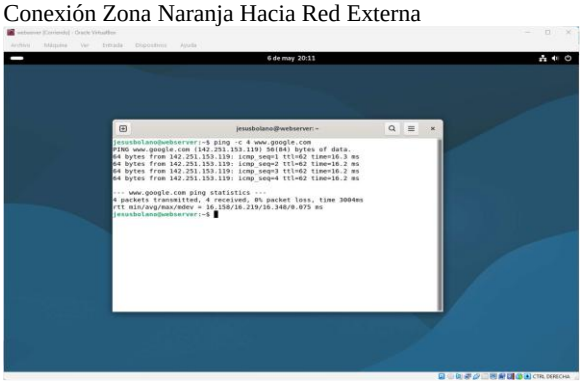
Figura 52.
Conexión Zona Verde Hacia Red Externa



Fuente: Autoría Propia

Ejecución de pruebas de conectividad desde la zona Naranja hacia red externa.

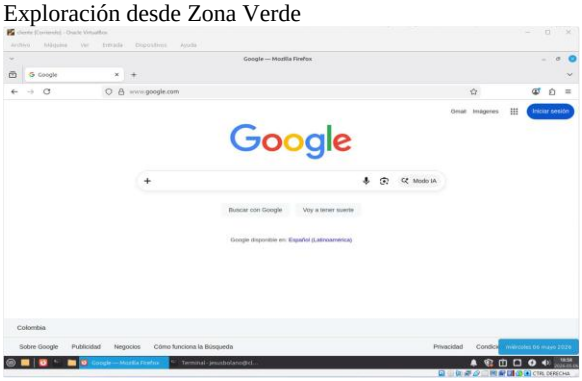
Figura 53.
Conexión Zona Naranja Hacia Red Externa



Fuente: Autoría Propia

Se realiza una exploración en el navegador desde la zona verde verificando que posee conexión. En esta prueba se evidenció que la zona verde (LAN interna) posee conectividad hacia Internet, lo cual confirma que las reglas de acceso configuradas en el firewall permiten la navegación controlada de los clientes internos. Este resultado valida la correcta segmentación de la red y la coherencia entre la configuración teórica y el comportamiento práctico.

Figura 54.
Exploración desde Zona Verde



Fuente: Autoría Propia

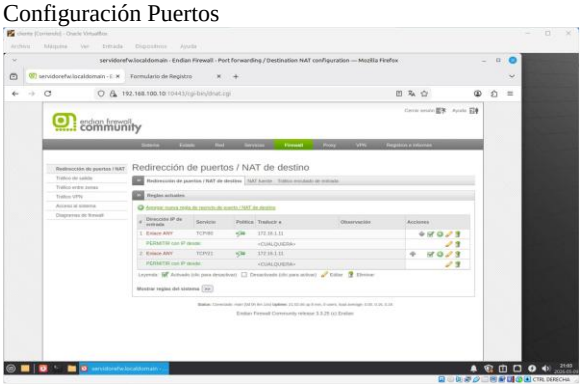
Se realiza un despliegue del cliente en el servidor. El despliegue del servidor en la DMZ demuestra la capacidad de aislar servicios críticos en un segmento intermedio, reduciendo riesgos de intrusión desde la WAN. Esto es vital en arquitecturas corporativas, ya que garantiza que los servicios expuestos (HTTP/FTP) no comprometan la red de la LAN.

Figura 55.
Servidor Desplegado Zona Naranja

Fuente Autoría Propia

En esta opción se configuran las reglas NAT de los puertos 80 y 21. La habilitación de los puertos 80 (HTTP) y 21 (FTP) en la DMZ permitió establecer reglas específicas de acceso, asegurando que únicamente el tráfico autorizado pueda alcanzar los servidores. Este control granular fortalece la seguridad perimetral y evita accesos no deseados.

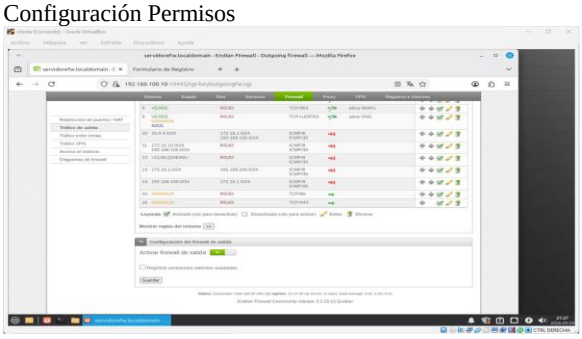
Figura 56.
Configuración Puertos



Fuente: Autoría Propia

Se realiza la configuración de los permisos en el panel de ENDIAN. La configuración de los permisos en el panel de Endian Firewall permitió establecer políticas de acceso diferenciadas para cada zona de la red. Este proceso asegura que los usuarios internos solo puedan interactuar con los servicios autorizados, mientras se restringe el acceso a recursos sensibles desde la WAN. La correcta definición de permisos constituye un mecanismo esencial de control, ya que garantiza la trazabilidad de las acciones, refuerza la protección de los servidores ubicados en la DMZ y contribuye a la estabilidad del sistema al evitar accesos no deseados. Además, esta práctica refleja un escenario corporativo real, donde la administración de permisos se convierte en un componente estratégico para la gestión de políticas de seguridad y cumplimiento normativo.

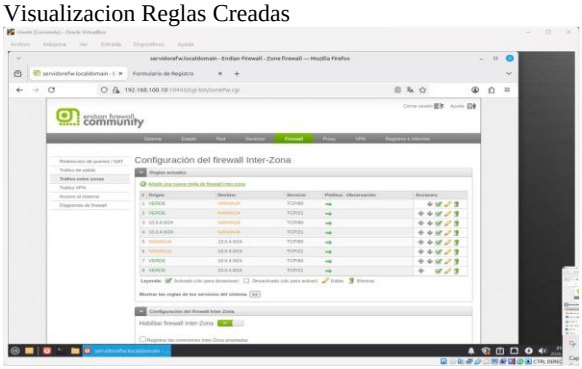
Figura 57.
Configuración Permisos



Fuente: Autoría Propia

Se Procede a visualizar en el panel de ENDIAN las reglas creadas. La visualización de las reglas en el panel de Endian Firewall permitió comprobar que las políticas de seguridad configuradas estaban activas y funcionando correctamente. Este paso es fundamental porque ofrece al administrador una visión clara del tráfico permitido y bloqueado entre las diferentes zonas (LAN, WAN y DMZ). Además, la interfaz gráfica facilita la gestión y el monitoreo en tiempo real [6], lo que contribuye a detectar posibles anomalías y garantizar la trazabilidad de las configuraciones aplicadas. De esta manera, se asegura que las reglas implementadas no solo estén registradas, sino que también se ejecuten de forma coherente con los objetivos de seguridad perimetral.

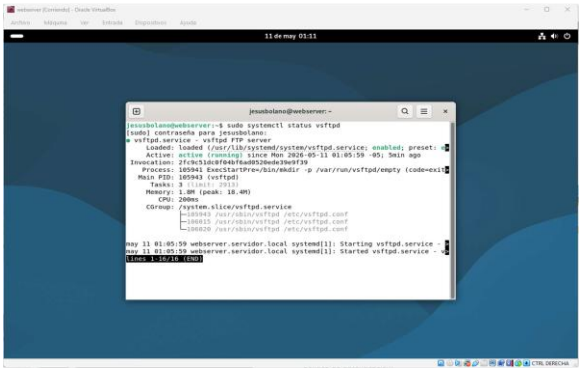
Figura 58.
Visualizacion Reglas Creadas



Fuente: Autoría Propia

Creadas las reglas verificamos en el servidor el servicio de FTP el cual debe estar corriendo y activo. La comprobación del servicio FTP en la DMZ permitió validar que el servidor se encontraba activo y en ejecución, garantizando la disponibilidad de un servicio crítico para la transferencia de archivos [9]. Este paso es esencial en la administración de sistemas, ya que asegura que los protocolos de comunicación estén correctamente configurados y que los usuarios autorizados puedan acceder de manera confiable a los recursos compartidos.

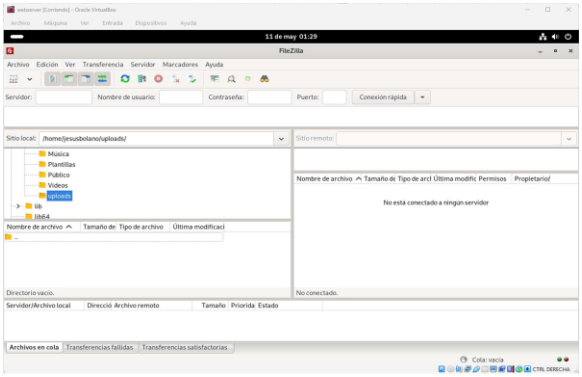
Figura 59.
Verificación de Servicio FTP



Fuente: Autoría Propia

Se realiza la conexión local por medio de FTP con FileZilla. La conexión establecida mediante FileZilla evidenció la interoperabilidad entre el cliente de la zona verde y el servidor ubicado en la DMZ. Este resultado confirma que las reglas de acceso configuradas en Endian Firewall permiten la comunicación controlada entre segmentos de red, reforzando la seguridad perimetral. Además, la prueba práctica con un cliente gráfico como FileZilla demuestra la aplicabilidad de la configuración en escenarios reales de administración corporativa.

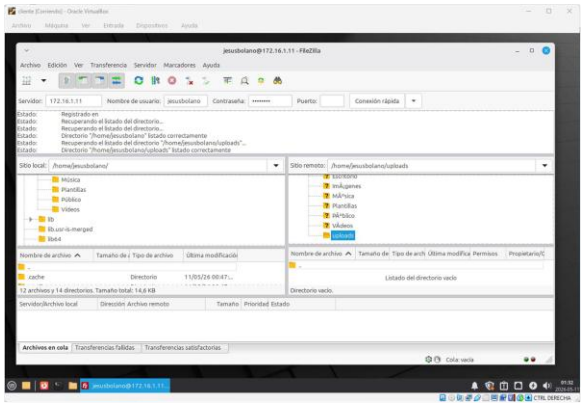
Figura 60.
Conexión Local FTP-FileZilla



Fuente: Autoría Propia

Se realiza una verificación del servicio desde la zona verde la cual ya habíamos configurado. Se efectuó la verificación del servicio desde la zona verde (LAN interna) previamente configurada, con el objetivo de confirmar que los clientes internos pudieran acceder de manera controlada a los recursos disponibles en la DMZ y hacia la red externa. Este procedimiento permitió validar que las reglas de acceso y las políticas de seguridad aplicadas en Endian Firewall estaban funcionando correctamente, garantizando que únicamente el tráfico autorizado pudiera establecer comunicación. La comprobación desde la zona verde evidenció la coherencia entre la configuración teórica y el comportamiento real del sistema, reforzando la seguridad perimetral y asegurando la protección de los recursos internos frente a accesos no deseados.

Figura 61.
Verificación de Servicio



Fuente: Autoría Propia

7 TEMATICA #5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Anticipadamente y siguiendo las temáticas anteriores tenemos instalado ENDIAN y previamente configuradas las tarjetas con sus respectivas zonas, así mismo instalamos un Ubuntu desktop y un servidor para la implementación del proxy y las reglas que vamos a generar dentro del panel de configuración del ENDIAN.

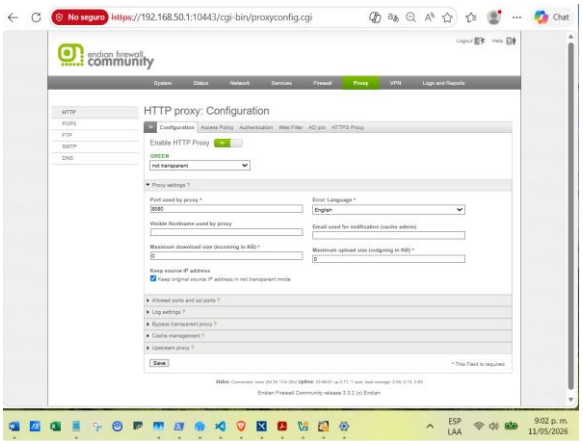
Se Accede a Endian en la dirección que le asignó el asistente de instalación.

Figura 62.
Acceso a Endian

Fuente: Autoría Propia

Se procede a habilitar el servicio de Proxy HTTP en modo no transparente sobre la interfaz GREEN, siguiendo configuraciones recomendadas por la documentación oficial de Endian [5].

Figura 63.
Configuración HTTP proxy



Fuente: Autoría Propia

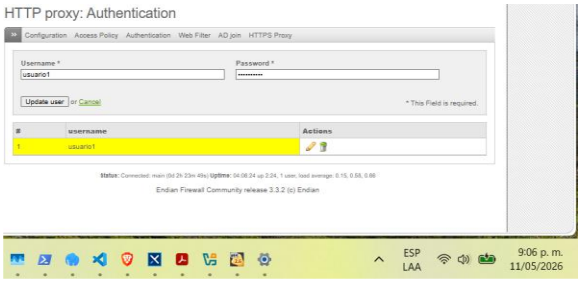
Se configura el método de autenticación local NCSA para validar usuarios mediante credenciales almacenadas localmente en el firewall [5]. Esta configuración garantiza que el acceso a la navegación web se realice únicamente por parte de usuarios autorizados, reforzando el control de identidad y evitando accesos no deseados. La autenticación local constituye un mecanismo esencial en entornos corporativos, ya que asegura trazabilidad en el uso de servicios, facilita la gestión de políticas de acceso y fortalece la seguridad perimetral al limitar la exposición de recursos internos. Además, este procedimiento evidencia la importancia de integrar mecanismos de autenticación en la administración de sistemas GNU/Linux, consolidando competencias prácticas en la gestión de firewalls y servicios de red.

Figura 64.
Configuración Método Autenticación

Fuente: Autoría Propia

Posteriormente, se creó el usuario denominado “usuario1”, el cual fue utilizado para realizar la autenticación y control de acceso al servicio proxy HTTP desde los equipos cliente ubicados en la red LAN, permitiendo aplicar las políticas de navegación y seguridad configuradas en Endian Firewall.

Figura 65.
Creación de Usuario



Fuente: Autoría Propia

Se crea el grupo Grupo_Tematica5, asociando el usuario creado previamente con el fin de aplicar políticas de acceso y filtrado web de forma organizada.

Figura 66.
Creación de Grupo

Fuente: Autoría Propia

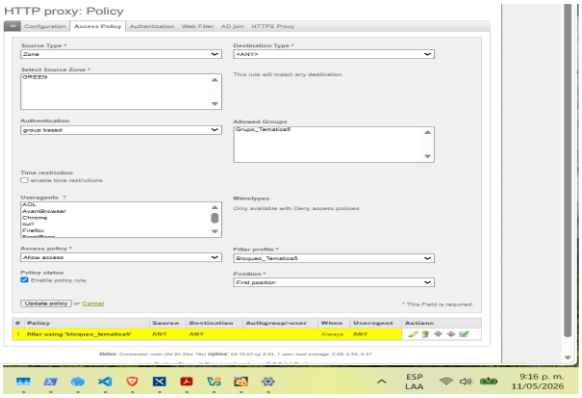
Se crea el perfil de filtrado Bloqueo_Tematica5, configurando una lista negra para restringir el acceso a los sitios web: “www.youtube.com”, “www.hotmail.com”, “www.elnuevodia.com.co”. Esta configuración permitió implementar control de contenido web dentro de la red.

Figura 67.
Creación de Filtros de Bloqueo

Fuente: Autoría Propia

Se configura la política de acceso del proxy HTTP, relacionando el grupo de usuarios con el perfil de filtrado creado anteriormente. La política permitió definir reglas de navegación y aplicar restricciones de a sitios web específicos.

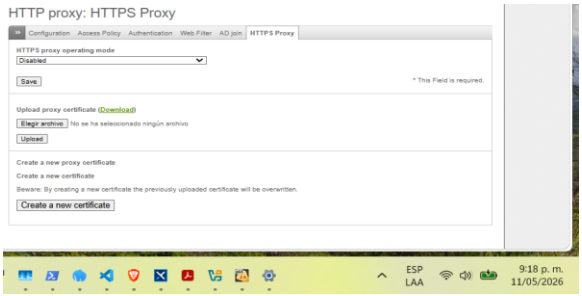
Figuro 68.
Configuración Política proxy



Fuente: Autoría Propia

En la sección la pestaña HTTPS Proxy se dejó deshabilitada debido a que la práctica se enfocó únicamente en la implementación de un Proxy HTTP no transparente. Esto evitó conflictos relacionados con certificados y túneles HTTPS.

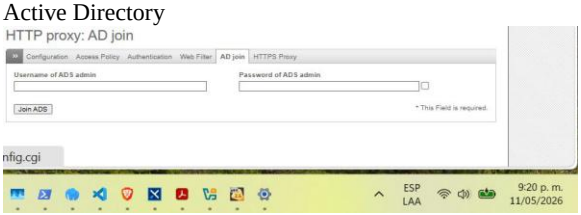
Figura 69
Pestaña HTTPS Deshabilitada



Fuente: Autoría Propia

La integración con Active Directory no fue utilizada en esta práctica, debido a que la autenticación se realizó mediante usuarios locales NCSA configurados directo en el firewall.

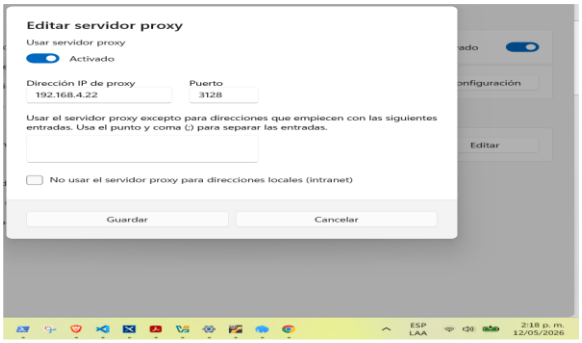
Figura 70.
Active Directory



Fuente: Autoría Propia

Finalmente, se realizó la validación del funcionamiento de lista negra configurada en el servicio HTTP, comprobando el bloqueo de los sitios web establecidos en las políticas de acceso aplicadas a los equipos cliente de la red LAN.

Figura 71.
Prueba de Funcionamiento Bloqueo Paginas



Fuente Autoría Propia

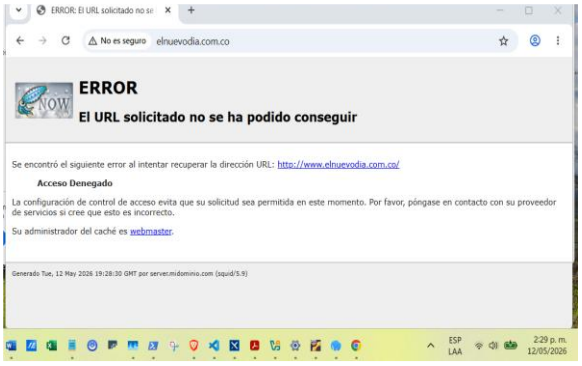
El resultado es que solicita usuario y clave en la prueba realizada apuntando a la dirección que habíamos colocado en la lista de bloqueadas.

Figura 72.
Resultado de Prueba

Fuente: Autoría Propia

Posteriormente, se realizó una prueba de autenticación en el servicio proxy HTTP utilizando las credenciales del usuario autorizado. Sin embargo, aun ingresando correctamente el nombre de usuario y la contraseña, el sistema restringió el acceso al sitio web bloqueado, evidenciando el correcto funcionamiento de las políticas de filtrado y de la lista negra configurada en Endian Firewall.

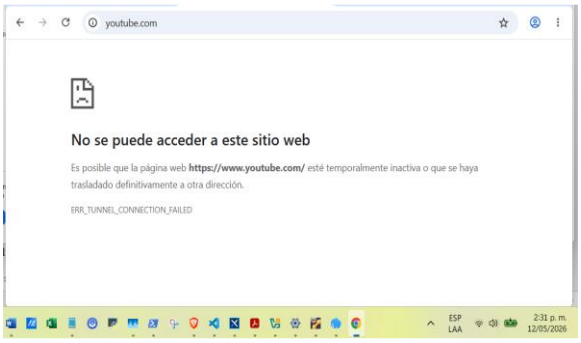
Figura 73.
Resultado de Prueba



Fuente: Autoría Propia

Se realiza la prueba en la dirección de YouTube, la cual tampoco permite el acceso, lo que nos confirma que las reglas y filtros están funcionando.

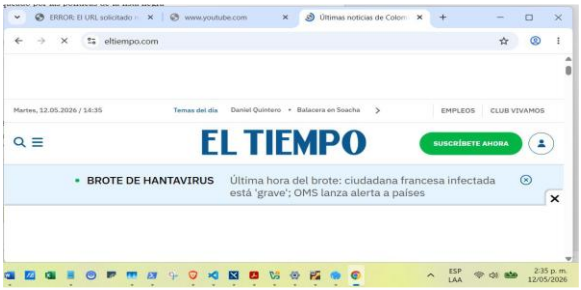
Figura 74.
Resultado de Prueba



Fuente: Autoría Propia

Finalmente, se realizó una prueba de navegación hacia un sitio web permitido correspondiente a un periódico nacional, comprobando que el acceso se realizara correctamente desde los equipos cliente de la red LAN y verificando el adecuado funcionamiento de las políticas de filtrado configuradas en el servicio proxy HTTP.

Figura 75.
Resultado de la Prueba



Fuente: Autoría Propia

8 CONCLUSIONES

1. La instalación de Endian Firewall en Oracle VM VirtualBox posibilitó la creación de un entorno de red segmentado con las zonas LAN (verde), WAN (roja) y DMZ (naranja). La adecuada configuración de interfaces y direcciones IP aseguró una comunicación controlada entre los segmentos y reforzó la seguridad perimetral en el entorno virtual. Esta práctica también permitió reconocer la relevancia de la segmentación de redes y del uso de firewalls para proteger servicios esenciales y aplicaciones corporativas [4], [5], [10].

2. La definición de reglas NAT (SNAT y DNAT) hizo posible la interacción entre LAN, DMZ y WAN, mostrando cómo el firewall actúa como núcleo en la traducción y gestión del tráfico. Las pruebas confirmaron que Endian Firewall facilita tanto el acceso seguro a Internet como la publicación controlada de servicios internos, consolidando aprendizajes prácticos sobre arquitecturas seguras y administración de sistemas GNU/Linux [5], [11].

3. La activación de servicios HTTP y FTP en la DMZ permitió comprobar el funcionamiento de servidores expuestos de manera controlada dentro de una infraestructura segura. A su vez, el bloqueo del protocolo ICMP evidenció la correcta aplicación de políticas de restricción y filtrado de tráfico mediante reglas de firewall. Estas configuraciones fortalecieron las competencias en administración de servicios, conectividad y seguridad perimetral en entornos Linux [7], [11].

4. La creación de reglas de acceso entre zonas permitió regular la comunicación entre LAN, WAN y DMZ a través de los protocolos HTTP y FTP, verificando el comportamiento del tráfico permitido y restringido. Las pruebas de conectividad realizadas desde navegadores y consolas demostraron la eficacia de las políticas aplicadas en Endian Firewall, resaltando la importancia del control de acceso y del monitoreo del tráfico en redes corporativas [5], [6].

5. La implementación del proxy HTTP no transparente con autenticación posibilitó la gestión del acceso a Internet desde la LAN mediante políticas de usuarios, grupos y filtrado de contenido. La creación de listas negras y el bloqueo de sitios específicos confirmaron el correcto funcionamiento de las políticas de navegación y autenticación en Endian Firewall. Esta práctica reforzó conocimientos sobre administración de servicios proxy, control de acceso y seguridad informática en sistemas GNU/Linux [5], [8].

9 REFERENCIAS

[1] Linux Professional Institute, "LPIC-1 Exam 101: Determinar y configurar los ajustes de hardware," Learning Materials, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[2] Canonical, Guía del Ubuntu desktop 20.04 LTS, 2023. [En línea]. Disponible en: https://help.ubuntu.com

[3] Debian Project, El manual del administrador de Debian 12.5.0, Debian, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle Corporation, Manual de usuario VirtualBox, Oracle, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] Endian Documentation, Endian UTM 3.2 - Manual de referencia, Endian, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[6] P. F. Hernández y J. Sánchez, "Monitoreo y administración de sistemas Linux," Objeto virtual de información OVI, Repositorio Institucional UNAD, 2022. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/53211

[7] P. F. Hernández y J. Sánchez, "Servidores para administración remota y compartir recursos," Objeto virtual de información OVI, Repositorio Institucional UNAD, 2022. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/53212

[8] J. LaCroix, Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server, Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[9] E. Nemeth, G. Snyder, T. R. Hein, B. Whaley y D. Mackin, UNIX and Linux system administration handbook, 5.ª ed. Addison Wesley Professional, 2018.

[10] Endian UTM 3.2 Reference Manual—Endian UTM 3.2 Reference Manual. (s. f.). Recuperado 18 de mayo de 2026, de https://docs.endian.com/3.2/utm/index.html