SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL: SEGMENTACIÓN DE RED, SERVICIOS EN DMZ Y CONTROL DE ACCESO EN GNU/LINUX

Andrés Felipe Dávila Cuesta
e-mail. afdavilac@unadvirtual.edu.co
Sara Valentina Gaviria Calle
e-mail: svgaviriac@unadvirtual.edu.co
Julián Arturo Gutiérrez Rodas
e-mail. jagutierrezroda@unadvirtual.edu.co
Leidy Natalia Hernández Rodríguez
e-mail: lnhernandezro@unadvirtual.edu.co
Juan Sebastián Quimbayo Cifuentes
e-mail: jsquimbayoc@unadvirtual.edu.co

RESUMEN: *El presente artículo documenta la implementación de una arquitectura de seguridad perimetral en GNU/Linux mediante Endian Firewall Community sobre VirtualBox. Se describe la segmentación de red en zonas LAN, DMZ y WAN, la configuración de NAT, servicios HTTP y FTP en la zona DMZ, reglas de acceso inter_zona y un proxy HTTP no transparente con autenticación NCSA. Las pruebas realizadas confirmaron el correcto filtrado de paquetes y el bloqueo efectivo de tráfico no autorizado, validando una postura de seguridad basada en el principio de mínimo privilegio. [1]*

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

1. INTRODUCCIÓN

En este trabajo se presenta la implementación práctica realizada por el grupo 202338299_3, abarcando la configuración de Endian Firewall en VirtualBox, políticas NAT, servicios en zona DMZ, reglas de acceso inter_zona y un proxy HTTP con autenticación, demostrando la viabilidad de estas herramientas en entornos académicos y empresariales. [1]

2. TEMÁTICA 1: Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

2.1 Esquema de Red

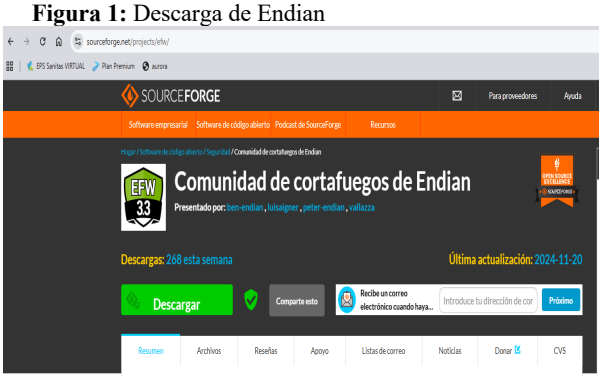
Verde (LAN) eth1 192.168.10.0/24 192.168.10.1
Naranja (DMZ) eth2 192.168.20.0/24 192.168.20.1
Roja (WAN) eth0 DHCP (Internet) Asignada por el router.

2.2 Configuración

2.2.1 Descarga de Endian Firewall

Endian Firewall Community (EFW) es una distribución de seguridad Linux "llave en mano" que convierte su sistema en un dispositivo de seguridad completo con funcionalidades de Gestión Unificada de Amenazas (UTM). El software ha sido diseñado para ofrecer la mejor usabilidad, es muy fácil de instalar, usar y administrar y a la vez es sumamente flexible. [1]

Figura 1: Descarga de Endian



Fuente: Autoría Propia

Posteriormente, se procedió con el despliegue del sistema operativo Linux Lite, el cual fue seleccionado como la distribución base tanto para la estación de trabajo de la red local (Zona Verde) como para el servidor de la zona perimetral (Zona Naranja). Esta elección técnica se fundamenta en la ligereza y eficiencia de dicha distribución, garantizando un rendimiento óptimo y un consumo controlado de recursos dentro del entorno virtualizado. Como se ilustra en la Figura 2, el proceso comenzó con la obtención de la versión correspondiente desde su plataforma oficial.

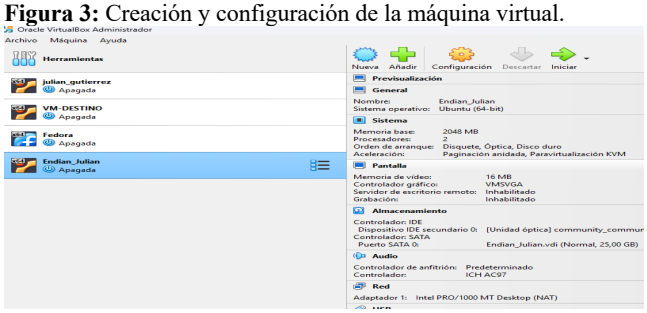
Figura 2: Descarga de Linux Lite 7.8

Fuente: Autoría Propia

Una vez obtenidas las imágenes ISO requeridas tanto para el firewall perimetral como para los equipos cliente y

servidor, la siguiente fase consistió en preparar el entorno de hardware virtualizado. Se procedió a estructurar la máquina virtual en Oracle VirtualBox, asignando los recursos computacionales necesarios (como memoria RAM, almacenamiento y procesadores) para garantizar la estabilidad del sistema UTM. Como se detalla en la Figura 3, se configuró el entorno principal destinado a alojar la instancia de Endian Firewall.

Figura 3: Creación y configuración de la máquina virtual.

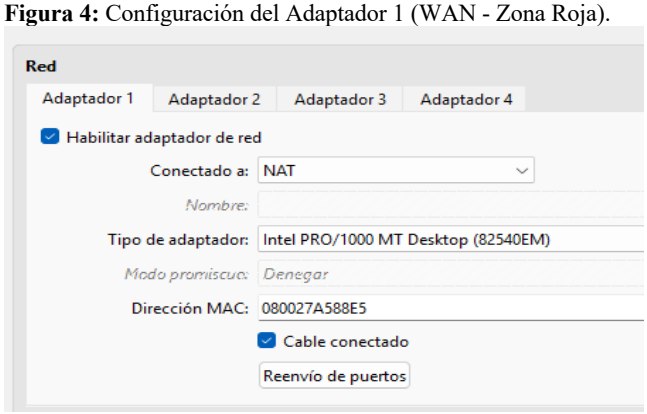


Fuente: Autoría Propia

Con los recursos de hardware de la máquina virtual definidos, la fase más crítica para el funcionamiento del UTM consistió en la segmentación de las interfaces de red. Para simular correctamente una arquitectura de seguridad perimetral, fue necesario habilitar y mapear tres adaptadores de red distintos en VirtualBox, cada uno representando un nivel de confianza específico: la red externa (Roja), la red interna (Verde) y la zona desmilitarizada (Naranja). El enrutamiento preciso de estas tarjetas virtuales es fundamental para garantizar que el firewall pueda interceptar y filtrar los paquetes adecuadamente.

Para el caso del **Adaptador 1 (WAN - Internet)**, como se observa en la Figura 4, la interfaz se configuró en modo NAT para establecer la conexión hacia el mundo exterior. Este segmento corresponde a la zona roja, la cual representa la red insegura desde donde pueden originarse potenciales ataques, motivo por el cual el firewall debe vigilar exhaustivamente todo el tráfico entrante por esta puerta.

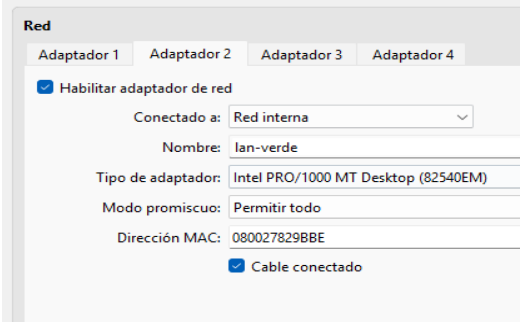
Figura 4: Configuración del Adaptador 1 (WAN - Zona Roja).



Fuente: Autoría Propia

Posteriormente, para el **Adaptador 2 (Red interna)**, tal como se detalla en la Figura 5, la tarjeta de red se configuró bajo la modalidad de red interna con la nomenclatura "lan-verde". Este segmento representa la zona de confianza dentro de la topología lógica, lugar donde se interconectan los equipos de cómputo de los empleados y el personal administrativo. Al tratarse de un área altamente protegida, el sistema restringe por completo el ingreso de cualquier paquete de datos proveniente de la red pública (Internet), a menos que las reglas de acceso del firewall lo permitan explícitamente.

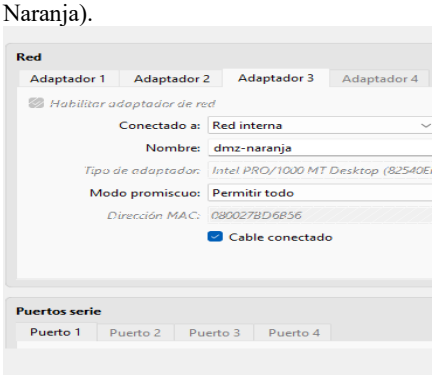
Figura 5: Configuración del Adaptador 2 (LAN - Zona Verde).



Fuente: Autoría Propia

Finalmente, para el **Adaptador 3 (Zona Desmilitarizada o DMZ)**, la interfaz se configuró igualmente como una red interna bajo la nomenclatura "dmz-naranja", tal como se detalla en la Figura 6. Este segmento funciona como una zona intermedia destinada exclusivamente a albergar aquellos servidores que requieren ser visibles y accesibles desde redes públicas (como una página web o un servidor de archivos), pero que no deben estar dentro de la red privada local (Zona Verde). Esta separación lógica constituye una capa crítica de seguridad perimetral: si un atacante logra comprometer la integridad de un servidor expuesto en la Zona Naranja, las políticas de aislamiento del firewall impedirán que realice movimientos laterales o "salte" lateralmente hacia los equipos de la red administrativa de confianza. Asimismo, durante las pruebas de laboratorio, el parámetro de "Modo promiscuo" se estableció en "Permitir todo" para optimizar el flujo de datos y facilitar el diagnóstico de conectividad entre las distintas máquinas virtuales.

Figura 6: Configuración del Adaptador 3 (DMZ - Zona Naranja).

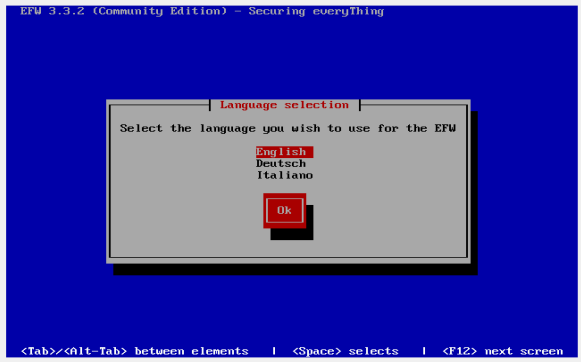


Fuente: Autoría Propia

Una vez concluida la parametrización de las tres interfaces de red en la plataforma de virtualización, se procedió a iniciar la ejecución de la máquina virtual cargando la imagen ISO correspondiente. Este paso marca el final de la configuración del hardware virtual y el inicio

del despliegue del sistema operativo. Como se ilustra en la Figura 7, el asistente de instalación arranca de forma interactiva, presentando en primera instancia la ventana para la selección del idioma del sistema.

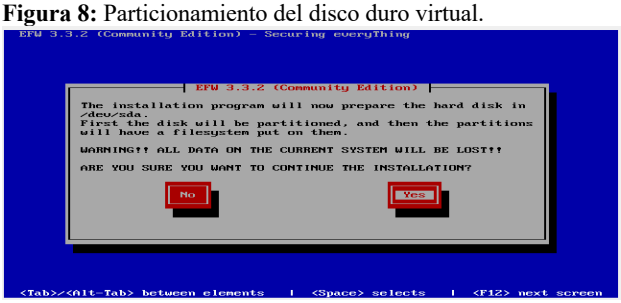
Figura 7: Instalación de Endian



Fuente: Autoría Propia

Luego de definir el idioma de la interfaz, el asistente interactivo inicia formalmente la preparación del sistema de archivos dentro del entorno virtual. Como se ilustra en la Figura 8, el instalador solicita una confirmación explícita para proceder con el particionamiento automático del disco duro virtual dev/sda. Este paso es crítico, ya que el sistema operativo advierte sobre la eliminación de cualquier dato previo con el fin de estructurar las particiones nativas de GNU/Linux necesarias para el correcto funcionamiento del núcleo del firewall.

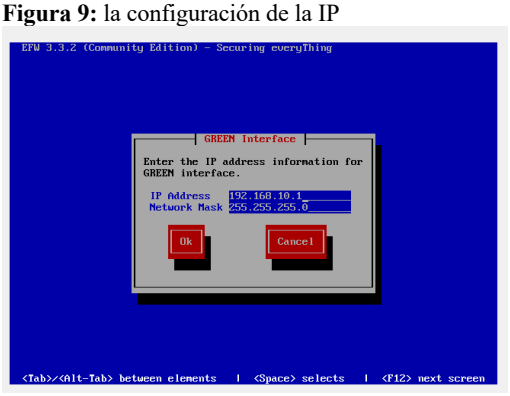
Figura 8: Particionamiento del disco duro virtual.



Fuente: Autoría Propia

Después del particionamiento del almacenamiento y finalizada la copia de los archivos base del sistema, el instalador completa la carga del núcleo y reinicia la máquina virtual para dar paso a la configuración inicial de las interfaces a través de la consola de comandos. Como se ilustra en la Figura 9, el primer parámetro crítico requerido por el asistente es la parametrización de la interfaz de la red local (GREEN). En esta etapa se define la dirección IP estática que asumirá el cortafuegos dentro de la intranet, la cual cumplirá la función primordial de puerta de enlace (Gateway) predeterminada para todos los dispositivos internos que conformen la red administrativa local.

Figura 9: la configuración de la IP



Fuente: Autoría Propia

Tras consolidar la dirección de la intranet y guardados los parámetros lógicos de la tarjeta, el asistente finaliza los scripts automatizados de la instalación base y ejecuta el primer reinicio autónomo del sistema operativo. Este hito marca la culminación definitiva de la fase de despliegue por terminal. Como se ilustra en la Figura 10, la plataforma arranca de manera exitosa y despliega el menú principal de administración en modo texto (CLI). En esta interfaz de consola se confirma el estado activo de la zona GREEN (asociada al dispositivo eth0), detallando tanto la máscara de red como la URL de gestión web protegida (https://192.168.10.1:10443), la cual es indispensable para realizar las configuraciones perimetrales avanzadas en las siguientes etapas.

Figura 10: Implementación exitosa de Endian Firewall.

Fuente: Autoría Propia

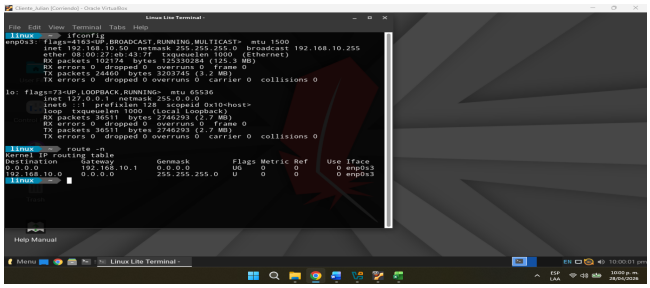
Tras confirmar el arranque exitoso del cortafuegos y obtener su dirección de gestión local, la siguiente fase operativa consistió en inicializar la estación de trabajo que actuará como cliente interno. Para este propósito, se encendió la máquina virtual correspondiente a la intranet administrativa. Como se ilustra en la Figura 11, este entorno fue desplegado utilizando la distribución Linux Lite, situándose lógicamente dentro de la Zona Verde (LAN). Este equipo cumplirá el rol fundamental de nodo de gestión, permitiendo al administrador acceder de forma segura al panel web del sistema UTM y validar las políticas de filtrado perimetral.

Figura 11: Creación de VM (Cliente_Julian) con Linux Lite

Fuente: Autoría Propia

Posteriormente, se realiza la creación de una máquina virtual cliente basada en Linux Lite, la cual será utilizada para ejecutar pruebas de conectividad, navegación y validación de reglas de seguridad implementadas en el firewall. Como se ilustra en la Figura 11, esta estación de trabajo se integra a la zona GREEN con el propósito de simular un entorno corporativo interno.

Figura 12: Identidad al cliente por comandos ya que no hay DHCP



Fuente: Autoría Propia

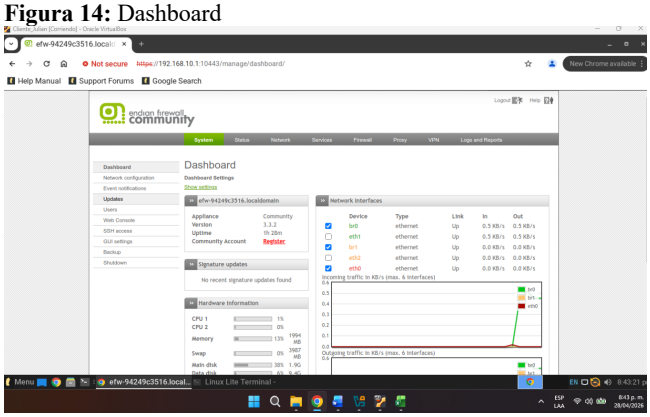
Debido a que el servicio DHCP no fue habilitado inicialmente en la red interna, fue necesario realizar la configuración manual de los parámetros de red en el cliente Linux Lite. Como se muestra en la Figura 12, se asignó una dirección IP estática junto con la puerta de enlace predeterminada, permitiendo establecer comunicación con el firewall y acceso controlado hacia otras zonas de la arquitectura de red.

Figura 13: Acceso a la Interfaz Web (GUI)

Fuente: Autoría Propia

Una vez configurada correctamente la conectividad del cliente, se procedió a validar el acceso remoto al panel de administración de Endian Firewall mediante el navegador web. Como se evidencia en la Figura 13, la conexión se realizó utilizando el puerto seguro 10443, confirmando la disponibilidad del servicio de administración gráfica dentro de la red LAN.

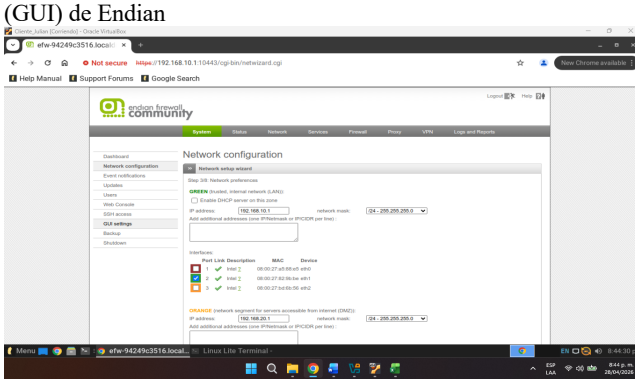
Figura 14: Dashboard



Fuente: Autoría Propia

El dashboard principal de Endian Firewall proporciona información relevante sobre el estado operativo del sistema, interfaces activas, tráfico monitoreado y políticas configuradas. Como se observa en la Figura 14, esta interfaz centralizada facilita la administración integral de los servicios de seguridad implementados en la infraestructura de red.

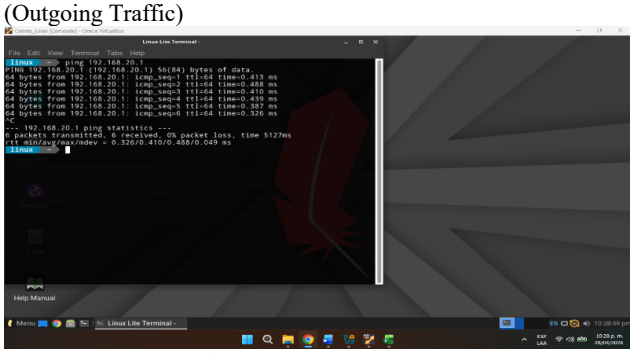
Figura 15: Panel de configuración de red en la interfaz gráfica (GUI) de Endian



Fuente: Autoría Propia

Como se ilustra en la Figura 15, el asistente de configuración de red permite administrar de manera organizada las interfaces GREEN, ORANGE y RED, facilitando la segmentación lógica del tráfico y la implementación de políticas de seguridad dentro del entorno perimetral.

Figura 16: Configuración de Políticas de Tráfico Saliente (Outgoing Traffic)



Fuente: Autoría Propia

En esta fase se configuró la regla de firewall necesaria para permitir que los paquetes de datos se desplacen desde la red interna hacia la red pública. Por defecto, Endian Firewall aplica una política de "Denegación Implícita", por lo que fue necesario definir una regla explícita de Permisión (ALLOW). [1]

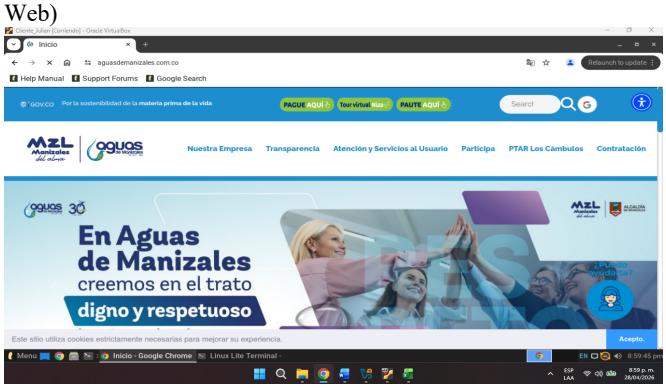
Figura 17: Validación y Ajuste de DNS

Fuente: Autoría Propia

Se noto que el ping a IPs (como 8.8.8.8) funcionaba, pero a nombres (como google.com) no.

Comando: echo "nameserver 8.8.8.8" | sudo tee /etc/resolv.conf.

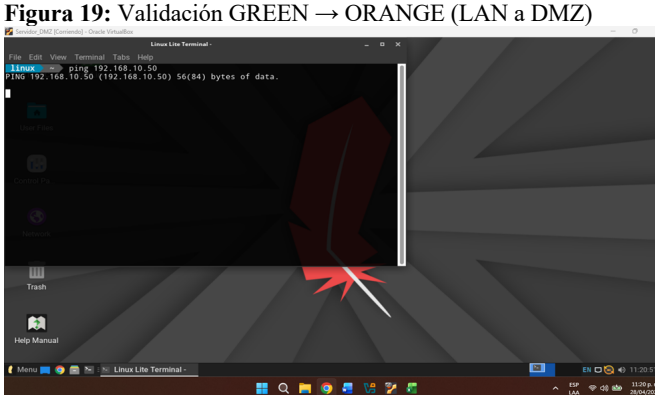
Figura 18: Validación de la Capa de Aplicación (Navegación Web)



Fuente: Autoría Propia

Como prueba definitiva de la operatividad del sistema, se realizó una petición HTTPS desde el navegador Google Chrome en el host cliente hacia el dominio de una entidad externa

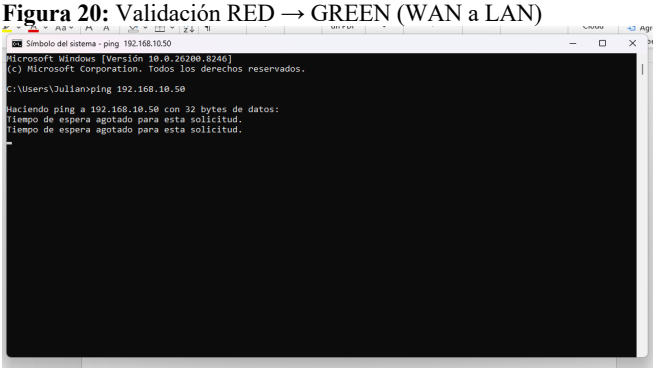
Figura 19: Validación GREEN → ORANGE (LAN a DMZ)



Fuente: Autoría Propia

Esta prueba verificó la conectividad permitida desde la zona GREEN (LAN) hacia la zona ORANGE (DMZ). Se ejecutó un ping desde el cliente Linux Lite ubicado en la red interna (192.168.10.50) hacia la interfaz naranja del firewall (192.168.20.1). El resultado exitoso confirma que los equipos de la red de mayor confianza pueden acceder a los servidores alojados en la DMZ, tal como está definido por defecto en las políticas de Endian Firewall.

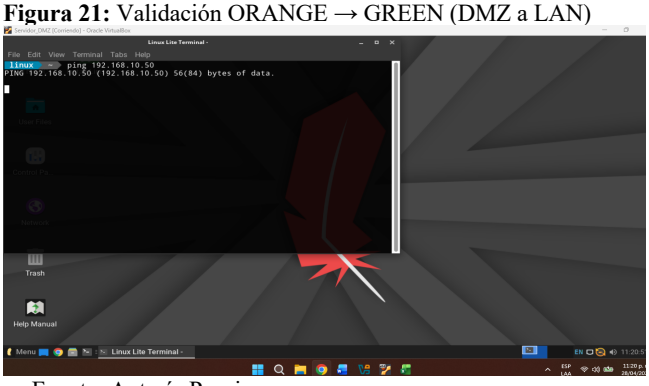
Figura 20: Validación RED → GREEN (WAN a LAN)



Fuente: Autoría Propia

Con el propósito de validar la protección de la red interna, se simuló un ataque desde la zona externa (WAN). Se intentó realizar ping desde el equipo host físico hacia el cliente de la zona GREEN (192.168.10.50). El tráfico fue bloqueado completamente por el firewall, demostrando que Endian Firewall protege eficazmente la LAN contra accesos no autorizados provenientes de Internet.

Figura 21: Validación ORANGE → GREEN (DMZ a LAN)



Fuente: Autoría Propia

Esta validación es crítica para comprobar el aislamiento de la DMZ. Se intentó establecer comunicación (ping) desde un servidor ubicado en la zona naranja hacia un equipo en la zona verde. El resultado de timeout confirma que, aunque un atacante comprometa un servidor en la DMZ, no podrá moverse lateralmente hacia la red interna, cumpliendo con uno de los principios fundamentales de la seguridad perimetral.

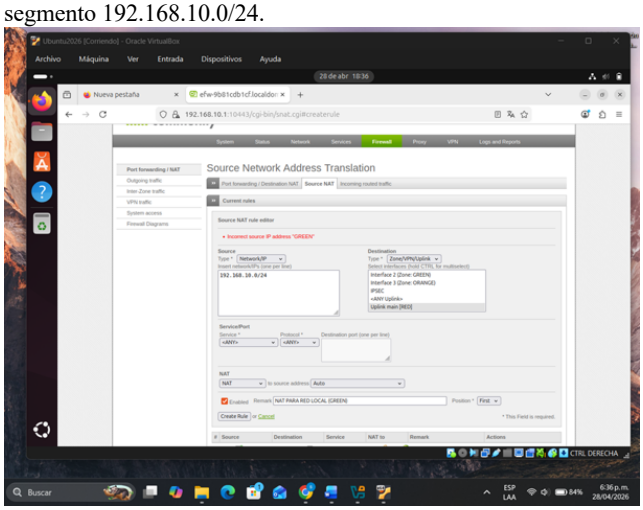
3. TEMÁTICA 2: CONFIGURACIÓN NAT.

3.1 Configuración de Source NAT (SNAT) para la Zona Verde (LAN)

Se creó una regla de Source NAT en el módulo de Firewall de Endian para permitir el acceso a Internet desde la LAN. Se definió como origen el segmento 192.168.10.0/24 (Zona Verde) y como destino la interfaz Uplink main (RED). Esta configuración habilita la salida a la red externa mediante la traducción de direcciones de origen.

Como se evidencia en la figura 22, la política SNAT permite que los equipos de la red LAN accedan a Internet mediante traducción dinámica de direcciones IP, garantizando conectividad segura y controlada [1].

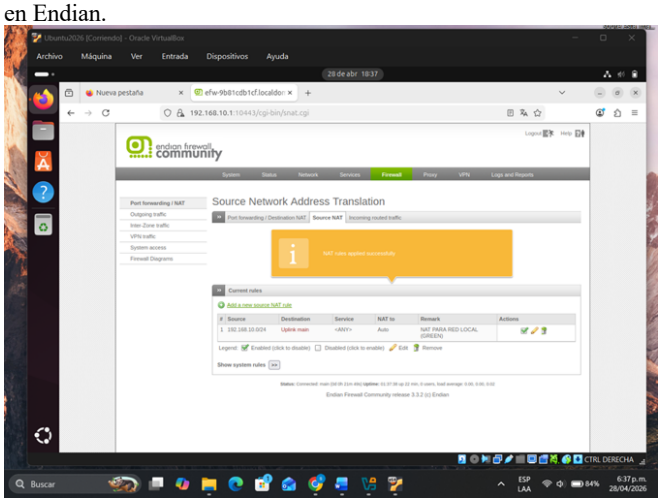
Figura 22: Configuración de regla Source NAT para el segmento 192.168.10.0/24.



Fuente: Autoría Propia

La figura 23 confirma que las reglas NAT fueron aplicadas correctamente dentro de Endian Firewall, permitiendo el tráfico autorizado entre las zonas configuradas.

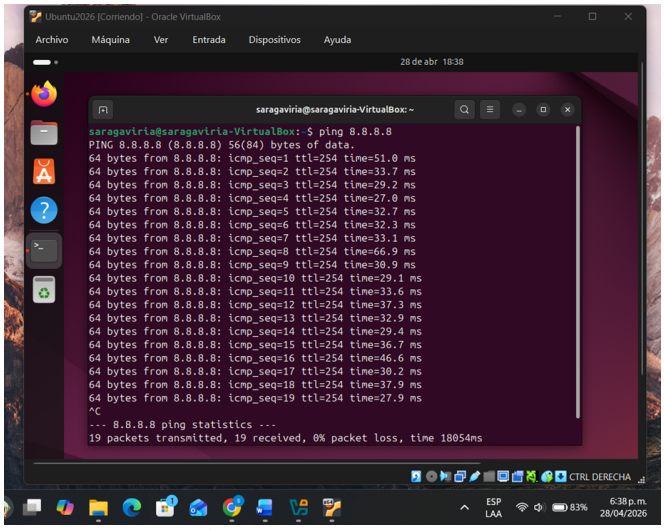
Figura 23. Confirmación de aplicación exitosa de reglas NAT en Endian.



Fuente: Autoría Propia

La validación de esta regla se realizó mediante una prueba de conectividad ICMP (ping) desde una estación de trabajo Ubuntu situada en la LAN hacia los servidores DNS de Google (8.8.8.8), obteniendo una respuesta exitosa y confirmando la salida a internet. [4]

Figura 24: Verificación de salida a Internet mediante ICMP desde la Zona Verde.



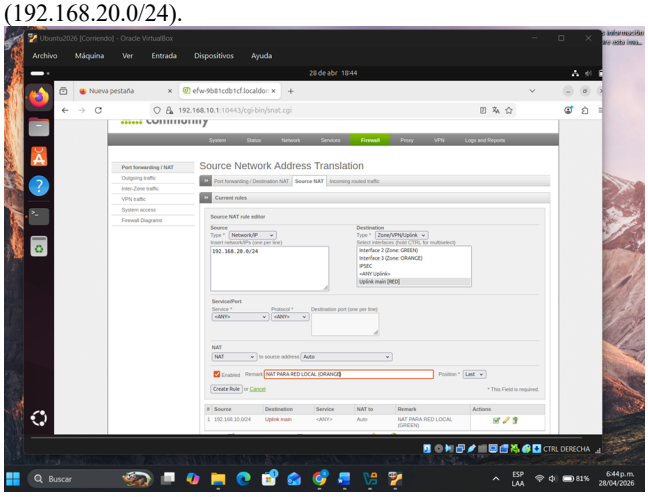
Fuente: Autoría Propia

Los resultados obtenidos en esta prueba confirman el correcto funcionamiento de la directiva de traducción dinámica de direcciones (SNAT). Esto demuestra que los hosts de la intranet pueden establecer conexiones salientes hacia la red pública de manera transparente y segura, manteniendo oculto el direccionamiento IP privado de la red local. Con esta validación de conectividad en la zona de confianza, se completan los requerimientos básicos de salida para la LAN.

3.2 Configuración de NAT para la Zona Naranja (DMZ)

Con el objetivo de que los servidores alojados en la zona DMZ puedan realizar actualizaciones o consultas externas de forma controlada, se implementó una regla de NAT para el segmento 192.168.20.0/24. Esta configuración garantiza que el servidor web pueda comunicarse con la red WAN manteniendo el aislamiento de la red interna.

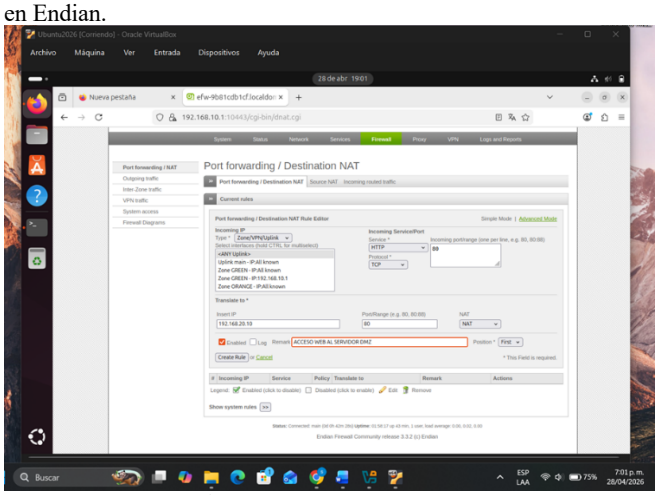
Figura 25: Creación de política NAT para la red Orange (192.168.20.0/24).



Fuente: Autoría Propia

Se configuró una regla Source NAT específica para la zona ORANGE, permitiendo que los servidores alojados en la DMZ puedan realizar actualizaciones de paquetes, consultas DNS y otras comunicaciones necesarias hacia Internet, sin comprometer el aislamiento de la red LAN.

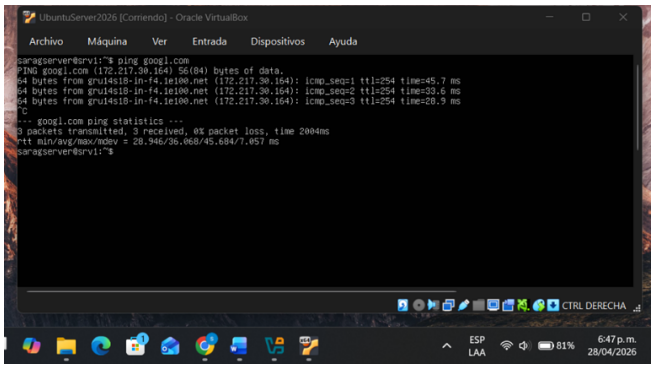
Figura 26: Confirmación de aplicación exitosa de reglas NAT en Endian.



Fuente: Autoría Propia

Se verificó la conectividad desde el servidor Ubuntu Server alojado en la DMZ mediante la resolución de nombres y ping hacia el dominio google.com, validando la correcta traducción de direcciones para esta zona. [4]

Figura 27: Acceso exitoso al servidor web en la DMZ desde la red externa.



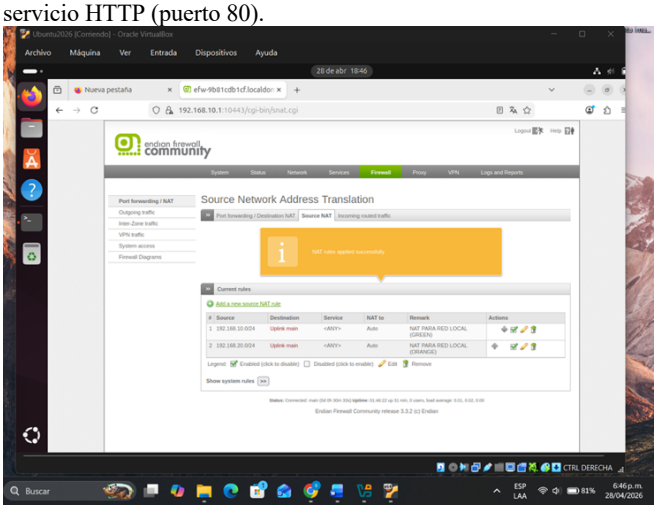
Fuente: Autoría Propia

Se validó la conectividad desde el servidor Ubuntu ubicado en la zona DMZ. La prueba incluyó resolución de nombres y acceso a sitios externos, confirmando que las reglas NAT permiten la comunicación necesaria para el mantenimiento y operación de los servicios publicados.

3.3 Implementación de Port Forwarding / Destination NAT (DNAT)

Para permitir que los servicios de la zona DMZ sean accesibles desde el exterior de forma segura, se configuró una regla de reenvío de puertos (Port Forwarding). La regla redirige el tráfico entrante desde cualquier origen en la interfaz RED (WAN) a través del puerto TCP 80 hacia la dirección IP privada del servidor web (192.168.20.10).

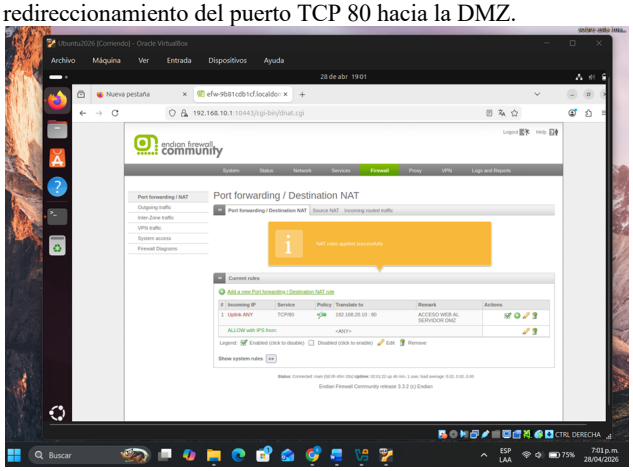
Figura 28: Configuración de DNAT para publicación del servicio HTTP (puerto 80).



Fuente: Autoría Propia

Se implementó una regla de Destination NAT para redirigir el tráfico entrante por el puerto 80 (HTTP) desde la zona WAN hacia el servidor web ubicado en la DMZ con dirección 192.168.20.10. Esta técnica permite publicar servicios de forma segura sin exponer directamente las direcciones privadas.

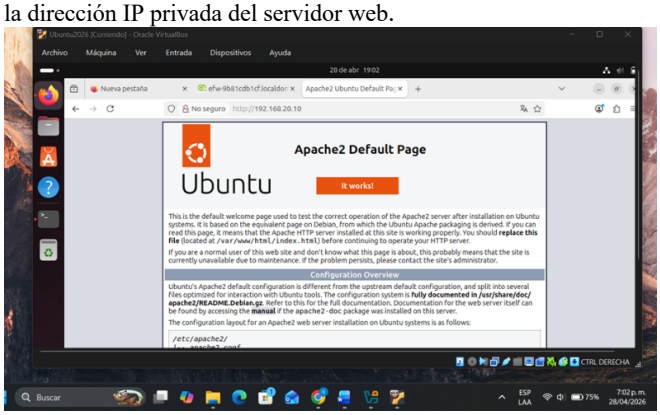
Figura 29: Implementación de la regla de Port Forwarding para redireccionamiento del puerto TCP 80 hacia la DMZ.



Fuente: Autoría Propia

Esta técnica permite publicar el servicio web sin exponer la dirección IP real del servidor a la red pública, actuando el firewall como un escudo perimetral. La efectividad de la regla se comprobó accediendo a la página por defecto de Apache desde el navegador.

Figura 30: Verificación de acceso al servidor Apache mediante la dirección IP privada del servidor web.



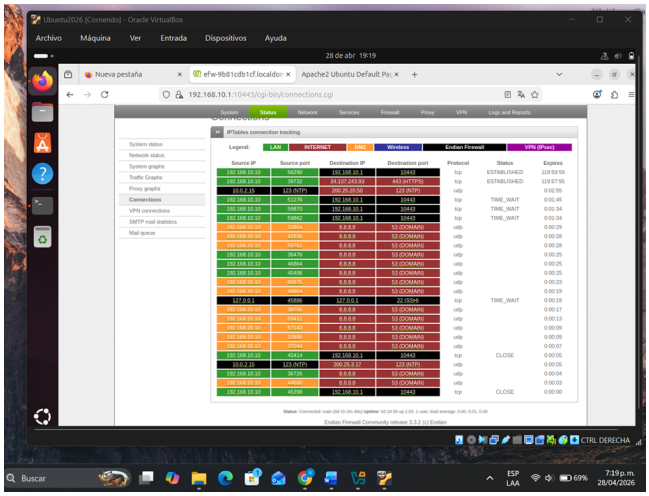
Fuente: Autoría Propia

Se realizó la prueba definitiva de publicación de servicios accediendo al servidor Apache desde un navegador externo. El resultado exitoso confirma que el Port Forwarding funciona correctamente y que el servicio HTTP está disponible de forma segura desde Internet.

3.4. Monitorización de Conexiones (IPtables)

Finalmente, se realizó una auditoría del tráfico en tiempo real utilizando el monitor de conexiones de Endian (basado en IPtables). En el panel se observaron flujos de datos activos con estado ESTABLISHED desde las IPs 192.168.10.10 (GREEN) y 192.168.20.10 (ORANGE) hacia destinos externos, lo que ratifica que las políticas de NAT se están aplicando correctamente según el diseño de seguridad propuesto.

Figura 31: Registro de conexiones activas (ESTABLISHED) en el monitor de IPtables.



Fuente: Autoría Propia

A través del monitor de conexiones de Endian Firewall se observaron las sesiones activas en tiempo real. Se pudieron identificar conexiones ESTABLISHED desde las zonas GREEN y ORANGE hacia destinos externos, validando el correcto funcionamiento de las reglas NAT y políticas de tráfico.

4. TEMÁTICA 3: SERVICIOS HTTP Y FTP EN ZONA DMZ

4.1 Verificar fecha y hora del sistema

En primera instancia, se ejecutó el comando respectivo para mostrar la fecha y hora actual del sistema en las evidencias:

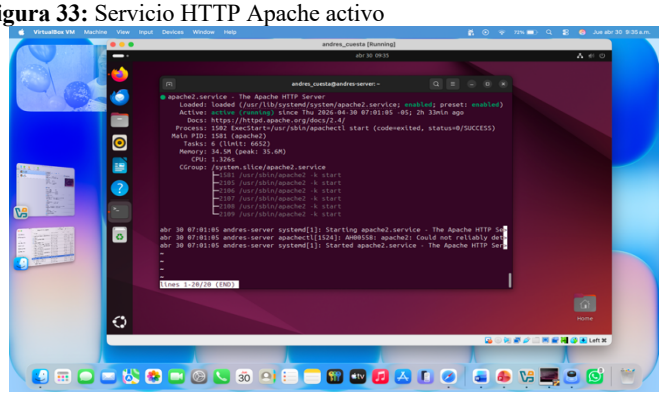
Figura 32: Fecha y hora del sistema en DMZ.

Fuente: Autoría Propia

Evidencia la fecha y hora actual del sistema al momento de ejecutar los procedimientos de configuración de servicios en la zona DMZ.

Posteriormente, se ingresó la directiva para validar el estado del servicio Apache:

Figura 33: Servicio HTTP Apache activo



Fuente: Autoría Propia

Esta captura evidencia que el servicio Apache Web Server está activo y funcionando en el puerto 80, correspondiente al servicio HTTP habilitado en el servidor de la zona DMZ.

Figura 34 : Puerto 80 HTTP activo

Fuente: Autoría Propia

Esta captura evidencia que el servicio Apache está escuchando activamente en el puerto 80 (HTTP), confirmando que el servicio web está disponible y funcionando correctamente en el servidor de la zona DMZ.

4.2 Instalar y configurar FTP

Figura 35: Ejecución correcta que verifica el FTP

Fuente: Autoría Propia

Se procedió con la instalación del paquete vsftpd en el servidor de la zona DMZ. Esta captura muestra la ejecución exitosa del comando de instalación del servidor FTP.

Figura 36: Ejecución correcta que verifica el FTP.

Fuente: Autoría Propia

Tras la instalación, se verificó el estado del servicio vsftpd. El resultado indica que el servidor FTP se encuentra activo y en ejecución, preparado para gestionar transferencias de archivos.

Figura 37: Servicio FTP activo en puerto 21

Fuente: Autoría Propia

Esta captura evidencia que el servicio FTP vsftpd está instalado, activo y escuchando en el puerto 21, confirmando que el servicio FTP está disponible en el servidor de la zona DMZ.

4.3. Denegar protocolo ICMP (ping)

Configuración de reglas ICMP con iptables.

Figura 38: Bloqueo ICMP mediante iptables.

Fuente: Autoría Propia

Con el objetivo de aplicar el principio de mínimo privilegio, se configuraron reglas iptables para denegar el protocolo ICMP tanto de entrada como de salida en el servidor DMZ. Esta medida reduce la superficie de ataque del servidor.

4.4 Verificaciones finales de todos los servicios.

Figura 39: Verificación de fecha y hora en el servidor DMZ.

Fuente: Autoría Propia

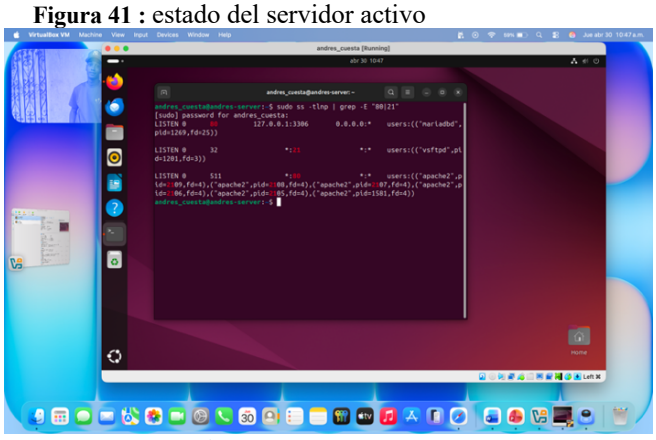
Al finalizar la configuración de servicios se realizó una última verificación de fecha y hora del servidor en la DMZ, asegurando la integridad de los registros generados durante todo el proceso.

Figura 40: Estado del servicio FTP (vsftpd).

Fuente: Autoría Propia

Se comprobó nuevamente el estado del servicio vsftpd tras completar todas las configuraciones, confirmando que continúa activo y funcional.

Figura 41 : estado del servidor activo



Fuente: Autoría Propia

Se listaron todos los puertos en estado de escucha en el servidor DMZ. Esta verificación permitió confirmar que únicamente los servicios HTTP y FTP se encuentran disponibles según lo requerido.

Figura 42: Reglas finales de iptables.

Fuente: Autoría Propia

Esta captura evidencia la verificación final de las reglas iptables aplicadas en el servidor de la zona DMZ, mostrando las reglas DROP para icmp type 8 en la cadena INPUT y icmp type 0 en la cadena OUTPUT, confirmando el correcto bloqueo del protocolo ICMP con fecha y hora del sistema 19 de marzo de 2026.

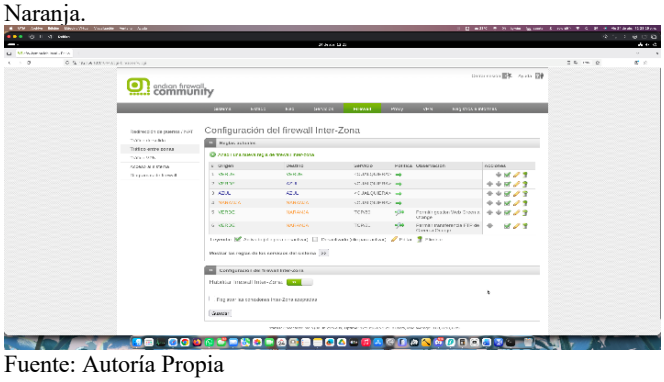
5. TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO. PRODUCTO ESPERADO:

Desarrollo Técnico y Validación de Productos

5.1. Gestión de Tráfico Inter-Zona y Publicación de Servicios

La primera fase operativa consistió en romper el aislamiento predeterminado entre la red administrativa y el segmento de servidores. Se implementaron reglas específicas para autorizar flujos de gestión hacia la DMZ, habilitando los protocolos TCP/80 (HTTP) para servicios web y TCP/21 (FTP).

Figura 43: Configuración de reglas inter-zona activas para la comunicación controlada entre el segmento Verde y el segmento Naranja.

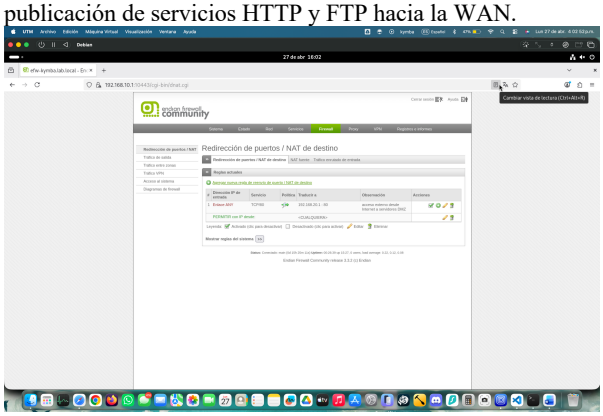


Fuente: Autoría Propia

Simultáneamente, para habilitar la visibilidad de estos servicios desde redes externas (Internet), se configuró la técnica de Traducción de Direcciones de Red de Destino (DNAT) o Port Forwarding. Esta configuración permite que peticiones externas dirigidas a la interfaz WAN sean

interceptadas y canalizadas de forma transparente hacia el servidor interno 192.168.10.2, protegiendo la topología real de la red ante escaneos no autorizados

Figura 44: Implementación de reglas de DNAT para la publicación de servicios HTTP y FTP hacia la WAN.

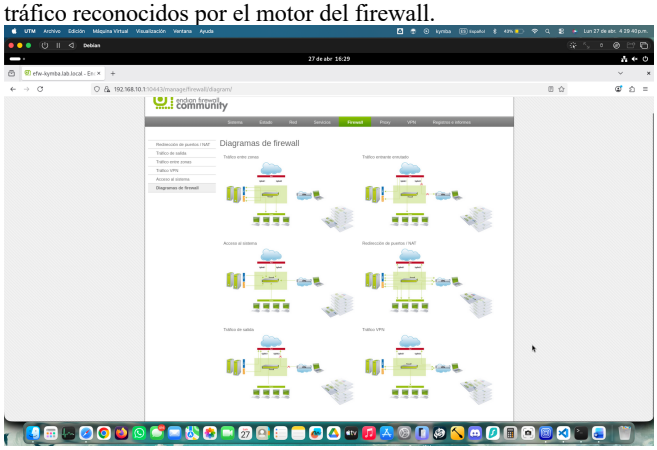


Fuente: Autoría Propia

5.2. Auditoría Lógica de Topología y Conectividad de Capa 7

La persistencia y coherencia de las políticas fueron verificadas mediante una auditoría visual utilizando la herramienta Diagramas de Firewall de Endian. Esta representación gráfica validó la existencia de los túneles de comunicación autorizados y la ausencia de conflictos lógicos en la tabla de reglas.

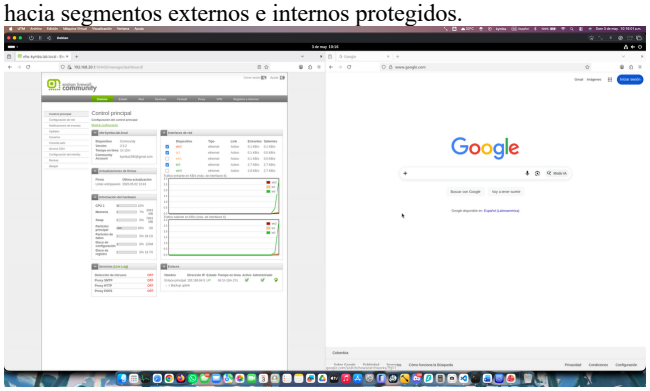
Figura 45: Auditoría gráfica de la arquitectura lógica y flujos de tráfico reconocidos por el motor del firewall.



Fuente: Autoría Propia

Posteriormente, se realizó la validación funcional desde la estación de gestión Debian. Se comprobó el éxito del NAT Masquerading permitiendo una navegación fluida hacia la WAN (Google.com) mientras se mantenía una sesión administrativa activa hacia el Dashboard del firewall en la zona DMZ, certificando la correcta resolución de nombres (DNS) y el enrutamiento inter-zona. [5]

Figura 46: Validación funcional de navegación web simultánea hacia segmentos externos e internos protegidos.



Fuente: Autoría Propia

5.3. Segmentación De Tráfico Saliente Y Validación De Sockets

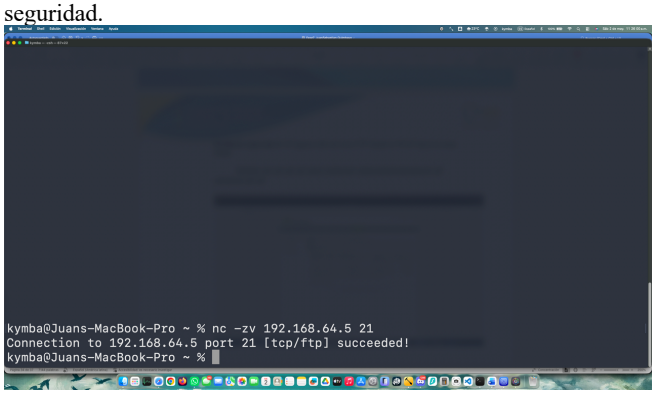
Para mitigar riesgos de exfiltración de datos, se blindó la frontera de salida aplicando una política de "Denegación por Defecto". Se estructuró un conjunto de 10 reglas jerárquicas que segmentan el tráfico saliente; por ejemplo, se restringió el uso de FTP exclusivamente a la zona LAN y se autorizó el tráfico DNS e ICMP solo para fines de diagnóstico y resolución técnica.

Figura 47: Política de seguridad de salida granular fundamentada en el principio de menor privilegio.

Fuente: Autoría Propia

La prueba reina de esta arquitectura se ejecutó desde un host externo simulando un cliente en Internet; mediante la utilidad Netcat (nc), se realizó un escaneo de socket hacia la IP pública del firewall. El resultado "succeeded!" en el puerto 21 confirmó que la regla de DNAT es totalmente operativa y que el firewall procesa correctamente las peticiones de entrada hacia los recursos protegidos de la DMZ.

Figura 48: Prueba técnica de conectividad extrema confirmando la apertura exitosa del socket a través del perímetro de seguridad.



Fuente: Autoría Propia

La validación sistemática de estos productos confirma que una arquitectura perimetral robusta depende de la granularidad de sus reglas. La combinación de filtrado inter-zona, DNAT y políticas de salida restrictivas no solo garantiza la disponibilidad de los servicios, sino que establece una postura de seguridad proactiva capaz de mitigar movimientos laterales y accesos no autorizados en infraestructuras híbridas

6. Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

El control del acceso a Internet dentro de una red corporativa es una necesidad operativa y de seguridad que va más allá de simplemente bloquear sitios web. Mediante la implementación de un proxy HTTP no transparente sobre la plataforma Endian Firewall, es posible exigir autenticación a cada usuario, registrar sus actividades y aplicar políticas de filtrado de contenido de forma centralizada. En esta temática se documenta la creación de listas negras, la configuración de autenticación NCSA mediante usuario y contraseña, y la verificación del bloqueo efectivo sobre tráfico tanto HTTP plano como HTTPS cifrado. [1]

6.1. Configuración de Lista Negra (Blacklist)

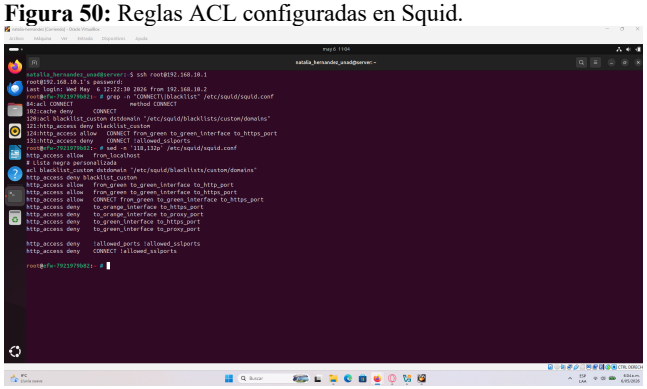
Se creó un perfil de filtrado personalizado en el módulo Proxy HTTP de Endian, incluyendo en la lista negra los siguientes dominios requeridos: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Para garantizar el bloqueo también sobre tráfico HTTPS, se verificó y ajustó la regla de denegación del método CONNECT en el archivo de configuración de Squid, impidiendo el establecimiento de túneles TLS hacia los dominios restringidos.

Figura 49: Lista negra personalizada en Endian Firewall.

Fuente: Autoría Propia

Tras la configuración gráfica de los dominios restringidos, se procedió a validar el comportamiento del motor de filtrado a nivel de consola. Como se observa en la Figura 50, se realizó una verificación directa sobre el archivo de configuración de Squid para confirmar la correcta declaración de las listas de control de acceso (ACL).

Figura 50: Reglas ACL configuradas en Squid.

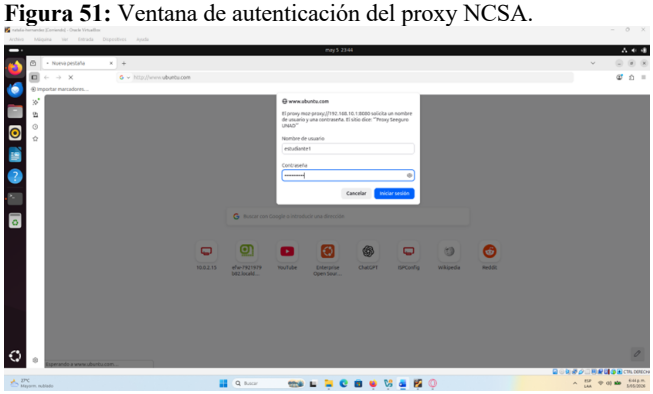


Fuente: Autoría Propia

6.2. Autenticación por Usuario

A través del módulo de proxy de Endian se creó el usuario estudiante1 con contraseña segura, asignándolo a un grupo de usuarios con una política de acceso activa. Esta política vincula el perfil de filtrado (lista negra) con la autenticación NCSA, de modo que ningún equipo de la LAN puede navegar sin presentar credenciales válidas.

Figura 51: Ventana de autenticación del proxy NCSA.



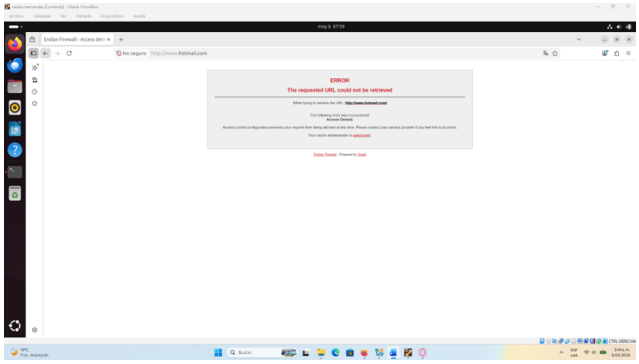
Fuente: Autoría Propia

6.3. Pruebas de Navegación y Análisis de Logs

Se realizaron pruebas desde el equipo cliente (192.168.10.2) en la Zona Verde hacia los portales de la lista negra. Los resultados evidenciaron dos comportamientos diferenciados según el protocolo utilizado por el sitio de destino.

Para tráfico HTTP plano (http://www.hotmail.com), Squid intercepta la solicitud GET y responde con su página predeterminada de acceso denegado (TCP_DENIED/403), siendo esta respuesta plenamente visible en el navegador del cliente.

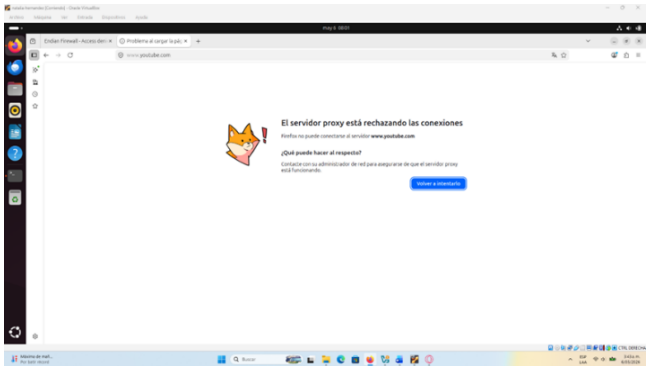
Figura 52: Bloqueo HTTP con código de respuesta 403 Forbidden.



Fuente: Autoría Propia

Para tráfico HTTPS (https://www.youtube.com), el navegador muestra el mensaje "El servidor proxy está rechazando las conexiones". Esto ocurre porque Squid deniega la solicitud de túnel CONNECT antes de que se establezca el cifrado TLS. Al no existir un canal HTTP disponible para inyectar una respuesta HTML, el navegador interpreta el rechazo TCP y muestra su propio mensaje de error nativo. Este comportamiento es técnicamente correcto y esperado en un proxy configurado sin interceptación SSL (SSL Bumping).

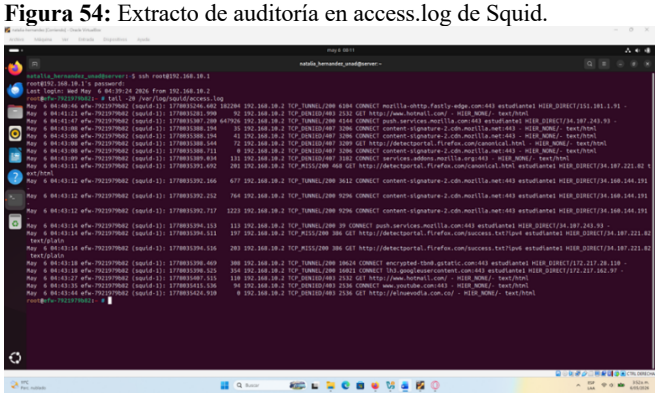
Figura 53: Bloqueo HTTPS y denegación del método CONNECT.



Fuente: Autoría Propia

La trazabilidad del sistema fue verificada mediante el archivo /var/log/squid/access.log, donde se evidenciaron los registros de bloqueo con estado TCP_DENIED/403 para ambos protocolos, así como la identidad del usuario autenticado estudiante1 en cada transacción registrada, permitiendo una auditoría completa de la actividad de navegación.

Figura 54: Extracto de auditoría en access.log de Squid.



Fuente: Autoría Propia

7. CONCLUSIONES

La configuración de Endian Firewall Community en un entorno virtualizado sobre VirtualBox demostró ser una estrategia viable para simular arquitecturas de seguridad reales en contextos académicos. La correcta asignación de las interfaces de red en tres zonas diferenciadas —LAN (verde), DMZ (naranja) y WAN (roja)— permitió establecer una segmentación lógica del tráfico que reproduce el modelo de defensa en profundidad utilizado en entornos empresariales, consolidando competencias prácticas en la instalación y configuración inicial de sistemas UTM sobre plataformas de virtualización. [1]

La implementación de reglas de traducción de direcciones de red (NAT) confirmó que el control del tráfico saliente e entrante puede gestionarse de forma precisa mediante Endian Firewall. La configuración de SNAT para las zonas verde y naranja garantizó la salida controlada a Internet, mientras que el Port Forwarding (DNAT) permitió publicar servicios de la DMZ hacia la WAN sin exponer la topología interna, cumpliendo con el principio de mínimo privilegio. [1]

La habilitación de los servicios Apache (HTTP, puerto 80) y vsftpd (FTP, puerto 21) en el servidor de la zona DMZ evidenció la correcta separación entre la red interna y los recursos publicados hacia el exterior. La aplicación de reglas iptables para bloquear el protocolo ICMP reforzó la postura de seguridad del servidor, confirmando que es posible ofrecer servicios accesibles públicamente sin comprometer la integridad de la red interna.

La configuración de reglas inter-zona en Endian Firewall demostró que una arquitectura perimetral sólida depende de la granularidad y jerarquía de sus políticas de filtrado. La combinación de reglas de acceso entre zonas, DNAT y una política de salida basada en denegación por defecto permitió controlar con precisión los flujos autorizados, mitigando riesgos de movimientos laterales, hecho que fue validado mediante pruebas con Netcat desde perspectivas internas y externas. [1]

La implementación de un proxy HTTP no transparente con autenticación NCSA sobre Endian Firewall demostró que es posible aplicar políticas de control de navegación auditables en entornos corporativos. La creación de listas negras y la exigencia de credenciales para el acceso a Internet garantizaron que ningún usuario pudiera navegar de forma anónima ni acceder a sitios restringidos en tráfico HTTP o HTTPS, siendo los registros del access.log de Squid la evidencia de trazabilidad completa del sistema. [1]

8. REFERENCIAS BIBLIOGRÁFICAS

[1] Endian. (2016). Endian UTM 3.2 Manual de referencia. Endian. http://docs.endian.com/3.2/utm/index.html

[2] Linux Professional Institute. (2022). LPIC-1 Exam 101 – Tema 101: Determinar y configurar los ajustes de hardware. LPI. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[3] Oracle. (2020). Manual de usuario VirtualBox. Oracle. https://www.virtualbox.org/manual/

[4] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

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

[6] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux

[7] Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53211

[8] Hernández, P. F., & Sánchez, J. (2022). Servidores para administración remota y compartir recursos [Objeto virtual de información OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53212

[9] Canonical. (2023). *Help Ubuntu*. Ubuntu. https://help.ubuntu.com/

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