IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD EN GNU/LINUX

Fabio Jesús Diazgranados Martelo
fjdiazgranadosm@unadvirtual.edu.co,
Henry Antonio Rivero Altamar
hariveroa@unadvirtual.edu.co
Jair Jose Valdes Carrascal
jjvaldesc@unadvirtual.edu.co
Julio Gabriel Sanchez Monterroza
jgsanchezmo@unadvirtual.edu.co
Kevin Alberto Salas López
kasalas@unadvirtual.edu.co

RESUMEN: *La protección de sistemas GNU/Linux es un pilar crítico en la gestión de infraestructuras TI, orientada a salvaguardar y proteger los principios de confidencialidad, integridad y disponibilidad de los datos [1]. El presente artículo detalla el despliegue de soluciones de seguridad perimetral mediante la virtualización de Endian Firewall. El proceso técnico abarca desde la implementación de interfaces de red y el enrutamiento NAT, hasta la segregación de servicios en zonas DMZ. Asimismo, se profundizó en la administración del flujo de datos mediante políticas de filtrado y la optimización del acceso web a través de un Proxy HTTP basado en identidades.*

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

1 INTRODUCCIÓN

En la actualidad, la seguridad informática representa uno de los pilares más importantes dentro de la administración de sistemas y redes, debido al crecimiento constante de amenazas digitales y accesos no autorizados a la información. Los sistemas basados en GNU/Linux se han consolidado como una alternativa robusta y segura para la implementación de servicios de red, gracias a su estabilidad, flexibilidad y amplio conjunto de herramientas orientadas a la administración y protección de entornos tecnológicos [2].

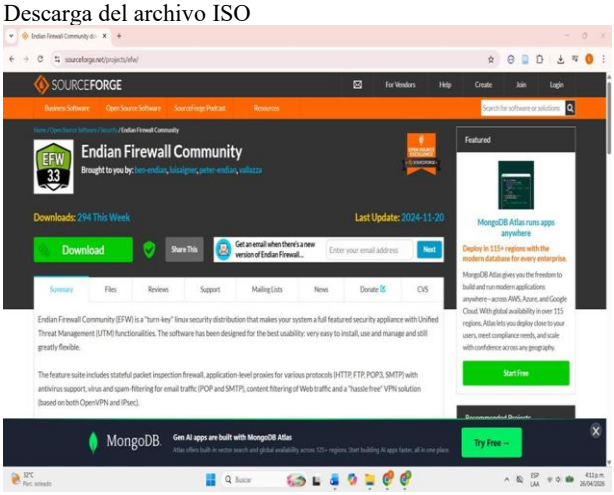
El presente trabajo tiene como propósito aplicar conceptos y técnicas relacionadas con la implementación de seguridad en GNU/Linux, mediante el desarrollo de diferentes actividades prácticas en un entorno virtualizado con VirtualBox y GNU/Linux Endian. Durante el proceso se realizaron configuraciones de red utilizando NAT y DMZ, se definieron reglas de acceso para el control del tráfico y se implementó un Proxy HTTP no transparente con autenticación, permitiendo gestionar y supervisar el acceso a Internet dentro de la red [3].

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

2.1 CARACTERÍSTICAS GENERALES

Para llevar a cabo el proceso de configuración e implementación del sistema de gestión de hosting, el usuario ha descargado el archivo ISO de Endian desde su página web oficial. Este paso ha sido crucial, ya que le ha permitido obtener la versión más actualizada y segura del software [4].

Figura 1.
Descarga del archivo ISO



Fuente: Autoría Propia

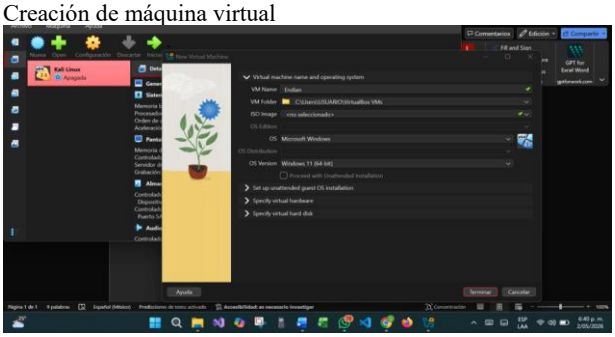
En esta figura se puede observar la página de descarga de Endian Firewall. Esta es herramienta de seguridad de red que permite proteger infraestructuras informáticas mediante firewall, segmentación de zonas, VPN, filtrado web y monitoreo del tráfico. Su implementación mejora la seguridad, el control y la administración de redes empresariales y académicas [4].

Figura 2.
Creación de máquina virtual

Fuente: Autoría Propia

El usuario ha procedido a configurar la máquina virtual de Endian, de acuerdo con los requerimientos necesarios para la actividad. Este paso ha sido fundamental para asegurar que la instalación cumpla con las especificaciones técnicas requeridas y funcione de manera óptima en el entorno de red establecido.

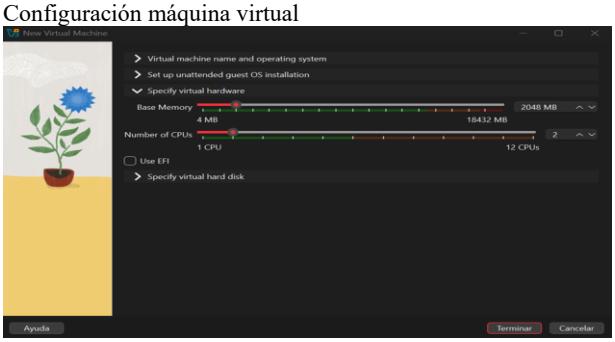
Figura 3.
Creación de máquina virtual



Fuente: Autoría Propia

Una vez que el usuario ha creado la máquina virtual, ha configurado los adaptadores de red conforme a las siguientes zonas: Zona verde para la red interna (LAN), Zona roja para el acceso a internet (WAN) y Zona naranja para los servidores (DMZ).

Figura 4.
Configuración máquina virtual



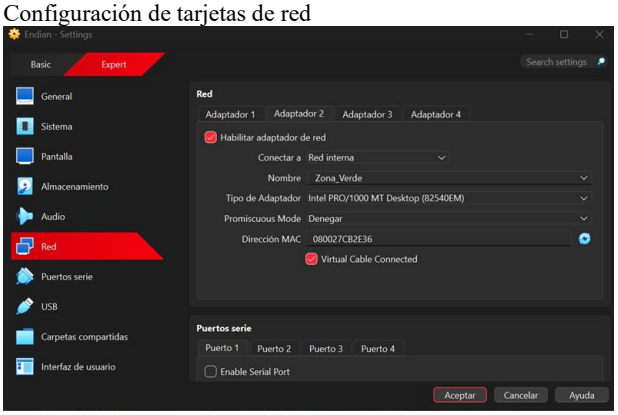
Fuente: Autoría Propia

El usuario procede con la instalación de Endian en la máquina virtual. Este paso es crucial para completar la configuración del sistema de gestión de hosting, asegurando que todos los componentes necesarios estén correctamente instalados y listos para su uso en el entorno de red.

2.2 CONFIGURACIÓN DE LA ZONA VERDE DE ACUERDO CON LO SOLICITADO.

En este procedimiento se configuran las tarjetas de red en VirtualBox para asignar las diferentes zonas y establecer las conexiones de red para que Endian controle el tráfico.

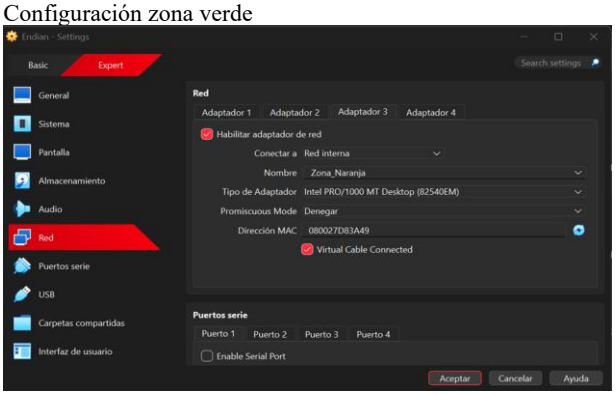
Figura 5.
Configuración de tarjetas de red



Fuente: Autoría Propia

Configuración de la zona Naranja de acuerdo con lo solicitado, se activa un adaptador de red en modo NAT.

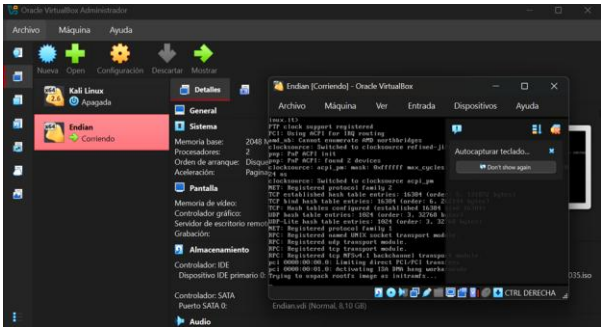
Figura 6.
Configuración zona verde



Fuente: Autoría Propia

Continuamos con la instalación de Endian, El usuario sigue las instrucciones y asigna la dirección IP junto con la máscara de red, completando así la instalación de Endian. Este paso finaliza el proceso de configuración, permitiendo que el sistema esté listo para su funcionamiento en el entorno de red.

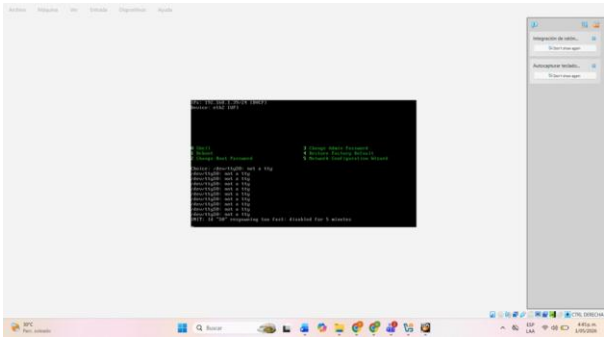
Figura 7.
Instalación Endian



Fuente: Autoría Propia

Ahora el usuario verifica la configuración de la máquina cliente, en este caso, la máquina Desktop, de manera específica el adaptador de red que corresponda a Red Interna (LAN, VERDE). Este paso es esencial para asegurar que la conexión y las configuraciones de red sean correctas, para el funcionamiento adecuado dentro del entorno establecido.

Figura 8.
Verificación zona verde



Fuente: Autoría Propia

El usuario inicia la máquina y procede a abrir un explorador web, digitando la dirección asignada para Endian, en este caso, 192.168.0.15:10443. Esto presenta el mensaje de bienvenida a Endian, indicando que el acceso a la interfaz de gestión ha sido exitoso**.**

Figura 9.
Confirmación de máquinas virtuales.

Fuente: Autoría Propia

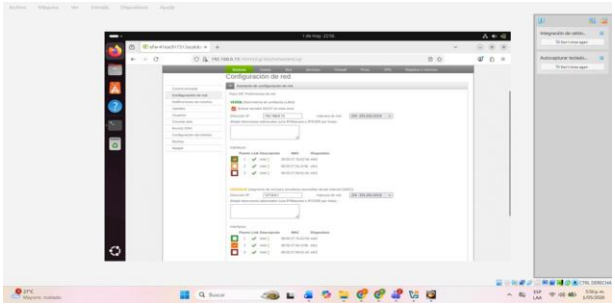
El usuario sigue las indicaciones para la aceptación de la licencia. Este paso es fundamental para continuar con el proceso de configuración y garantizar que se cumplen los términos y condiciones establecidos por Endian.

Figura 10.
Ingresó a la interfaz de Edian.

Fuente: Autoría Propia

Se observa que se identifican los tres adaptadores de red. Ahora, en la configuración WAN, se pueden ver las tres zonas activas. Esto indica que la red está correctamente configurada y operativa.

Figura 11.
Validación de zonas Activas



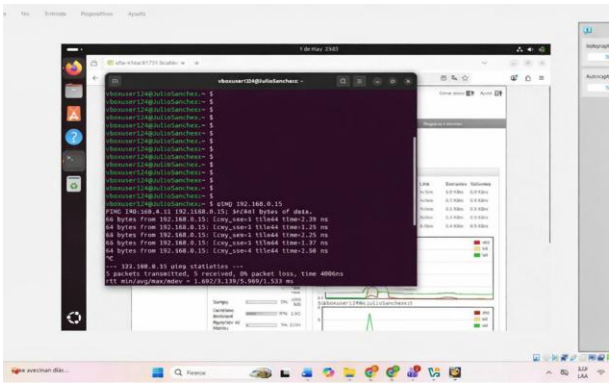
Fuente: Autoría Propia

En la interfaz de administración de Endian Firewall se observa la validación de las zonas de red activas. En este caso, el sistema reconoce correctamente los tres adaptadores de red configurados, correspondientes a las diferentes interfaces de comunicación de la infraestructura.

Dentro de la configuración WAN se evidencian las tres zonas activas y habilitadas, lo que confirma que las interfaces fueron configuradas correctamente y que la segmentación de red se encuentra operativa. Esta validación es importante para garantizar el adecuado funcionamiento de la comunicación entre la red interna, la DMZ y la conexión a Internet.

Posteriormente, desde la terminal del sistema se realiza una prueba de conectividad mediante el comando ping 8.8.8.8, dirigido al servidor DNS público de Google. Esta prueba permite verificar que el firewall tiene acceso a Internet y que las rutas de comunicación se encuentran funcionando correctamente. Además, confirma que la configuración de red, gateway y reglas de salida están correctamente establecidas en el entorno Endian.

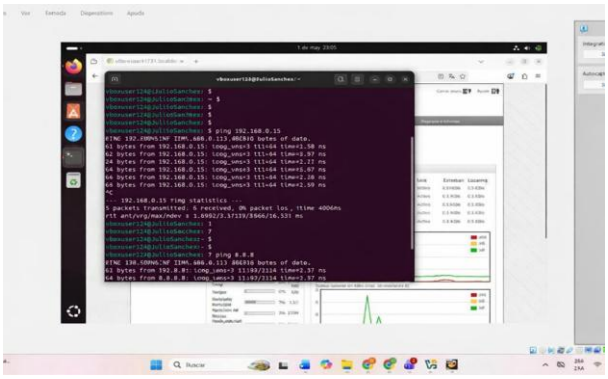
Figura 12.
Validación de conectividad.



Fuente: Autoría Propia

Seguido se realiza una prueba de internet. Este paso es fundamental para comprobar que la conexión a la red externa está funcionando correctamente y que se puede acceder a recursos en línea.

Figura 13.
Validación de conectividad a internet.



Fuente: Autoría Propia

Se busca IPv4 y se evidencia el acceso a través de DHCP. Esto confirma que la configuración de la dirección IP se realiza de manera automática mediante el protocolo DHCP.

Figura 14.
Configuración de Direccionamiento IP.

Fuente: Autoría Propia

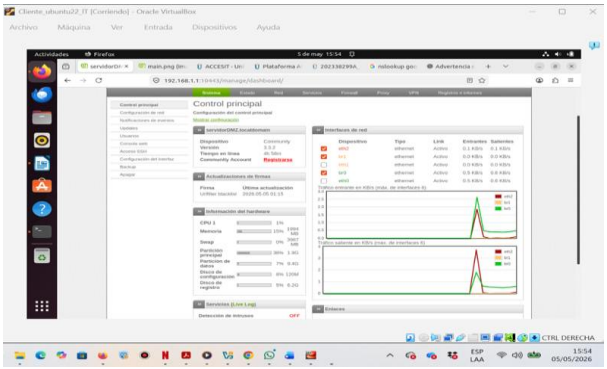
3 TEMÁTICA 2: CONFIGURACIÓN NAT

En esta práctica se utilizó Endian Firewall para implementar reglas NAT y Port Forwarding, estas traducen las direcciones IP privadas (no enrutables en Internet) de las zonas LAN y DMZ a la dirección IP pública de la interfaz WAN de Endian, permitiendo que múltiples dispositivos internos compartan una sola IP pública [5].

3.1 INSTALACIÓN Y VALIDACIÓN DE ENDIAN FIREWALL

En la Figura 14 se observa el correcto funcionamiento del firewall luego de su instalación. El sistema se encuentra operativo y listo para administrar el tráfico de red

Figura 15.
Funcionamiento correcto de Endian Firewall



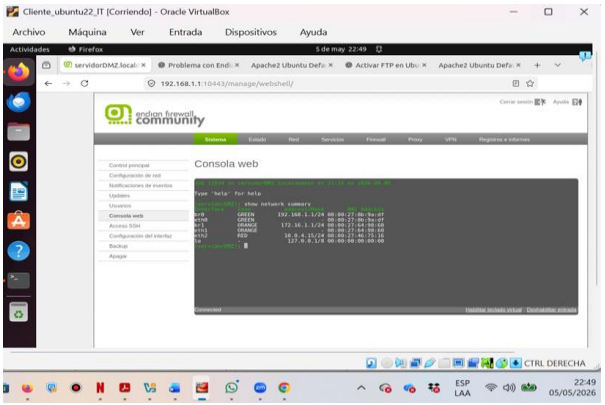
Fuente: Autoría Propia

3.2 VALIDACIÓN DE INTERFACES

En esta etapa se muestran las interfaces activas configuradas en el firewall:

- GREEN: Red LAN interna.
- ORANGE: Zona DMZ.
- RED: Conexión WAN/Internet.

Figura 16.
Interfaces activas del firewall.



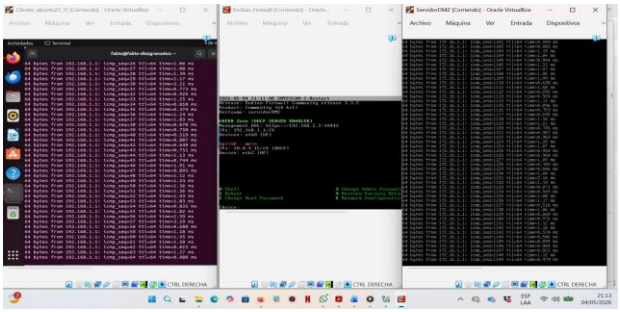
Fuente: Autoría Propia

3.3 VALIDACIÓN DE CONECTIVIDAD

A Continuación, se realizaron pruebas de conexión entre las interfaces orange y green por medio del comando ping con sus respectivas puertas de enlace de edian. La verde a su ip la ip 192.168.1.1 desde el cliente y la naranja a su ip 192.16.1.1, también podemos realizar pruebas de conectividad entre zona para más adelante realizar las configuraciones correspondientes al laboratorio.

En la Figura se muestra la conectividad entre las interfaces mediante pruebas de puerta de enlace utilizando comandos de red.

Figura 17.
Validación de conectividad entre interfaces.



Fuente: Autoría Propia

3.4 CONFIGURACIÓN NAT PARA LA RED LAN (GREEN → WAN)

La traducción de direcciones de red (NAT) permite que múltiples dispositivos de una red privada accedan a Internet utilizando una única dirección IP pública.

3.5 CONFIGURACIÓN DE REGLAS NAT

En este procedimiento se configuraron reglas NAT en Endian Community para habilitar el acceso a Internet desde las redes GREEN y ORANGE mediante SNAT/MASQUERADE, así como reglas DNAT o Port Forwarding para publicar servicios HTTP y FTP alojados en un servidor de la DMZ [6].

En la Figura 18 se muestra la configuración inicial de NAT para las redes GREEN y ORANGE.

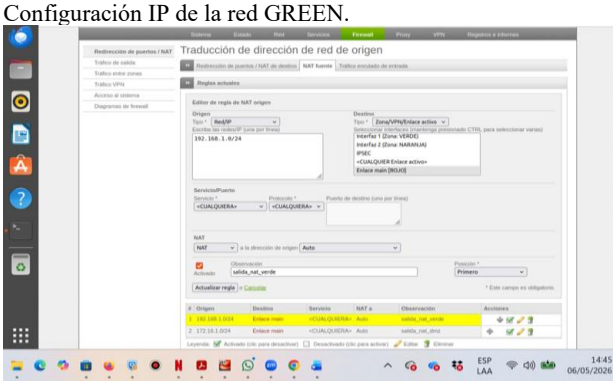
Figura 18.
Configuración NAT para GREEN y ORANGE

Fuente: Autoría Propia

3.6 ASIGNACIÓN DE DIRECCIONES IP

En la Figura se observa la configuración específica de la red GREEN junto con las direcciones IP correspondientes.

Figura 19.
Configuración IP de la red GREEN.



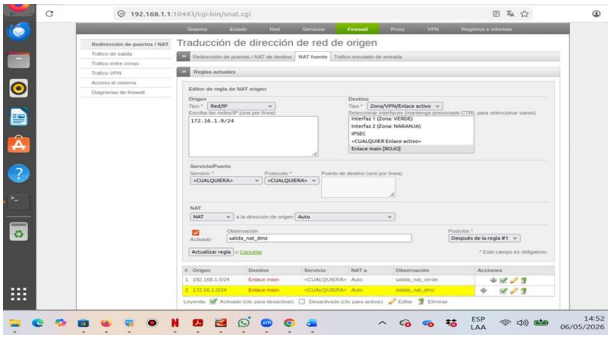
Fuente: Autoría Propia

3.7 CONFIGURACIÓN NAT PARA LA DMZ (ORANGE → WAN)

La zona ORANGE fue configurada como DMZ para alojar servicios accesibles desde el exterior manteniendo aislamiento respecto de la red interna [6].

En la Figura se muestra la configuración NAT aplicada a la red ORANGE.

Figura 20.
Configuración NAT para la DMZ



Fuente: Autoría Propia

3.8 CONFIGURACIÓN DE PORT FORWARDING / DNAT

El Port Forwarding permite redirigir tráfico externo hacia servicios específicos alojados en la DMZ.

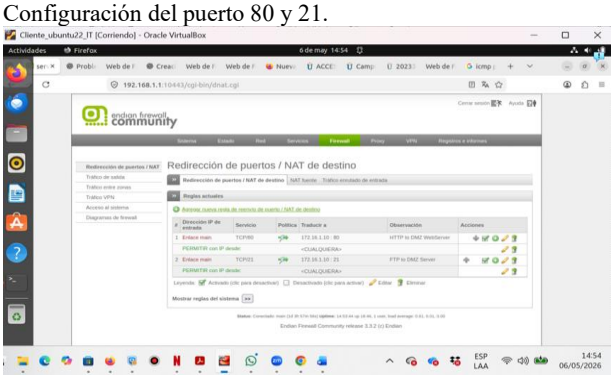
En las Figuras 21 y 22 se configuró la redirección de los puertos:

- Puerto 80 (HTTP)
- Puerto 21 (FTP)

Estas reglas permiten el acceso externo a los servicios web y FTP del servidor DMZ.

En la Figuras se muestra la salida de los puertos en el servidor DMZ puerto HTTP y FTP para acceder a estos servicios desde la zona naranja.

Figura 21.
Configuración del puerto 80 y 21.

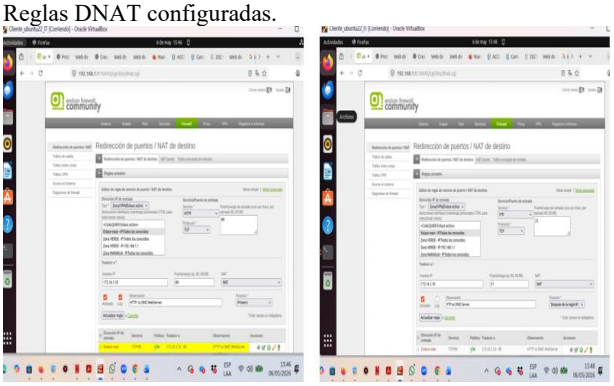


Fuente: Autoría Propia

En la Figura se observa la configuración para la salida de los puertos puerto 80 HTTP y 21 FTP en el servidor DMZ, para acceder a estos servicios desde la zona naranja ingresando por la zona roja que es internet y redirigiendo a la ip de la zona naranja que es 172.16.1.10.

En la siguiente figura también se observa las reglas en las zonas que corresponden para la navegación de internet y el servicio a asignado.

Figura 22.
Reglas DNAT configuradas.



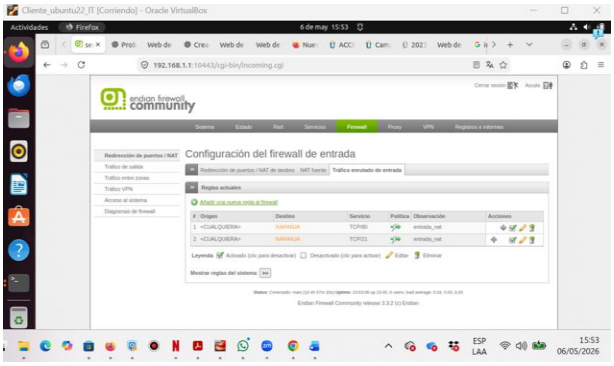
Fuente: Autoría propia.

3.9 VALIDACIÓN DE TRÁFICO DE ENTRADA

En algunas configuraciones no es necesario debido a que se encuentra por default o no es necesario tener acceso al servidor DMZ a través de una red externa. Es de vital importancia aplicar este cambio cuando tenemos servidores que alojan páginas web o ingresos controlados de monitoreo, dependiendo del caso muchas veces se implementa.

La Figura muestra las reglas NAT aplicadas al tráfico entrante.

Figura 23.
Validación del tráfico de entrada NAT.

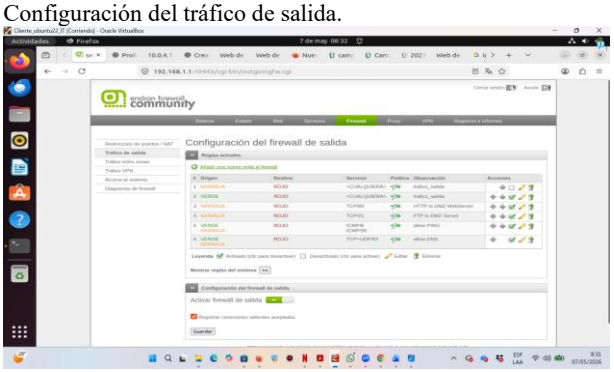


Fuente: Autoría Propia

3.10 VALIDACIÓN DE TRÁFICO DE SALIDA

En esta zona de configuración se administró la salida de los puertos habilitados en la configuración Nat de la zona naranja para darle salida, como lo requería el laboratorio, como es una la zona del servidor DMZ es necesario tener más restricción para brindar una buena seguridad.

Figura 24.
Configuración del tráfico de salida.



Fuente: Autoría Propia

En la Figura se evidencia la configuración del tráfico de salida. Las reglas predeterminadas fueron modificadas permitiendo la salida general de la zona verde y algunas necesarias para la zona naranja, aunque estas se pueden ajustar según las necesidades del usuario

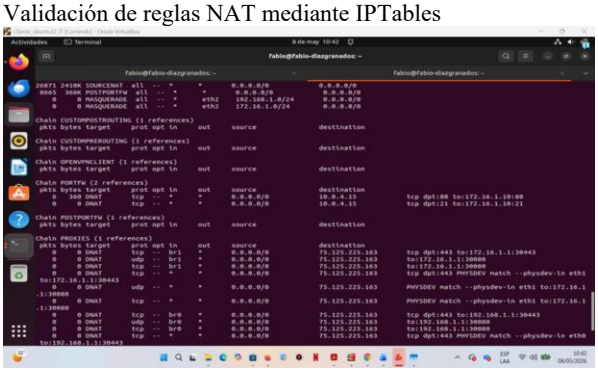
3.11 VALIDACIÓN DE REGLAS NAT

Para verificar las reglas configuradas se utilizó el comando: iptables -t nat -L -n -v en el endian.

La salida permitió visualizar las reglas MASQUERADE y DNAT configuradas en el sistema.

En particular, las reglas MASQUERADE permiten que las redes privadas salgan hacia Internet mediante traducción de direcciones.

Figura 25.
Validación de reglas NAT mediante IPTables

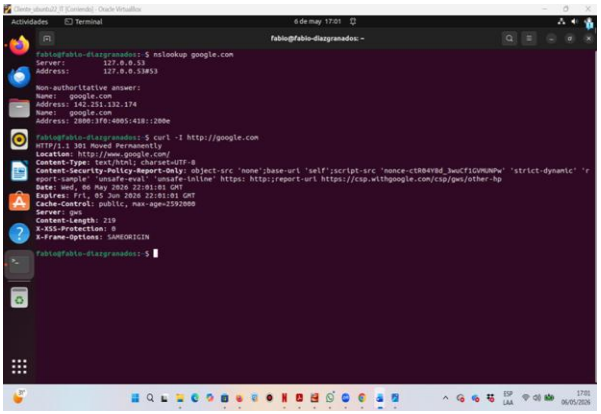


Fuente: Autoría Propia

3.12 PRUEBAS DE CONECTIVIDAD

Por medio de la consola del cliente en este caso ubuntu 22 realizamos pruebas de conectividad a través de comandos esto con el fin de evaluar el servicio HTTP.

Figura 26.
Validación de acceso HTTP desde LAN.



Fuente: Autoría Propia

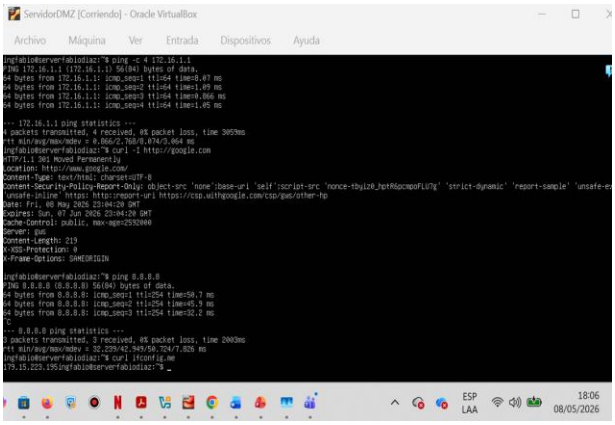
En la Figura se observa el acceso desde la red LAN hacia Internet mediante tráfico HTTP.

3.13 VERIFICACION DMZ – INTERNET

La verificación DMZ – Internet permite comprobar que la arquitectura de seguridad si funciona correctamente, garantizando acceso controlado a los servicios públicos mientras se protege la red interna frente a amenazas externas

En la Figura se muestra cómo se comprueba la salida hacia Internet NAT por el puerto HTTP desde el servidor ubicado en la DMZ utilizado un comando para validar la conectividad mediante acceso a Google.

Figura 27.
Validación de acceso desde DMZ hacia Internet



Fuente: Autoría Propia

Como se puede observar en la figura las pruebas realizadas con comandos para validar si hay navegación en el servidor DMZ.

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

La arquitectura de seguridad de endian permite la gestión de servicios dentro de la Zona Desmilitarizada (DMZ) mediante la apertura selectiva de puertos. A continuación, se describe la habilitación de los protocolos HTTP y FTP a través de los puertos 80 y 21, respectivamente. Asimismo, se incluye un escenario de restricción de tráfico orientado a la denegación del protocolo ICMP (tipos 8 y 30), con el fin de validar la eficacia de las políticas de filtrado en la protección de activos críticos.

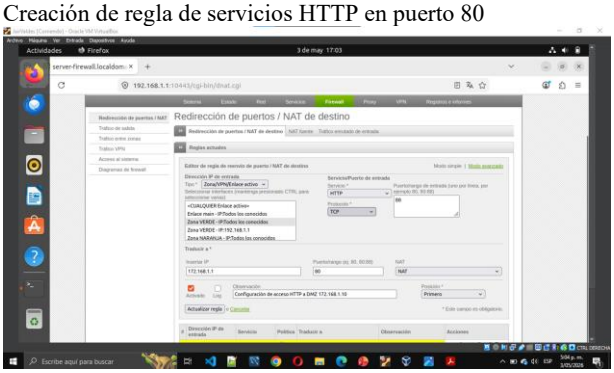
4.1 IMPLEMENTACIÓN SERVICIOS HTTP (PUERTO 80)

El puerto 80 es el puerto estándar utilizado para la comunicación web sin cifrado y permite que los navegadores establezcan conexión con servidores web para solicitar y visualizar contenido como páginas HTML, imágenes y aplicaciones web.

Para habilitar el tráfico HTTP a través del puerto 80, se accede a la interfaz de gestión de Endian mediante la dirección IP configurada (https://192.168.1.1:10443). Tras la autenticación, se debe navegar hacia el módulo de 'Firewall' y seleccionar la sección de 'Redirección de puertos / NAT'.

La creación de la nueva regla implica definir la Zona Naranja como origen y la interfaz Roja como destino. Se especifica el protocolo TCP con el puerto 80, estableciendo la acción en 'Permitir' y asegurando que la casilla 'Activado' esté marcada, manteniendo el resto de los parámetros según los valores predeterminados (Figura 28).

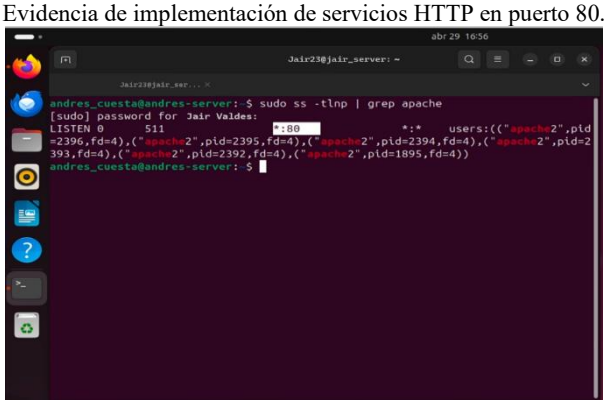
Figura 28.
Creación de regla de servicios HTTP en puerto 80



Fuente: Autoría Propia

Se realizaron pruebas de conectividad orientadas al puerto 80 (HTTP) desde los equipos cliente. Los resultados obtenidos confirman que la regla de 'Tráfico de salida' en Endian opera de manera óptima, permitiendo la resolución y despliegue de las peticiones HTTP provenientes de la zona desmilitarizada (Zona Naranja). La navegación se ejecuta sin interrupciones a través del protocolo TCP, lo que evidencia que la política de permisión cumple con el objetivo de exponer de forma segura y controlada los servicios web de la infraestructura hacia la red externa.

Figura 29.
Evidencia de implementación de servicios HTTP en puerto 80.



Fuente: Autoría Propia

4.2 IMPLEMENTACIÓN SERVICIOS FTP (PUERTO 21)

Continuando en el módulo de 'Firewall' dentro de la interfaz de Endian, se procede a la apertura del servicio FTP. En la sección de 'Redirección de puertos / NAT', se genera una nueva regla de acceso parametrizada de la siguiente manera: se establece la Zona Naranja como origen y la Roja como destino. Se define el protocolo TCP asociado al puerto 21, asignando la acción de 'Permitir' y validando su ejecución mediante la opción 'Activado'. Como se detalla en la Figura correspondiente, los parámetros adicionales se conservan en sus valores predefinidos para asegurar la compatibilidad del protocolo.

Figura 30.
Regla para implementación de servicios FTP en puerto 21

Fuente: Autoría Propia

Una vez integrada la regla de acceso para el protocolo FTP, se realizaron las pruebas operacionales para validar la comunicación en la red. La evidencia demuestra que las peticiones orientadas al puerto 21 son admitidas por la interfaz de Endian, logrando una conexión exitosa entre los segmentos correspondientes.

Figura 31.
Evidencia de implementación de servicios FTP en puerto 21.

Fuente: Autoría Propia

4.3 DENEGAR ICMP PUERTOS 8 Y 30, INHABILITANDO EL PING EN RED

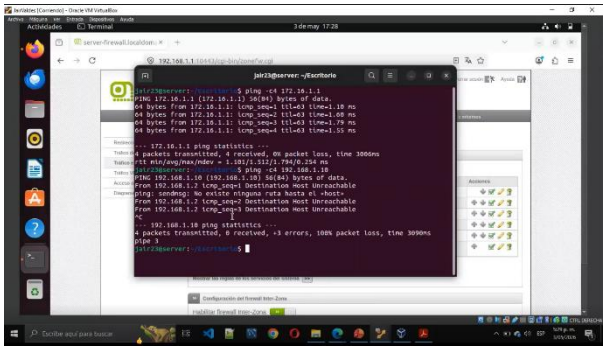
Para restringir las respuestas de diagnóstico de red y evitar la ejecución de comandos 'ping', se debe configurar la denegación del protocolo ICMP. Para ello, dentro del menú de 'Firewall' de Endian, se accede a la sección 'Tráfico entre zonas' para generar una regla restrictiva. Definiendo un servicio personalizado ICMP. Al especificar los identificadores 8 y 30, y seleccionar la acción de 'Denegar', se inhabilita este tráfico, manteniendo el resto de los parámetros de la regla en sus valores predeterminados.

Figura 32
Regla para implementación de servicios HTTP en puerto 80

Fuente: Autoría Propia

Posterior a la configuración de la regla de denegación ICMP (tipos 8 y 30), se realizaron las pruebas de conectividad ejecutando comandos ping entre los segmentos de red. Los resultados confirmaron el bloqueo absoluto del tráfico de diagnóstico; el firewall rechazó cada solicitud de manera inmediata, impidiendo la visibilidad mutua entre las zonas especificadas. Las zonas configuradas quedaron incomunicadas bajo este protocolo específico, lo cual valida la efectividad de las reglas de 'Tráfico entre zonas' en Endian.

Figura 33.
Evidencia de conectividad fallida (ping) tras la política restrictiva ICMP.



Fuente: Autoría Propia

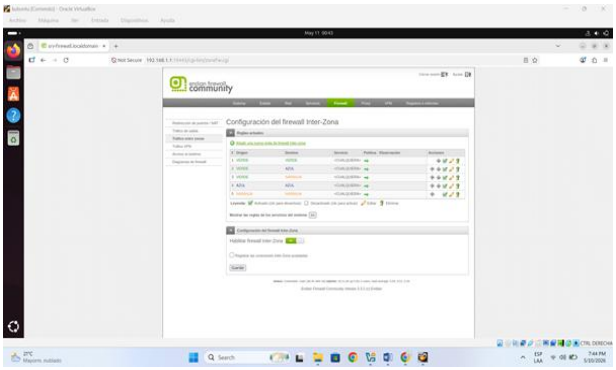
5 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La administración del tráfico inter-zona constituye el núcleo operativo de la seguridad en Endian Firewall, permitiendo la transición de una política de denegación implícita a un esquema de comunicación controlada basado en el principio de mínimo privilegio. En esta fase, se procedió a la creación y validación de directivas específicas de filtrado para gestionar el flujo de datos entre las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). El enfoque técnico se centró en la implementación de reglas de acceso para los protocolos HTTP y FTP, garantizando no solo la visibilidad de los servicios alojados en la DMZ desde el exterior mediante técnicas de DNAT, sino también la capacidad de navegación segura de los clientes internos hacia la red pública.

5.1 CONFIGURACIÓN DE POLÍTICAS INTER-ZONA

Para el despliegue de las reglas, se accedió a la interfaz de gestión mediante la dirección 192.168.1.1:10443. Dentro del módulo Firewall > Tráfico entre zonas, se definieron las siguientes directivas:

Figura 34.
Módulo Firewall > Tráfico entre zonas



Fuente: Autoría Propia

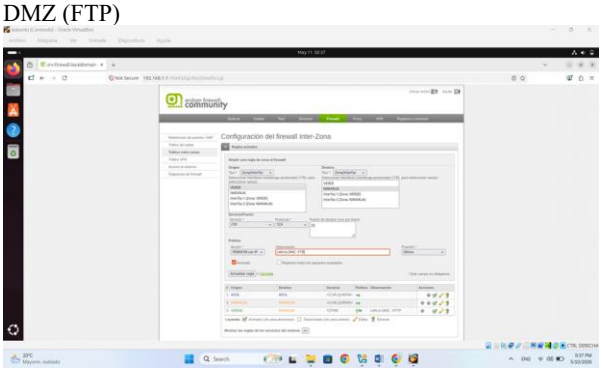
Comunicación LAN a DMZ (HTTP/FTP): Se habilitaron reglas para permitir el acceso desde la red interna hacia el servidor en la zona naranja (172.16.1.10) mediante los protocolos HTTP y FTP, garantizando la administración de servicios.

Figura 35.
Regla para permitir el acceso a la red LAN a DMZ (HTTP)

Fuente: Autoría Propia

En la figura se evidencia el proceso de configuración y validación de las interfaces de red dentro del firewall,en este caso dándole tráfico al servicio HTTP por el puerto 80, garantizando la correcta segmentación de la red y el control seguro del tráfico entre las distintas zonas. Esta configuración es fundamental para asegurar conectividad, administración centralizada y protección de la infraestructura de red frente a accesos no autorizados.

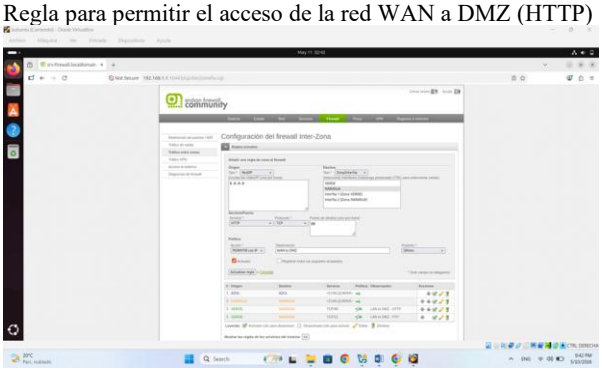
Figura 36.
Creación de regla para permitir el acceso de la red LAN a DMZ (FTP)



Fuente: Autoría Propia

Acceso WAN - DMZ: Se implementaron políticas de entrada y redirección para permitir que el tráfico externo alcance los servicios web y de transferencia de archivos en la zona desmilitarizada.

Figura 37.
Regla para permitir el acceso de la red WAN a DMZ (HTTP)



Fuente: Autoría Propia

Figura 38.
Regla para permitir el acceso de la red WAN a DMZ (FTP)

Fuente: Autoría Propia

Salida a Internet (LAN → WAN y DMZ → WAN): Se establecieron reglas de salida para permitir que tanto los clientes de la red verde como el servidor de la zona naranja realicen consultas externas hacia la zona roja.

Figura 39.
Regla para permitir la salida de la red LAN a WAN (HTTP)

Fuente: Autoría Propia

Figura 40.
Regla para permitir la salida de la red LAN a WAN (FTP)

Fuente: Autoría Propia

En esta figura se puede observar como se habilita el servicio FTP que es un protocolo de red utilizado para la transferencia de archivos entre computadores a través de una red TCP/IP, como Internet o una red local.

Figura 41.
Regla para permitir la salida de la red DMZ a WAN (HTTP)

Fuente: Autoría Propia

La figura muestra la interfaz de administración web de Endian Firewall durante el proceso de configuración de una zona de red habilitando el puerto 80 para la navegación. En la parte superior se observa el menú de configuración de red, mientras que en el panel central aparece el formulario

denominado “Configuración de interfaz Zona”, donde se establecen los parámetros de una de las interfaces del firewall.

Figura 42.
Regla para permitir la salida de la red DMZ a WAN (FTP)

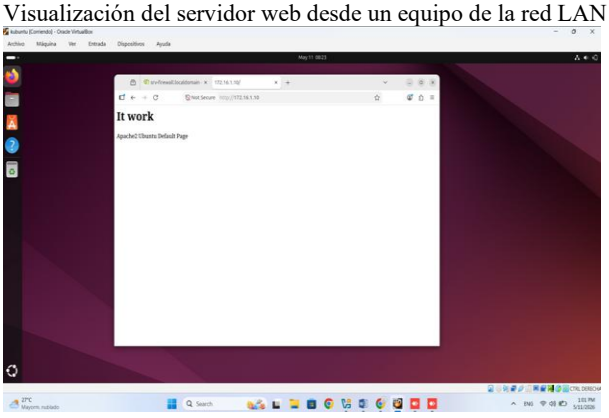
Fuente: Autoría Propia

5.2 VERIFICACIÓN Y PRUEBAS DE CONECTIVIDAD

La validación de las reglas se realizó mediante un proceso de pruebas cruzadas para asegurar el cumplimiento de las políticas de acceso:

Prueba LAN → DMZ (HTTP): Desde el cliente Ubuntu-LAN, se verificó el acceso mediante navegador a la URL http://172.16.1.10, confirmando la visibilidad del servidor web interno.

Figura 43.
Visualización del servidor web desde un equipo de la red LAN



Fuente: Autoría Propia

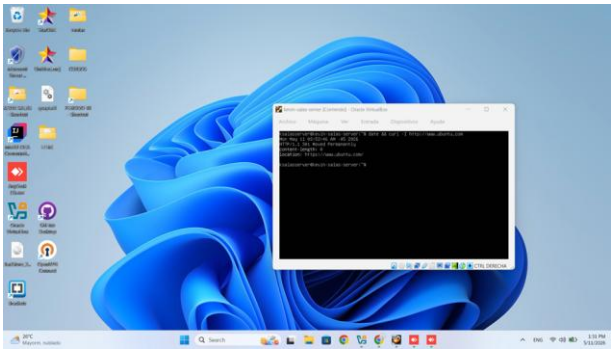
Prueba LAN → WAN (HTTP): Se validó la navegación a Internet y la resolución de nombres mediante el comando curl -I http://www.google.com, obteniendo una respuesta satisfactoria del servidor remoto.

Figura 44.
Validación de conectividad y resolución de nombres mediante protocolo HTTP (LAN a WAN)

Fuente: Autoría Propia

Prueba DMZ → WAN (HTTP): Se comprobó la capacidad del servidor alojado en la DMZ para establecer conexiones externas mediante el comando date && curl -I http://www.ubuntu.com, garantizando el acceso a repositorios y servicios externos.

Figura 45.
Verificación de acceso a repositorios externos y resolución de nombres desde el servidor en DMZ



Fuente: Autoría Propia

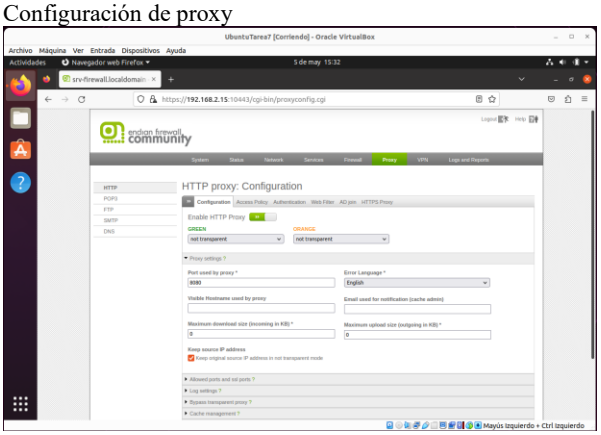
Prueba WAN → DMZ (Acceso Externo): Se simuló el acceso desde la red externa utilizando la IP de la interfaz Roja del Endian (10.0.4.15). La validación mediante curl -I confirmó que el tráfico es correctamente procesado por las reglas de acceso y redirigido al servidor final en la DMZ.

6 TEMÁTICA 5: PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN.

6.1 HABILITAR SERVICIO PROXY EN ENDIAN

Se habilitó el servicio Proxy HTTP en Endian Firewall mediante la interfaz web de administración, utilizando el navegador Mozilla Firefox desde el equipo cliente.

Figura 46.
Configuración de proxy

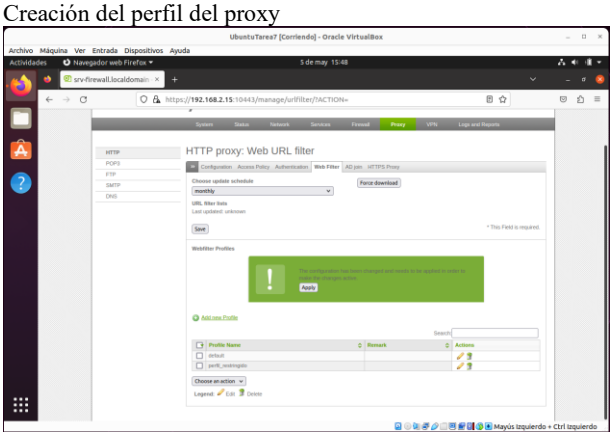


Fuente: Autoría Propia

6.2 CREACIÓN DE LISTA NEGRA CON LOS SITIOS BLOQUEADOS

En la configuración de proxy buscaremos la sección de contenido filtrado o lista negra de URL's donde crearemos un perfil nuevo llamado "perfil restringido". este perfil tendrá sitios bloqueados para los usuarios de la LAN.

Figura 47.
Creación del perfil del proxy



Fuente: Autoría Propia

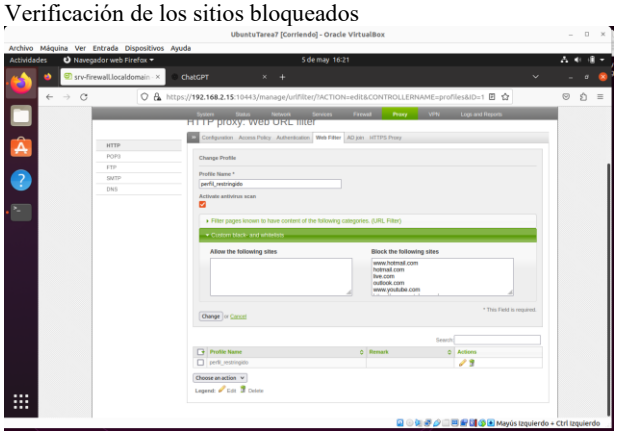
6.3 AGREGAR SITIOS A LA LISTA NEGRA.

Agregar sitios a la lista negra consiste en configurar el firewall o sistema de filtrado web para bloquear el acceso a determinadas páginas o dominios de Internet considerados no permitidos dentro de la red.

Una lista negra (Blacklist) es un conjunto de direcciones web, dominios o sitios específicos que el administrador de red restringe para impedir que los usuarios puedan acceder a ellos desde la red corporativa o institucional.

En la pestaña proxy vamos a web filter y editamos el perfil restringido y en blacklist agregamos los sitios web que estarán bloqueados por endian.

Figura 48.
Verificación de los sitios bloqueados

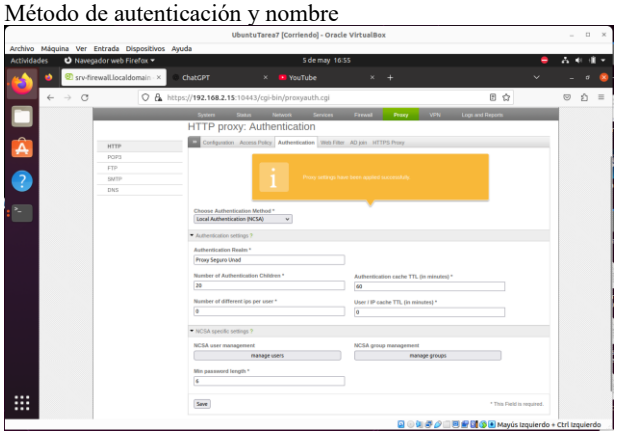


Fuente: Autoría Propia

6.4 CONFIGURACION AUTENTICACION DE USUARIO

Se selecciona el método de autenticación y se define el nombre real de la autenticación el cual llamaremos "proxy seguro unad".

Figura 49.
Método de autenticación y nombre

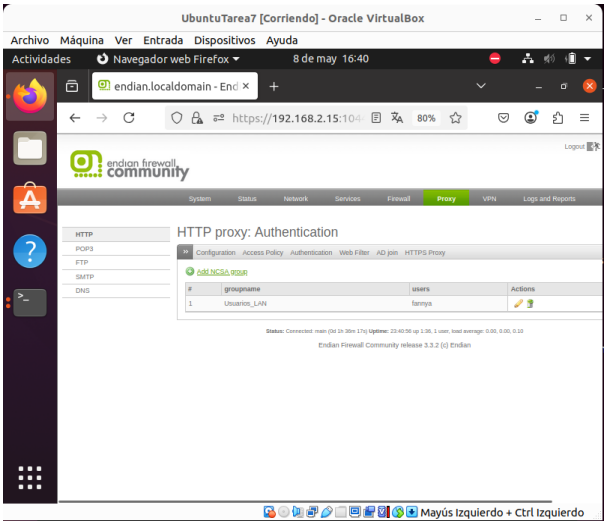


Fuente: Autoría Propia

La imagen muestra la interfaz web de configuración de Endian Firewall específicamente en el apartado de HTTP Proxy Authentication. En esta sección se administran las políticas de autenticación y control de acceso para la navegación web de los usuarios dentro de la red.

En la parte superior se observa un mensaje de advertencia del sistema indicando que el proxy requiere configuración adicional para funcionar correctamente. Debajo del aviso aparecen diferentes opciones relacionadas con la autenticación del proxy HTTP, permitiendo definir cómo los usuarios deberán identificarse para acceder a Internet.

Figura 50.
Creación de usuarios desde GUI

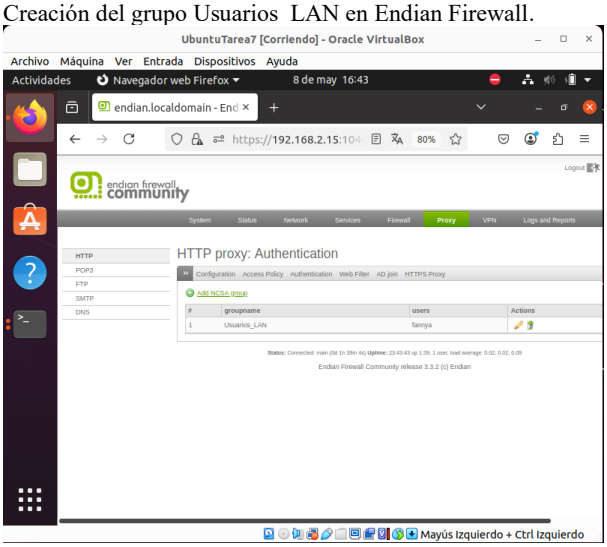


Fuente: Autoría propia

6.5 CREACIÓN DE GRUPO

Se crea el grupo desde el interfaz GUI en la pestaña de autenticación y manejo de grupos

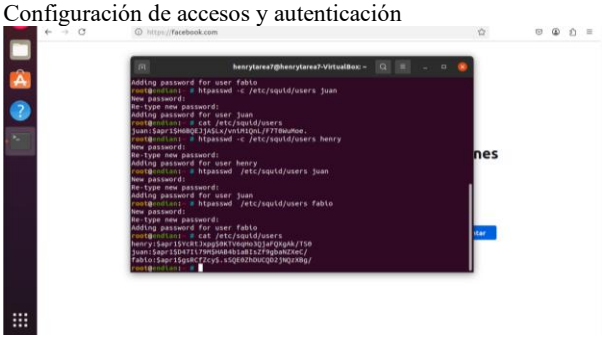
Figura 51.
Creación del grupo Usuarios LAN en Endian Firewall.



Fuente: Autoría propia

Se realiza la configuración en el archivo de configuración squid.conf donde se definen los parámetros de acceso, desde la consola se crearon los usuarios utilizando el comando htpasswd para pedir autenticación.

Figura 52.
Configuración de accesos y autenticación



Fuente: Autoría propia

Posteriormente, se configuró el archivo misquid.conf, agregando las líneas correspondientes a la autenticación de usuarios.

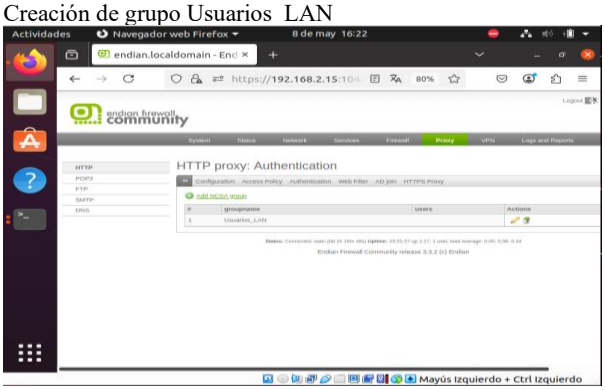
Figura 53.
Verificación de autenticación del proxy

Fuente: Autoría propia

6.6 CREACION DE USUARIOS

Se Realiza la creación del grupo desde la interfaz GUI para poder asociar los usuarios con los grupos.

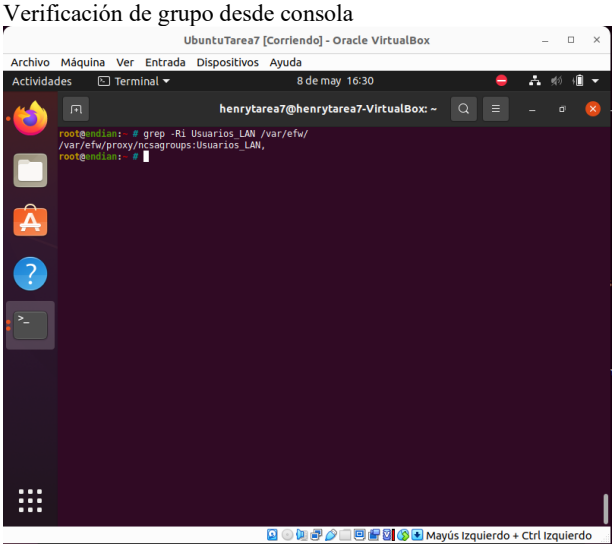
Figura 54.
Creación de grupo Usuarios LAN



Fuente: Autoría propia

Posteriormente se realiza la verificación del grupo desde la consola identificando que este creado correctamente.

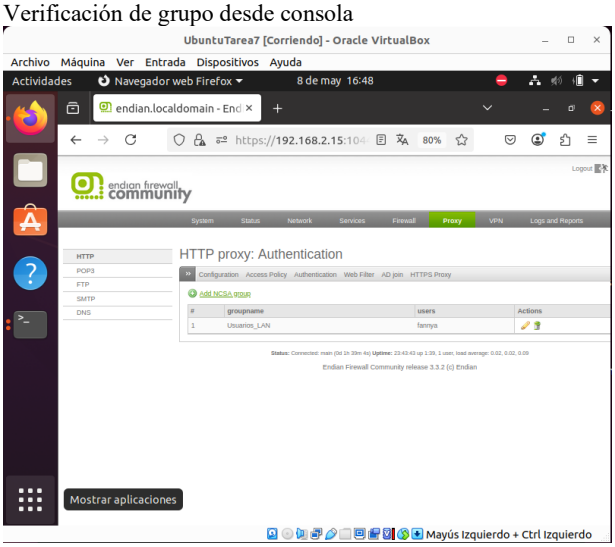
Figura 55.
Verificación de grupo desde consola



Fuente: Autoría propia

Asociamos al usuario al grupo creado llamado Usuarios_LAN.

Figura 56.
Verificación de grupo desde consola



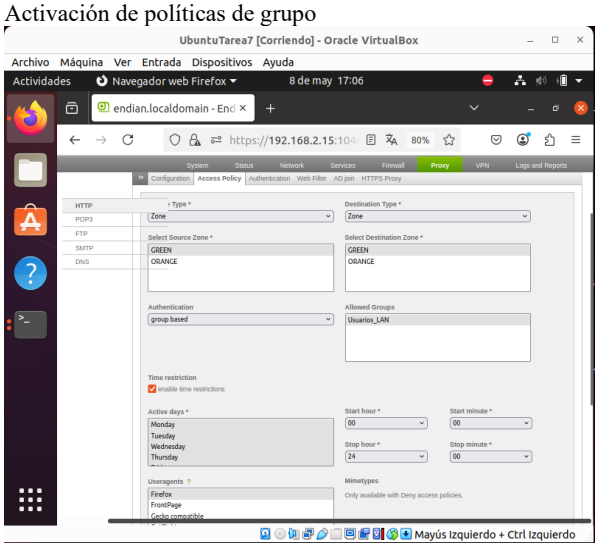
Fuente: Autoría propia

Se realiza la creación de los usuarios desde especificando el nombre del grupo y asociándolo con el usuario que para este caso utilice usuario1.

6.7 CREACIÓN POLÍTICA DE ACCESO

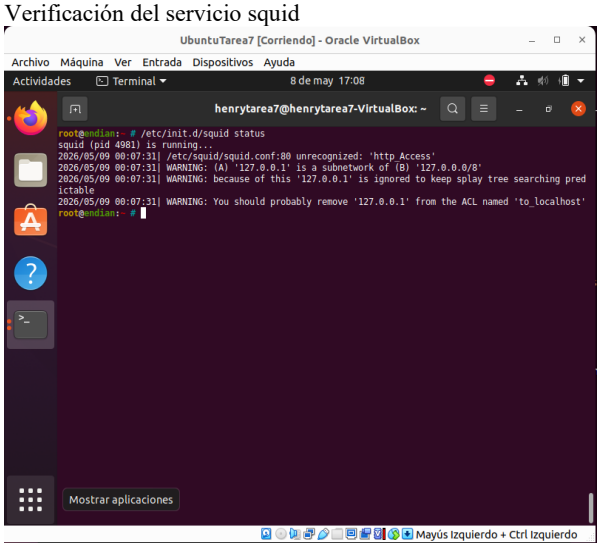
La creación de la política de accesos puede ser aplicadas tanto en grupos como los usuarios donde se definen los accesos, horarios entre otros.

Figura 57.
Activación de políticas de grupo



Fuente: Autoría propia

Figura 58.
Verificación del servicio squid

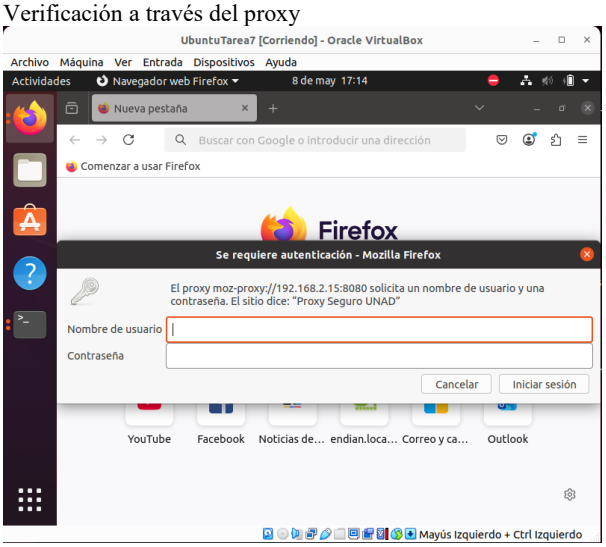


Fuente: Autoría propia

6.8 CONFIGURACION DEL CLIENTE

Para aplicar la configuración y trabajar a través del proxy debemos realizar la configuración en el navegador para este caso utilizaremos firefox donde iremos a ajustes -> configuracion de red -> configuración -> configuración manual del proxy -> proxy http colocamos la ip de la zona verde y el puerto 8080 y marcamos que utilice lo mismo para https [9].

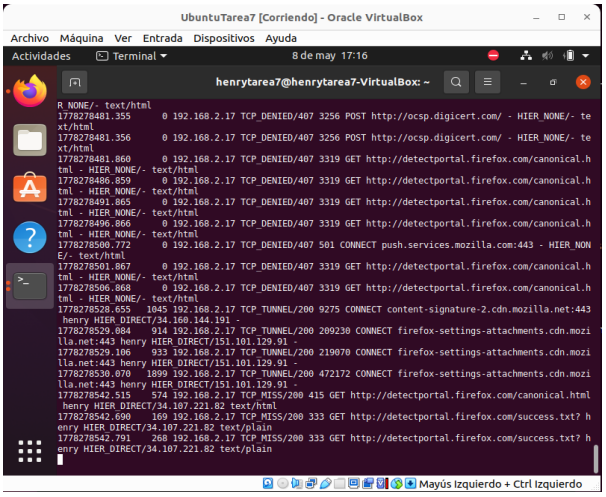
Figura 59.
Verificación a través del proxy



Fuente: Autoría propia

Se realiza la validación del tráfico por medio del proxy desde la consola por medio del comando de monitoreo tail -f /var/log/squid/access.log.

Figura 60.
Verificación de autenticación



Fuente: Autoría propia

6.9 VERIFICACIÓN DE LOS SITIOS BLOQUEADOS

La verificación de los sitios bloqueados consiste en comprobar que las reglas de filtrado web y las políticas de seguridad configuradas en el firewall estén funcionando correctamente. Este proceso permite validar que los dominios o páginas agregadas a la lista negra no puedan ser accedidos por los usuarios de la red [10].

Durante esta etapa, Se realiza la navegación en las páginas que se encuentran en la lista negra del proxy, las cuales no nos permitirán el acceso al momento de ingresa la dirección URL de los sitios bloqueados tales como son: googlevideo, youtube, live.com y Outlook.

Figura 61.
Bloqueo de página live.com

Fuente: Autoría propia.

Figura 62.
Bloqueo de página youtube.com

Fuente: Autoría propia

Figura 63.
Bloqueo de página live.com

Fuente: Autoría propia

Figura 64.
Bloqueo de página googlevideo.com

Fuente: Autoría propia

7 CONCLUSIONES

La Temática 1 permitió evidenciar el proceso completo de instalación y configuración de Endian Firewall en VirtualBox, garantizando la correcta asignación de las zonas de red (LAN, WAN y DMZ) y la validación de su operatividad. La descarga del ISO oficial aseguró el uso de una versión confiable, mientras que la creación de la máquina virtual y la configuración de los adaptadores de red establecieron la base para un entorno seguro. Las pruebas de conectividad, direccionamiento IP mediante DHCP y acceso al panel web confirmaron la funcionalidad del sistema, logrando un entorno virtualizado estable y preparado para la gestión segura de servicios [9].

La implementación de las reglas NAT y de redirección de puertos en Endian Community permitió comprender la manera en que un firewall administra y controla el tráfico entre diferentes zonas de red. A través de la configuración de las redes GREEN, ORANGE y RED, fue posible establecer acceso seguro a Internet y publicar servicios ubicados en la DMZ, garantizando una adecuada segmentación de la red. Además, las pruebas realizadas permitieron validar el correcto funcionamiento del firewall y de las reglas configuradas. Esta práctica fortaleció habilidades relacionadas con administración de redes, seguridad informática y uso de herramientas Linux para monitoreo y validación de servicios.

La implementación de una Zona Desmilitarizada (DMZ) mediante Endian Firewall demuestra ser una estrategia eficaz para el equilibrio entre la disponibilidad de servicios y la seguridad perimetral. Al permitir de forma controlada el tráfico en los puertos 80 y 21, y restringir protocolos de diagnóstico como ICMP, se logra reducir significativamente la superficie de ataque del sistema. Esta administración granular garantiza que los servicios esenciales permanezcan accesibles externamente, así mismo, establece una barrera robusta contra el reconocimiento de red no autorizada.

El desarrollo de la Temática 4 permitió implementar y validar de manera satisfactoria las reglas de acceso necesarias para controlar el tráfico entre las zonas LAN, DMZ y WAN mediante el uso de Endian Firewall Community. A través de la creación de políticas de tráfico inter-zona, fue posible permitir y restringir el acceso a servicios específicos como HTTP y FTP, garantizando una comunicación segura entre las diferentes redes del entorno virtualizado.

Asimismo, las pruebas realizadas desde clientes, servidores y la consola del firewall evidenciaron el correcto funcionamiento de las reglas configuradas, permitiendo validar la conectividad entre la red interna, la zona desmilitarizada y el acceso hacia Internet. La implementación de reglas WAN → DMZ demostró la importancia de la publicación controlada de servicios mediante mecanismos de seguridad perimetral, mientras que las políticas LAN → WAN y DMZ → WAN permitieron verificar el acceso seguro a recursos externos.

La implementación del Proxy HTTP no transparente con autenticación en Endian Firewall permitió fortalecer la seguridad y el control del acceso a Internet dentro de la red local. Mediante la configuración de políticas de filtrado, autenticación de usuarios, listas negras y grupos de acceso, fue posible supervisar y administrar el tráfico web de manera más segura y organizada. Asimismo, el uso de herramientas como Squid y archivos de configuración en GNU/Linux permitió comprender la importancia de los servicios proxy en la protección de redes y la administración de usuarios. Las pruebas realizadas demostraron el correcto funcionamiento del sistema, garantizando navegación controlada y mejorando la seguridad perimetral del entorno virtualizado [10].

8 REFERENCIAS

[1] LPI LPIC-1 Exam 101, “Tema 10: Comandos GNU y Unix,” 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/ [Accedido: 20-may-2026].
[2] Canonical, “Help Ubuntu,” Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/ [Accedido: 20-may-2026].
[3] Debian, “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 [Accedido: 20-may-2026].
[4] Oracle Corporation, “Manual de usuario VirtualBox,” VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/ [Accedido: 20-may-2026].
[5] Endian, “Endian UTM 3.2 Manual referencia,” Endian Documentation, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html [Accedido: 20-may-2026].
[6] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu *Server*. Birmingham, UK: Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952 [Accedido: 20-may-2026].
[7] Canonical Ltd., “Ubuntu Desktop Guide 20.04 LTS,” Ubuntu Documentation, 2023. [En línea]. Disponible en: https://help.ubuntu.com/ [Accedido: 12-may-2026].
[8] Debian Project, “Debian 12 Administrator’s Handbook,” Debian Documentation, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/ [Accedido: 12-may-2026].
[9] Oracle Corporation, “Oracle VM VirtualBox User Manual,” VirtualBox Documentation, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/ [Accedido: 12-may-2026].
[10] Endian, “Endian UTM 3.2 Reference Manual,” Endian Documentation, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html [Accedido: 12-may-2026].