Endian UTM como Plataforma de Defensa: Integración de NAT, Proxy y Control de Servicios en GNU/Linux

Jeiner Andrey Grijabala Delacruz
e-mail: jagrigalbad@unadvirtual.edu.co
Fabian Andres Lopez Martinez
e-mail: falopezmar@unadvirtual.edu.co
Paula Andrea Ortiz Mejia
e-mail: paortizme@unadvirtual.edu.co
Juan David Restrepo Marulanda
e-mail: jdrestrepoma@unadvirtual.edu.co
Joan Sebastian Trilleras Villada
e-mail: jstrillerasv@unadvirtual.edu.co

RESUMEN: *Este artículo presenta los resultados de la implementación de un sistema de seguridad perimetral en entornos GNU/Linux utilizando Endian UTM como plataforma de firewall. Se llevó a cabo la configuración de la arquitectura de red segmentada en zonas LAN, DMZ y WAN, integrando servicios esenciales como HTTP y FTP, así como reglas de traducción de direcciones (NAT) y control de tráfico Inter-Zona. Adicionalmente, se implementó un proxy HTTP con autenticación y filtrado de contenidos para reforzar las políticas de acceso. Los procedimientos documentados evidencian el fortalecimiento de la seguridad perimetral mediante la gestión eficaz del flujo de datos y la protección de los servicios expuestos en la DMZ, demostrando la capacidad de Endian UTM para aplicar controles consistentes y mejorar la postura de seguridad de la infraestructura.*

PALABRAS CLAVE: Endian UTM, GNU/Linux, Firewall, Seguridad Perimetral, Proxy HTTP.

INTRODUCCIÓN

La seguridad informática en entornos GNU/Linux requiere la implementación de controles que permitan segmentar redes, gestionar servicios y aplicar políticas de acceso. En este contexto, el proyecto busca fortalecer la infraestructura tecnológica mediante la instalación y configuración del firewall Endian UTM y la integración de servicios en zonas LAN, DMZ y WAN.

El desarrollo de la actividad aborda de manera práctica la configuración de un entorno perimetral basado en la arquitectura de seguridad por zonas, incorporando tecnologías como NAT, reenvío de puertos, control de tráfico Inter-Zona y filtrado de servicios. Cada temática profundiza en componentes esenciales para garantizar la integridad, disponibilidad y confiabilidad del sistema: desde la implementación inicial de Endian y la asignación de roles a las interfaces de red, hasta la habilitación selectiva de servicios web y FTP en la DMZ, la creación de reglas de acceso entre las diferentes zonas, y la aplicación de políticas avanzadas mediante un proxy HTTP con autenticación.

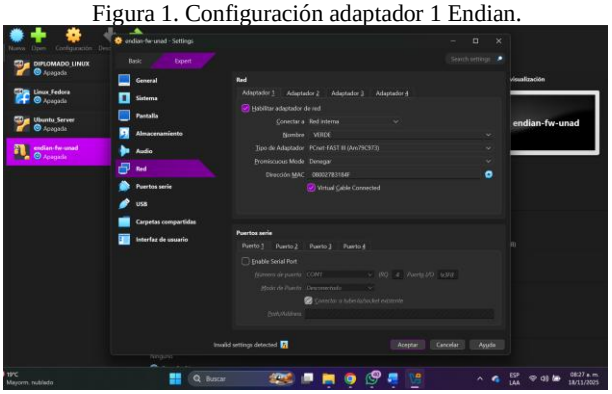
Este conjunto de prácticas permite analizar el funcionamiento real de un firewall UTM en un entorno de laboratorio, evidenciando cómo la segmentación y el control fino del tráfico contribuyen a la reducción de riesgos y al fortalecimiento de la seguridad perimetral en infraestructuras GNU/Linux.

TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

Endian Firewall es una distribución de GNU/Linux orientada a la seguridad perimetral, diseñada para funcionar como un firewall unificado y una plataforma de gestión de redes. Surgió en 2003 como un proyecto de código abierto basado inicialmente en IPCop, con el propósito de ofrecer una solución más robusta y simplificada para la protección de redes empresariales. Con el tiempo, Endian integró funciones avanzadas como filtrado de contenido, prevención de intrusiones, VPN, gestión de zonas segmentadas (Green, Orange, Red) y monitoreo centralizado. Gracias a su filosofía "UTM" (Unified Threat Management), Endian se consolidó como una herramienta ampliamente utilizada en entornos educativos, corporativos y de investigación, destacándose por su enfoque en la facilidad de administración, estabilidad y alto nivel de seguridad.

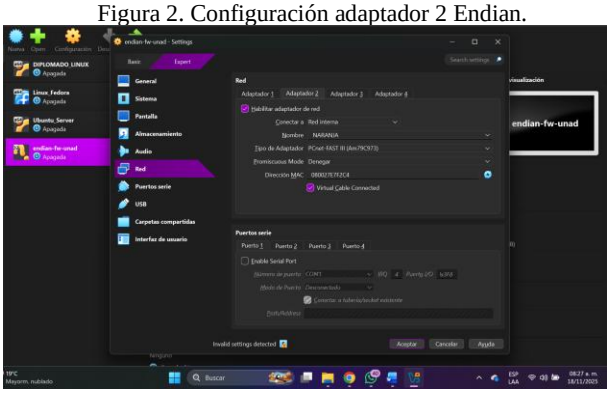
Para iniciar el proceso de implementación, se procede con la descarga de la distribución Endian Firewall desde su repositorio oficial. Una vez obtenida la imagen, se lleva a cabo la instalación en Oracle VM VirtualBox, junto con la preparación de los sistemas operativos complementarios: Ubuntu Desktop (como cliente) y Ubuntu Server (como servidor ubicado en la DMZ). Durante la configuración inicial de Endian, se asignan las interfaces de red de la siguiente manera: la tarjeta de red 1 se define como zona Verde (LAN), la tarjeta de red 2 como zona Naranja (DMZ) y la tarjeta de red 3 bajo modo NAT, la cual corresponde a la zona Roja (WAN) y proporciona conectividad hacia Internet.

Figura 1. Configuración adaptador 1 Endian.



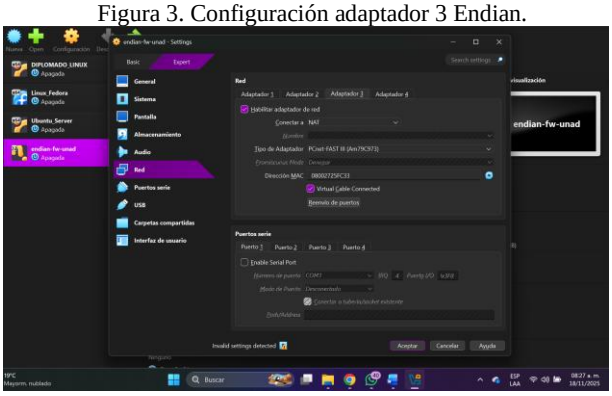
Fuente: Autoría propia

Figura 2. Configuración adaptador 2 Endian.



Fuente: Autoría propia

Figura 3. Configuración adaptador 3 Endian.



Fuente: Autoría propia

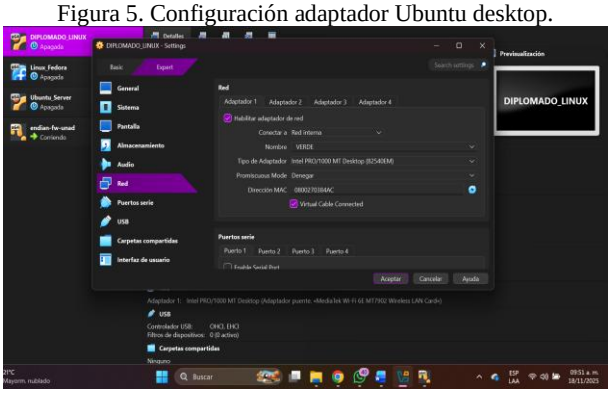
Una vez completada la instalación y configuración inicial de Endian, el sistema presenta una interfaz de administración donde es posible verificar el estado de las zonas configuradas. En esta vista se observa que las interfaces correspondientes a la zona Verde (LAN) y la zona Roja (WAN) se encuentran correctamente habilitadas y operativas, confirmando que el firewall reconoce la asignación realizada durante el proceso de configuración.

Figura 4. Interfaz Endian.

Fuente: Autoría propia

Posteriormente, se procede con la configuración de la máquina Ubuntu Desktop. En VirtualBox, el adaptador de red 1 se establece en modo *Red Interna* y se asigna al segmento correspondiente a la zona Verde. Esto permite que el equipo funcione como un cliente dentro de la red LAN gestionada por Endian, garantizando su comunicación directa con el firewall.

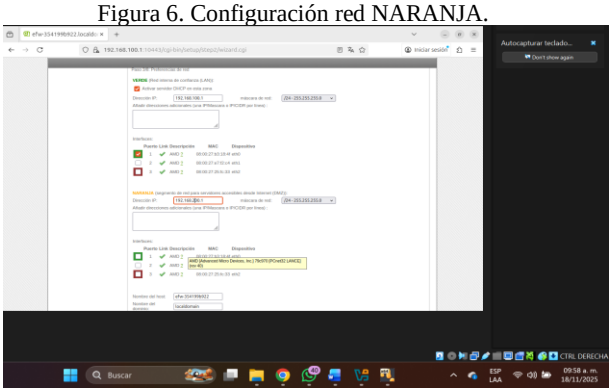
Figura 5. Configuración adaptador Ubuntu desktop.



Fuente: Autoría propia

A continuación, desde el navegador web de la máquina Ubuntu Desktop, se accede a la interfaz de administración de Endian utilizando la dirección IP asignada a la zona Verde (192.168.100.1). Desde este panel se continúa con la configuración de la zona Naranja, definiendo su dirección de red dentro del segmento 192.168.200.0/24, con la IP del firewall establecida en 192.168.200.1. Esta operación habilita la DMZ y permite incorporar posteriormente el servidor Ubuntu a dicho entorno.

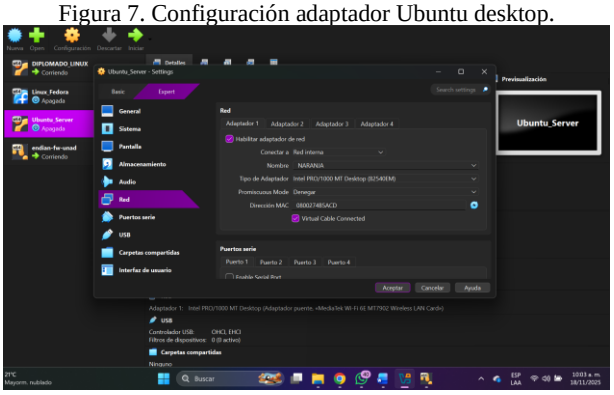
Figura 6. Configuración red NARANJA.



Fuente: Autoría propia

Posteriormente, se configura el adaptador de red 1 de la máquina Ubuntu Server. Este se establece en modo *Red Interna* y se asigna al segmento correspondiente a la zona Naranja previamente definida en Endian. Con esta configuración, el servidor queda correctamente ubicado dentro de la DMZ, permitiendo su comunicación directa con el firewall a través de la dirección 192.168.200.1.

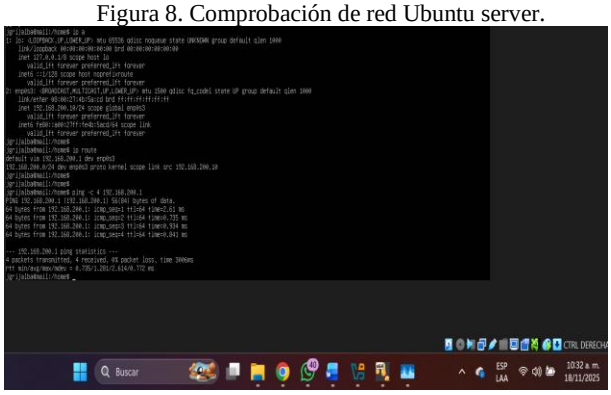
Figura 7. Configuración adaptador Ubuntu desktop.



Fuente: Autoría propia

Para verificar la conectividad de red desde el servidor, se ejecuta un ping a la IP 192.168.200.10, obteniendo respuesta satisfactoria.

Figura 8. Comprobación de red Ubuntu server.



Fuente: Autoría propia

Asimismo, desde el navegador de Ubuntu Desktop se accede a una página como Facebook para confirmar que la navegación funciona correctamente.

Figura 9. Comprobación de red Ubuntu desktop.

Fuente: Autoría propia

TEMÁTICA 2: CONFIGURACIÓN NAT.

DESCRIPCIÓN GENERAL

Primero debemos comprender que es la NAT y su función, la NAT es un servicio que opera como plataforma perimetral para conectar redes privadas a redes públicas añadiendo una capa de seguridad básica, para reducir el riesgo de ataques o amenazas al ocultar las IPs de las redes internas a las redes publicas como lo es internet, que solo verá la dirección pública del router. En el desarrollo de la temática 2 se configuran dos tipos de NAT, SNAT (Source NAT) y DNAT (Destination NAT).

La SNAT está encargada de enmascarar la dirección IP privada a la IP publica cuando el tráfico sale a internet y la DNAT traduce la dirección IP de destino de un paquete a la dirección privada dentro de la red.

El objetivo principal de la temática 2, es permitir que las terminales de la red VERDE y los servidores de la red DMZ o NARANJA tengan conectividad hacia la internet o red ROJA, garantizando además que el firewall maneje correctamente la traducción de direcciones en el tráfico saliente de cualquiera de estas dos zonas usando el enmascarado de las IP.

Después de la instalación de Endian y la configuración las zonas desarrolladas en la temática 1, se tiene para esta etapa la siguiente segmentación:

Tabla 1. Características de red para la NAT.

Distribución Linux	Función	IP
Endian 3.3.25	Servidor firewall	192.168.100.1

Ubuntu 24.04.3 live server	Servidor (web-correo-base datos-etc)	192.168.200.10
Ubuntu 24.04.3 desktop	Terminal de escritorio	192.168.100.3

Nota: Características usadas para la temática 2.

Fuente: Autoría propia

Las configuraciones necesarias para los objetivos de comunicación se realizan a través de Endian UI módulo Firewall. La función de este módulo Firewall es gestionar todo el tráfico que fluye en las zonas establecidas en el dispositivo Endian, incluyendo el tráfico entrante y saliente.

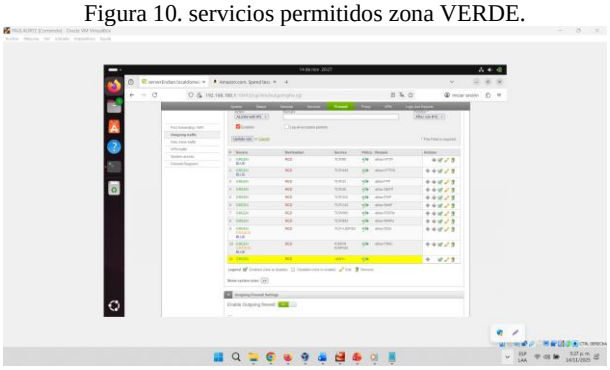
Con la opción Outgoing *traffic* que es el encargado del flujo del tráfico de servicios, puertos y aplicaciones específicas, desde las distintas zonas hacia la interfaz Roja, es decir internet y con el *Source NAT* (SNAT) que tiene como principal objetivo, controlar en el tráfico de salida qué IP o puerto se enmascara ante Internet.

Por defecto, el Endian enmascara todas las conexiones salientes a la dirección IP de la interfaz Red principal, por lo que se necesita SNAT en los casos en que no se desea que esto ocurra.

METODOLOGÍA Y CONFIGURACIÓN APLICADA

Se crean las reglas para la zona Verde donde se especifican uno a uno los servicios a los que se le permiten conectar esto es para una mejor administración y seguridad, sin embargo, es importante aclarar que estos servicios en su mayoría en su mayoría vienen por defecto en Endian.

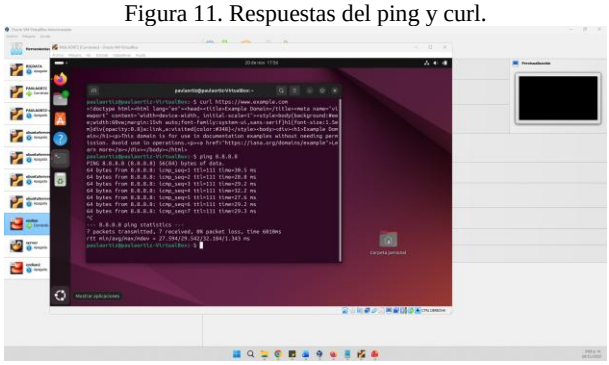
Figura 10. servicios permitidos zona VERDE.



Fuente: Autoría propia

Desde la consola del terminal desktop que pertenece a la zona VERDE, se hace el ping a una IP publica para confirmar de comunicación a la zona ROJA.

Figura 11. Respuestas del ping y curl.

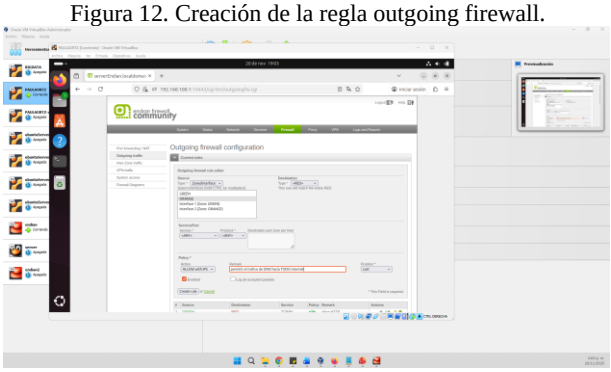


Fuente: Autoría propia

La configuración de la comunicación desde la zona DMZ hacia el exterior, es decir, Internet, se realiza a través de dos acciones importantes que son complementarias, la primera parte es permitir el tráfico desde una IP de origen hacia una IP destino y la segunda acción es cambiar la IP de la red privada por una IP pública estableciendo así un control en el flujo del tráfico tanto entrante como saliente a los servidores externos. A continuación, se describen cuáles fueron los pasos realizados en Endian para establecer esta comunicación:

En primer lugar, esta permitir el tráfico desde un origen interno DMZ hacia el exterior, para cumplir con este punto se procede a configurar el tráfico saliente, agregando una nueva regla que va a permitir la comunicación desde la Zona DMZ hacia la Zona de Internet o Roja.

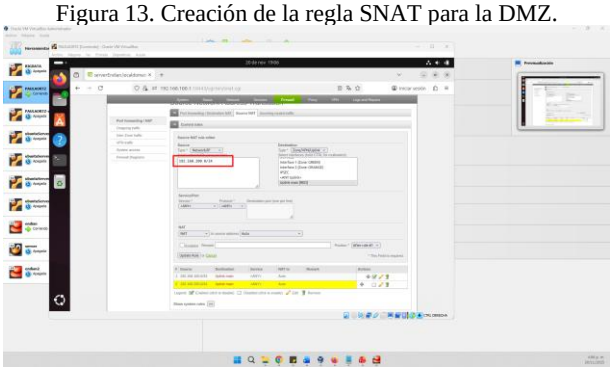
Figura 12. Creación de la regla outgoing firewall.



Fuente: Autoría propia

Posteriormente se debe garantizar la seguridad del tráfico de paquetes salientes a internet desde el servidor de la zona DMZ, para cumplir este propósito se agrega una nueva regla SNAT que se aplicara a la segmentación de la zona DMZ y de esta manera enmascarar las IPs privadas de la red con la IP pública del firewall.

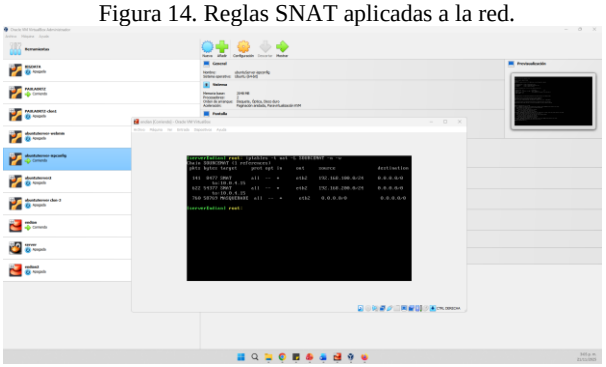
Figura 13. Creación de la regla SNAT para la DMZ.



Fuente: Autoría propia

Desde la consola de Endian, se visualiza las iptables con todas las reglas SNAT aplicadas.

Figura 14. Reglas SNAT aplicadas a la red.



Fuente: Autoría propia

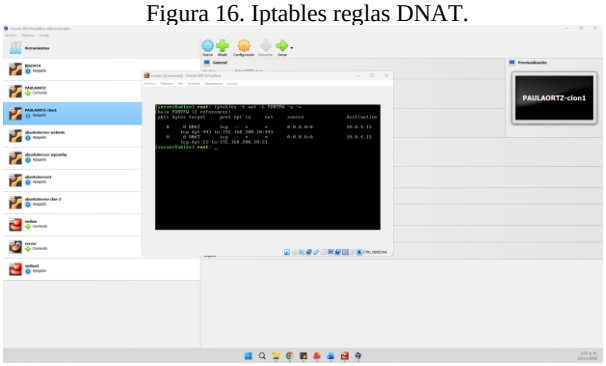
Finalmente se emplea una Destination NAT para limitar el acceso a la red DMZ desde la red Roja y para redirigir el tráfico proveniente desde la internet a la Ip interna indicada, esta acción se hace desde el módulo Port forwarding, se agrega una nueva regla DNAT. Se crean las reglas con los datos del servidor de la zona DMZ y el servicio permitido, en este caso se crean y se aplican para HTTPS(443) y FTP(22).

Figura 15. Creación reglas DNAT.

Fuente: Autoría propia

En las Iptables se almacenan todas las reglas DNAT, aquí se comprueba las reglas aplicadas.

Figura 16. Iptables reglas DNAT.



Fuente: Autoría propia

Se ejecuta ping para validar la comunicación de la red DMZ a internet

Figura 17. Conexión a internet servidor zona DMZ.

Fuente: Autoría propia

TEMÁTICA 3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

DESCRIPCIÓN GENERAL

La Zona Desmilitarizada (DMZ) constituye un segmento intermedio entre la red interna y la red externa, permitiendo alojar servidores expuestos sin comprometer la LAN. En esta temática se implementó un servidor web y un servidor FTP en la zona Naranja (DMZ) utilizando Ubuntu Server, gestionado a través del firewall perimetral Endian UTM. El objetivo fue habilitar el acceso controlado desde la red Verde (LAN) hacia la DMZ, garantizando el uso de servicios HTTP y FTP, y aplicando restricciones mediante la denegación del protocolo ICMP.

METODOLOGÍA Y CONFIGURACIÓN APLICADA

Se configuró una topología con tres segmentos de red definidos en VirtualBox:

Zona Verde (LAN): 192.168.100.0/24

Zona Naranja (DMZ): 192.168.200.0/24

Zona Roja (WAN): NAT con acceso a Internet

En Ubuntu Desktop se asignó la dirección 192.168.100.14, mientras que el servidor Ubuntu Server en la DMZ utilizó la 192.168.200.14, configurada mediante Netplan.

Figura 18. Segmentación de Red

ITEM	RED 1	RED 2	RED 3
N/A	VERDE	NARANAJA	ROJA
N/A	192.168.100.0/24	192.168.200.0/24	NAT
N/A	Desactivado	Desactivado	DHCP
Puerta de Enlace	192.168.100.1	192.168.200.1	N/A
Mascara de red	255.255.255.0	255.255.255.0	N/A
Ramgo de IP	192.168.100.2 - 192.168.100.253	192.168.200.2 - 192.168.200.253	N/A
IP FIJA	192.168.100.14	192.168.200.14	N/A

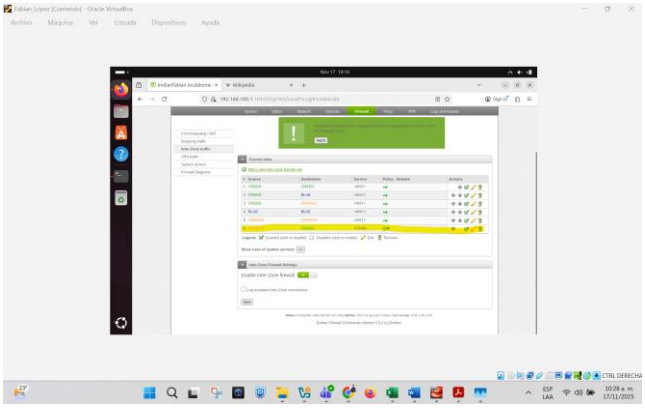
Fuente: Autoría propia

Posteriormente, desde la consola de administración de Endian UTM, se realizaron las siguientes configuraciones:

1. Permitir HTTP (puerto 80) desde la LAN hacia la DMZ.
2. Habilitar el servicio FTP (puerto 21) hacia el servidor en DMZ.
3. Crear reglas de denegación para ICMP tipo 8 y 30, bloqueando completamente el uso de ping entre ambas zonas.
4. Implementar pruebas funcionales, validando conectividad en cada caso.

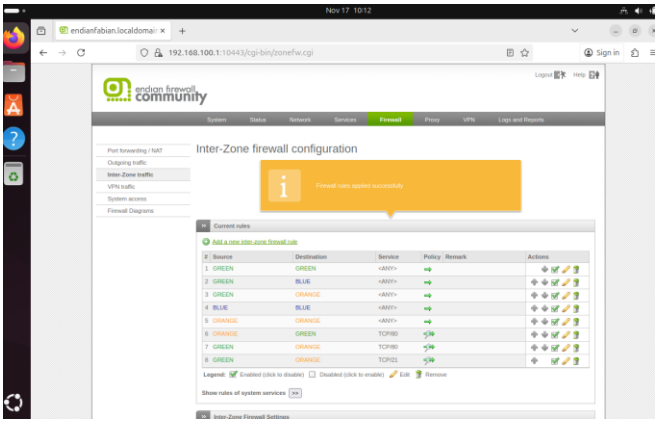
Adicionalmente, se creó una página web básica HTML para comprobar la publicación del servicio HTTP y se probó acceso FTP desde la LAN hacia la DMZ.

Figura 19. Creación de la regla permisos http del desktop al servidor



Fuente: Autoría propia

Figura 20. Creación de la regla permisos ftp del desktop al servidor



Fuente: Autoría propia

RESULTADOS OBTENIDOS

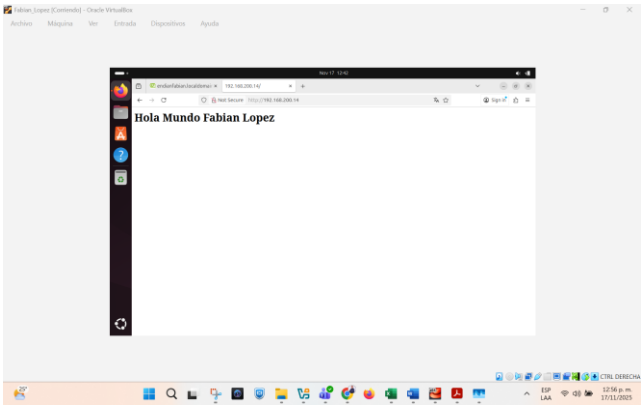
Se verificó que las reglas creadas en Endian UTM permitían el acceso correcto a:

1. Página web del servidor DMZ mediante http://192.168.200.14

2. Conexión al servicio FTP utilizando credenciales locales del servidor

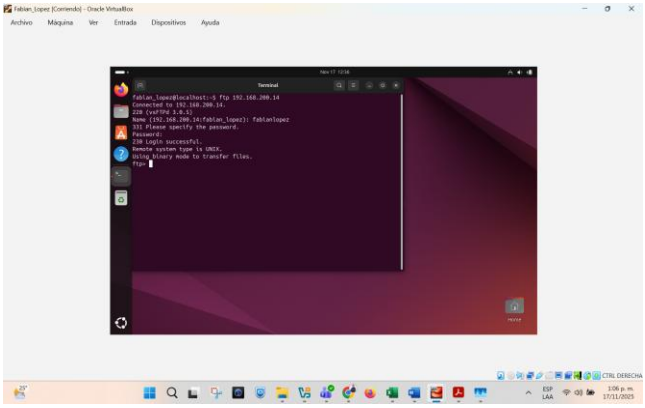
Las pruebas ICMP demostraron que las restricciones aplicadas funcionaron correctamente, impidiendo la ejecución de comandos ping tanto desde la LAN hacia la DMZ como en sentido contrario. Esto evidencia una reducción efectiva de la superficie de reconocimiento en la red interna.

Figura 21. Prueba de conexión por http a una página en el servidor



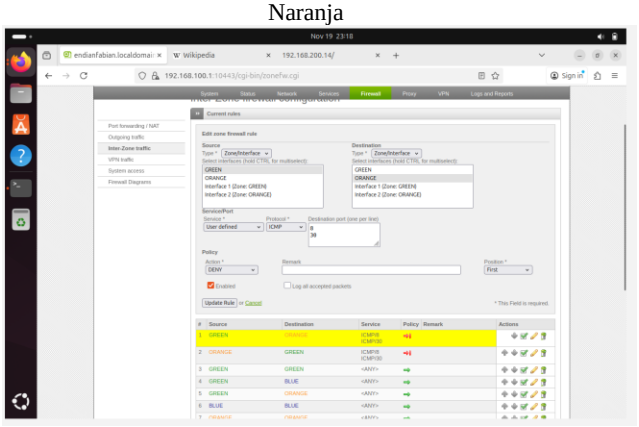
Fuente: Autoría propia

Figura 22. Validación de conexión equipo de escritorio al servidor



Fuente: Autoría propia

Figura 23. Creación de regla ICMP 8 y 30 de red Verde a Naranja



Fuente: Autoría propia

Figura 23. Validación perdida de ping entre la red Verde y la Red Naranja

Fuente: Autoría propia

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

DESCRIPCIÓN GENERAL

La Temática 4 se centra en la implementación de un **firewall inter-zonas** dentro de una arquitectura segmentada que contiene tres áreas funcionales: **WAN, DMZ y LAN**. El objetivo de este desarrollo es entender cómo el tráfico circula entre estas zonas y cómo un firewall, mediante políticas de enrutamiento y filtrado, controla y limita dicho tráfico para garantizar seguridad y disponibilidad de los servicios.

Durante la práctica se construyó un entorno virtual usando VirtualBox, configurando un equipo central que actúa como firewall/router y que interconecta las tres zonas. Cada zona fue configurada con su propia red IP, su rol y políticas específicas. La prueba final consiste en validar comunicación entre zonas, acceso controlado desde WAN hacia servicios en DMZ y restricciones específicas hacia la LAN.

Este desarrollo demuestra cómo funcionan los principios de seguridad perimetral aplicados a un entorno realista.

CONCEPTOS CLAVES

Inter-Zone Firewall: Un **inter-zone firewall** es un cortafuegos que opera entre distintas zonas de seguridad, controlando el tráfico que cruza de una zona a otra. No protege únicamente un perímetro externo, sino que regula los flujos **entre segmentos internos**, por ejemplo:

- WAN ↔ DMZ
- DMZ ↔ LAN
- LAN ↔ WAN

En un entorno segmentado, cada zona tiene un nivel distinto de confianza. El firewall evalúa las reglas definidas para permitir, denegar o transformar (NAT/DNAT) el tráfico entre zonas.

Características principales:

- Define **políticas explícitas** entre zonas.
- Evita movimiento lateral dentro de la red.
- Permite separar servicios públicos (DMZ) de recursos internos (LAN).
- Maneja NAT, DNAT y forwarding de forma centralizada.

METODOLOGIA APLICADA

metodología general:

1. Se configuraron las interfaces del Endian Firewall asignando IPs a cada zona:
    a. **Green:** 192.168.100.1
    b. **Orange:** 192.168.200.1
    c. **Red:** DHCP
2. Se desplegaron máquinas virtuales:
    a. PC en LAN: 192.168.100.10
    b. Servidor DMZ con Apache + FTP: 192.168.200.10

c. Internet simulado: NAT VirtualBox

3. Se accedió a la interfaz web de Endian y se ingresó al módulo: **Firewall → Inter-Zone Firewall**
4. Se crearon reglas específicas para:
    a. Permitir HTTP y FTP entre LAN y DMZ
    b. Permitir tráfico HTTP y FTP entre DMZ y WAN
    c. Permitir accesos desde WAN a DMZ
5. Se verificaron reglas en la tabla Inter-Zone.
6. Se realizaron pruebas desde los navegadores y clientes FTP.
7. Se inspeccionaron logs en: Logs → Firewall → Inter-Zone

METODOLOGIA APLICADA

Para la creación de las reglas, se tiene en cuenta lo siguiente, para esta gestión, se debe acceder al siguiente apartado del administrador. Firewall → Inter-Zone Firewall.

El enfoque se basa en permitir únicamente el tráfico necesario entre zonas, restringiendo todo lo demás bajo políticas de mínima exposición. Para ello se inhabilitan las configuraciones predeterminadas

Comunicación GREEN -> ORANGE (HTTP Y FTP):

Para lograr esta comunicación se realiza la creación de las siguientes reglas:

- Regla #1: HTTP desde LAN hacia DMZ
    - Origen: **Green → Orange**
    - Servicio: **HTTP (TCP 80)**
    - Acción: **Allow**
    - Registrar logs: Habilitado
- Regla 2: Permitir FTP desde LAN → DMZ
    - Origen: **Green → Orange**
    - Servicio: **FTP (TCP 21)**
    - Acción: Allow

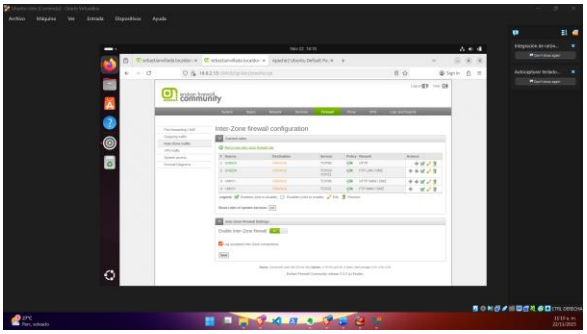
Comunicación RED -> ORANGE (HTTP y FTP)

Para lograr una comunicación desde la zona RED al DMZ, se deben tener en cuenta las siguientes reglas:

- Regla #3: HTTP desde WAN hacia DMZ
    - Origen: **Red → Orange**
    - Servicio: HTTP
    - Acción: Allow
- Regla #4: FTP desde WAN hacia DMZ
    - Origen: **Red → Orange**
    - Servicio: FTP
    - Acción: Allow

Por medio de la configuración de las siguientes reglas se podrá evidenciar el siguiente resultado de configuración y asignación

Figura 25. Verificación resultado final creación de reglas Inter-zona



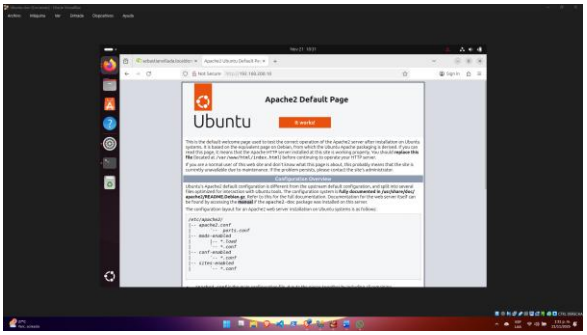
Fuente: Autoría propia

RESULTADOS ESPERADOS

Para validar la efectividad de las reglas se realizan pruebas desde distintos segmentos de la red.

Acceso HTTP desde LAN → DMZ: HTTP desde Green hacia la DMZ, para ello desde el navegador accedemos a la siguiente ruta http://192.168.200.10. Siendo todo correcto debe cargar correctamente la página del servidor DMZ.

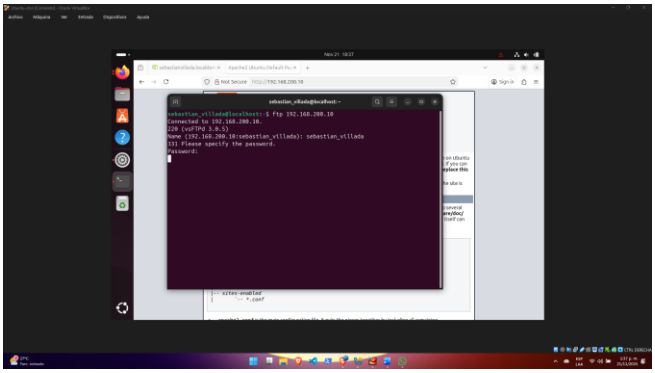
Figura 25. Validación de acceso dese de LAN al servidor encontrado en la zona DMZ.



Fuente: Autoría propia

Para validar el FTP desde Green hacia la DMZ, desde la consola del equipo se escribe el siguiente comando ftp 192.168.200.10. Estando todo correcto debe permitir autenticación y listar contenidos.

Figura 26. Pruebas de conexión FTP al servidor alojado en la DMZ.



Fuente: Autoría propia

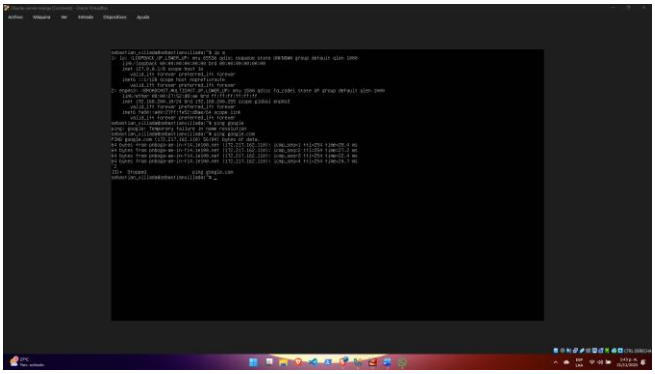
Acceso desde la LAN hacia la WAN: Para realizar las pruebas HTTP hacia la zona WAN desde el navegador accedemos a la siguiente URL http://10.0.2.15

Figura 27. Prueba de acceso a la WAN desde el equipo perteneciente a la zona LAN

Fuente: Autoría propia

Acceso desde la DMZ hacia la WAN: Desde el servidor alojado en la dirección 192.168.200.10, realizar una petición ping hacia la red estarna, en este caso a Google. Si el resultado es correcto debe mostrar conectividad a Internet.

Figura 28. Validación de conectividad al exterior desde el servidor encontrado en la zona DMZ.



Fuente: Autoría propia

TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

DESCRIPCIÓN GENERAL

La presente temática tuvo como objetivo implementar un servicio de Proxy HTTP no transparente usando la plataforma de seguridad perimetral Endian Firewall Community, con el fin de gestionar, autenticar y controlar el tráfico de navegación proveniente de la red LAN hacia internet. Se configuraron perfiles de filtrado, listas negras, usuarios con autenticación y políticas de acceso, garantizando un control granular sobre los recursos web permitidos para los clientes internos. La actividad se desarrolló dentro de un entorno virtualizado en Oracle Virtual Box, utilizando maquinas GNU/Linux y definiendo una infraestructura con zonas red (WAN), Green (LAN) y Orange (DMZ), siguiendo las buenas prácticas para segmentación de redes.

CONCEPTOS CLAVES

Proxy HTTP no Transparente: Servicio que filtra y controla el trafico web, requiriendo configuración explicita del proxy en los navegadores. Permite autenticación por usuario y políticas detalladas de acceso.

Blacklist: Conjunto de dominios o URLs bloqueados explícitamente para ser negados por el proxy.

Autenticación del Proxy: Mecanismo por el cual el usuario final debe ingresar credenciales antes de hacer uso del servicio de navegación.

Perfil del Proxy: Conjunto de reglas, filtros y permisos aplicados a un grupo de usuarios o a toda la red LAN durante la navegación web.

DMZ: Área intermedia entre la red interna y la red externa, destinada a alojar servidores accesibles desde internet con seguridad reforzada.

METODOLOGIA APLICADA

La metodología utilizada en esta actividad se desarrolló a través de los siguientes pasos estructurados:

Configuración de la Infraestructura:

Implementación de Endian Firewall en Virtual Box
Asignación de direcciones IP para las zonas: WAN, LAN Y DMZ. Configuración del Ubuntu Desktop dentro de la zona Green con IP estática.

Habilitación del proxy HTTP no transparente en Edian:

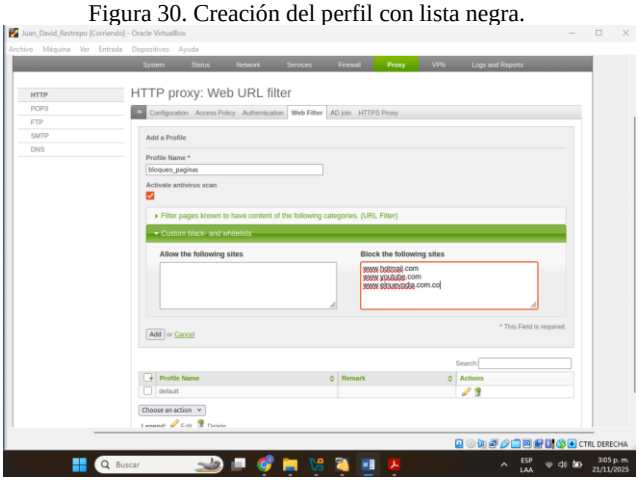
Activación del servicio de Proxy en la interfaz web.
Configuración del puerto del proxy para uso por clientes LAN.

Figura 29. Habilitación del HTTP Proxy no transparente.

Fuente: Autoría propia

Creación del perfil con lista negra: Registro de un nuevo perfil de filtrado. Inclusión de los dominios: www.hotmail.com – www.youtube.com – www.elnuevodia.com.co. Verificación del correcto funcionamiento del filtrado de contenidos.

Figura 30. Creación del perfil con lista negra.



Fuente: Autoría propia

Configuración de Autenticación por Usuario:

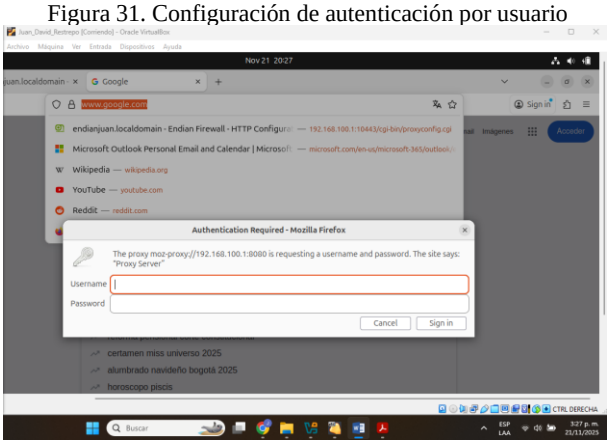
Creación de un usuario en la sección Proxy → Autenticación.

Creación de un grupo y asociación del usuario.

Asociación del usuario con el perfil previamente creado.

Configuración del navegador Firefox en Ubuntu Desktop para usar el proxy (IP Green + puerto Proxy).

Figura 31. Configuración de autenticación por usuario



Fuente: Autoría propia

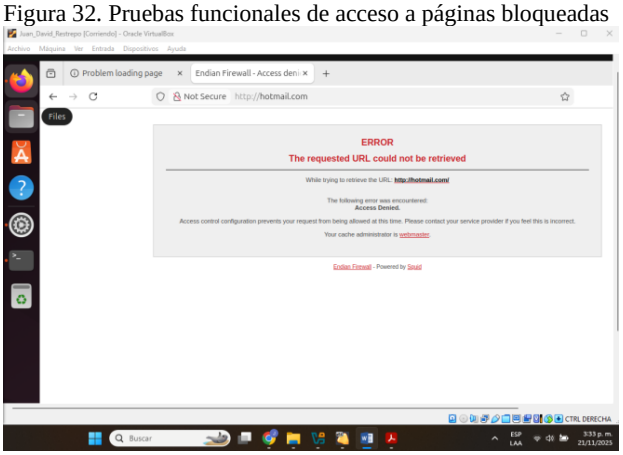
Pruebas Funcionales desde la LAN

Intentos de acceso hacia los dominios en la lista negra, verificando el bloqueo.

Acceso a otros sitios permitidos para verificar funcionamiento normal.

Validación de credenciales requeridas en el navegador antes de permitir conexión.

Figura 32. Pruebas funcionales de acceso a páginas bloqueadas



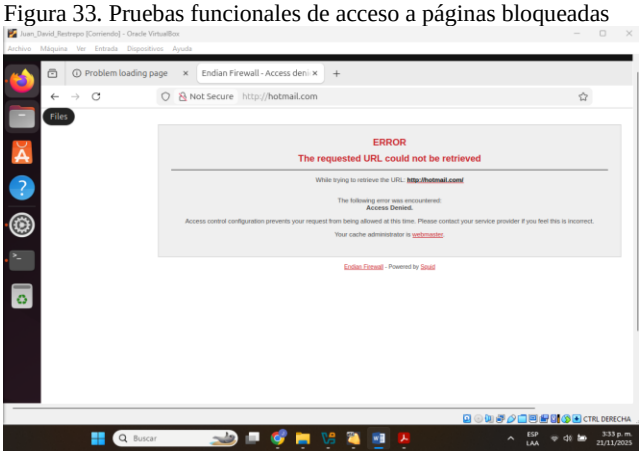
Fuente: Autoría propia

RESULTADOS ESPERADOS

Los resultados esperados y obtenidos en la práctica fueron:

Bloqueo efectivo de los dominios configurados en la lista negra mediante el perfil de filtrado.

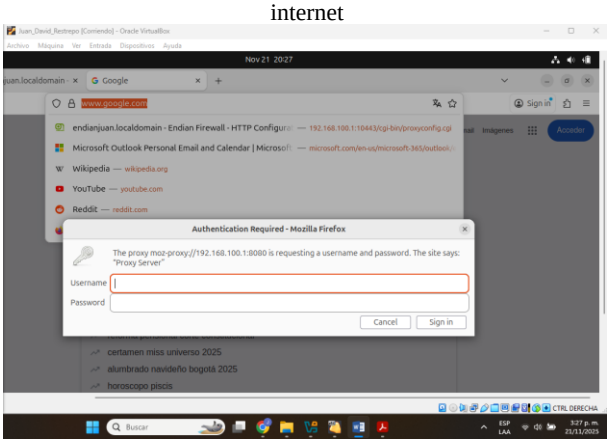
Figura 33. Pruebas funcionales de acceso a páginas bloqueadas



Fuente: Autoría propia

Autenticación obligatoria de los usuarios antes de permitir acceso a Internet mediante el proxy.

Figura 34. Pruebas de autenticación antes de navegar por internet

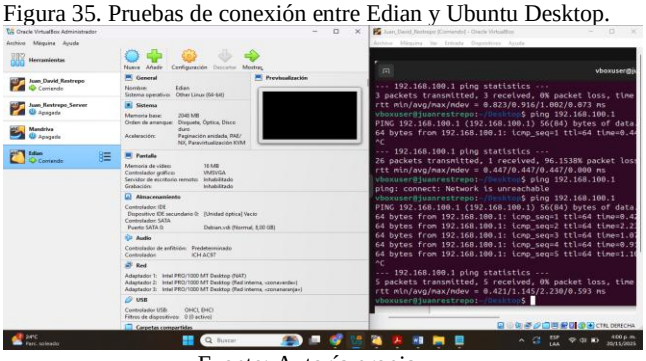


Fuente: Autoría propia

Navegación controlada y filtrada desde la LAN hacia Internet.

Evidencia de comunicación estable y correcta entre Ubuntu Desktop (cliente) y Endian Firewall (proxy).

Figura 35. Pruebas de conexión entre Edian y Ubuntu Desktop.



Fuente: Autoría propia

1.1.1 Conclusiones.

La segmentación de red mediante Endian UTM permitió un control granular y seguro del tráfico entre las zonas LAN y DMZ, evidenciándose en el funcionamiento adecuado de los servicios HTTP y FTP, así como en la correcta restricción del protocolo ICMP, lo cual fortaleció la seguridad interna al limitar actividades de reconocimiento no autorizadas.

El aislamiento del tráfico permite asegurar el anonimato a través del enmascaramiento NAT protegiendo, así las identidades de los servidores y terminales que acceden a internet desde la red. Con esta técnica se refuerza la seguridad ante las amenzas especialmente en las zonas DMZ evitando que se comparta la estructura interna y la ubicación de los hosts.

La implementación de reglas de acceso en Endian Firewall permitió comprobar de manera práctica cómo el control del tráfico inter-zona es fundamental para mantener una arquitectura de red segura y funcional. La segmentación por zonas —LAN, DMZ y WAN— facilitó la aplicación del principio de separación de responsabilidades, permitiendo que cada área operara bajo sus propias políticas de seguridad sin comprometer la integridad del conjunto.

Las reglas creadas demostraron que es posible habilitar únicamente los servicios necesarios (HTTP y FTP) sin abrir la red a riesgos innecesarios. El flujo controlado desde la LAN hacia la DMZ, y entre la DMZ y la WAN, evidenció que el firewall gestiona de forma adecuada la publicación de servicios, mientras que las pruebas de acceso desde la WAN hacia la DMZ validaron la exposición segura de recursos públicos. Adicionalmente, la inspección de los logs confirmó que el tráfico autorizado coincidió exactamente con lo definido en las políticas, lo que refleja un funcionamiento estable y confiable del sistema.

La implementación del Proxy HTTP no transparente en Endian permitió establecer un control efectivo sobre la navegación desde la red LAN, validando en la práctica el funcionamiento de políticas de filtrado y autenticación de usuarios. A través de la creación de un perfil de acceso, una lista negra personalizada y un esquema basado en credenciales, se logró restringir correctamente portales específicos como hotmail.com, youtube.com y elnuevodia.com.co, cumpliendo con los requerimientos de la actividad.

REFERENCIAS

Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

Cyberleon. (2019). Instalación y configuración Firewall ENDIAN. Slideshare. https://es.slideshare.net/slideshow/instalacin-y-configuracin-firewall-endian/39219423

Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04 . [Objeto_virtual_de_información_OVI].

Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

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

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

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

Endian UTM 5.0 Reference Manual. (2025). https://docs.endian.com/5.0/utm/firewall.html#inter-zone-traffic

Kurose, J. F., & Ross, K. W. (2017). Redes de computadoras
Un enfoque descendente. Person (pp. 278–288)

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

LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/