IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL Y ADMINISTRACIÓN DE SERVICIOS GNU/LINUX MEDIANTE FIREWALL ENDIAN

Daniel Stiven Barragan Calderon
dsbarraganc@unadvirtual.edu.co
Juan Pablo Marin Marin
jpmarinm@unadvirtual.edu.co
John Alexander Oviedo Mancera
jaoviedoma@ unadvirtual.edu.co
Juan Pablo Pascuas Lopez
jppascuasl@unadvirtual.edu.co
Jose Armando Cuellar Uyuco
jacuellaru@ unadvirtual.edu.co

RESUMEN: *El presente artículo técnico describe la implementación de una infraestructura de seguridad perimetral robusta diseñada para la protección de activos de red en entornos corporativos. Mediante el uso de Endian UTM como plataforma firewall y estaciones de trabajo GNU/Linux, se muestra el proceso de segmentación de la red en zonas verde (LAN), roja (WAN) y naranja (DMZ). El desarrollo incluye desde la configuración de hardware y ajustes del núcleo según el estándar LPI 101, hasta la ejecución de políticas de traducción de direcciones de red (NAT), reglas de filtrado de tráfico para servicios HTTP/FTP y gestión de acceso mediante un proxy no transparente con políticas de autenticación. Los resultados evidencian la efectividad de la zona desmilitarizada para aislar servidores críticos de la intranet, protegiendo la integridad de las bases de datos y aplicaciones web frente a tráfico no autorizado desde redes externas.*

Abstract: This technical article presents the implementation of a robust perimeter security infrastructure designed to protect network assets in corporate environments. By employing Endian UTM as a firewall platform and GNU/Linux workstations, the process of network segmentation into green (LAN), red (WAN), and orange (DMZ) zones is demonstrated. The development spans from hardware configuration and kernel adjustments according to the LPI 101 standard to the execution of network address translation (NAT) policies, traffic filtering rules for HTTP/FTP services, and access management through a non-transparent proxy with authentication policies. The results highlight the effectiveness of the demilitarized zone in isolating critical servers from the intranet, thereby safeguarding the integrity of databases and web applications against unauthorized traffic from external networks.

PALABRAS CLAVE: DMZ, Endian, UTM, Firewall, GNU/Linux, Seguridad. Apache2, FTP, Proxy.

1 INTRODUCCIÓN

Se documenta la solución técnica a un problema de seguridad perimetral donde se busca garantizar la protección de una intranet (LAN) y una extranet (WAN) mediante la implementación de una zona DMZ (Zona Desmilitarizada).

Como punto de partida se tomó como base la distribución GNU/Linux Endian (EFW), la cual actúa como plataforma de seguridad principal para la interconexión de zonas. El desarrollo se divide en cinco ejes temáticos fundamentales: La configuración inicial de instancias en entornos virtuales, la implementación de reglas NAT para la comunicación inter-zona, la gestión de servicios web seguros, la creación de directivas de acceso y la configuración de servidores proxy con listas negras de navegación.

Cada sección del artículo representa el desarrollo técnico, integrando comandos de administración de sistemas alineados con la certificación Linux Essentials del Linux Professional Institute (LPI) y validando el estado de los servicios mediante pruebas de ejecución.

2 METODOLOGÍA Y HERRAMIENTAS

La metodología aplicada en este proyecto es de carácter experimental y colaborativo, enfocada en el despliegue de una infraestructura de red segura. Se utiliza la virtualización como entorno de pruebas mediante Oracle VirtualBox, permitiendo la interacción entre diferentes sistemas operativos y la segmentación lógica de la red. El núcleo de la seguridad perimetral se basa en la distribución Endian UTM 3.2, la cual se encarga de gestionar el tráfico en tres zonas distintas: la red interna (Verde), la zona de servicios (Naranja) y el acceso externo (Roja). Para la administración de servicios y estaciones de trabajo, se emplean distribuciones basadas en Debian y Ubuntu, basada en las prácticas de configuración contempladas en el examen LPI 101. A continuación, se describen los parámetros de direccionamiento lógico establecidos para

garantizar la comunicación y el aislamiento de los segmentos de red:

Tabla 1. Parámetros de direccionamiento por zonas de red.

Zona	Descripción de la Interfaz	Segmento de Red/IP	Rol en la Seguridad
Verde	Red interna (LAN)	192.168.1.0/24	Confianza total / Estaciones de trabajo
Naranja	Servidores (DMZ)	192.168.2.0/24	Servicios públicos (HTTP/FTP)
Roja	Acceso a Internet (WAN)	DHCP / IP Pública	Red no confiable (Internet)

Fuente. Autoría Propia

El direccionamiento IP definido en esta tabla es la base para la configuración de las reglas NAT y las políticas de tráfico inter-zona desarrolladas en las secciones posteriores.

2.1 INFRAESTRUCTURA DE RED

La topología utilizada garantiza que el tráfico de la red LAN esté protegido por el firewall, y los servidores Web y de bases de datos se encuentran en la DMZ para permitir el acceso controlado desde el exterior, sin poner en peligro la integridad de la red interna. Mediante comandos de consola se valida el estado y mantenimiento de estos servicios, asegurando la trazabilidad de cada acción ejecutada.

3 DESARROLLO TÉCNICO

En esta sección se detalla la ejecución de las temáticas propuestas, integrando la administración de servicios bajo estándares GNU/Linux y la validación de reglas en el firewall Endian.

3.1 Temática 1: Configuración de la instancia e instalación de Endian

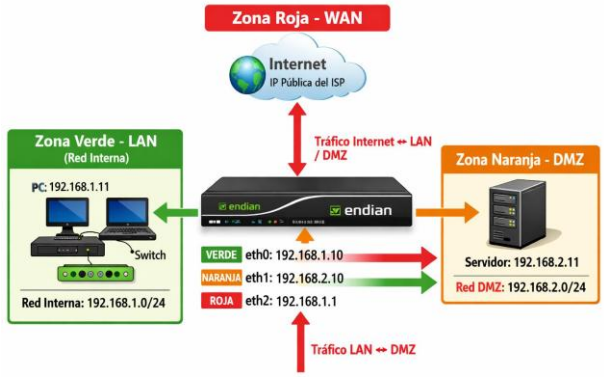
A. Arquitectura de red y virtualización

La base de la seguridad perimetral implementada reside en la correcta segmentación de redes mediante la virtualización con Oracle VirtualBox. En esta fase, se definieron los parámetros de hardware necesarios para soportar el firewall Endian UTM 3.2.2. Se asignó una memoria base de 1024 MB y dos núcleos de procesamiento para garantizar la estabilidad de los servicios de inspección de paquetes.

La configuración más crítica en esta etapa es la gestión de los adaptadores de red, los cuales se organizaron de la siguiente manera para cumplir con el esquema de zonas de seguridad:

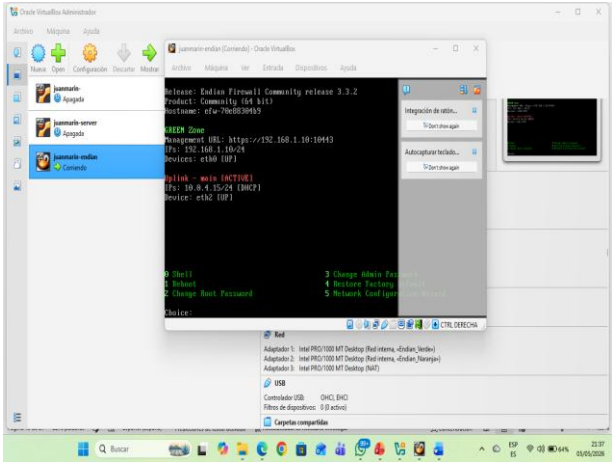
- Adaptador 1 (Zona Roja/WAN): Configurado en modo "Adaptador Puente" o "NAT" para proveer salida a Internet al firewall y, por extensión, a toda la red protegida.
- Adaptador 2 (Zona Verde/LAN): Configurado como "Red Interna" para comunicar de forma segura las estaciones de trabajo locales.
- Adaptador 3 (Zona Naranja/DMZ): Configurado como una "Red Interna" independiente para aislar los servidores web y de bases de datos.

Fig 1. Diagrama de flujo de red y enrutamiento para zonas.



Fuente: Autoría Propia

Fig 2. Instalación de Endian con adaptadores de red habilitados.



Fuente: Autoría Propia

B. Implementación del sistema operativo y comandos de hardware (LPI 101)

Una vez configurado el hardware virtual, se procedió con la carga de la imagen ISO de Endian y el proceso de instalación. Durante esta etapa, se aplicaron conocimientos del estándar LPI 101 para la identificación y gestión de dispositivos de red. Se utilizó la consola de comandos para validar que el núcleo

(kernel) de Linux reconociera correctamente las interfaces de red asignadas.

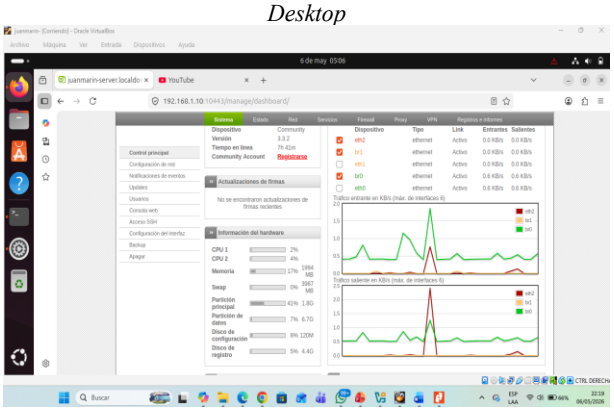
El uso de comandos como dmesg | grep eth permitió confirmar la detección de los adaptadores Ethernet, mientras que la configuración de las direcciones IP estáticas para cada zona se realizó siguiendo el direccionamiento lógico previamente definido.

C. Validación de la puesta en marcha y estado del sistema

Tras completar la instalación, la validación final se realizó mediante el acceso a la interfaz web de administración desde una máquina desktop configurada en la zona Verde. El Dashboard principal de Endian sirve como herramienta de monitoreo inicial, permitiendo verificar en tiempo real el consumo de recursos de CPU y memoria, así como el estado de enlace (Up/Down) de cada zona.

Desde el punto de vista de administración de sistemas, se confirmó que los servicios esenciales estuvieran operativos, asegurando que el firewall esté listo para recibir las políticas de tráfico y NAT que se describen en las secciones posteriores.

Fig 3. Dashboard de Endian desde el navegador del equipo Desktop



Fuente: Autoría Propia

3.2 Temática 2: Configuración NAT

En esta fase se implementaron las políticas de traducción de direcciones para garantizar que los hosts situados en los segmentos protegidos (Verde y Naranja) pudieran establecer comunicaciones con redes externas (Zona Roja). La correcta configuración de NAT fue esencial para ocultar el direccionamiento interno y optimizar el uso de IPs públicas.

A. Configuración de NAT de origen (Source NAT) para la red LAN

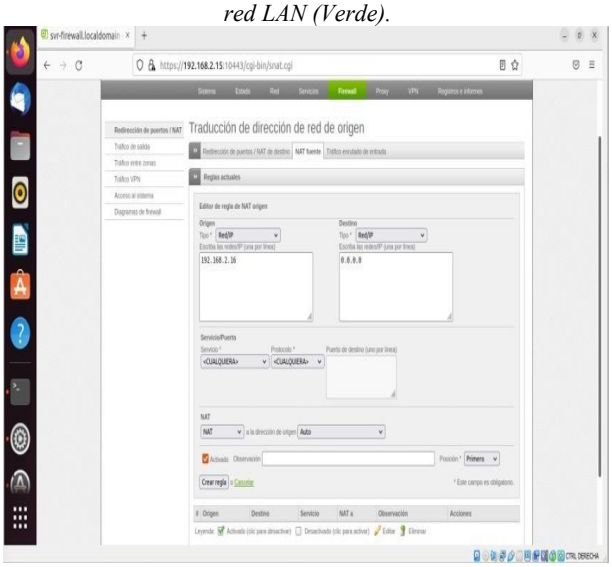
El primer objetivo consistió en permitir que las estaciones de trabajo de la zona Verde (LAN) tuvieran salida hacia la WAN. Para ello, se accedió al módulo de Firewall - NAT Fuente en la interfaz de Endian UTM. Se definió una regla de traducción que permite que todo el tráfico originado en el segmento 192.168.1.0/24 sea enmascarado con la dirección IP de la interfaz Roja.

Este proceso asegura que las peticiones hacia servidores externos sean procesadas por el firewall, manteniendo la integridad de la red interna al no exponer directamente las IPs privadas a Internet.

Fig 4. Traducción de dirección de red de origen.

Fuente: Autoría Propia

Fig 5. Configuración de la regla de acceso de internet sobre la red LAN (Verde).



Fuente: Autoría Propia

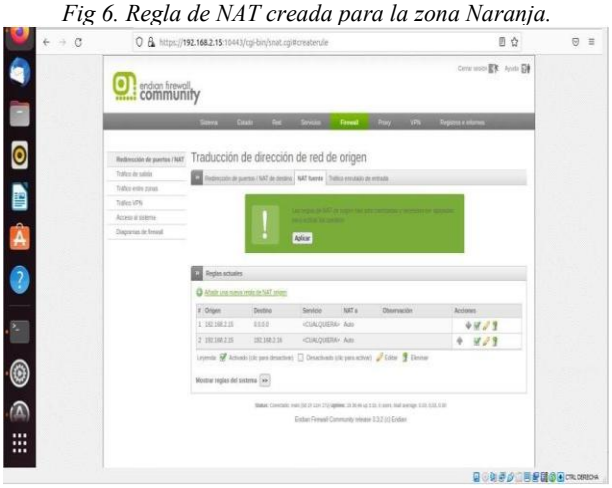
B. Comunicación de la zona DMZ hacia la WAN

De forma análoga a la red interna, se procedió a configurar la salida para la zona Naranja (DMZ). Aunque los servidores en esta zona están destinados a recibir peticiones externas, también requieren realizar conexiones de salida (por ejemplo, para actualizaciones de repositorios de Linux).

Se estableció una regla de NAT de origen específica para el segmento de la DMZ, validando mediante pruebas de conectividad que los servidores Ubuntu Server pudieran

alcanzar dominios externos. La creación de estas reglas se verificó en la tabla de estados del firewall, confirmando la persistencia de las traducciones.

Fig 6. Regla de NAT creada para la zona Naranja.



Fuente: Autoría Propia

Fig 7. Reglas almacenadas.

Fuente: Autoría Propia

Fig 8. Navegación desde la maquina cliente.

Fuente: Autoría Propia

C. Verificación y validación de reglas NAT

La validación técnica se realizó mediante el monitoreo del tráfico en tiempo real. Se verificó que las tablas de reenvío de puertos y NAT estuvieran operativas, permitiendo el flujo bidireccional necesario para el protocolo TCP/IP.

Desde la perspectiva de administración de sistemas, se relacionó esta actividad con los objetivos de red del estándar LPI 101, específicamente en lo que respecta a la configuración básica de red y la comprensión de cómo el sistema gestiona las rutas y el enmascaramiento de paquetes a nivel de núcleo.

3.3 Temática 3: implementación de servicios DMZ y políticas de filtrado

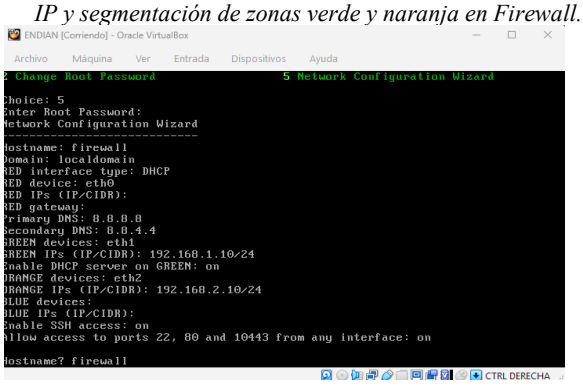
A. Configuración de la zona DMZ y segmentación de red.

La infraestructura se desarrolló sobre un entorno virtualizado mediante Oracle VirtualBox utilizando Endian Firewall Community como sistema principal de administración y seguridad perimetral. Para el aislamiento de servicios se configuró la zona DMZ (Naranja), asignando el segmento de red 192.168.2.0/24, mientras que la red interna (Verde) utilizó el direccionamiento 192.168.1.0/24

La segmentación realizada permitió dividir los servicios públicos de los equipos pertenecientes a la red LAN, minimizando la exposición de la infraestructura interna y mejorando el control del tráfico entre zonas.

Durante el asistente de configuración de Endian Firewall se realizó la asignación de interfaces y direccionamiento IP para cada zona. La zona Verde fue configurada con la dirección 192.168.1.10/24 habilitando además el servicio DHCP para la red LAN, mientras que la zona Naranja destinada a la DMZ fue configurada con la dirección 192.168.2.10/24 para el alojamiento del servidor Ubuntu Server. Asimismo, la zona Roja fue establecida mediante configuración DHCP permitiendo la salida a Internet desde el entorno virtualizado.

Fig 9. Configuración inicial de interfaces, direccionamiento IP y segmentación de zonas verde y naranja en Firewall.



Fuente: Autoría Propia

B. Implementación de servicios HTTP y FTP.

Sobre el servidor Ubuntu Server ubicado en la zona DMZ se realizó la instalación y configuración de los servicios Apache2 y VSFTPD. Apache2 fue utilizado para habilitar el servicio web mediante el puerto 80, mientras que VSFTPD permitió establecer conexiones FTP mediante el puerto 21. facilitando la transferencia y acceso remoto de archivos dentro del entorno virtualizado.

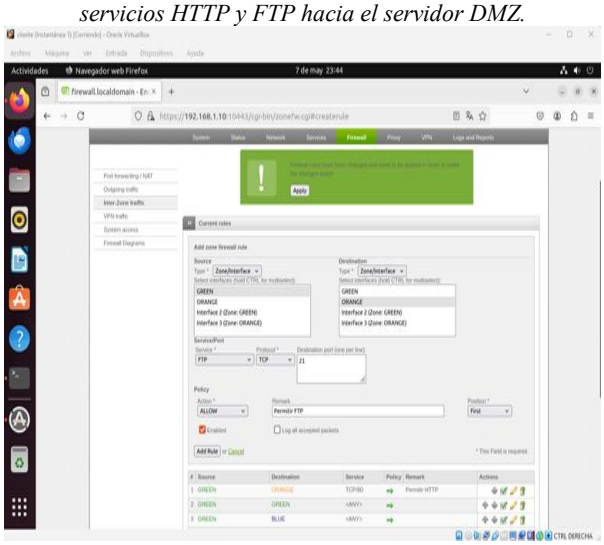
Los servicios fueron instalados sobre Ubuntu Server mediante el gestor de paquetes APT utilizando los siguientes comandos:

- Sudo apt update
- Sudo apt install apache2 -y
- Sudo apt install vsftpd -y

Una vez finalizada la instalación, se verificó el estado operativo de los servicios mediante herramientas administrativas propias de GNU/Linux.

Posteriormente, dentro de la configuración de Endian Firewall Community se crearon reglas inter-zona para permitir el tráfico como zona fuente la red verde hacia el destino la zona naranja únicamente sobre los puertos asociados a HTTP y FTP. Esto permitió mantener un esquema de acceso controlado hacia los servicios ofrecidos en la red.

Fig 10. Configuración de reglas inter-zona para habilitar servicios HTTP y FTP hacia el servidor DMZ.



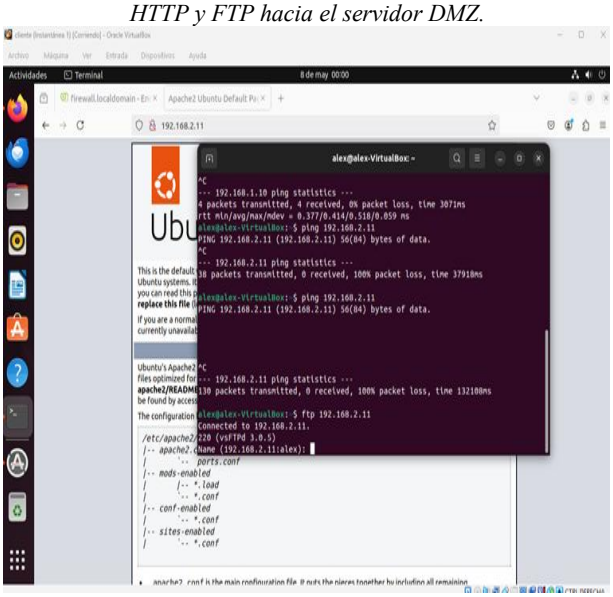
Fuente: Autoría Propia

C. Restricción de tráfico ICMP y validación de conectividad

Con el objetivo de fortalecer la seguridad perimetral, se implementó una política de restricción ICMP den el firewall Endian. Esta configuración impidió las respuestas ante los ping realizados desde la red LAN hacia el servidor ubicado en la zona DMZ, reduciendo tareas básicas de reconocimiento de red.

Las pruebas finales permitieron verificar el comportamiento era el esperado de las reglas configuradas. Desde el cliente LAN fue posible acceder correctamente a los servicios HTTP y FTP publicados sobre el servidor DMZ, como evidenciamos las pruebas ICMP presentaron pérdida total de paquetes debido al bloqueo por la regla de firewall de Endian.

Fig 11. Verificación reglas inter-zona para habilitar servicios HTTP y FTP hacia el servidor DMZ.



Fuente: Autoría Propia

D. Verificación de servicios y validación de políticas

Después de la configuración de los servicios y reglas de seguridad, se realizaron diferentes pruebas de conectividad desde el cliente ubicado en la red GREEN hacia el servidor DMZ implementado en la zona naranja donde Inicialmente se verificó la disponibilidad del servicio web mediante el acceso desde un navegador hacia la dirección IP del servidor, obteniendo correctamente la página predeterminada de Apache2.

Una vez se realizaron las pruebas FTP desde consola utilizando el cliente integrado de Ubuntu, estableciendo conexión satisfactoria con el servicio VSFTPD configurado previamente sobre el servidor DMZ. Estas pruebas permitieron validar el correcto funcionamiento de las reglas creadas dentro de Endian Firewall Community para el tráfico autorizado.

Finalmente, se ejecutaron pruebas ICMP utilizando el comando ping desde el cliente LAN IP 192.168.1.11 hacia el servidor ubicado en la zona ORANGE con IP 192.168.2.11 Como resultado, el sistema presentó pérdida total de paquetes debido a las políticas de denegación configuradas sobre el firewall, confirmando el correcto filtrado del tráfico ICMP entre zonas de red.

3.4 Temática 4: reglas de acceso para permitir o denegar el tráfico

Se utilizo VirtualBox como plataforma de virtualización. Se configuraron los diferentes adaptadores de red para simular las zonas de seguridad requeridas por Endian Firewall Community:

- Zona verde: Red LAN.
- Zona naranja: Red DMZ.
- Zona roja: Conexión WAN.

La máquina Ubuntu fue utilizada como cliente para realizar pruebas de conectividad y acceso a servicios.

A. configuración de Endian Firewall Community

Después de instalar Endian Firewall Community se accedió al dashboard web mediante la dirección IP asignada a la zona verde.

Dentro del panel administrativo se configuraron las interfaces de red, las políticas de tráfico y las reglas de firewall necesarias para permitir el acceso controlado a diferentes servicios.

Asimismo, se verificó el funcionamiento correcto de las interfaces eth0, eth1 y eth2, asociadas a las zonas verde, naranja y roja.

B. Implementación de reglas de firewall

Posteriormente se crearon reglas de salida para permitir diferentes protocolos desde la red interna hacia Internet. Las reglas configuradas incluyeron:

- HTTP (TCP/80)
- HTTPS (TCP/443)
- FTP (TCP/21)
- DNS (TCP+UDP/53)
- ICMP (PING)

Estas políticas permitieron controlar el tráfico saliente desde las zonas verde y naranja hacia la zona roja.

Además, se realizaron pruebas de navegación web y resolución DNS para validar el funcionamiento de las reglas configuradas.

C. Configuración de reglas inter-zona

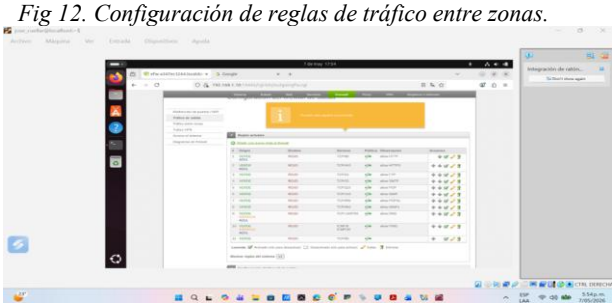
En esta etapa se implementaron políticas de acceso dentro de Endian Firewall Community con el objetivo de permitir y controlar la comunicación entre las diferentes zonas de red definidas previamente: verde (LAN), naranja (DMZ) y roja (WAN). Estas configuraciones permitieron aplicar conceptos de segmentación y filtrado de tráfico mediante reglas específicas de firewall.

Inicialmente se verificó el funcionamiento de las interfaces de red y el direccionamiento IP asignado a cada zona. Posteriormente, desde el módulo de firewall de Endian se procedió a la creación de reglas de salida y reglas inter-zona para habilitar protocolos específicos como HTTP, HTTPS, FTP, DNS e ICMP.

Las reglas implementadas permitieron la comunicación entre la zona Verde y la zona Naranja mediante los protocolos HTTP y FTP utilizando sus respectivos puertos TCP/80 y TCP/21. Asimismo, se habilitó el tráfico HTTP desde la LAN hacia la WAN y desde la DMZ hacia Internet.

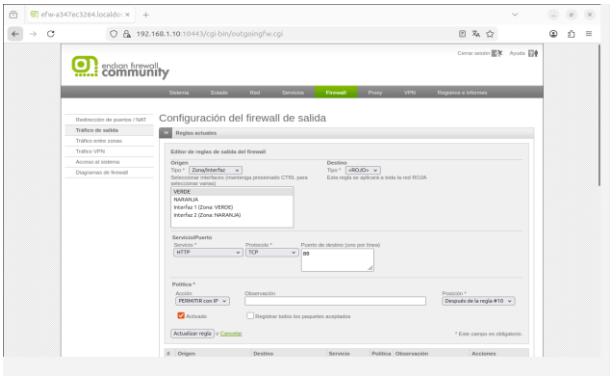
Además, se configuraron políticas de resolución DNS y validación ICMP con el propósito de comprobar la conectividad entre las diferentes zonas y validar el correcto funcionamiento del firewall.

Fig 12. Configuración de reglas de tráfico entre zonas.



Fuente: Autoría Propia

Fig 13. Creación de regla HTTP para permitir tráfico entre zonas.



Fuente: Autoría Propia

D. Comunicación entre zonas y validación de conectividad

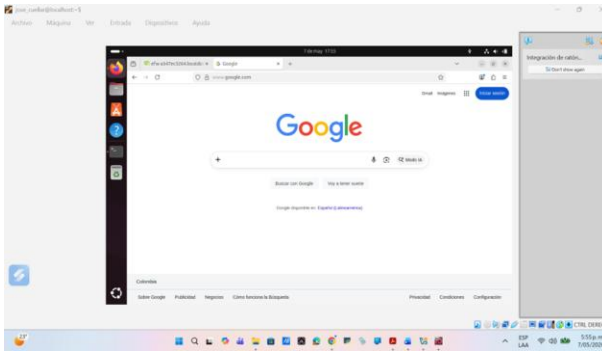
Después de configurar las reglas de acceso, se realizaron pruebas de conectividad desde la máquina cliente Ubuntu para validar el funcionamiento de las políticas implementadas.

Inicialmente se realizaron pruebas ping hacia el firewall Endian para comprobar la comunicación entre la red LAN y la zona DMZ. Posteriormente, se verificó la navegación HTTP desde la LAN hacia Internet mediante acceso a páginas web desde Mozilla Firefox.

De igual manera, se realizaron pruebas FTP hacia servidores externos, confirmando que el tráfico correspondiente al puerto TCP/21 era permitido correctamente por las políticas del firewall.

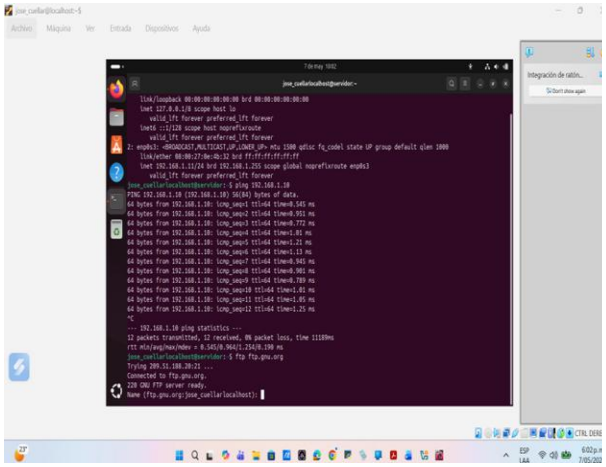
Durante las pruebas también se verificó la resolución de nombres mediante consultas DNS y conectividad hacia servidores públicos, permitiendo validar el correcto enrutamiento y acceso hacia la WAN.

Fig 14. Validación de acceso HTTP desde la red LAN hacia Internet.



Fuente: Autoría Propia

Fig 15. Validación del servicio FTP desde la red LAN hacia la WAN.



Fuente: Autoría Propia

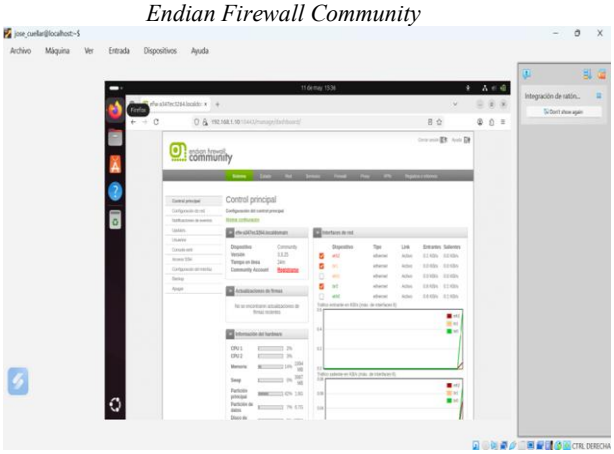
E. Verificación del tráfico y aplicación de políticas

Finalmente, se verificó el funcionamiento de las reglas creadas desde el panel administrativo de Endian Firewall Community. Dentro del módulo de tráfico inter-zona se confirmó que las políticas permitían o restringían el acceso según la configuración definida previamente.

Las pruebas realizadas demostraron que el firewall lograba controlar adecuadamente el tráfico entre las zonas GREEN, ORANGE y RED, permitiendo únicamente los servicios autorizados y bloqueando aquellos que no estaban habilitados dentro de las políticas de seguridad.

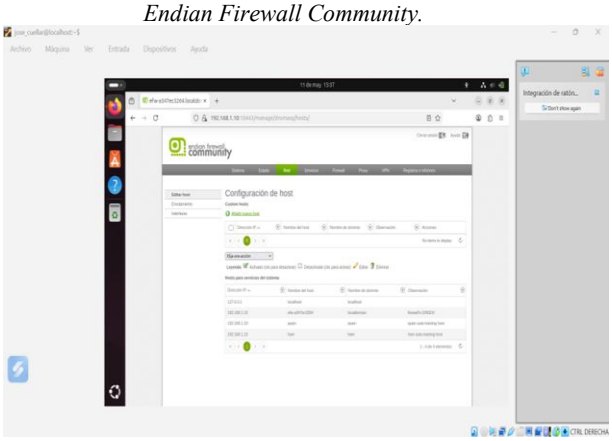
Asimismo, se evidenció la importancia de la segmentación de red para proteger servicios internos y controlar el acceso entre diferentes segmentos de red mediante reglas de firewall.

Fig 16. Monitoreo de interfaces y tráfico de red en Endian Firewall Community



Fuente: Autoría Propia

Fig 17. Verificación de hosts y configuración de red en Endian Firewall Community.



Fuente: Autoría Propia

3.5 Temática 5: Implementación de proxy HTTP y políticas de autenticación

En esta sección se documenta el despliegue inicial del Firewall Endian UTM sobre un entorno virtualizado.

A. Parámetros de red y activación del módulo proxy

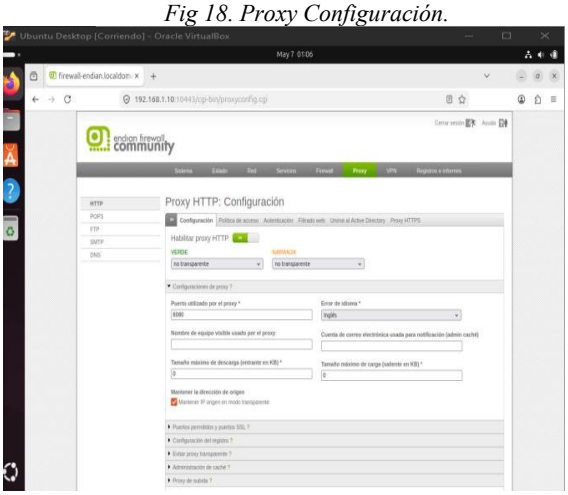
Una vez establecida la infraestructura base, se procedió a la activación del servicio de Proxy en modo No Transparente. A diferencia del modo transparente, esta configuración exige que los terminales de la red Verde (LAN) apunten explícitamente a la dirección IP del Gateway en el puerto 8080, lo que permite un control más estricto y la posibilidad de requerir credenciales de acceso.

Para asegurar el cumplimiento de las políticas de navegación, se configuró un perfil de filtrado de contenido donde se establecieron restricciones específicas para mitigar el uso de redes sociales, servicios de correo externo y portales de noticias no autorizados. Los dominios bloqueados mediante la lista negra (Blacklist) incluyeron:

- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co

A continuación, se evidencia el paso a paso para implementar un filtro de contenidos para restringir el acceso a sitios web que pueden afectar la productividad o la seguridad.

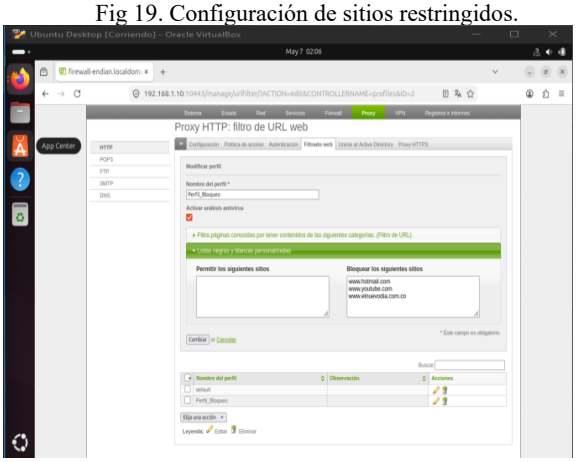
Fig 18. Proxy Configuración.



Fuente: Autoría Propia

Aquí la imagen muestra que, desde la sección de Proxy, primero en configuración habilitamos Proxy HTTP para luego poder filtrar las webs.

Fig 19. Configuración de sitios restringidos.



Fuente: Autoría Propia

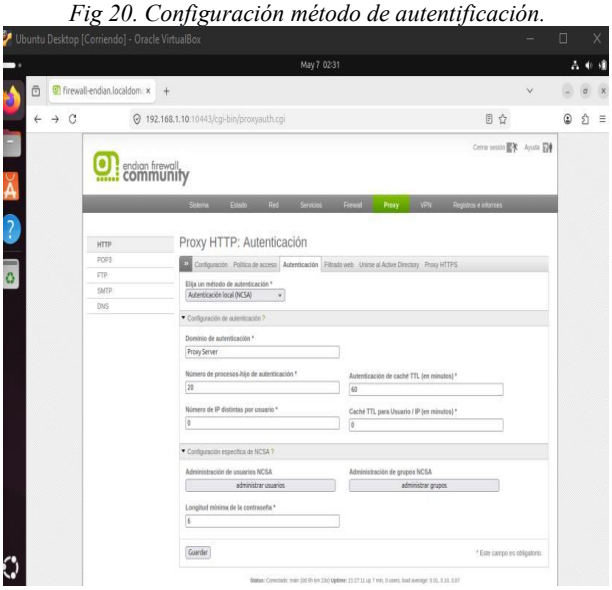
Aquí la imagen muestra que se creó y configuró el perfil denominado “Perfil_Bloqueo”, habilitando el análisis antivirus y creando una lista negra personalizada. En esta lista se añadieron los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, con el fin de bloquear el acceso a estos sitios de manera controlada desde la red.

B. Gestión de identidad y autenticación NCSA

El fortalecimiento de la seguridad perimetral se logró mediante la implementación de una política de autenticación de usuario. Se creó un grupo de usuarios dentro de la plataforma Endian, vinculando a un usuario administrativo con credenciales únicas. Al utilizar el método de autenticación NCSA, el sistema garantiza que cualquier petición hacia la zona Roja (WAN) sea identificada y registrada, eliminando el anonimato en la red corporativa.

La política de acceso se diseñó para cruzar los perfiles de los usuarios con el filtro de contenido previamente establecido, asegurando que las restricciones de la lista negra se apliquen de manera uniforme a todos los miembros del grupo definido.

Fig 20. Configuración método de autentificación.



Fuente: Autoría Propia

Fig 21. Creación y confirmación del grupo de usuarios Estudiantes.

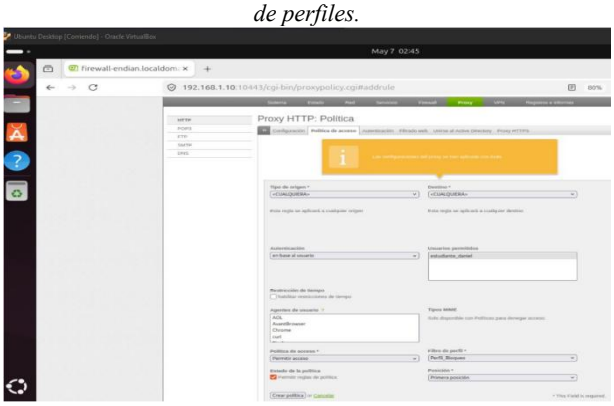
Fuente: Autoría Propia

Aquí la imagen muestra la creación exitosa del grupo "Estudiantes" bajo el método de autenticación NCSA. El recuadro informativo de color naranja confirma que los cambios han sido procesados y aplicados correctamente en el motor del proxy.

Fig 22. Gestión de cuentas de usuario en el servidor Proxy.

Fuente: Autoría Propia

Fig 23. Establecimiento de la política de acceso y vinculación de perfiles.



Fuente: Autoría Propia

Aquí la imagen muestra que se definió la regla de acceso principal, integrando tres componentes clave: el origen de la red (LAN), la identidad del usuario (estudiante_daniel) y el perfil de restricción (Perfil_Bloqueo). Además, la regla se ubicó en la primera posición para garantizar que se ejecute con prioridad sobre las demás configuraciones.

Fig 24. Resumen de política de acceso activa para el usuario estudiante Daniel.

Fuente: Autoría Propia

Aquí la imagen muestra la tabla que detalla la política número 1 denominada “filter using Perfil_Bloqueo”. En ella se observa que tanto el origen como el destino están configurados como “CUALQUIERA”, asociados específicamente al usuario estudiante_daniel. Además, el ícono de verificación verde ubicado a la izquierda confirma que la regla se encuentra habilitada y funcionando correctamente.

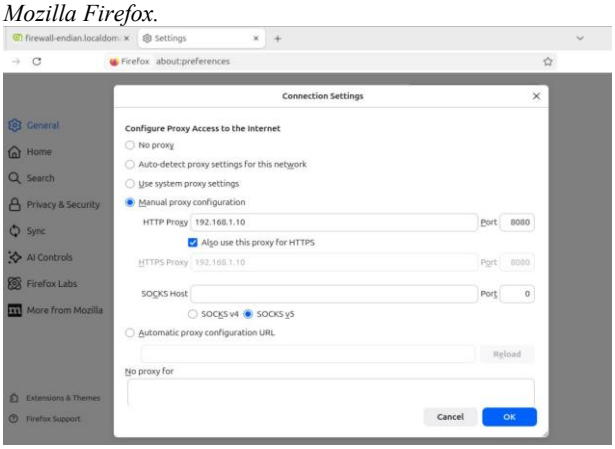
C. Pruebas de funcionamiento y auditoría de tráfico

La fase final consistió en la validación de las reglas desde una estación de trabajo en la zona Verde. Tras configurar el navegador cliente, se realizaron intentos de acceso a los dominios restringidos, obteniendo como resultado un mensaje de "Access Denied" generado por el motor de filtrado de Endian.

Desde la perspectiva del administrador, la efectividad del bloqueo se verificó mediante la revisión de los registros en tiempo real (Live Logs). Esta auditoría permite visualizar el código de estado HTTP 403 (Prohibido) para las peticiones bloqueadas, detallando la IP del cliente y la URL exacta que activó el filtro de seguridad.

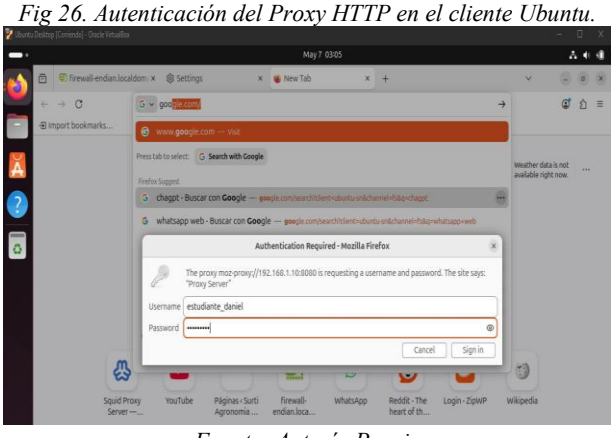
La siguiente imagen muestra que se configuró la sección “Manual proxy configuration” utilizando la dirección IP de la interfaz verde del Firewall (192.168.1.10) y el puerto estándar 8080. Además, se habilitó la opción “Also use this proxy for HTTPS” para garantizar que el tráfico cifrado también sea supervisado y procesado por las políticas de seguridad del sistema.

Fig 25. Configuración manual de Proxy en el navegador Mozilla Firefox.



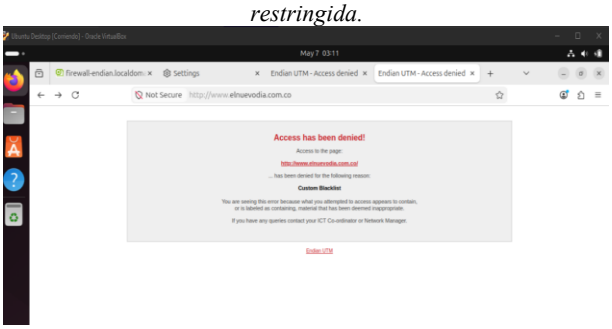
Fuente: Autoría Propia

Fig 26. Autenticación del Proxy HTTP en el cliente Ubuntu.



Fuente: Autoría Propia

Fig 27. Mensaje de bloqueo del Firewall ante una URL restringida.



Fuente: Autoría Propia

Aquí se evidencia el bloqueo correcto al intentar ingresar a www.elnuevodia.com.co.

El sistema Endian UTM intercepta la solicitud y muestra el mensaje "¡Access has been denied!", indicando que el sitio pertenece a la "Custom Blacklist" configurada por el administrador. Esta evidencia confirma el funcionamiento integrado del servicio Proxy, la autenticación de usuarios y el filtro de contenidos aplicado en la red.

4. CONCLUSIONES

Con la creación de una zona DMZ se pueden aislar los servicios críticos del interior de la red, reduciendo de forma importante la superficie de ataque del servidor expuesto a Internet.

En la arquitectura perimetral, el NAT se hace imprescindible para permitir que múltiples hosts internos salgan a internet usando una sola dirección IP pública.

La implementación de una arquitectura segmentada mediante zonas GREEN, ORANGE y RED permitió fortalecer la seguridad perimetral de la infraestructura de la red, generando un mayor control sobre el tráfico entre redes.

Mediante la implementación de reglas inter-zona en Endian Firewall Community fue posible restringir el tráfico y controlar el funcionamiento de políticas de filtrado ICMP dentro de la infraestructura.

El desarrollo de la práctica permite fortalecer habilidades en funcion de la administración de sistemas GNU/Linux - configuración de firewalls orientados a la protección de servicios y segmentación de las redes.

4 REFERENCIAS

[1] Canonical. (2020). Cuentas de usuario Ubuntu 18.04 LTS. Help Ubuntu. https://help.ubuntu.com/stable/ubuntu help/user-accounts.html.es

[2] Debian. (2020). Creación de cuentas Debian 10.04. The Debian Administrator's Handbook. https://www.debian.org/doc/manuals/debian-handbook/sect.creating-accounts.es.html

[3] Endian. (2016). Endian UTM 3.2 manual referencia. http://docs.endian.com/3.2/utm/index.htm

[4] Gaviria Jiménez, J. A. (2024). Fortaleciendo la seguridad en GNU/Linux: Estrategias y mejores prácticas [PDF]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/68716/jagaviriaj.pdf

[5] Gómez, L. J., & Gómez, L. O. D. (2014). Administración de sistemas operativos (pp. 202–208). eLibro. https://elibro.net/es/ereader/unad/62479

[6] Internet Engineering Task Force. (1999). Hypertext Transfer Protocol -- HTTP/1.1 (RFC 2616). https://datatracker.ietf.org/doc/html/rfc2616

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

[8] Ubuntu Documentation Team. (2024). Ubuntu Server Networking. https://ubuntu.com/server/docs/network-configuration