# IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Andrea Biviana Acero Arévalo
e-mail: abaceroa@unadvirtual.edu.co
Andrés Mauricio Rodríguez Camargo
e-mail: amrodriguezcam@unadvirtual.edu.co
Fausto Stip Villa Duque
e-mail: fsvillad@unadvirtual.edu.co
Liceth Milena Mendez Hernández
e-mail: lmmendez@unadvirtual.edu.co

**RESUMEN:** Dentro *de la administración de sistemas GNU/linux es importante la configuración eficiente y segura de interfaces gráficas (GUI) y los entornos de escritorio, dentro de este documento se presenta la implementación de seguridad perimetral utilizando la distribución GNU/Linux Endian en VirtualBox. Se desarrollaron cuatro temáticas: configuración de la instancia con segmentación en zonas Green, Red y Orange; aplicación de reglas NAT para permitir la comunicación entre LAN y WAN, habilitación de servicios HTTP y FTP en la zona DMZ y la implementación proxy HTTP. Dentro de este trabajo se incluye la preparación del entorno, asignación de direcciones IP, pruebas de conectividad y verificación de reglas de firewall permitiendo que en el resultado se evidencie la correcta segmentación y la funcionalidad básica de los servicios, estableciendo la base para una infraestructura segura.*

**PALABRAS CLAVE**: DMZ, Endian, Firewall, NAT, Virtual Box

## INTRODUCCIÓN

La seguridad en redes es un componente crítico en entornos corporativos y académicos ya que dentro de los entornos actuales en la administración de sistemas operativos, la configuración eficiente y segura representa una competencia clave para garantizar la funcionalidad, accesibilidad y escalabilidad en la administración de los entornos dentro de este artículo se realizó la implementación de Endian Firewall este basado en GNU/Linux que permite segmentar la red en zonas con diferentes niveles de acceso y aplicar políticas de seguridad, este también describe la configuración inicial de Endian en VirtualBox, la implementación de NAT y la habilitación de servicios en la zona DMZ, siguiendo los lineamientos para una correcta administración de servicios.

La implementación adecuada de medidas de seguridad en GNU/LINUX no solo es fundamental para proteger los datos y la privacidad de los usuarios sino que también permite garantizar la correcta administración de los servicios como segmentación de las redes, el uso de cortafuegos, la implementación de zonas delimitadas (DMZ)y la adopción de servicios controlados que permiten reducir los ataques y mitigar los riesgos asociados a vulnerabilidades, fallos de configuración y accesos indebidos.

En este sentido la implementación adecuada de medidas de seguridad es crucial para proteger los sistemas y los datos que se gestionen dentro de una organización, dentro de estas medidas se destaca la configuración de NAT, creación de zonas desmilitarizadas DMZ, el uso de un proxy HTTP y la integración de herramientas como Endian Firewall.

El uso de Endian Firewall, una solución de seguridad robusta para entornos GNU/Linux, es otro componente clave en la estrategia de seguridad de redes. Este firewall de código abierto proporciona una serie de características avanzadas, como el filtrado de paquetes, la inspección profunda de paquetes (DPI), y la integración de VPNs y servicios de proxy, lo que fortalece la protección contra amenazas externas. A través de estas herramientas y técnicas, los administradores de sistemas pueden garantizar un entorno seguro para las aplicaciones y servicios críticos, protegiendo tanto la infraestructura como los datos sensibles.

GNU/Linux proporciona diversas herramientas nativas y soluciones especializadas que facilitan la implementación de políticas de seguridad eficientes, tales como el filtrado de tráfico mediante iptables o nftables, la utilización de servicios de proxy para la supervisión y control de la navegación, y la aplicación de mecanismos de autenticación y registro de eventos. Estas herramientas permiten establecer controles preventivos y correctivos frente a amenazas internas y externas, fortaleciendo la postura de seguridad del sistema.

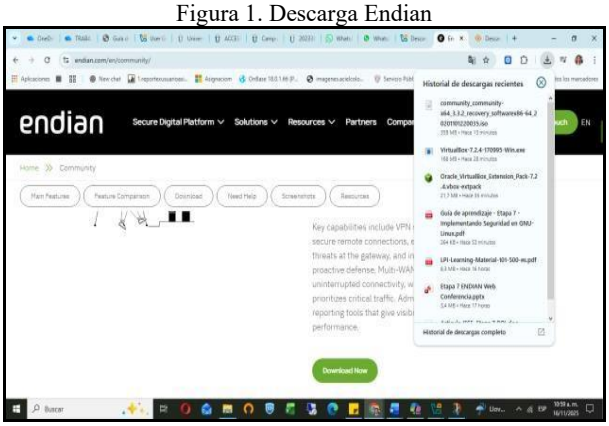
presente artículo tiene como objetivo describir la implementación de medidas de seguridad en sistemas GNU/Linux, con énfasis en la configuración segura de servicios de red y en la aplicación de buenas prácticas orientadas a la protección de los recursos del sistema. A través de un enfoque práctico, se pretende evidenciar cómo una correcta planificación y configuración de los mecanismos de seguridad contribuye a la reducción de riesgos y al fortalecimiento de la seguridad en entornos GNU/Linux utilizados en escenarios reales.

## DESARROLLO

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

Endian Firewall es una solución de seguridad robusta y flexible que permite gestionar redes de forma eficiente si se desea implementar en un entorno de virtualización utilizando VirtualBox, este artículo lo guiará a través de los pasos esenciales para configurarlo correctamente creando una infraestructura de red segmentada y segura. Para iniciar se creó una máquina virtual en VirtualBox donde se ató una imagen ISO de Endian Firewall.

Figura 1. Descarga Endian



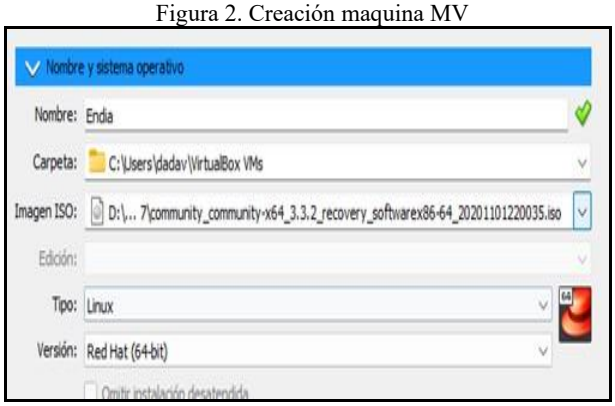

Fuente: Autoría Propia

Esta figura 1 muestra la pagina desde donde se realiza la descarga de la ISO que se atara a la maquina virtual que se va a crear.

Para la implementación dentro de la máquina virtual se configurarán tres adaptadores de red: eth0 (Green), eth1 (Red), eth2 (Orange), donde se asignarán IPs y se verificara la conectividad [5]. Se procedió a definir las siguientes direcciones IP: Zona Green (LAN): 192.168.10.1 / 24, Zona Orange (DMZ): 192.168.20.1 / 24**,** Zona Red (WAN): DHCP

Se procede a crear la maquina virtual por lo que se inicia VirtualBox y hacer clic en "Nuevo" para crear una nueva máquina virtual, se asigna un nombre descriptivo como "Endian" para el tipo de sistema operativo, se procede a atar la imagen iso descargada en el punto anterior seleccionar Linux como sistema operativo y la versión de OS basado en Red Hat y en la versión elegir" Other Linux (64-bit), ya que Endian Firewall está basado en Debian, se asigna RAM: se recomienda al menos 512 MB de RAM para el funcionamiento básico del sistema, aunque se puede asignar más si se tiene recursos disponibles [5].

Figura 2. Creación maquina MV




Fuente: Autoría Propia

Dentro de la figura 2 se muestra los parámetros que se incluyeron dentro de la creación de la maquina virtual basada en Endian con la cual se trabajara.

Figura 3. Configurar máquina virtual

Fuente: Autoría Propia

Esta figura 3 muestra las redes que se crearon dentro de los adaptadores de red, el primero y el segundo para red interna y el tercero en NAT que es el puente que permitirá el acceso a internet, la red Green se configura dentro del cliente, dentro del server se crea la red Orange y dentro de la maquina que se crea se procede a crear el DHCP.

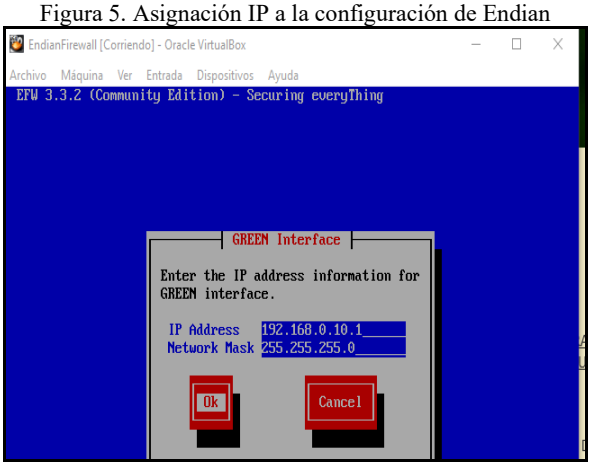
Después de haber configurado la maquina virtual y los segmentos de red se procede a configurar Endian donde se debe seguir el paso a paso de la instalación, en primera instancia la selección del idioma el cual se deberá escoger el inglés, se configura la partición del disco duro, se configura la dirección IP de la interfaz de red teniendo en cuenta la segmentación ya hecha, que permitirá la configuración y administración a través de un navegador web como se muestra en las figuras 4.

Figura 4. Configuración de Endian idioma


Fuente: Autoría Propia

Configuración IP Segmentada:
- Zona Verde: IP 192.168.10.1 / Máscara 255.255.255.0.
- Zona Roja: DHCP.
- Zona Naranja: IP 192.168.20.1 / Máscara 255.255.255.0.

Figura 5. Asignación IP a la configuración de Endian



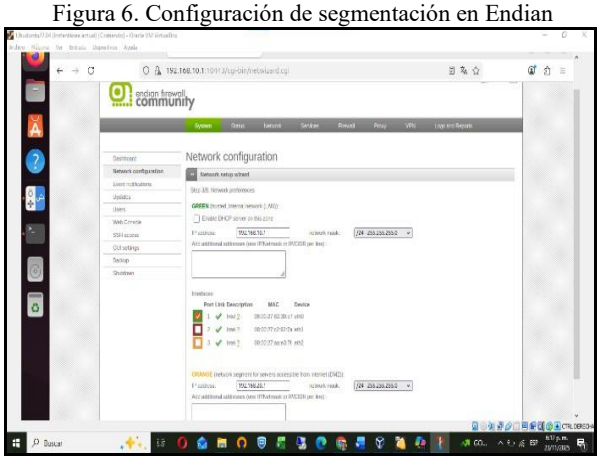

Fuente: Autoría Propia

En la figura 5 se muestra cómo se incluye la configuración de la IP de la zona verde que permitirá la configuración y administración a través de un navegador web desde el desktop del cliente, donde también se configura la partición del disco duro, ya configurada esta parte aparecerá la venta de configuración de Endian de la red que se ha utilizado.

Después de haber configurado Endian en el sistema operativo se podrá acceder al administrador donde aparecerá el asistente de configuración de red, en la pantalla de segmentación en Endian se elegirá el enrutamiento y su correspondiente tipo de enlace que será Ethernet por DHCP así como la configuración de la zona naranja [3].

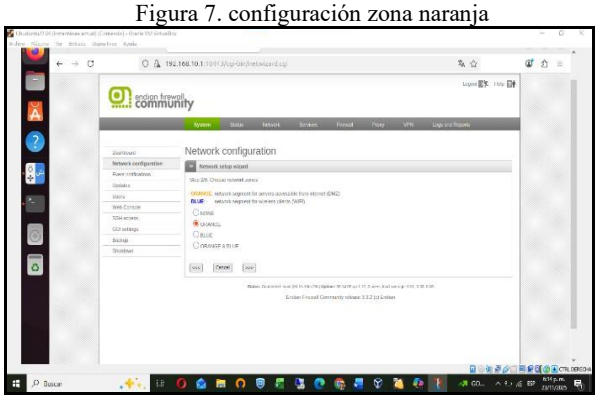
En el asistente de configuración de red se deberá elegir el enrutamiento y su correspondiente tipo de enlace que será ethernet por DHCP, dentro de la figura 6 se puede observar la configuración de la segmentación que se utilizará en Endian, en la figura 7 y 8 se observa la configuración que se realiza para las zonas Green y Orange.

Figura 6. Configuración de segmentación en Endian




Fuente: Autoría Propia

Figura 7. configuración zona naranja




Fuente: Autoría Propia

Figura 8. configuración zona roja


Fuente: Autoría Propia

## 2.2 TEMATICA2: CONFIGURACION NAT

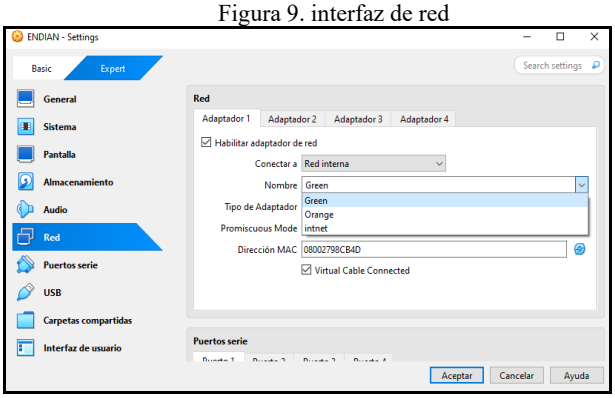
La traducción de direcciones de red (NAT) es un mecanismo esencial para la seguridad perimetral y en la gestión del tráfico de red especialmente en escenarios donde se utiliza direcciones IP privadas para redes internas. NAT permite que múltiples dispositivos accedan a redes externas mediante una dirección IP publica,

modificando el encabezado de los paquetes IP dentro del punto de salida de la red [8].

Endian que es basado en GNU/Linux integra la funcionalidad del NAT como parte de su arquitectura de seguridad, a través de su interfaz de administración web facilita la configuración de NAT sin necesidad de manipular directamente reglas de bajo nivel lo que reduce errores de configuración y mejora la administración del sistema [9]. a configuración de NAT se aplica principalmente para permitir que las zonas internas (GREEN) y desmilitarizadas (ORANGE) accedan a redes externas (RED). Mediante el uso de IP Masquerading, los equipos internos pueden comunicarse con Internet utilizando la dirección IP asignada a la interfaz externa del firewall. La configuración de NAT es esencial para controlar el acceso entre redes internas y externas, permitiendo que los sistemas internos se comuniquen con el mundo exterior sin exponer directamente las direcciones IP internas [8].

Se procedió a realizar la configuración de la interfaz de red dentro de VirtualBox (Green para LAN, Orange para la WAN y Red para el DHCP) dentro de Virtual Box que permita la conexión con el cliente y el servidor como se muestra en la figura 9.

Figura 9. interfaz de red




Fuente: Autoría Propia

Una vez configurado esto se procede a configurar las reglas de NAT (Network Address Translation) con el objetivo de demostrar la capacidad de establecer comunicación entre distintas zonas. Dentro de Endian en el asistente de configuración de red se elegirá el enrutamiento y su correspondiente tipo de enlace que será Ethernet por DHCP [3].se configura la IP de la red Green y Orange y el hostname para que haya conexión con la red WAN.

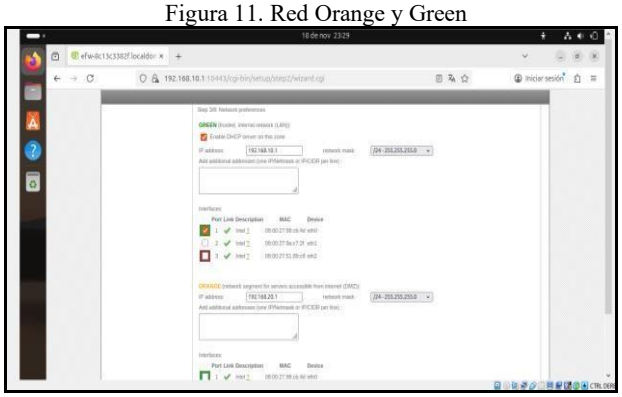
La figura 10 muestra la definición del enrutamiento que se le da al routed y la definición de la zona DHCP que permite la conexión a internet.

Figura10. Enrutamiento de las zonas

Fuente: Autoría Propia

Dentro de la figura 11 se observa que dentro de la zona Green esta habilitado el internet, la IP que se definió anteriormente así como la Orange y el hostname.

Figura 11. Red Orange y Green



Fuente: Autoría Propia

Después de aplicar la configuración, Endian muestra el Dashboard, donde se pueden ver todas las interfaces de red activas. Allí se confirma la dirección IP asignada a cada zona y el estado del enlace, esto permite asegurarse de que las tarjetas quedaron funcionando correctamente. El panel muestra gráficas de tráfico en tiempo real, lo que facilita verificar si las interfaces están enviando y recibiendo datos. Esta información ayuda a validar que la segmentación entre Green, Red y Orange está operativa. Así se confirma que los ajustes aplicados fueron exitosos como muestra la figura 12.

Figura 12. Interfaz tarjeta de red


Fuente: Autoría Propia

Una vez aplicados los parámetros de configuración inicial, el sistema redirige automáticamente al Dashboard de Endian Firewall , para proceder a agregar las reglas se ingresará a la pestaña de firewall y desde esta ventana se configurar las reglas , ingresando en la pestaña NAT estará la opción para empezar a añadir las reglas.es posible verificar en tiempo real el estado operativo del dispositivo y, de manera particular, la información relacionada con las interfaces de red previamente configuradas como se representa en la figura 13.

Figura 13. Menú configuración de reglas


Fuente: Autoría Propia

Ya establecida la configuración del entorno se procede añadir nuevas reglas:

Comunicación entre la LAN y WAN: se implementa regla NAT permitiendo que todos los dispositivos conectados a la zona LAN puedan acceder a la red WAN utilizando la IP pública del firewall [3].

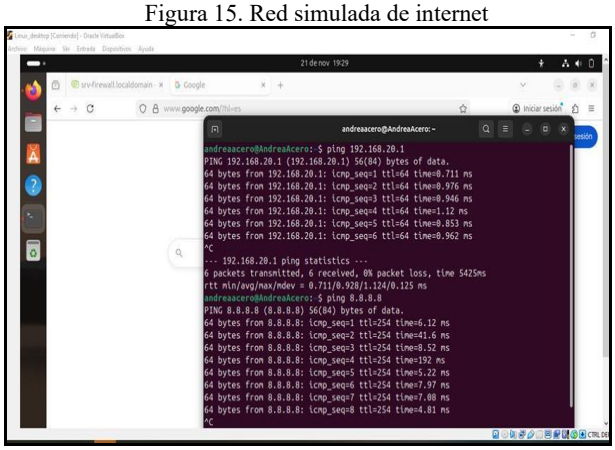
Comunicación DMZ hacia la WAN: para permitir que servicios expuestos en la zona DMZ también tengan acceso a internet. Esta medida permite mantener segmentado los servicios públicos, pero brindando la conectividad necesaria sin comprometer la red LAN [3].

Como se muestra en la figura 14 dentro del administrador se añade la regla y se aplican los cambios para que estos repliquen en el firewall.

Figura 14. Regla de acceso de internet


Fuente: Autoría Propia

Figura 15. Red simulada de internet




Fuente: Autoría Propia

Dentro de la figura 15 se observa que se valida desde la LAN hacia la WAN siendo esta la (red simulada de internet).

Adicional del proceso de realizar la configuración de la regla NAT, se debe agregar una regla de tráfico enrutado de entrada esto para detener el acceso de la WAN a la LAN, mediante el reenvío de puertos (port fordwarding) se debe implementar y verificar el reenvió de puertos creando reglas específicas, se deben crear dos servicios que apuntarán a los puertos web por defecto el 80 en http y el 443 en https según muestra la figura 16 se realiza una configuración de redireccionamiento de puertos

Figura 16. Reenvío de puertos


Fuente: Autoría Propia

Finalmente se realiza prueba de conectividad desde estaciones dentro de las zonas LAN y DMZ, utilizando herramientas básicas como ping, curl y date, lo que permite comprobar tanto la salida a Internet como la correcta configuración de fecha y hora del sistema: ping 8.8.8.8 -c 4 curl ifconfig. que permiten comprobar la operatividad de la red, sino que también permiten detectar posibles errores de configuración en las interfaces o en las reglas de NAT [4][6].

## 2.3 TEMÁTICA 3: SERVICIOS EN DMZ

Una DMZ o zona desmilitarizada es una red perimetral que protege y agrega una capa adicional de seguridad a la red de área local interna de una organización del trafico no confiable, donde su objetivo principal es permitir que una organización acceda a redes no confiables, como el internet, mientras que garantiza que la red privada o LAN permanezca segura. Las organizaciones tienden a almacenar servicios y recursos externos, así como servidores para sistema de dominio DNS, protocolo de trasferencia SFTP, correo, proxy protocolo de voz y los servidores de la web en la DMZ [11].

El principal beneficio que tiene una DMZ es proporcionar una red interna con una capa de seguridad avanzada al restringir el acceso a datos sensibles, actúa como una zona intermedia entre la red interna y externa, facilita un modelo de seguridad de múltiples capas, reduciendo significativamente los puntos de ataque. Un DMZ permite que los visitantes del sitio web obtenga ciertos servicios mientras proporcionan un búfer entre ellos y la red privada dentro de la organización, es un a red abierta pero hay varios enfoques de diseño y arquitectura que lo protegen que pueden estar diseñados desde un enfoque de cortafuegos único hasta uno doble y múltiple [11].

Una red DMZ proporciona un búfer entre internet y la red privada dentro de una organización implementación de una DMZ contribuye a reducir la superficie de ataque al establecer un modelo de defensa en profundidad, en el cual el tráfico proveniente de la red externa es filtrado y controlado antes de alcanzar los sistemas internos.

Es necesario configurar adecuadamente los dispositivos de seguridad, como cortafuegos (firewalls) y reglas de filtrado de paquetes, que gestionan el tráfico entre la DMZ y las redes internas y externas. Se instalo Apache y FTP en la zona Orange y se configuro reglas en el firewall donde puede descargar y abrir la plantilla y copiar su texto y las ilustraciones en la plantilla.

En primer lugar, se descarga la distribución de Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86 [6]. Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

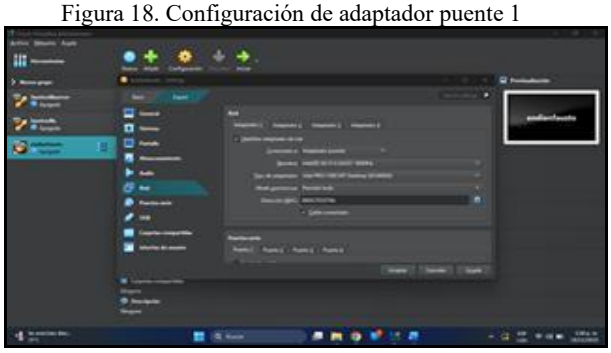
En la figura 17 se muestra la configuración de la maquina virtual que se utilizara para implementar los servicios DMZ en Endian a si como su OS y versión de OS.

Figura 17. Creación de máquina virtual

Fuente: Autoría Propia

Actualmente la virtualización se ha convertido en una tecnología fundamental dentro del ámbito de las redes y la seguridad informática, permitiendo ejecutar múltiples sistemas operativos de manera simultánea sobre un mismo equipo físico, dentro del adaptador 1 de Endian se configuro como adaptador puente (WAN) como lo muestra la figura 18.

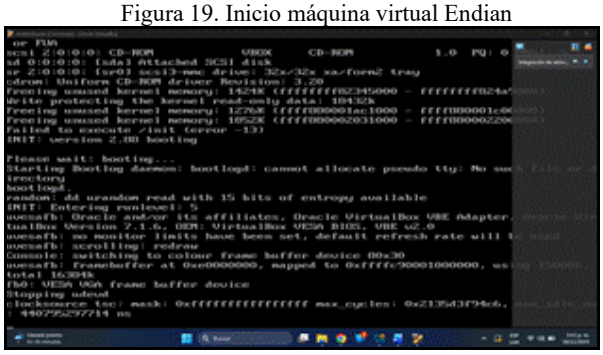
Figura 18. Configuración de adaptador puente 1



Fuente: Autoría Propia

Seguido de haber configurado el adaptador puente se inicia la máquina virtual de Endian donde se constatará que la configuración haya quedado bien según figura 19.

Figura 19. Inicio máquina virtual Endian



Fuente: Autoría Propia

Teniendo en cuenta el producto esperado, se realizó la autenticación de usuario y contraseña en Endian, desde

desktop se accede a Endian por medio de https://192.168.10.1:10443 y se procede a loguearse.

•Se confirmo la configuración de RED (WAN).
•Se confirmo la IP de GREEN y ORANGE
•Se confirmo la configuración de RED en DHCP.
•Se confirmo eth0 para RED.
•Se realizo configuración de port fordwarding en Endian Firewall para permitir el tráfico HTTP (puerto 80) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

Figura 20. Configuración de reglas de puerto 80

Fuente: Autoría Propia

Dentro de la figura 20 se observa la configuración de la regla del puerto 80, Con el fin de permitir el acceso controlado a servicios web, se configuró una regla de firewall en Endian Firewall que autoriza el tráfico entrante a través del puerto 80 (HTTP) hacia un servidor ubicado en la zona ORANGE (DMZ). Esta configuración se realizó siguiendo el principio de mínimo privilegio, permitiendo únicamente el tráfico estrictamente necesario para el funcionamiento del servicio.

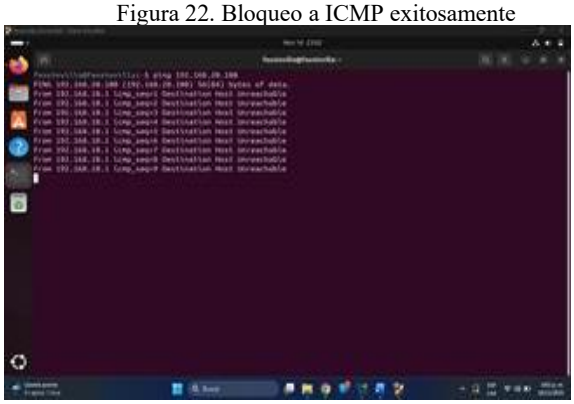
Figura 21. Configuración de reglas de puerto 21

Fuente: Autoría Propia

La configuración de reglas para los puertos permite exponer servicios específicos (FTP y HTTP) alojados en un servidor Ubuntu dentro de la DMZ, garantizando el acceso controlado desde Internet y manteniendo la seguridad de la red interna. Se Aplico la regla de firewall en Endian Firewall para bloquear el tráfico ICMP desde la IP 192.168.10.1 en la interfaz GREEN (DMZ) con acción de denegar el tráfico. La regla está habilitada y aplicada, posterior al bloqueo realizado se actualizan los paquetes en server, se hace la instalación de Apache y FTP en Ubuntu server bajo la configuración de servicios HTTP Y FTP.

Por último, se valida que el ping a la dirección IP de la red DMZ está siendo bloqueado, mostrando "Destination Host Unreachable", lo que indica que la regla para bloquear ICMP está funcionando correctamente Figura 22.

Figura 22. Bloqueo a ICMP exitosamente



Fuente: Autoría Propia

El bloqueo exitoso de ICMP consiste en la implementación de reglas de seguridad que impiden la recepción o envío de estos mensajes, con el objetivo de reducir la superficie de ataque y reforzar la protección de la red.

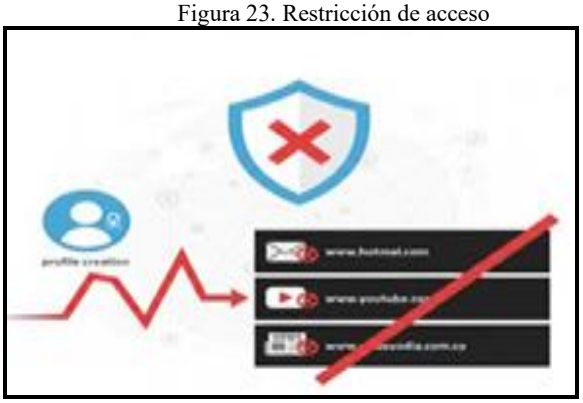
## 2.4 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

El uso de un proxy HTTP constituye una estrategia eficaz para el control, monitoreo y aseguramiento del acceso a internet dentro de una red, la implementación de un Proxy HTTP contribuye a un control más estricto sobre las solicitudes de red, lo que permite filtrar contenidos no deseados y proteger a los usuarios internos de sitios web maliciosos. A diferencia de los proxies transparentes un proxy HTTP no transparente requiere de una configuración explicita dentro de los clientes y permite aplicar mecanismos avanzados de autenticación y control de acceso.

En entornos basados en GNU/Linux la implementación de un proxy HTTP no transparente se realiza comúnmente mediante un servicio Squid una solución ampliamente adoptada por su estabilidad, flexibilidad y capacidad de integración con sistemas de autenticación. Squid permite interceptar solicitudes HTTP/HTTPS, aplicar listas de control de acceso (ACL) y registrar la actividad de los usuarios, lo cual facilita la auditoría y el cumplimiento de políticas institucionales [10].

Mecanismo de Restricción de Acceso Mediante Perfil y Lista Negra: El proceso determina un perfil concreto de usuario, al que se le imponen normas de acceso. Este perfil habilita una lista negra que ha sido configurada para filtrar el tráfico hacia los dominios $hotmail.com$, $youtube.com$ y $elnuevodia.com.co$. Este procedimiento se suele aplicar en un proxy o firewall, y su propósito es interceptar y denegar las peticiones de conexión a esos lugares con el fin de aumentar la productividad y optimizar el empleo del ancho de banda en la red [2].

Figura 23. Restricción de acceso



Fuente: Autoría Propia

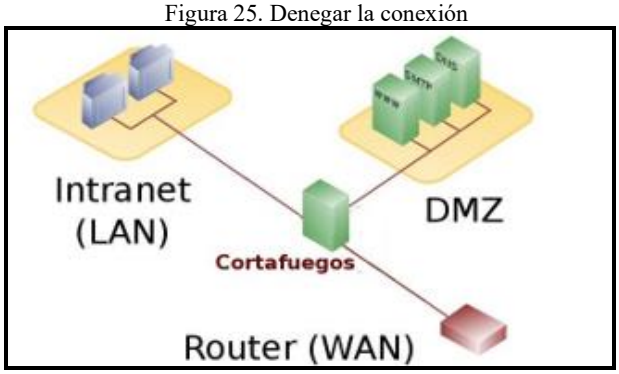
Este paso describe cómo limitar la navegación por usuario utilizando un servidor proxy. La acción comienza al crear una cuenta de usuario única dentro del proxy y asociarla a un grupo específico. Una vez hecho esto se define una política de acceso que establece qué recursos están permitidos o denegados. Finalmente, se vinculan tres elementos clave: el usuario, el perfil de navegación restringido (creado en el punto anterior, con la lista negra de sitios) y la política de autenticación. Esto significa que, para poder navegar el usuario debe ingresar sus credenciales (autenticarse) a través del proxy y solo entonces se aplicarán las reglas de restricción específicas de su perfil como muestra la figura 24.

Figura 24, Diagramas o interfaces genéricas


Fuente: Autoría Propia

Probar desde la LAN a través de un navegador Web el acceso a los portales referenciados en la lista negra, la fase de prueba implica verificar la efectividad de las restricciones de navegación desde un punto de la red de área local (LAN), donde un usuario debe utilizar un navegador web para intentar acceder a cada uno de los sitios que previamente se incluyeron en la lista negra. El resultado esperado y que confirma la correcta implementación de las políticas es que el servidor proxy o firewall debe interceptar y denegar la conexión de forma inmediata, impidiendo la carga del portal y confirmando que la seguridad del perfil está operativa como se muestra en la imagen 25.

Figura 25. Denegar la conexión




Fuente: Autoría Propia

Para implementar un proxy HTTP no transparente con autenticación en Endian se debe activar el servicio, configurarlo para no ser transparente usando un puerto como el 8080, definir las zonas (Green/Orange), habilitar el filtrado web y la autenticación, crear perfiles de usuario y políticas de acceso para controlar que sitios serán permitidos o bloqueados, y luego configurar los navegadores de los clientes para usar IP de Endian y el puerto proxy.

Para restringir el acceso a sitios web, es necesario configurar el proxy HTTP no transparente con políticas de autenticación en Endian Firewall para la distribución de red establecida. Los sitios que se procederán a bloquear son www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.

Para configurar el filtrado de contenido en Endian Firewall, se accede al panel de administración y se selecciona la opción Proxy en el menú superior. Dentro de las configuraciones disponibles, se procede a activar y ajustar los parámetros correspondientes al módulo de Filtrado Web, el cual permite gestionar políticas de acceso a sitios según los criterios predefinidos. Dentro del módulo de Filtrado Web, se genera un nuevo perfil donde se definen los parámetros de bloqueo.

En la configuración del perfil creado, se registran los dominios o URLs a restringir mediante su inclusión en la lista negra. Este mecanismo permite un control sobre el acceso a contenidos no permitidos según las políticas de seguridad establecidas. Para verificar la identidad de los usuarios antes de permitirles conectarse a la web, en el módulo de autenticación del proxy, se registran los usuarios y grupos autorizados, definiendo credenciales únicas para cada uno.

dentro de la políticas de acceso se define una nueva donde se agregaran los permisos de navegación para el grupo de usuarios que se ha establecido, se procede a encender el

proxy que se establece como no transparente después de haber guardado los cambios, donde será necesario configurar de manera manual los navegadores web para redirigir el tráfico HTTP/HTTPS mediante el servicio de proxy que se ha implementado.

## CONCLUSIONES

La implementación de los entornos basados en GNU/Linux representa oportunidad para las organizaciones que quieren tener una optimización en el uso de los recursos tecnológicos, dentro de la realización de estas temáticas se puede evidenciar que GNU/Linux es un sistema adaptable y en constante evolución.

La configuración de la NAT es un componente esencial en la administración de redes ya que es indispensable para la comunicación entre redes internas y externas, la configuración de estas fortalece la eficiencia operativa de las redes pequeñas y medianas constituyendo una habilidad fundamental dentro del campo de la administración de sistemas.

La habilitación controlada de servicios en DMZ representa una de las practicas más efectivas reduciendo riesgos y garantizando la disponibilidad de los servicios que permite la optimización de la gestión del tráfico y resiliencia del sistema ante amenazas.

Implementar un Proxy HTTP no transparente con autenticación permite controlar quién accede a Internet, asociar cada sesión a un usuario específico y aplicar políticas de acceso de forma centralizada. Esto mejora la seguridad, facilita el monitoreo del tráfico y ayuda a gestionar eficientemente los recursos de red.

## REFERENCIAS


[1] Autenticación y Políticas de Acceso en Proxy, Configuración de autenticación de usuario y políticas de acceso en servidor proxy, Proveedor de servicio de imágenes web, 2025.

[2] Asistente de IA, Bloqueo de sitios web (lista negra): Ilustración conceptual de perfil de usuario y bloqueo de sitios web mediante lista negra, imagen generada digitalmente, 2023.

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

[4] Funcionamiento del Bloqueo y Prueba de Acceso (Diagrama de Flujo), Diagrama de flujo conceptual de acceso denegado por filtro de contenido o proxy, Proveedor de servicio de imágenes web, 2025. [En línea]. Disponible en: http://googleusercontent.com/image_collection/image_retrieval/6065008525228921814

[5] Linux Professional Institute, Tema 101: Determinar y configurar los ajustes de hardware. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/

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

[7] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Boston, MA, USA: Pearson, 2011.

[8] P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator (Traditional NAT),” RFC 3022, Internet Engineering Task Force (IETF), Jan. 2001.

[9] Endian S.r.l., Endian Firewall Community Documentation, 2023. [Online]. Available: https://docs.endian.com.

[10] “How to Set Up The HTTPS Proxy,” Endian,2025.[Online].Available:https://help.endian.com/hc/en-us/articles/115006253507-How-to-Set-Up-The-HTTPS-Proxy.

[11]“What Is a DMZ?,” Fortinet. [Online]. Available: https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz. Accessed: Dec. 16, 2025.