# IMPLEMENTACION DE SEGURIDAD PARA LA GESTION DE ZONAS LAN – DMZ -WAN EN VIRTUALIZACIÓN

María del Pilar Martínez Peralta
e-mail: mdmartinezpe@unadvirtual.edu.co
Linda Yineth Sánchez Rodríguez
e-mail: lysanchezrod@undavirtual.edu.co
Enuar Emilio Rosales Salazar
e-mail: eerosaless@unadvirtual.edu.co
Martha Liliana Rojas Ortiz
Email: mlrojasor@unadvirtual.edu.co

**RESUMEN:** *La seguridad en GNU/Linux es un proceso integral que combina configuraciones del sistema, herramientas especializadas y buenas prácticas de administración. Aunque GNU/Linux es reconocido por su robustez y arquitectura segura, su protección depende directamente de una correcta gestión por parte del administrador. La implementación de seguridad comienza con la actualización constante del sistema y la configuración adecuada de permisos, usuarios y grupos. Se complementa con el uso de mecanismos como firewalls (iptables, UFW), sistemas de detección de intrusos (Fail2Ban, Snort), y servicios de auditoría (SELinux, AppArmor). Además, es fundamental asegurar el acceso remoto mediante SSH, aplicar políticas de contraseñas, cifrado de discos y copias de seguridad. Con estas medidas, GNU/Linux puede ofrecer un entorno altamente resistente frente a ataques internos y externos, garantizando la integridad, disponibilidad y confidencialidad de la información.*

**PALABRAS CLAVE**: Firewall UTM, Segmentación de red, Endian Community.

## 1 INTRODUCCIÓN

La seguridad informática se ha convertido en un componente esencial en la administración de sistemas, especialmente en un entorno donde las amenazas digitales evolucionan continuamente. GNU/Linux, conocido por su estabilidad y arquitectura abierta, es una de las plataformas más utilizadas en servidores, infraestructuras críticas y sistemas empresariales. Sin embargo, su seguridad no es automática: requiere una configuración adecuada, monitoreo constante y la implementación de políticas que garanticen el resguardo de la información.

Este artículo aborda las principales estrategias y herramientas necesarias para fortalecer la seguridad en GNU/Linux, desde la gestión de usuarios y permisos hasta el uso de firewalls, servicios de auditoría y mecanismos de protección del sistema. Al comprender y aplicar estas medidas, los administradores pueden construir entornos más confiables, minimizar vulnerabilidades y responder eficazmente ante posibles ataques. Implementar seguridad en GNU/Linux no solo es una práctica recomendada, sino una necesidad para mantener la integridad y disponibilidad de los sistemas en el mundo digital actual.

## 2 INSTALACIÓN ENDIAN

### 2.1 CARACTERÍSTICAS GENERALES

Se descarga la distribución Endian desde la página oficial, luego se procede a crear en la máquina virtual VirtualBox estas configuraciones está en tipo Linux la versión es Oracle Linux como se observará a continuación.

### 2.2 PROCESO DE INSTALACION

Figura 1. Instalación Endian


Fuente: Autoría propia

Se evidencia la configuración de red de los 3 adaptadores en Endian.

Figura 2. detalle Endian

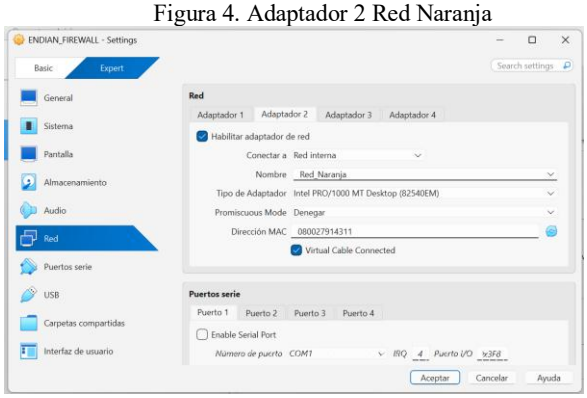

Fuente: Autoría propia

Configuración de adaptadores las cuales se indicarán a continuación.

Figura 3. Adaptador 1 Red verde

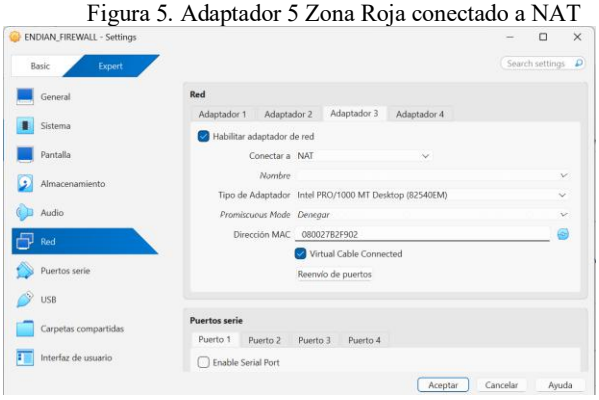

Fuente: Autoría propia

Figura 4. Adaptador 2 Red Naranja




Fuente: Autoría propia

Figura 5. Adaptador 5 Zona Roja conectado a NAT

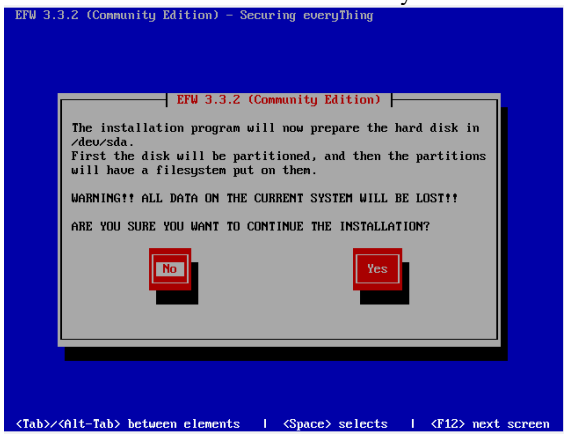



Fuente: Autoría propia

Figura 6. continuidad de Instalación

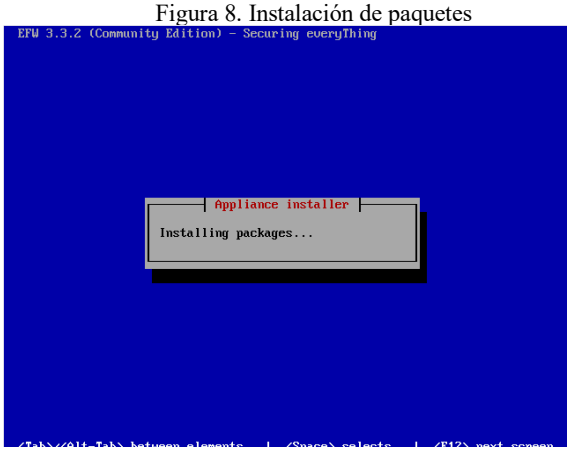

Fuente: Autoría propia

Figura 7. se crea partición para llevar a cabo instalación seleccionamos yes




Fuente: Autoría propia

Figura 8. Instalación de paquetes

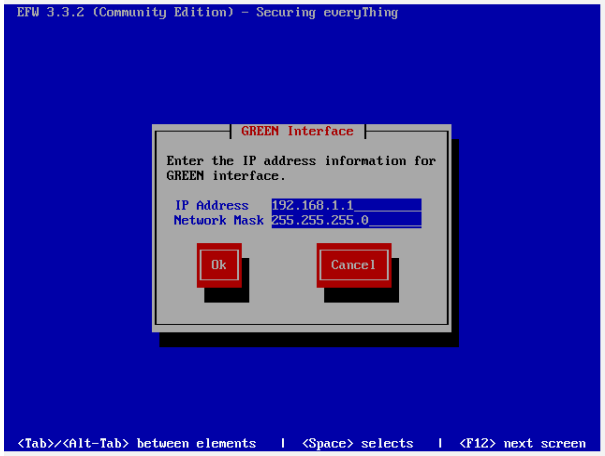



Fuente: Autoría propia

Figura 9. No habilitamos el puerto serial en este caso la selección es “NO” el motivo es porque no se necesita habilitar acceso al firewall de un puerto serial

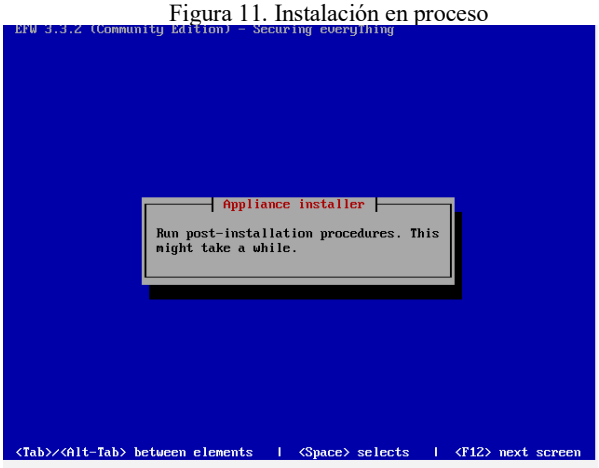

Fuente: Autoría propia

Figura 10. Debemos establecer ip GREEN y la máscara.



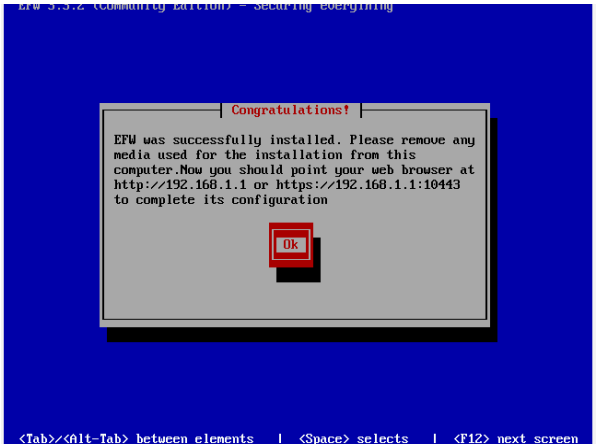

Fuente: Autoría propia

Figura 11. Instalación en proceso



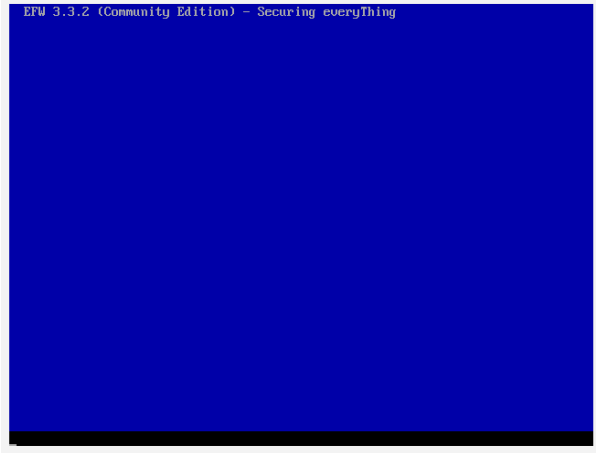

Fuente: Autoría propia

Figura 12. Instalación y configuración inicial en Endian Firewall finalizada.




Fuente: Autoría propia

Figura 13. Procesando

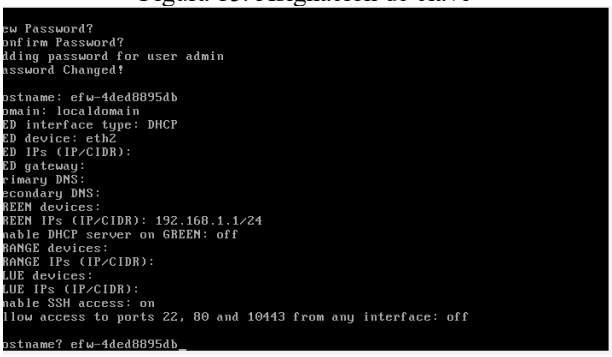



Fuente: Autoría propia

Figura 14. Inicio del sistema seis campos enumerados que nos permiten realizar diferentes funciones

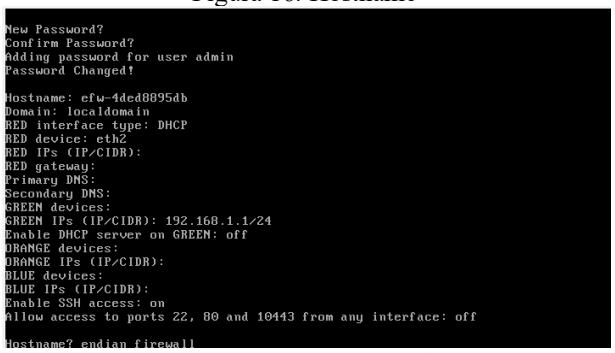

Fuente: Autoría propia

Figura 15. Asignación de clave



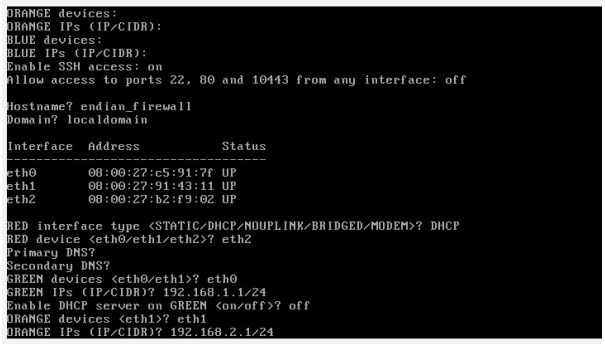

Fuente: Autoría propia

Figura 16. Hostname




Fuente: Autoría propia

Figura 17. Después de realiza las configuraciones se genera la confirmación




Fuente: Autoría propia

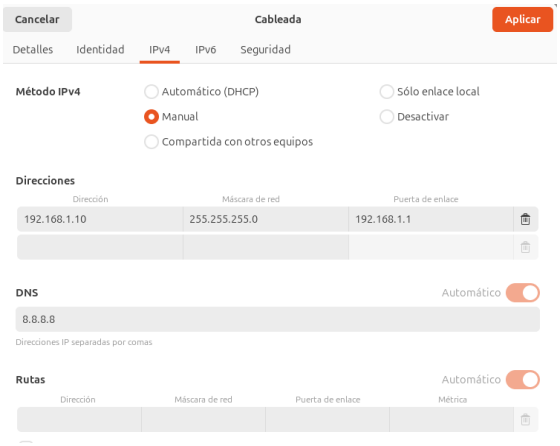
# 3 DESARROLLO TEMÁTICAS

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

La temática desarrollada inicialmente se generó en instalación y configuración de Endian en VirtualBox, se trabajó la segmentación de zonas de seguridad implementado en tres segmentos zona roja, verde y naranja asignando las ip a cada zona, validando comunicación entre sí, se evidencia que firewall controla tráfico y administra como resultado demuestra seguridad y funcionamiento en la red.

La configuración de Ubuntu se evidencia a continuación de IPV4.

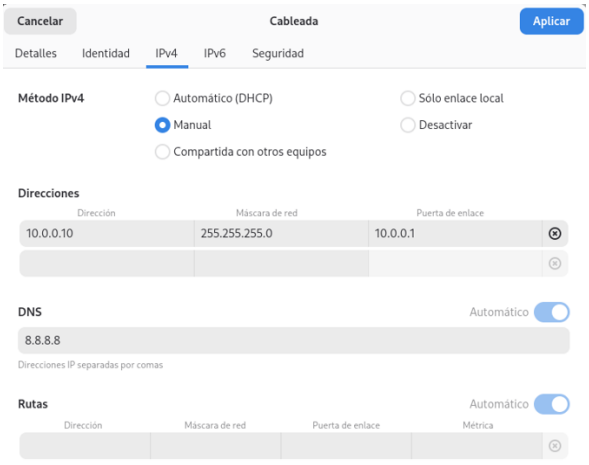
Figura 18. Configuración adaptador 1




Fuente: Autoría propia

Se evidencia la configuración de Debian la IPv4, método manual, dirección, mascara de red, puerta de enlace y DNS

Figura 19. Configuración




Fuente: Autoría propia

Figura 20 Endian

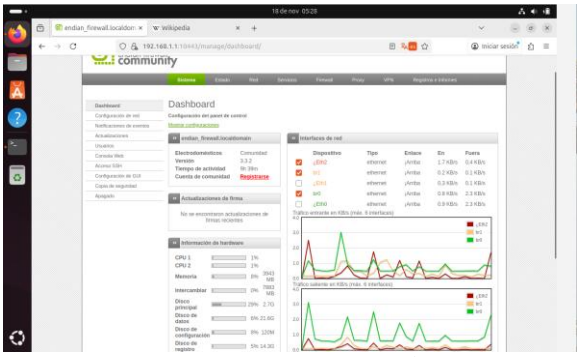

Fuente: Autoría propia

Figura 21 Ingreso a Endian firewall


Fuente: Autoría propia

La configuración demuestra el perfecto funcionamiento en el tráfico como lo es el rendimiento, comportamiento en tiempo real y el estado de las interfaces, la zona roja WAN apunta al proveedor de internet, zona verde LAN acceso completo a internet y la naranja la zona desmilitarizada.

Figura 22. Configuración de reglas de las zonas



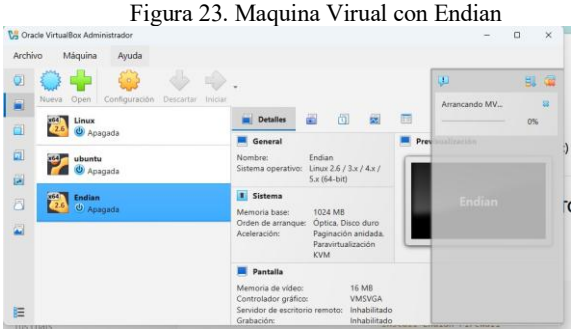

Fuente: Autoría propia

## 3.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La temática se centra en habilitar y comprobar la traducción de direcciones de red (NAT) dentro de Endian Firewall, permitiendo que los equipos de la zona verde (LAN) y la zona naranja (DMZ) puedan acceder hacia la zona roja (Internet/WAN). Esta práctica buscó simular una infraestructura real donde el firewall controla el tráfico entre redes internas y externas, garantizando seguridad y permitiendo únicamente el tráfico autorizado.

Para el desarrollo, se instaló Endian como firewall y se definieron las zonas correspondientes: GREEN (LAN), ORANGE (DMZ) y RED (WAN).

Figura 23. Maquina Virual con Endian

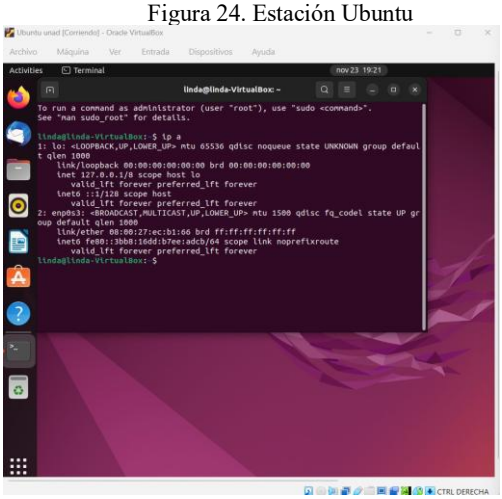



Fuente: Autoría propia

Luego se procedió a configurar las reglas de NAT desde la interfaz de administración, habilitando tanto el SNAT/MASQUERADE para la LAN como el NAT para la DMZ, asegurando que ambas redes internas pudieran salir a Internet utilizando la dirección pública simulada en la RED.

Una vez creadas las reglas, se realizaron pruebas desde una estación Ubuntu ubicada en la zona GREEN. Se configuró la interfaz del cliente con una IP dentro del segmento interior y se estableció como puerta de enlace la IP verde del Endian. Posteriormente, se realizaron pruebas de conectividad mediante comandos como ping, curl y apt update, verificando que el tráfico efectivamente era traducido y enviado a través del firewall hacia la WAN. De igual manera, se probó la conectividad desde un servidor Ubuntu ubicado en la DMZ para validar que esta zona también contara con acceso controlado hacia Internet.

Figura 24. Estación Ubuntu




Fuente: Autoría propia

Los resultados mostraron que la comunicación desde la LAN hacia la WAN se estableció correctamente, confirmando que la regla de NAT estaba funcionando.

En la interfaz de Endian se verificó, dentro del módulo de Reenvío de puertos / NAT, la creación automática de las reglas de traducción según la configuración aplicada. Así mismo, se comprobó la salida a Internet desde la zona DMZ, lo cual validó que ambas reglas de NAT estaban operativas.

## 3.3 TEMÁTICA 3: Permitir servicios de la Zona DMZ para la red.

Como se mencionó al inicio de este artículo, la seguridad informática es un factor determinante para el correcto desarrollo de los procesos internos de una organización. Garantizar la integridad, disponibilidad y confidencialidad de la información permite que los sistemas funcionen adecuadamente y que las operaciones empresariales se realicen sin interrupciones ni vulnerabilidades. En este contexto, el control y la correcta configuración de los servicios expuestos en la zona DMZ se vuelven esenciales para proteger la infraestructura interna y asegurar un flujo seguro de comunicaciones entre la red corporativa y los servicios externos.

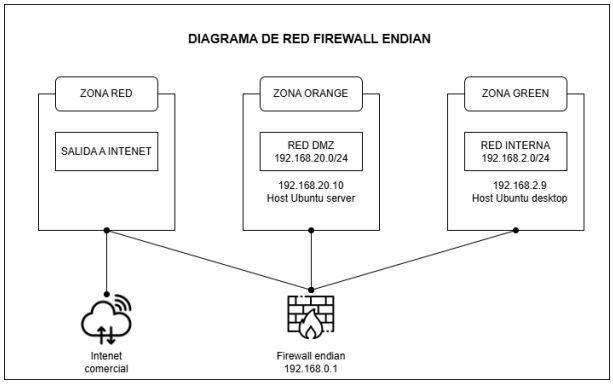
La DMZ (Zona Desmilitarizada) es un segmento de red especialmente diseñado para alojar aplicaciones y servicios que deben ser accesibles desde Internet, tales como servidores web, servicios de correo, DNS públicos o aplicaciones corporativas expuestas. Su propósito es agregar una capa adicional de seguridad que permita aislar los servicios externos de la red interna (Green), evitando que un acceso no autorizado comprometa directamente los recursos críticos de la organización.

Dentro de un esquema de seguridad perimetral, la DMZ funciona como un buffer o zona de contención. Si un atacante logra vulnerar un servicio alojado en la DMZ, su alcance quedará limitado, ya que no podrá acceder de manera directa a la red interna. Esto se logra mediante reglas estrictas de firewall, control de acceso, segmentación de red y políticas de comunicación entre zonas.

**Arquitectura de red con Endian**

A continuación, se presenta la arquitectura utilizada para el ejercicio práctico. Esta estructura permite comprender cómo se distribuyen y gestionan las diferentes zonas de red, así como el rol que cumple cada una dentro del esquema de seguridad implementado.

Figura 25. Arquitectura de red




Fuente: Autoría propia

En la ilustración anterior se evidencia cómo Endian Firewall actúa como el orquestador de la red, realizando funciones de capa 3 del modelo OSI, tales como enrutamiento, filtrado de paquetes y gestión del tráfico interzonal. Gracias a esta estructura es posible definir políticas y reglas específicas entre las distintas zonas configuradas:

Green (LAN interna): red segura y de confianza, donde se ubican las estaciones de trabajo y sistemas internos.

Orange (DMZ): zona semisegura destinada a servicios públicos o expuestos.

Red (WAN/Internet): conexión hacia proveedores externos o redes no confiables.

Blue (Wi-Fi): red inalámbrica, usualmente segmentada para usuarios invitados o dispositivos móviles.

En nuestro caso puntual, se implementó una regla que bloquea que la zona Green realice solicitudes ICMP hacia la DMZ y hacia Internet, reduciendo el riesgo de reconocimiento de red y controlando de manera precisa qué tipo de tráfico puede salir o ingresar a la organización. Esta política contribuye a fortalecer los mecanismos de seguridad interna, minimizando potenciales vectores de ataque.

Además, se habilitó únicamente el tráfico necesario desde la zona DMZ hacia la red WAN, en función de los servicios expuestos. Esto garantiza un enfoque de mínimo privilegio, donde cada flujo cumple un propósito particular y está estrictamente limitado.

**Ampliación adicional sugerida**

La correcta administración de la DMZ permite implementar servicios como:

NAT estático (1:1): para publicar servidores con IP privada hacia Internet.

Port Forwarding: habilitar puertos específicos para servicios como HTTP, HTTPS, SMTP o SSH.

Monitoreo del tráfico: mediante logs, IDS/IPS y filtrado avanzado.

Control de aplicaciones: permitiendo o bloqueando protocolos según su criticidad.

Asimismo, una mala configuración de la DMZ puede generar riesgos como:

Exposición total de servicios internos.

Puertos abiertos innecesarios.

Falta de inspección profunda de paquetes (DPI).

Carencia de segmentación adecuada.

Por este motivo, Endian proporciona una interfaz centralizada que facilita la gestión de reglas, inspección de tráfico y protección perimetral, haciendo posible mantener una arquitectura robusta, escalable y segura.

Tabla 1. Reglas firewall

| Zona origen | Zona destino | Protocolo | Acción | Descripción |
|---|---|---|---|---|
| Green | WAN | HTTP/HTTPS | Permit | Navegación general |
| Orange | WAN | HTTP | Permit | Publicación de servidor web |
| Green | Orange | ICMP | Deny | Restricción de ping a DMZ |

Fuente: Autoría propia

## 3.4 TEMÁTICA 5: Implementación de un Proxy HTTP no transparente con autenticación

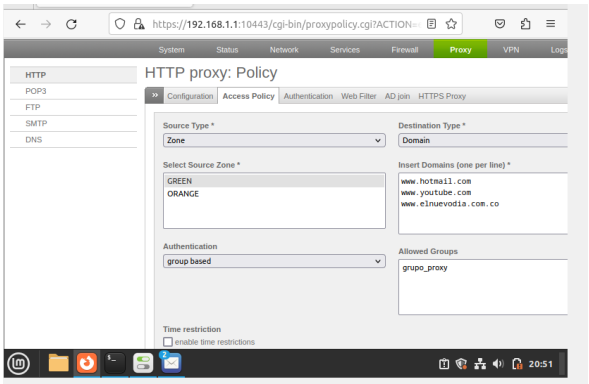
En esta práctica se implementó un mecanismo de control de navegación en el Endian Firewall mediante un proxy HTTP operando en modo no transparente, lo cual exige que cada cliente de la red se configure manualmente para usar el proxy, y además permite exigir autenticación de usuario antes de permitir navegación.

El objetivo principal fue establecer políticas de acceso basadas en credenciales y restricciones de contenido, simulando un escenario real de una organización en el que se controla el uso de Internet para asegurar productividad y seguridad.

Primero, se habilitó el servicio Proxy Web en Endian y se configuró en modo no transparente. Posteriormente, se creó un perfil de filtrado que incluye una lista negra de sitios a bloquear considerados recreativos o no permitidos dentro del entorno controlado:

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

Figura 26. Configuración del proxy




Fuente: Autoía propia

Además, se creó un usuario y su correspondiente grupo de acceso restringido, configurando autenticación obligatoria para navegación web. Luego, se aplicó una política de acceso que vincula el usuario con el perfil de filtrado previamente creado. Con esto, únicamente usuarios autenticados y autorizados pueden navegar, y aun así respetando las restricciones.

Finalmente, desde un equipo en la zona LAN, se configuró el navegador para usar el proxy y se realizó la validación práctica: al intentar ingresar a los sitios listados, el acceso fue denegado, mostrando la página de bloqueo del firewall, confirmando que las políticas funcionan correctamente.

### 3.4.1 CONCLUSIONES.

La implementación de GNU Linux Endian en VirtualBox se genera la práctica de arquitectura en la segmentación de redes, en base a ello los roles lo cual genera la importancia de firewall en seguridad perimetral en las zonas roja WAN, Verde LAN y Naranja DMZ, diseñando la red de aislamiento, tráfico y la protección, en la temática 1 se genera asignación de adaptadores, acceso, administración, pruebas de conectividad, en este proceso se genera segmentación, interfaces, reglas de tráfico, seguridad toda esta implementación fortalece la comprensión de una infraestructura de red.

La configuración de las reglas de NAT en Endian Firewall permitió validar exitosamente la traducción de direcciones de red y el enrutamiento del tráfico entre las zonas definidas, evidenciando una comunicación efectiva desde la zona LAN hacia la WAN y desde la zona DMZ hacia Internet. Se comprobó que las reglas de reenvío de puertos funcionaron correctamente, garantizando que los servicios publicados desde la DMZ fueran accesibles de manera controlada desde redes externas.

La implementación de la zona DMZ en Endian permitió separar los servicios expuestos de la red interna, reduciendo la superficie de ataque y fortaleciendo la seguridad perimetral. La configuración de reglas específicas, como la habilitación de HTTP/FTP y el bloqueo de ICMP, demostró un control efectivo del tráfico entre zonas. Este ejercicio validó la importancia de la segmentación y de aplicar políticas de mínimo privilegio para mantener una infraestructura más segura y estable.

La implementación del proxy HTTP no transparente en Endian permitió controlar de manera efectiva el acceso a Internet mediante autenticación de usuarios y la aplicación de listas negras. La configuración del perfil de filtrado y la validación desde un equipo en la LAN demostraron que solo los usuarios autorizados pueden navegar y que los sitios restringidos son bloqueados correctamente. Este proceso evidenció cómo el uso de políticas de acceso y filtrado contribuye a mejorar la seguridad, la administración del tráfico y el cumplimiento de normas dentro de la red.

## 4 REFERENCIAS


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

[2] Canonical. (2023). Guía del Ubuntu Desktop 20.04 LTS. https://help.ubuntu.com/20.04/ubuntu-help/index.html

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

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

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

[6] 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