IMPLEMENTANDO SEGURIDAD EN GNU/LINUX EJERCICIO GRUPAL

Andrea Rodríguez Ospina
e-mail: arodriguezosp@unadvirtual.edu.co
David Fernando Acevedo
e-mail: dafeacevedo@utp.edu.co
Ervin Andrés Del Rio Agudelo
e-mail: eadelrioa@unadvirtual.edu.co
Mariluz Correa González
e-mail: marycorreagonza@gmail.com
Yeimi Alexandra Hernández Ruiz
e-mail: yahernandezru@unadvirtual.edu.co

RESUMEN: *El presente artículo describe la implementación de una arquitectura de red perimetral segura y funcional utilizando GNU/Linux Endian Firewall en un entorno virtualizado mediante VirtualBox. El procedimiento metodológico se centró en la segmentación de la red en tres zonas críticas (Verde/LAN, Roja/WAN y Naranja/DMZ) y la configuración de la Traducción de Direcciones de Red (NAT) para asegurar la conectividad saliente. Adicionalmente, se establecieron políticas de seguridad, habilitando controladamente servicios esenciales como HTTP y FTP hacia la DMZ, y aplicando el bloqueo de tráfico ICMP para minimizar la superficie de ataque. Se finalizó con la integración de Squid como Proxy HTTP no transparente, implementando autenticación por usuario y listas negras para control de contenido. Los resultados validaron la segmentación efectiva, la conectividad y el control preciso del tráfico. Esta implementación confirma la viabilidad de un sistema robusto, eficiente y de bajo costo, cumpliendo los requerimientos de gestión y seguridad del tráfico en entornos organizacionales*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Proxy HTTP no transparente.

1 INTRODUCCIÓN

En el ámbito de la administración de redes, garantizar la seguridad y el control del tráfico es un desafío constante para las organizaciones. En este sentido, el uso de soluciones como GNU/Linux Endian y Squid resulta clave para implementar infraestructuras de red robustas y seguras. Este proyecto aborda distintas temáticas relacionadas con la configuración de redes, comenzando con la implementación de GNU/Linux Endian en un entorno virtualizado mediante VirtualBox, estructurando la red en tres zonas: Verde (LAN), Roja (WAN) y Naranja (DMZ). Posteriormente, se configura el NAT (Network Address Translation) para permitir la comunicación de la LAN y la DMZ con la WAN, seguido de la habilitación y restricción de servicios específicos como HTTP y FTP en la zona DMZ. Asimismo, se establecen políticas de acceso y reglas para permitir o denegar tráfico entre zonas específicas y validar el correcto funcionamiento de las configuraciones. Finalmente, utilizando Squid como proxy HTTP no transparente, se incluye un sistema de listas negras y autenticación basada en usuarios, que garantiza el acceso controlado a Internet, consolidando así un entorno de red funcional, eficiente y seguro para organizaciones.

2.DESARROLLO DE TEMÁTICAS COLABORATIVAS Y DOCUMENTACIÓN DE RESULTADOS FASE DE REVISIÓN

A partir de la instalación y configuración del Endian Firewall cada integrante debía realizar una temática donde se trabajarían con reglas para denegar o partir accesos entre las diferentes zonas configuradas, a continuación, se documentarán las pruebas y resultados obtenidos para cada una.

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

El objetivo es instalar GNU/Linux Endian Firewall en VirtualBox y configurarlo para que tenga tres zonas de red:

Zona Verde (LAN): Red interna donde estarán los equipos locales.

Zona Roja (WAN): Conexión a Internet.

Zona Naranja (DMZ): Donde se ubican servidores expuestos.

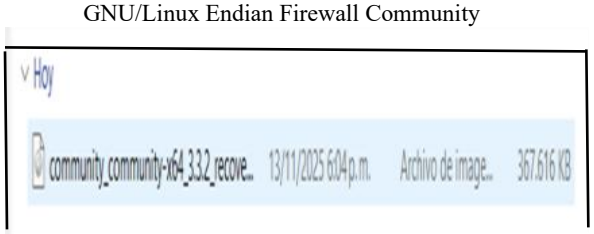
Iniciamos ingresando a la página web oficial para obtener la imagen del software GNU/Linux Endian Firewall Community, el cual es la solución de código abierto utilizado para implementar la arquitectura de seguridad

Figura 1. Página de descarga del software Endian Firewall Community.

Fuente: Elaboración propia

Validamos la imagen ISO descargada del sistema operativo GNU/Linux Endian Firewall Community, indispensable para iniciar la instalación en el entorno de virtualización VirtualBox

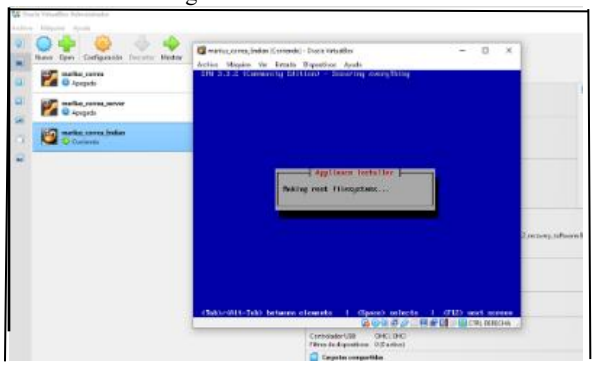
Figura 2. Archivo de imagen ISO del sistema operativo GNU/Linux Endian Firewall Community



. Fuente: Elaboración propia

Revisamos el proceso de configuración inicial del firewall, donde se realiza la asignación de las interfaces de red a las tres zonas de seguridad críticas (Verde/LAN, Roja/WAN y Naranja/DMZ)

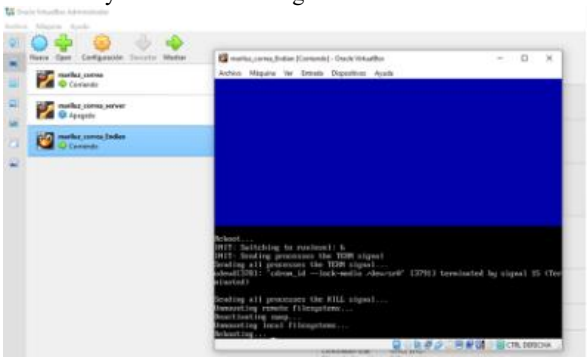
Figura 3. Asignación de zonas de red (Verde, Roja y Naranja) durante la configuración inicial del Endian Firewall.



Fuente: Elaboración propia.

Se hace la comprobación posterior a la configuración inicial, confirmando que las interfaces de red tienen las direcciones IP correctas y están asignadas a sus respectivas zonas de seguridad (Verde, Roja y Naranja)

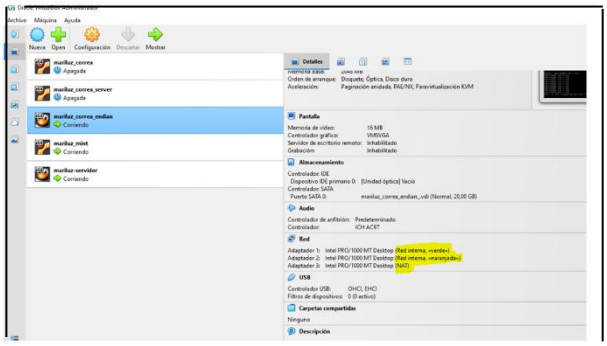
Figura 4. Verificación de la configuración de interfaces de red y direcciones IP asignadas a las tres zonas



Fuente: Elaboración propia.

Se valida la configuración de las tarjetas de red virtuales dentro de VirtualBox, asegurando que el Endian Firewall pueda interactuar correctamente con las redes simuladas para la LAN, WAN y DMZ, cumpliendo con el requisito de virtualización

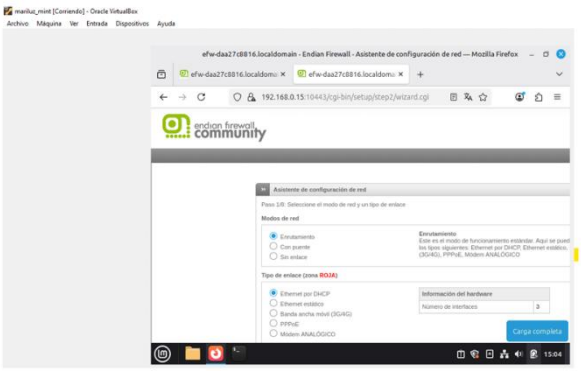
Figura 5. Configuración de interfaces de red de Endian Firewall en entorno VirtualBox



Fuente: Elaboración propia

Se visualiza la arquitectura de red implementada, mostrando la interconexión lógica de las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ) controladas por el Endian Firewall

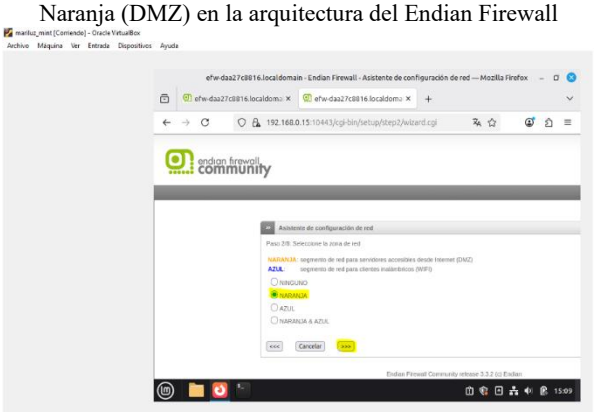
Figura 6. Diagrama conceptual de la configuración de red y zonas de seguridad del Endian Firewall



Fuente: Elaboración propia

Se realiza la configuración del segmento de red y las direcciones IP asociadas específicamente a la Zona Naranja (DMZ), el área designada para alojar servidores expuestos de manera controlada

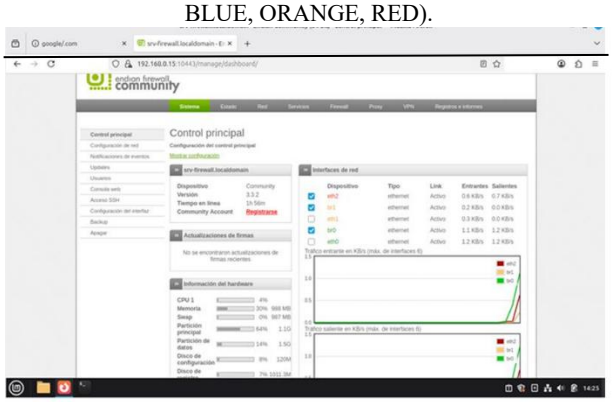
Figura 7. Configuración del segmento de red y la Zona Naranja (DMZ) en la arquitectura del Endian Firewall



Fuente: Elaboración propia

Revisamos la interfaz de administración del Endian Firewall donde se visualiza la correcta asignación de las interfaces virtuales o físicas a las zonas de seguridad (GREEN, ORANGE, RED)

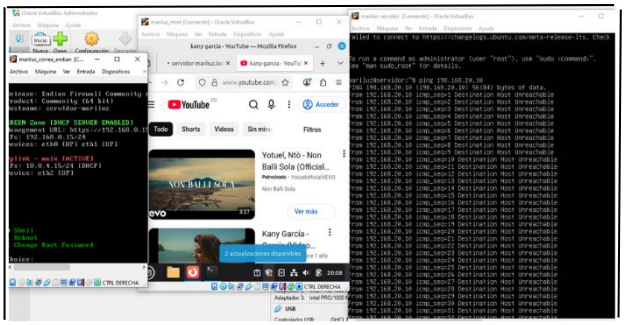
Figura 8. Interfaz de configuración de red del Endian Firewall mostrando la asignación de interfaces y zonas (GREEN, BLUE, ORANGE, RED).



Fuente: Elaboración propia.

Se valida la configuración completa y funcionamiento de las configuraciones realizadas y navegación

Figura 9. Vista de la arquitectura de red en Endian Firewall: visualización de las zonas de seguridad (GREEN, ORANGE, RED) y los servicios asociados



Fuente: Elaboración propia.

B. TEMÁTICA 2: CONFIGURACIÓN NAT.

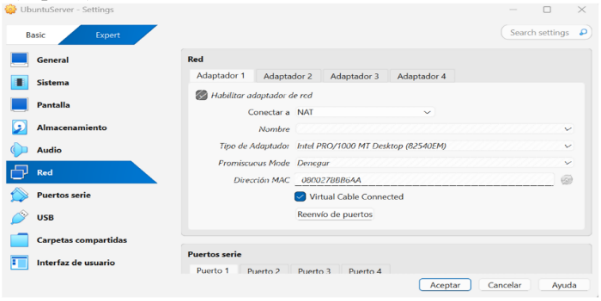
En esta temática se configuró NAT en un servidor Ubuntu para permitir que la LAN accediera a Internet a través de la red NAT de VirtualBox. El servidor actuó como punto intermedio entre la red interna (donde también estaba conectado un Ubuntu desktop) y la red externa simulada. Primero se habilitó el reenvío de paquetes IPv4, indispensable para que el servidor pudiera funcionar como router entre ambas interfaces. Luego se creó una regla NAT tipo masquerade para la red interna y, tras aplicarla, se verificó en la tabla NAT que estuviera cargada correctamente.

La prueba de conectividad se realizó desde el Ubuntu desktop, enviando un ping a 8.8.8.8 (DNS público de Google). Esta prueba confirmó que el tráfico del desktop estaba saliendo a internet a través del servidor y que la regla NAT funcionaba como se esperaba.

Además, se creó una segunda regla para una DMZ simulada, cumpliendo con el requisito de demostrar la configuración NAT para otro segmento de red. Con esto se cumplieron ambos objetivos: habilitar la comunicación LAN–WAN y demostrar la configuración de NAT aplicada a una DMZ.

Para ello se configura la interfaz que simula la conexión a Internet (WAN, enp0s3) del servidor Ubuntu se configura en VirtualBox utilizando la opción NAT, esencial para la conectividad saliente

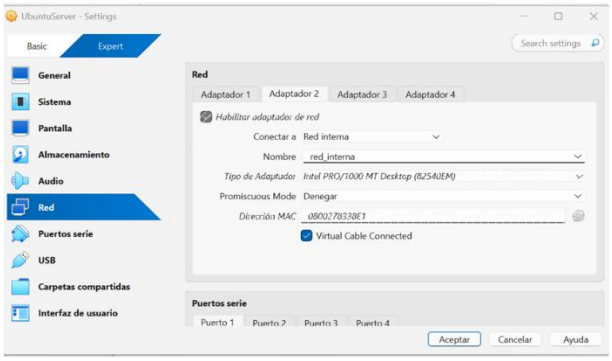
Figura 10. Configuración de la interfaz de red WAN (enp0s3) del Servidor Ubuntu utilizando NAT en VirtualBox



Fuente: Elaboración propia.

Se configura la interfaz interna (LAN, enp0s8) del servidor Ubuntu, en modo Red Interna en VirtualBox para comunicarse con el cliente LAN.

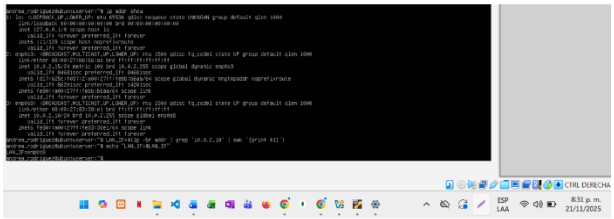
Figura 11. Configuración de la interfaz de red LAN (enp0s8) del Servidor Ubuntu utilizando la opción de Red Interna en VirtualBox.



Fuente: Elaboración propia.

Se confirma que las interfaces de red (WAN y LAN) del Servidor Ubuntu tienen las direcciones IP asignadas correctamente antes de implementar el enrutamiento.

Figura 12. Verificación de las interfaces de red (enp0s3 y enp0s8) y sus direcciones IP en el Servidor Ubuntu.



Fuente: Elaboración propia.

Se habilita el reenvío de paquetes IPv4, lo cual es indispensable para que el servidor actúe como router y permita el flujo de tráfico entre la red interna (LAN) y la externa (WAN)

Figura 13. Habilitación del reenvío de paquetes IP (net.ipv4.ip_forward=1) para permitir el enrutamiento entre zonas de red.

Fuente: Elaboración propia.

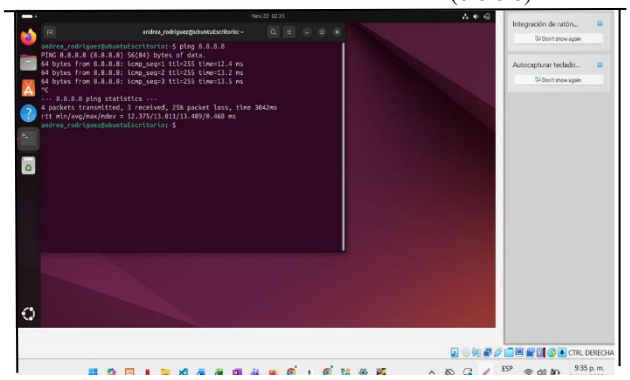
Se aplica regla NAT tipo Masquerade utilizando iptables en el servidor Ubuntu, la cual traduce las direcciones IP privadas de la LAN a la dirección pública del servidor para permitirles acceder a Internet

Figura 14. Aplicación de la regla NAT Masquerade con iptables para permitir la comunicación de la red LAN hacia la WAN.

Fuente: Elaboración propia.

Se valida en pruebas el resultado exitoso del ping desde el cliente de la LAN hacia el DNS público 8.8.8.8, validando que la configuración NAT funciona según lo previsto y que el tráfico interno puede salir a Internet

Figura 15. Comprobación de la conectividad (ping) desde el cliente de la red LAN hacia Internet (8.8.8.8).



Fuente: Elaboración propia.

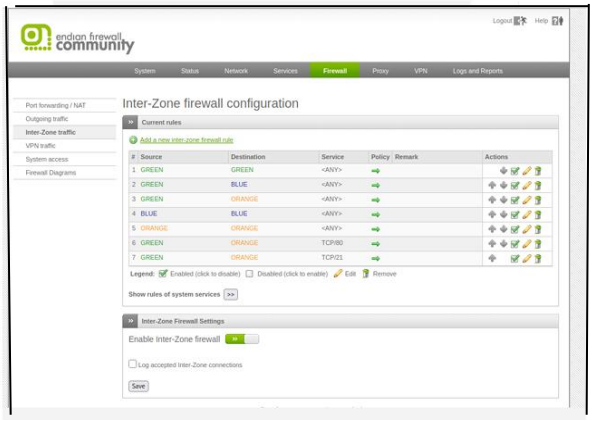
C. TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

La presente sección documenta los resultados obtenidos en el marco de la Temática 3: Permitir servicios de la Zona DMZ para la red, la cual conformó la parte colaborativa del trabajo. La implementación se centró en el desarrollo de una arquitectura de seguridad perimetral segmentada mediante el firewall Endian Firewall Community, estableciendo la conectividad y el control de tráfico entre la Zona Verde (LAN) y la Zona Naranja (DMZ).

Para la validación de la Temática, se configuró el servidor DMZ {192.168.20.10) y se procedió a la activación de los servicios HTTP (Puerto 80) y FTP (Puerto 21). Los resultados se presentan mediante la verificación de la operatividad de los servicios esenciales a través de las reglas de Port Forwarding (NAT) aplicadas en el Endian, y se complementan con la comprobación de la política de seguridad implementada para la denegación del tráfico ICMP (ping). Las evidencias subsiguientes confirman el cumplimiento funcional y de seguridad de la infraestructura implementada.

Se configuro la regla de firewall en Endian para permitir selectivamente el tráfico desde la LAN hacia la DMZ, restringiendo el acceso únicamente a los puertos 80 (HTTP) y 21 (FTP), garantizando el principio de mínimo privilegio.

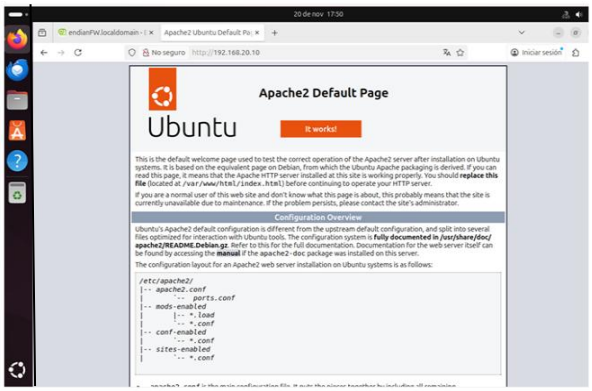
Figura 16. Creación de reglas de firewall en Endian para permitir el tráfico desde la Zona Verde (LAN) hacia la Zona Naranja (DMZ) únicamente por los puertos 80 (HTTP) y 21 (FTP).



Fuente: Elaboración propia.

Se confirma la operatividad del servicio HTTP (Puerto 80) en el servidor DMZ, demostrando que la regla de firewall creada permite la conexión exitosa desde la LAN a la DMZ

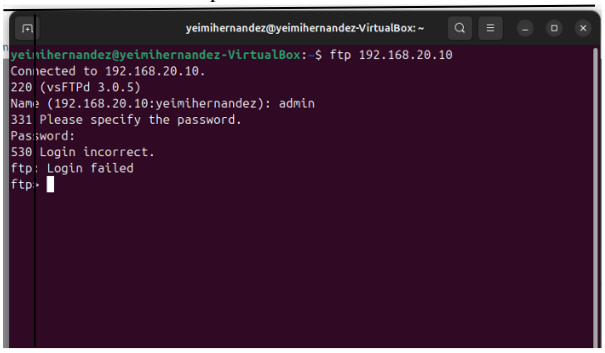
Figura 17. Evidencia de la conexión remota exitosa al Servidor Ubuntu mediante el puerto HTTP (80).



Fuente: Elaboración propia.

Se confirma la operatividad del servicio FTP (Puerto 21), verificando que las reglas de Port Forwarding y firewall permiten el acceso controlado desde la Zona Verde hacia el servidor de la DMZ

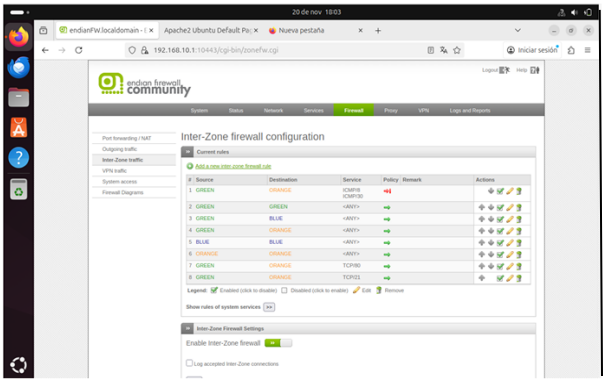
Figura 18. Evidencia de conectividad exitosa desde la Zona Verde hacia la Zona Naranja (DMZ) utilizando el puerto 21, correspondiente al servicio FTP.



Fuente: Elaboración propia.

Se configura la política de seguridad en el Endian para denegar explícitamente el tráfico ICMP (ping) entre la LAN y la DMZ, una medida crucial para minimizar el reconocimiento y la superficie de ataque.

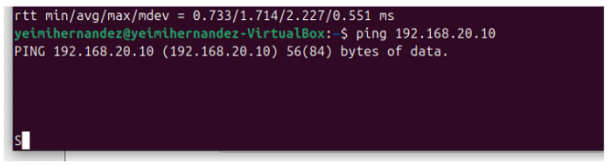
Figura 19. Regla de seguridad implementada en Endian Firewall para bloquear peticiones ICMP (Ping) desde la Zona Verde (LAN) hacia la Zona Naranja (DMZ).



Fuente: Elaboración propia.

Posterior a ello se evidencia el resultado de la prueba de conectividad fallida (Timeout), lo cual valida la efectividad de la regla de bloqueo de tráfico ICMP configurada en el firewall

Figura 20. Prueba de conectividad fallida (Timeout) desde la Zona Verde hacia la Zona Naranja (DMZ), validando la regla de bloqueo ICMP



Fuente: Elaboración propia.

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

En esta temática se aborda la configuración de reglas en Endian Firewall para controlar el tráfico entre las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). El objetivo es permitir únicamente los servicios necesarios y bloquear todo flujo no autorizado, aplicando segmentación y principios de mínimo privilegio.

Para la comunicación entre la zona Verde y la DMZ se habilitaron reglas que permiten los protocolos HTTP y FTP, permitiendo que los usuarios de la LAN accedan al servidor web y al servidor FTP ubicados en la zona Naranja. Estas configuraciones garantizan que los servicios internos funcionen sin exponer innecesariamente la red local.

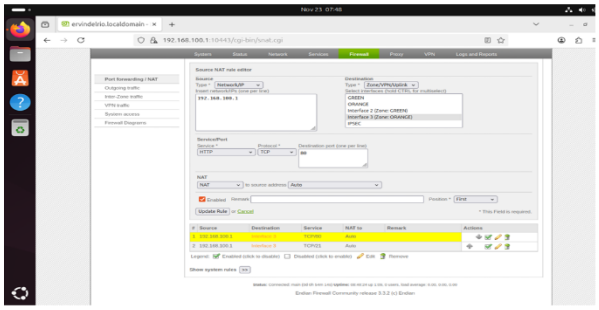
También se establecieron políticas que permiten el acceso desde Internet hacia la DMZ únicamente para los servicios publicados. Esto evita que la LAN quede expuesta directamente a solicitudes externas, manteniendo a la DMZ como zona controlada para la publicación de aplicaciones y servicios.

Una vez configuradas las reglas, se verifico el tráfico entre zonas mediante el módulo de Trafico asegurando que las políticas aplicadas permitieran únicamente el transito autorizado y que no existieran conflictos entre reglas. Las pruebas realizadas desde la LAN, la DMZ y la WAN confirmaron el funcionamiento correcto del acceso HTTP y FTP, tanto hacia internos como hacia servicios externos, validando la efectividad de la configuración del firewall.

En conjunto la implementación de estas reglas fortalece la seguridad perimetral, permitiendo el control preciso del tráfico entre segmentos críticos de la red y garantizando una operación segura de los servicios publicados en la DMZ, a continuación, se relatan las configuraciones y pruebas realizadas.

Se configura la regla de firewall que permite la comunicación específica del servicio FTP (Puerto 21) desde la red interna (LAN) hacia el servidor en la DMZ, asegurando el acceso interno a servicios publicados.

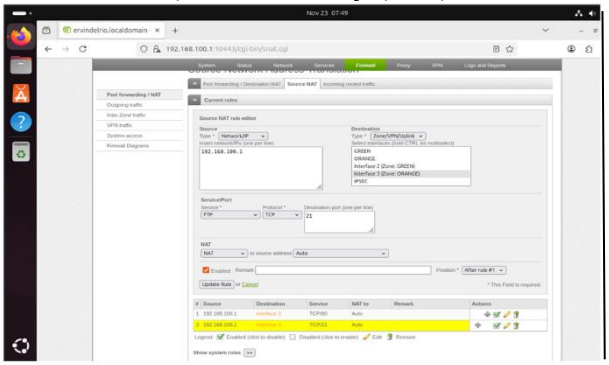
Figura 21. Configuración de la regla de firewall en Endian para permitir el tráfico FTP (Puerto 21) desde la Zona Verde (LAN) hacia la Zona Naranja (DMZ).



Fuente: Elaboración propia.

Se crea regla de acceso clave que permite el tráfico entrante de Internet (WAN/Roja) hacia el servicio FTP (Puerto 21) en la DMZ, garantizando que los servicios publicados sean accesibles externamente bajo control

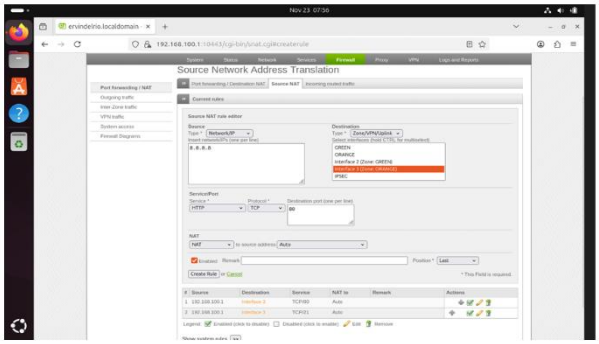
Figura 22. Configuración de la regla de tráfico de entrada en Endian Firewall para permitir el acceso al servicio FTP (Puerto 21) en la Zona Naranja (DMZ).



Fuente: Elaboración propia.

Se configura la regla NAT necesaria para que los servidores alojados en la DMZ puedan iniciar comunicaciones salientes hacia Internet (Zona Roja/WAN), vital para actualizaciones y operaciones de servicio

Figura 23. Configuración de la regla NAT para permitir la comunicación del tráfico saliente de la Zona (DMZ) hacia la Zona (Internet).



Fuente: Elaboración propia.

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

En este trabajo se explica como se hizo la implementación de un Proxy HTTP no transparente usando Squid para controlar la navegación en una red local. Primero, se instaló Squid en un servidor GNU/Linux y se configuraron las reglas básicas en el archivo squid.conf. Al principio, me confundí con la sintaxis de algunas reglas y tuve que buscar ejemplos en internet. Se creo una lista negra con sitios como www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, pero al principio no se bloqueaban bien porque me falto reiniciar el servicio después de editar el archivo.

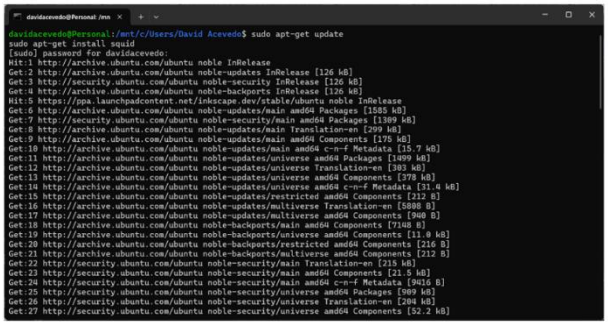
También se activó la autenticación por usuario usando htpasswd, aunque algunos usuarios no podían entrar porque escribieron mal su contraseña o no estaban agregados correctamente. Esto ayudo a que solo los usuarios autenticados pudieran navegar, pero hubo problemas cuando algunos olvidaron sus credenciales y tuve que reiniciarlas varias veces.

Después de configurar todo, se hicieron pruebas para ver si el proxy funcionaba. Los intentos de entrar a los sitios bloqueados desde la LAN fueron rechazados, aunque en una prueba se me olvido agregar un sitio a la lista negra y si se pudo acceder. Los usuarios que si estaban autenticados pudieron navegar en los sitios permitidos. Los logs de Squid mostraron el tráfico y ayudaron a revisar si las reglas estaban bien aplicadas.

En conclusión, Squid resulto ser una herramienta bastante util y flexible para controlar la navegación web en la red, aunque la configuración puede ser complicada si no se revisa bien cada paso. El sistema permite un control centralizado y seguro del tráfico, reforzando las políticas de seguridad en el acceso a Internet, a continuación, se detalla el procedimiento realizado.

Se instala del servidor proxy Squid en el servidor GNU/Linux utilizando el gestor de paquetes APT

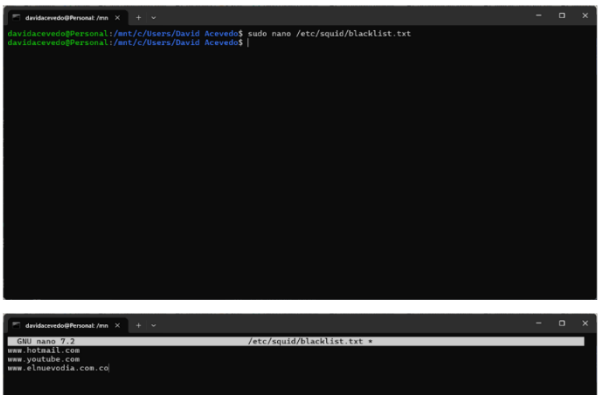
Figura 24. Instalación del servidor proxy Squid en el Servidor Ubuntu utilizando el gestor de paquetes APT



Fuente: Elaboración propia

Se configura dentro del archivo principal de Squid (squid.conf) donde se definen las Listas de Control de Acceso (ACLs) y se habilita el método de autenticación por usuario (htpasswd), asegurando que solo usuarios autorizados puedan navegar

Figura 25. Definición de las Listas de Control de Acceso (ACLs) y configuración del método de autenticación en el archivo squid.conf.



Fuente: Elaboración propia

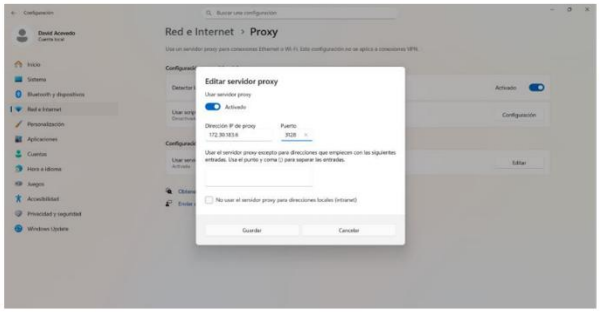
Se implementan políticas de contenido se integra la lista negra, especificando los dominios (como www.youtube.com) que deben ser bloqueados para reforzar las políticas de seguridad y control de contenido

Figura 26. Definición e integración de la Lista Negra (Blacklist) en el archivo de configuración del Proxy Squid (squid.conf) para restringir la navegación a dominios específicos

Fuente: Elaboración propia

Se realiza el ajuste manual requerido en el navegador del cliente de la LAN para forzar que el tráfico HTTP pase por el Proxy no transparente, especificando la dirección IP y el puerto del servidor Squid.

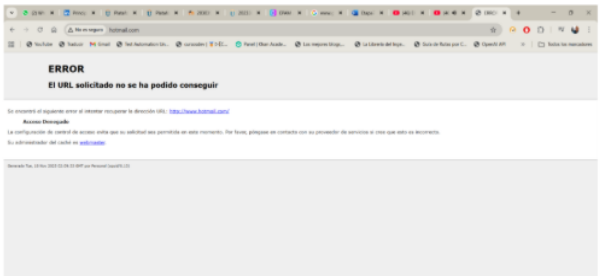
Figura 27. Configuración del navegador del cliente (Mozilla Firefox) para utilizar el Proxy HTTP no transparente, especificando la dirección IP y el puerto del servidor Squid



Fuente: Elaboración propia

Finalmente se evidencia el resultado exitoso de la aplicación de la lista negra y las políticas de seguridad, mostrando el mensaje de "Acceso Denegado" que recibe el usuario al intentar acceder a una URL restringida a través del proxy Squid

Figura 28. Validación de la política de seguridad: Mensaje de "Acceso Denegado" del Proxy Squid al intentar acceder a una URL restringida



Fuente: Elaboración propia

4. CONCLUSIONES

El desarrollo de este proyecto demostró la viabilidad y eficacia de construir una arquitectura de red perimetral robusta utilizando soluciones de código abierto, específicamente GNU/Linux Endian Firewall en un entorno virtualizado. Se logró con éxito la segmentación de la red en las tres zonas críticas (Verde/LAN, Roja/WAN y Naranja/DMZ), estableciendo la base para una gestión de seguridad multicapa.

La correcta implementación de la Traducción de Direcciones de Red (NAT) fue verificada, garantizando la conectividad saliente para la LAN y la DMZ hacia Internet. Este avance se complementó con la definición de políticas de seguridad estrictas, como la habilitación controlada de servicios esenciales (HTTP y FTP) hacia la DMZ, y la validación del bloqueo de tráfico ICMP entre zonas, un punto crucial para minimizar la superficie de ataque del servidor de servicios.

Finalmente, la integración del Proxy HTTP no transparente (Squid) no solo añadió una capa de seguridad y autenticación por usuario, sino que también confirmó la capacidad del sistema para aplicar políticas de control de contenido, bloqueando el acceso a sitios específicos mediante listas negras. Estos resultados validan que la combinación de GNU/Linux Endian y Squid es una solución eficiente y de bajo costo para cumplir con los requerimientos de seguridad y control de tráfico en entornos de red modernos

5. REFERENCIAS

[1] Debian. (2023). *El manual del administrador de Debian 12.5.0*. Debian. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html.
[2] Endian. (2016). *Endian UTM 3.2 Manual referencia*. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html
[3] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server*. Packt Publishing. [En línea]. Disponible en: https://open.spotify.com/track/36p2NEHQ7nR1zAi2vznrOF
[4] LPI. (2022). *LPI LPIC-1 Exam 101. Tema 102: Comandos GNU y Unix*. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/10500/102/
[5] Oracle. (2020). *Manual de usuario VirtualBox*. VirtualBox. [En línea]. Disponible en: https://www.virtualbox.org/manual/