ARQUITECTURA DE DEFENSA EN LA CAPA EXTERNA DE LA RED CON ENDIAN FIREWALL

Juan Carlos Pulido Sierra
jcpulidosi@unadvirtual.edu.co
Javier Mauricio Cárdenas Aguirre
jmcardenasa@unadvirtual.edu.co
Omar Ricardo Cortes Triana
orcortest@unadvirtual.edu.co
Erik Johan Hernández Torres
ejhernandezt@unadvirtual.edu.co
Julio Cesar Ramos Guevara
jcramosgu@unadvirtual.edu.co

RESUMEN: *Este informe describe el armado de un banco de pruebas de comunicaciones utilizando Endian Firewall. Se trabajaron cinco frentes preparación de la instancia de GNU/Linux Endian en VirtualBox incluyendo mapeo de interfaces y su instalación completa; traducción de direcciones mediante NAT, provisión de servicios ubicados en la zona desmilitarizada (DMZ), elaboración de políticas para permitir o bloquear intercambios entre segmentos y puesta en marcha de un proxy con autenticación para regular el acceso a la web. El propósito es mostrar, desde la óptica de la defensa perimetral y la administración de plataformas, la ductilidad de Endian como recurso pedagógico. Además, se cubren prácticas sobre zonificación, tránsito entre redes, exposición controlada de servidores y gobierno del flujo de datos, también se verifican procedimientos repetibles que fortalecen diseño seguro, registro de cambios y validaciones técnicas, útiles en cursos, laboratorios y contextos operativos y ambientes de producción.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad perimetral

1 INTRODUCCIÓN

Endian es una plataforma UTM basada en GNU/Linux que concentra cortafuegos de estado, traducción de direcciones, filtrado web y capacidades de proxy en una consola sencilla, ideal para aprender seguridad perimetral con segmentación por zonas (RED/WAN, GREEN/LAN y ORANGE/DMZ). En el laboratorio se parte de la preparación de la instancia en VirtualBox con sus interfaces de red y la instalación adecuada del sistema, se habilita la configuración NAT para permitir la salida hacia Internet desde los segmentos internos, se disponen servicios en la zona DMZ para aislar y exponer servidores de forma controlada, se establecen reglas de acceso que autorizan o bloquean flujos específicos entre las áreas y hacia la WAN, y se incorpora un proxy con autenticación para gobernar la navegación. Así, Endian sirve como marco práctico para integrar operación diaria y criterios de defensa en el perímetro.

2 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VB

2.1 DESCRIPCIÓN GENERAL

Se crearán tres máquinas en VirtualBox: Endian con tres interfaces (RED, GREEN, ORANGE), un Desktop en GREEN (Ubuntu o Debian) y un Server en ORANGE (Ubuntu o Debian). Se instalará Endian Community [1], se configurará direccionamiento por zonas, NAT para LAN y DMZ, servicios en DMZ, reglas interzona y proxy HTTP autenticado.

Figura 1. Descarga desde el sitio oficial

Fuente: Autoría Propia

3 CONFIGURACIÓN NAT CON ENDIAN

DESCRIPCIÓN GENERAL

Se implementarán dos configuraciones de traducción de direcciones en Endian para garantizar salida controlada a Internet. Primero, se creará una regla de NAT de salida (MASQUERADE) para la subred GREEN, de modo que los equipos de la LAN utilicen la IP de la interfaz RED al comunicarse con la WAN simulada. Segundo, se definirá una

regla equivalente para la subred ORANGE, permitiendo que los servidores en la DMZ accedan a recursos externos sin exponer direcciones privadas. Ambas configuraciones se validarán mediante pruebas de conectividad (ping, DNS, curl), revisión de registros del firewall y verificación en NAT/Outgoing y Port Forward/NAT activas.

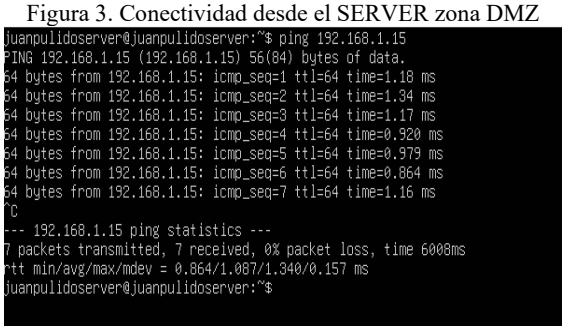
3.1 IMPLEMENTACIÓN NAT DE SALIDA, LAN – WAN (GREEN – RED) Y DMZ (ORANGE) CON ENDIAN FIREWALL

Primero se enciende Endian y se espera a que obtenga dirección por DHCP en la interfaz RED. Luego se inicia el Desktop en GREEN [2] y se inicia el Server en ORANGE. Se verifican IP, gateway y DNS. Desde el Desktop se accede a la consola web. Se configura NAT GREEN RED y ORANGE [3], se habilitan políticas. Se prueba conectividad básica.

Figura 2. Conectividad desde el Ubuntu hacia la zona GREEN

Fuente: Autoría Propia

Figura 3. Conectividad desde el SERVER zona DMZ



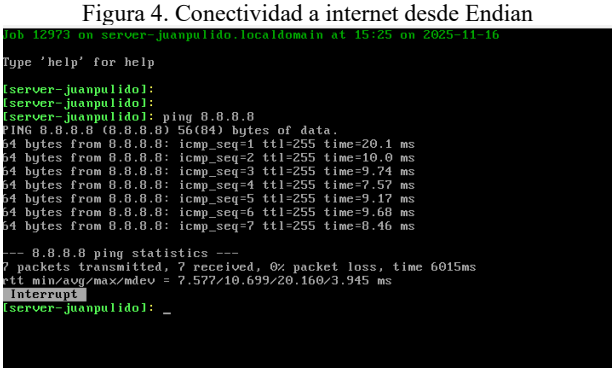
.

Fuente: Autoría Propia

3.2 CONEXIÓN A RED DE INTERNET DESDE ENDIAN

La finalidad de esta comprobación es asegurar que los segmentos LAN y DMZ salgan a la red pública empleando la interfaz ROJA del cortafuegos. Para ello, se abrió la consola de Endian y se ejecutó ping 8.8.8.8 [4]. Con este ensayo se verifica la salida hacia el exterior utilizando utilidades de diagnóstico de red como *ping*.

Figura 4. Conectividad a internet desde Endian



.

Fuente: Autoría Propia

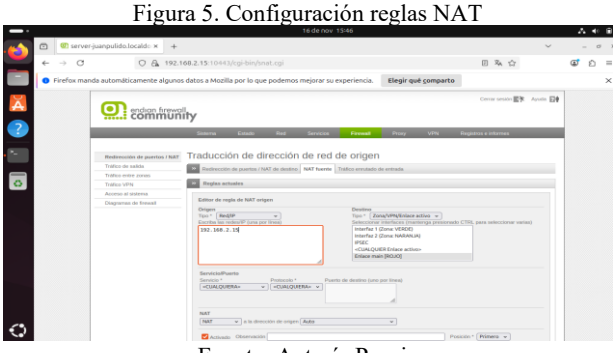
Como evidenciamos se al realiza el ping desde Endian obtenemos los siguientes resultados:

- La respuesta de ping 8.8.8.8 confirma desde el firewall hacia Internet y la existencia de una ruta por **defecto** operativa vía interfaz RED.
- Corrobora que está funcionando para tráfico originado en Endian.
- Latencia y pérdida (si 0%) sugieren enlace estable, valores altos/pérdidas indicarían congestión o limitaciones del host/VirtualBox.
- El ping a una IP pública no valida resolución de nombres, conviene probar google.com o navegación HTTP/HTTPS desde clientes.
- Debe observarse tráfico saliente en **logs** y contadores de NAT [4].

3.3 REGLAS DE CONFIGURACIÓN NAT

En la barra principal del cortafuegos se abrió el módulo de reenvío y traducción, eligiendo SNAT, donde se definieron dos políticas generadas por el sistema. Una de ellas enmascara el origen del segmento VERDE, utilizando como pasarela 192.168.2.15 [5], y dirige el tráfico por la interfaz ROJA hacia la red pública.

Figura 5. Configuración reglas NAT



Fuente: Autoría Propia

3.4 CONFIGURACIÓN DE REENVÍO DE PUERTOS

El reenvío de puertos redirige solicitudes entrantes desde la IP pública hacia un servidor interno en la DMZ mediante

DNAT. Se implementará creando una regla en Endian [5] Uplink/RED como destino, servicio requerido, traducción a IP privada y puerto [6], habilitando registro y permitiendo el flujo controlado.

- Se accede a la interfaz web de Endian desde LAN 192.168.2.15 [5]
- Se navega a Firewall Redirección de puertos / NAT posteriormente NAT fuente [5]
- Se crea una regla para la DMZ: en Origen, tipo Red/IP, se ingresa 192.168.1.0/24 en destino, tipo Zona/VPN/Enlace activo, se selecciona Enlace main ROJO, en Servicio/Protocolo se deja CUALQUIERA posteriormente en NAT se selecciona NAT con dirección de origen Auto y se marca Activado, posición primero y se guarda.[6]
- Se crea una regla para la LAN: en Origen se ingresa 192.168.2.0/24; Destino Enlace main ROJO, servicio y Protocolo CUALQUIERA, NAT con dirección de origen Auto, activada y guardada.[6]
- Por último se realizan las validaciones pertinentes para indicar si el funcionamiento es el adecuado [6].

Figura 6. Configuración de reglas y puertos

Fuente: Autoría Propia

3.5 EJECUCIÓN DE PRUEBA UBUNTU DESKTOP

Se realiza el test desde el CLIENTE comprobando así que está funcionando de acuerdo con los requerimientos planteados en la actividad, por tanto, podemos dar por satisfactorio y completo esta ejecución. [7]

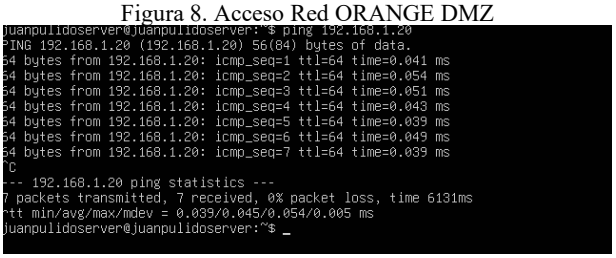
Figura 7. Acceso Red Green

. Fuente: Autoría Propia

3.6 EJECUCIÓN DE PRUEBA SERVER DMZ

Se realiza el test desde el SERVER comprobando así que está funcionando de acuerdo con los requerimientos planteados en la actividad, por tanto, podemos dar por satisfactorio y completo esta ejecución. [8]

Figura 8. Acceso Red ORANGE DMZ



Fuente: Autoría Propia

3.7 RESULTADOS FINALES

Se verificó conectividad completa desde LAN y DMZ hacia Internet mediante Endian, confirmando NAT funcional, rutas correctas y resolución DNS. [8]

Las pruebas mostraron latencias estables, sin pérdidas en ICMP, navegación HTTP/HTTPS exitosa y contadores de traducción aumentando en NAT fuente. Se validaron políticas de salida Green y Orange, garantizando control del tráfico y segmentación adecuada entre zonas con gateway Red.

La consola registró eventos coherentes y reglas activas, evidenciando administración centralizada efectiva. Se cumplieron objetivos académicos y operativos, dejando una base reproducible para ejercicios posteriores.

4 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Objetivo

- El procedimiento establece la configuración del firewall óptimo para servidores Ubuntu que garantice:

Acceso ininterrumpido a servicios web esenciales en conexión de (HTTP en puerto 80 y FTP en puerto 21).

Implementación:

1. Preparación del sistema:

- Instalar el paquete UFW (Uncomplicated Firewall) si no está presente.

- Iniciar el servicio de firewall y configurarlo para arranque automático.

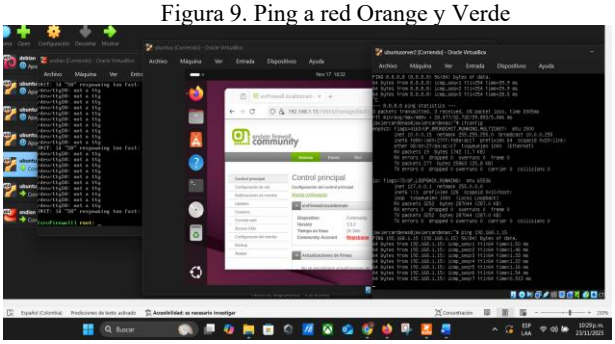
4.1 DESCRIPCION GENERAL

Durante el proceso se configuro la interfaz verde (LAN interna) y naranja (DMZ) en Endian Firewall, se crearon reglas en el módulo Firewall → Access para autorizar tráfico hacia el servidor DMZ (10.0.0.15), y se verificó el bloqueo de ICMP mediante pruebas de conectividad. Esta práctica permitió comprender cómo se aíslan servicios públicos dentro de una DMZ para mejorar la seguridad y control del tráfico en una red organizacional.

4.2 PERMITIR SERVICIOS HTTP Y FTP

Se realizo un ping desde la maquina server Ubuntu hacia la ip 192.168.1.15 que es la ip de Endian Firewall, de igual forma desde el Ubuntu desktop abierto el firewall Endian desde el navegador usando la ip 192.168.1.15 y realizando las configuraciones necesarias en la red para que logren la comunicación exitosa en el Endian, así poder hacer ping entre maquinas desde la red ver y naranjada hacia el Endian Firewall con éxito [9].

Figura 9. Ping a red Orange y Verde



Fuente: Autoría Propia

El objetivo principal fue permitir únicamente los servicios autorizados —HTTP (puerto 80) y FTP (puerto 21)— hacia la DMZ [9].

Figura 10. Acceso web desde Ubuntu Desktop

Fuente: Autoría Propia

Desde el navegador de Ubuntu desktop por medio de http://10.0.0.15 con la regla de Acceso creada en el (Firewall) de Endian, permitiendo HTTP desde la zona verde hacia la zona naranjada (DMZ) en el puerto 80 el cual está se realizó con éxito [10].

Figura 11 Permitir servicio FTP (PORT 21).

Fuente: Autoría Propia

El resultado del comando ftp 10.0.0.15 y posterior conexión, login (javiercardenas), y confirmación (230 OK) indican que el servidor FTP (Pure-FTPd) está instalado y en funcionamiento en el Ubuntu desktop DMZ (10.0.0.15).
La regla de Acceso (Firewall) de Endian que permite el tráfico TCP/21 (FTP) desde la zona verde hacia la zona naranja (DMZ) está correctamente configurada y activa [11].

4.3 DENEGAR PROTOCOLO ICMP

Por medio de la creación de la regla para denegar acceso por ICMP desde la zona verde a la zona naranjada en puertos 8 y 30 ya con esto no permitir hacer ping entre las zonas.

Figura 12 Denegar el protocolo ICMP (Puerto 8 y 30)

Fuente: Autoría Propia

Se realiza la configuración en el Endian Firewall en la zona Firewall y luego en tráfico entre zonas y desde allí se realizó la configuración en origen (tipo) se seleccionó zona/interfaz. En origen se seleccionó zona VERDE (Zona de escritorio/Ubuntu). destino (tipo): se seleccionó Red/IP. Destino (campo de texto) escribí la ip 10.0.0.15 (La IP del servidor Ubuntu - DMZ). El servicio lo deje en definido por el usuario. Protocolo seleccione ICMP. Política (Acción) lo deje en Denegar. La casilla la deje en activado. Añadir regla acá le di clic en el botón para crear la regla y poder denegar por ICMP mediante ping en la terminal de Ubuntu desktop hacia la zona ORANGE. [12]

Figura 13 Denegar el protocolo ICMP (Puerto 8 y 30)

Fuente: Autoría Propia

Se hace la denegación de ping hacia la ip 10.0.0.15 que sería la zona desmilitarizada DMZ o zona ORANGE donde se evidencia que no hay conexión lo cual hace denegar el acceso por ICMP desde la zona VERDE a la zona ORANGE en puertos 8 y 30 y con esto no permitir hacer ping entre las zonas [13].

5 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRAFICO

5.1 DESCRIPCION GENERAL

Las reglas de acceso son las instrucciones que sigue un firewall para decidir qué tráfico puede entrar, salir o moverse a través de una red, y cuáles deben ser bloqueados. Su objetivo es proteger la red, gestionar el flujo de información y prevenir accesos no autorizados.

Esta fase se centró en definir políticas de seguridad perimetralmente para filtrar tráfico entre las zonas LAN, DMZ y WAN mediante Endian Firewall.

Se configuraron reglas de firewall en Endian para permitir el paso de tráfico en HTTP por el (puerto 80) y FTP por el (puerto 21) entre las zonas Verde del rango definido 192.168.1.1 (LAN), Naranja rango 10.0.0.1 (DMZ) y Roja (WAN). Para validar su funcionamiento, se realizaron pruebas prácticas utilizando navegador web y terminal desde estaciones de trabajo y servidores virtualizados en cada zona.

Las políticas de firewall se definieron en el panel de firewall de Endian y así controlar el tráfico entre las zonas:

- **HTTP LAN - DMZ**: Desde la zona verde a la zona Naranja se garantiza el acceso interno a servicios web alojados en la DMZ o donde se aloja el servidor, se configuró una regla explícita en Endian Firewall que permite tráfico HTTP (puerto 80) desde la LAN.

Figura 14. Conexión de la NAT a las redes

Fuente: Autoría Propia

- **FTP WAN - DMZ**: Habilitado para transferencias de archivos desde Internet

Figura 15. Trasferencia de wan – a DMZ

Fuente: Autoría Propia

5.2 CONFIGURACIÓN DE REGLAS ENTRE ZONAS:

Propósito se definieron y aplicaron reglas de firewall en la sección "Acceso Inter-Zona" del panel de administración de Endian Firewall

- **Regla HTTP LAN - DMZ:** Permite tráfico web desde estaciones de trabajo de la zona Verde (LAN) hacia servidores en la zona Naranja (DMZ).
- **Regla FTP LAN - DMZ:** Permite transferencias de archivos desde la zona verde (LAN) hacia servidores en la zona Naranja (DMZ).
- **Regla HTTP WAN - DMZ:** Habilita el acceso externo al servidor de la zona roja (WEB) de la zona Naranja (DMZ) mediante redireccionamiento de puertos.
- **Regla FTP WAN - DMZ:** Permite conexiones FTP desde la zona Roja (WAN hacia servicios alojados en la zona Naranja (DMZ).

Estas reglas se configuraron seleccionando el protocolo correspondiente (HTTP o FTP), origen y destino por zonas, y activando el estado de la regla.

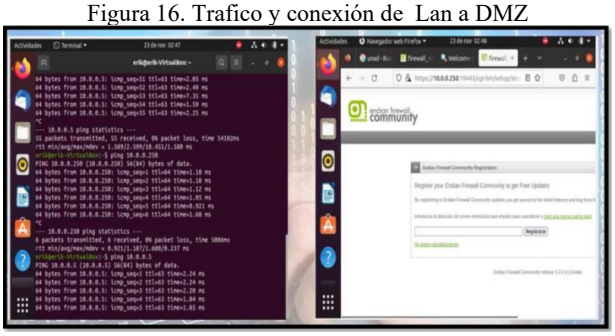
5.3 VERIFICACION Y PRUEBAS DE TRAFICO DE RED

Propósito: Comprobar el tráfico de red a través un navegador web según las reglas configuradas.

Implementación: Las pruebas de conectividad se realizaron desde un navegador web y comprobación de estas por medio del comando ping según correspondiera desde la maquina desktop Ubuntu Desktop (zona Verde). Se validó:

Acceso HTTP desde LAN a DMZ: Mediante IP del servidor web en la zona naranja.

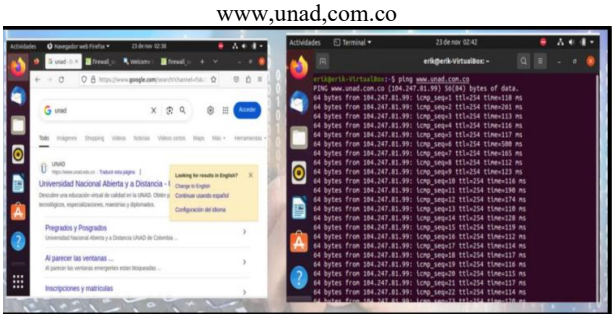
Figura 16. Trafico y conexión de Lan a DMZ



Fuente: Autoría Propia

Acceso HTTP desde LAN a WAN: Accediendo exitosamente a sitios públicos como www.unad.com.co

Figura 17. Trafico y conexión de Lan a WAN, www,unad,com.co



Fuente: Autoría Propia

Acceso HTTP desde WAN a DMZ: Simulado desde el host físico, usando la IP pública/NAT del Endian redirigida hacia un servidor en DMZ.

Acceso FTP desde LAN a WAN: Se probó con direcciones FTP públicas, confirmando la conexión.

6 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE AUTENTICACION PARA NAVEGACION EN INTERNET

6.1 DESCRIPCION GENERAL

Implementación de un proxy HTTP no transparente con control de acceso basado en autenticación por usuario y listas negras de sitios web. La solución permite a las organizaciones gestionar de manera centralizada el uso de internet, reforzando la seguridad y cumpliendo con políticas internas de navegación. La práctica se centró en bloquear portales específicos y validar la autenticación de los usuarios antes de permitir el acceso a la red.

6.2 DESCRIPCIÓN DEL SISTEMA

La arquitectura implementada se compone de los siguientes elementos:

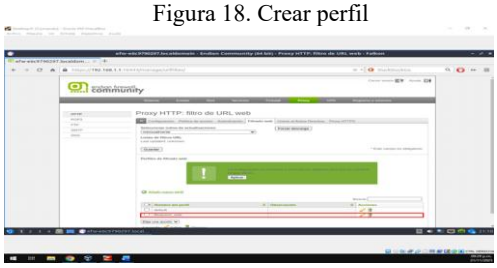
- Proxy HTTP no transparente: Intercepta y filtra el tráfico web saliente sin que los clientes modifiquen su configuración de red de manera forzada.
- Sistema de autenticación de usuarios: Los usuarios deben iniciar sesión en el proxy para navegar por internet, garantizando que las políticas se apliquen según perfiles y grupos.
- Lista negra de sitios web: Se configuró un perfil para restringir el acceso a los siguientes portales:
  www.hotmail.com
  www.youtube.com
  www.elnuevodia.com.co

6.3 PASOS DE IMPLEMENTACIÓN

1. Creación de perfiles de restricción:

- Se definió un perfil de navegación que incluye los sitios web bloqueados [18].

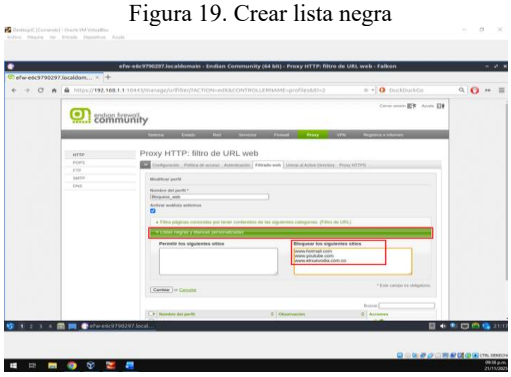
Figura 18. Crear perfil



Fuente: Autoría Propia

- Se establecieron reglas de filtrado en el proxy para denegar el acceso a estas direcciones [19].

Figura 19. Crear lista negra

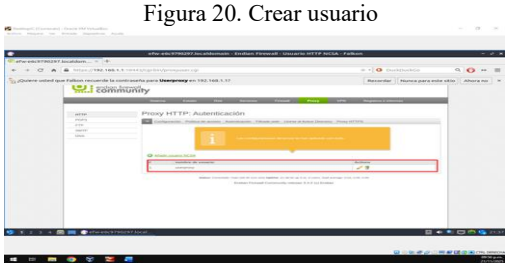


Fuente: Autoría Propia

2. Configuración de autenticación y grupos:

- Se creó un usuario y se asignó a un grupo específico dentro del proxy [20].

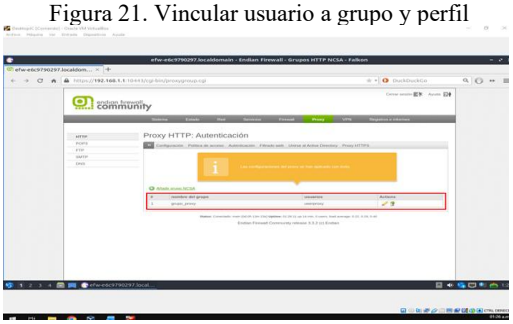
Figura 20. Crear usuario



Fuente: Autoría Propia

- Se configuró una política de acceso que vincula la autenticación del usuario con el perfil de restricción [21].

Figura 21. Vincular usuario a grupo y perfil



Fuente: Autoría Propia

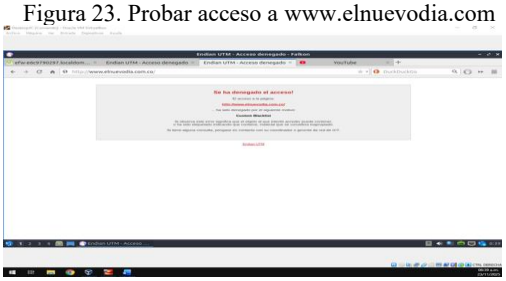
3. Pruebas de funcionamiento:

- Desde un navegador en la LAN, se intentó acceder a los sitios bloqueados [22].

Figura 22. Probar acceso a www.hotmail.com

Fuente: Autoría Propia

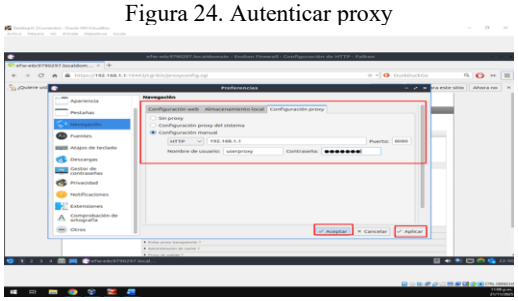
Figura 23. Probar acceso a www.elnuevodia.com



Fuente: Autoría Propia

- El proxy solicitó autenticación y aplicó las restricciones, mostrando mensajes de bloqueo para los portales restringidos [23].

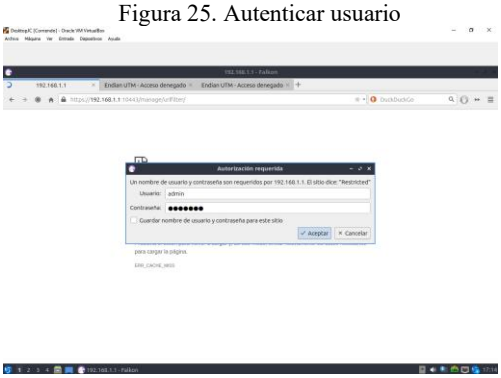
Figura 24. Autenticar proxy



Fuente: Autoría Propia

- Se verificó que el usuario autenticado podía navegar por sitios permitidos sin inconvenientes [24].

Figura 25. Autenticar usuario



Fuente: Autoría Propia

Figura 26. Validar sitios no bloqueados

Fuente: Autoría Propia

7 CONCLUSIONES

Se confirmó la salida a internet desde lan y dmz mediante reglas de nat y se registró evidencia de su operación estable

Se configuraron y activaron políticas de tráfico además se verificó la conectividad icmp dns y http https en ambos segmentos observando los contadores ascendentes en nat

Se logro documentar el procedimiento para futuras réplicas con sus capturas y parámetros clave en la configuración implementada.

La implementación de un proxy HTTP no transparente permite un control centralizado del tráfico web, mejorando la seguridad y el cumplimiento de políticas de navegación.

La integración de listas negras y autenticación por usuario proporciona flexibilidad y personalización, aplicando restricciones de manera selectiva según el perfil del usuario o grupo.

La prueba demuestra que la gestión proactiva del acceso a internet es eficiente y verificable, reduciendo riesgos de navegación no autorizada y promoviendo el uso responsable de recursos de red.

8 REFERENCIAS

[1] Endian Firewall Community. (s. f.). SourceForge. 20 de noviembre de 2023, de https://sourceforge.net/projects/efw/

[2] Endian. (s. f.). Endian UTM 3.2 Reference Manual. Recuperado de http://docs.endian.com/3.2/utm/index.html

[3] Endian. (s. f.). EndianOS UTM: Powerful cybersecurity solutions for secure network management and advanced threat protection.http://www.endian.com/products/utm/

[4] InfoRed [@InfoRedes]. (2019, abril 22). Cómo configurar reglas Inter-Zone Traffic Endian [Video]. YouTube. https://www.youtube.com/watch?v=XK0QdHYk6pg

[5] Red Hat. (2023). Understanding Network Address Translation (NAT). Red Hat Customer Portal. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/

[6] Endian Community Documentation. (s. f.). Port Forwarding and NAT Configuration in Endian Firewall. https://docs.endian.com/

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

[8] SC Tech Academy. (2019). How to install and configure endian firewall [Video]. YouTube. https://www.youtube.com/watch?v=Jlv9sgmgr4k