SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL

Gladys Viviana Gómez Rojas
gvgomezro@unadvirtual.edu.co
Adriana Lucia Goyeneche Goyeneche
algoyenecheg@unadvirtual.edu.co
Natalia Julieth Moreno Guaidia
njmorenogu@unadvirtual.edu.co
Yamid Tibocha Coronado
ytibochac@unadvirtual.edu.co

RESUMEN: *En el presente artículo se expone la configuración de un laboratorio de red basado en Endian Firewall, en el cual se desarrollaron cinco temáticas principales: la configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del sistema, la configuración NAT, los servicios de la zona DMZ para la red, la creación de reglas de acceso para permitir o denegar tráfico, y la configuración de un proxy HTTP no transparente con políticas de autenticación para la navegación en Internet. Este trabajo busca demostrar la versatilidad de Endian como herramienta de formación en seguridad de redes y administración de sistemas.*

PALABRAS CLAVE: Endian Firewall, proxy HTTP, autenticación, seguridad perimetral.

1 INTRODUCCIÓN

Hoy en día, la seguridad perimetral es fundamental para proteger las redes informáticas frente a amenazas internas y externas. Por ello, es importante conocer y disponer de herramientas que permitan controlar el acceso, filtrar contenidos y gestionar el tráfico en diferentes entornos.

Dentro de la amplia gama de soluciones gratuitas y de código abierto, destaca Endian Firewall Community [1], una plataforma que podría considerarse un "todo en uno", ya que ofrece una solución robusta de seguridad perimetral con múltiples funcionalidades [3]. Su interfaz intuitiva y su enfoque modular de servicios la convierten en una opción accesible y eficaz para diversos escenarios.

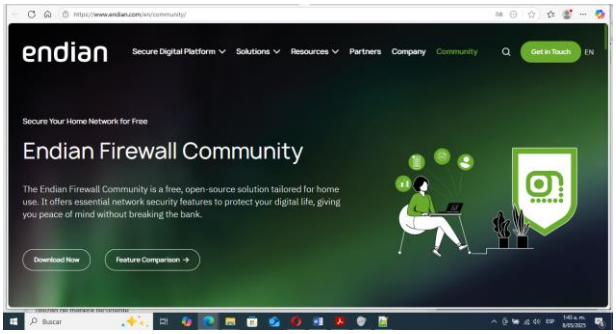
2 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN FIREWALL

Para iniciar la implementación del laboratorio de seguridad perimetral, se llevó a cabo la instalación del sistema Endian Firewall en un entorno virtualizado. A continuación, se describe el proceso de descarga, creación de la máquina virtual y configuración de los adaptadores de red para cada zona: WAN, LAN y DMZ.

2.1 DESCARGA E INSTALACIÓN DEL SISTEMA

Se accedió al sitio oficial de Endian para descargar la imagen ISO [1]. El proceso de instalación puede seguirse paso a paso mediante el video tutorial disponible en [8], así como en la guía detallada presentada en [11].

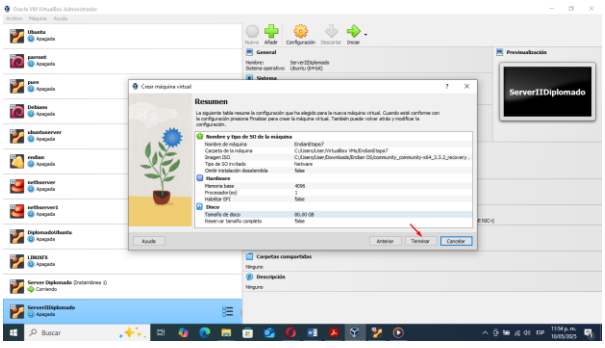
Figura 1. Página oficial de Endian.



Fuente: Autoría propia.

Una vez descargada, se creó una nueva máquina virtual en VirtualBox [13] con las características recomendadas.

Figura 2. Creación nueva MV



Fuente: Autoría propia.

2.2 INSTALACIÓN SO ENDIAN FIREWALL

Al dar doble clic sobre la máquina virtual [13] previamente creada, se inicia el proceso de instalación del sistema ENDIAN.

Durante la instalación se seleccionó el idioma, se aceptaron los términos y se establecieron las configuraciones iniciales del sistema.

Al finalizar la instalación, el sistema confirma la IP de acceso al entorno web de la consola de Endian, este acceso se realiza desde un navegador web en otro equipo cliente ya que el servidor de Endian no tiene entorno gráfico.

Figura 3. IP de acceso (192.168.10.1 NETWORK MASK 255.255.255.0) para acceder a la consola de Endian.

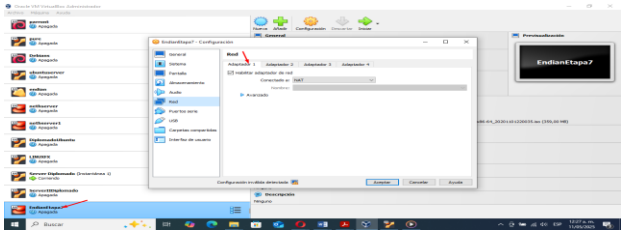
Fuente: Autoría propia.

2.3 CONFIGURACIÓN DE LAS TARJETAS Y/O ADAPTADORES DE RED.

En VirtualBox se configuraron tres adaptadores para representar las zonas del firewall [13]:

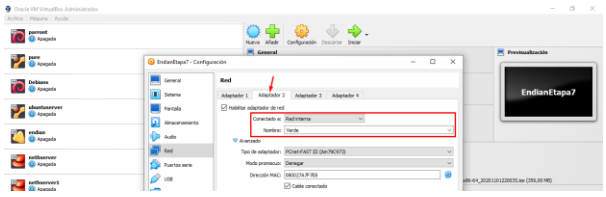
- Adaptador 1 (WAN - Roja): conectado mediante NAT para acceso a Internet.
- Adaptador 2 (LAN - Verde): red interna con segmento 192.168.10.0/24.
- Adaptador 3 (DMZ - Naranja): red interna con segmento 192.168.20.0/24.

Figura 4. Configuración del adaptador WAN en VirtualBox.



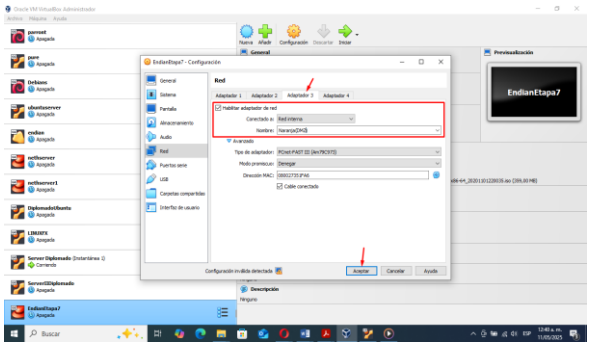
Fuente: Autoría propia.

Figura 5. Configuración del adaptador LAN en VirtualBox.



Fuente: Autoría propia.

Figura 6. Configuración del adaptador DMZ en VirtualBox



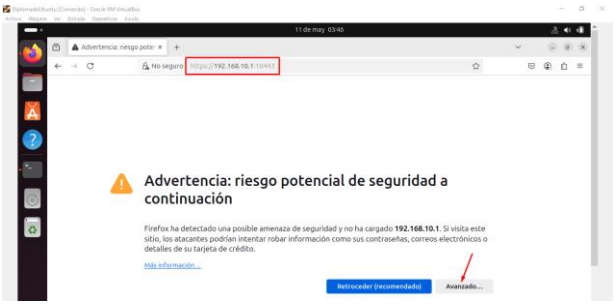
Fuente: Autoría propia.

2.4 ACCESO A LA CONSOLA WEB DE ENDIAN

Una vez configurado los 3 adaptadores de red en VirtualBox e instalado el sistema de Endian [13].

Desde un navegador, se accedió a la consola de administración a través de https://192.168.10.1:10443, aceptando el certificado autofirmado y autenticándose como administrador.

Figura 7. Acceso entorno web de Endian



Fuente: Autoría propia.

El navegador muestra una advertencia al acceder a la IP del firewall debido a un certificado autofirmado.

Se debe seleccionar “Aceptar el riesgo y continuar” para acceder a la consola de administración de Endian Firewall.

2.5 IMPLEMENTACIÓN BÁSICA DE ENDIAN FIREWALL

Esta configuración inicial sigue los pasos recomendados en el manual de referencia de Endian [2] y [10] a través de su entorno web, el cual consta de un asistente con 8 pasos, que se resumen así:

Modo de red y tipo de Uplink (Paso 1): Se selecciona el modo de operación, generalmente Routed, y el tipo de conexión a Internet (Uplink), como DHCP o IP estática.

Zonas de red adicionales (Paso 2): Se eligen las zonas de red a habilitar, además de las básicas ROJA (WAN) y VERDE (LAN), como la NARANJA (DMZ) o AZUL (WiFi).

Configuración de red interna (Paso 3): Se define la IP de la zona VERDE, se habilita el servidor DHCP y se establece el nombre de host y dominio local.

Configuración de zona roja (Paso 4): Se selecciona la interfaz correspondiente a la zona ROJA (Internet) y se configuran parámetros como MTU, MAC y DNS.

Configuración del DNS (Paso 5): Se determina si el sistema usará DNS automático o manual; por defecto, se elige automático.

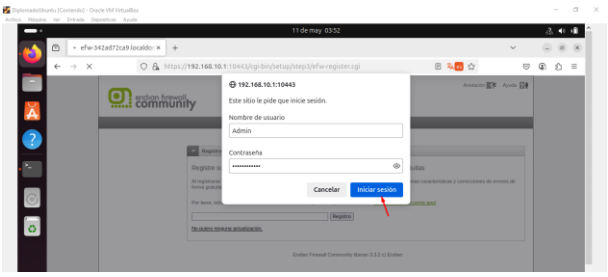
Correo del administrador (Paso 6): Se ingresan opcionalmente direcciones de correo del administrador y del remitente, así como un smarthost si se desea.

Confirmación de configuración (Paso 7): Se revisa toda la configuración realizada y se confirma haciendo clic en "OK, apply configuration".

Aplicación y recarga de servicios (Paso 8): Se guarda la configuración y se recargan los servicios dependientes.

Estos pasos establecen las bases para que Endian funcione como un firewall y sistema de gestión de red en un entorno seguro.

Figura 8. Inicio de sesión en Endian



Fuente: Autoría propia.

3 CONFIGURACIÓN DE NAT EN ENDIAN FIREWALL

3.1 DESCRIPCIÓN GENERAL

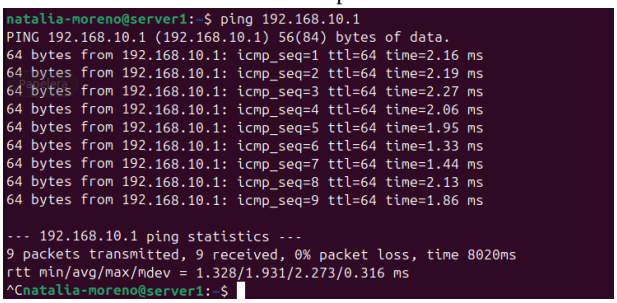
NAT es una técnica ampliamente documentada por proveedores como Red Hat [5], ya que es esencial para la protección de recursos internos, el uso de NAT (Network Address Translation), permite modificar direcciones IP [6] en los paquetes que atraviesan el firewall, facilitando la conexión con redes externas sin comprometer la seguridad interna.

Este apartado describe la configuración de NAT en la plataforma Endian Firewall, como parte de la implementación de una solución de seguridad perimetral práctica, la cual se realizó en un entorno virtualizado, con tres zonas definidas: GREEN (LAN), ORANGE (DMZ) y RED (WAN).

3.2 VERIFICACIÓN DE CONECTIVIDAD ENTRE ZONAS

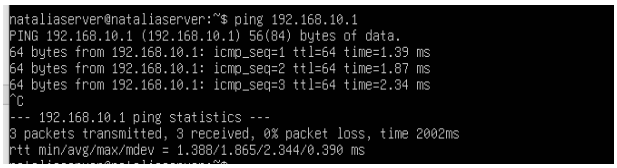
Una vez iniciadas las máquinas virtuales en VirtualBox (Server Endian Firewall, un cliente Ubuntu Desktop en GREEN y un servidor Ubuntu Server en ORANGE) se procedió a verificar la conectividad básica. Se realizaron pruebas de ping desde ambas estaciones hacia la IP de la interfaz GREEN de Endian (192.168.10.1), confirmando la comunicación entre zonas internas [6].

Figura 9. Conectividad zona GREEN desde Ubuntu Desktop



Fuente: Autoría propia.

Figura 10. Conectividad desde el servidor hacia la zona DMZ



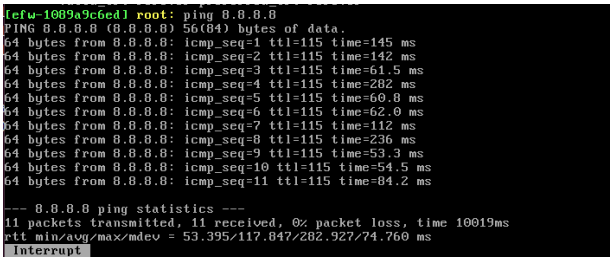
Fuente: Autoría propia.

3.3 SALIDA A INTERNET DESDE ENDIAN

El objetivo de esta validación es confirmar que las redes LAN y DMZ puedan acceder a Internet a través de la interfaz RED del firewall. Para esto, se ingresó a la terminal de la consola de Endian, y se ejecutó el comando: ping 8.8.8.8

Validando la conectividad externa mediante comandos de red como ping.

Figura 11. Verificación de salida a Internet desde Endian



Fuente: Autoría propia.

El resultado del comando ping 8.8.8.8 muestra que:

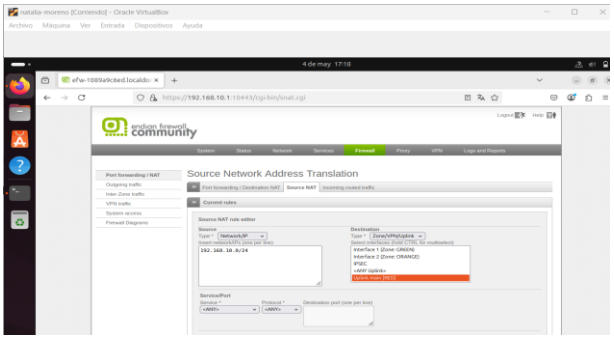
- El firewall tiene acceso a Internet mediante la interfaz RED.
- Las rutas de red están configuradas correctamente.
- No hay pérdida de paquetes (0% packet loss), lo que demuestra estabilidad en la conexión.
- El tiempo promedio de respuesta (latencia) es de aproximadamente 117.8 ms, lo cual es aceptable para una conexión de red estándar [6].

3.4 CONFIGURACIÓN DE REGLAS NAT

Para permitir el acceso a Internet desde las zonas internas, se ingresó a la opción Firewall del menú superior, luego a la sección de Port Forwarding / NAT, nos ubicamos en Source NAT, en donde se crearon dos reglas automáticas.

Una para permitir la traducción de direcciones desde la red GREEN (192.168.10.0/24) hacia la zona RED (Uplink main).

Figura 12. Reglas NAT configuradas para LAN



Fuente: Autoría propia.

Otra para permitir la salida desde la red ORANGE (192.168.20.0/24) hacia la zona RED.

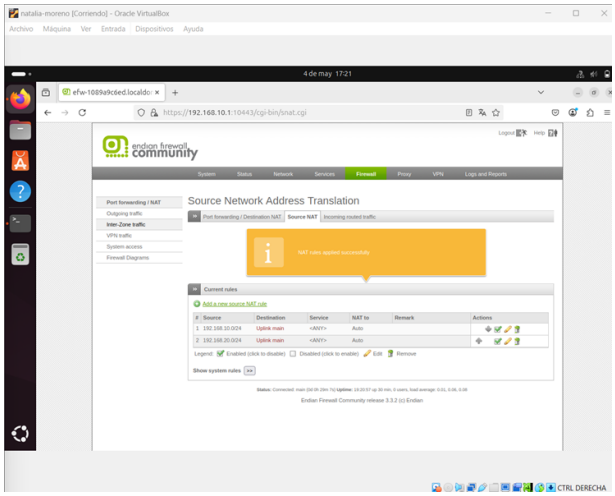
Estas reglas permiten que los dispositivos en las redes LAN y DMZ puedan navegar por Internet, ocultando sus direcciones IP privadas y utilizando la IP pública o compartida de la interfaz RED [6].

3.5 COMPROBACIÓN DE REGLAS NAT

En la sección Source NAT, se observó que las reglas creadas anteriormente, se encontraban activas, con origen en las subredes internas y destino en el Uplink main.

También se verificó que el NAT se estaba aplicando con la opción “Auto”, asegurando que la IP de salida correspondiera a la de la interfaz RED.

Figura 13. Comprobación de reglas NAT activas



Fuente: Autoría propia.

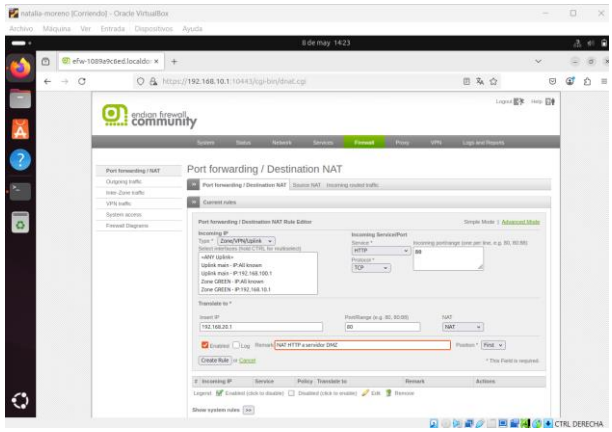
3.6 CONFIGURACIÓN DEL REENVÍO DE PUERTOS (PORT FORWARDING)

Se configuró una regla de Port Forwarding en Endian Firewall para redirigir el tráfico HTTP desde el exterior hacia un servidor ubicado en la zona DMZ.

Para ello, en el menú superior de Endian se accedió a la ruta Firewall a la sección Port forwarding / NAT, luego en la opción Port Forwarding se creó la nueva regla.

La regla permite que las solicitudes entrantes al puerto 80 (HTTP) en la interfaz RED sean redirigidas a la dirección IP 192.168.20.1, correspondiente al servidor web en la zona ORANGE. Se especificaron el servicio (HTTP), el protocolo (TCP), la IP de destino y el puerto interno, y se activó la regla con un comentario descriptivo para su identificación [6].

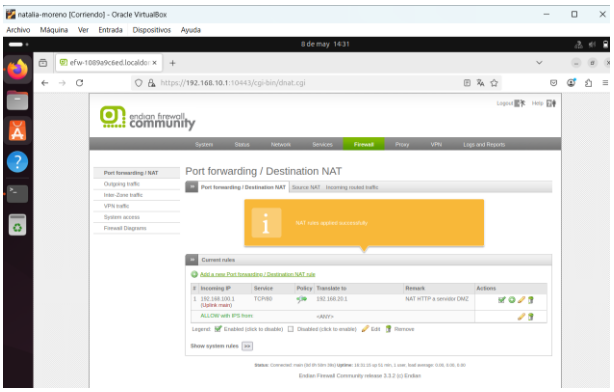
Figura 14. Regla de Port Forwarding configurada



Fuente: Autoría propia.

Se confirma que la regla fue creada exitosamente. En la tabla se muestra el reenvío del puerto TCP 80 desde la IP 192.168.10.1 hacia 192.168.20.1, con la política "ALLOW".

Figura 15. Comprobación de regla de redirección del puerto HTTP



Fuente: Autoría propia.

3.7 NAVEGACIÓN DESDE LAN Y DMZ

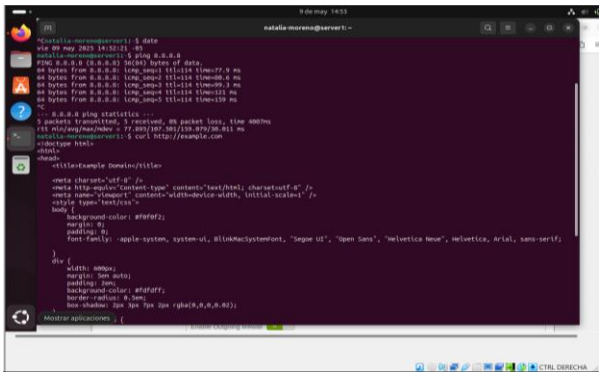
Finalmente, se realizó una prueba de conexión a Internet desde Ubuntu Desktop y Ubuntu Server, haciendo ping a la dirección pública 8.8.8.8. Al recibir respuesta, se confirmó que el tráfico desde la red GREEN y la red ORANGE estaba siendo correctamente enmascarado por el firewall y redirigido hacia Internet mediante la interfaz RED.

Este resultado evidenció que la configuración NAT había sido exitosa y que los dispositivos internos podían acceder a recursos externos sin estar directamente expuestos, cumpliendo así con los objetivos de seguridad perimetral planteados en la temática.

3.8 PRUEBA DESDE LA MAQUINA DE UBUNTU DESKTOP (LAN)

Comprobación exitosa de navegación o conexión desde la red LAN hacia Internet, demostrando que la regla NAT para GREEN está funcionando correctamente.

Figura 16. Verificación de acceso a la red GREEN

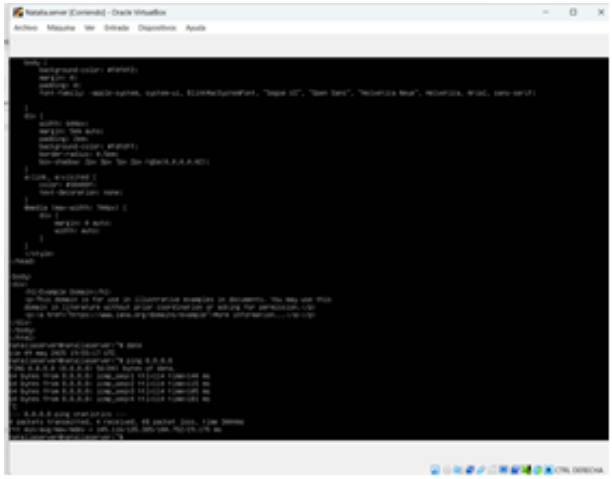


Fuente: Autoría propia.

3.9 DESDE UBUNTU SERVER (DMZ)

Verificación del acceso a Internet desde la DMZ, indicando que la configuración de NAT para ORANGE es operativa.

Figura 17. Verificación de acceso a Internet desde la red ORANGE (DMZ)



Fuente: Autoría propia.

3.10 RESULTADOS OBTENIDOS

Una vez completadas todas las configuraciones, se realizaron pruebas de conectividad desde clientes externos para validar que el tráfico HTTP era correctamente redirigido al servidor en la DMZ.

Además, se comprobó que las reglas NAT permitían la navegación desde las zonas GREEN y ORANGE hacia Internet sin inconvenientes.

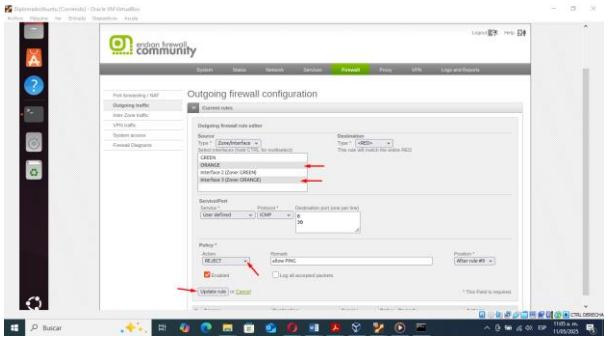
Esta verificación confirmó que el firewall Endian estaba gestionando correctamente el enrutamiento, el reenvío de puertos y la seguridad entre zonas. Con ello, se cumplió el objetivo de la temática 2, garantizando la funcionalidad de NAT como parte esencial de la seguridad perimetral en redes segmentadas.

4 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Cuando se permiten servicios en la zona DMZ, se debe tener en cuenta que debe hacerse con cuidado y con un propósito o razón específica, cuando se colocan servicios expuestos como un servidor web o ftp, evita o reduce el compromiso si llega a ser atacado.

Permitir el acceso solo a servicios específicos desde GREEN o RED reduce la superficie de ataque, mientras que el servidor sigue siendo accesible donde debe serlo.

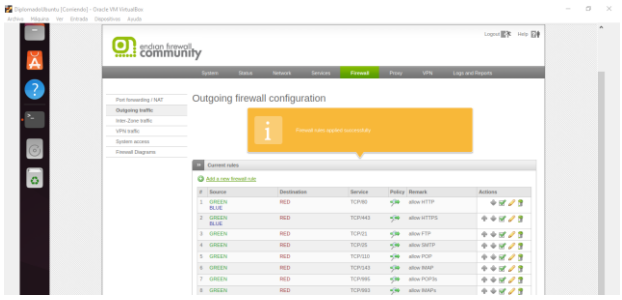
Figura 18. Configuración de regla de firewall saliente**.**



Fuente: Autoría propia.

Se realiza la creación de una regla saliente de Endian Firewall Community, donde se bloquea el protocolo ICMP (ping) desde las zonas GREEN y ORANGE hacia la zona RED. La acción configurada es "REJECT" y la regla está habilitada.

Figura 19. Reglas de tráfico saliente en Endian.



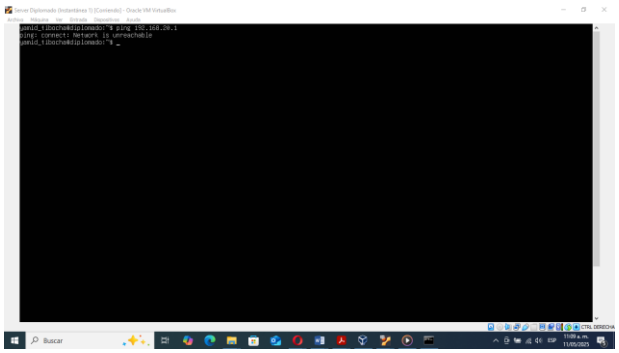
Fuente: Autoría propia.

Se visualiza el listado de reglas configuradas para el tráfico saliente en Endian Firewall Community.

Las reglas permiten servicios como HTTP, HTTPS, FTP, SMTP, IMAP y DNS desde las zonas GREEN, BLUE y ORANGE hacia la zona RED.

También se incluye una regla para bloquear el tráfico ICMP (PING).

Figura 20. Verificación del rechazo de la conexión



Fuente: Autoría propia.

5 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En entornos Linux, la gestión de las reglas de acceso para permitir o denegar el tráfico de red es un componente fundamental de la administración del sistema.

Esta tarea es un componente clave de la seguridad de la información y se lleva a cabo mediante herramientas robustas como iptables, nftables y sistemas de firewall como ufw (Uncomplicated Firewall) y firewalld. El uso de comandos como iptables y ufw resulta esencial para la administración de políticas de red, tal como lo señala la documentación referenciada en [12].

En esta temática, se aborda cómo establecer políticas de control que garanticen un flujo de red seguro, eficiente y adaptado a las necesidades del sistema.

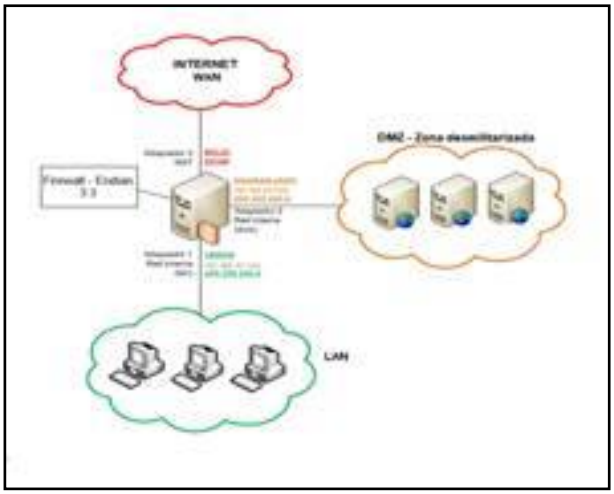
5.1 ¿QUÉ SON LAS REGLAS DE ACCESO?

Las reglas de acceso son instrucciones que permiten o bloquean paquetes de datos que intentan ingresar o salir del sistema, con base en parámetros como dirección IP, puertos, protocolos y estado de conexión. Estas reglas son esenciales para:

- Proteger servicios críticos expuestos a Internet.
- Restringir el acceso a usuarios no autorizados.
- Definir políticas internas de comunicación entre redes y servidores.

5.2 DIAGRAMA DE ARQUITECTURA

Figura 21. Diagrama de Arquitectura



Fuente: Díaz, R. (s.f.). Configuración básica de Endian Firewall. https://ingdiaz.org/firewall-utm-opensource-configuracion-basica-endian-firewall/

Según Díaz, en el diagrama de arquitectura se tiene múltiples interfaces de red (adaptadores), cada uno conectado a una zona diferente:

Adaptador 1 (Red externa / RED)

- Conectado a Internet (WAN)
- IP: Pública (probablemente dinámica)

Esta zona suele ser completamente insegura y se deben aplicar reglas estrictas para limitar el tráfico hacia la red interna.

Adaptador 2 (Red DMZ / ORANGE)

- Conectado a la zona desmilitarizada (DMZ)
- IP: 192.168.20.1
- Aquí se ubican servidores que deben ser accesibles desde el exterior (por ejemplo, web, correo, FTP), pero aislados del resto de la red interna.

Las reglas de acceso en esta zona deben ser muy específicas, permitiendo solo ciertos puertos desde el exterior y restringiendo el acceso desde la DMZ hacia la LAN.

Adaptador 3 (Red interna / GREEN)

- Conectado a la LAN (red local confiable)
- IP: 192.168.10.1

Aquí se encuentran los equipos de los usuarios o empleados.

Esta red es considerada confiable, por lo que tiene mayor libertad de salida a Internet, pero no necesariamente acceso total a la DMZ o WAN sin pasar por reglas de seguridad.

5.3 SEGMENTACIÓN DE LA RED

Esta arquitectura aplica el principio de seguridad por zonas, que consiste en separar la red en distintos segmentos según su nivel de confianza.

Tabla 1. Clasificación de zonas de red

Zona	Nivel de confianza	Acceso Típico
WAN (RED)	Nada confiable	Solo se permite el tráfico necesario.
DMZ	Parcialmente confiable	Accesible desde Internet con reglas específicas.
LAN (GREEN)	Totalmente confiable	Tiene salida a Internet, pero acceso limitado a DMZ

Fuente: Autoría propia

5.4 VENTAJAS DE ESTA ARQUITECTURA

- Seguridad reforzada mediante segmentación.
- Control granular del tráfico entre zonas.
- Reducción de la superficie de ataque a la red interna.
- Aplicación sencilla de políticas basadas en IP y puertos.

5.5 COMUNICAR LA ZONA VERDE (LAN) CON LA ZONA NARANJA (DMZ) USANDO HTTP Y FTP

La gestión del tráfico entre zonas se puede complementar visualmente con ejemplos como los mostrados en [4].

Puertos involucrados:

- HTTP: puerto 80
- FTP: puerto 21 (y puertos pasivos si es necesario)

Figura 22. Comunicación de zonas

Fuente: Autoría propia.

En la figura 22 podemos ver la interfaz de configuración del firewall Endian donde se define la política de comunicación entre zonas de red. En este caso, se visualiza la creación de reglas de acceso que permiten o restringen el tráfico entre la zona DMZ (naranja) y la LAN (verde).

Estas reglas forman parte de la segmentación de red, permitiendo solo el tráfico necesario entre zonas con distinto nivel de confianza.

La configuración de reglas de comunicación entre zonas en Endian Firewall es un aspecto crucial para garantizar una segmentación segura de la red.

Al definir con precisión qué tipo de tráfico puede circular entre la LAN, la DMZ y la WAN, se refuerzan los principios de control de acceso y defensa en profundidad.

Esta estrategia no solo protege los recursos internos frente a amenazas externas, sino que también minimiza el riesgo de movimientos laterales en caso de compromisos dentro de la red.

La correcta implementación de estas políticas es clave para una arquitectura de red robusta y alineada con las mejores prácticas de seguridad perimetral.

5.6 PRUEBAS DESDE NAVEGADOR WEB

Se realizan las pruebas con navegador web o cliente FTP, y su interpretación esperada si las reglas están bien configuradas:

Tabla 2. Pruebas de conectividad desde el navegador web y cliente FTP

Prueba realizada	Resultado Esperado (si reglas están aplicadas correctamente)
HTTP desde LAN (VERDE) hacia DMZ (NARANJA)	Acceso permitido: usuarios internos pueden abrir páginas en la DMZ
HTTP desde LAN (VERDE) hacia WAN (INTERNET)	Acceso permitido: navegación externa desde la LAN
HTTP desde DMZ (NARANJA) hacia WAN (INTERNET)	Bloqueado por defecto, salvo que se requiera actualización remota
HTTP desde WAN (INTERNET) hacia DMZ (NARANJA)	Acceso permitido si se trata de servidores públicos (web/ftp)
FTP desde LAN (VERDE) hacia WAN (INTERNET)	Permitido si los usuarios suben archivos a servidores remotos
FTP desde WAN (INTERNET) hacia DMZ (NARANJA)	Permitido si hay un servidor FTP público expuesto en la DMZ

Fuente: Autoría Propia

5.7 CONSIDERACIONES DE SEGURIDAD

Verificar que no haya reglas que permitan acceso desde WAN a LAN.

Registrar accesos sospechosos y monitorear puertos abiertos.

Si se usa FTP pasivo, habilitar también el rango de puertos pasivos en el firewall.

5.8 RIESGOS DE SEGURIDAD Y CÓMO MITIGARLOS

Riesgos:

- Ataques de fuerza bruta a servicios abiertos en la DMZ.
- FTP sin cifrado.
- Exposición innecesaria de servicios a la WAN.

Medidas:

- Uso de IDS/IPS (como Snort o Suricata)
- Implementación de fail2ban
- Uso de VPNs para acceso remoto seguro

6 PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN EN ENDIAN

6.1 PRERREQUISITOS

Para el desarrollo del laboratorio correspondiente a la implementación del proxy HTTP no transparente con políticas de autenticación en Endian Firewall, se establecieron los siguientes requerimientos de hardware y software:

Máquina virtual Endian Firewall:

- 3 núcleos de CPU
- 3 GB de memoria RAM (3072 MB)
- 20 GB de disco duro
- 3 interfaces de red configuradas como
- RED (WAN), GREEN (LAN) y ORANGE (DMZ)

Cliente Ubuntu Desktop (máquina de prueba):

- 2 GB de memoria RAM
- Conexión a la red GREEN
- Navegador Firefox para realizar las pruebas

En este laboratorio se hace uso de Hyper-V el virtualizador de Microsoft Windows. La creación de las 3 interfaces de red o conmutadores se hicieron mediante un script que se ejecutó con PowerShell.

6.2 DIAGRAMA DE ARQUITECTURA

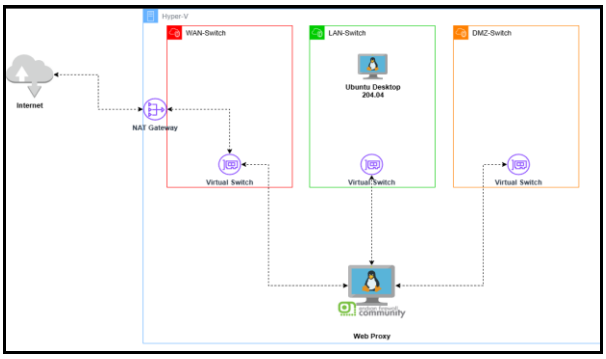
El diagrama ilustra la arquitectura virtual implementada en Hyper-V para el laboratorio de seguridad perimetral con Endian Firewall. La solución incluye tres interruptores virtuales correspondientes a las zonas de red:

WAN-Switch (zona roja): Conectado al Gateway NAT que proporciona acceso a Internet.

LAN-Switch (zona verde): Conecta el cliente Ubuntu Desktop, configurado para usar el proxy HTTP.

DMZ-Switch (zona naranja): Reservado para futuras pruebas con servidores expuestos.

Figura 23. Diagrama de Arquitectura



Fuente: Autoría propia.

EndianOS actúa como firewall y proxy, interconectando las tres zonas a través de interfaces virtuales. Se encarga de gestionar el tráfico entre ellas y aplicar políticas de filtrado y autenticación para el acceso a Internet.

6.3 TOPOLOGÍA Y ASIGNACIÓN DE ZONAS DE RED

Para la implementación del proxy HTTP no transparente, fue necesario configurar las zonas de red en Endian Firewall.

Cada zona fue asociada a un adaptador de red (NIC) virtual distinto, segmentando así el tráfico entre la red externa (Internet), la red interna (LAN) y una zona desmilitarizada (DMZ) para servicios públicos o pruebas futuras.

La siguiente tabla muestra el detalle de la configuración de zonas utilizada, especificando el tipo de red, la interfaz asignada y el rango de direcciones IP para cada una de ellas.

Tabla 3. Topología de red y asignación de interfaces en Endian Firewall

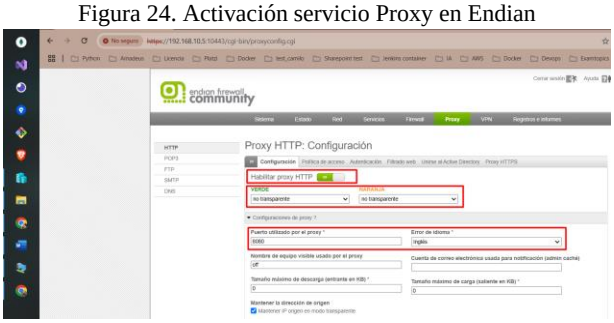
Zona	Interfaz (NIC)	Tipo de red	Ejemplo de IP
Red WAN (Roja)	NIC1	Publica	192.168.100.0/24 (Gateway 192.168.100.1)
Red LAN (Verde)	NIC2	Privada	192.168.10.1/24
DMZ (Naranja)	NIC3	Privada	192.168.20.1/24

Fuente: Autoría Propia

6.4 ACTIVACIÓN DEL SERVICIO PROXY

Para habilitar el servicio proxy HTTP desde la interfaz web de Endian Firewall, se accedió a la opción Proxy HTTP y se activó el servicio marcando la casilla correspondiente.

Figura 24. Activación servicio Proxy en Endian



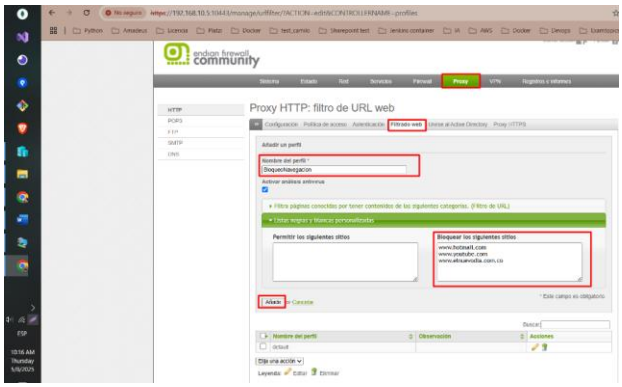
Fuente: Autoría propia.

Se seleccionó el modo “No Transparente” para las zonas GREEN (LAN) y ORANGE (DMZ), lo que implica que el navegador del cliente debe ser configurado manualmente para utilizar el proxy en la navegación. Esta configuración es requerida para poder aplicar la autenticación de usuarios.

6.5 CREACIÓN PERFIL FILTRADO WEB

Para crear el perfil de filtrado web o el perfil de acceso, se accedió a la sección de HTTP Proxy, seleccionado la pestaña de “Filtrado web”, se dio clic en “Añadir nuevo perfil”, y se estableció el nombre como “BloqueoNavegacion”.

Figura 25. Creación lista negra en el perfil de acceso



Fuente: Autoría propia.

En la sección de “Lista negra”, se incluyeron los siguientes dominios o sitios web para ser bloqueados:

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

Este perfil será utilizado para restringir la navegación de los usuarios autenticados en el proxy.

6.6 AUTENTICACIÓN LOCAL

Para implementar el control de acceso por grupo de usuarios locales o del proxy, se habilitó la autenticación local desde la sección Proxy Autenticación.

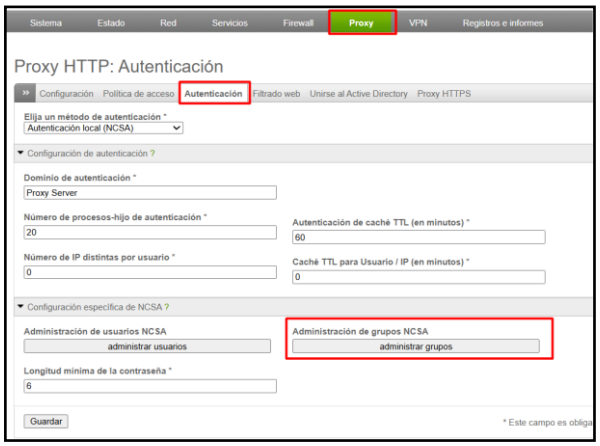
Se creó un usuario proxy o local (Vivianag) con su respectiva contraseña.

Figura 26. Creación del usuario local
Fuente: Autoría propia.

El usuario Vivianag fue asignado al grupo UsuariosProxy, lo cual resulta más eficiente, ya que permite aplicar una única política de acceso al grupo, haciendo que todos sus miembros hereden automáticamente dicha configuración.

Esto evita la necesidad de crear y gestionar políticas individuales para cada usuario.

Figura 27. Creación grupo del proxy



Fuente: Autoría propia.

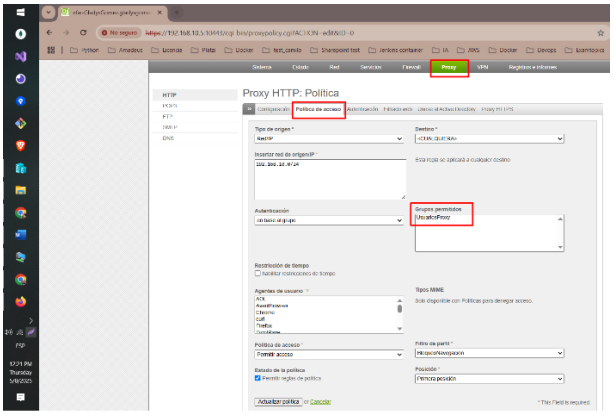
6.7 CREACIÓN DE POLÍTICA DE ACCESO CON AUTENTICACIÓN

En la sección Proxy se seleccionó “Política de acceso” se añadió una nueva política denominada "bloqueonavegacion".

Esta política permite la navegación desde la red interna únicamente a usuarios autenticados, aplicando las restricciones definidas en el perfil de filtro web, en el cual configuramos la lista negra.

Le indicamos que la autenticación sea basada por grupos y le asociamos el grupo “UsuariosProxy” que tiene como usuario a Vivianag.

Figura 28. Creación de política de acceso



Fuente: Autoría propia

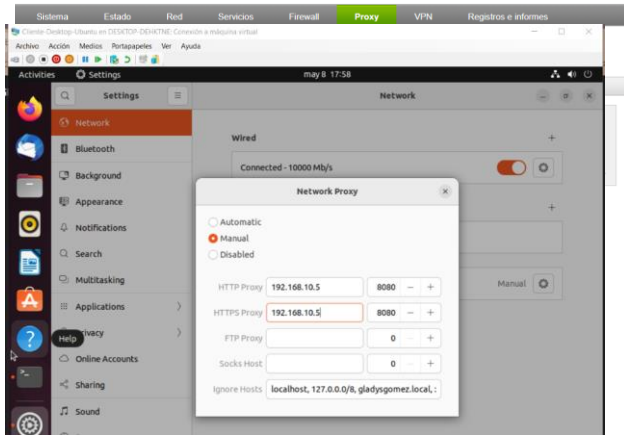
6.8 PRUEBA DESDE CLIENTE UBUNTU

La configuración del proxy en Ubuntu sigue las recomendaciones de la guía oficial [7].

La prueba se realizó en la máquina cliente (Cliente-Ubuntu-Desktop [7]) conectada a la red LAN.

Para ello nos vamos al settings y realizamos la configuración manual de proxy en Ubuntu 22.04 LTS [7], en la sección de “Network Proxy” activamos la opción, con HTTP Proxy y HTTPS Proxy ambos apuntando a la dirección 192.168.10.5 y puerto 8080.

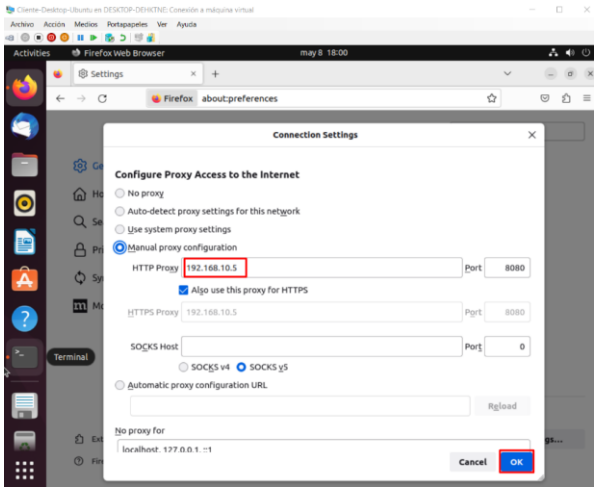
Figura 29. Configuración manual del proxy en Ubuntu desktop



Fuente: Autoría propia

Esta configuración manual es necesaria para que el tráfico de la máquina cliente sea redirigido a través del proxy HTTP configurado en Endian, permitiendo así aplicar las políticas de autenticación y filtrado establecidas.

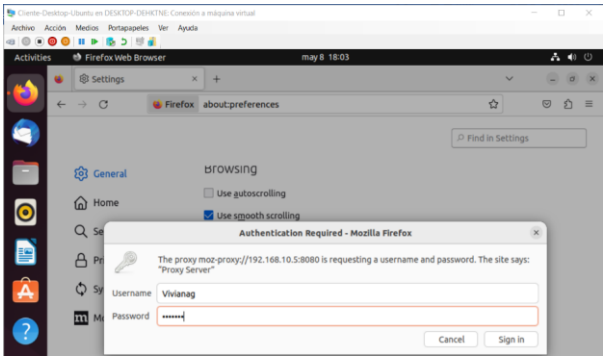
Figura 30. Configuración del proxy en Firefox



Fuente: Autoría propia.

Al intentar acceder a cualquier sitio web, el navegador solicitó autenticación.

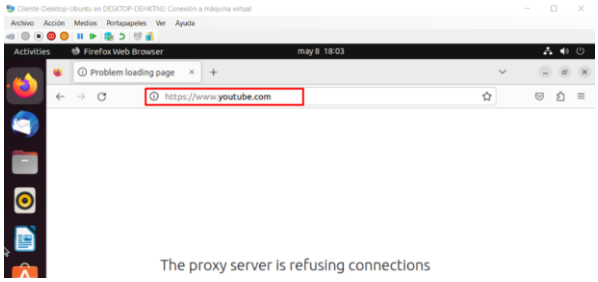
Figura 31. Ingreso de usuario y clave en el Firefox



Fuente: Autoría propia.

Tras ingresar el usuario, se permitió la navegación hacia sitios no bloqueados, mientras que los sitios incluidos en la lista negra fueron correctamente restringidos, validando así el funcionamiento de las políticas establecidas.

Figura 32. Bloqueo proxy dominio de la lista negra



Fuente: Autoría propia.

7 CONCLUSIONES

Estas configuraciones se alinean con las prácticas recomendadas en la administración de sistemas Debian [9].

La implementación de NAT en Endian Firewall permitió que las redes internas (LAN y DMZ) pudieran salir a Internet de manera segura, sin exponer sus direcciones privadas.

El uso de reglas automáticas y el reenvío de puertos facilitó la gestión del tráfico, demostrando que Endian es una herramienta funcional y efectiva para controlar el enrutamiento y el acceso desde entornos segmentados

Con el desarrollo de esta actividad se comprende la importancia de los servicios y la seguridad dentro del sistema operativo Linux, destacando su relevancia en el funcionamiento de redes, servidores y otros componentes del sistema.

Estas parametrizaciones, aunque puedan parecer técnicas y detalladas, representa la primera línea de defensa contra accesos no autorizados y ataques cibernéticos.

Herramientas como iptables, nftables, ufw y firewalld brindan al profesional de TI un control total sobre el tráfico, permitiendo garantizar la integridad y disponibilidad de los servicios en un entorno Open Source.

Este tipo de configuraciones fortalecen la seguridad perimetral en redes Linux y fomentan buenas prácticas en administración de sistemas.

La implementación del proxy HTTP no transparente en Endian Firewall permitió establecer un control preciso sobre la navegación en la red local, exigiendo autenticación por usuario antes de acceder a Internet.

A través de la creación de perfiles de filtrado, políticas de acceso y mecanismos de autenticación local, fue posible restringir sitios específicos y monitorear el uso del servicio web proxy.

Esta configuración demuestra que Endian es una herramienta robusta y versátil para la gestión de seguridad perimetral, incluso en entornos virtuales.

El desarrollo de los laboratorios, refuerzan la importancia del conocimiento en administración de servicios y la seguridad como una competencia fundamental para cualquier profesional del área de sistemas, especialmente en ambientes donde Linux es la plataforma principal.

El conocimiento y la correcta implementación de reglas de acceso son competencias clave para todo administrador de sistemas Linux.

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

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

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

[11] NetSet, "*Install Endian Firewall step by step*," YouTube, Aug. 29, 2017. [Online]. Available: https://www.youtube.com/watch?v=f2gPg0_8dLw

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

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