IMPLEMENTACIÓN INTEGRAL DE ENDIAN FIREWALL: CONFIGURACIÓN EN UNA RED SIMULADA APLICANDO SEGMENTACIÓN, NAT, POLÍTICAS DE ACCESO Y FILTRADO WEB

Alejandro Ospina Escobar
e-mail: aospinae@unadvirtual.edu.co
Katherine Sánchez Molano
e-mail: ksanchezmo@unadvirtual.edu.co
Andrés Mauricio Valencia López
e-mail: amvalencialop@unadvirtual.edu.co
Erick Suarez Naranjo
e-mail: esuarezn@unadvirtual.edu.co

RESUMEN: *El presente informe técnico detalla la implementación y configuración del firewall Endian sobre un entorno virtualizado en VirtualBox, estructurando el trabajo alrededor de la seguridad perimetral y el control de tráfico. Inicialmente, se establece una arquitectura de red segmentada utilizando la zona verde (LAN), roja (WAN) y naranja (DMZ), esencial para fortalecer la seguridad y optimizar la comunicación interzonal. Posteriormente, el proceso aborda la configuración de reglas de traducción de direcciones (SNAT y DNAT) para gestionar la publicación segura de servicios internos, como servidores web, sin comprometer la integridad de la red local. Finalmente, el informe cubre la definición de políticas de acceso detalladas, incluyendo la activación controlada de servicios (HTTP y FTP) y medidas preventivas (bloqueo de ICMP), junto con la implementación de un proxy HTTP no transparente con autenticación, permitiendo así un control granular y exhaustivo del tráfico web saliente.*

PALABRAS CLAVE: Dirección IP, LAN, WAN, DMZ, Interfaz de red, Máquina Virtual, Firewall, NAT, DNAT, SNAT, ICMP, FTP, Proxy HTTP, Endian Firewall, autenticación, filtrado web.

1 INTRODUCCIÓN

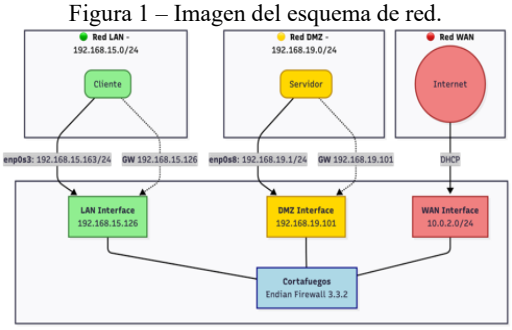
Históricamente, la seguridad perimetral surgió como una estrategia defensiva fundamental en la arquitectura de redes, inspirada en las fortificaciones físicas donde la protección se concentraba en el límite de la red. En esta evolución, el cortafuegos (firewall) se consolidó como la herramienta central, actuando como un punto de control que filtra y regula todo el tráfico entre la red interna (confiable) y las redes externas (no confiables). Su función es esencialmente aplicar políticas de seguridad predefinidas para decidir qué tráfico debe ser permitido, denegado o modificado.

El proyecto se inicia con la correcta configuración e instalación de la instancia GNU/Linux Endian y el establecimiento de una arquitectura de red segmentada utilizando la zona verde (LAN), roja (WAN) y naranja (DMZ). El núcleo del trabajo se centra en la aplicación de políticas de seguridad exhaustivas: desde la configuración de reglas de traducción de direcciones (SNAT y DNAT) para la publicación controlada de servicios, hasta la definición de reglas de acceso inter-zona que permiten la comunicación de protocolos esenciales como HTTP y FTP, mientras se deniega el tráfico no esencial (e.g., ICMP). Finalmente, se implementa un Proxy HTTP no transparente con autenticación, lo que permite la creación de perfiles de usuario y la aplicación de listas negras para asegurar un control granular y una trazabilidad completa del tráfico web saliente en la red interna.

2 DESARROLLO

Inicialmente se debe plantear el diagrama de red el cual será implementando en la infraestructura simulada teniendo presente las zonas que se encuentran segmentadas por su tipo (LAN, DMZ y WAN) como también por su color (VERDE, NARANJA, ROJO) para así ejecutar una planeación y proceder con la creación, modificación, restricción y activación de servicios y/o reglas que permitan o denieguen el tráfico mediante temáticas ya definidas para aprender a no solo usar una herramienta de cortafuegos sino también a comprender el funcionamiento de una red totalmente aislada manteniendo una seguridad y confiabilidad en una infraestructura simulada.

Figura 1 – Imagen del esquema de red.



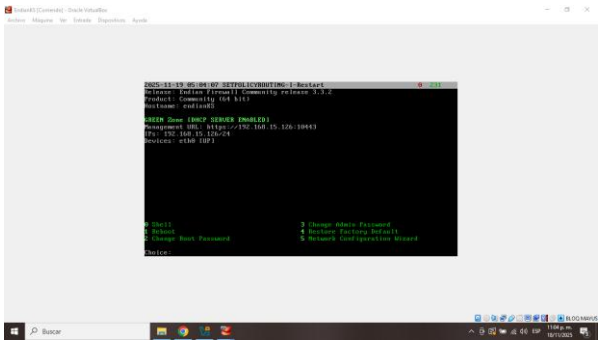
Fuente: Autoría Propia.

2.1 TEMÁTICA 1: Configuración de la instancia para GNU/Linux Endian en VirtualBox (tarjetas de red) e instalación efectiva del mismo

Realizamos la descarga, instalación y configuración de la distribución GNU/Linux Endian en VirtualBox. Posteriormente en VirtualBox realizamos la configuración de red habilitando el primer interfaz para la zona verde, la segunda interfaz para la

red naranja y la tercera para la red roja, guardamos la configuración e iniciamos el proceso de arranque de la máquina, en este proceso nos solicita la dirección IP de la zona verde que en este caso trabajaremos con 192.168.15.126/24 y con su mascara por defecto, terminamos el proceso y visualizamos la Fig. 2 donde evidencia los datos de la zona verde.

Figura 2 – Imagen de la finalización de la configuración inicial de Endian.

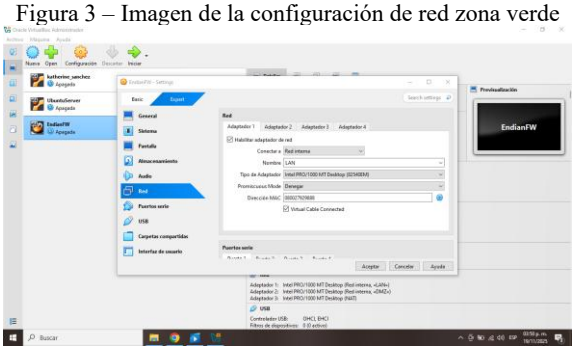


Fuente: Autoría Propia.

2.1.1 Implementación zona verde

Inicialmente configuramos la máquina virtual Endian Firewall la sección de red habilitando la interfaz de red eth0 como red interna para establecer la LAN, visualizamos esta configuración en la Fig. 3. Posteriormente iniciamos la máquina virtual para realizar configuración de red desde la consola en está no solicita las direcciones IPs de las 3 zonas y habilitamos DCHP.

Figura 3 – Imagen de la configuración de red zona verde

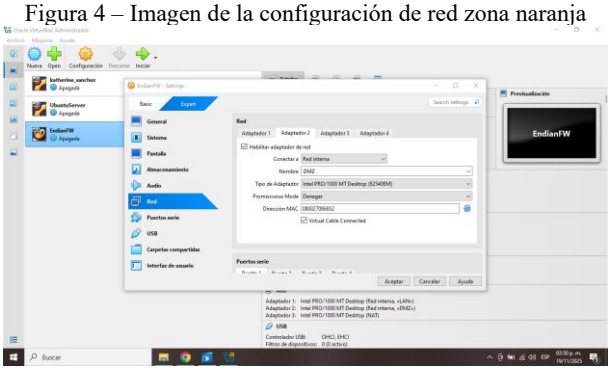


Fuente: Autoría Propia.

2.1.2 Implementación zona naranja

En la sección de red configuramos la máquina virtual Endian Firewall habilitando la interfaz de red eth1 como red interna para establecer la DMZ, visualizamos esta configuración en la Fig. 4. Posteriormente iniciamos la máquina virtual para realizar configuración de red desde la consola.

Figura 4 – Imagen de la configuración de red zona naranja

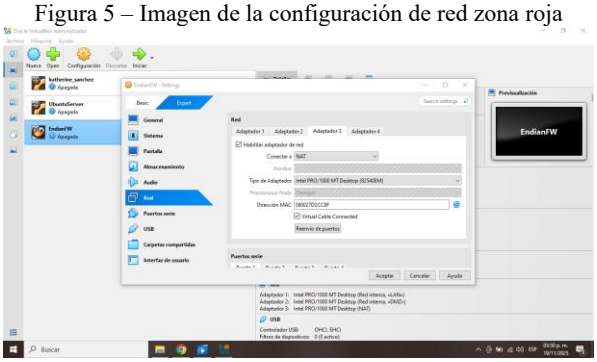


Fuente: Autoría Propia.

2.1.3 Implementación zona roja

Configuramos la máquina virtual Endian Firewall la sección de red habilitando la interfaz de red eth2 como red interna para establecer la WAN, visualizamos esta configuración en la Fig. 5. Posteriormente iniciamos la máquina virtual para realizar configuración de red desde la consola.

Figura 5 – Imagen de la configuración de red zona roja

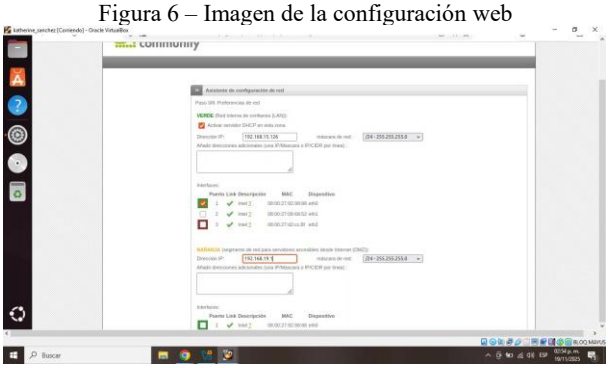


Fuente: Autoría Propia.

2.1.4 Configuración

Ingresamos desde el navegador en Ubuntu desktop por medio de https://192.168.15.126 por el puerto 10443 para realizar la configuración de red restante, se evidencia en las Fig. 6, 7 y 8.

Figura 6 – Imagen de la configuración web

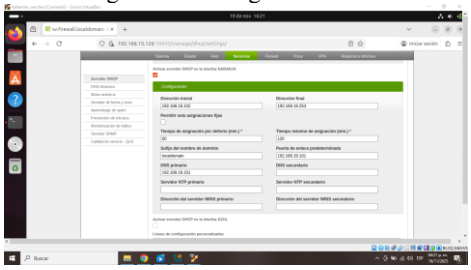


Fuente: Autoría Propia.

Figura 7 – Imagen de la configuración web zona verde

Fuente: Autoría Propia.

Figura 8 – Imagen de la configuración web zona naranja

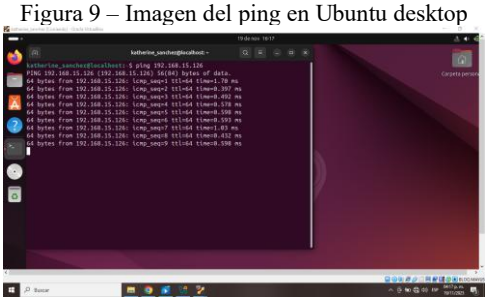


Fuente: Autoría Propia.

2.1.5 Validación de conectividad

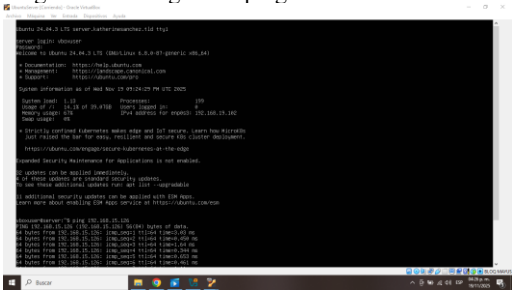
Para verificar que la red está conectada ingresamos al Ubuntu desktop y por medio de la consola realizamos ping al Endian por 192.168.15.126 y lo mismo hacemos para el servidor Ubuntu. Se visualiza en las Fig. 9 y 10.

Figura 9 – Imagen del ping en Ubuntu desktop



Fuente: Autoría Propia.

Figura 10 – Imagen del ping en el servidor Ubuntu



Fuente: Autoría Propia.

2.2 TEMÁTICA 2: Configuración NAT.

Durante la planeación para la implementación de las reglas NAT solicitadas, se ejecutó la instalación y configuración de una máquina virtual sobre VirtualBox con una imagen en formato ISO de Endian Firewall v3.3.2 asignando tres (3) interfaces de red: **eth0** identificado como **enp0s3** dentro del segmento LAN (Verde), **eth1** identificado enp0s8 dentro del segmento DMZ (Naranja) y **eth2** identificado como Etapa7 dentro del segmento WAN (Rojo). El esquema de red anteriormente señalado se encuentra de forma detallada como se visualiza en la Fig. 1 para tener una arquitectura simulada lo más organizada y funcional posible para así garantizar una correcta aplicación de las reglas NAT.

2.2.1 Definición de reglas.

Inicialmente se plantea la definición de dos (2) reglas en las cuales se intervienen las zonas LAN a WAN y DMZ a WAN permitiendo la resolución de dominios y peticiones de conectividad hacia internet. De acuerdo con el esquema generado como diagrama de red en la Fig. 1 el cortafuegos de Endian permite segmentar las zonas asociadas en donde tenemos:

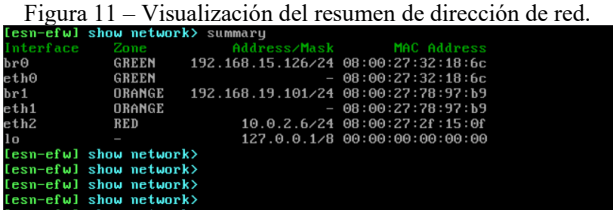
- LAN (Verde) con segmento de red estático **192.168.15.0/24** donde se encuentra la maquina "Desktop" o "Cliente".
- DMZ (Naranja) con segmento de red estático **192.168.19.101/24** donde se aloja los servidores como el "Server" exponiendo servicios como aplicaciones web.
- WAN (Rojo) con segmento de red con DHCP **10.0.2.0/24** sobre VirtualBox el cual permite crear una red simulada para permitir el acceso a NAT.

En este orden de ideas se debe configurar el Endian Firewall para que se establezca la configuración y la asignación de interfaces correspondientes de acuerdo con el esquema inicialmente definido.

2.2.2 Configuración.

Una vez teniendo presente las reglas propuestas a implementar, así como también la arquitectura de red como identificadores, tipos de red (interna, nat, bridge) como también máquinas y servicios a intervenir se procede a ejecutar las configuraciones oportunas. Tener presente que Endian Firewall una vez se configura las interfaces de red automáticamente crea interfaces tipo bridge que están asociadas a la zona LAN como a la DMZ por lo que podemos identificarlas de una manera más puntual relacionándolas según su dirección MAC asignada.

Figura 11 – Visualización del resumen de dirección de red.



Fuente: Autoría Propia.

En el momento que se está realizando la configuración de las zonas también se debe asignar una dirección IP disponible

que se encuentre dentro del segmento de red según su zona, en este caso y acorde con el esquema de red se asignaría así:

- **Interfaz LAN**: Dirección 192.168.15.126/24, es importante tener presente ya que está actúa como gateway de la zona verde.
- **Interfaz DMZ**: Dirección 192.168.19.101/24, es importante tener presente ya que está actúa como gateway de la zona naranja.
- **Interfaz WAN**: Dirección 10.0.2.x/24, es importante tener presente ya que está actúa como la zona roja, a la par que está interfaz tiene activo DHCP.

Ahora, para configurar la primera regla que comprende la zona LAN (Verde) hacia la zona WAN (Roja) se debe ingresar al panel web del cortafuegos accediendo directamente desde la maquina "cliente" o "desktop" por el puerto **10443**, es decir https://192.168.15.126:10443 con el usuario "admin" el cual es generado por defecto al momento de realizar la instalación de Endian Firewall.

Desde el panel de control web del Endian Firewall nos redireccionamos a la pestaña Firewall → Redirección de puertos / NAT → NAT fuente o Source NAT (SNAT) en esta sección se podrá crear, modificar, y eliminar cualquiera regla de trafico de origen privado de una zona hacia una red pública como internet gracias al protocolo de traducción (NAT).

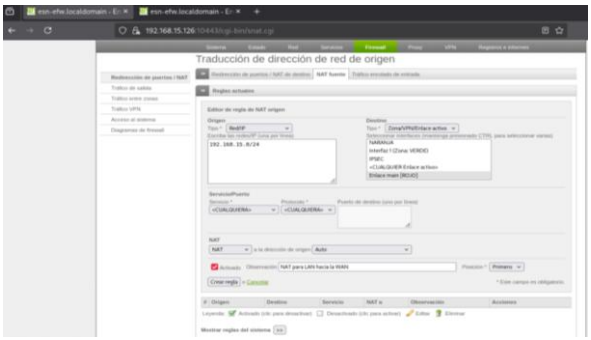
Figura 122 – Visualización de las reglas SNAT

Fuente: Autoría Propia.

Al crear una nueva regla se presentará campos que se deben diligenciar:

- **Origen:** Se debe digitar la dirección de red, en este caso la zona LAN (192.168.15.0/24)
- **Destino:** Aplicaría para la zona roja (WAN) para permitir la salida del tráfico hacia internet.
- **Servicio/Puerto:** Será cualquiera ya que no se estaría aplicando alguna restricción.
- NAT: Se aplicaría NAT de forma automática para la salida hacia internet.
- **Descripción:** Nos ayuda a identificar el propósito de la regla.
- **Posición:** Es importante tener presente la posición porque permite tener prioridad de una regla sobre otra.

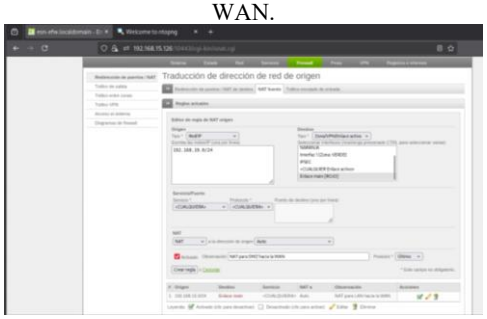
Figura 13 – Creación de regla SNAT de la zona LAN hacia la WAN.



Fuente: Autoría Propia.

Una vez creada la regla se debe replicar una regla con la misma estructura pero que permita el tráfico de la zona DMZ como origen y destino la zona WAN:

Figura 14 – Creación de regla SNAT de la zona DMZ hacia la WAN.



Fuente: Autoría Propia.

Como se puede observar en la Fig. 14 los campos diligenciados se replica como en la regla creada previamente donde se interviene la zona LAN hacia la zona WAN, pero esta vez se modifica el origen como también su descripción.

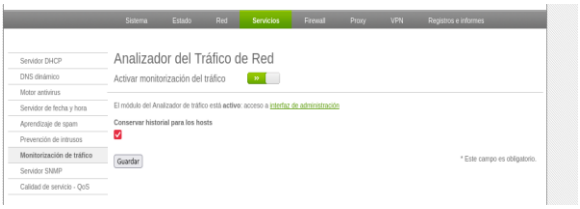
2.2.3 Pruebas de conectividad y visualización de las reglas creadas.

De acuerdo con las reglas SNAT creadas observando la Fig. 13 y Fig. 14 se debe realizar una prueba de conectividad desde las zonas origen como lo es la LAN y la zona DMZ para así comprobar que las reglas creadas en el cortafuegos estén funcionando de manera óptima. En este orden de ideas el objetivo es verificar la correcta implementación de las reglas por consiguiente se podría realizar de diferentes formas, para evaluar su funcionalidad.

- **LAN a WAN:** Para la prueba se utilizó la herramienta nativa "ntop" la cual se puede habilitar desde la opción "Servicios" → Monitorización de Trafico y activar el servicio. Una vez activo se puede seleccionar el host a monitorear para así verificar que peticiones de red ha realizado.
- **DMZ a WAN:** Se ejecutó la prueba de conectividad con la herramienta nativa "ping" directamente desde el host "Server" hacia los DNS de Google por medio de su dominio (Google.com) de esta manera

confirmando dos (2) premisas: La correcta resolución de dominios y la conectividad hacia redes públicas como lo es internet.

Figura 15 – Activación del servicio de analizador de trafico de red.

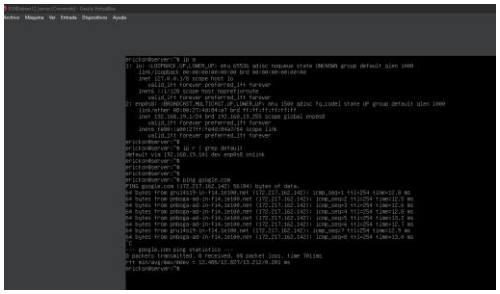


Fuente: Autoría Propia.

Figura 16 – Visualización de tráfico del host "Desktop" con ntop hacia internet.

Fuente: Autoría Propia.

Figura 17 – Prueba de conectividad mediante el comando ping desde el host "Server" hacia internet.



Fuente: Autoría Propia.

Así se logra consolidar de forma eficaz las reglas SNAT solicitadas mediante el enmascaramiento de direcciones IP privadas hacia la zona WAN configuradas en la zona LAN y DMZ con las pruebas de conectividad que confirman la correcta implementación de las reglas solicitadas. Cabe resaltar que el orden de las reglas creadas es algo importante en lo que respecta a su ejecución, en este caso como primera (1) regla se estableció la zona LAN debido a que generalmente los usuarios finales son quienes consumen más tráfico saliente hacia internet a diferencia de la segunda (2) regla que abarca la zona DMZ incluyendo los servidores quienes no generan tanto tráfico prominente a redes públicas ya que generalmente son redes privadas como intranets.

Figura 18 – Visualización de las reglas.

Fuente: Autoría Propia.

2.3 TEMÁTICA 3: Permitir servicios de la zona DMZ para la red.

El objetivo de la temática tres (3) fue configurar la distribución GNU/Linux Endian Firewall para permitir servicios desde la zona DMZ hacia la red LAN, fortaleciendo la seguridad perimetral mediante reglas de acceso y bloqueo específicas. Se trabajó con un servidor Ubuntu Server en la zona naranja (DMZ) y un cliente Ubuntu Desktop en la zona verde (LAN).

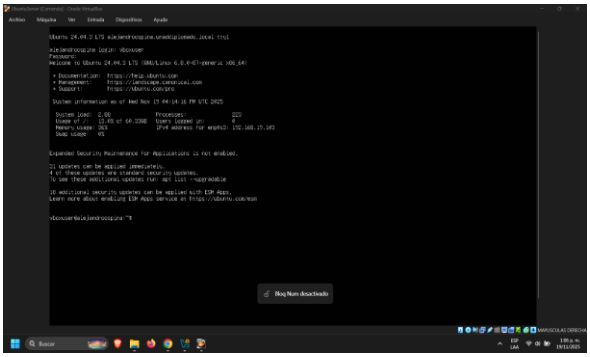
2.3.1 Descripción de la Topología Implementada.

- Zona VERDE (LAN): 192.168.15.126/24
- Zona NARANJA (DMZ): 192.168.19.101/24
- Zona ROJA (WAN/NAT): acceso a Internet

2.3.2 Configuración del Servidor Ubuntu en la DMZ.

En este paso se verifica la dirección IP asignada a él Ubuntu servidor por medio de la red naranja, en este caso se le asigno la dirección IP 192.168.19.103 como se puede visualizar en la Fig. 19. También verificamos el funcionamiento de los servicios http y ftp desde los puertos 80 y 21, véase Fig. 20.

Figura 19 – Verificación de dirección IP asignada al servidor



Fuente: Autoría Propia.

Figura 20 – Verificación de los servicios http y ftp.

Fuente: Autoría Propia.

2.3.3 Configuración del Firewall en Endian.

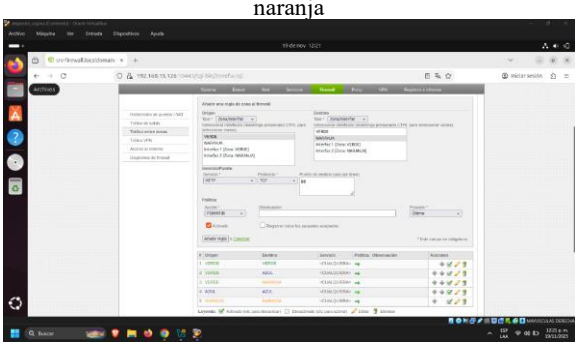
Para realizar la configuración del firewall por medio de la herramienta debes establecer las siguientes reglas, cuando hacemos este proceso creamos la regla para permitir acceso http puerto 80 de la zona verde a la naranja, véase Fig.21, además creamos la regla para permitir acceso ftp puerto 21 de la zona verde a la naranja. véase Fig.22.

2.3.3.1 Permitir servicio HTTP (Puerto 80)

Se creó una regla en Firewall → Tráfico entre Zonas.

- Origen: VERDE
- Destino: NARANJA
- Servicio: HTTP
- Acción: PERMITIR

Figura 21 – Creación de la regla para permitir acceso http zona naranja



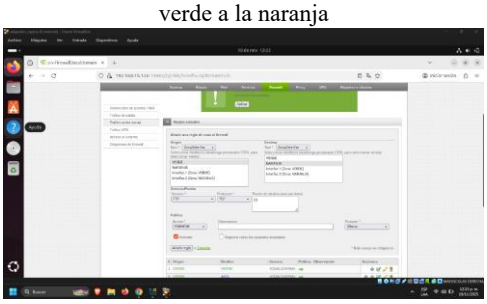
Fuente: Autoría Propia.

2.3.3.2 Permitir servicio FTP (Puerto 21)

Regla ubicada en Firewall → Tráfico entre Zonas.

- Origen: VERDE
- Destino: NARANJA
- Servicio: FTP
- Acción: PERMITIR

Figura 22 – Creación de la regla para permitir acceso ftp zona verde a la naranja



Fuente: Autoría Propia.

2.3.4 Bloqueo del Protocolo ICMP.

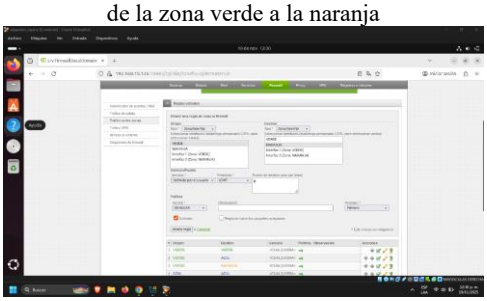
Para el bloqueo de protocolo se debe realizar el siguiente proceso de establecimiento de reglas en la herramienta: Creación de la regla para bloquear acceso ICMP puerto 8 de la zona verde a la naranja por medio de ping, véase Fig. 23, y seguido de esto se crea la regla para bloquear acceso ICMP puerto 30 de la zona verde a la naranja por medio de ping, véase Fig. 24.

2.3.4.1 Creación de regla de bloqueo ICMP puerto 8

Se creó una regla en Firewall → Tráfico entre Zonas.

- Origen: VERDE
- Destino: NARANJA
- Servicio: ICMP
- Acción: DENEGAR

Figura 23 – Creación de la regla para bloquear acceso puerto 8 de la zona verde a la naranja



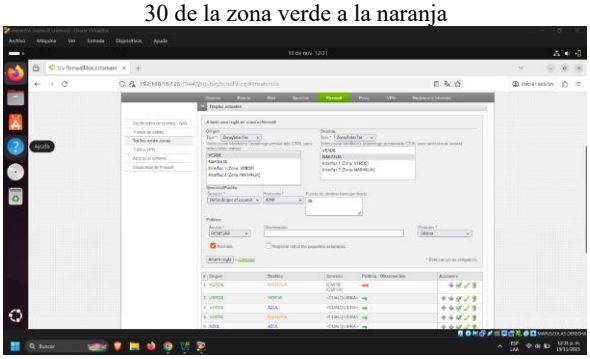
Fuente: Autoría Propia.

2.3.4.2 Creación de regla de bloqueo ICMP puerto 30

Se creó una regla en Firewall → Tráfico entre Zonas para así definir cada una de ellas para controlarlas por medio de las reglas.

- Origen: VERDE
- Destino: NARANJA
- Servicio: ICMP
- Acción: DENEGAR

Figura 24 – Creación de la regla para bloquear acceso puerto 30 de la zona verde a la naranja



Fuente: Autoría Propia.

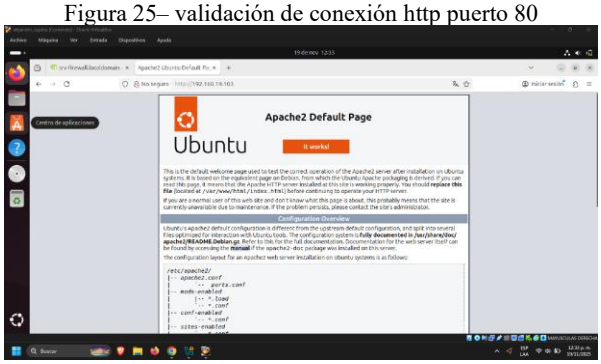
2.3.5 Funcionamiento de las reglas entre zonas

Para verificar que las reglas previamente establecidas funcionen se muestran las siguientes validaciones por el puerto 80 para el acceso http, véase Fig. 25. y por el puerto 21 para el acceso ftp, véase Fig. 26. Además, se valida el bloqueo ICMP desde el puerto 8 y 30, véase Fig. 27.

2.3.5.1 Funcionamiento de la regla de acceso HTTP puerto 80

Para esta regla desde el Ubuntu desktop conectado a la zona verde se accede desde el navegador web que en este caso es Mozilla Firefox y se ingresa desde la barra de direcciones usando la dirección IP del Ubuntu servidor dirección IP 192.168.19.103 conectado a la zona naranja y que tiene activado el servicio de http con el puerto 80 por defecto.

Figura 25– validación de conexión http puerto 80

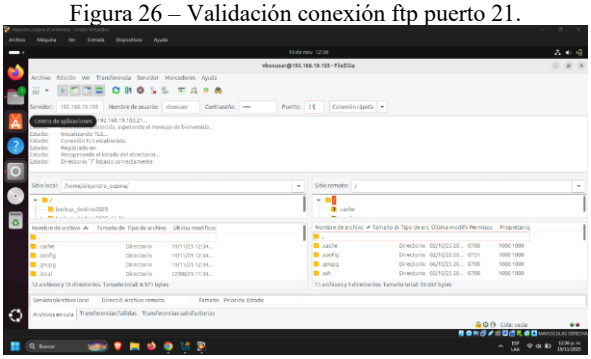


Fuente: Autoría Propia.

2.3.5.2 Funcionamiento de la regla de acceso FTP puerto 21

Para esta regla desde el Ubuntu desktop conectado a la zona verde se accede desde el aplicativo ftp que en este caso es FileZilla y se usa los datos de ingreso usando la dirección IP del Ubuntu servidor dirección IP 192.168.19.103 conectado a la zona naranja y que tiene activado el servicio de ftp con el puerto 21 por defecto.

Figura 26 – Validación conexión ftp puerto 21.



Fuente: Autoría Propia.

2.3.5.3 Funcionamiento de la regla de bloqueo ICMP desde los puertos 8 y 30

Para esta regla desde el Ubuntu desktop conectado a la zona verde se accede desde la terminal del sistema operativo y se usa el comando ping usando la dirección IP del Ubuntu servidor conectado a la zona naranja y que tiene bloqueado desde Endian Firewall los puertos 8 y 30 para hacer ping y se demuestra que si hace ping a él firewall Endian y que Ubuntu desktop se encuentra en la otra red mostrando la dirección IP.

Figura 27 – Se muestra el funcionamiento del bloqueo ICMP.

Fuente: Autoría Propia.

2.4 TEMÁTICA 5: Implementar un proxy HTTP (No transparente) con políticas de autenticación para navegación en internet.

Está temática tuvo como objetivo habilitar e implementar un proxy HTTP no transparente en Endian Firewall, realizando desde cero la configuración del filtrado web y los mecanismos de autenticación que permiten tener un control específico sobre la navegación de los usuarios en una red interna. Este tipo de funcionalidades regulan, controlan y administran la forma en la que se fortalece la seguridad perimetral, evitando accesos no autorizados y garantizando la navegación dentro de una estructura corporativa o empresarial cumpla con políticas previamente definidas y establecidas.

2.4.1 Descripción de la topología implementada

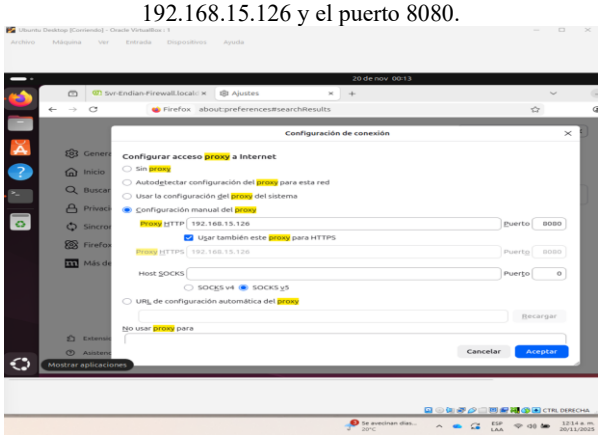
La configuración se realizó siguiendo la arquitectura de red definida en las temáticas anteriores, segmentando de la misma manera las zonas:

- **Zona VERDE (LAN):** 192.168.15.0/24

- **Zona NARANJA (DMZ):** 192.168.19.0/24
- **Zona ROJA (WAN):** Servicio DHCP.

El proxy HTTP se activó para las zonas VERDE y NARANJA, de forma no transparente lo que implica que en cada uno se debe configurar de manera manual el proxy en el navegador que esté utilizando o en el proxy de internet del sistema operativo para estandarizar el acceso a Internet.

Figura 28 – Se muestra la configuración manual del proxy en el navegador Mozilla Firefox especificando la dirección IP 192.168.15.126 y el puerto 8080.



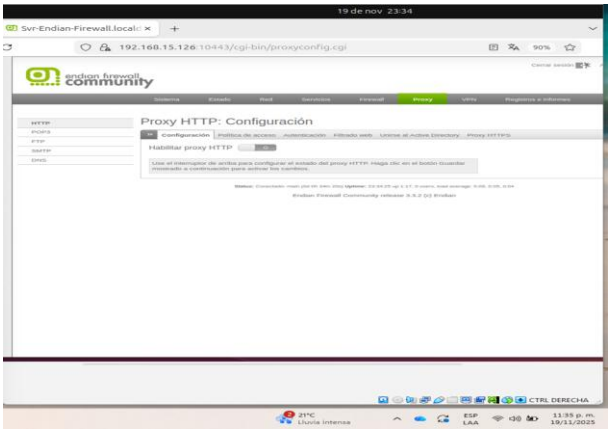
Fuente: Autoría Propia.

La configuración manual del proxy permite que todo el tráfico HTTP salga obligatoriamente autenticado, supervisado y filtrado.

2.4.2 Activación del Proxy HTTP y configuración inicial

Accedemos a la interfaz web del Endian Firewall, donde procedemos habilitar el proxy HTTP mediante la ruta: Proxy -> Proxy HTTP.

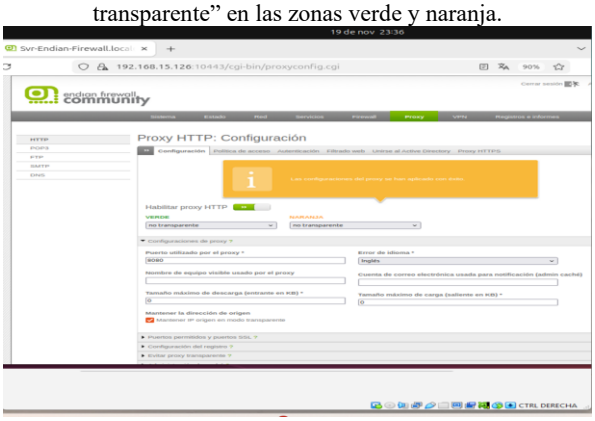
Figura 29 – Habilitación de Proxy HTTP: Configuración desde la interfaz web del Endian Firewall.



Fuente: Autoría Propia.

Una vez activado, se procede a establecer el modo "No transparente" en las zonas VERDE y NARANJA. Y se confirma que el puerto 8080 sea el asignado para la operación del servicio.

Figura 30 – Configuración del proxy HTTP de modo "No transparente" en las zonas verde y naranja.



Fuente: Autoría Propia.

2.4.3 Configuración del filtrado web

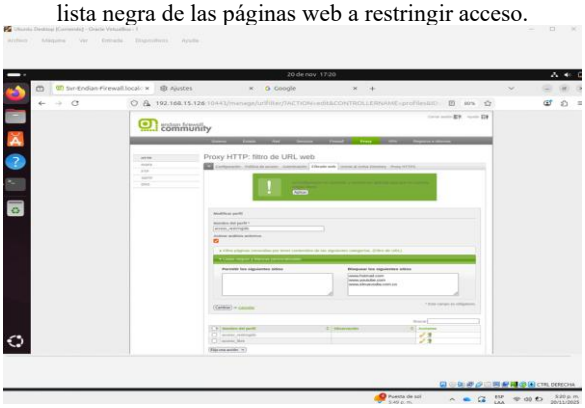
Para poder aplicar el control y la restricción de las páginas web, se debe crear un perfil de filtrado específico en:

- Proxy -> Filtrado web -> Añadir nuevo perfil

Donde se definen dos perfiles:

1. acceso_restringido: Bloquea los paginas web que se incluyen en la lista negra: www.hotmail.com, www.youtube.com, www.elnuevodia.com.co
2. acceso_libre: Permite el acceso total a Internet sin restricciones y no se especifica ninguna página web en la lista blanca o negra.

Figura 31 – Personalización de perfil de filtrado listando la lista negra de las páginas web a restringir acceso.



Fuente: Autoría Propia.

Los perfiles de filtrado son utilizados como método de filtrado en las políticas de acceso.

2.4.4 Administración de usuarios y grupos

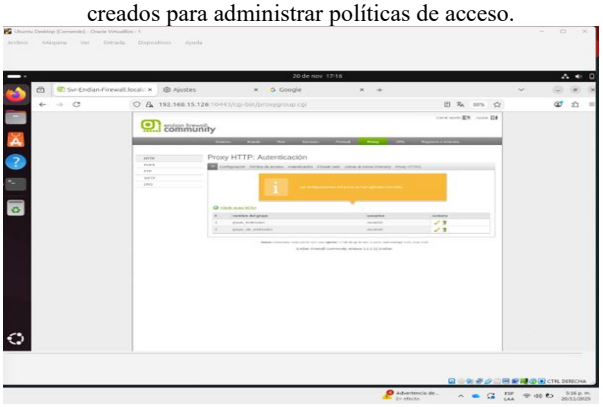
Para poder habilitar la autenticación de usuarios, debemos ir a la siguiente ruta: Proxy -> Autenticación

Luego se realiza la creación de:

- **Usuarios:** cada uno con credenciales de acceso al proxy.

- **Grupos:** se vinculan los usuarios según el nivel de acceso requerido.

Figura 32 – Creación de grupos y vinculación de usuarios creados para administrar políticas de acceso.



Fuente: Autoría Propia.

De esta forma, se implementa un control basado en perfiles, permitiendo que los usuarios de distintos grupos puedan tener permisos diferenciados.

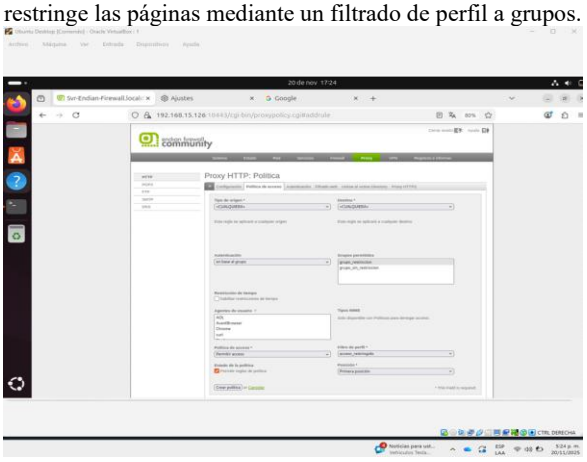
2.4.5 Creación de la política de acceso al proxy

Para realizar la creación de la política de acceso, debemos dirigirnos a la ruta: Proxy -> Política de acceso.

Los parámetros que se deben establecer son:

- Origen y destino: Cualquiera
- Autenticación: Basada en grupo
- Grupo permitido: grupo_restriccion
- Política de acceso: Permitir acceso
- Filtro de perfil: acceso_restringido

Figura 33 – Parametrización de la política de acceso que restringe las páginas mediante un filtrado de perfil a grupos.



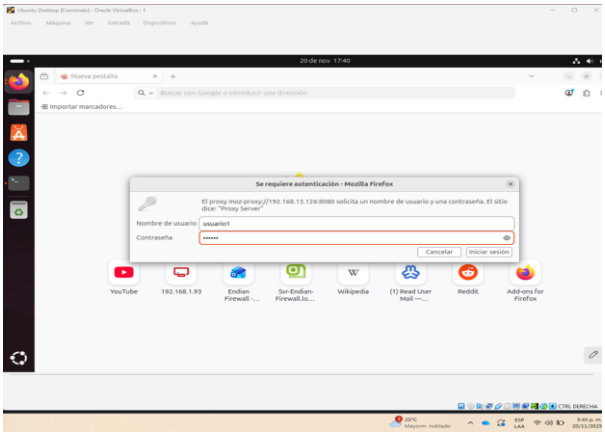
Fuente: Autoría Propia.

Con esta política de acceso, todos los usuarios que hagan parte del grupo (grupo_restriccion) quedan sujetos al filtrado definido, incluyendo las restricciones dadas en la lista negra.

2.4.6 Prueba de funcionamiento de política acceso

Para las pruebas debemos realizar la configuración manual del proxy HTTP en el navegador, como se referenció en la figura 28. Una vez habilitado el proxy, procedemos autenticarnos con el perfil usuario1, el cual hace parte del grupo_restriccion, el cual aplica la política de acceso de filtrado web acceso_restringido con las páginas de la lista negra.

Figura 34 – Autenticación de usuario y contraseña al proxy HTTP.

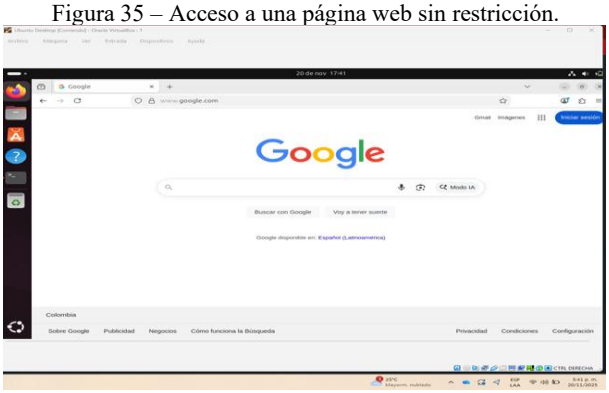


Fuente: Autoría Propia.

2.4.6.1 Navegación permitida

Después de la autenticación con un usuario válido, se realiza acceso a páginas que no hacen parte de la lista negra para evidenciar la navegación, en este caso al sitio www.google.com.co

Figura 35 – Acceso a una página web sin restricción.

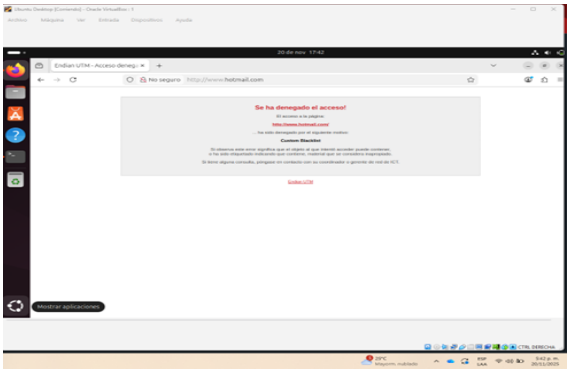


Fuente: Autoría Propia.

2.4.6.2 Bloqueo de la lista negra

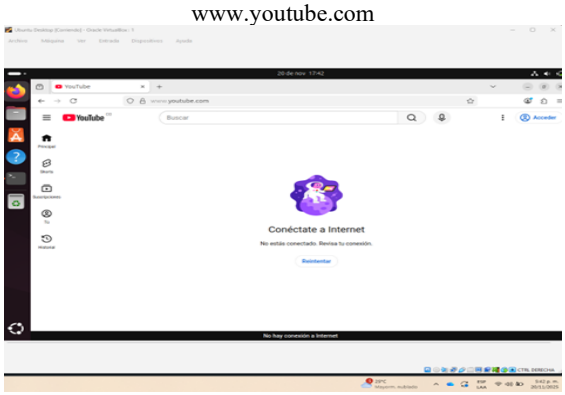
Posteriormente, se realiza intento de acceso a las páginas que hacen parte de la lista negra, el cual Proxy denegó el acceso conforme a la configuración del perfil de filtrado: acceso_restringido.

Figura 36 – Denegación de acceso a la página web www.hotmail.com



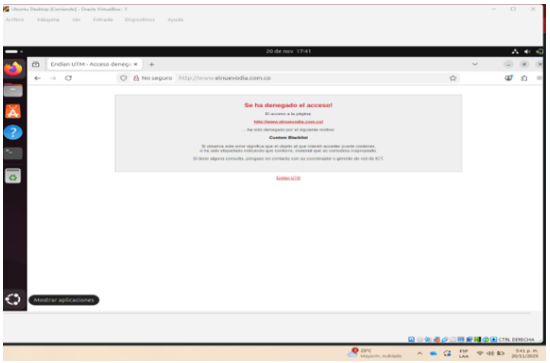
Fuente: Autoría Propia.

Figura 37 – Denegación de acceso a la página web www.youtube.com



Fuente: Autoría Propia.

Figura 38 – Denegación de acceso a la página web www.elnuevodia.com.co



Fuente: Autoría Propia.

3 CONCLUSIONES

3.1 TEMÁTICA 1

En el desarrollo de la guía el proceso de instalación e implementación de GNU/Linux Endian para la zona verde (LAN), zona naranja (DMZ) y zona roja (WAN), nos permitió establecer la conexión de red de máquinas virtuales de distribuciones de escritorio y de servidor por medio de VirtualBox, para prepáranos a un entorno real de como configurar un firewall empresarial, lo que nos permitió adquirir habilidades para el campo laboral por medio de conceptos de infraestructura, ciberseguridad, redes corporativas y nube. Además, Endian es una herramienta practica y apropiada para el desarrollo de las temáticas planteadas, debido a su facilidad de uso, descarga, instalación y configuración inicial, todo el proceso necesario para el desarrollo de la temática uno (1) nos brindó la posibilidad de aprendizaje real y nos permitió afianzar los conocimientos obtenidos mediante la parte teórica.

3.2 TEMÁTICA 2

De acuerdo con la ejecución y desarrollo realizado en la temática dos (2) donde se plantea una solución de configuración de reglas interviniendo las zona de área local (LAN), desmilitarizada (DMZ) y la red de área extensa (WAN) a través del uso de protocolo SNAT (Traducción de Direcciones de Red de Origen) el cual permite que la dirección IP que abarca la zona LAN y DMZ como también el puerto del tráfico origen se reescriba para así lograr dirigir hacia la WAN para que simule originarse de una dirección IP Pública de esta manera logrando la comunicación entre otras redes como Internet la cual se considera como la red de área extensa más grande del mundo debido a que se conecta muchas otras redes de área local a través de las diferentes zonas geográficas.

3.3 TEMÁTICA 3

La temática 3 consistió en configurar la distribución GNU/Linux Endian Firewall para gestionar y asegurar el acceso desde la red LAN hacia los servicios del servidor Ubuntu que corre en la zona DMZ. Para ello se habilitaron solamente los servicios que eran necesarios, para ser concretos el de HTTP (puerto 80) y el de FTP (puerto 21); de este modo se construyeron reglas de tráfico entre zonas que permitieron el tráfico que estaba permitido desde la zona VERDE hacia la zona NARANJA.

También se implementaron políticas de seguridad que identificaron el protocolo ICMP, ya que estaba prohibiendo que los equipos de la LAN pudieran hacer solicitudes de eco (ping) al DMZ. Se configuró esta restricción mediante reglas de firewall que fueron bloqueando tipos de ICMP, de este modo se fortaleció la protección del servidor ante actividades de tipo reconocimiento. Finalmente, la ejecución de las reglas se verificó mediante pruebas de conectividad y por la revisión de los logs del firewall, comprobando así que se eran cumplidos los requisitos de accesibilidad y seguridad que la actividad pedía.

3.4 TEMÁTICA 5

La temática 5 tuvo como objetivo implementar un proxy HTTP no transparente en Endian Firewall, realizando habilitación de mecanismos de autenticación y filtrado web, que permitieron un control granular sobre la navegación de los usuarios de una red interna. La implementación de este tipo de funcionalidades, permitieron que se fortaleciera la seguridad perimetral, evitando que acceda a paginas no autorizadas y generando garantía que la navegación cumpla con políticas corporativas o empresariales según se requiera.

En conclusión, la correcta ejecución de las pruebas de navegación, autenticación y restricción confirmaron que la

configuración realizada del proxy opera de manera estable y se encuentra alineada con las políticas que se definieron de bloqueo de las páginas web en la lista negra del perfil de filtrado, atribuyendo control de accesos del tráfico HTTP y permitiendo que el entorno sea más controlado y seguro dentro de la red interna.

4 REFERENCIAS

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

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

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

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

[5] Endian. (2016). Endian UTM 3.3 Manual referencia. Endian. Recuperado de http://docs.endian.com/3.3/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. Recuperado de https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952.

[7] Ubuntu Server documentation. (s. f.). (2025) (para Ubuntu 20.04 LTS en adelante) Ubuntu Server. https://documentation.ubuntu.com/server/

[8] Guía del escritorio de Ubuntu. (s. f.). Ubuntu 25.04 https://help.ubuntu.com/25.04/ubuntu-help/index.html.es