GNU/LINUX COMO SOLUCION EN REDES: IMPLEMENTACION DE UN SO SEGURO Y PARAMETRIZADO PARA LAS NECESIDADES ESPECIFICAS DEL CLIENTE

Daniel Camio Parra Diaz
e-mail: dcparradi@unadvirtual.edu.co
Hermes Osuna Forero
e-mail: hosunaf@unadvirtual.edu.co
Juan Carlos Diaz lopez
e-mail: jcdiazlope@unadvirtual.edu.co

ABSTRACT: *This article presents the implementation of a network security system based on GNU/Linux Endian Firewall in a virtualized environment with VirtualBox. The architecture segments the network into green, orange, and red zones, facilitating the management and protection of different levels of trust. The installation and configuration process for interfaces, access rules, and services in the DMZ is detailed, ensuring effective separation between internal and external networks. Additionally, an HTTP proxy is implemented with authentication policies and site-specific blocking, strengthening web access security. The results demonstrate a secure, flexible, and parameterizable architecture that complies with the principles of perimeter security and traffic control in virtual environments. This approach allows organizations to manage critical services and improve protection against external threats, demonstrating the viability of GNU/Linux-based systems for network security in enterprise environments.*

***KEYWORDS**: Endian, firewall, DMZ*

RESUMEN: *Este artículo presenta la implementación de un sistema de seguridad de red basado en GNU/Linux Endian Firewall en un entorno virtualizado con VirtualBox. La arquitectura segmenta la red en zonas verde, naranja y roja, facilitando la gestión y protección de diferentes niveles de confianza. Se detalla el proceso de instalación y configuración de interfaces, reglas de acceso y servicios en la zona DMZ, garantizando una separación efectiva entre redes internas y externas. Además, se implementa un proxy HTTP con políticas de autenticación y bloqueo de sitios específicos, fortaleciendo la seguridad del acceso web. Los resultados demuestran una arquitectura segura, flexible y parametrizable, que cumple con los principios de seguridad perimetral y control de tráfico en entornos virtuales. Este enfoque permite a las organizaciones gestionar servicios críticos y mejorar la protección contra amenazas externas, demostrando la viabilidad de sistemas basados en GNU/Linux para la seguridad de redes en entornos empresariales.*

***PALABRAS CLAVE**: Endian, firewall, DMZ*

1. INTRODUCCIÓN

En esta actividad grupal se trabaja la implementación de medidas de seguridad perimetral en una red que incluye zonas LAN, WAN y DMZ, utilizando como herramienta principal la distribución GNU/Linux Endian Firewall (EFW). El objetivo es proteger los servicios y servidores ubicados en la red DMZ y controlar el acceso desde la red interna hacia el exterior. Para ello, se desarrollan varias temáticas clave: la configuración inicial de Endian con sus zonas de red (verde, roja y naranja), la habilitación de servicios HTTP y FTP desde la DMZ, la restricción del protocolo ICMP para mayor seguridad, y la implementación de un proxy HTTP no transparente con políticas de autenticación y filtrado web. Cada configuración será documentada con evidencias prácticas que incluyen comandos, fechas y resultados obtenidos desde consola.

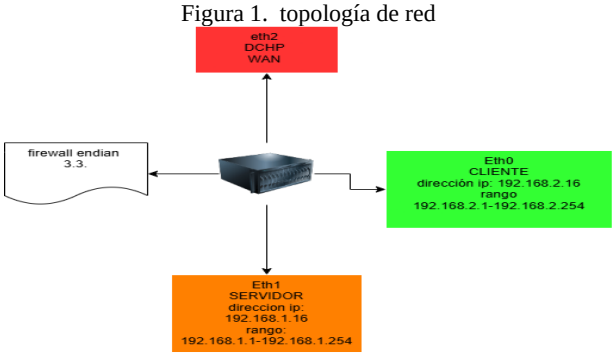
2. DESARROLLO

2.1 INSTALACIÓN DE ENDIAN FIREWALL EN VIRTUALBOX

Se presenta el proceso de la instalación y configuración de la distribución GNU/Linux Endian Firewall (EFW) el cual será el componente principal para la seguridad perimetral en redes que serán segmentadas, en total habrá tres redes segmentadas que serán la zona verde, la zona naranja y la zona roja. en sistema Endian se va a implementar en un entorno virtualizado en el software VirtualBox.

En la siguiente imagen se muestra cómo se van a dividir las IPs en cada una de las zonas.

Figura 1. topología de red

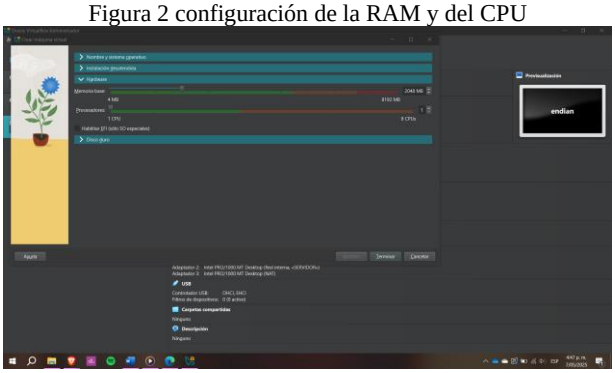


Fuente: autoría individual de Hermes Osuna.

Para generar el sistema de seguridad perimetral, se va a crear una nueva máquina virtual con las siguientes características:

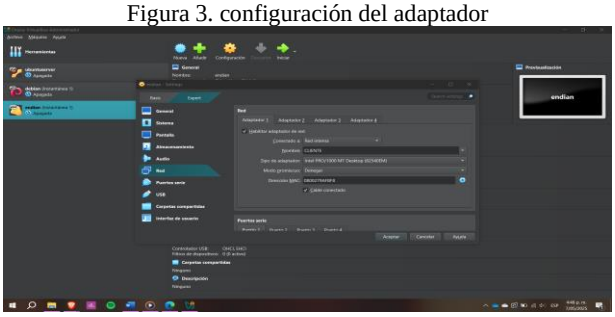
1 núcleo de CPU y 2048 MB de RAM.
almacenamiento virtual en disco de 20 GB
tres adaptadores de red configurados como:
zona verde: red interna (nombre: CLIENTE)
zona roja: NAT (acceso a internet)
zona naranja: red interna (nombre: SERVIDOR)

Figura 2 configuración de la RAM y del CPU



Fuente: autoría individual de Hermes Osuna.

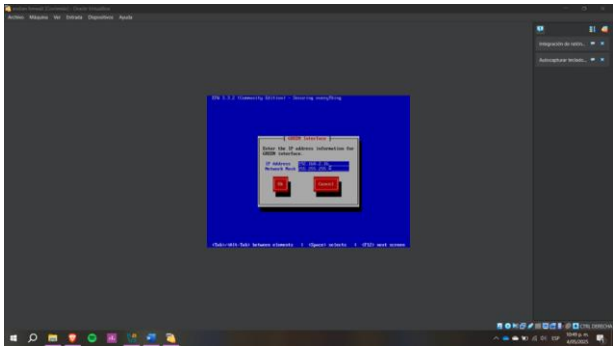
Figura 3. configuración del adaptador



Fuente: autoría individual de Hermes Osuna.

Se configurar los tres adaptadores para cada una de las zonas. Las zonas verde y naranja tienen que estar en red interna con el nombre respectivo de la red mientras que la roja en NAT, conteniendo ya configurado los tres adaptadores de la máquina Endian. Se inicia con la instalación del sistema Endian, donde se configura lo que es el idioma. y se sigue el proceso que indica el cual es sencillo. Se sigue el proceso de instalación definido como vaya apareciendo hasta que se llega a este apartado:

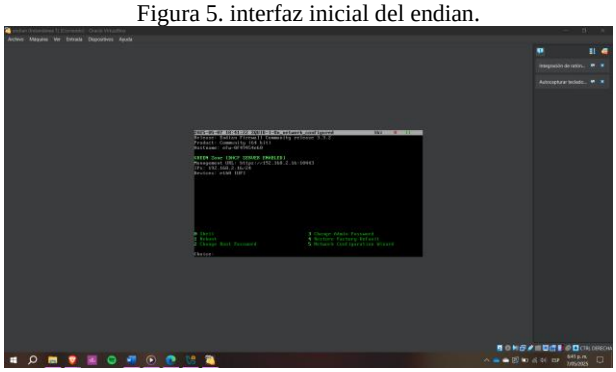
Figura 4. colocar IP de la zona verde



Fuente: autoría individual de Hermes Osuna.

En este apartado se tiene que colocar la dirección IP y la máscara de la misma que se va a manejar. Luego de configurarla y darle en "ok" se sigue con la instalación, al final el sistema te indicará que retirar el medio de instalación. Para hacerlo dentro el VirtualBox se tiene que ir al menú de dispositivos en la ventana de la máquina virtual. Al hacer clic en "dispositivos ópticos" se tiene que ir a ver el archivo ISO de Endian listado y hacer clic en "Desmontar" o en el nombre del archivo ISO para desmarcarlo. si sale un mensaje si forzar el desmontaje se tiene que confirmar y darle en la ventana "ok" y se reinicia la máquina virtual.

Figura 5. interfaz inicial del endian.

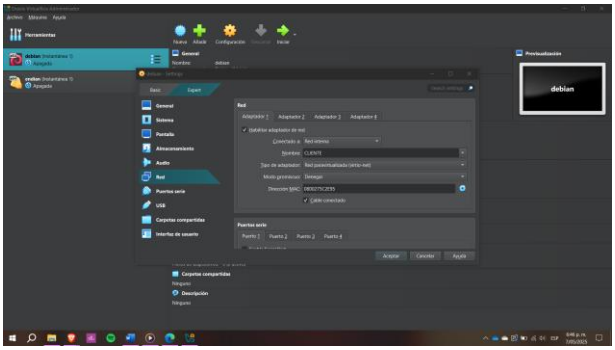


Fuente: autoría individual de Hermes Osuna.

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

Ahora con el Endian instalado, lo que se tiene que hacer es usar un navegador web que en este caso será el navegador Mozilla dentro de otra máquina virtual que tiene el sistema Linux debian, esta nueva máquina virtual tendrá modificado en el apartado de red en el adaptador 1 tenerlo como red interna y el nombre de la red tiene que ser el mismo del de la zona verde que es CLIENTE.

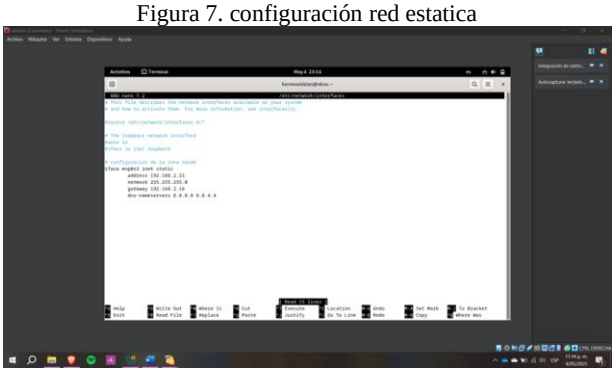
Figura 6. configuración de la red del Debian



Fuente: autoría individual de Hermes Osuna.

Una vez encendida y ya dentro de Debian, al hacerlo por primera vez después de la instalación del Endian, se mostrará que no tiene conexión a internet esto se debe a que no se ha configurado el Endian completamente, para hacerlo se tiene que usar un navegador y entra a una dirección específica que en este caso es https://192.168.2.16:10443 la dirección se puede encontrar dentro del sistema Endian. pero como se dijo aún no se puede conectarse al Endian desde Debian en este caso se entra al terminal y se edita el archivo de configuración de red por medio del comando sudo nano /etc/network/interfaces. y se coloca el siguiente comando.

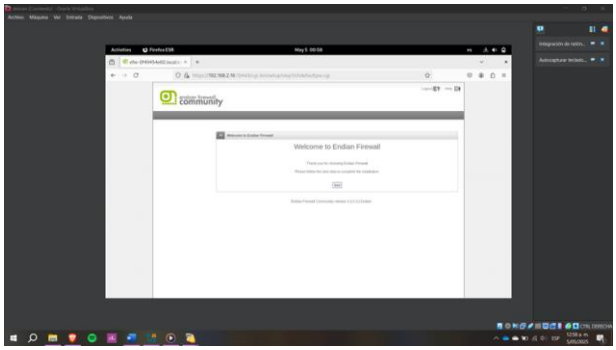
Figura 7. configuración red estatica



Fuente: autoría individual de Hermes Osuna.

Tener en cuenta que se tiene que colocar una ip estática dentro de la zona verde del Endian, la máscara, el gateway de la IPs y el dns-nameservers y se guarda y sale del archivo. se puede verificar si funciono si se coloca en el terminal el comando ping 192.168.2.16 que es el de la zona verde. verificando que tiene ping, en el navegador se coloca la dirección https://192.168.2.16:10443. que se ve así.

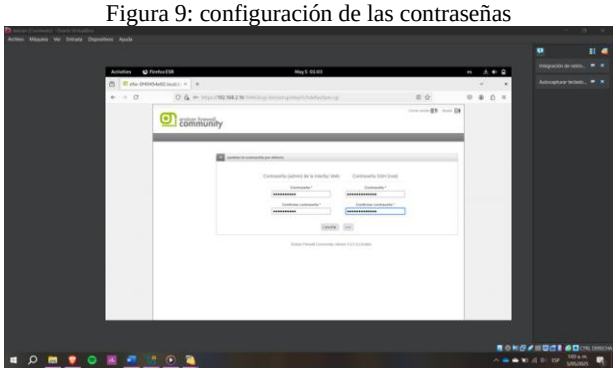
Figura 8. Endian interfaz web



Fuente: autoría individual de Hermes Osuna.

Aquí el proceso es ir dándole en el botón ">>>". Se selecciona el idioma, se acepta la licencia. si se quiere un backup o no. luego va a ver el siguiente apartado

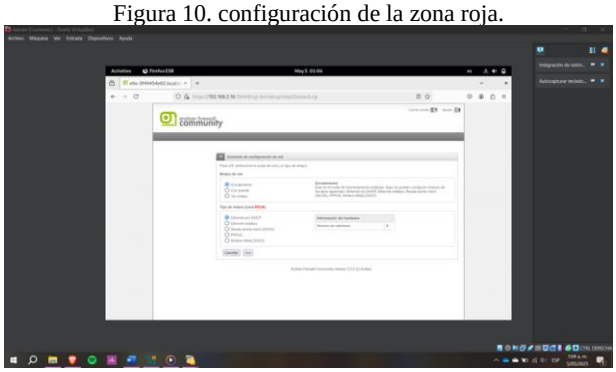
Figura 9: configuración de las contraseñas



Fuente: autoría individual de Hermes Osuna.

En este apartado se coloca una contraseña para el root y el ssh . Luego sigue el proceso de configurar las zonas como se muestra a continuación.

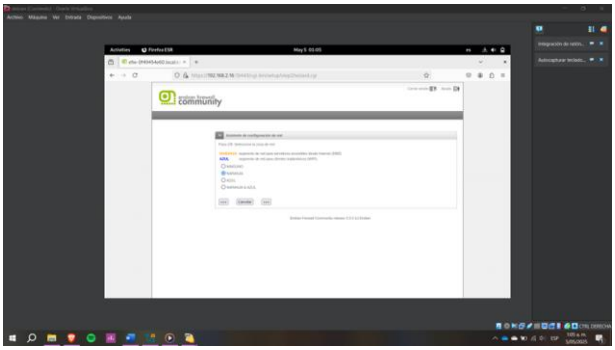
Figura 10. configuración de la zona roja.



Fuente: autoría individual de Hermes Osuna.

Se tiene que dejar el apartado de DHCP para que las IPs se establezcan automáticamente.

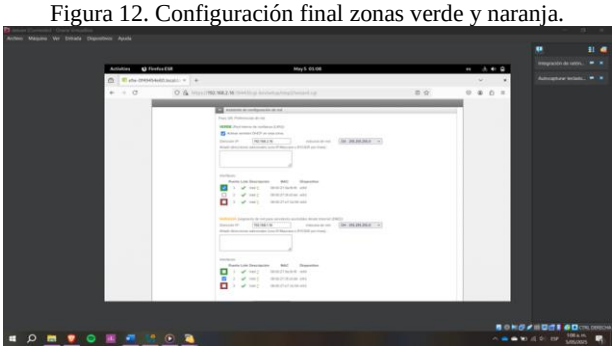
Figura 11. configuración de la zona naranja



Fuente: autoría individual de Hermes Osuna.

Seleccionamos las zonas que queremos que en este caso será solo la naranja, tener claro la zona naranja (DMZ) está diseñada para alojar servidores que deben estar accesibles desde redes externas; esta debe estar separada de la red verde (LAN) para contener cualquier intrusión y evitar que se comprometan otros equipos internos [5].

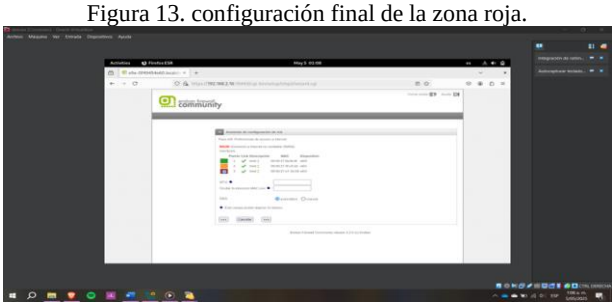
Figura 12. Configuración final zonas verde y naranja.



Fuente: autoría individual de Hermes Osuna.

En este apartado se configura el huerto y la dirección IPs de las zonas verde y naranja teniendo presente que, al configurar las interfaces, se recomienda utilizar direcciones IP en distintos segmentos de red, respetando las direcciones privadas definidas por la IANA en la RFC 1918 [1].

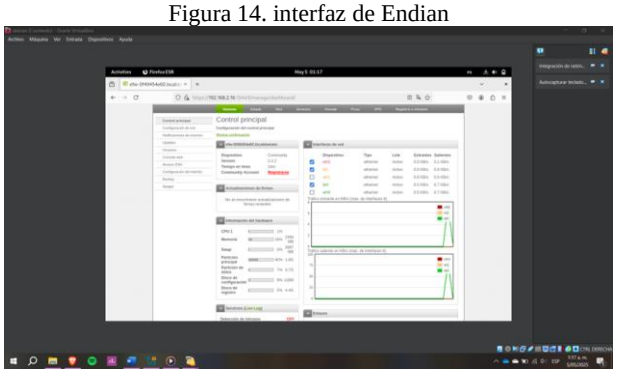
Figura 13. configuración final de la zona roja.



Fuente: autoría individual de Hermes Osuna.

En este apartado se deja predeterminado en este caso. y configurado se puede dejar predeterminado los demás aspectos. y al final se sale un mensaje diciendo que ya se configuró la red y aparece un botón “Aceptar, aplica configuración”. se espera un poco y aparecerá una ventana donde se tendrá que colocar usuario y contraseña. El usuario es “admin” y la contraseña será la que se definió en el proceso de configuración.

Figura 14. interfaz de Endian



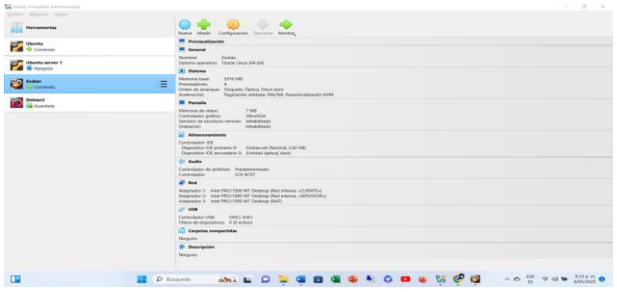
Fuente: autoría individual de Hermes Osuna.

En la imagen se puede notar que los apartados que están seleccionados están en brX y no en ethX esto se debe a que Endian Firewall gestiona las zonas como interfaces en puente (bridge), denominadas brX en lugar de ethX, independientemente del número de interfaces asignadas [1].

2.3 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED. PRODUCTO ESPERADO

Permitir servicios de la Zona DMZ para la red, cuyo objetivo principal es gestionar el acceso controlado a servicios específicos en un entorno perimetral utilizando Endian Firewall (EFW). Se implementó un servidor web con Ubuntu Server en la Zona DMZ, configurando reglas para permitir únicamente los servicios HTTP (puerto 80) y FTP (puerto 21). Asimismo, se establecieron restricciones para bloquear el protocolo ICMP, impidiendo la respuesta al comando ping como medida de seguridad adicional. Esta práctica integra conceptos clave de seguridad de red, administración de servicios y gestión de tráfico mediante firewall.

Figura 15. Configuración Maquina Con dos adaptadores internos



Fuente: autoría individual de Juan Carlos Diaz.

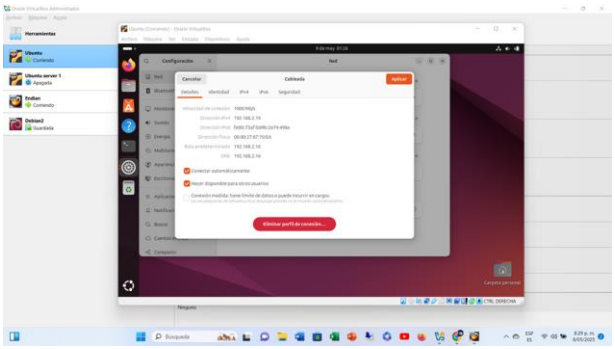
Se ha completado con éxito la instalación del sistema Endian Firewall Community (EFW) en el entorno virtualizado/local. Durante el proceso, se configuraron adecuadamente las interfaces de red (zona verde, roja y/o DMZ), se establecieron las direcciones IP estáticas correspondientes y se verificó la conectividad entre las zonas.

Figura 16. Endian Instalado

Fuente: autoría individual de Juan Carlos Diaz.

Se procedió a configurar el adaptador de red 2 de la máquina virtual (o del host, según corresponda) en modo red interna o adaptador puente, según la topología establecida, apuntando a la dirección IP del firewall Endian: 192.168.2.16. Esta dirección corresponde a la interfaz de red asignada a la zona verde (red interna segura) dentro de la arquitectura de Endian.

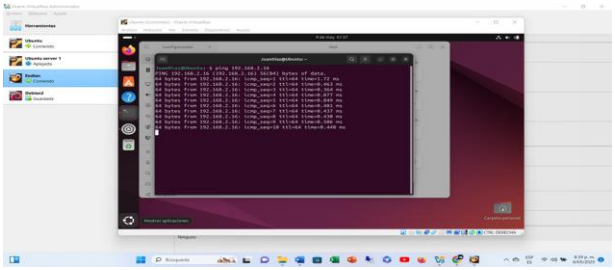
Figura 17. Configuración del adaptador de red 2 apuntando a la ruta de la ruta del endian 192.168.2.16



Fuente: autoría individual de Juan Carlos Diaz.

Para comprobar la correcta comunicación entre la máquina cliente y el firewall Endian, se utilizó la herramienta de diagnóstico de red `ping` apuntando a la dirección IP 192.168.2.16, correspondiente a la interfaz de la zona verde del firewall

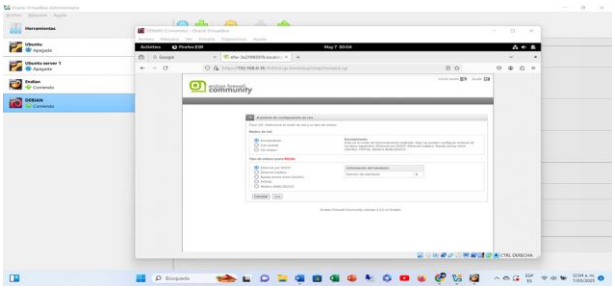
Figura 18. Ping para comprobar conexión al firewall



Fuente: autoría individual de Juan Carlos Diaz.

Con el objetivo de simplificar la configuración de red y facilitar la administración de los dispositivos dentro del entorno controlado, se configuró la interfaz de red de la máquina cliente para obtener una dirección IP de forma automática utilizando el protocolo DHCP (Dynamic Host Configuration Protocol).

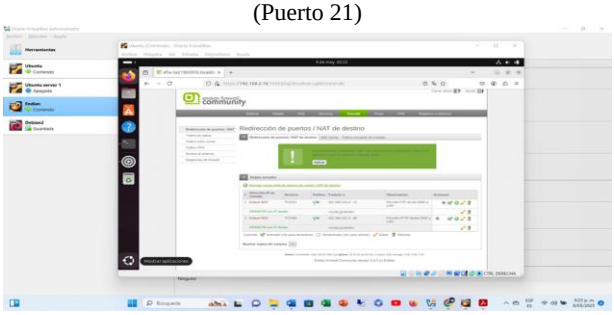
Figura 19. La ip como la queremos automática queda en DHCP



Fuente: autoría individual de Juan Carlos Diaz.

Con el objetivo de habilitar el acceso a servicios ubicados en la zona DMZ del firewall Endian, se procedió a configurar las reglas necesarias para permitir el tráfico entrante hacia los puertos 80 (HTTP) y 21 (FTP).

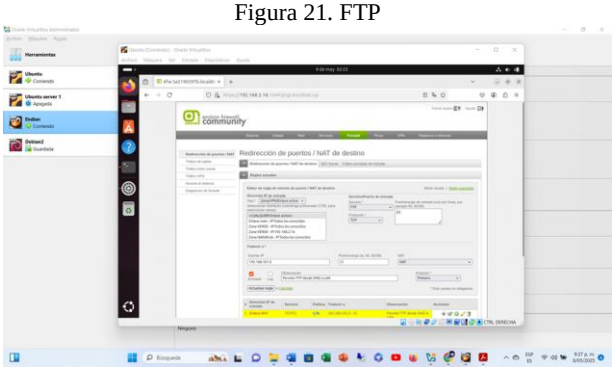
Figura 20. Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21)



Fuente: autoría individual de Juan Carlos Diaz.

Para permitir el acceso al servicio de transferencia de archivos FTP (File Transfer Protocol) ubicado en un servidor dentro de la zona DMZ, se procedió a crear una regla específica en el firewall de Endian que habilita el tráfico entrante hacia el puerto 21 TCP, el cual es el puerto estándar para conexiones FTP.

Figura 21. FTP



Fuente: autoría individual de Juan Carlos Diaz.

Como parte del proceso de aseguramiento de la red y validación de la configuración del firewall Endian, se procedió a revisar y verificar las reglas de salida aplicadas a la Zona Roja, que representa la conexión hacia Internet o redes externas no confiables.

Figura 22. Verificamos reglas de salida ZONA ROJA

Fuente: autoría individual de Juan Carlos Diaz.

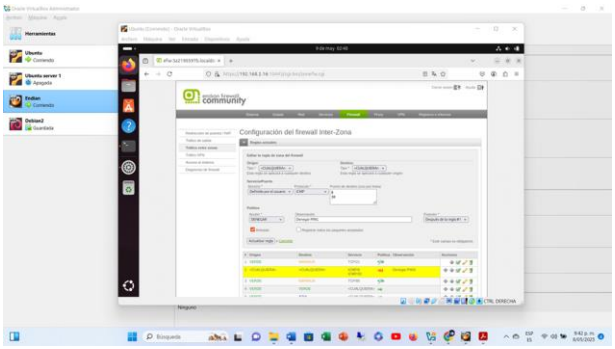
Dentro de la arquitectura de red implementada con Endian Firewall, uno de los aspectos clave en la seguridad y funcionamiento es el control del tráfico entre las diferentes zonas de seguridad. Endian segmenta la red en zonas lógicas —como Zona Verde (LAN interna segura), Zona Roja (Internet), Zona Naranja o DMZ (zona desmilitarizada) y, opcionalmente, Zona Azul (red Wi-Fi)—, lo cual permite establecer reglas específicas de comunicación entre ellas.

Figura 23. tráfico entre zonas

Fuente: autoría individual de Juan Carlos Diaz.

Bloqueo del protocolo ICMP para evitar respuestas a solicitudes de ping en la red:
Como medida preventiva dentro de la estrategia de seguridad perimetral, se configuró el firewall Endian para denegar el tráfico del protocolo ICMP, específicamente los tipos Echo Request (Tipo 8) y Echo Reply (Tipo 0), comúnmente utilizados por la herramienta `ping`.

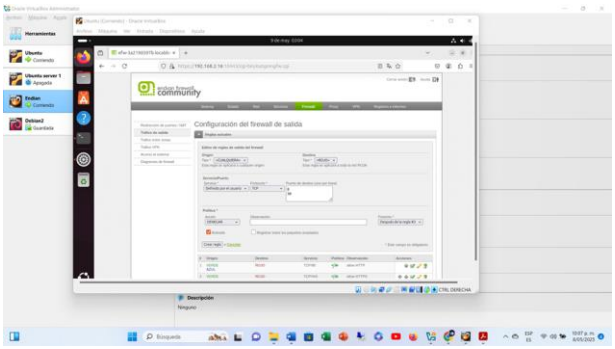
Figura 24. Denegamos el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red.



Fuente: autoría individual de Juan Carlos Diaz.

Con el fin de reforzar la seguridad de la red y reducir su exposición a escaneos o análisis de infraestructura por parte de posibles atacantes externos, se procedió a bloquear selectivamente tipos específicos de mensajes ICMP mediante reglas personalizadas en el firewall Endian.

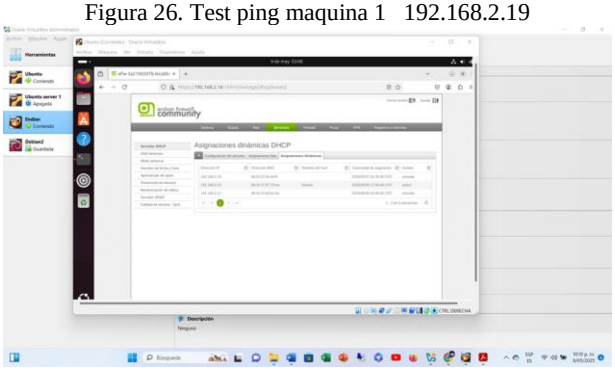
Figura 25. configuración para denegar puerto 8 y puerto 30



Fuente: autoría individual de Juan Carlos Diaz.

Para verificar la conectividad y la correcta configuración de red entre los dispositivos dentro de la zona interna (Zona Verde), se realizó una prueba de ping desde el equipo administrador hacia la máquina 1, asignada con la dirección IP 192.168.2.19.

Figura 26. Test ping maquina 1 192.168.2.19

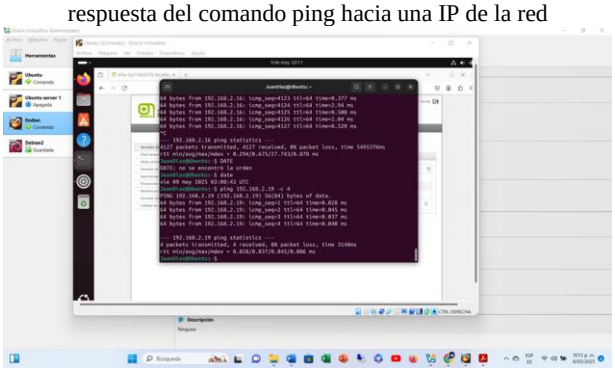


Fuente: autoría individual de Juan Carlos Diaz.

Para validar la correcta implementación de las políticas de seguridad en el firewall Endian, específicamente el bloqueo del protocolo ICMP, se realizó una prueba desde una consola o

terminal. Se ejecutó el comando `ping` dirigido a una dirección IP específica dentro de la red protegida, con el objetivo de comprobar que no se recibieran respuestas a las solicitudes de eco ICMP.

Figura 27. compruebo a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red



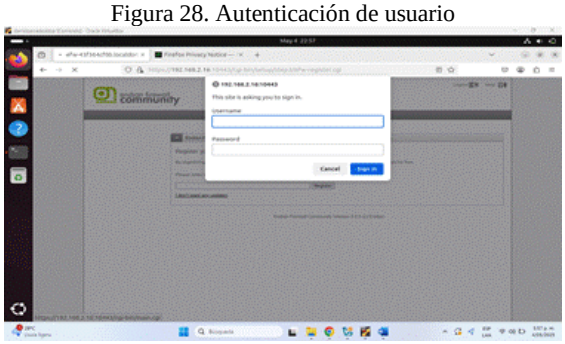
Fuente: autoría individual de Juan Carlos Diaz.

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

El objetivo final de la Temática 5 es desarrollar un perfil de seguridad que incluya una lista negra para restringir el acceso a los sitios web www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Paralelamente, se configurará un sistema de autenticación por usuario, donde se creará una cuenta específica, se asignará a un grupo determinado y se vinculó a una política de acceso asociada al perfil establecido. Para verificar el correcto funcionamiento, se realizan pruebas Desde la red local (LAN) intentando acceder a las páginas bloqueadas mediante un navegador web.

En esta parte se muestra la interfaz de ingreso de endian, se intenta ingresar a la página objetivo con usuario y contraseña.

Figura 28. Autenticación de usuario



Fuente: autoría individual de Daniel Camilo Parra Diaz

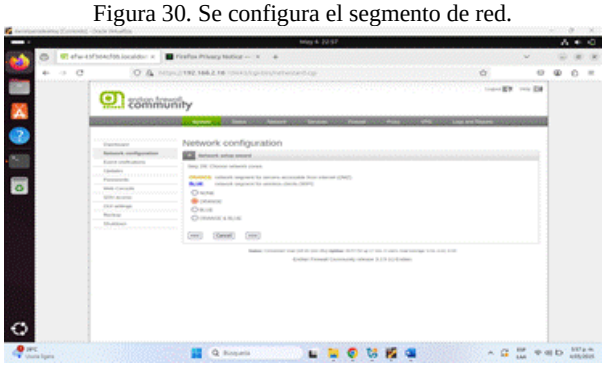
Se accede al apartado de configuración de red (Network Configuration) y se establecen los parámetros de la conexión RED en modo DHCP para asignación automática de direcciones IP

Figura 29. Configuración de RED DHCP.

Fuente: autoría individual de Daniel Camilo Parra Diaz

En esta parte, se procede a definir la configuración de red para las zonas del firewall. Se ha asignado el tipo ORANGE, correspondiente a la DMZ (Zona Desmilitarizada), con el fin de establecer un segmento de red accesible desde Internet y aislado de la red interna para mayor seguridad.

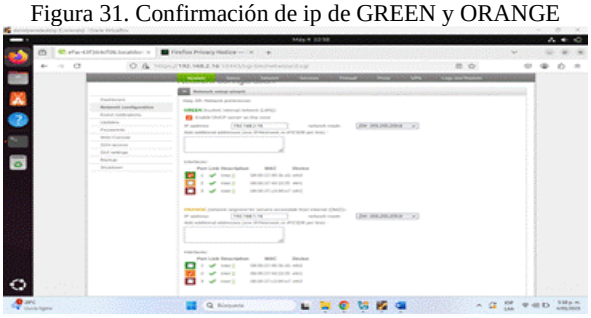
Figura 30. Se configura el segmento de red.



Fuente: autoría individual de Daniel Camilo Parra Diaz

Se verifican las direcciones IP asignadas a cada segmento: la red GREEN con la IP 192.168.2.16 y la red ORANGE con la IP 192.168.1.16, asegurando una correcta segmentación y conectividad según los parámetros de seguridad establecidos.

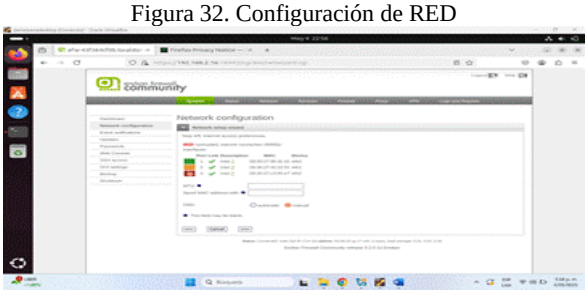
Figura 31. Confirmación de ip de GREEN y ORANGE



Fuente: autoría individual de Daniel Camilo Parra Diaz

De manera similar, se verifica que el segmento RED se encuentre configurado en modo DHCP, permitiendo la asignación automática de direcciones IP según los parámetros establecidos.

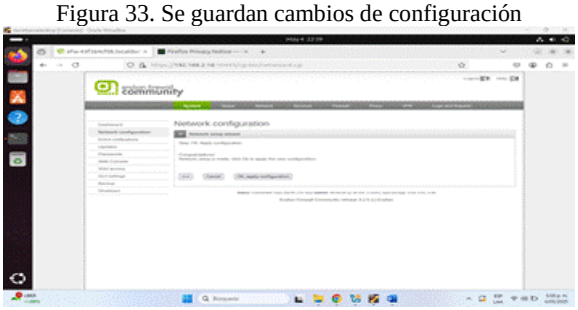
Figura 32. Configuración de RED



Fuente: autoría individual de Daniel Camilo Parra Diaz

En este apartado, se aplican todas las configuraciones realizadas y se procede a guardar los cambios en el sistema.

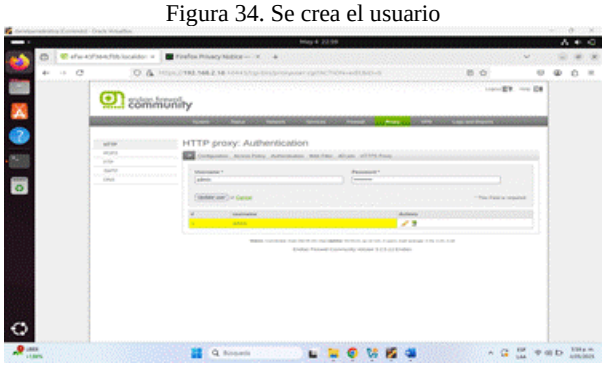
Figura 33. Se guardan cambios de configuración



Fuente: autoría individual de Daniel Camilo Parra Diaz

En esta etapa, se crea la cuenta de usuario dentro del módulo de autenticación, completando todos los campos obligatorios

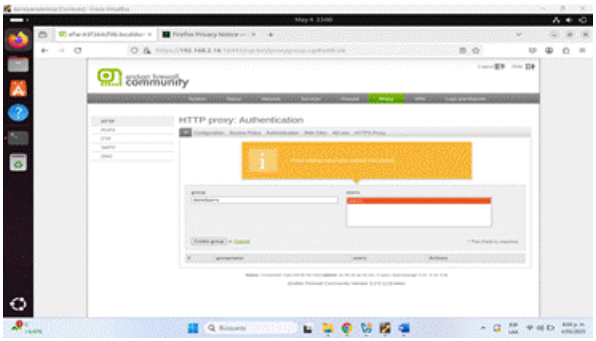
Figura 34. Se crea el usuario



Fuente: autoría individual de Daniel Camilo Parra Diaz

En la configuración del proxy HTTP, se crea un nuevo grupo de acceso llamado “danielparra” y se asigna el usuario admin como miembro de este, garantizando así los permisos de navegación y políticas de filtrado correspondientes

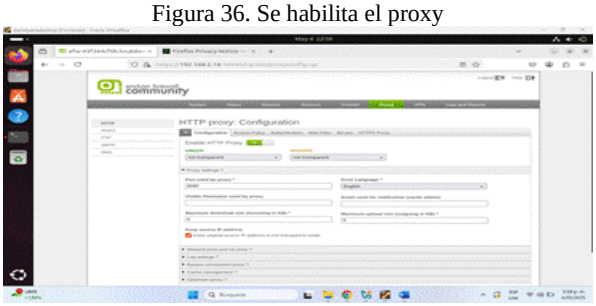
Figura 35. Creación de grupo.



Fuente: autoría individual de Daniel Camilo Parra Diaz

Se procede a habilitar el servicio de proxy en el sistema, activando así la funcionalidad de intermediario para las solicitudes HTTP y aplicando las políticas de filtrado configuradas previamente [6]

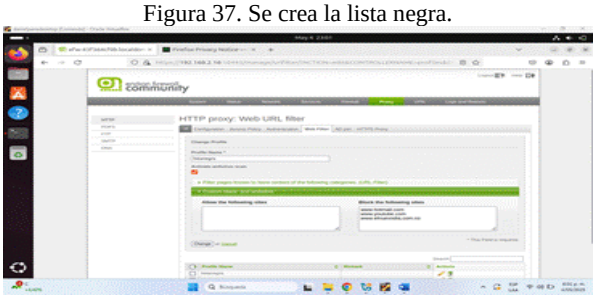
Figura 36. Se habilita el proxy



Fuente: autoría individual de Daniel Camilo Parra Diaz

Se crea un nuevo filtro denominado “listanegra” dentro del sistema de control de contenido, donde se configuró el bloqueo de los siguientes dominios: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Posteriormente, se aplicaron y guardaron los cambios para que la restricción entrara en efecto.

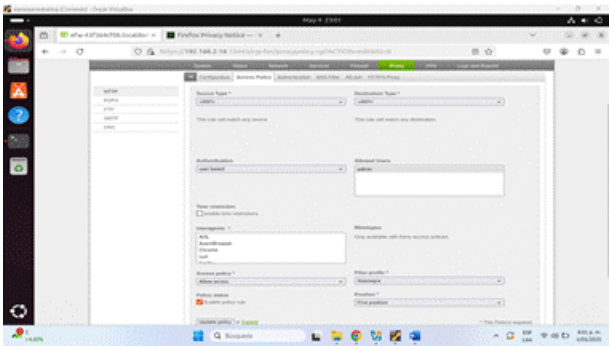
Figura 37. Se crea la lista negra.



Fuente: autoría individual de Daniel Camilo Parra Diaz

Se configura una nueva política de acceso en el sistema, asociando al usuario “admin” como responsable de la aprobación y gestión de la regla previamente creada denominada “listanegra”.

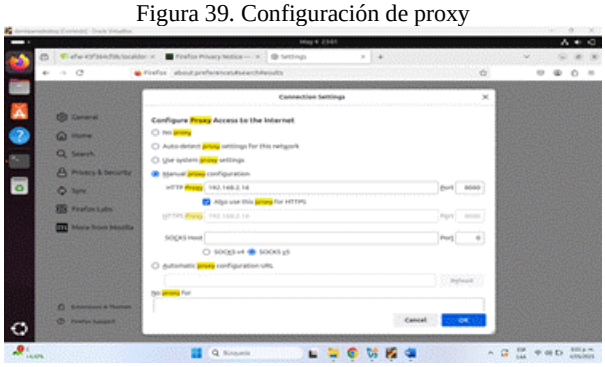
Figura 38. Se aplican las normas de acceso.



Fuente: autoría individual de Daniel Camilo Parra Diaz

Se accedió a la configuración de proxy del navegador Firefox, donde se estableció manualmente la dirección IP 192.168.10.1 como servidor proxy para el tráfico HTTP. Además, se activó la opción para utilizar el mismo proxy en conexiones HTTPS, asegurando que todo el tráfico web pase por el servidor intermediario configurado

Figura 39. Configuración de proxy



Fuente: autoría individual de Daniel Camilo Parra Diaz

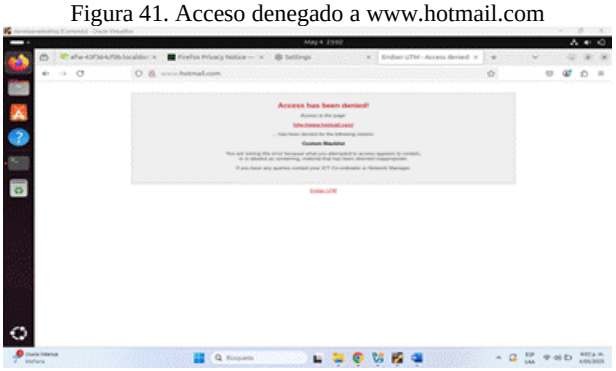
Al intentar acceder a la página web www.hotmail.com, el sistema solicita credenciales de autenticación, mostrando un mensaje de solicitud de usuario y contraseña para autorizar el ingreso al servicio de correo electrónico

Figura 40. Se realiza la autenticación de usuario

Fuente: autoría individual de Daniel Camilo Parra Diaz

Al tratar de ingresar a www.hotmail.com se requiere la autenticación de usuario y contraseña, posteriormente aparece el mensaje previamente configurado de acceso denegado.

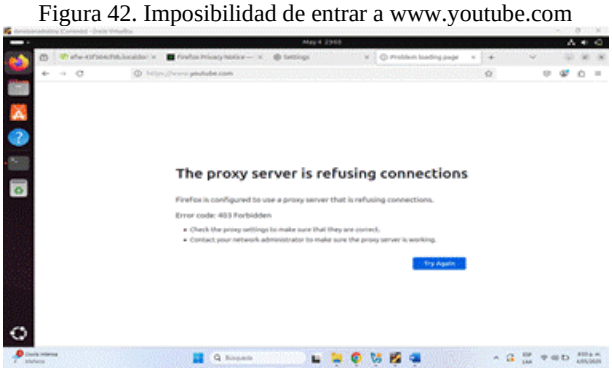
Figura 41. Acceso denegado a www.hotmail.com



Fuente: autoría individual de Daniel Camilo Parra Diaz

En este apartado, al intentar acceder a la página web www.youtube.com, el sistema muestra un mensaje de restricción indicando que el acceso al sitio no está permitido bajo las políticas de red configuradas previamente.

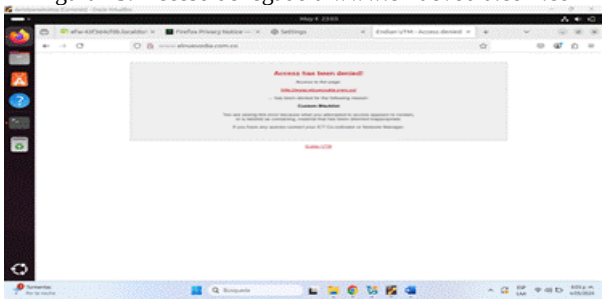
Figura 42. Imposibilidad de entrar a www.youtube.com



Fuente: autoría individual de Daniel Camilo Parra Diaz

Finalmente, al intentar acceder a la página www.elnuevodia.com.co, el sistema también presentó un mensaje de acceso denegado, confirmando que el dominio está bloqueado bajo las mismas políticas de filtrado aplicadas anteriormente.

Figura 43. Acceso denegado a www.elnuevodia.com.co



Fuente: autoría individual de Daniel Camilo Parra Diaz

3. CONCLUSIONES.

La implementación de la instancia GNU/Linux Endian en el programa VirtualBox permite configurar exitosamente una arquitectura de red que esté segmentada en tres distintas zonas que son verde, roja y naranja estas zonas cumplen con los principios de seguridad perimetral. Con la configuración de las interfaces de red y la asignación de la dirección ip privadas que van a usar cada una de las zonas se pudo llegar a un entorno controlado que muestre las bases para la protección de los servicios expuestos en la DMZ.

La configuración de las reglas de acceso desde la zona DMZ permitió garantizar que únicamente los servicios necesarios, como HTTP y FTP, estuvieran disponibles, fortaleciendo así la seguridad del servidor web en Ubuntu Server. Además, la restricción del protocolo ICMP evitó la ejecución de comandos de diagnóstico como *ping*, reduciendo posibles vectores de reconocimiento por parte de atacantes. Estas medidas, implementadas correctamente en Endian Firewall, demuestran la importancia del control granular del tráfico en redes perimetrales.

La implementación de un proxy HTTP no transparente en una red segmentada mejora la seguridad y el control del tráfico web, permitiendo el bloqueo de sitios específicos y una gestión eficiente de recursos mediante políticas de acceso y autenticación. Su integración en entornos virtualizados como VirtualBox facilita pruebas seguras sin afectar la infraestructura física, mientras que la configuración adecuada de reglas NAT, zonas de confianza y servicios web fortalece la arquitectura de red, garantizando seguridad perimetral y protección de servicios críticos.

4. REFERENCIAS

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

[2] Endian srl, “System Settings,” Endian Firewall Reference Manual, version 2.2, [Online]. Available: https://docs.endian.com/archive/2.2/efw.system.html [Accessed: May 10, 2025].

[3] Endian Community. (2023). Endian Firewall Documentation. https://www.endian.com/

[4] LaCroix, J. (2020). Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting.

[5] Endian Team. (2025). *Endian Firewall Community: Access Control and Service Rules* (Version 3.3.2) [User documentation]. Endian.
URL: https://docs.endian.com/efw/community/services/firewall.html

[6] Squid Project. (2025). Squid Proxy: Authentication and access control (Version 4.15) [User guide]. Squid-Cache. URL: http://www.squid-cache.org/Doc/config/acl/

[7] Endian UTM. (s. f.). Endian UTM 3.2 Reference Manual. https://docs.endian.com/3.2/utm/index.html

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

[9] Ubuntu Server Guide. (2024). Ubuntu Server 22.04 LTS Documentation. Canonical Ltd. https://ubuntu.com/server/docs

[10] Nemeth, E., Snyder, G., Hein, T. R., & Whaley, B. (2017). UNIX and Linux System Administration Handbook (5th ed.). Pearson Education.
https://www.pearson.com/en-us/subject-catalog/p/unix-and-linux-system-administration-handbook/P200000004847

[11] Ubuntu Documentation. (2023). Squid Proxy Server Setup on Ubuntu 22.04 LTS. Canonical. https://help.ubuntu.com/community/Squid