IMPLEMENTACION Y DESARROLLO DE PROTOCOLOS DE SEGURIDAD CON ENDIAN

David Esteban Forero
e-mail: deforeroh@unadvirtual.edu.co
Cristian Duvan Gil
e-mail: cdgilr@unadvirtual.edu.co
Michael Steve Carrillo
e-mail: mscarrillos@unadvirtual.edu.co

RESUMEN: *Este documento presenta la configuración e implementación de una infraestructura básica en Ubuntu Server, incluyendo la asignación de direcciones IP estáticas, instalación y validación de servicios esenciales relacionados a seguridad perimetral con Endian, así como el despliegue de un formulario web funcional. Se configuró manualmente la red utilizando Netplan, definiendo una IP fija y una puerta de enlace específica. El formulario alojado permite el registro de datos en una base de datos MySQL y el envío de correos de confirmación al administrador. Además, se resolvieron errores relacionados con permisos, acceso proxy y denegación de servicio. Los resultados demuestran la correcta integración de los componentes del servidor, permitiendo acceso remoto, registro y visualización de datos, lo cual valida la funcionalidad esperada de las diferentes zonas (WAN, LAN y DMZ). Esta implementación proporciona una base sólida para entornos de pruebas o despliegue de servicios en redes controladas.*

PALABRAS CLAVE: DMZ, LAN, PROXY, WAN.

1 INTRODUCCIÓN

La implementación de plataformas de seguridad perimetral en entornos virtualizados constituye un componente fundamental en la administración de redes modernas. En este contexto, se configuró e instaló una instancia de GNU/Linux Endian dentro del entorno de virtualización VirtualBox, asignando interfaces de red a las zonas verde (LAN), roja (WAN) y naranja (DMZ), con el propósito de segmentar y controlar el flujo de tráfico entre las distintas áreas de la red.

A partir de esta arquitectura, se desarrolló la configuración de reglas NAT para permitir la comunicación entre zonas, garantizando el acceso desde la LAN hacia la WAN, y desde la DMZ hacia la red externa, con validación mediante pruebas de navegación y reenvío de puertos. Posteriormente, se establecieron políticas de filtrado para permitir o denegar servicios específicos, como HTTP y FTP, y se restringieron protocolos como ICMP, verificando el impacto en el tráfico inter-zona.

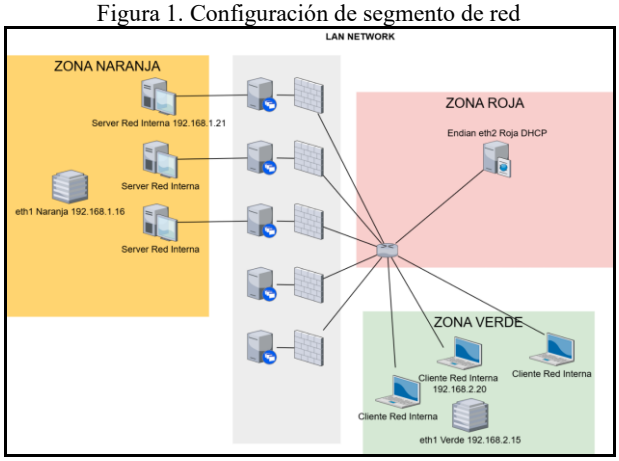
Adicionalmente, se implementó un proxy HTTP no transparente con mecanismos de autenticación por usuario y aplicación de políticas de control de contenido, incluyendo listas negras que bloquean el acceso a sitios predeterminados desde la LAN. Esta configuración integral demuestra la capacidad del sistema Endian para funcionar como una solución efectiva de seguridad y gestión de tráfico en redes estructuradas.

2 TEMÁTICA 01: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN

Para este paso se implementó en primera medida un diagrama de red que refleja la segmentación lógica de una infraestructura de red segura. Esta segmentación incluye tres zonas bien definidas: la zona Naranja (Servidores DMZ), encargada de albergar servicios expuestos al exterior; la zona Roja (Acceso a Internet WAN), utilizada como puerta de enlace hacia la red pública; y la zona Verde (Red Interna LAN), que contiene los equipos de uso interno de la organización. Esta distribución permite aplicar políticas de control granular sobre el tráfico entre zonas, garantizando tanto la seguridad como la disponibilidad de los servicios.

El diagrama se elabora de la siguiente manera, tal como se puede apreciar en la siguiente figura

Figura 1. Configuración de segmento de red



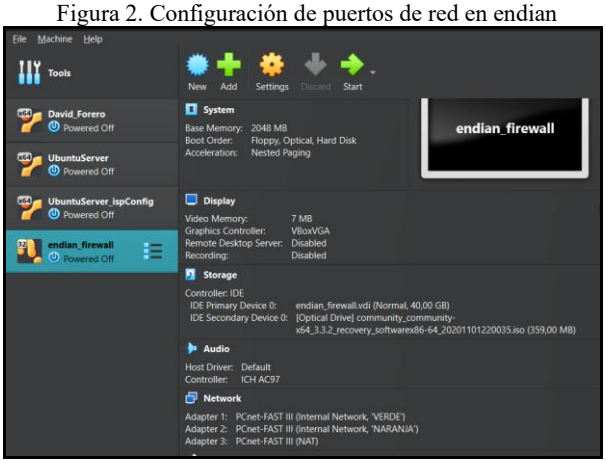
Fuente: Autoría Propia

Con este diagrama, se va a implementar el servicio endian para las diferentes zonas servidores y clientes.

En base a esta configuración de red, se procede a realizar la instalación del servicio endian en el entorno de virtual box con la configuración de las 3 tarjetas de red para cada zona establecida.

En esta etapa se realiza la asignación de los puertos de red virtuales que permitirán establecer la comunicación entre las zonas definidas del firewall Endian. Es fundamental vincular cada adaptador de red virtual a la interfaz lógica correcta (verde, roja y naranja), de forma que cada segmento de red quede correctamente aislado y gestionado. Este paso es clave para que el sistema reconozca adecuadamente las rutas de entrada y salida del tráfico, habilitando los controles de seguridad pertinentes tal como se puede apreciar en la siguiente figura

Figura 2. Configuración de puertos de red en endian



Fuente: Autoría Propia

El siguiente paso consiste en configurar adecuadamente la tarjeta de red del servidor para asignarle un segmento de red y una dirección IP estática, de acuerdo con el esquema definido previamente en el diagrama. Esta acción es fundamental para asegurar que cada interfaz del servidor se comunique correctamente con su zona respectiva (LAN, WAN o DMZ), y que los servicios de red funcionen de manera predecible, facilitando además la gestión y monitoreo del tráfico a través de herramientas especializadas.

Para esto, se modifica el archivo alojado en el directorio /etc/netplan/01-netcfg.yaml. El archivo de configuración de red `/etc/netplan/01-netcfg.yaml` es editado para asignar direcciones IP estáticas a cada interfaz del servidor. Esta operación garantiza que las interfaces no dependan del servicio DHCP, lo cual es esencial en entornos de red donde se requiere estabilidad, control y facilidad de acceso remoto. Las direcciones asignadas deben coincidir con los segmentos definidos previamente para asegurar una comunicación coherente y efectiva con cada zona del Endian Firewall tal como se puede apreciar en la siguiente figura

Figura 3. Configuración de ip en servidor ubuntu

Fuente: Autoría Propia

El siguiente paso es instalar la imagen ISO del servicio endian.

La zona verde representa el segmento interno y confiable de la red (LAN), usualmente utilizado por los clientes o dispositivos internos. En la configuración del servicio Endian, esta zona se parametriza manualmente, indicando la subred, el rango de direcciones IP, la máscara de red y otros parámetros que permitan identificar claramente los dispositivos autorizados. La correcta configuración de esta zona es vital para asegurar que solo dispositivos internos tengan acceso privilegiado a los servicios internos tal como se puede apreciar en la siguiente figura

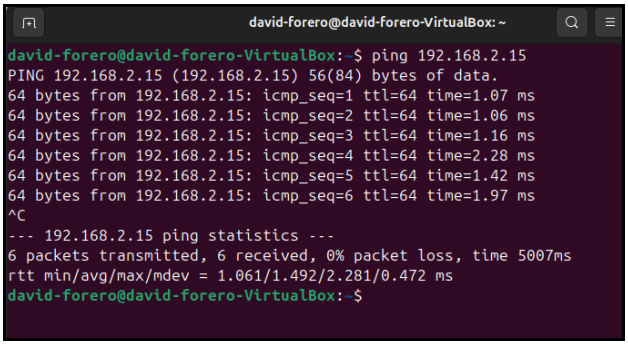
Figura 4. Configuración de zona verde en servicio endian

Fuente: Autoría Propia

El siguiente paso es configurar la zona verde para el servicio endian y validar que responda correctamente desde el equipo cliente.

Una vez configurada la zona verde, se valida la comunicación mediante una prueba de conexión desde un equipo cliente. Esta validación confirma que la configuración IP, las reglas de firewall y la ruta de red están funcionando correctamente. La respuesta positiva indica que el cliente puede comunicarse con el servicio Endian, lo cual es un paso fundamental antes de proceder con las zonas restantes tal como se puede apreciar en la siguiente figura

Figura 5. Respuesta exitosa desde equipo cliente a servicio endian



Fuente: Autoría Propia

Una vez que se genera la respuesta exitosa, ya se puede continuar con la configuración de las dos zonas restantes accediendo al servicio endian desde el equipo cliente vía web.

Ahora el siguiente paso es configurar las 2 zonas restantes (zona naranja y zona roja). Se configura primero el acceso a endian desde el equipo cliente ingresando a través de la interfaz web.

Esta configuración adicional en el servidor Ubuntu busca garantizar la conectividad de múltiples interfaces, alineadas con las distintas zonas de red. Cada interfaz debe configurarse cuidadosamente para evitar conflictos y facilitar la administración del tráfico que se enruta hacia Endian. Además, se emplean buenas prácticas como la verificación de rutas activas y la persistencia de la configuración tras reinicios del sistema tal como se puede apreciar en la siguiente figura

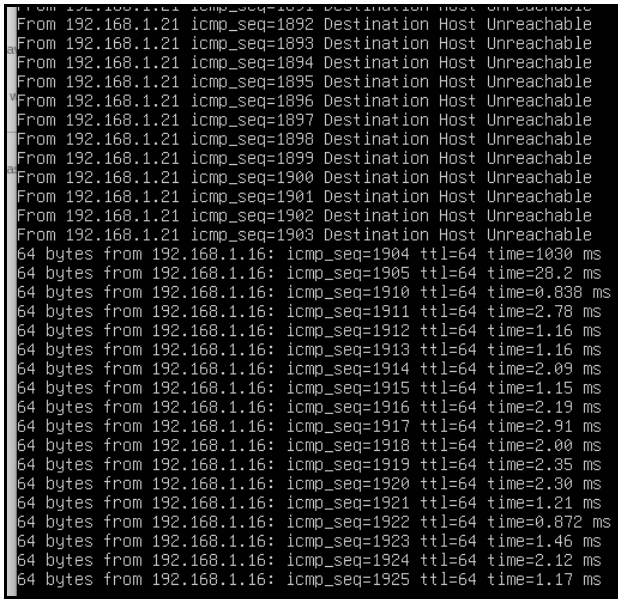
Figura 6. Configuración de ip en servidor ubuntu

Fuente: Autoría Propia

Una vez completada la configuración básica, es necesario validar la conectividad de la zona naranja. Para ello, se ejecuta una prueba de red utilizando el comando ping desde el servidor hacia la IP asignada al equipo Endian en dicha zona. Este procedimiento permite confirmar que la interfaz de red está operativa, que no hay conflictos de direccionamiento IP y que el firewall no está bloqueando el tráfico esencial entre los dispositivos conectados a la zona DMZ.

La zona naranja o DMZ (Zona Desmilitarizada) es utilizada para alojar servidores que requieren estar parcialmente expuestos a internet, como servidores web o FTP. Desde el servidor Ubuntu, se prueba la conectividad hacia Endian para garantizar que los servicios alojados en la DMZ sean accesibles de forma controlada. La DMZ actúa como una zona intermedia de seguridad, aislando los recursos internos de accesos externos directos tal como se puede apreciar en la siguiente figura

Figura 7. Configuración correcta de zona naranja desde servidor ubuntu

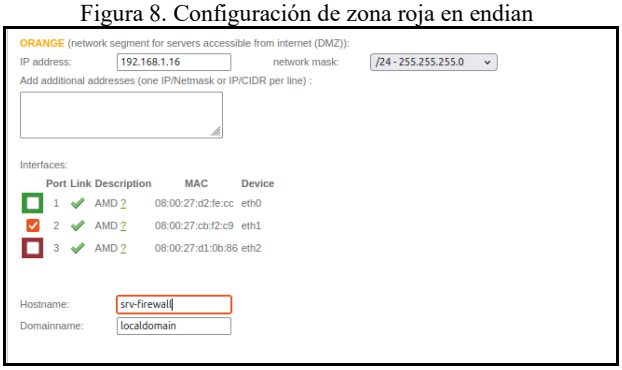


Fuente: Autoría Propia

Ahora se procede a configurar la ultima zona que es la roja de acceso a internet. Esta zona el servicio endian la configura de forma automática por dhcp.

La zona roja está destinada a la conexión con Internet. En Endian, esta zona se configura para obtener su dirección IP por DHCP, lo que facilita su implementación en redes dinámicas. Es importante verificar que el enlace esté operativo, que se haya asignado una IP válida y que el tráfico de salida esté correctamente enrutado a través de esta interfaz para habilitar la navegación externa desde las zonas internas tal como se puede apreciar en la siguiente figura

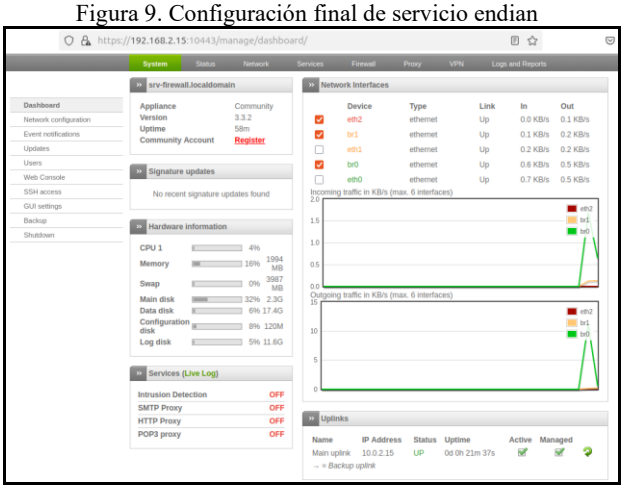
Figura 8. Configuración de zona roja en endian



Fuente: Autoría Propia

Una vez configuradas todas las zonas en el servicio endian y comprobado que se da respuesta exitosa entre cliente-endian y servidor-endian, ya se finaliza la etapa correspondiente a la temática 01 y se procede a la implementación de la siguiente temática validando que todos los servicios estén operativos como se aprecia en la siguiente figura

Figura 9. Configuración final de servicio endian



Fuente: Autoría Propia

3 TEMÁTICA 2: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Para el desarrollo de esta temática, se dispone de la configuración de los servicios http (puerto 80) y ftp (puerto 21) desde el servidor web bajo ubuntu server.

Se ejecutan 2 comandos para su correcta configuración. el primer comando es sudo ufw allow 80/tcp para el servicio http y el segundo comando es sudo ufw allow 21/tcp para el servicio ftp.

Esta figura representa el proceso de habilitación de los puertos de red necesarios para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) desde los servidores ubicados en la zona DMZ. Utilizando la herramienta 'ufw' (Uncomplicated Firewall), se establecen reglas explícitas que permiten el ingreso de conexiones entrantes a través de estos servicios, los cuales son esenciales para la publicación de contenido web y la transferencia de archivos. Esta configuración permite validar la disponibilidad de los servicios desde redes externas y verificar que el firewall no esté bloqueando tráfico legítimo tal como se puede apreciar en la siguiente figura,

Figura 10. Configuración de servicios http y ftp en ubuntu

Fuente: Autoría Propia

El siguiente paso es la denegación del servicio ICMP (puerto 8 y puerto 30) para no permitir hacer ping en la red.

Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Tras haber habilitado los servicios HTTP y FTP, se procede a restringir el tráfico ICMP para fortalecer la seguridad de la red. El protocolo ICMP es comúnmente utilizado para operaciones de diagnóstico como 'ping', pero también puede ser explotado para reconocimiento de red por atacantes. En esta etapa se emplean reglas específicas utilizando iptables para bloquear tipos de paquetes ICMP relacionados con solicitudes de eco y marcas de tiempo, lo que dificulta significativamente los intentos de escaneo o mapeo de la red desde el exterior tal como se puede apreciar en la siguiente figura

Figura 11. Configuración de servicios http y ftp en ubuntu

Fuente: Autoría Propia

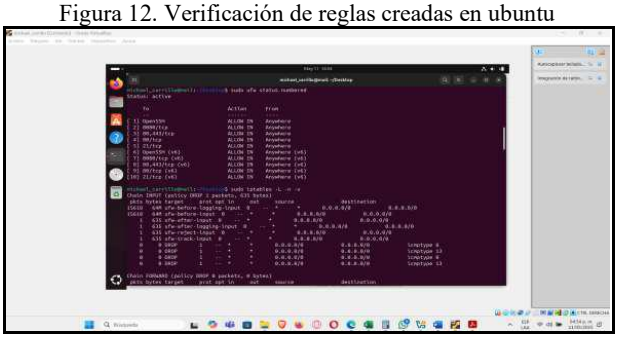
Para este proceso se aplican los siguientes comandos. El primer comando es sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP y el segundo comando es sudo iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP.

El siguiente paso es verificar las reglas creadas. Para eso se aplican 2 comandos que muestran la información de las reglas creadas

Una vez aplicadas las políticas de firewall, es fundamental verificar que dichas reglas se hayan

implementado correctamente. Para ello, se utilizan comandos como 'ufw status numbered' para listar las reglas activas de forma numerada, y 'iptables -L -n -v' para revisar el detalle de las cadenas, protocolos, puertos y bytes procesados. Esta verificación asegura que el comportamiento del firewall corresponde con las restricciones configuradas, validando así su efectividad en el entorno simulado. tal como se puede apreciar en la siguiente figura

Figura 12. Verificación de reglas creadas en ubuntu



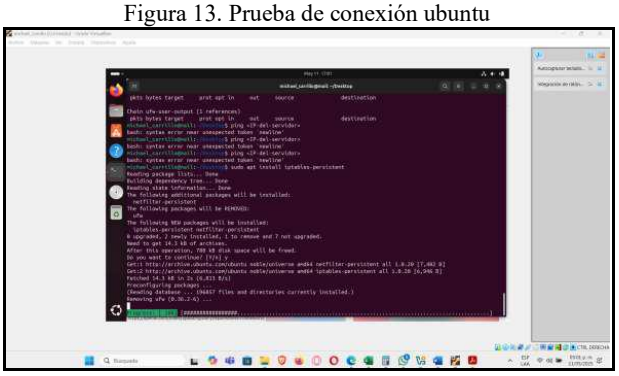
Fuente: Autoría Propia

Los comandos ejecutados en esta fase son sudo ufw status numbered y sudo iptables -L -n -v. Con esto se asegura que los servicios se hayan denegado de forma exitosa.

El paso final para esta temática es realizar la prueba de conexión mediante la ejecución del comando sudo apt install iptables-persistent

La validación final de esta etapa consiste en probar la persistencia y el impacto de las reglas configuradas mediante la instalación de la utilidad 'iptables-persistent', la cual asegura que las reglas se mantendrán tras reinicios del sistema. Además, se ejecuta el comando 'netfilter-persistent save' para guardar la configuración actual. Esta práctica representa un paso crítico en ambientes de producción donde se requiere estabilidad y consistencia en la política de seguridad aplicada a los servicios tal y como se puede apreciar en la siguiente figura

Figura 13. Prueba de conexión ubuntu



Fuente: Autoría Propia

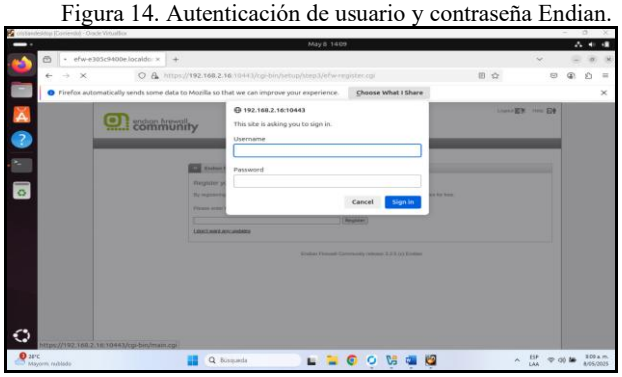
La ejecución del comando sudo netfilter-persistent save verifica y valida que los servicios solicitados en la temática 03 se cumplen exitosamente y con esto se procede a la implementación de la siguiente temática.

4 TEMÁTICA 3: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Para el desarrollo de esta temática es necesario como producto esperado crear un perfil y establecer una lista negra para algunos sitios web, A través de la opción proxy crear un usuario y asociarlo a un grupo. Establecer una política de acceso y vincular el perfil creado en el punto anterior para relacionarlo también con la política de autenticación.

Durante la implementación del proxy HTTP no transparente, se inicia sesión en la interfaz administrativa del sistema Endian. El sistema solicita credenciales válidas, lo cual representa un primer filtro de seguridad. Este acceso autenticado permite aplicar políticas de navegación según perfiles de usuario, garantizando que solo usuarios autorizados puedan configurar o modificar reglas relacionadas con el acceso a Internet desde la red interna. tal como se puede apreciar en la siguiente figura

Figura 14. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

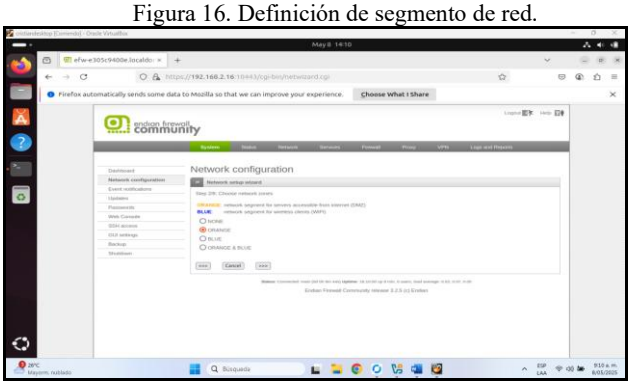
En esta sección se configura la red en modo DHCP, permitiendo que el sistema Endian asigne dinámicamente direcciones IP dentro del rango definido para cada zona. Esta opción es útil durante las pruebas iniciales o en entornos donde se desea facilitar la gestión de IPs. Sin embargo, se recomienda validar que las direcciones asignadas estén dentro del segmento correcto para evitar conflictos o fugas de tráfico tal como se puede apreciar en la siguiente figura

Figura 15. Configuración de red en modo dhcp.

Fuente: Autoría propia

Se configura el módulo de Network configuration y luego se configura la red en modo dhcp, para lo cual se procede a definir explícitamente el segmento de red para cada zona. En este caso, se asigna el rol de 'orange' a un segmento que será parte de la zona DMZ. Esta clasificación permite a Endian aplicar reglas de control específicas según la zona, permitiendo un mayor control sobre el flujo de tráfico que ingresa o sale hacia Internet. Esta definición es crítica para establecer políticas diferenciadas de seguridad entre zonas expuestas y privadas tal como se puede apreciar en la siguiente figura

Figura 16. Definición de segmento de red.

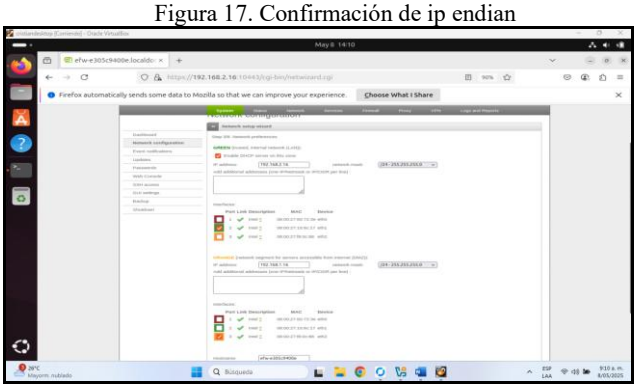


Fuente: Autoría propia

En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado orange para definir el segmento de red que será accesible desde Internet dmz.

A continuación, se presentan las direcciones IP asignadas a las zonas verde y naranja del firewall Endian. Estas direcciones deben coincidir con las configuraciones realizadas previamente en los equipos cliente y servidor, asegurando así una comunicación efectiva y sin errores de enrutamiento. Esta verificación es clave antes de habilitar servicios como el proxy o las reglas de contenido tal como se puede apreciar en la siguiente figura

Figura 17. Confirmación de ip endian

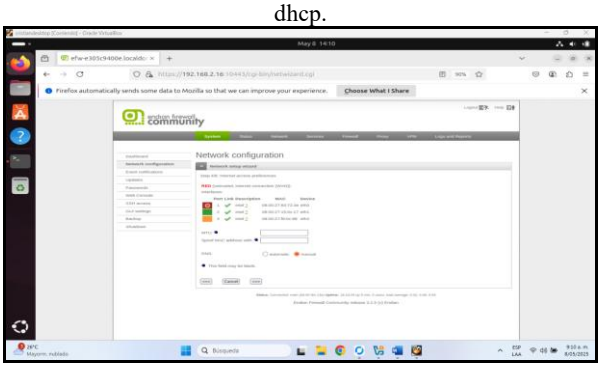


Fuente: Autoría propia.

Se confirman las ips para las zonas verde y naranja de acuerdo con la temática 01.

Aquí se confirma que la zona roja, encargada de la salida a Internet, ha recibido correctamente su configuración por medio de DHCP. Esto valida que el enlace externo está operativo y que el firewall puede conectarse con servidores remotos, condición indispensable para aplicar filtrado de navegación desde zonas internas mediante el proxy configurado tal como se puede apreciar en la siguiente figura

Figura 18. Confirmación de configuración de red en dhcp.

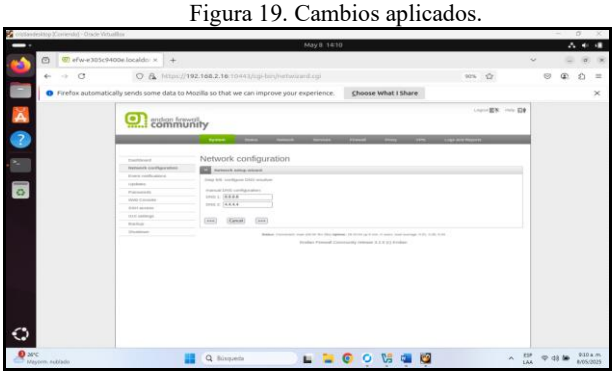


Fuente: Autoría propia

De igual forma se confirma la zona red dhcp.

Una vez finalizadas todas las configuraciones, se aplican los cambios para que entren en vigor. Este paso permite que el sistema recargue su configuración de red, políticas de proxy y listas negras. El correcto guardado y activación de estos cambios asegura que las políticas establecidas comiencen a operar en tiempo real sin necesidad de reiniciar el sistema tal como se puede apreciar en la siguiente figura

Figura 19. Cambios aplicados.

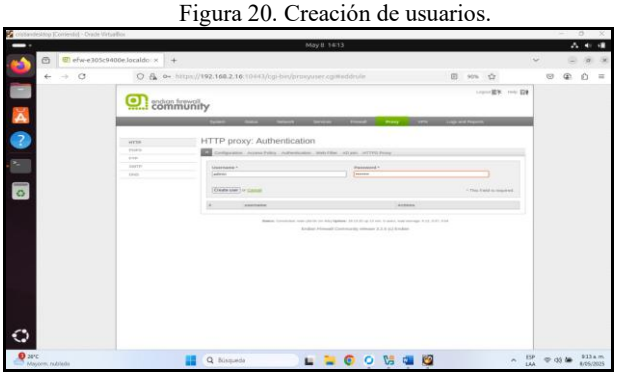


Fuente: Autoría propia

Se aplican los cambios y se procede a la creación de usuarios.

Se crea un nuevo usuario en el módulo de autenticación del sistema Endian. Este usuario podrá ser vinculado a perfiles de navegación específicos, lo cual permite establecer un control granular sobre las páginas que puede visitar, los horarios de acceso y las restricciones definidas por la organización. Este enfoque refuerza la trazabilidad y el cumplimiento de políticas internas de uso de Internet tal como se puede apreciar en la siguiente figura

Figura 20. Creación de usuarios.

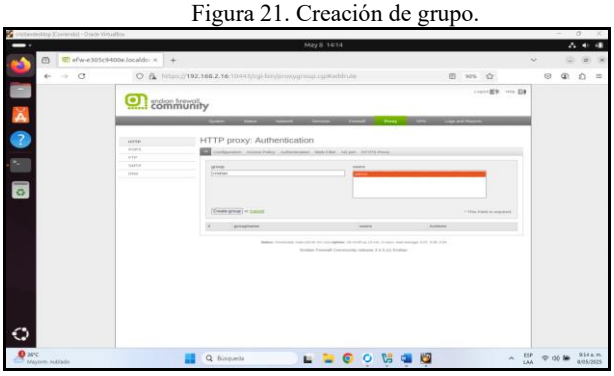


Fuente: Autoría propia

Se crea el usuario en el módulo de autenticación.

Además del usuario, se procede a la creación de un grupo al cual se asocia dicho usuario. La utilización de grupos facilita la administración de múltiples usuarios que comparten las mismas reglas de navegación. Esta práctica es común en entornos corporativos, donde se definen perfiles como 'administradores', 'soporte' o 'usuarios estándar', cada uno con distintos niveles de acceso a contenido web tal como se puede apreciar en la siguiente figura

Figura 21. Creación de grupo.

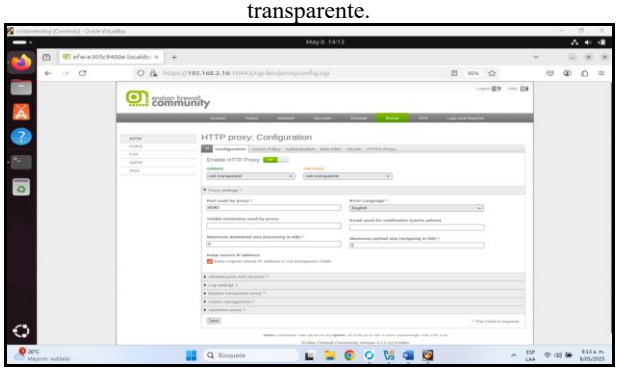


Fuente: Autoría propia

Se crea el grupo y se asocia el usuario admin a dicho grupo.

Aquí se muestra la activación del servicio de proxy en modo no transparente, lo que significa que los usuarios deben configurar explícitamente sus navegadores para usar el proxy. Esta modalidad ofrece mayor control y seguridad, ya que permite aplicar autenticación por usuario y políticas de filtrado más estrictas. Se crea además una lista negra denominada 'listanegra', en la que se incluyen dominios bloqueados de forma categórica tal como se puede apreciar en la siguiente figura

Figura 22. Habilitación de proxy y modo no transparente.

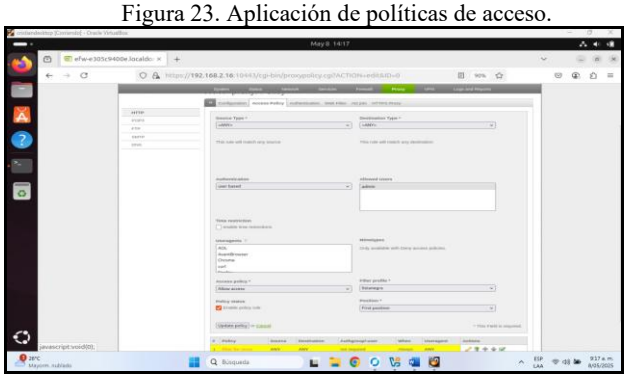


Fuente: Autoría propia

Se habilita el servicio proxy.y se crea un nuevo filtro con el nombre listanegra, donde se bloquean las páginas solicitadas y se guardan los cambios.

Con la lista negra creada y el servicio de proxy activo, se genera una política de acceso donde se vincula al usuario 'admin' y se aplica la regla de restricción definida. Esta política asegura que todo tráfico web proveniente del usuario autenticado pase por los filtros del proxy, y que los sitios incluidos en la lista negra sean bloqueados inmediatamente, conforme a las políticas de seguridad definidas por la institución tal como se puede apreciar en la siguiente figura

Figura 23. Aplicación de políticas de acceso.

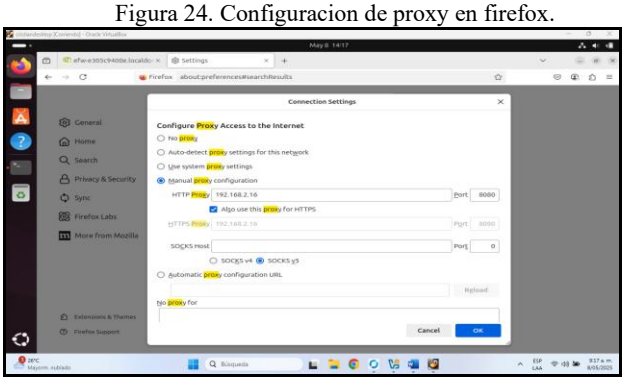


Fuente: Autoría propia

Se crea una política de acceso donde se asocia el usuario admin, se aprueba la regla que se creó llamada listanegra y se ajusta la configuración.

En esta etapa se configura manualmente el navegador Firefox para utilizar el proxy Endian. Se especifica la IP del firewall como servidor proxy tanto para HTTP como para HTTPS. Esta configuración asegura que todo el tráfico web generado por el navegador sea interceptado y evaluado por el sistema Endian antes de llegar a su destino, garantizando la aplicación de las políticas de autenticación y filtrado establecidas previamente como se aprecia en la siguiente figura

Figura 24. Configuracion de proxy en firefox.

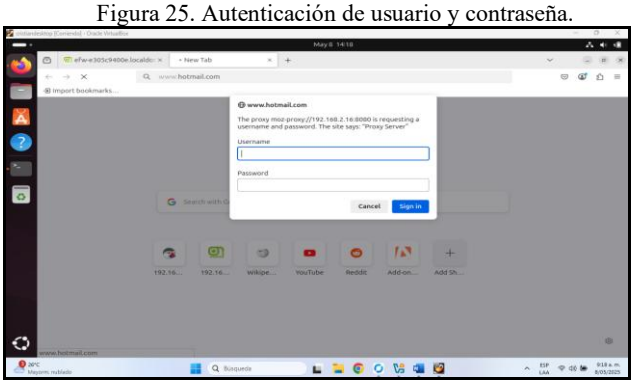


Fuente: Autoría propia

En firefox se configura el proxy donde se define la ip 192.168.10.1 y el mismo proxy en HTTPS.

Tras configurar el proxy en el navegador, se accede a un sitio web bloqueado como www.hotmail.com. El sistema solicita autenticación de usuario, lo que valida la implementación del mecanismo de control de acceso. Solo los usuarios autenticados podrán navegar, lo que añade una capa adicional de seguridad y control en el acceso a contenido externo desde la red interna tal como se puede apreciar en la siguiente figura

Figura 25. Autenticación de usuario y contraseña.



Fuente: Autoría propia

Al acceder a www.hotmail.com ya solicita autenticación de usuario.

Una vez autenticado el usuario, el sistema responde con un mensaje de acceso denegado al intentar ingresar a www.hotmail.com. Esto confirma que la política de restricción funciona correctamente y que el sitio está incluido en la lista negra. Esta validación refuerza la efectividad del proxy como herramienta de cumplimiento de políticas de navegación tal como se puede apreciar en la siguiente figura

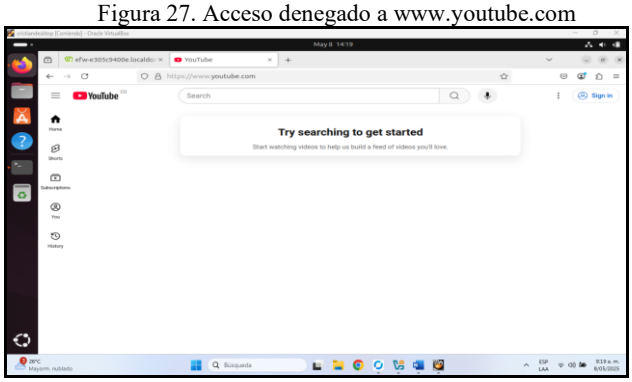
Figura 26. Acceso denegado de www.hotmail.com

Fuente: Autoría propia (Cristian)

Luego de colocar la autenticación muestra un mensaje de acceso restringido.

De manera similar, el intento de acceso a www.youtube.com es bloqueado por el sistema, demostrando que múltiples dominios pueden ser incluidos en las políticas de restricción. Este control permite a las organizaciones mejorar la productividad y minimizar riesgos de exposición a contenido no deseado o inseguro desde la red interna tal como se puede apreciar en la siguiente figura

Figura 27. Acceso denegado a www.youtube.com



Fuente: Autoría propia

De igual forma al entrar a www.elnuevodia.com.co aparece un mensaje de acceso restringido.

El último ejemplo confirma que incluso sitios de noticias pueden ser restringidos si así lo requiere la política organizacional. La capacidad de Endian para filtrar sitios específicos ofrece flexibilidad total al administrador de red, quien puede adaptar las reglas a las necesidades puntuales de cada grupo de usuarios o periodo de tiempo tal y como se puede apreciar en la siguiente figura

Figura 28. Acceso denegado a www.elnuevodia.com.co

Fuente: Autoría propia

Con esto se garantiza la configuración correcta y el producto esperado para todo lo solicitado en la temática 05.

5 CONCLUSIONES

La implementación de GNU/Linux Endian en VirtualBox permitió comprender la estructura lógica de una red segmentada en zonas de seguridad: verde (LAN), roja (WAN) y naranja (DMZ). La correcta asignación de tarjetas de red y su correspondiente configuración facilitaron el aislamiento y control del tráfico entre segmentos, sentando las bases para políticas más avanzadas. Esta instalación demostró la importancia de establecer un entorno de pruebas que simule una red real, permitiendo validar esquemas de seguridad desde un entorno controlado.

La habilitación selectiva de servicios desde la zona DMZ confirmó la efectividad del modelo de seguridad por capas implementado con Endian. Al permitir únicamente los puertos HTTP (80) y FTP (21) desde servidores en Ubuntu Server, se logró una exposición controlada hacia otras zonas de la red. La restricción del protocolo ICMP evidenció la capacidad de Endian para bloquear tipos específicos de tráfico, mejorando así la seguridad frente a escaneos o intentos de reconocimiento. Las pruebas realizadas mediante consola y monitoreo de tráfico validaron la aplicación de las reglas establecidas.

La configuración de un proxy HTTP no transparente con autenticación demostró ser una solución eficaz para el control del acceso a contenidos desde la red interna. La creación de perfiles con políticas de restricción, listas negras y usuarios autenticados permitió definir un entorno de navegación supervisado. La verificación del bloqueo de sitios específicos como YouTube y Hotmail desde la LAN confirmó el funcionamiento correcto del proxy y su integración con el sistema de políticas. Esta funcionalidad refuerza la importancia del proxy como herramienta para la gestión del tráfico web y la aplicación de políticas organizacionales.

6 REFERENCIAS

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

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

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

[4] Fernández, A. (2011). Cámbiate a LINUX. RC Libros.

[5] Hernández, P. F., & Sánchez, J. (2022). Servidores para administración remota y compartir recursos. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53212.

[6] Jiménez, J. H. (2016). Shell Script para Bash. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/9758.

[7] LaCroix, J. (2020). Mastering Ubuntu Server. Packt Pub. https://research-ebsco/com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952.

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

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

[10] Torvalds, L. (1999). The linux edge. Communications of the ACM, 42(4), 38-39.