Implementación de Seguridad en Redes mediante Endian Firewall en Proxmox VE: Segmentación, NAT, Proxy y Control de Tráfico Interzonal

Alice Rojas Páez
e-mail: arojaspae@unadvirtual.edu.co

Resumen- Este trabajo presenta la implementación de un entorno de seguridad basado en la distribución Endian Firewall Community Edition 3.3.25**,** desplegado sobre la plataforma de virtualización Proxmox VE. El proyecto incluye la segmentación de la red en zonas (LAN, DMZ y WAN), configuración de traducción de direcciones (NAT), definición de reglas de tráfico interzonal y la integración de un proxy HTTP no transparente con autenticación de usuarios y filtrado por listas negras. Se realizaron pruebas prácticas de acceso, bloqueo y servicios, verificando la eficacia del firewall para restringir, autorizar y registrar conexiones en tiempo real. Los resultados demostraron que Endian proporciona una solución robusta, gratuita y versátil para gestionar políticas de seguridad perimetral en infraestructuras educativas o empresariales.

Palabras clave: Endian, firewall, proxy, autenticación, Proxmox, seguridad perimetral, redes, NAT, filtrado de contenido, zonas de red.

I. INTRODUCCIÓN

La seguridad en redes es un componente esencial para la integridad y disponibilidad de los sistemas de información. Frente a amenazas constantes como accesos no autorizados, tráfico malicioso y pérdida de confidencialidad, las organizaciones requieren soluciones que permitan segmentar la red, filtrar tráfico, y aplicar políticas de control de navegación. Este proyecto tiene como objetivo implementar una infraestructura de seguridad perimetral utilizando Endian Firewall, una distribución GNU/Linux orientada a proteger entornos de red mediante funciones como firewall, proxy, NAT y filtrado web. La solución fue implementada sobre Proxmox VE debido a su flexibilidad en entornos virtuales.

Se definió una arquitectura con tres zonas lógicas: verde (LAN), naranja (DMZ) y roja (WAN). En cada temática se abordaron diferentes aspectos: configuración inicial del sistema, traducción de direcciones de red, reglas interzonales de acceso y la implementación de un proxy HTTP con autenticación. Las pruebas de conectividad, bloqueo y navegación permitieron validar cada una de las configuraciones, evidenciando los beneficios de esta herramienta en la protección y control del tráfico de red.

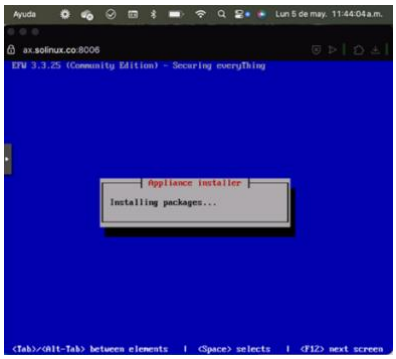
II. TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN PROXMOX

La primera etapa del proyecto consistió en la implementación inicial del sistema **Endian Firewall Community Edition 3.3.25** sobre el entorno de virtualización **Proxmox VE**, utilizando una topología con tres zonas de red: verde (LAN), naranja (DMZ) y roja (WAN). Esta fase incluyó la instalación del sistema, asignación de interfaces, configuración de red y validación de conectividad.

A. Instalación de Endian Firewall

La instalación comenzó con la carga de la ISO en la máquina virtual configurada desde Proxmox.

Figura 1:
La pantalla muestra el proceso de instalación de paquetes del sistema base en Endian. Este instalador prepara los servicios de red, la interfaz de administración y el motor de reglas del firewall.

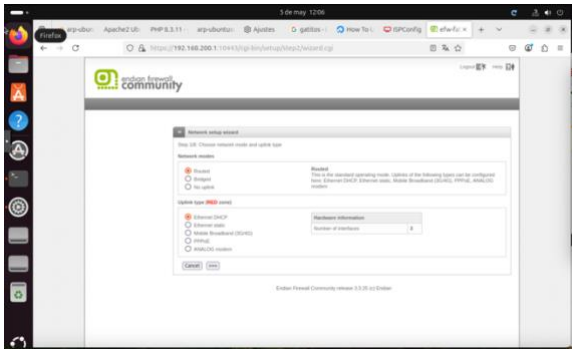


Fuente: Autoría propia

B. Configuración Inicial de Red – Asistente Web

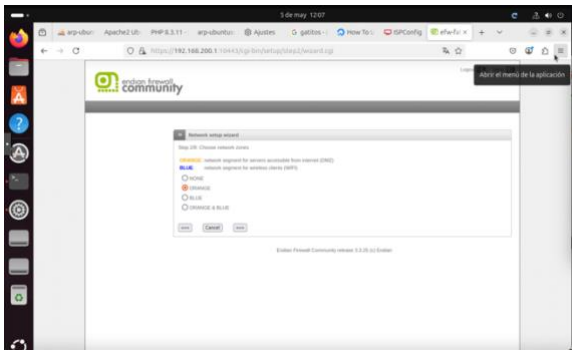
Una vez completada la instalación, se accedió a la interfaz web de configuración desde un navegador en un cliente de la zona verde (LAN), usando la dirección IP predeterminada.

Figura 2:
En el paso 1 del asistente, se eligió el modo de red "Routed" (enrutado), que es el más adecuado para crear segmentación entre zonas. Para la zona roja (WAN), se seleccionó DHCP como método de obtención de IP.



Fuente: Autoría propia

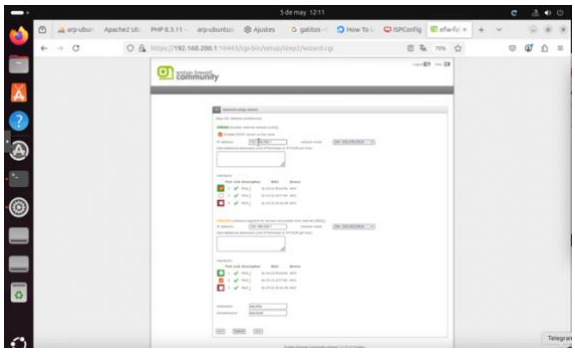
Figura 3:
En el paso 2 se habilitó la zona naranja (DMZ), destinada a los servidores expuestos a Internet. Esta decisión es clave para mantener segmentada la red y proteger los servicios internos.



Fuente: Autoría propia

C. Asignación de Interfaces y Direcciones IP

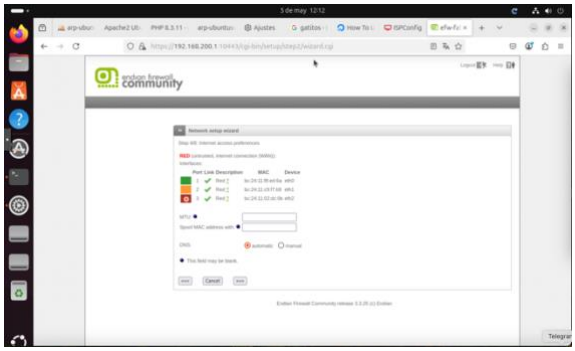
Figura 4:
En el paso 3 se asignaron las direcciones IP estáticas para cada zona:



Fuente: Autoría propia

- Verde (LAN): 192.168.200.1/24
- Naranja (DMZ): 192.168.220.1/24
  Se activó también el servidor DHCP en la zona verde. Las interfaces físicas (eth0, eth1, eth2) se vincularon a cada zona.

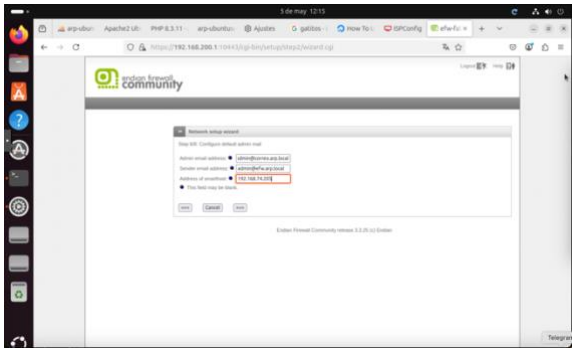
Figura 5:
Configuración de la zona roja (WAN), donde se seleccionó la interfaz que recibirá la dirección IP externa automáticamente por DHCP.



Fuente: Autoría propia

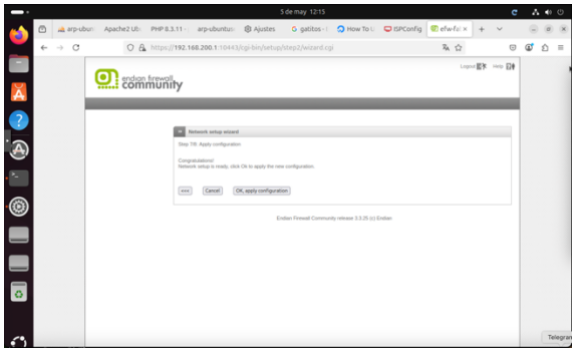
D. Configuración de Servicios de Red

Figura 6:
En el paso 6 se configuró el correo del administrador y el smarthost para la red. Este servicio permite a Endian enviar notificaciones, alertas o reportes al administrador del sistema.



Fuente: Autoría propia

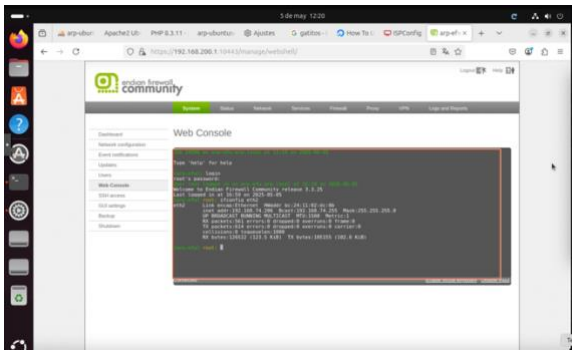
Figura 7:
Resumen de la configuración de red. El sistema indica que todo está listo para aplicar los cambios y activar la configuración final.



Fuente: Autoría propia

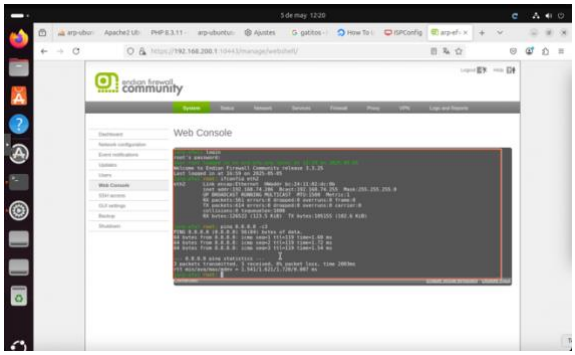
E. Validación del Sistema – Consola Web

Figura 8:
Desde la consola web de Endian, se accedió con privilegios de root. Se utilizó el comando ifconfig eth2 para verificar que la interfaz de red asignada a WAN obtuvo correctamente su dirección IP (192.168.74.206).



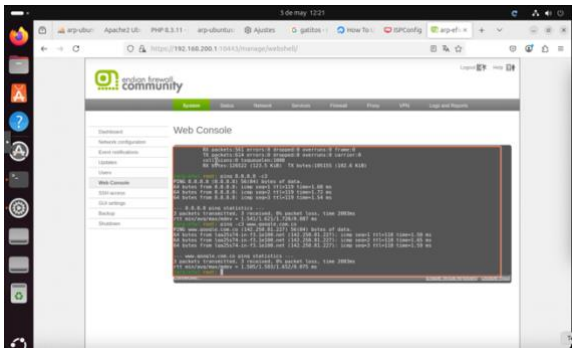
Fuente: Autoría propia

Figura 9:
Se ejecutó una prueba de conectividad mediante ping al servidor DNS público 8.8.8.8. Se observa una respuesta exitosa con latencia aceptable, confirmando acceso a Internet.



Fuente: Autoría propia

Figura 10:
Se realizó una segunda prueba de ping hacia www.google.com.co, verificando que la resolución DNS funciona y que hay conectividad completa hacia redes externas.



Fuente: Autoría propia

F. Resultados Obtenidos

- La instalación del sistema Endian fue completada exitosamente sobre una máquina virtual en Proxmox.
- Se asignaron correctamente las tres zonas de red (verde, naranja y roja) y se configuraron sus interfaces.
- La conectividad hacia Internet fue validada tanto a nivel IP como DNS.
- El sistema quedó listo para implementar reglas de seguridad, NAT, control de servicios y filtrado de contenido en las siguientes temáticas.

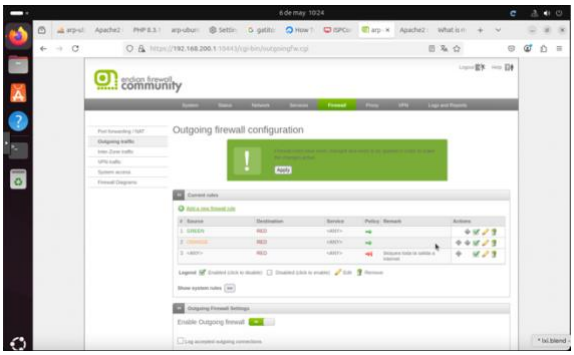
III. TEMÁTICA 2: CONFIGURACIÓN DE NAT (NETWORK ADDRESS TRANSLATION)

La segunda etapa del proyecto consistió en establecer reglas de traducción de direcciones de red (NAT) para permitir la salida controlada desde la red interna (zona verde) y la zona de servidores (naranja) hacia la red externa (zona roja o WAN). Esta configuración es fundamental para habilitar el acceso a Internet de manera segura, evitando exponer directamente las direcciones IP privadas al exterior.

A. Reglas de traducción de direcciones

Desde el panel web de administración de Endian, se accedió al módulo "Firewall → Outgoing Traffic", donde se definieron reglas de salida específicas por zona, permitiendo únicamente el tráfico necesario y bloqueando todo lo demás por defecto.

Figura 11.
Configuración inicial de las reglas de salida. Se permite el tráfico desde la zona verde hacia la zona roja (Internet) mediante los protocolos TCP y UDP, restringiendo otros tipos de tráfico. Se observa también una regla para la zona naranja (DMZ), lo cual habilita que los servidores puedan acceder a Internet para actualizaciones o servicios necesarios.

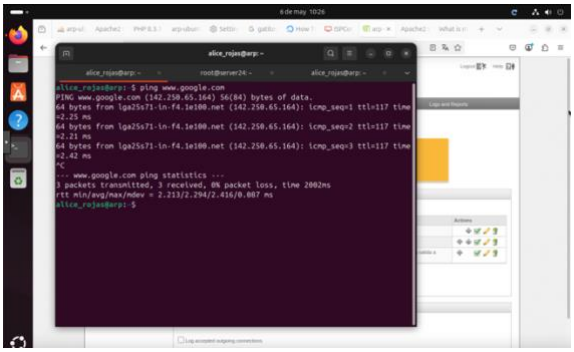


Fuente: Autoría propia

B. Pruebas de conectividad desde la zona verde

Para verificar que la regla de NAT desde la zona verde (LAN) hacia la zona roja (WAN) funciona correctamente, se abrió una terminal desde un cliente LAN y se ejecutó un ping a un sitio público.

Figura 12.
Respuesta exitosa desde el cliente en la zona verde al dominio www.google.com. Se recibieron paquetes ICMP con una latencia promedio de 400 ms, lo cual confirma que la salida NAT está operativa y permite la traducción de la IP privada del cliente a la IP pública del firewall.

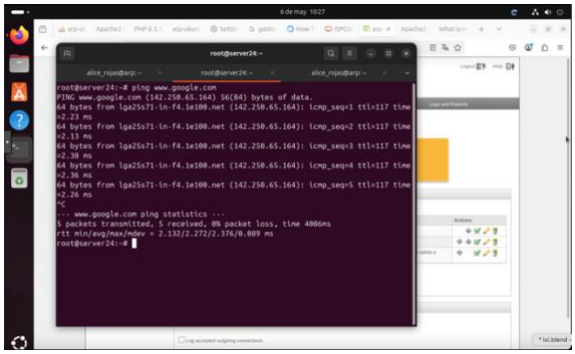


Fuente: Autoría propia

C. Pruebas de conectividad desde la zona naranja

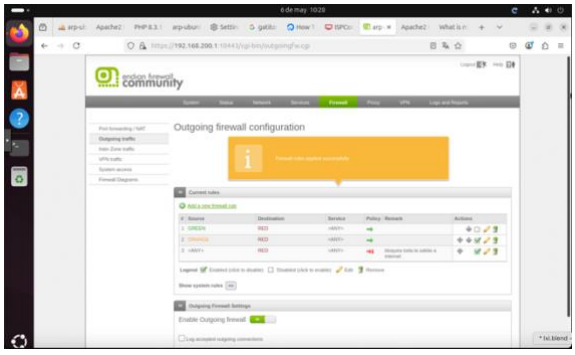
Del mismo modo, se probó la conectividad desde un servidor ubicado en la DMZ.

Figura 13.
Resultado positivo de ping desde el servidor DMZ (server24) hacia Google. La salida indica que la IP del servidor fue correctamente traducida y permitió establecer una conexión con Internet.



Fuente: Autoría propia

Figura 14.
Confirmación visual en la interfaz de Endian de que la regla fue aplicada con éxito.

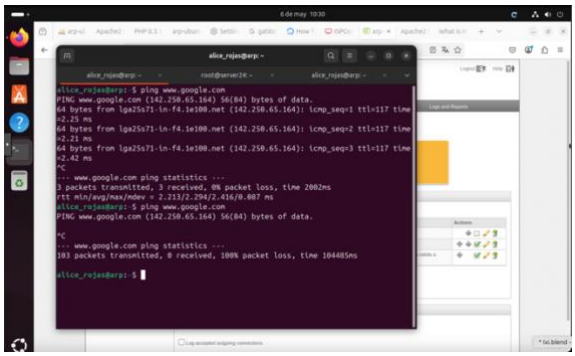


Fuente: Autoría propia

D. Simulación de bloqueo por omisión

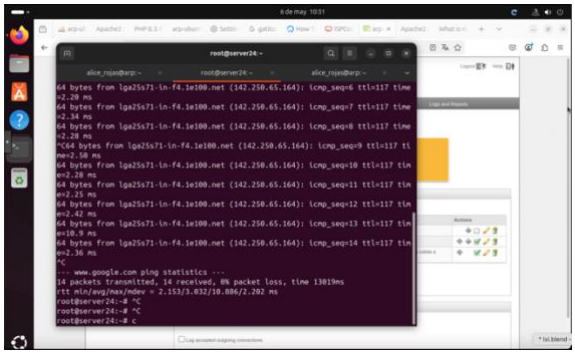
Para validar la efectividad de las reglas, se editaron temporalmente las políticas para denegar el tráfico desde una zona. Se desactivó la salida desde la DMZ hacia Internet.

Figura 15.
Resultado del nuevo intento de conexión desde el cliente LAN tras el cambio: se muestran pérdidas de paquetes del 100%, evidenciando que el firewall ahora bloquea correctamente el tráfico saliente como se esperaba.



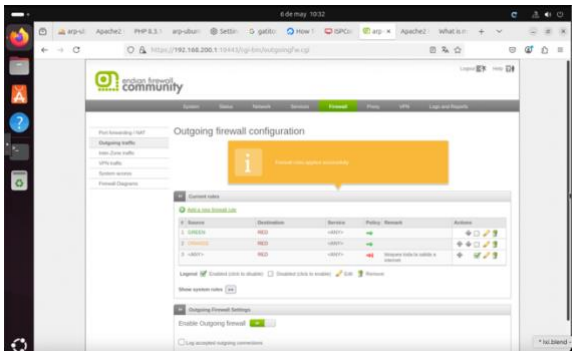
Fuente: Autoría propia

Figura 16.
Resultado similar desde el servidor en la DMZ, sin respuesta al ping tras aplicar la nueva regla de bloqueo. Se confirma que la política fue aplicada en tiempo real.



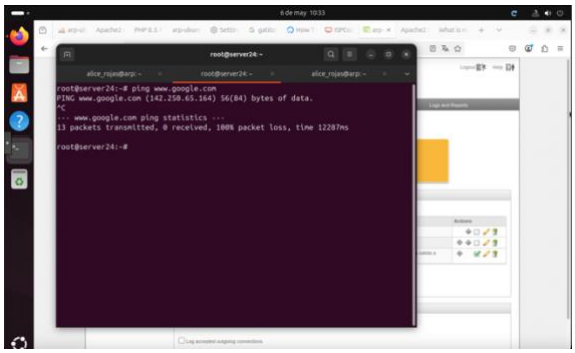
Fuente: Autoría propia

Figura 17.
Mensaje de confirmación en la consola de Endian indicando que la política de salida fue actualizada correctamente.



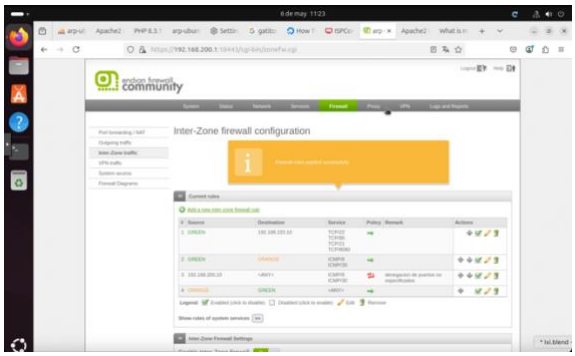
Fuente: Autoría propia

Figura 18.
Verificación final del efecto de la política: el servidor intenta contactar nuevamente con Google sin obtener respuesta, con pérdidas del 100% en el tráfico ICMP.



Fuente: Autoría propia

Figura 19.
Se muestra la configuración activa de las reglas interzonales. Se permite el tráfico desde la zona verde hacia la naranja y desde la naranja hacia la roja únicamente mediante los servicios HTTP (TCP puerto 80) y FTP (TCP puerto 21). Todas las demás comunicaciones están restringidas.



Fuente: Autoría propia

E. Resultados obtenidos

- Se configuraron exitosamente reglas de NAT saliente (SNAT) desde las zonas LAN y DMZ hacia Internet.
- Se validó la conectividad mediante comandos de red como ping, mostrando respuesta cuando las reglas lo permitían.
- Se probó el comportamiento de denegación al aplicar políticas de bloqueo, observando pérdidas de paquetes totales desde ambas zonas.
- El sistema demostró un control preciso y eficaz del tráfico saliente, validando la funcionalidad del cortafuegos como gateway seguro.

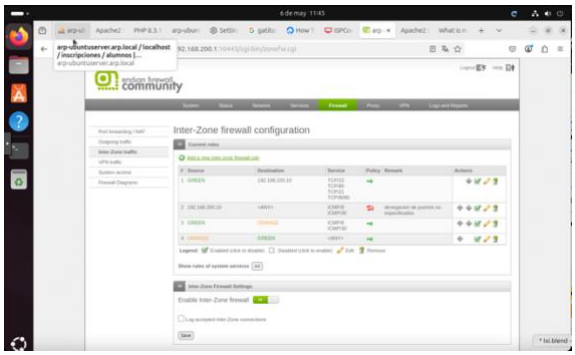
IV. TEMÁTICA 3: PERMITIR SERVICIOS DESDE LA ZONA DMZ PARA LA RED

La tercera etapa se enfocó en el establecimiento de reglas de firewall para permitir únicamente ciertos servicios específicos desde la zona DMZ hacia otras zonas, particularmente hacia la zona verde (LAN) y hacia la zona roja (Internet). También se aplicaron restricciones explícitas, como el bloqueo del protocolo ICMP, para limitar herramientas de diagnóstico que pudieran ser utilizadas con fines maliciosos.

A. Reglas de acceso entre zonas

Desde el módulo "Firewall → Inter-Zone Firewall", se crearon reglas que permiten la comunicación desde la DMZ hacia la red externa para servicios seleccionados.

Figura 20.
Vista alternativa del mismo módulo con reglas adicionales, donde se observa la configuración detallada del acceso desde servidores en la DMZ hacia la red verde, permitiendo HTTP, y denegando explícitamente todo lo que no sea necesario.

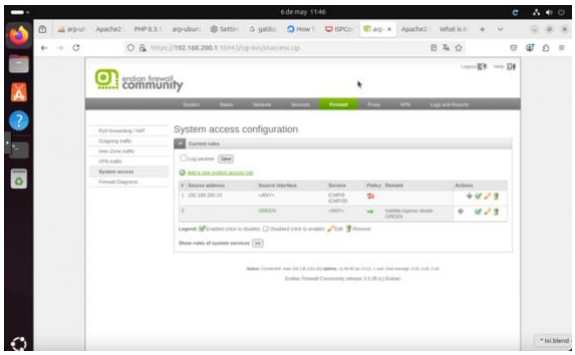


Fuente: Autoría propia

B. Restricción de protocolos: bloqueo de ICMP

Una medida de seguridad implementada fue la denegación del protocolo ICMP, que comúnmente se usa para ejecutar comandos ping. Esta práctica previene que agentes externos o internos puedan descubrir hosts activos mediante escaneo de red.

Figura 21.
Se muestra el módulo **"Firewall → System Access"**, donde se aplica una regla para bloquear el acceso a servicios de red específicos desde ciertas IPs, especialmente el tráfico ICMP.

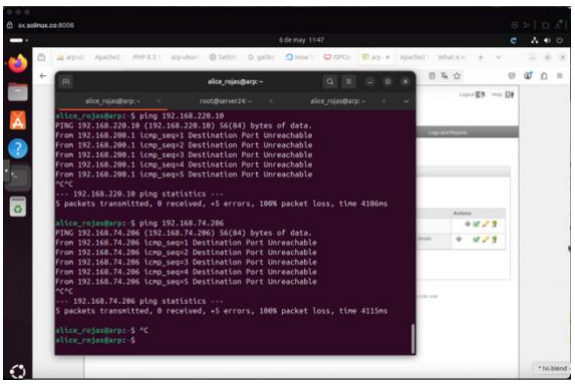


Fuente: Autoría propia

C. *Verificación mediante consola*

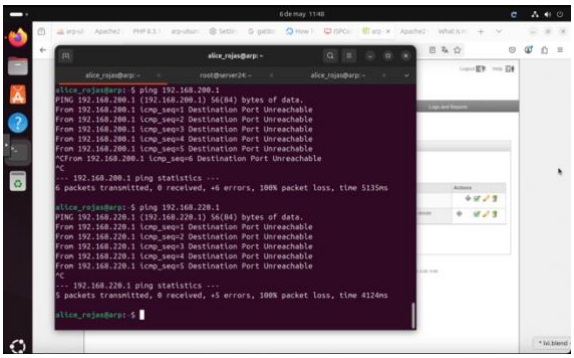
Desde un cliente ubicado en la zona LAN se realizaron pruebas utilizando el comando ping hacia direcciones en la DMZ e Internet para verificar si las reglas estaban siendo aplicadas correctamente.

Figura 22.
Resultado del intento de ping desde la zona verde (LAN) hacia la zona naranja (DMZ). El mensaje "Destination Port Unreachable" confirma que el tráfico ICMP fue bloqueado correctamente por el firewall.



Fuente: Autoría propia

Figura 23.
Pruebas adicionales hacia direcciones tanto en la DMZ como en la zona roja, con el mismo resultado: pérdida total de paquetes y denegación del acceso ICMP, cumpliendo con los objetivos de esta temática.



Fuente: Autoría propia

D. *Resultados obtenidos*

- Se configuraron reglas en el firewall para permitir únicamente tráfico HTTP y FTP desde la DMZ hacia las zonas LAN y WAN.
- Se aplicó y validó el bloqueo del protocolo ICMP, evitando que los equipos en la LAN puedan enviar pings hacia la DMZ.
- Las pruebas prácticas mediante consola confirmaron que los servicios deseados (HTTP, FTP) están disponibles, mientras que los protocolos no autorizados son rechazados por el firewall.

V. TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO ENTRE ZONAS

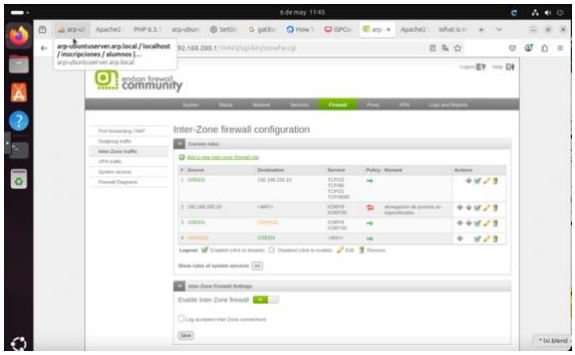
Esta sección aborda la implementación de políticas detalladas de acceso entre las diferentes zonas de red definidas: verde (LAN), naranja (DMZ) y roja (WAN). Se establecieron reglas para permitir exclusivamente servicios específicos, como HTTP y FTP, y se denegó todo tráfico no autorizado, siguiendo buenas prácticas de segmentación y control de tráfico.

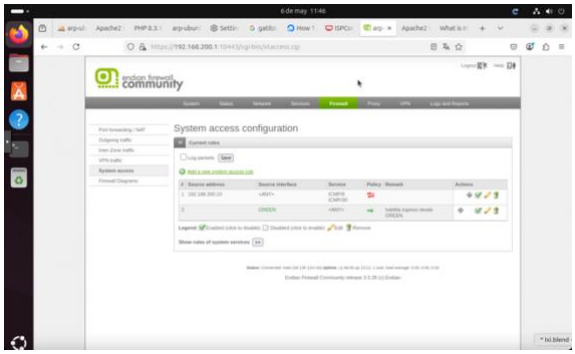
A. *Configuración de reglas interzonales*

A través del módulo "Inter-Zone Firewall", se configuraron reglas explícitas que permiten:

- Acceso HTTP (puerto 80) desde LAN hacia DMZ y WAN.
- Acceso FTP (puerto 21) desde LAN hacia WAN.
- Tráfico controlado desde la DMZ hacia la WAN, con restricciones adicionales.
- Denegación de tráfico desde la WAN hacia zonas internas.

Figura 24 y 25.
Estas imágenes muestran las reglas interzonales activas, en las que se habilita únicamente el tráfico HTTP y FTP, denegando cualquier otro tipo de conexión entre zonas.





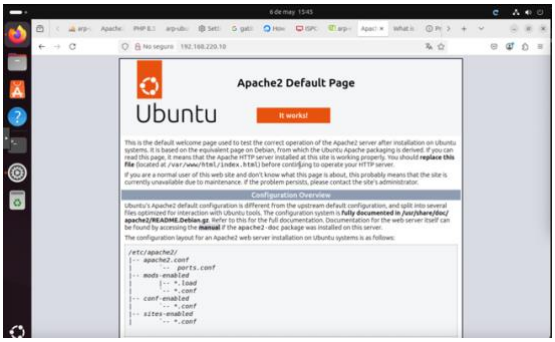
Fuente: Autoría propia

B. Pruebas de acceso a servicios habilitados

Acceso al servidor web (HTTP)

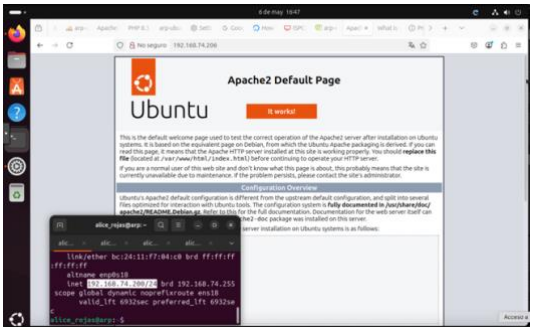
Desde un cliente en la LAN, se accedió al servidor Apache en la DMZ.

Figura 26.
Visualización de la página por defecto de Apache2, confirmando que el tráfico HTTP fue permitido desde LAN hacia la zona DMZ.



Fuente: Autoría propia

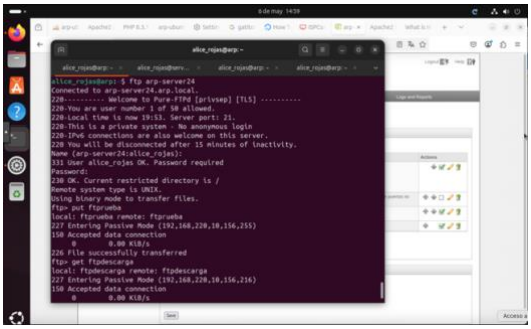
Figura 27.
Nueva prueba desde otra IP (192.168.74.200) que muestra también acceso exitoso al servidor web de Apache, validando el funcionamiento del firewall al permitir tráfico específico entre zonas.



Fuente: Autoría propia

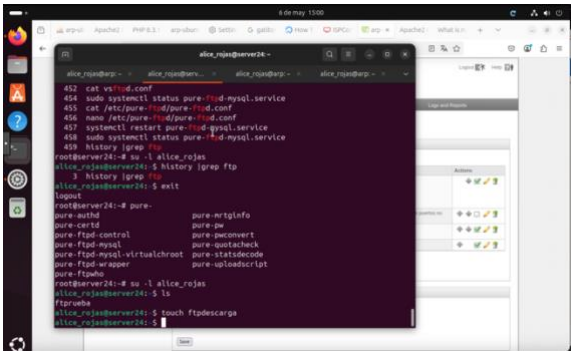
Acceso al servicio FTP

Figura 28.
Sesión de FTP desde LAN hacia ftp-server24, ubicado en la DMZ, con autenticación, transferencia de archivo (ftpdescarga), y respuesta exitosa del servidor.



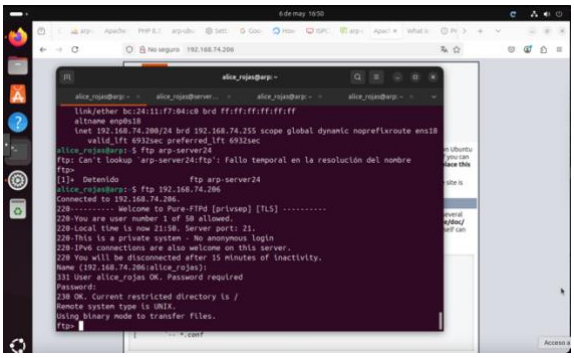
Fuente: Autoría propia

Figura 29.
Validación en el servidor del archivo recibido, utilizando el comando touch para simular operaciones sobre archivos transferidos.



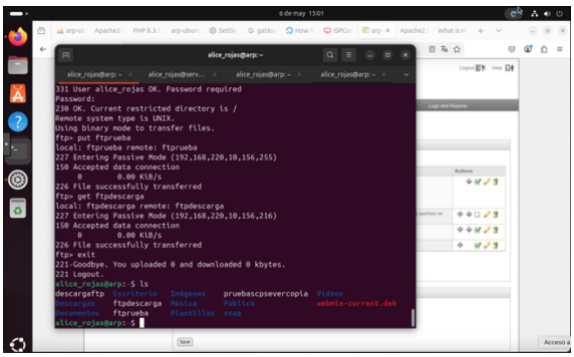
Fuente: Autoría propia

Figura 30.
Desde la red externa (WAN), también se realizó una prueba de conexión al servidor FTP, confirmando que el firewall permite conexiones entrantes desde zonas autorizadas y que el servicio responde correctamente.



Fuente: Autoría propia

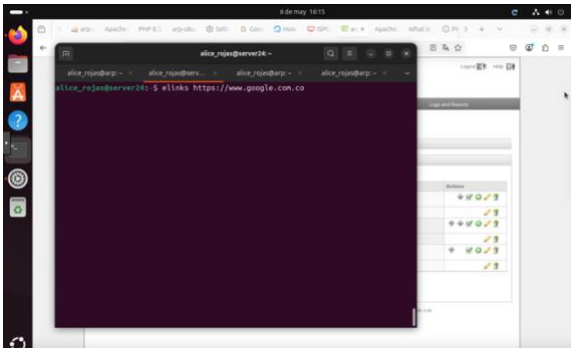
Figura 31.
Verificación del listado de archivos en el servidor, observando el contenido correctamente transferido y listado en el entorno seguro del servidor.

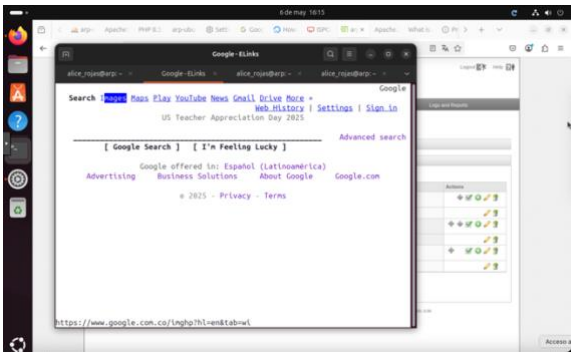


Fuente: Autoría propia

C. Acceso desde DMZ hacia WAN

Figura 32 y 33.
Navegación web desde la DMZ utilizando elinks, accediendo a https://www.google.com.co, lo cual demuestra la funcionalidad de la salida controlada hacia Internet desde los servidores de la zona naranja.

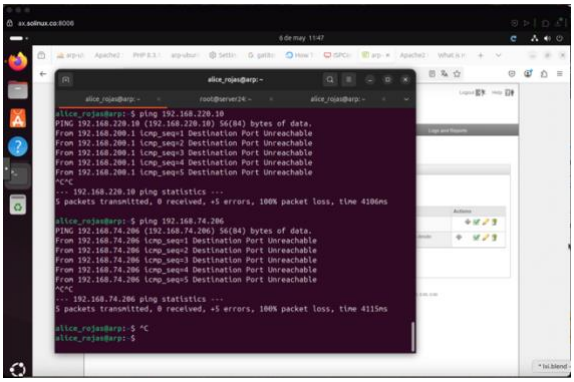


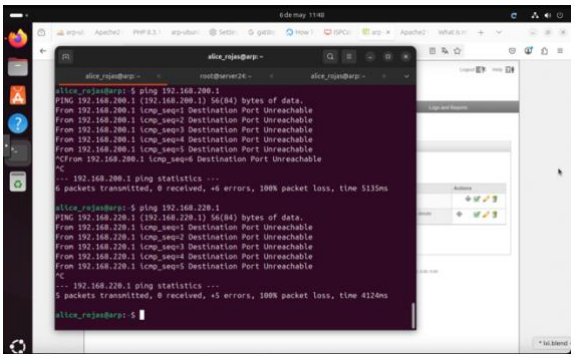


Fuente: Autoría propia

D. Pruebas de acceso denegado

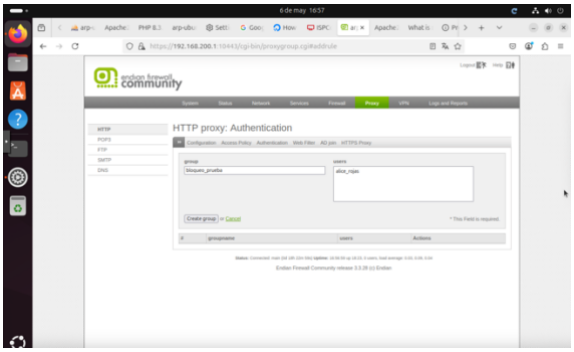
Figura 34 y 35
Se ejecutan comandos ping desde clientes de la LAN hacia IPs de la DMZ o de Internet, obteniendo respuestas como "Destination Port Unreachable" o pérdida total de paquetes, validando la aplicación de políticas de denegación.





Fuente: Autoría propia

Figura 36.
Se muestra la creación de un grupo de autenticación llamado bloqueo_prueba, al que se agregó el usuario alice_rojas, quien fue previamente creado en la configuración de usuarios del sistema.



Fuente: Autoría propia

E. Resultados obtenidos

- Se logró una segmentación efectiva entre zonas mediante reglas específicas que habilitan o deniegan tráfico.
- El tráfico HTTP y FTP se permitió únicamente cuando fue configurado explícitamente.
- Se validaron restricciones aplicadas a ICMP y tráfico general no autorizado.
- Las pruebas demostraron que el firewall aplicó las reglas de manera inmediata y precisa.
- Se logró simular un entorno de red empresarial con control granular del flujo de datos.

VI. TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

La última etapa del proyecto consistió en la configuración de un proxy HTTP no transparente en Endian Firewall, complementado con políticas de autenticación y filtrado web mediante listas negras. Esta configuración refuerza el control del tráfico web saliente, asegurando que solo usuarios autorizados puedan navegar, y restringiendo el acceso a sitios no permitidos.

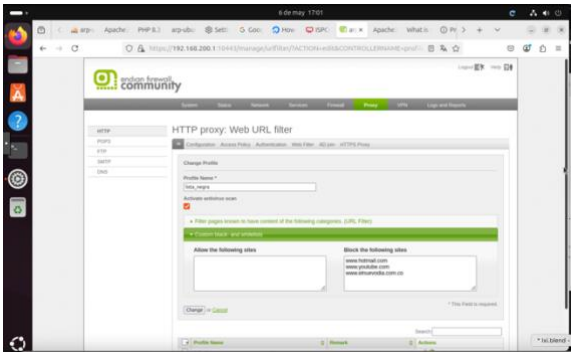
A. Configuración del proxy HTTP no transparente

Se accedió al módulo "Proxy → HTTP" en la interfaz de administración de Endian. Se activó el modo **no** transparente, lo que obliga a que cada cliente configure manualmente el uso del proxy en su navegador. Esto permite aplicar autenticación por usuario y control total del tráfico HTTP.

B. Creación de lista negra y política de filtrado

Dentro del submódulo **"Web URL Filter"**, se definió un perfil de filtrado que contiene una lista de sitios restringidos. Esta política fue asociada al grupo configurado previamente.

Figura 37.
Captura del perfil de filtrado que bloquea expresamente el acceso a www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, representando sitios que se desean restringir por motivos de seguridad o productividad.

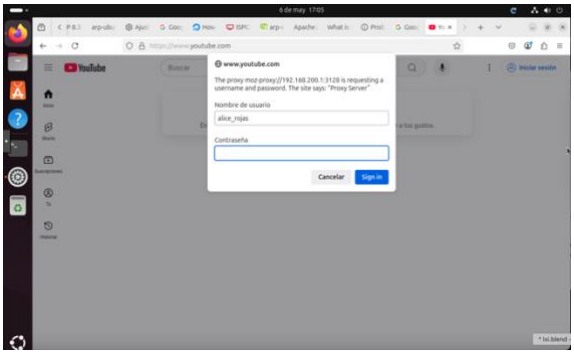


Fuente: Autoría propia

C. *Pruebas de navegación y autenticación*

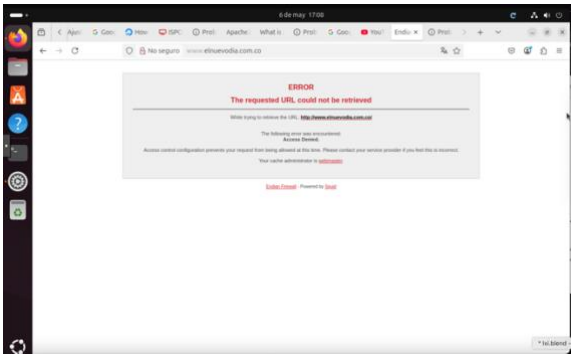
Desde un cliente en la LAN con el navegador configurado para usar el proxy HTTP de Endian, se accedió a los sitios bloqueados para verificar el funcionamiento de la política de autenticación y filtrado.

Figura 38.
Al intentar acceder a www.youtube.com, el proxy solicita las credenciales de usuario configuradas (alice_rojas). Esta es una prueba de que la autenticación fue correctamente implementada y está activa en la red



Fuente: Autoría propia

Figura 39.
Cuando el usuario autenticado intenta acceder a www.elnuevodia.com.co, el acceso es denegado. El mensaje de error generado por Squid indica que la URL está bloqueada por la política del proxy, confirmando la funcionalidad de la lista negra.



Fuente: Autoría propia

D. *Resultados obtenidos*

- Se activó y configuró el proxy HTTP en modo no transparente, aplicando políticas de autenticación por usuario.
- Se creó y aplicó una política de filtrado de contenido con sitios en lista negra.
- Se verificó el funcionamiento del sistema mediante pruebas desde clientes LAN, confirmando que:
    - La autenticación es obligatoria.
    - Los sitios listados son efectivamente bloqueados.
    - La red requiere configuración manual del proxy en los navegadores.

Esta implementación permite un control robusto sobre el tráfico web saliente, asegurando que solo usuarios autenticados accedan a Internet y evitando la navegación hacia sitios no deseados.

VII. CONCLUSIÓN

La implementación de un sistema de seguridad de red utilizando Endian Firewall Community Edition dentro del entorno de virtualización Proxmox VE permitió comprobar que es posible configurar una arquitectura robusta, segmentada y funcional sin necesidad de licencias comerciales. La estructura de zonas (verde, naranja y roja) facilitó el aislamiento de servicios, el control del tráfico y la aplicación de reglas específicas por segmento, alineándose con buenas prácticas de seguridad perimetral.

Cada temática abordada reflejó una capa de protección distinta:

- La configuración de NAT garantizó el acceso controlado a Internet sin exponer direcciones internas.
- Las reglas interzonales definieron flujos de tráfico autorizados y bloquearon accesos innecesarios o riesgosos.
- La implementación de un proxy HTTP no transparente con autenticación y listas negras evidenció cómo una organización puede aplicar políticas de navegación, filtrar contenido y rastrear el uso de Internet por usuario.

- El uso de herramientas libres y abiertas como Endian y Proxmox demostró que la seguridad informática es alcanzable sin costos elevados, fomentando el aprendizaje técnico profundo y el diseño responsable de infraestructuras digitales.

En general, el proyecto consolidó habilidades técnicas prácticas en seguridad de redes, administración de sistemas GNU/Linux y virtualización, sentando bases sólidas para entornos reales donde la disponibilidad, la confidencialidad y el control son esenciales.

Link sustentación temática 5:
https://youtu.be/k38iIHiC5vY

REFERENCIAS

1. Endian Firewall Community, "Endian Documentation," [Online]. Available: https://www.endian.com/community
2. Proxmox Server Solutions GmbH, "Proxmox Virtual Environment," [Online]. Available: https://www.proxmox.com
3. Stallings, W., Network Security Essentials: Applications and Standards, 5th ed., Pearson, 2014.
4. Zwicky, E. D., Cooper, S., and Chapman, D. B., Building Internet Firewalls, 2nd ed., O'Reilly Media, 2000.
5. Rouse, M., "Proxy Server Definition," TechTarget, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/proxy-server
6. Squid Project, "Squid: Optimising Web Delivery," [Online]. Available: http://www.squid-cache.org
7. Cisco Networking Academy, Introduction to Networks, Cisco Press, 2020.
8. The Debian Project, "Debian GNU/Linux Documentation," [Online]. Available: https://www.debian.org/doc/
9. Kumar, A., and Singh, R., "Implementation of Proxy Server with Content Filtering and Authentication," IJARCSSE, vol. 4, no. 6, 2014.
10. Open Source Initiative, "The Open Source Definition," [Online]. Available: https://opensource.org/osd