CONFIGURACIÓN DE UNA ARQUITECTURA PERIMETRAL UTILIZANDO ENDIAN FIREWALL EN ENTORNOS VIRTUALIZADOS

Geovanny Pino Castillo
e-mail: gpinoc@unadvirtual.edu.co
Yessica Patricia Polo Molina
e-mail: Yppolom@unadvirtual.edu.co
Oscar David Salamanca Echeverri
e-mail: odsalamancae@unadvirtual.edu.co
Andrea Arias Bermúdez
e-mail: aariasbe@unadvirtual.edu.co
Jaime Andrés García Quintero
e-mail: jagarciaqu@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo de cinco temáticas orientadas a la implementación de seguridad perimetral utilizando la distribución GNU/Linux Endian como firewall central. En la primera temática se realiza la instalación y configuración inicial del sistema con sus zonas Verde, Roja y Naranja. Posteriormente, se implementan reglas de NAT para permitir la comunicación controlada entre la LAN, la DMZ y la WAN. Las siguientes temáticas abordan el acceso a servicios desde la DMZ, la aplicación de reglas de tráfico entre zonas y la implementación de un proxy HTTP con políticas de autenticación y listas negras. Cada temática incluye procedimientos técnicos, validaciones y evidencias ejecutadas desde consola. Los resultados obtenidos demuestran la correcta operación del firewall y la efectividad de las políticas aplicadas para fortalecer la seguridad de la infraestructura.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad Perimetral.

1 INTRODUCCIÓN

La seguridad perimetral constituye un componente esencial en la protección de redes corporativas, especialmente en entornos donde coexisten servicios internos, zonas expuestas y accesos a Internet. La implementación de firewalls, segmentación de redes y políticas de control de tráfico permite fortalecer la integridad, disponibilidad y confidencialidad de los sistemas que soportan operaciones críticas. En este contexto, la distribución GNU/Linux Endian se presenta como una plataforma robusta para la gestión perimetral mediante funciones como filtrado de paquetes, traducción de direcciones, administración de zonas, control de servicios y políticas de navegación.

El presente artículo desarrolla cinco temáticas orientadas a la configuración y aseguramiento de una infraestructura perimetral simulada. Cada temática aborda procesos fundamentales, incluyendo la instalación y preparación de Endian, la configuración de NAT, el control de servicios desde la DMZ, la definición de reglas entre zonas y la implementación de un proxy HTTP con autenticación. El conjunto de tareas ejecutadas permite evidenciar las capacidades de Endian como solución integral para la gestión de seguridad en redes bajo entornos educativos y profesionales.

2 DESARROLLO

2.1 Temática 1: Configuración de la Instancia Endian En VirtualBox

La primera temática tiene como propósito preparar el entorno de virtualización y realizar la instalación efectiva del sistema operativo Endian Firewall, definiendo correctamente las zonas de red que permitirán la gestión perimetral del entorno. Para este proceso se utilizó Oracle VirtualBox como plataforma de virtualización, debido a su compatibilidad con GNU/Linux y a su flexibilidad para la asignación de interfaces de red.

El procedimiento inició con la creación de una nueva máquina virtual destinada para Endian, asignando recursos mínimos recomendados por el fabricante, incluyendo 2 GB de memoria RAM, 2 procesadores y un disco virtual de al menos 20 GB. Posteriormente, se configuraron las tres interfaces de red necesarias para establecer las zonas de seguridad requeridas:

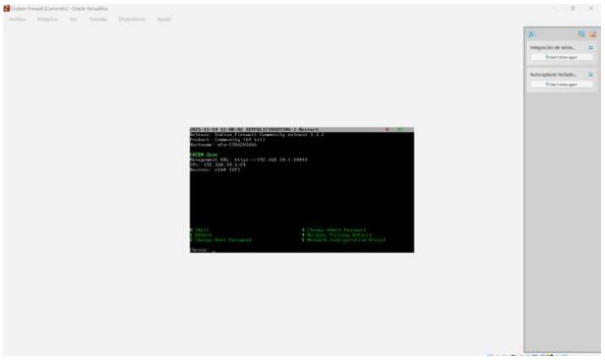
- **Tarjeta 1 – Zona Roja (WAN):** configurada como Adaptador puente o NAT, permitiendo la conexión a Internet.
- **Tarjeta 2 – Zona Verde (LAN):** configurada como Red interna, destinada al segmento seguro de la red.

- **Tarjeta 3 – Zona Naranja (DMZ):** configurada también como Red interna, aislada de la LAN, donde se ubicarán los servicios expuestos.

Una vez definida la estructura de red, se procedió a iniciar la instalación de Endian mediante su imagen ISO oficial. El instalador permitió seleccionar las opciones por defecto, configurar el idioma, asignar contraseñas administrativas y detectar automáticamente las interfaces de red. Finalmente, se verificó desde la consola la correcta asignación de cada interfaz mediante comandos de identificación y estado de red, confirmando el funcionamiento de las zonas Verde, Roja y Naranja según su direccionamiento correspondiente.

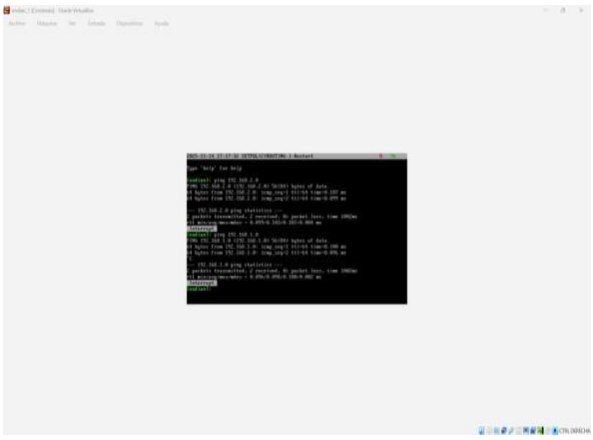
La configuración inicial dejó preparada la plataforma para las siguientes temáticas, en las cuales se implementarán reglas NAT, control de servicios, políticas de acceso y mecanismos de navegación segura.

Figura 1. Zona Verde (LAN)



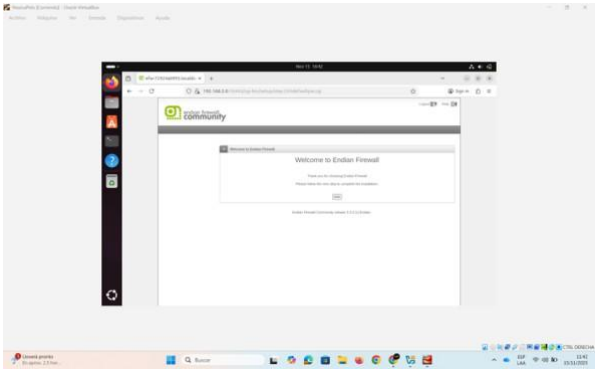
Fuente: Autoría propia (Yessica Polo)

Figura 2. Se demuestra el funcionamiento de la zona haciendo ping a la ip de zona naranjada y verde.



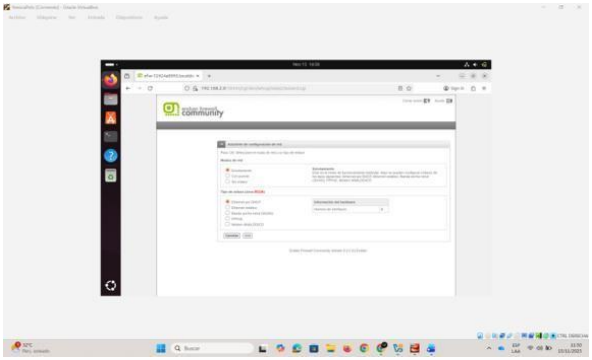
Fuente: Autoría propia (Yessica Polo)

Figura 3. Configurar Endian desde la maquina Desktop



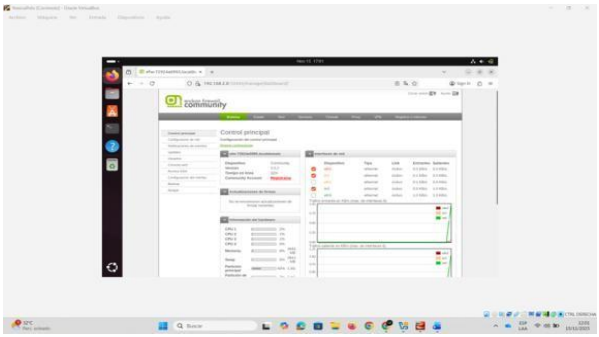
Fuente: Autoría propia (Yessica Polo)

Figura 4. Configuración de la zona roja



Fuente: Autoría propia (Yessica Polo)

Figura 5. Redes conectadas correctamente



Fuente: Autoría propia (Yessica Polo)

2.2 Temática 2: Configuración NAT

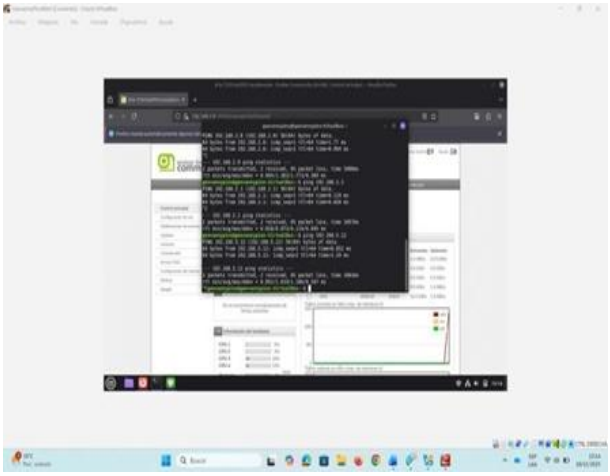
La segunda temática se centró en la configuración de reglas de Traducción de Direcciones de Red (NAT), un mecanismo fundamental para permitir la comunicación controlada entre los diferentes segmentos definidos en Endian. La función principal de NAT es permitir que los equipos de la red interna (LAN) y de la zona desmilitarizada (DMZ) accedan a servicios externos ubicados en Internet, utilizando una sola dirección pública asignada a la zona Roja (WAN).

El proceso inició desde la interfaz administrativa de Endian, donde se accedió al módulo de Firewall y posteriormente a la sección de NAT. La primera configuración consistió en habilitar la regla que permite la traducción de direcciones de la zona Verde hacia la zona Roja, garantizando que los equipos internos pudieran establecer comunicación con la red simulada de Internet. Esta regla se validó mediante pruebas de conectividad y acceso web desde un equipo perteneciente a la LAN.

Posteriormente, se definió la regla NAT correspondiente a la zona Naranja, con el propósito de habilitar la salida de los servicios alojados en la DMZ hacia la WAN. Esta regla asegura que los servidores de la DMZ puedan acceder a actualizaciones, repositorios y otros recursos externos sin exponer directamente sus direcciones privadas.

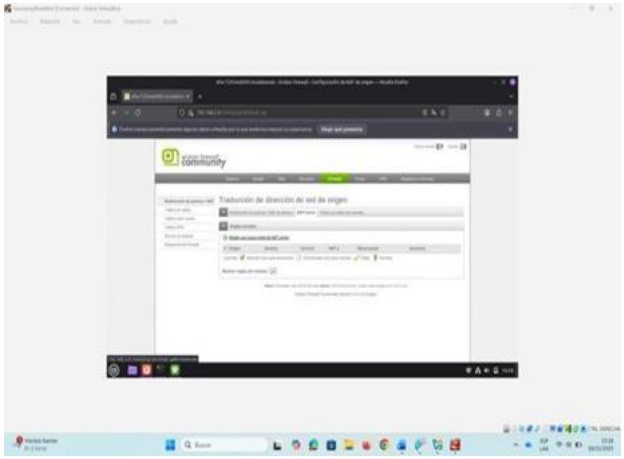
Una vez creadas ambas reglas, se verificó su registro en el apartado de Port Forwarding / NAT y se ejecutaron pruebas de conectividad desde la DMZ para comprobar el correcto funcionamiento de la traducción de direcciones. Las pruebas confirmaron que tanto la LAN como la DMZ podían establecer comunicación con la WAN, evidenciando un comportamiento adecuado en el firewall y sentando las bases para las temáticas siguientes orientadas al control de servicios y tráfico entre zonas.

Figura 6. Demostración de conexión exitosa entre las máquinas y las zonas.



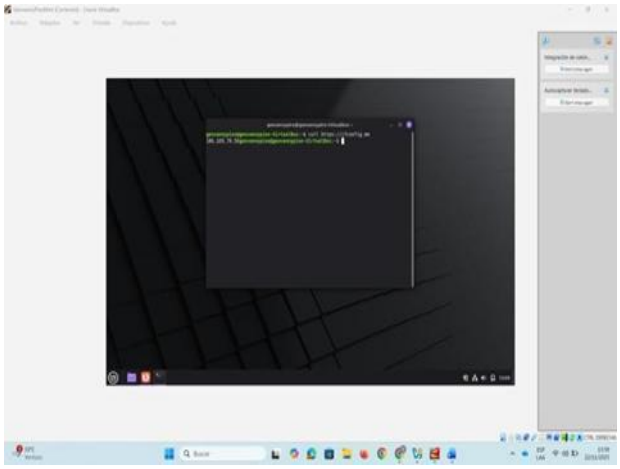
Fuente: Autoría propia (Geovanny Pino)

Figura 7. Ingresar a la interfaz web de Endian, buscar la opción firewall en el menú, posteriormente nos dirigimos a NAT fuente y agregamos una nueva regla y la configuramos para hacer envío de GREEN a RED



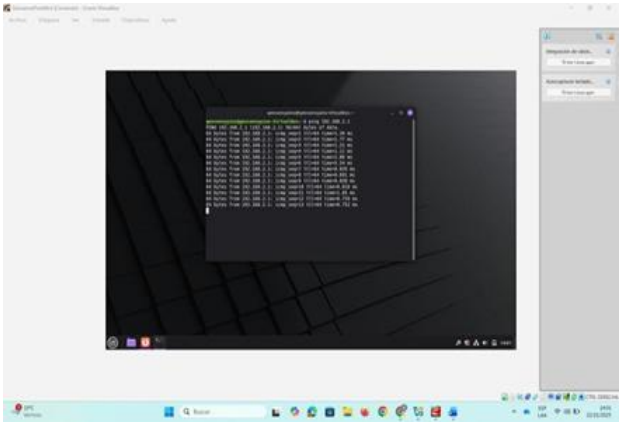
Fuente: Autoría propia (Geovanny Pino)

Figura 8. Evidenciamos NAT activo
Esto demuestra que Mint (LAN) está saliendo a Internet usando NAT a través de Endian.



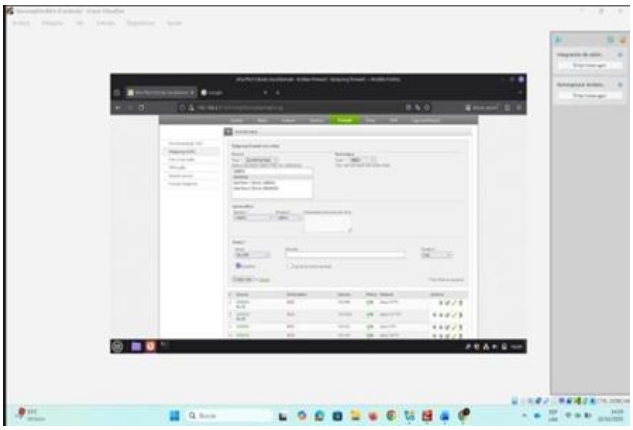
Fuente: Autoría propia (Geovanny Pino)

Figura 9. Hacemos la confirmación de la conectividad LAN con Endian -> gateway haciendo ping a 192.168.2.1. esto nos valida lo comunicación LAN con el firewall.



Fuente: Autoría propia (Geovanny Pino)

Figura 10. Se crea regla desde la interfaz web de Endian que salga de ORANGE y su destino sea RED, permitimos es Masquerade y creamos la regla.



Fuente: Autoría propia (Geovanny Pino)

2.3 Temática 3: Permisos Y Restricciones De Servicios En La DMZ

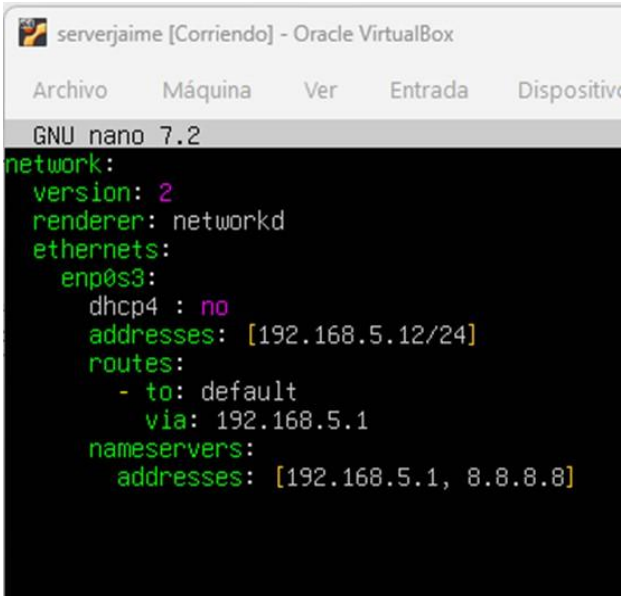
La tercera temática se enfocó en la habilitación y restricción de servicios dentro de la zona desmilitarizada (DMZ), donde se aloja el servidor web configurado bajo Ubuntu Server. Esta zona cumple un rol estratégico en la infraestructura perimetral, ya que permite exponer servicios hacia otras zonas sin comprometer directamente la red interna. En este caso, se requería permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde la DMZ, al tiempo que se restringía el uso del protocolo ICMP, con el propósito de evitar respuestas a solicitudes ping y reducir la superficie de posibles ataques.

El proceso inició accediendo al módulo de Firewall en Endian, específicamente a la sección de reglas de tráfico saliente. Allí se creó una primera regla destinada a permitir las conexiones provenientes de la zona Naranja hacia las zonas que requieren acceder a los servicios HTTP y FTP. Se configuraron explícitamente los puertos correspondientes y se verificó que el tráfico fuese aceptado para asegurar el funcionamiento del servidor web ubicado en la DMZ.

Posteriormente, se implementó una regla para denegar el protocolo ICMP, parámetro que se aplica tanto a solicitudes tipo echo request (puerto 8) como echo reply (puerto 30). Tras aplicar la regla, se efectuaron pruebas desde una terminal intentando realizar ping hacia direcciones IP de la red, confirmando la ausencia de respuesta y validando que el bloqueo estuviera correctamente aplicado.

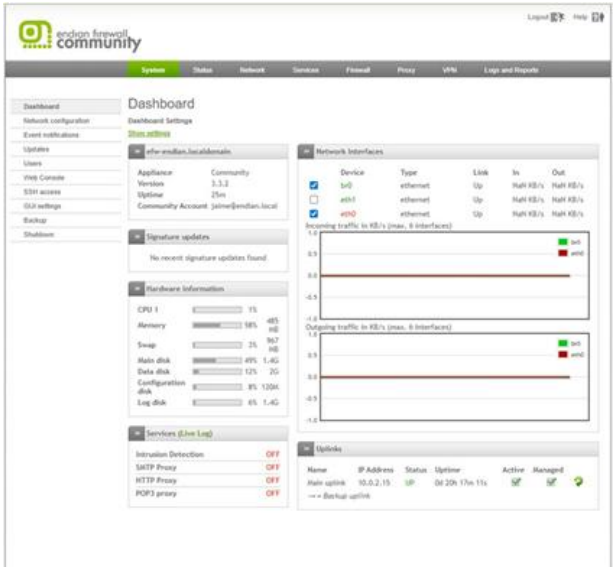
Finalmente, se verificaron las reglas creadas en el apartado de tráfico saliente de Endian, asegurando su funcionamiento adecuado. Esta temática permitió establecer un control granular sobre los servicios en la DMZ, garantizando la disponibilidad de los puertos necesarios mientras se restringen protocolos sensibles para mitigar riesgos de exploración y diagnósticos no autorizados.

Figura 11. Verificar la configuración en Netplan en server.



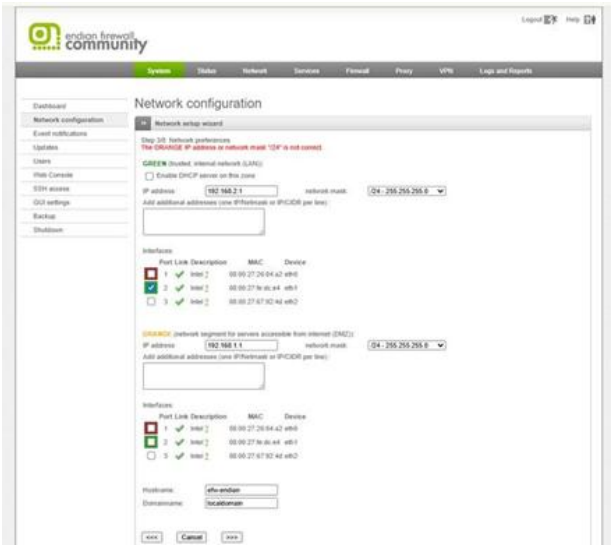
Fuente: Autoría propia (Jaime Andres Garcia)

Figura 12. Se realiza la configuración de Endian desde el entorno de configuración accediendo desde desktop Ubuntu.



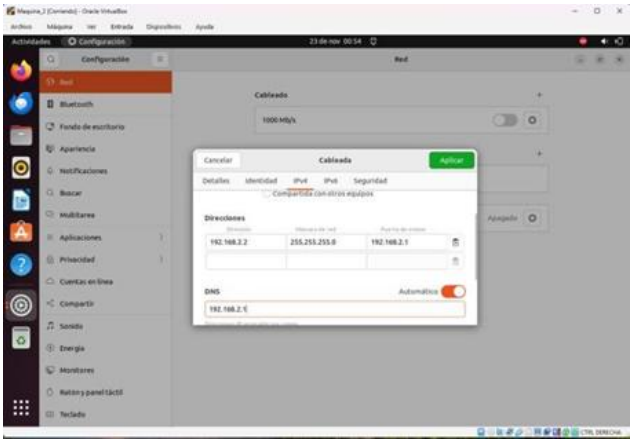
Fuente: Autoría propia (Jaime Andres Garcia)

Figura 13. En el entorno de Endian firewall procedo a realizar la network Configuration de cada una de las redes Green, Orange y Red.



Fuente: Autoría propia (Jaime Andres Garcia)

Figura 14. Es necesario realizar la configuración de red en desktop con los valores de Endian Zona Green.



Fuente: Autoría propia (Jaime Andres Garcia)

Figura 15. Hacer ping de desktop a server y se verifica su buen funcionamiento, en esta lamina se pueden ver las tres maquinas al tiempo lo que hizo muy lento el proceso, esto porque mi maquina host tiene recursos limitados.

Fuente: Autoría propia (Jaime Andres Garcia)

2.4 Temática 4: Reglas de Acceso entre Zonas

La cuarta temática se orientó a la creación y verificación de reglas de acceso entre las diferentes zonas configuradas en Endian: Verde (LAN), Naranja (DMZ) y Roja (WAN). Estas reglas permiten controlar de manera precisa qué servicios pueden transitar entre segmentos, estableciendo un marco de seguridad perimetral acorde con las necesidades del entorno. El objetivo principal consistió en permitir o denegar explícitamente el tráfico HTTP y FTP entre zonas, además de validar la comunicación en distintos sentidos mediante pruebas funcionales.

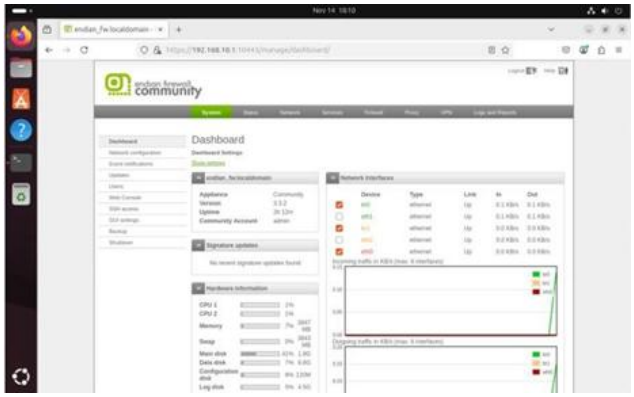
El proceso inició desde la sección Firewall → Inter-Zone de Endian, donde se configuraron las reglas que permiten la comunicación desde la zona Verde hacia la zona Naranja a través de los puertos correspondientes a HTTP (80) y FTP (21). Esta configuración garantiza que los equipos ubicados en la LAN puedan acceder a los servicios alojados en los

servidores de la DMZ. Asimismo, se habilitó el tráfico entrante desde Internet (Zona Roja) hacia la DMZ, lo cual es fundamental para exponer servicios web públicos sin comprometer la seguridad de la red interna.

Posteriormente, se verificaron las reglas en la tabla de tráfico Inter-Zona y se realizaron pruebas prácticas desde un navegador web y desde clientes FTP ubicados en las diferentes zonas. Entre las pruebas ejecutadas se incluyeron: acceso HTTP desde la LAN hacia la DMZ, acceso HTTP desde la LAN hacia la WAN, acceso HTTP desde la DMZ hacia la WAN y pruebas de ingreso FTP desde la LAN o la WAN hacia la DMZ. Cada una de estas pruebas permitió comprobar la correcta operación de las reglas creadas y el flujo controlado del tráfico entre zonas.

Los resultados confirmaron que Endian aplicó adecuadamente las restricciones establecidas, habilitando únicamente los servicios autorizados y garantizando que las comunicaciones se produzcan bajo parámetros seguros. Esta temática consolidó el esquema de protección perimetral al permitir un control granular y preciso sobre las interacciones entre segmentos críticos de la red.

Figura 16. Creación de nueva regla para la red de zona Orange DMZ.

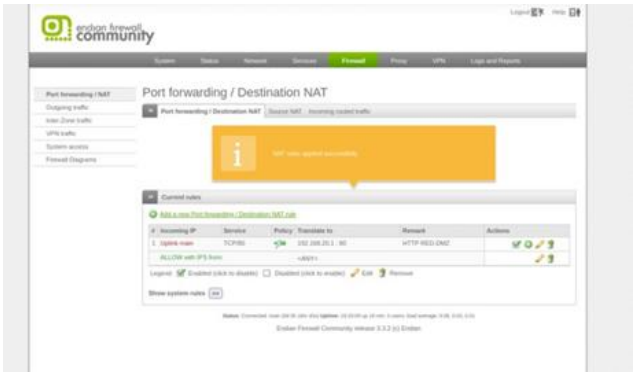


Fuente: Autoría propia (Oscar David Salamanca)

Figura 17. Creación de la regla para comunicación usando HTTP y FTP.

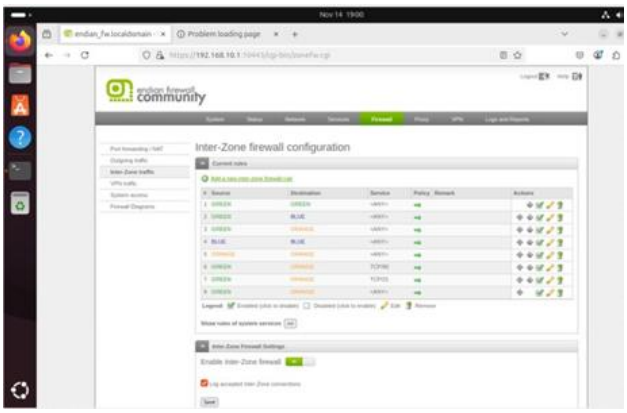
Fuente: Autoría propia (Oscar David Salamanca)

Figura 18. Regla numero 1 permitir HTTP a Servidor DMZ.



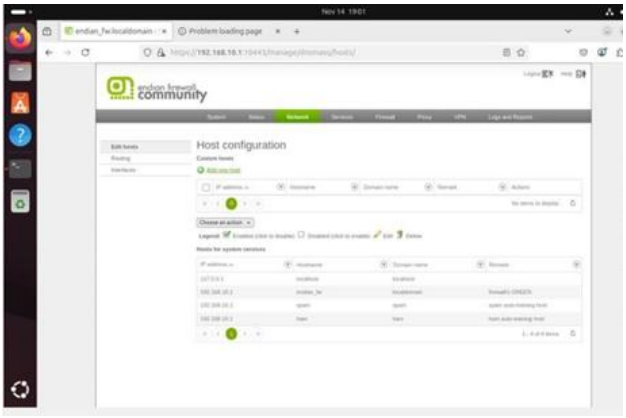
Fuente: Autoría propia (Oscar David Salamanca)

Figura 19. Verificación de conexión interna entre Servidor-DMZ-LAN.



Fuente: Autoría propia (Oscar David Salamanca)

Figura 20. Verificación de conexión FTP y Host.



Fuente: Autoría propia (Oscar David Salamanca)

2.5 Temática 5: Proxy HTTP no Transparente con Autenticación

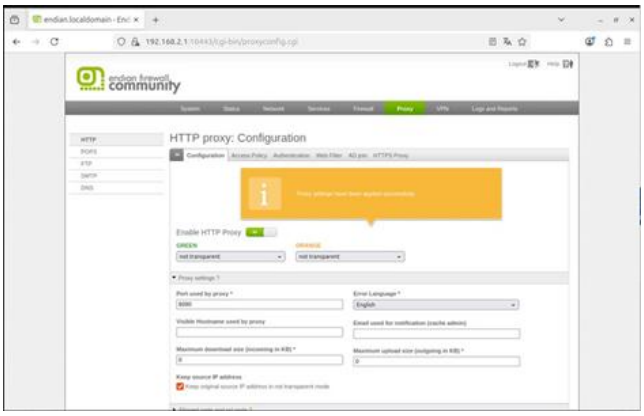
La quinta temática se enfocó en la implementación de un proxy HTTP no transparente en Endian, orientado al control del acceso web mediante autenticación de usuarios y políticas de restricción basadas en listas negras. Este componente resulta fundamental en la gestión de la seguridad perimetral, ya que permite supervisar, filtrar y registrar el tráfico de navegación proveniente de la red interna, además de establecer controles específicos sobre la disponibilidad de contenidos.

El proceso inició activando el servicio de proxy HTTP en modo no transparente, lo que obliga a que todos los equipos de la LAN configuren manualmente el uso del proxy para navegar. Posteriormente, se creó un perfil de filtrado en el cual se incluyó una lista negra de sitios web a bloquear, abarcando dominios como: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Esta política permite restringir sitios considerados no autorizados, innecesarios o potencialmente riesgosos para el entorno institucional.

Luego, se procedió a la creación de un usuario y su respectivo grupo en la sección de autenticación del proxy. Dicho usuario fue vinculado tanto al perfil de filtrado como a la política de acceso, asegurando que cada intento de navegación requiriera credenciales válidas. Esta capa adicional de control incrementa la trazabilidad y la seguridad, dado que cada acción queda asociada a un usuario identificado.

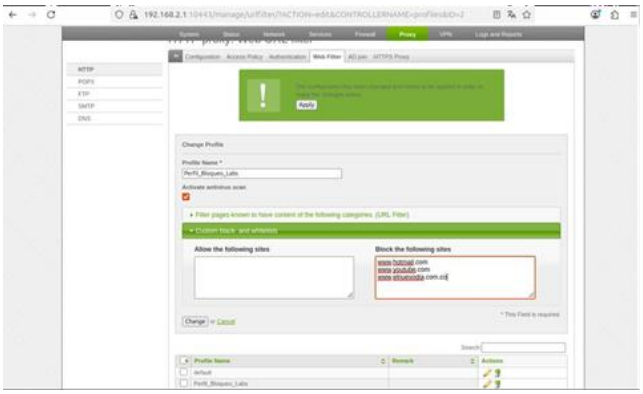
Finalmente, se realizaron pruebas desde un cliente en la LAN configurando el proxy en el navegador. Durante las pruebas, los sitios incluidos en la lista negra mostraron mensajes de denegación, mientras que las páginas no restringidas se cargaron correctamente tras autenticarse. Los resultados confirmaron el funcionamiento adecuado del proxy no transparente y la efectividad de las políticas de autenticación y bloqueo, fortaleciendo el control de navegación dentro del entorno protegido.

Figura 21. Habilitar y configurar el Proxy HTTP, donde confirmamos que en LAN este en Non-transparent y verificamos el proxy port, en este caso se dejó puerto 8080:



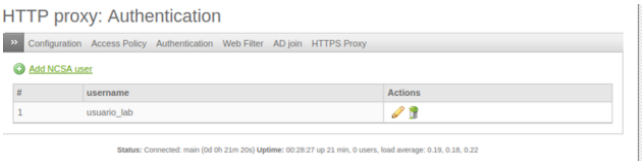
Fuente: Autoría propia (Andrea Arias)

Figura 22. Para crear el perfil de filtro y lista negra, en Web URL filter se crea un nuevo perfil, donde ponemos el nombre de Perfil_Bloqueo_Labs y en Block the following sites ingresamos las direcciones a restringir:



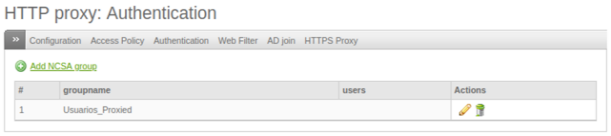
Fuente: Autoría propia (Andrea Arias)

Figura 23. Usuario usuario_lab:



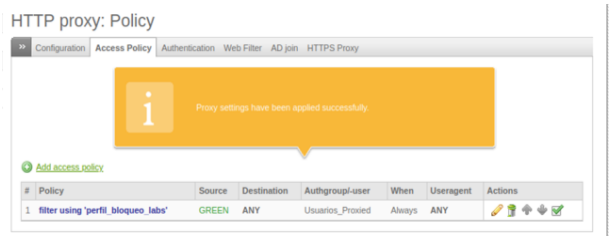
Fuente: Autoría propia (Andrea Arias)

- *Grupo Usuarios_Proxied:*



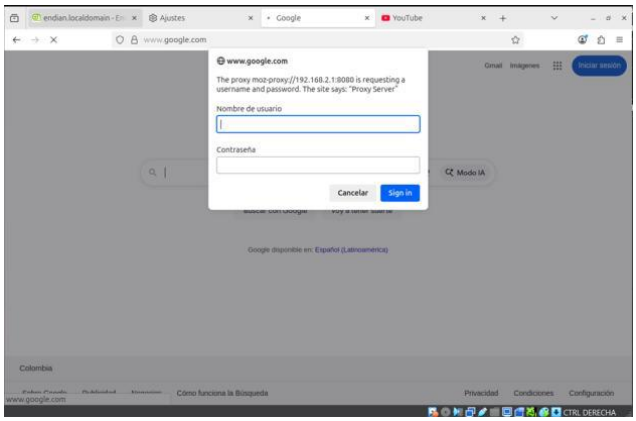
Fuente: Autoría propia (Andrea Arias)

Figura 24. Una vez creado el grupo y usuario, se agrega a la política de filtro y bloqueo creado:



Fuente: Autoría propia (Andrea Arias)

Figura 25. Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.



Fuente: Autoría propia (Andrea Arias)

Figura 26. Verificamos que la dirección www.youtube.com, Hotmail y www.elnuevodia.com.co se encuentra restringida:

Fuente: Autoría propia (Andrea Arias)

3 CONCLUSIONES

Conclusión 1 – Temática 1:

La instalación y configuración inicial de Endian Firewall en un entorno virtualizado permitió establecer una arquitectura perimetral funcional, en la cual la correcta asignación de las zonas Verde, Roja y Naranja resultó fundamental para garantizar el control segmentado del tráfico. Este proceso evidenció la importancia de una adecuada planificación de interfaces para asegurar la coherencia en el modelado de la red.

Conclusión 2 – Temática 2:

La implementación de las reglas NAT demostró la relevancia del direccionamiento público y privado en escenarios perimetrales. La traducción de direcciones habilitó el acceso controlado desde la LAN y la DMZ hacia redes externas, garantizando simultáneamente la protección de los equipos internos. Su correcta configuración aseguró un funcionamiento fluido y estable del tráfico saliente.

Conclusión 3 – Temática 3:

El control de servicios en la DMZ permitió reforzar la seguridad al habilitar únicamente los puertos esenciales para el funcionamiento del servidor web y FTP. La restricción del protocolo ICMP redujo la exposición del entorno ante actividades de reconocimiento no autorizado, confirmando la importancia de aplicar políticas de mínima exposición en zonas críticas.

Conclusión 4 – Temática 4:

La creación de reglas de acceso entre zonas evidenció la necesidad de controlar de manera precisa la comunicación entre LAN, DMZ y WAN. Las pruebas realizadas demostraron que el firewall permite un flujo selectivo del tráfico conforme a políticas previamente definidas, fortaleciendo la seguridad perimetral al evitar conexiones innecesarias o no autorizadas.

Conclusión 5 – Temática 5:

La configuración del proxy HTTP no transparente, junto con la implementación de autenticación y filtrado por listas negras, permitió establecer controles efectivos sobre la navegación interna. Este mecanismo no solo reforzó la seguridad del entorno, sino que además brindó trazabilidad y supervisión del tráfico web, elementos fundamentales en redes organizacionales modernas.

4 REFERENCIAS

[1] Endian. (2023). Endian Firewall Community Documentation. https://docs.endian.com/

[2] Internet Assigned Numbers Authority (IANA). (s.f.). Service Name and Transport Protocol Port Number Registry. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[3] LaCroix, J. (2021). Mastering Ubuntu Server (3.ª ed.). Packt Publishing.

[4] Linux Professional Institute (LPI). (s.f.). Linux Essentials 010–160: Learning Materials. https://learning.lpi.org/es/learning-materials/

[5] Open Web Application Security Project (OWASP). (2023). Secure Configuration Guidelines. https://owasp.org/www-project-cheat-sheets/cheatsheets/

[6] Oracle. (2023). VirtualBox User Manual. https://www.virtualbox.org/manual/UserManual.html

[7] Ubuntu Documentation. (s.f.). Ubuntu Server Guide. Canonical Ltd. https://ubuntu.com/server/docs