IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD SEGMENTADA CON ENDIAN FIREWALL PARA LA PROTECCIÓN DE REDES GNU/LINUX EMPRESARIALES

Daniel Esteban Cortés Blanco
e-mail: dcortesb@unadvirtual.edu.co
Claudia Patricia Valderrama Gonzalez
e-mail: cpvalderramag@unadvirtual.edu.co
Mildred Socorro Garcia Muñoz
e-mail: msgarciamu@unadvirtual.edu.co
Jhonatan Peláez Magnoler
e-mail: jpelaezm@unadvirtual.edu.co
Gabriel Londoño Ortiz
e-mail: glondonoo@unadvirtual.edu.co

RESUMEN: *Ante la creciente de las amenazas cibernéticas, se vuelve importante adoptar medidas de seguridad sólidas y segmentadas que protejan los activos críticos de una red. En este artículo se propone un enfoque práctico para implementar una arquitectura de seguridad basada en la distribución GNU/Linux con Endian Firewall. Mediante la segmentación en zonas (LAN, WAN y DMZ), la configuración de reglas, el control de acceso a servicios, la restricción de protocolos y la incorporación de un proxy con filtrado de contenido, se demuestra como Endian puede reforzar de forma significativa la protección de las redes empresariales. Además, se documenta las configuraciones aplicadas, las pruebas realizadas y los resultados que se obtuvieron, evidenciando la eficacia de Endian como recurso de seguridad adaptable y centrada.*

PALABRAS CLAVE: Endian Firewall, Segmentación de red, GNU/Linux, control de acceso.

ABSTRACT: *In light of the growing threat of cyberattacks, it is increasingly important to adopt solid and segmented security measures to protect a network's critical assets. This article proposes a practical approach to implementing a security architecture based on the GNU/Linux distribution with Endian Firewall. Through network segmentation into zones (LAN, WAN, and DMZ), rule configuration, service access control, protocol restriction, and the integration of a proxy with content filtering, it is demonstrated how Endian can significantly strengthen the protection of enterprise networks. Additionally, the applied configurations, the tests carried out, and the resulting outcomes are documented, highlighting the effectiveness of Endian as an adaptable and focused security resource.*

KEYWORDS: Access control, Endian Firewall, GNU/Linux, Network segmentation.

1 INTRODUCCIÓN

En la actualidad, la seguridad se ha convertido en parte esencial para las organizaciones que buscan proteger sus infraestructuras de red y datos de amenazas externas e internas. La necesidad de segmentar las redes en zonas de seguridad y asignar políticas para inspección y controlar el acceso a internet cada vez son requisitos fundamentales para garantizar la confidencialidad, la integridad y la disponibilidad de los recursos.

Endian Firewall (EFW) aparece como una distribución de seguridad de código abierto que cuenta con una arquitectura de zonas de seguridad donde Verde es para LAN, roja es para WAN y naranja para DMZ, facilita la implementación de políticas de seguridad para cada segmento de la red. El objetivo principal de este artículo es demostrar la eficacia de Endian Firewall como defensa para redes basadas en GNU/Linux. A través de la implementación y verificación en cada temática, proporcionando una guía detallada para la adaptación de Endian Firewall como una solución de seguridad. Este artículo se estructura de la siguiente manera: primero se describe la configuración inicial de la infraestructura con sus respectivas zonas, después se detalla la implementación de las reglas y posteriormente, se aborda la configuración del acceso a servicios y denegación de protocolos, se exploran las reglas de acceso y finalmente se presenta la implementación de un proxy con políticas de autenticación y filtrado de contenido. Cada temática demuestra la efectividad de las configuraciones implementadas con Endian Firewall.

2 MARCO TEÓRICO

En este marco teórico se exploran los conceptos fundamentales involucrados en la implementación de una arquitectura de seguridad utilizando GNU/Linux Endian Firewall (EFW).

2.1 SEGURIDAD PERIMETRAL

Se refiere a estrategias y tecnología utilizadas para controlar el acceso entre una red interna y externa. El objetivo es prevenir accesos no autorizados, ataques maliciosos y fugas de información. Un firewall es un componente importante de la

seguridad perimetral, actuando como una barrera que revisa el tráfico de red y aplica políticas de control de accesos.

2.2 GNU/LINUX ENDIAN FIREWALL (EFW)

Es una distribución de seguridad GNU/Linux de código abierto diseñada para la implementación y gestión de la seguridad perimetral. Su arquitectura está basada en la segmentación de la red por zonas y aplicación de políticas de seguridad. Esta incluye control de tráfico, traducción de direcciones, análisis del tráfico de red, filtrado de contenido y generación de registro de eventos para monitoreo y análisis.

2.3 NETWORK ADDRESS TRANSLATION (NAT)

Permite traducir las direcciones IP privadas dentro de una red local a una dirección IP pública para la comunicación con redes externas. El reenvío de puertos es una funcionalidad de NAT, permite dirigir el tráfico entrante a puertos específicos de la dirección IP pública hacia servidores específicos dentro de la red privada.

2.4 CONTROL DE ACCESO Y REGLAS

El control de acceso se implementa mediante reglas creadas en el firewall que determinan que tráfico de red está permitido o denegado entre las zonas de seguridad.

Cada una de estas reglas especifica la zona de origen, la zona de destino, la dirección IP, el protocolo y los puertos. El firewall evalúa estas reglas, y aplica la opción definida. Además, el orden de las reglas es de mucha importancia ya que el firewall procesa las reglas de arriba abajo, aplicando la primera regla que coincida con el tráfico.

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

Para una correcta implementación de los procesos, se debe empezar por establecer buenas bases que garanticen que todos los involucrados trabajen en la misma sintonía y de esta forma estandarizar los procesos.

Para este objetivo, en esta temática se establecerán las configuraciones de red, como las direcciones, puertas de enlace, adaptadores de red, máscara de red y demás configuraciones necesarias para el correcto funcionamiento del sistema que se espera montar.

3.1 CREACIÓN DE MÁQUINAS VIRTUALES.

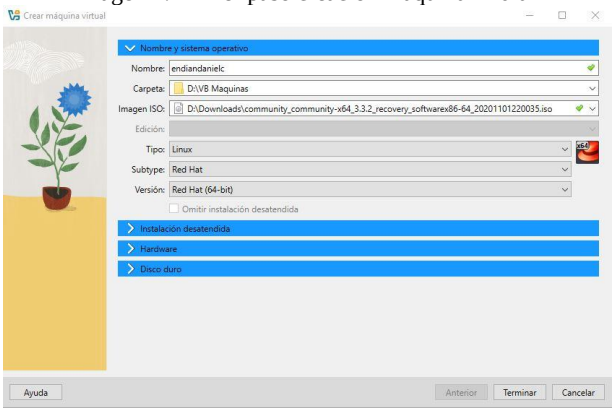
Para iniciar con la configuración de la red, se crearon 3 máquinas virtuales con Virtualbox, esto nos facilita la interacción entre máquinas, el monitoreo de estas, y una correcta configuración de la red que garantice la conexión entre ellas.

3.1.1 CREACIÓN DE MÁQUINA FIREWALL

Para el firewall usaremos Endian en su versión 3.3.2, a través de una ISO proveída por la comunidad.

Se define el nombre, se carga la ISO, y se definen los recursos.

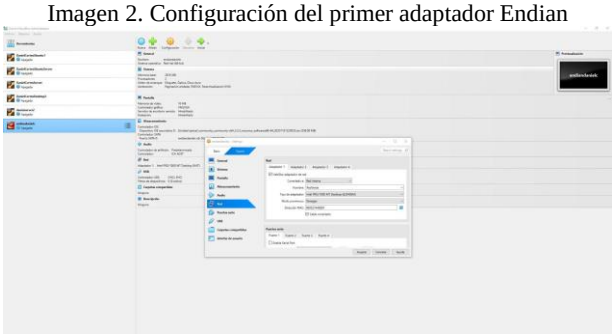
Imagen 1. Primer paso creación máquina Endian



Fuente: Autoría propia

Se configura el adaptador de red como una red interna (RedVerde).

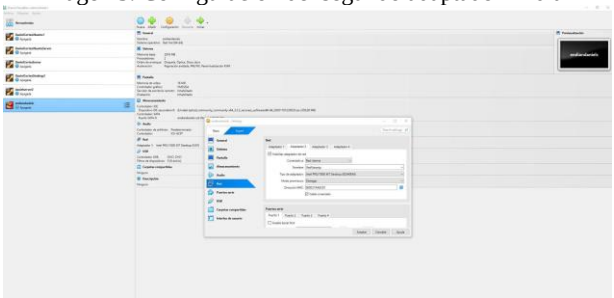
Imagen 2. Configuración del primer adaptador Endian



Fuente: Autoría propia

Se configura el adaptador de red como una red interna (RedNaranja).

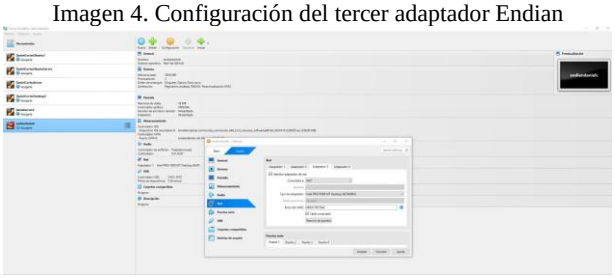
Imagen 3. Configuración del segundo adaptador Endian



Fuente: Autoría propia

Se configura el adaptador de red como una red NAT.

Imagen 4. Configuración del tercer adaptador Endian



Fuente: Autoría Propia

Una vez se termina de configurar los adaptadores de red, se inicia la máquina y se hacen las configuraciones iniciales, donde se define la dirección de la red verde.

Imagen 5. Configuración de la red verde en Endian

Fuente: Autoría propia

3.1.2 CREACIÓN DE MÁQUINA DESKTOP.

Para el equipo desktop, se usará un sistema Ubuntu Desktop en su versión 24.04.2 a través de una ISO descargada del sitio oficial.

define el nombre, se carga la ISO, y se definen los recursos.

Imagen 6. Primer paso creación máquina desktop

Fuente: Autoría propia

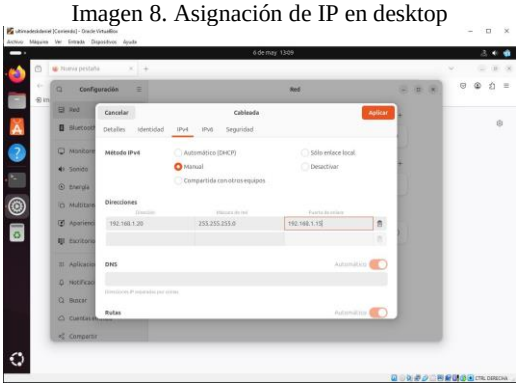
Se configura el adaptador de red, seleccionando la RedVerde previamente creada para Endian.

Imagen 7. Asignación de la RedVerde en Desktop

Fuente: Autoría propia

Una vez iniciada la máquina desktop, en configuración de red se le asigna la IP.

Imagen 8. Asignación de IP en desktop



Fuente: Autoría propia

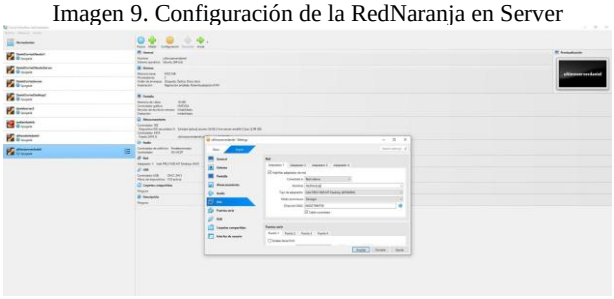
3.1.3 CREACIÓN DE MÁQUINA SERVER.

Para el equipo server, se usará un sistema Ubuntu Server en su versión 24.04.02 a través de una ISO descargada del sitio oficial.

Se define el nombre, se carga la ISO, y se definen los recursos.

Se configura el adaptador de red, configurando la RedNaranja (DMZ).

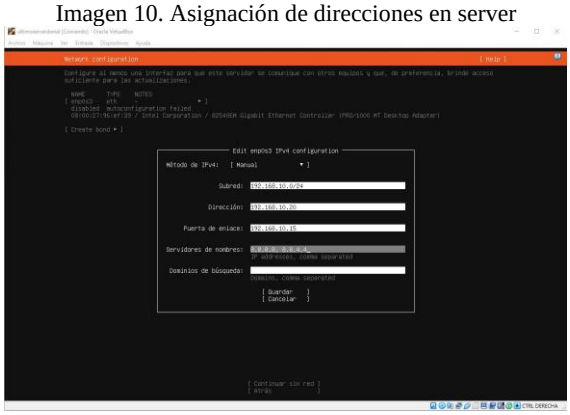
Imagen 9. Configuración de la RedNaranja en Server



Fuente: Autoría propia

Una vez iniciada la máquina server, en la configuración inicial, se definen las direcciones de red.

Imagen 10. Asignación de direcciones en server



Fuente: Autoría propia

3.2 CONFIGURACIÓN DEL FIREWALL.

Una vez tenemos creadas y configuradas las 3 máquinas, debemos configurar la red en el Firewall a través de la interfaz gráfica a la cual se accedió por medio del desktop.

Desde nuestra máquina Desktop, la cual está en la RedVerde, ingresamos al administrador de Endian por medio de la ip asignada.

Imagen 11. Página inicial del administrador de Endian

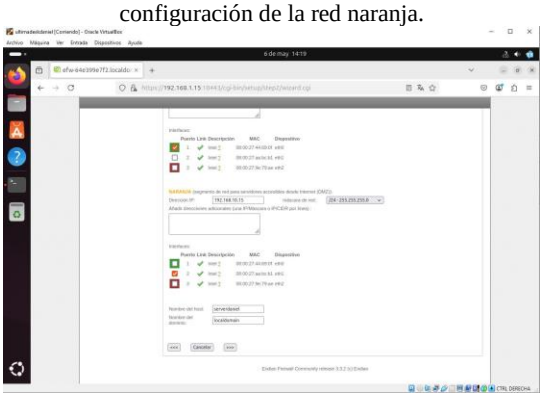
Fuente: Autoría propia

Se inicia la configuración de red e inicialmente se configura la red Naranja (DMZ).

Imagen 12. Se selecciona la red naranja como la red a configurar.

Fuente: Autoría propia

Imagen 13. Se verifican adaptadores de red y se finaliza la configuración de la red naranja.



Fuente: Autoría propia

Se visualiza las 3 redes ya configuradas en el firewall.

Imagen 14. Visual de las 3 redes configuradas

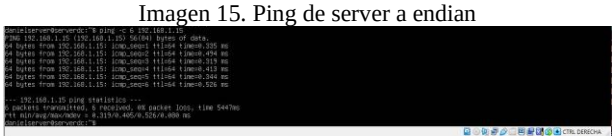
Fuente: Autoría propia

3.3 RESULTADOS Y PRUEBAS

Finalmente, después de haber configurado nuestras máquinas y configurado la red en Endian, procedemos a verificar con algunas pruebas que la red quedó bien configurada.

Se realiza un ping desde el server al firewall para verificar la conexión correcta y la funcionalidad de esta red.

Imagen 15. Ping de server a endian



Fuente: Autoría propia

Se realiza un ping desde el desktop al Endian para verificar la conexión correcta y la funcionalidad de esta red.

Imagen 16. Ping de desktop a endian

Fuente: Autoría propia

Se realiza un ping desde el desktop al server para verificar la comunicación entre estas dos zonas.

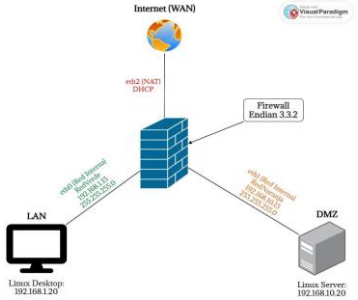
Imagen 17. Ping de desktop a server

Fuente: Autoría propia

3.3.1 DIAGRAMA DE RED.

Como producto final y luego de haber comprobado que la red funciona de manera correcta, se construye el diagrama de red, el cual se le proveerá a los demás miembros del grupo para que en base a esta red realicen los demás procedimientos solicitados.

Imagen 18. Diagrama de Red



Fuente: Autoría propia

4 TEMÁTICA 2: CONFIGURACIÓN NAT

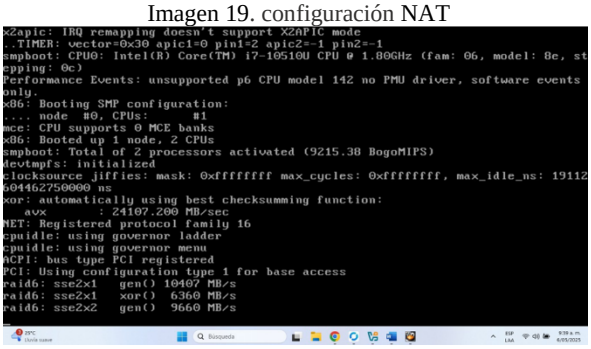
La correcta configuración de NAT (Network Address Translation) en Endian Firewall es fundamental para permitir que los dispositivos de la red interna (LAN y DMZ) puedan comunicarse de manera controlada con la red externa (Internet). En el entorno simulado, se establecieron reglas de Source NAT (SNAT) para asegurar que el tráfico saliente desde la red interna sea traducido y enrutado adecuadamente hacia la WAN.

El primer paso fundamental para la implementación de la seguridad perimetral en nuestro entorno simulado es iniciar la máquina virtual de Endian Firewall. Este firewall de código abierto es el componente central encargado de gestionar la comunicación y la seguridad entre las distintas zonas de la red: LAN (Green), DMZ (Orange) y WAN (Red).

Al arrancar la máquina virtual de Endian, se habilita la interfaz de administración que nos permitirá realizar todas las configuraciones necesarias, incluyendo la asignación de direcciones IP estáticas a cada interfaz de red y la creación de reglas de NAT. Esta puesta en marcha es esencial para garantizar que el firewall esté operativo y listo para recibir las configuraciones que permitirán el enmascaramiento del tráfico interno y su salida controlada hacia la red externa (Internet).

Con la máquina virtual de Endian en funcionamiento, se procede a acceder a su consola o interfaz web para continuar con la configuración de las reglas de Source NAT, asegurando así que tanto la red LAN como la DMZ puedan comunicarse de forma segura y eficiente con la WAN, cumpliendo los objetivos de segmentación y control de tráfico definidos en el proyecto.

Imagen 19. configuración NAT



Fuente: Autoría propia

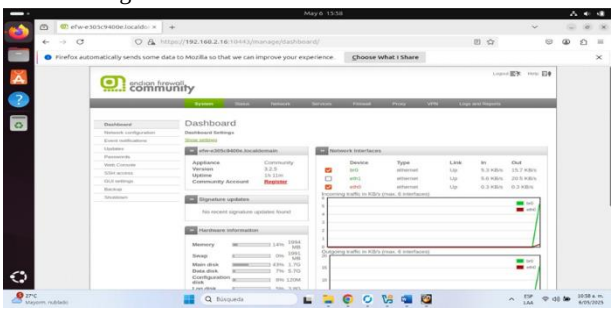
4.1 ACCESO AL PORTAL DE ADMINISTRACIÓN DE ENDIAN FIREWALL

Después de iniciar la máquina virtual de Endian Firewall, el siguiente paso clave consiste en acceder a su portal de administración. Este acceso se realiza a través de un navegador web, ingresando la dirección IP asignada a la interfaz de gestión del firewall (por ejemplo, https://192.168.1.1). Al hacerlo, se presenta la pantalla de inicio de sesión donde se deben introducir las credenciales de administrador previamente configuradas.

El ingreso exitoso al portal de Endian permite disponer de todas las herramientas necesarias para la administración y configuración de la seguridad perimetral de la red. Desde esta interfaz gráfica intuitiva, es posible gestionar las distintas zonas de la red (LAN, DMZ y WAN), así como crear y modificar reglas de NAT, asignar direcciones IP estáticas y monitorear el tráfico de red en tiempo real.

Este acceso es fundamental para continuar con la configuración de las reglas de Source NAT, que permitirán el enmascaramiento del tráfico interno y su salida controlada hacia la red externa. Además, la interfaz web de Endian facilita la visualización y validación de los cambios realizados, asegurando así que la red funcione de manera segura y eficiente.

Imagen 20. Acceso al Portal de Administración



Fuente: Autoría propia

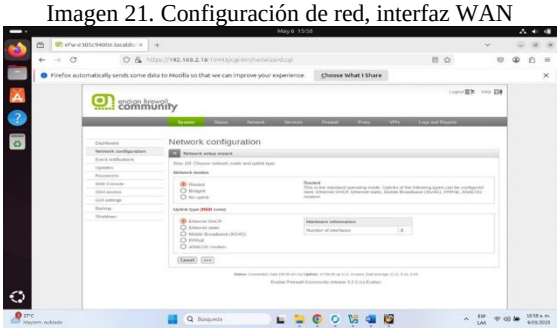
4.2 VERIFICACIÓN DE LA CONFIGURACIÓN DE RED PARA LA INTERFAZ WAN

Como parte fundamental de la configuración inicial en Endian Firewall, es necesario asegurarse de que la interfaz correspondiente a la zona RED (WAN) esté correctamente configurada para obtener su dirección IP mediante DHCP. Este ajuste permite que el firewall reciba automáticamente una dirección IP válida desde el proveedor de servicios de Internet o desde el router principal de la red externa, facilitando así la conectividad hacia Internet.

Para corroborar esta configuración, accedemos al portal de administración de Endian y navegamos hasta la sección de interfaces de red. Allí, verificamos que la interfaz asignada a la zona RED (WAN) tenga seleccionada la opción de obtención automática de dirección IP (DHCP). Esta comprobación es esencial antes de proceder con la creación de reglas de NAT, ya que garantiza que la interfaz WAN disponga de una dirección IP funcional y actualizada, necesaria para el enmascaramiento y la salida del tráfico desde la LAN y la DMZ hacia la red externa.

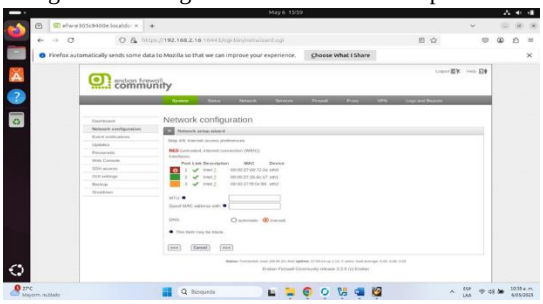
De esta manera, aseguramos que la infraestructura de red esté correctamente preparada para la siguiente etapa de configuración de seguridad perimetral y traducción de direcciones, cumpliendo con los requisitos de conectividad y gestión dinámica de la red externa.

Imagen 21. Configuración de red, interfaz WAN



Fuente: Autoría propia

Imagen 22. Configuración de Red WAN el puerto eth0



Fuente: Autoría propia

4.3 CONFIGURACIÓN DE SOURCE NAT PARA LA DMZ EN ENDIAN FIREWALL

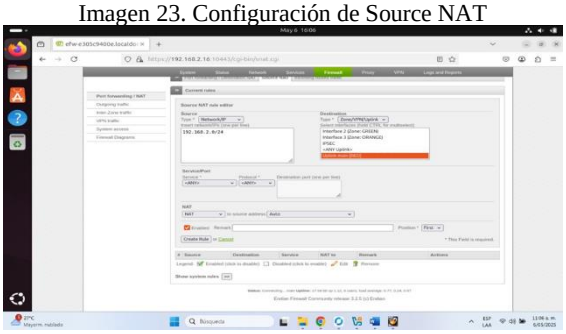
En la implementación de la seguridad perimetral de la red, uno de los pasos fundamentales fue la creación de una regla de Source NAT (SNAT) para la red ORANGE, correspondiente a la DMZ (zona desmilitarizada). Esta red utiliza el rango de direcciones 192.168.1.0/24 y, mediante la configuración en Endian Firewall, se logró que todo el tráfico originado en la DMZ se enmascare y salga a través de la interfaz RED (WAN), que representa la conexión a Internet.

Esta regla de NAT permite que los servidores y dispositivos ubicados en la DMZ puedan acceder a recursos externos en Internet, sin exponer directamente sus direcciones IP internas. Al aplicar SNAT, Endian Firewall traduce las direcciones privadas de la DMZ a la dirección pública asignada a la interfaz WAN, facilitando la comunicación hacia el exterior y asegurando que las respuestas de Internet lleguen correctamente a los equipos de la DMZ.

La configuración se realizó accediendo al portal de administración de Endian, donde se seleccionó la opción para crear una nueva regla de Source NAT. Se especificó la red de origen (192.168.1.0/24) y la interfaz de salida (RED/WAN), de modo que el tráfico saliente de la DMZ fuera correctamente enmascarado. Una vez aplicada la regla, se verificó su funcionamiento realizando pruebas de conectividad, como el uso del comando ping desde un servidor en la DMZ hacia una dirección pública (por ejemplo, 8.8.8.8). Los resultados exitosos confirmaron que la DMZ tenía acceso a Internet gracias a la regla de NAT aplicada.

De esta forma, la implementación de Source NAT en Endian Firewall para la red ORANGE (DMZ) habilitó el acceso seguro y controlado de la DMZ a la red externa, cumpliendo con los objetivos de segmentación y protección definidos para el entorno simulado.

Imagen 23. Configuración de Source NAT



Fuente: Autoría propia

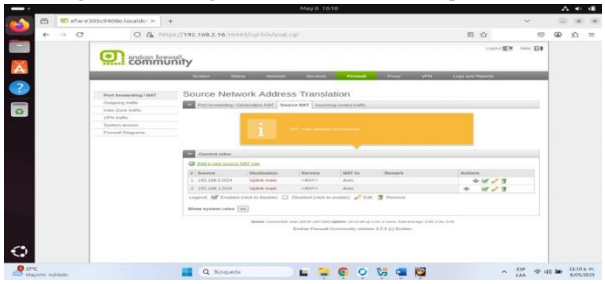
4.4 CONFIGURACIÓN DE SOURCE NAT PARA LA DMZ EN ENDIAN FIREWALL

En el proceso de asegurar la conectividad controlada entre las diferentes zonas de la red, se configuró una regla de Source NAT (SNAT) específicamente para la red ORANGE, que corresponde a la DMZ (zona desmilitarizada). Esta red utiliza el rango de direcciones 192.168.1.0/24 y, mediante la regla de NAT implementada en Endian Firewall, todo el tráfico originado en la DMZ se enmascara y se dirige hacia la interfaz RED (WAN), la cual representa la conexión a Internet.

Esta configuración tiene como objetivo principal permitir que los servidores y dispositivos ubicados en la DMZ puedan acceder a recursos externos en Internet, sin exponer directamente sus direcciones IP internas. Al aplicar SNAT, el firewall traduce las direcciones privadas de la DMZ a la dirección pública asignada a la interfaz WAN, garantizando así que las respuestas de Internet lleguen correctamente a los equipos de la DMZ y manteniendo la seguridad perimetral.

La verificación de esta configuración se realizó mediante pruebas de conectividad, como el uso del comando ping desde un servidor en la DMZ hacia una dirección pública (por ejemplo, 8.8.8.8). Los resultados exitosos confirmaron que la red DMZ tiene acceso a Internet gracias a la regla de NAT aplicada.

Imagen 24. Configuración de source NAT para la DMZ



Fuente: Autoría propia

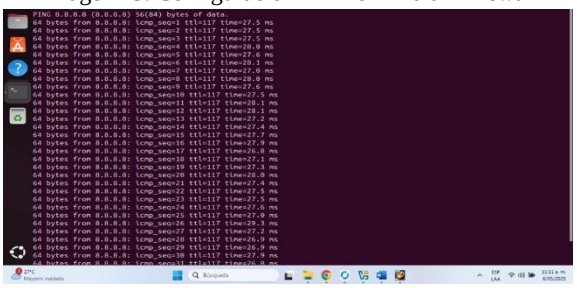
4.5 VERIFICACIÓN DE LA CONFIGURACIÓN NAT EN ENDIAN FIREWALL

Una vez completada la configuración de las reglas de Source NAT para la red ORANGE (DMZ) y la red GREEN (LAN) en Endian Firewall, se procedió a validar que ambas reglas estuvieran activas y correctamente almacenadas en el sistema. Al acceder a la interfaz de administración del firewall, se pudo observar que las reglas creadas para el enmascaramiento del tráfico de las redes internas hacia la interfaz RED (WAN) aparecen listadas y marcadas como activas.

Esta visualización confirma que el proceso de creación de las reglas NAT fue exitoso y que los cambios realizados se guardaron de forma adecuada. Gracias a esto, tanto la red LAN como la DMZ pueden acceder a recursos externos en Internet, cumpliendo con los objetivos de segmentación y control de tráfico definidos para el entorno simulado.

La correcta visualización y almacenamiento de estas reglas en Endian Firewall es fundamental, ya que garantiza la persistencia de la configuración incluso ante reinicios del sistema, asegurando así la continuidad y seguridad de la conectividad entre las distintas zonas de la red.4

Imagen 25. Configuración NAT en Endian Firewall



Fuente: Autoría propia

4.6 VERIFICACIÓN DE CONECTIVIDAD DESDE EL SERVIDOR

Como parte de la validación de la configuración de red y de las reglas de NAT implementadas en Endian Firewall, se realizó una prueba de conectividad desde el servidor interno. Para ello, se ejecutó el comando ping dirigido a la dirección pública 8.8.8.8 (servidor DNS de Google). El resultado exitoso de esta prueba confirma que el servidor, al igual que las demás máquinas de la red interna, cuenta con acceso a Internet.

Este resultado demuestra que tanto la configuración de red en el servidor como las reglas de Source NAT en Endian Firewall están funcionando correctamente. El tráfico generado por el servidor es enmascarado por el firewall y redirigido adecuadamente hacia la red externa, permitiendo la comunicación con servicios y recursos fuera de la red local.

La capacidad de realizar ping a una dirección pública desde el servidor es una evidencia fundamental de que la segmentación, el enrutamiento y la traducción de direcciones están correctamente implementados, asegurando que tanto la LAN como la DMZ puedan interactuar con el exterior de manera segura y controlada.

Imagen 26. Verificación de conectividad

Fuente: Autoría propia

5 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

La necesidad de ofrecer servicios de transferencia de datos o de archivos a usuarios dentro de una red o mediante internet, tiene desafíos significativos en cuanto a seguridad. La exposición directa de servidores a redes no confiables, aumentan las posibilidades de ataques que comprometen la seguridad.

La zona DMZ aparece como una arquitectura de seguridad esencial, donde proporciona un aislamiento entre la red interna que se encuentra protegida y la red externa que es menos confiable.

La implementación de una zona DMZ es una práctica para disminuir los riesgos de seguridad al crear un segmento de red aislado que actúa como un punto de contacto seguro entre redes no confiables y los recursos internos. Un elemento importante en la implementación de una DMZ es un firewall, robusto y capaz de aplicar políticas de control de acceso.

En esta temática se explora la configuración de Endian Firewall para asegurar un servidor web Ubuntu ubicado en una DMZ (zona naranja), permitiendo el acceso controlado a los servicios HTTP Y FTP desde la red interna (LAN – zona verde) y además, se restringe la accesibilidad mediante el protocolo ICMP. La denegación de ICMP es importante como medida de seguridad para prevenir ciertos tipos de ataques que dependen de la capacidad de hacer ping a los hosts.

5.1 ANÁLISIS DEL CONTROL DE ACCESO A SERVICIOS ESPECÍFICOS

La configuración de reglas de firewall para permitir el acceso a servicios específicos como HTTP y FTP desde la LAN al servidor DMZ requieren una comprensión de los protocolos y su seguridad.

Permite el tráfico al puerto 80, es fundamental para la funcionalidad del servidor y es importante considerar las posibles vulnerabilidades a nivel de aplicación. Además, si el servidor maneja información sensible, la implementación de certificados SSL/TLS robustos son recomendables.

El protocolo FTP presenta riesgos de seguridad importantes por la transmisión de credenciales y datos en texto plano. Para disminuir estos riesgos, se recomienda la implementación de alternativas seguras como SFTP o FTPS.

La definición de las reglas de firewall Endian, es esencial. Esto reduce cualquier ataque en caso de que otros sistemas se añadan a la misma zona en el futuro.

5.2 METODOLOGÍA

La implementación de esta temática se realizó en un laboratorio virtualizado, utilizando VirtualBox para emular la red con las siguientes zonas definidas:

Zona Verde (LAN): Estación de trabajo Linux Desktop (192.168.1.20/24)

Zona Naranja (DMZ): Servidor web Ubuntu (192.168.10.20), con puerta de enlace 192.168.10.15

Zona Roja (WAN): Conectada a la interfaz de red con acceso a internet.

Los pasos que realice para la implementación fueron los siguientes:

Se configuraron las interfaces de red virtualizadas para la zona verde, roja y naranja con los rangos de IP definidos anteriormente.

Se asignó la dirección estática, con la puerta de enlace y se instalaron los servicios de HTTP (Apache2) y FTP (vsftpd) y se confirmó que el estado fuera activo de ambos servicios.

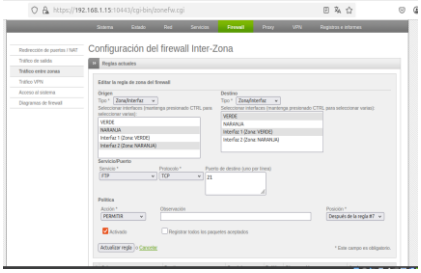
Permitir HTTP: Se creó una regla en “Tráfico entre Zonas” para permitir el tráfico TCP con destino al puerto 80 desde la zona verde hacia la zona naranja.

Imagen 27. Regla permitir HTTP (80)

Fuente: Autoría Propia

Permitir FTP: Se creó una regla similar para permitir el tráfico TCP con destino al puerto 21 desde la zona verde hacia la zona naranja.

Imagen 28. Regla permitir FTP



Fuente: Autoría Propia

Denegar ICMP: Se creó una regla para denegar el protocolo ICMP.

Imagen 29. Regla denegación ICMP

Fuente: Autoría Propia

Imagen 30. Reglas creadas en Endian

Fuente: Autoría Propia

Desde una máquina virtual (Linux Desktop) en la zona verde, se intentó acceder al servidor web a través de un navegador web HTTP y se realizó también la prueba mediante la consola del cliente (Linux Desktop) a FTP.

Desde la máquina virtual (Linux Desktop) en la zona verde, se intentó hacer ping a la dirección IP del servidor web en la zona naranja.

Se revisaron los registros del firewall de Endian para verificar la aplicación de las reglas de permitir y denegar el tráfico.

5.3 RESULTADOS Y PRUEBAS

Las pruebas de acceso a los servicios HTTP y FTP desde la máquina virtual (Linux Desktop) en la zona verde hacia el servidor Ubuntu en la zona naranja fueron exitosos.

Al ingresar al navegador, intento acceder a la dirección IP (http://192.168.10.20), se muestra la página predeterminada del servidor web (Apache) como se visualiza en la siguiente imagen:

Imagen 31. Resultado regla HTTP

Fuente: Autoría Propia

Los resultados de la regla de FTP desde la máquina virtual (Linux Desktop) se muestran en la siguiente imagen estableciendo una conexión con el servidor FTP:

Imagen 32. Resultado regla FTP

Fuente: Autoría Propia

Esto nos confirma la efectividad de las reglas de firewall configuradas en el Endian para permitir el tráfico específico a los puertos 80 y 21 desde la red interna hacia el servidor Ubuntu en la DMZ.

Por otro lado, las pruebas realizadas desde la máquina virtual (Linux Desktop) hacia el servidor Ubuntu en la zona naranja no recibieron respuesta, esta fue denegada, tal como se muestra en la siguiente imagen:

Imagen 33. Resultado regla denegación ICMP

Fuente: Autoría Propia

Este resultado verificó la implementación correcta de las reglas de denegación de protocolo ICMP, entre ambas zonas, esto dificulta la capacidad de realizar escaneos de red básicos y de esta manera prevenir ciertos tipos de ataques.

El análisis de los registros del firewall de Endian mostró entradas que corresponden a las conexiones HTTP y FTP permitidas con la regla establecida. Adicional, se observaron entradas para los intentos de ping entre la zona verde y naranja, con la política establecida de “Denegar o Rechazar”, esto nos permite confirmar que el firewall está aplicando las reglas configuradas de manera correcta.

5.4 VERIFICACIÓN Y MONITOREO

La creación de las reglas en firewall no es suficiente para la protección, además, se requiere una verificación y monitoreo continuo para garantizar la efectividad y detectar posibles problemas.

Herramientas de Prueba: Son especializadas para que se pueda simular diferentes tipos de gráficos de la red para probar la efectividad de las reglas. Esta herramienta envía diferentes paquetes con direcciones de origen y destino y puertos para validar si el firewall está funcionando según lo esperado.

Captura de paquetes**:** Utilizar herramientas que capturan paquetes en las interfaces del Endian y en las máquinas para proporcionar una visión detallada del tráfico de red. Al analizar las pruebas, se puede verificar si los paquetes están llegando al firewall y si las reglas se están aplicando correctamente.

Análisis de tráfico: Este análisis a largo plazo de los registros de Endian, puede revelar patrones de tráfico o intentos de acceder a servicios bloqueados y esto puede indicar si se requieren cambios o ajustes de las reglas de firewall.

Revisiones periódicas de las reglas: Las reglas de Endian Firewall deben revisarse periódicamente para garantizar que sigan siendo efectivas. Los cambios en la infraestructura de la red o nuevas vulnerabilidades pueden requerir ajustes en las políticas.

6 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

El diseño de una arquitectura de red segmentada en múltiples zonas —LAN, DMZ y WAN— permite establecer políticas de seguridad diferenciadas y más precisas para el control del tráfico entre ellas. Esta segmentación es fundamental en entornos donde conviven distintos niveles de confianza, como en el caso de servidores expuestos a Internet (DMZ) y estaciones de trabajo internas (LAN).

En esta temática se explora la implementación avanzada de reglas de firewall en Endian para permitir servicios específicos como HTTP y FTP entre distintas zonas, así como validar la conectividad cruzada entre ellas. También se contempla la configuración NAT y el monitoreo mediante registros, con el fin de garantizar la trazabilidad del tráfico y la aplicación correcta de las políticas de red.

6.1 IMPLEMENTACIÓN DE LA ARQUITECTURA DE SEGURIDAD

La práctica fue desarrollada en un entorno virtualizado sobre VirtualBox, con tres zonas claramente definidas:

Zona Verde (LAN): 192.168.1.20/24 – Estación Desktop.

Zona Naranja (DMZ): 192.168.10.20/24 – Servidor Ubuntu con HTTP y FTP activos.

Zona Roja (WAN): Interfaz conectada con acceso a internet por DHCP (NAT).

Se instalaron y configuraron los servicios FTP (vsftpd) en el servidor Ubuntu de la zona naranja. Además, se validaron sus estados activos para la correcta funcionalidad de las pruebas posteriores.

6.2 CONFIGURACIÓN DE FIREWALL Y REGLAS DE ACCESO

Se implementaron múltiples reglas de tráfico en Endian, orientadas a permitir servicios específicos entre zonas y verificar la interoperabilidad de estas:

Permitir HTTP desde la zona verde a la zona DMZ (Puerto 80, protocolo TCP).

Permitir FTP desde la zona verde a la zona DMZ (Puerto 21, protocolo TCP).

Permitir HTTP desde la zona roja hacia la zona DMZ, simulando acceso desde Internet.

Permitir FTP desde la zona verde hacia la zona roja, configurando Endian para permitir salida de datos hacia la WAN.

Aplicación de reglas NAT que redirecciona el tráfico de la WAN hacia servicios alojados en la DMZ.

Configuración de UFW en el servidor Ubuntu, habilitando el puerto 21 para tráfico FTP.

6.3 ANÁLISIS DEL CONTROL DE ACCESO A SERVICIOS ESPECÍFICOS

En esta implementación, los servicios HTTP y FTP fueron habilitados en un servidor Ubuntu alojado en la zona naranja (DMZ), permitiendo su acceso controlado desde la LAN y la WAN mediante reglas específicas:

HTTP (puerto 80 – protocolo TCP): Este servicio se permite desde la zona verde (LAN) y desde la zona roja (WAN) hacia la DMZ. El tráfico HTTP, aunque esencial para la navegación web, debe ser monitoreado constantemente.

FTP (puerto 21 – protocolo TCP): Se permitió desde la LAN hacia la DMZ y desde la LAN hacia la zona roja (WAN), habilitando el servicio mediante UFW y NAT. El uso de FTP implica riesgos inherentes al transmitir credenciales en texto plano, por lo cual en entornos reales se sugiere SFTP o FTPS.

Reglas NAT y UFW: Se utilizó traducción de direcciones para redirigir tráfico entrante desde la WAN a servicios internos. Además, se configuró UFW en el servidor para permitir específicamente el puerto 21, cerrando otros accesos innecesarios.

6.4 METODOLOGÍA

Los pasos que realice para la implementación fueron los siguientes:

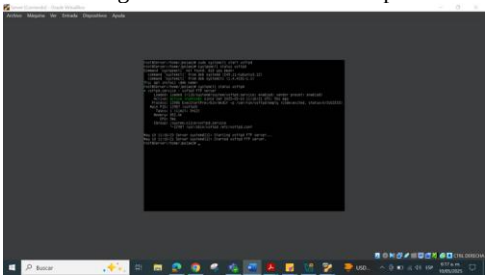
Se configuraron las interfaces de red virtualizadas para la zona verde, roja y naranja con los rangos de IP definidos.

Se asignó la dirección estática, con la puerta de enlace y se instalaron los servicios de FTP (vsftpd) confirmando que estuviera activo y funcional con el puerto 21.

Imagen 34. Configuración Red DMZ

Fuente: Autoría Propia

Imagen 35. Estado servicio vsftpd



Fuente: Autoría Propia

Creación de las reglas de Firewall en Endian:

Se creó una regla NAT para permitir el tráfico TCP con destino al puerto 80 y 21 de acuerdo con el servicio, desde la zona verde hacia la zona naranja.

Imagen 36. Regla permitir HTTP (80)

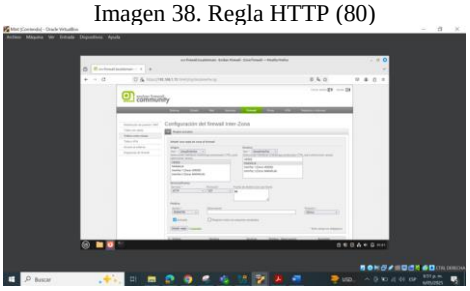
Fuente: Autoría Propia

Imagen 37. Regla permitir FTP (21)

Fuente: Autoría Propia

Tráfico entre Zonas HTTP y FTP: Se crean reglas similares seleccionando de la zona verde a la roja para permitir los servicios de HTTP y FTP con protocolo FTP y su respectivo puerto.

Imagen 38. Regla HTTP (80)



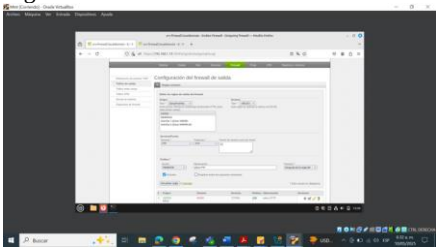
Fuente: Autoría Propia

Imagen 39. Regla FTP (21)

Fuente: Autoría Propia

Se crea un servicio para configurar el tráfico de salida de la Zona Verde a la Wan para el servicio FTP.

Imagen 40. Tráfico de Salida FTP Verde aWAN



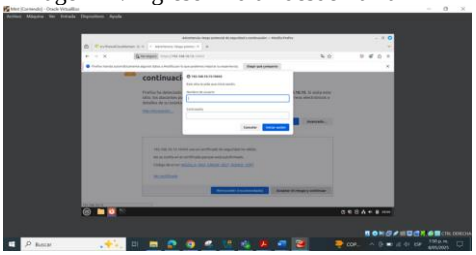
Fuente: Autoría Propia

6.5 RESULTADOS Y PRUEBAS

6.5.1 INGRESO SERVICIO HTTP DE LAN A DMZ

Ingresamos al endian utilizando la ip de la zona DMZ, y al salir el acceso al firewall del endian, demostramos la conexión HTTP desde la LAN a la zona DMZ.

Imagen 41. Ingreso Endian desde Lan a DMZ

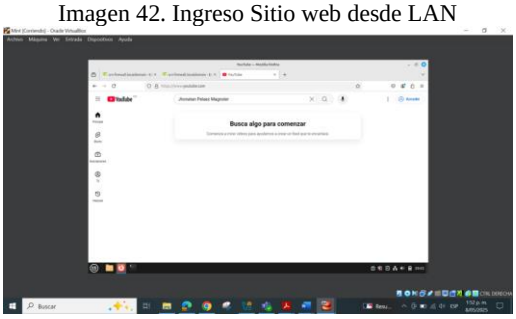


Fuente: Autoría Propia

6.5.2 INGRESO SERVICIO HTTP DE LAN A WAN

Para verificar el proceso de este servicio, simplemente abrimos el navegador e ingresamos a un sitio web y verificamos la navegabilidad, para este caso se ingresó a youtube.com.

Imagen 42. Ingreso Sitio web desde LAN



Fuente: Autoría Propia

6.5.3 INGRESO SERVICIO HTTP DE DMZ A WAN

En esta prueba se ingresó al ubuntu server y se hizo ping a la página de google.com, verificando así la salida de paquetes.

Imagen 43. Ping DMZ a Google.com

Fuente: Autoría Propia

6.5.4 INGRESO SERVICIO HTTP DE WAN A DMZ

Ingresamos a la consola del endian con la opción 0 y usando el comando Login para poder acceder desde el root y procedemos a hacer ping a la IP del servidor DMZ.

Imagen 44. Ping Endian a DMZ

Fuente: Autoría Propia

6.5.5 INGRESO SERVICIO FTP DE LAN A WAN

Para esta prueba se hizo una prueba de conexión FTP al servidor de Ubuntu.com, debido a que otros servidores tenían conexiones bloqueadas.

Imagen 45. FTP de LAN a Ubuntu

Fuente: Autoría Propia

6.5.6 INGRESO SERVICIO FTP DE WAN A DMZ

Para esta prueba se hace uso del servicio Netcat ya que es otro método que nos permite saber si llega hasta el FTP de un destino, en este caso al DMZ.

Imagen 46. Netcat WAN a DMZ

Fuente: Autoría Propia

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

La implementación de un proxy HTTP no transparente mediante la plataforma Endian Firewall Community constituye una solución eficaz para el control del tráfico web dentro de redes locales. El propósito principal de esta práctica es restringir el acceso a determinados sitios mediante listas negras, complementado con un esquema de autenticación por usuario que garantiza una navegación controlada y segura.

La actividad se desarrolló desde la creación de la máquina virtual que aloja el sistema Endian, hasta la configuración de perfiles de navegación, políticas de acceso y mecanismos de autenticación centralizada. Esta solución permite consolidar un entorno de red alineado con las políticas internas de uso de Internet, optimizando la gestión del ancho de banda y reduciendo los riesgos asociados al acceso no autorizado.

7.1 CREACIÓN E INSTALACIÓN DE MÁQUINA VIRTUAL ENDIAN.

El proceso inició con la descarga de la imagen ISO oficial de Endian Firewall Community, seleccionada por su robustez y capacidad para gestionar funciones de seguridad como firewall y proxy. Esta ISO se obtuvo desde el sitio web oficial y fue preparada para su implementación en un entorno virtualizado.

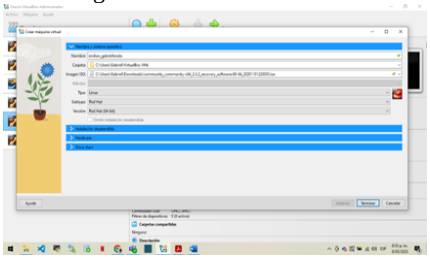
Endian ofrece una solución integral para la administración de redes, permitiendo aplicar políticas de control de acceso, autenticación de usuarios y filtrado de contenidos desde una única plataforma. Su distribución basada en Linux facilita la implementación en laboratorios de prueba o entornos reales.

Imagen 47. Descarga ISO Endian

Fuente: Autoría Propia

Posteriormente, se procedió a la creación de una máquina virtual utilizando la imagen ISO previamente descargada de Endian Firewall Community.

Imagen 48. Creación MV Endian

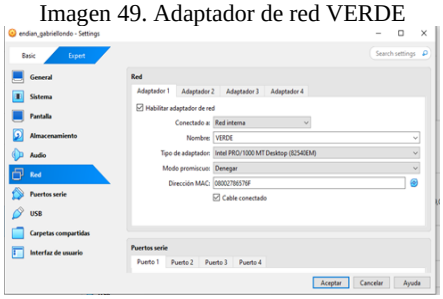


Fuente: Autoría Propia

A continuación, se crearon los tres adaptadores de red necesarios para el funcionamiento de Endian Firewall.

El primer adaptador se configuró como una red interna y fue asignado al segmento de red VERDE, correspondiente a la red LAN. Esta interfaz será responsable de gestionar el tráfico de los dispositivos locales hacia el proxy.

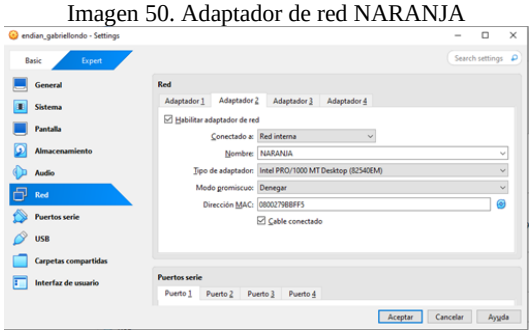
Imagen 49. Adaptador de red VERDE



Fuente: Autoría Propia

El segundo adaptador de red fue configurado como otra red interna, asignada al segmento NARANJA, correspondiente a la red DMZ.

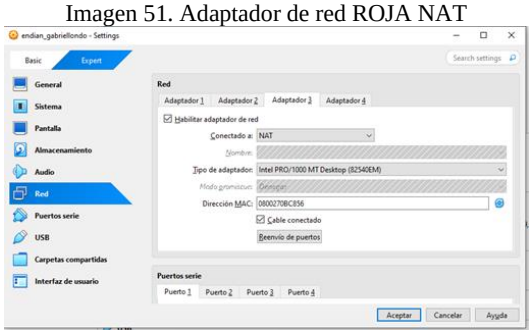
Imagen 50. Adaptador de red NARANJA



Fuente: Autoría Propia

El tercer adaptador fue configurado como red ROJA en modo NAT, destinado a proporcionar acceso a Internet desde el firewall.

Imagen 51. Adaptador de red ROJA NAT



Fuente: Autoría Propia

Una vez configurados los adaptadores de red, se procedió a iniciar la máquina virtual con la imagen ISO de Endian Firewall.

Durante el arranque inicial, el sistema solicitó la selección del idioma de instalación. Se elige el idioma inglés para facilitar la configuración y comprensión del entorno durante el proceso de instalación.

Imagen 52. Elección indio de instalación Endian

Fuente: Autoría Propia

Tras seleccionar el idioma, se procedió a iniciar el proceso de instalación del sistema operativo Endian Firewall Community.

Imagen 53. Instalación ISO Endian

Fuente: Autoría Propia

Una vez seleccionada la opción de instalación, se confirmó al sistema que inicie con el proceso de instalación en el disco.

Imagen 54. confirmación Instalación ISO Endian

Fuente: Autoría Propia

Finalizada la instalación, se configuró la dirección IP estática 192.168.10.20 para el adaptador asignado a la red VERDE.

Imagen 55. Asignación ip adpt VERDE

Fuente: Autoría Propia

Una vez configurada la IP en la red VERDE, se accedió sin inconvenientes a la interfaz web de Endian Firewall desde un navegador en el sistema Ubuntu Desktop.

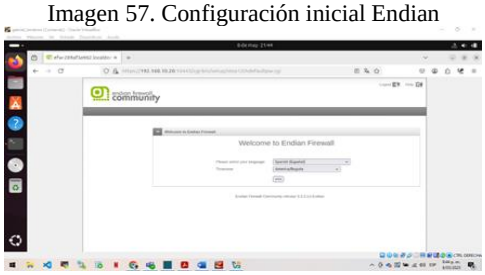
Imagen 56. Visualización Endian

Fuente: Autoría Propia

7.2 CONFIGURACIÓN INICIAL ENDIAN

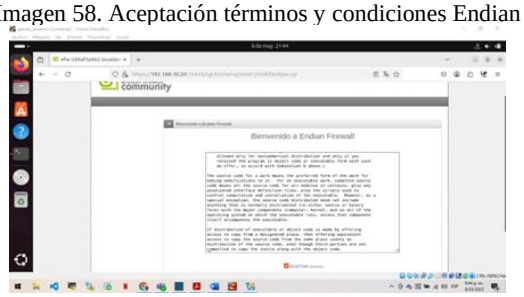
Se elige el idioma y la zona horaria para la configuración de ENDIAN.

Imagen 57. Configuración inicial Endian



Fuente: Autoría Propia

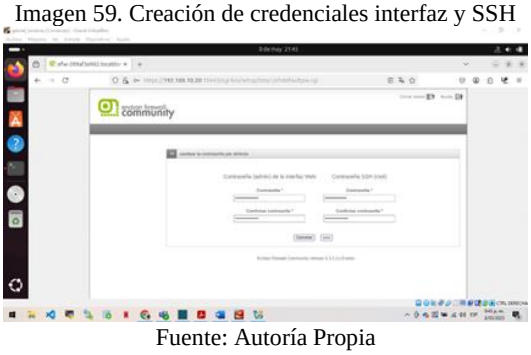
Imagen 58. Aceptación términos y condiciones Endian



Fuente: Autoría Propia

Se realiza la creación de las contraseñas para SSH y para la interfaz web.

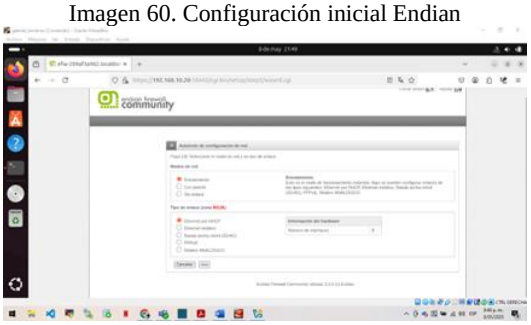
Imagen 59. Creación de credenciales interfaz y SSH



Fuente: Autoría Propia

Se inicia con la configuración de las zonas y el tipo de enrutamiento para el acceso a internet, pero también el enrutamiento por DHCP para la conexión.

Imagen 60. Configuración inicial Endian



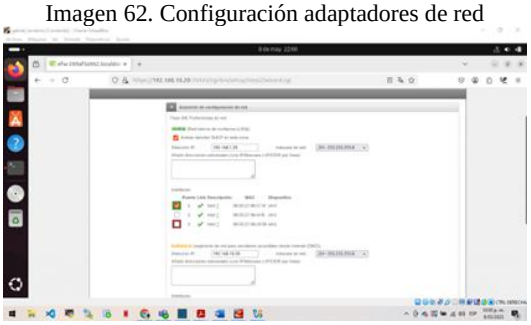
Fuente: Autoría Propia

Se configura los adaptadores de RED

Imagen 61. Configuración zona para DMZ

Fuente: Autoría Propia

Imagen 62. Configuración adaptadores de red



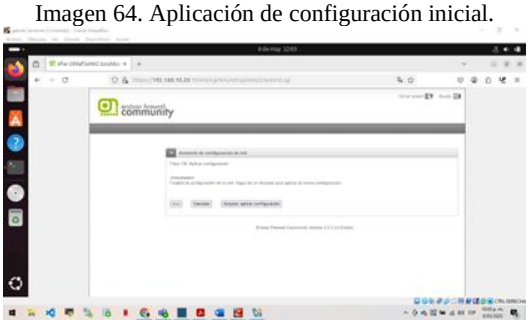
Fuente: Autoría Propia

Imagen 63. Configuración DNS automático

Fuente: Autoría Propia

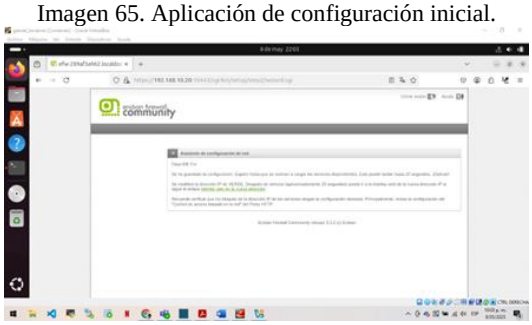
Se culmina la configuración inicial, le damos aceptar y aplicar y este se encargará de dejar listo el ambiente para trabajar.

Imagen 64. Aplicación de configuración inicial.



Fuente: Autoría Propia

Imagen 65. Aplicación de configuración inicial.



Fuente: Autoría Propia

7.3 CONFIGURACIÓN PROXY ENDIAN

Se ingresa como administrador a la interfaz para iniciar con la configuración del proxy.

Imagen 66. Interfaz admin Endian

Fuente: Autoría Propia

Configuración del proxy. Vamos hasta la pestaña Proxy y habilitamos el proxy http. Seleccionamos la opción de proxy no transparente para que deba ser configurado manualmente en los navegadores. Finalmente, elegimos el puerto 8080.

Imagen 67. Se activa el proxy HTTP

Fuente: Autoría Propia

Ahora nos dirigimos a crear la lista negra.

Imagen 68. Lista negra

Fuente: Autoría Propia

7.4 AUTENTICACIÓN POR USUARIO

Se inicia creando un usuario en la pestaña de Autenticación

Imagen 69. Interfaz Autenticación-usuario

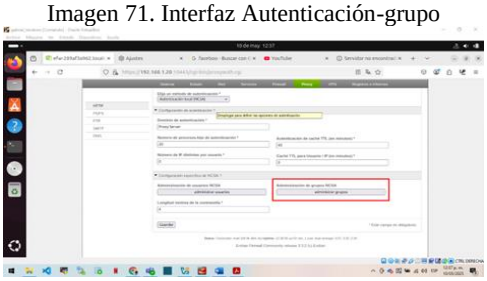
Fuente: Autoría Propia

Imagen 70. Creación del usuario

Fuente: Autoría Propia

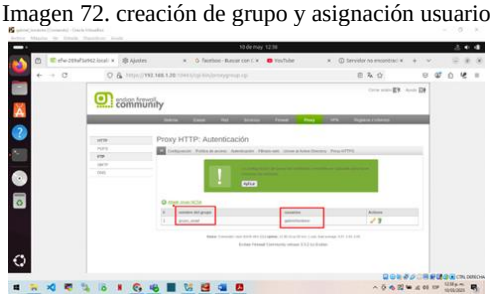
Ahora vamos a crear el grupo y a asignar el usuario anterior a este nuevo grupo. Este paso permite aplicar políticas específicas y gestionar permisos de manera más organizada dentro del sistema.

Imagen 71. Interfaz Autenticación-grupo



Fuente: Autoría Propia

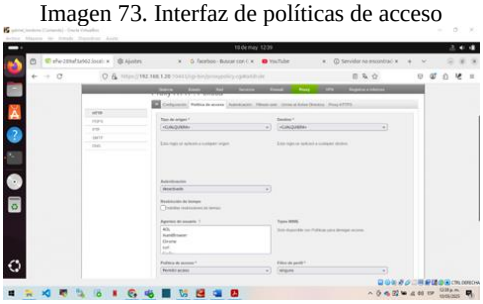
Imagen 72. creación de grupo y asignación usuario



Fuente: Autoría Propia

Ahora vamos a crear las políticas de acceso para el proxy. Estas políticas permiten definir y controlar los sitios web o servicios a los que los usuarios pueden acceder mediante el proxy.

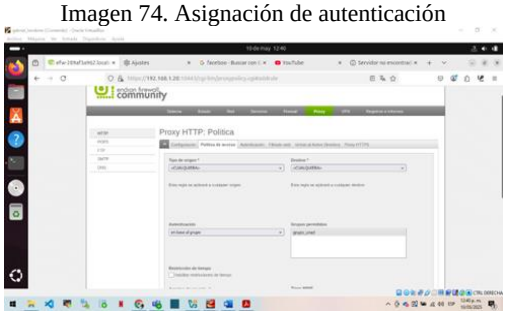
Imagen 73. Interfaz de políticas de acceso



Fuente: Autoría Propia

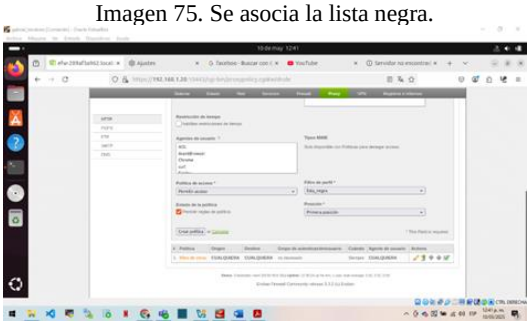
Se realizará la autenticación mediante el grupo creado.

Imagen 74. Asignación de autenticación



Fuente: Autoría Propia

Imagen 75. Se asocia la lista negra.

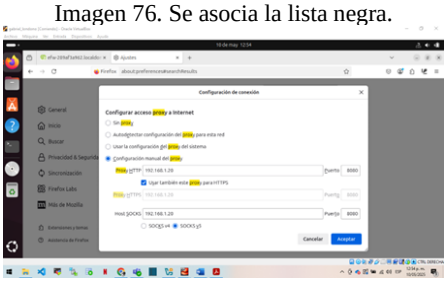


Fuente: Autoría Propia

7.5 PRUEBAS PROCESOS

En el navegador Firefox se configura el proxy con anterioridad creado en Endian,

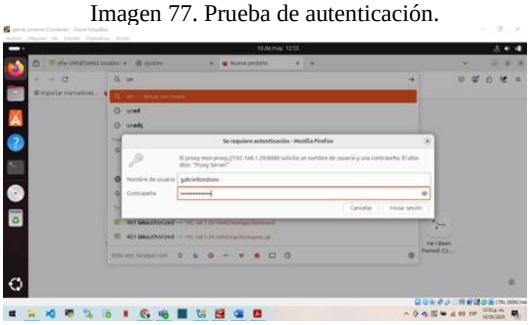
Imagen 76. Se asocia la lista negra.



Fuente: Autoría Propia

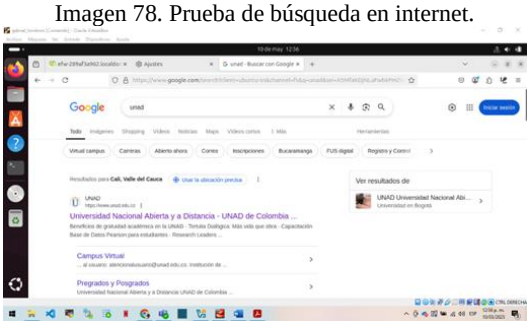
Al intentar ingresar al navegador nos pide autenticación.

Imagen 77. Prueba de autenticación.



Fuente: Autoría Propia

Imagen 78. Prueba de búsqueda en internet.



Fuente: Autoría Propia

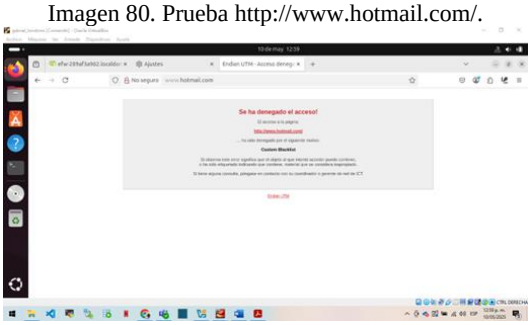
Imagen 79. Prueba ingreso a la red social X.

Fuente: Autoría Propia

Ahora vamos a probar los sitios que quedaron en la lista negra configurada.

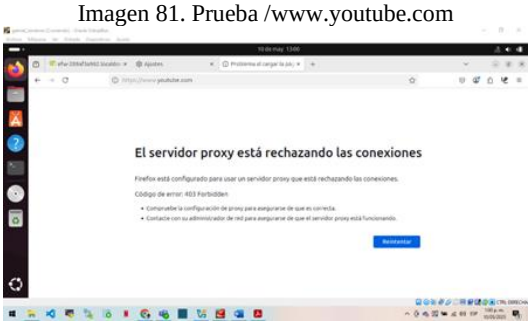
.

Imagen 80. Prueba http://www.hotmail.com/.



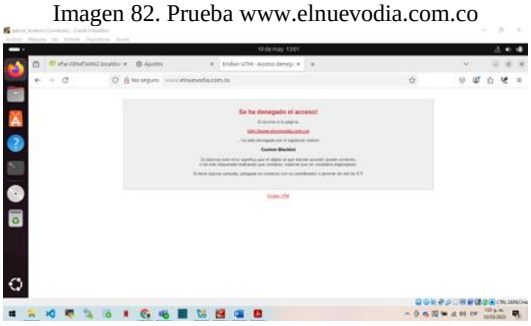
Fuente: Autoría Propia

Imagen 81. Prueba /www.youtube.com



Fuente: Autoría Propia

Imagen 82. Prueba www.elnuevodia.com.co



Fuente: Autoría Propia

8 CONCLUSIONES

La implementación de una arquitectura de red segmentada utilizando Endian Firewall ha demostrado ser una solución robusta, flexible y eficaz para fortalecer la seguridad en entornos empresariales que operan sobre sistemas GNU/Linux. A lo largo del desarrollo del proyecto, se evidenció que la correcta planificación y configuración de las zonas de red —verde (LAN), naranja (DMZ) y roja (WAN)— proporciona una base sólida para aplicar políticas diferenciadas de acceso y protección, reduciendo considerablemente el riesgo de ataques internos y externos.

La utilización de técnicas como Network Address Translation (NAT) permitió asegurar el tráfico saliente de las zonas internas hacia el exterior, manteniendo la privacidad de las direcciones IP internas y controlando la salida a Internet de forma eficiente. De igual forma, la implementación de reglas específicas para permitir servicios como HTTP y FTP desde zonas definidas, y la restricción de protocolos como ICMP, evidenció la capacidad de Endian Firewall para aplicar controles precisos y adaptados a los requerimientos de seguridad del entorno.

Asimismo, la integración de un proxy HTTP no transparente, acompañado de autenticación por usuario y políticas de filtrado de contenido, introdujo un nivel adicional de control sobre la navegación, reforzando la administración del uso de Internet dentro de la red corporativa. Esta funcionalidad no solo limita el acceso a contenidos no deseados, sino que también permite auditar el comportamiento de los usuarios y garantizar el cumplimiento de normativas internas.

Las pruebas realizadas en cada etapa del proyecto validaron la efectividad de las configuraciones, confirmando que los dispositivos y servicios alojados en la DMZ pueden ser accedidos de forma controlada desde otras zonas, sin comprometer la seguridad ni la integridad del sistema. El monitoreo constante y el análisis de registros facilitaron la trazabilidad del tráfico y permitieron ajustar las reglas en función de los resultados obtenidos.

En conclusión, este proyecto demuestra que una arquitectura segmentada, bien estructurada y respaldada por una herramienta como Endian Firewall, es una estrategia altamente efectiva para proteger activos críticos, controlar el flujo de datos y garantizar la disponibilidad de los servicios. Además, resalta la importancia de combinar aspectos técnicos como reglas de firewall, NAT y segmentación con elementos de gestión como autenticación, monitoreo y filtrado, para construir soluciones integrales y sostenibles en el tiempo.

9 REFERENCIAS

[1] *Basic Network Commands.* (2012, abril 19). Endian. https://help.endian.com/hc/en-us/articles/2181444668-Basic-Network-Commands

[2] *Endian Firewall Community.* (2023, octubre 4). SourceForge. https://sourceforge.net/projects/efw/

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

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

[5] *Canonical* (2023), Guia del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

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

[7] *Jai LaCroix* (2020), Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[8] *Guzmán, D. A.* (2017), OVI Unidad I_Nivelacion. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. http://hdl.handle.net/10596/10570

[9] *Hernández P. F.* (2022), OVI Monitoreo y administración de sistemas Linux. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53211

[10] *DigitalOcean* (2024), How to Secure Apache with Let's Encrypt on Ubuntu. https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu

10 ANEXOS

En este anexo se presenta un resumen cuantitativo de las imágenes o gráficos utilizados en el cuerpo del articulo:

Número total de imágenes: 82

Incluyen diagramas, capturas de pantalla esenciales y claves para la configuración, gráficos y otras representaciones donde se visualizan los resultados, proporcionando una comprensión más clara de la información presentada.