IMPLEMENTACIÓN DE ENDIAN FIREWALL EN UNA RED EMPRESARIAL SIMULADA CON CONFIGURACIÓN BÁSICA DE POLÍTICAS DE SEGURIDAD

Leidy Johana Luna Durán
e-mail: ljlunad@unadvirtual.edu.co
Jhan Carlos Holguín Mosquera
e-mail: jcholguinmo@unadvirtual.edu.co
Roymer Fabian Velandia Duran
e-mail: rfvelandiad@unadvirtual.edu.co
Daniel Andres Valbuena Gonzalez
e-mail: davalbuenag@unadvirtual.edu.co
Brayan Manuel Mateus Rodriguez
e-mail: bmmateusr@unadvirtual.edu.co

RESUMEN: *En este articulo se presenta la implementación y configuración de GNU/Linux Endian en un entorno virtualizado por medio de VirtualBox, orientado a la segmentación de red en zonas verde (LAN), roja (WAN) y naranjada (DMZ). Se realiza el respectivo diagrama de red en donde se define el direccionamiento para cada una de las zonas. Se detallan los pasos de instalación del sistema Endian, la configuración de reglas NAT, la habilitación y restricción de servicios específicos como HTTP, FTP e ICMP en la DMZ zona naranjada. También, se describen reglas de acceso para permitir o denegar el tráfico, por último, se implementa un Proxy HTTP con políticas de autenticación para la navegación en internet, creando listas negras que permitan bloquear ciertos sitios web.*

PALABRAS CLAVE: GNU/Linux Endian, Firewall, seguridad de red, DMZ.

1 INTRODUCCIÓN

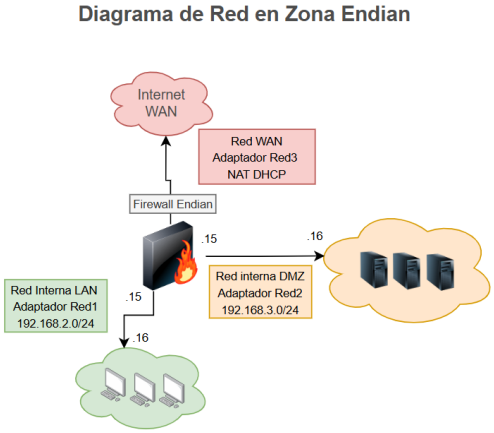
La creciente complejidad y dependencia de las redes informáticas ha llevado a las organizaciones a adoptar medidas rigurosas de seguridad perimetral. En este contexto, la segmentación de redes y el control de tráfico mediante firewalls y proxys son componentes fundamentales. Este proyecto tiene como objetivo implementar una infraestructura de red segura y segmentada en un entorno virtualizado, utilizando VirtualBox, Ubuntu Server y el sistema de seguridad Endian UTM 3.3. A través de cinco módulos temáticos, se abordaron aspectos clave como la configuración de zonas de red, reglas de NAT, habilitación de servicios en la DMZ, políticas de control de tráfico entre zonas, y la implementación de un proxy con autenticación. Esta práctica busca fortalecer las competencias en administración de redes seguras y control de accesos, replicando condiciones reales de una red corporativa.

2 DESARROLLO DE CONTENIDOS

2.1 INSTALACIÓN DE GNU/LINUX ENDIAN Y CONFIGURACIÓN DE LAS ZONAS DE RED

El primer paso para iniciar el proceso de instalación del firewall Endian consiste en elaborar el diagrama de red con el direccionamiento asignado a cada zona definida. En este caso, se establece la zona verde para la red LAN de la empresa, la zona naranja para la DMZ, donde se encuentran los servidores, y finalmente la zona roja, que corresponde al firewall, al cual se le asigna direccionamiento mediante DHCP. A continuación, se presenta el diagrama de red correspondiente.

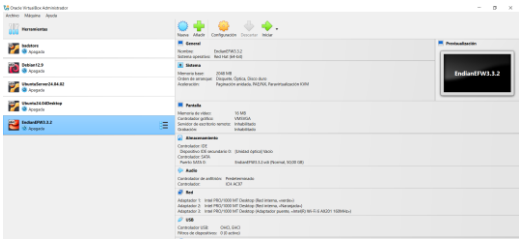
Figura 1 Diagrama de Red



Fuente: Autoría Propia

Una vez definido el direccionamiento, se procede a crear la máquina virtual Endian con las características mínimas requeridas para la instalación del sistema, que son: procesador x86 de 500 MHz, 256 MB de RAM, 4 GB de disco duro, y tres tarjetas de red (en lugar de las dos habituales). Además, se incluyen los periféricos necesarios para la instalación, tales como monitor, teclado y mouse.

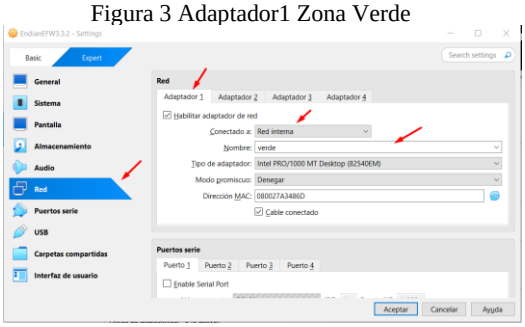
Figura 2 características maquina Endian



Fuente: Autoría Propia

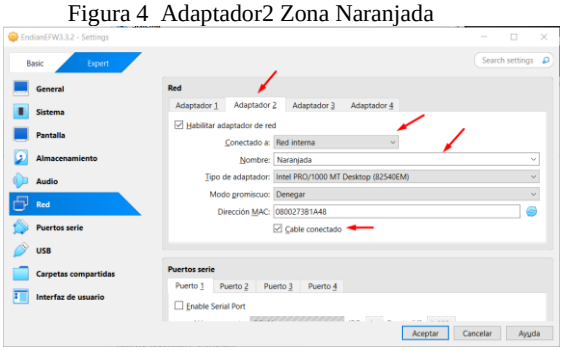
Para configurar las zonas de red en Endian Firewall en la máquina virtual, se asigna la zona verde al adaptador 1, la zona naranja al adaptador 2 y la zona roja al adaptador 3, tal como se muestra en las imágenes correspondientes.

Figura 3 Adaptador1 Zona Verde



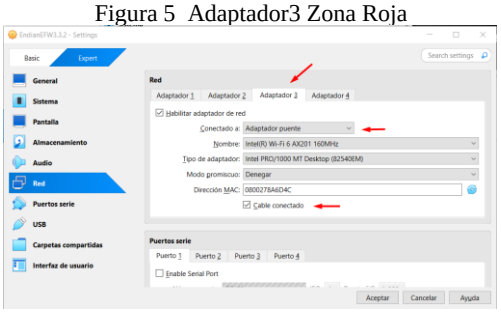
Fuente: Autoría Propia

Figura 4 Adaptador2 Zona Naranjada



Fuente: Autoría Propia

Figura 5 Adaptador3 Zona Roja



Fuente: Autoría Propia

Ahora se procede a iniciar la máquina virtual, la cual ya tiene vinculada la imagen ISO para su instalación. A continuación, se sigue el procedimiento paso a paso:

Primero, se selecciona el idioma que utilizará el Endian Firewall (EFW); en este caso, se elige el inglés.

Figura 6 Idioma EFW

Fuente: Autoría Propia

En esta sección se selecciona la opción **Yes** para permitir que el instalador utilice todo el disco duro.

Figura 7 Selección disco duro

Fuente: Autoría Propia

Luego de seleccionar la opción **Yes**, se muestra la siguiente imagen, donde el firewall Endian ya se encuentra instalado. Adicionalmente, se visualiza el direccionamiento asignado a las zonas verde y roja. Para acceder al shell, inicialmente se solicita la contraseña de root, la cual es **endian**.

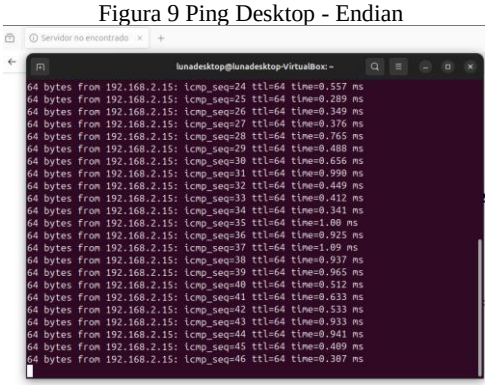
A continuación, se debe ingresar a la máquina de escritorio para realizar la configuración de Endian mediante acceso HTTP. Para ello, primero se verifica que la máquina haya obtenido la dirección IP correspondiente, que en este caso es 192.168.2.16/24, con puerta de enlace 192.168.2.15. La imagen siguiente confirma esta configuración.

Figura 8 Dirección desktop

Fuente: Autoría Propia

Se realiza un ping hacia el firewall Endian y este responde con éxito, lo que indica que la conectividad básica entre el equipo desde el cual se ejecuta el ping y el firewall está funcionando correctamente. Esta prueba es una de las más comunes para verificar la comunicación en la red y confirmar que el dispositivo está activo y accesible.

Figura 9 Ping Desktop - Endian



Fuente: Autoría Propia

Para acceder a la interfaz de administración de Endian Firewall desde la máquina desktop, se debe ingresar en el navegador la dirección IP del firewall seguida del puerto 10443, que es el puerto HTTPS configurado para su acceso seguro. En este caso, la dirección a utilizar es: https://192.168.2.15:10443

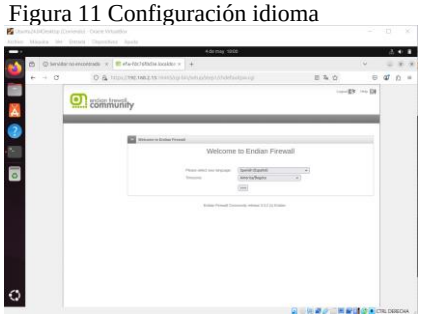
El puerto 10443 es una alternativa al puerto HTTPS estándar 443, comúnmente usado para la administración remota segura del firewall Endian. Es importante que este puerto esté abierto y permitido en el firewall para garantizar el acceso mediante HTTPS.

Al ingresar a la URL de acceso al firewall Endian, se muestra una ventana de bienvenida que inicia el asistente de configuración. A continuación, se procede a seleccionar el idioma de preferencia para la interfaz, así como la zona horaria correspondiente. Este paso es fundamental para personalizar la experiencia de uso y garantizar que los registros y eventos del sistema se ajusten al horario local.

Figura 10 Bienvenida Endian

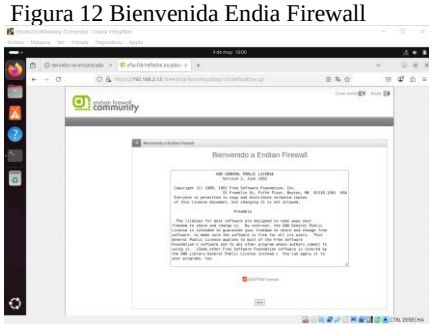
Fuente: Autoría Propia

Figura 11 Configuración idioma



Fuente: Autoría Propia

Figura 12 Bienvenida Endia Firewall



Fuente: Autoría Propia

Luego se configuran las contraseñas para acceder a Endian tanto mediante la interfaz web como por SSH. Se recomienda utilizar contraseñas diferentes para cada acceso, con el fin de aumentar la seguridad del sistema.

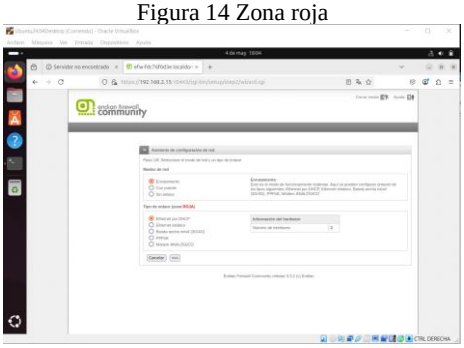
Esta recomendación es común en la configuración inicial de Endian Firewall, donde se asignan contraseñas separadas para el usuario **admin** (acceso a la interfaz web) y para el usuario **root** (acceso por consola o SSH), garantizando así un mejor control y protección frente a accesos no autorizados

Figura 13 Configuración contraseñas HTTP - SSH

Fuente: Autoría Propia

A continuación, se indica el modo de red que se va a utilizar y el tipo de direccionamiento para la zona roja; en este caso, se selecciona enrutamiento mediante DHCP.

Figura 14 Zona roja



Fuente: Autoría Propia

Se especifica la zona a utilizar para la DMZ.

Figura 15 Zona DMZ

Fuente: Autoría Propia

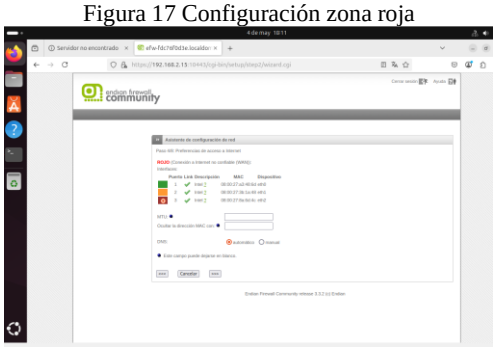
Se configura la dirección IP asignada para la zona verde y la zona naranja, junto con la máscara de red correspondiente.

Figura 16 Configuración direccionamiento zonas

Fuente: Autoría Propia

Se presenta la configuración de la zona roja con las interfaces configuradas en Endian.

Figura 17 Configuración zona roja



Fuente: Autoría Propia

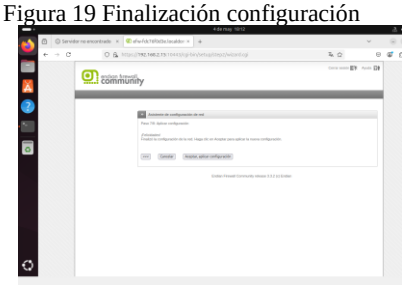
Se configura el DNS de forma automática y se finaliza la configuración inicial del firewall.

Figura 18 Configuración DNS

Fuente: Autoría Propia

Para ello, se hace clic en **Aceptar**, **aplicar configuración**.

Figura 19 Finalización configuración



Fuente: Autoría Propia

Posteriormente, se carga la plataforma Endian, donde en el ítem **Estado** se pueden visualizar los diferentes estados del sistema.

Figura 20 Inicio Endian

Fuente: Autoría Propia

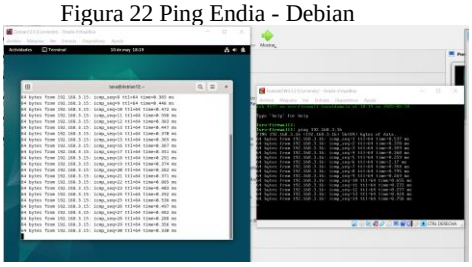
A continuación, se muestra el estado de las interfaces de red, en el cual se reflejan las zonas configuradas junto con su respectivo direccionamiento IP.

Figura 21 Estado de las interfaces

Fuente: Autoría Propia

Para verificar la conectividad, se realiza un ping desde el servidor Debian hacia Endian, el cual responde con éxito; de igual forma, se realiza un ping desde Endian hacia Debian, confirmando la comunicación bidireccional.

Figura 22 Ping Endia - Debian

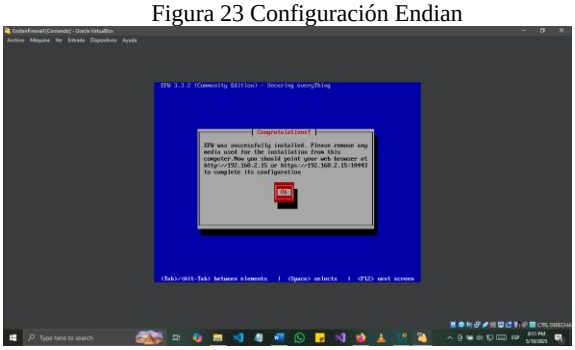


Fuente: Autoría Propia

2.2 CONFIGURACIÓN NAT

Partiendo de la instalación inicial del firewall Endian, se procede con la configuración de la Zona Verde (LAN) a través del asistente de instalación. En esta etapa, se asigna de forma manual la dirección IP 192.168.2.15 a la interfaz correspondiente, la cual actuará como puerta de enlace para los dispositivos de la red interna. Esta configuración es crucial, ya que establece el punto de acceso principal para la administración del sistema y la comunicación entre el firewall y los equipos conectados a la red LAN, como se muestra en la siguiente captura de configuración.

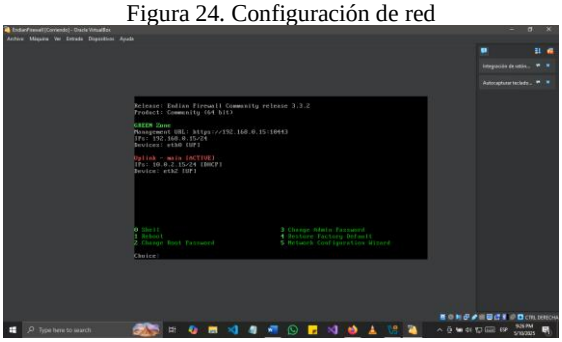
Figura 23 Configuración Endian



Fuente: Autoría Propia

Una vez completado el proceso de instalación y reiniciado el sistema, se accede al menú principal del firewall Endian, desde donde se lleva a cabo la configuración avanzada de red. En esta etapa, se procede a definir y asignar las interfaces físicas a las respectivas zonas de seguridad: Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN). Esta segmentación es esencial para establecer límites de seguridad, aplicar políticas diferenciadas y asegurar un flujo controlado de tráfico entre las distintas áreas de la red corporativa simulada.

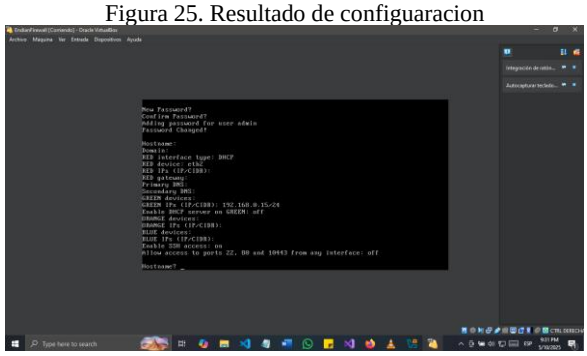
Figura 24. Configuración de red



Fuente: Autoría propia

Una vez finalizada la asignación de interfaces y parámetros de red para cada zona, la configuración general del sistema debería reflejarse de acuerdo con el diseño lógico establecido en el diagrama de red. Este diagrama representa la segmentación del tráfico y la estructura de comunicación entre las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), permitiendo visualizar de manera clara cómo se enrutan y controlan los flujos de datos dentro del entorno simulado. Esta configuración constituye la base para aplicar las políticas de seguridad y reglas de acceso que se implementarán en etapas posteriores del proyecto.

Figura 25. Resultado de configuaracion



Fuente: Autoria propia

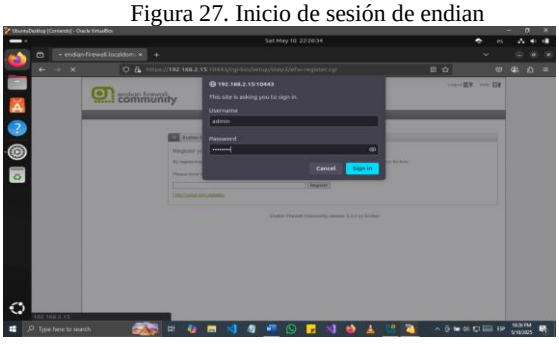
A continuación, desde VirtualBox se crea una nueva máquina virtual que simula un equipo cliente dentro de la red LAN, conectado a la Zona Verde del firewall Endian. Esta máquina, denominada *Desktop-LAN*, debe configurarse con una dirección IP estática dentro del mismo rango que la interfaz verde del firewall. En este caso, se asigna la dirección IP 192.168.2.16, asegurando que comparta la misma subred (192.168.2.0/24) y tenga como puerta de enlace la IP 192.168.2.15. Esta configuración permitirá la comunicación directa con el firewall y servirá como punto de prueba para validar la conectividad, las reglas de acceso y las políticas de navegación definidas posteriormente.

Figura 26. Equipo red LAN

Fuente: autoría propia

Posteriormente, se accede a la interfaz web de administración de Endian a través de su dirección IP asignada (http://192.168.2.15 o https://192.168.2.15:10443), siendo ambas opciones funcionales al redirigir al portal de gestión. Este acceso confirma la conectividad entre el firewall Endian y el equipo cliente a través de la Zona Verde (Red Interna).

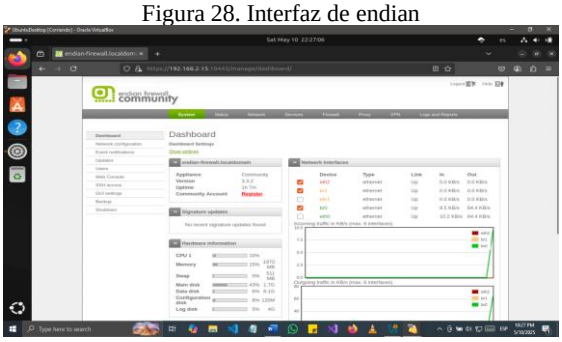
Figura 27. Inicio de sesión de endian



Fuente: autoría propia

Cuando se inicia sesión en la consola web de Endian a través de un navegador, se accede a la interfaz principal del sistema, la cual proporciona una visión general del estado del firewall. En esta pantalla inicial se pueden evidenciar indicadores clave como el estado de las interfaces de red, estadísticas de tráfico, servicios activos, alertas del sistema y accesos rápidos a configuraciones esenciales. Esta interfaz centralizada permite gestionar de forma intuitiva las políticas de seguridad, las reglas de firewall, la configuración de NAT, los servicios de red (HTTP, FTP, DNS, etc.), así como las herramientas de monitoreo y control de tráfico en tiempo real.

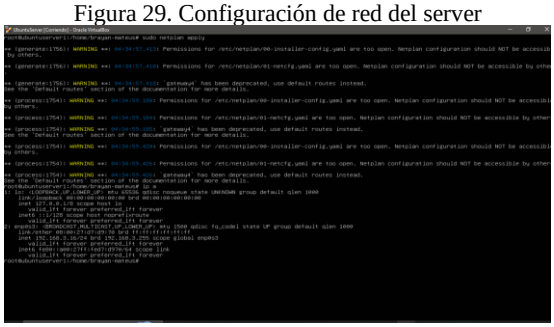
Figura 28. Interfaz de endian



Fuente: autoría propia

A continuación, se crea una máquina virtual adicional en VirtualBox destinada a funcionar como servidor dentro de la Zona Naranja (DMZ). Esta máquina utiliza Ubuntu Server como sistema operativo y se conecta a la interfaz correspondiente del firewall Endian. Una vez iniciada la máquina virtual, se procede a configurar manualmente su dirección IP mediante la edición del archivo de configuración de red de *Netplan*. Para ello, se accede al archivo ubicado en /etc/netplan/, donde se define una IP estática dentro del rango asignado a la DMZ.

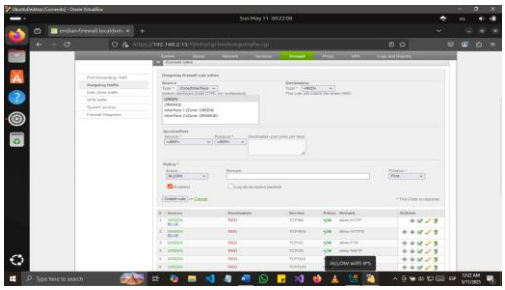
Figura 29. Configuración de red del server



Fuente: autoría propia

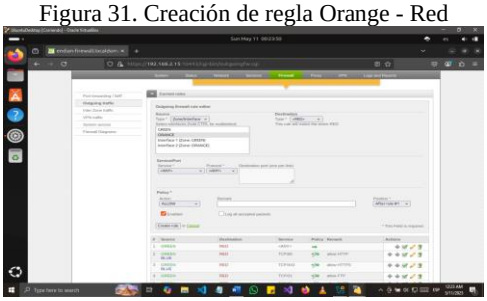
Una vez establecida la conectividad básica entre las zonas de red, se procede a configurar las reglas de acceso a Internet desde la interfaz web del firewall Endian. El primer paso consiste en permitir la salida hacia la red WAN (Zona Roja) desde el equipo cliente ubicado en la Zona Verde (LAN). Para ello, se accede al apartado **Firewall > Outgoing Traffic**, donde se define una regla de traducción de direcciones (NAT) que permita la comunicación desde la IP del *Desktop-LAN* (192.168.2.16) hacia el exterior.

Figura 30. Creación de regla Green - Red



Fuente: autoría propia

Figura 31. Creación de regla Orange - Red



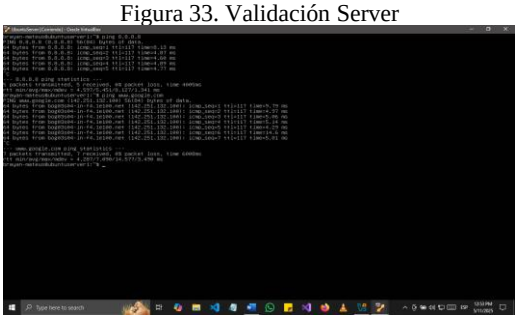
Fuente: autoría propia

Una vez creadas las reglas de NAT para permitir la conexión a Internet a través del firewall, es necesario validar su correcta implementación. Para ello, se realiza una prueba de conectividad utilizando el comando **ping** hacia una dirección IP externa, como la de los servidores de Google DNS (8.8.8.8). Al ejecutar este comando desde el equipo *Endian* o el servidor ubicado en la DMZ, se espera recibir respuestas exitosas, lo que confirmaría que las reglas de NAT y la conectividad a la red externa están funcionando correctamente. Esta prueba es un paso crucial para verificar que la traducción de direcciones se está realizando correctamente y que los equipos internos pueden acceder a Internet de manera adecuada, como se ilustra a continuación.

Figura 32. Validación Endian

Fuente: autoría propia

Figura 33. Validación Server



Fuente: autoría propia

2.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

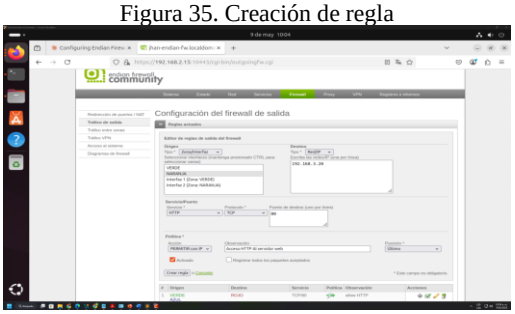
Una vez que el firewall Endian está en pleno funcionamiento y las zonas de red han sido correctamente configuradas, se procede a permitir los servicios HTTP (puerto 80) y FTP (puerto 21) en el servidor Ubuntu ubicado en la Zona Naranja (DMZ). Para habilitar el servicio HTTP, es necesario instalar y activar el servidor web Apache mediante los siguientes comandos ejecutados en la terminal: sudo apt update, sudo apt install apache2 -y, sudo systemctl enable apache2 y sudo systemctl start apache2. Estos pasos aseguran que el servidor web esté actualizado, instalado correctamente, habilitado para iniciarse automáticamente y en ejecución. Una vez que Apache está operativo, se podrá definir en la interfaz web de Endian las reglas de firewall necesarias para permitir el tráfico HTTP y, posteriormente, se procederá con la habilitación del servicio FTP siguiendo un procedimiento similar.

Figura 34. Intalacion apache

Fuente: autoría propia

Posteriormente, se procede a la creación de reglas en el firewall Endian para permitir el acceso al servicio HTTP ofrecido por el servidor ubicado en la Zona Naranja (DMZ). Desde la interfaz web de administración, se accede al apartado **Firewall > Port Forwarding**, donde se define una nueva regla que permita redirigir las solicitudes entrantes al puerto 80 desde la Zona Verde (LAN) hacia la IP del servidor web configurado en la DMZ (por ejemplo, 192.168.3.10). Esta regla especifica el protocolo TCP, el puerto de destino (80), la zona de origen (Verde) y la zona de destino (Naranja), garantizando así que los clientes internos puedan acceder al servicio web de forma controlada.

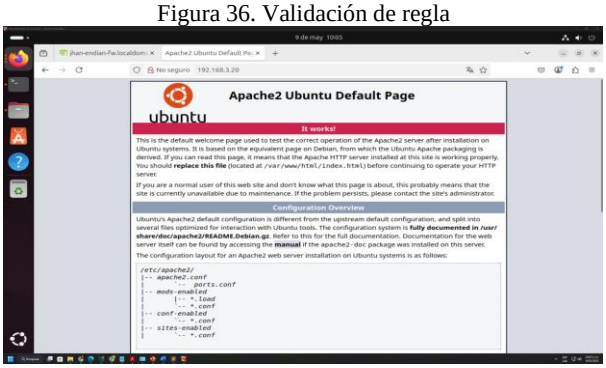
Figura 35. Creación de regla



Fuente: autoría propia

Una vez creada la regla de acceso HTTP en el firewall Endian, se procede a su validación accediendo desde un navegador web en el equipo cliente de la Zona Verde. Para ello, se ingresa la dirección IP del servidor web de la DMZ, lo cual debería redirigir a la página por defecto del servidor Apache. La correcta visualización de esta página confirma que la regla ha sido aplicada exitosamente, que el tráfico HTTP entre la zona LAN y la DMZ está permitido, y que el servidor Apache se encuentra funcionando de manera adecuada.

Figura 36. Validación de regla



Fuente: autoría propia

Para habilitar el servicio FTP en el servidor web ubicado en la Zona Naranja (DMZ), se procede con la instalación del servidor **vsftpd** en el sistema Ubuntu. Esto se realiza ejecutando los siguientes comandos en la terminal: sudo apt install vsftpd -y, sudo systemctl enable vsftpd y sudo systemctl start vsftpd. Estos pasos aseguran que el servicio FTP esté instalado, configurado para iniciarse automáticamente al arranque y activo en el sistema. Una vez operativo, se crea la regla correspondiente en la interfaz web del firewall Endian, accediendo al módulo **Firewall > Port Forwarding**, donde se define una regla que permita el tráfico entrante por el puerto 21 (protocolo TCP) desde la Zona Verde hacia la dirección IP del servidor en la DMZ. Esta configuración garantiza que los clientes ubicados en la red interna puedan establecer conexiones FTP con el servidor de manera segura y controlada.

Figura 37. Servicio ftp

Fuente: autoría propia

Figura 38. Regla creada

Fuente: autoría propia

Con el objetivo de reforzar la seguridad de la red, se procede a la creación de una regla de firewall para denegar el protocolo ICMP, lo cual impide la ejecución del comando **ping** entre zonas. Esta medida se implementa bloqueando el tráfico asociado a los tipos de mensaje ICMP correspondientes al **Echo Request (tipo 8)** y **Echo Reply (tipo 0)**. Desde la interfaz web de Endian, en el módulo **Firewall > Inter-Zone Traffic**, se define una regla explícita que bloquee el tráfico ICMP entre las zonas deseadas (por ejemplo, de la Zona Verde hacia la DMZ). Una vez aplicada la configuración, se valida su efectividad ejecutando el comando ping desde un equipo cliente hacia una IP de destino (por ejemplo, el servidor web en la DMZ). La ausencia de respuestas confirma que el bloqueo ha sido exitosamente implementado, restringiendo así la visibilidad y el diagnóstico de red desde zonas no autorizadas.

Figura 39. Denegación del protocolo

Fuente: autoría propia

Figura 40. Regla aplicada

Fuente: autoría propia

Una vez configuradas las reglas de denegación del protocolo ICMP, se procede a verificar su aplicación en el tráfico de salida desde los distintos dispositivos de la red. Esta verificación se realiza mediante intentos de conexión con el comando ping, los cuales deben fallar si la política ha sido correctamente implementada. En primer lugar, se intenta hacer ping desde el cliente *Desktop-LAN* hacia el servidor web en la DMZ, lo cual resulta denegado conforme a la regla definida. Del mismo modo, se ejecuta un ping desde el servidor hacia la interfaz del firewall Endian, así como desde el *Desktop-LAN* hacia la misma interfaz, obteniendo igualmente respuestas denegadas. Esta ausencia de respuesta confirma que las reglas de firewall están bloqueando correctamente los paquetes ICMP tipo 8 (Echo Request), reduciendo la exposición de la infraestructura a técnicas de escaneo o reconocimiento. La validez de estas reglas también puede observarse en la sección de monitoreo de tráfico de la interfaz de Endian, donde se registran los intentos bloqueados.

Figura 41. Ping al server

Fuente: autoría propia

Figura 42. Ping de server a endian

Fuente: autoría propia

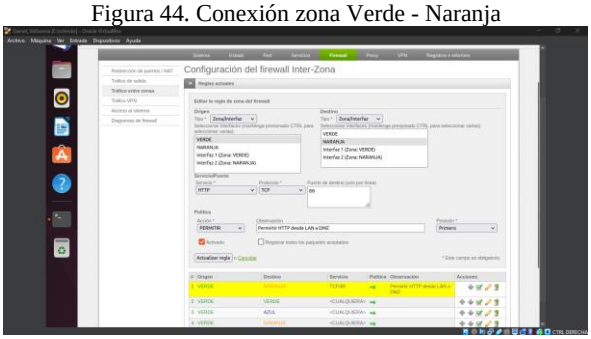
Figura 43. Ping de desktop a endian

Fuente: autoría propia

2.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR TRAFICO

A continuación, se muestra la comunicación creada para la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Figura 44. Conexión zona Verde - Naranja



Fuente: Autoría Propia

En figura 44 se muestra la creación de una regla de firewall que permite el tráfico HTTP (puerto 80/TCP) desde la zona Verde hacia la zona Naranja. Esta configuración garantiza que los dispositivos en la LAN puedan acceder a servicios web ubicados en la DMZ. La regla se establece seleccionando las interfaces correspondientes, el protocolo TCP y el puerto 80, con la acción "Permitir" habilitada.

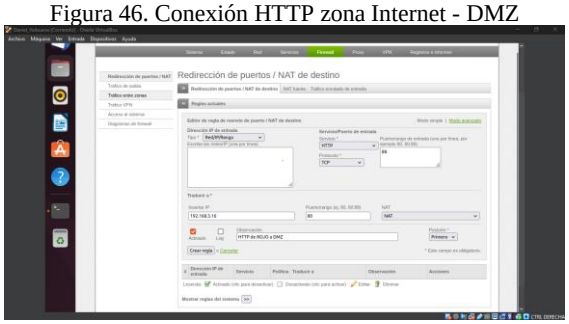
Figura 45. Aplicación de las reglas

Fuente: Autoría Propia

En la figura 45 se visualizan las reglas creadas para permitir el tráfico HTTP y FTP desde la zona Verde hacia la zona Naranja. Se observa que ambas reglas están activas y priorizadas en la lista del firewall. Además, se muestra el botón para aplicar los cambios realizados, lo cual es fundamental para que las reglas entren en efecto dentro del sistema.

A continuación, se configura la comunicación desde la zona Internet hacia la zona DMZ. Esta acción permite que los usuarios externos puedan acceder a los servicios publicados en la DMZ, como servidores web o FTP. Para lograrlo, se deben crear las reglas necesarias en el firewall que autoricen el tráfico específico entre ambas zonas, definiendo los protocolos, puertos y políticas correspondientes.

Figura 46. Conexión HTTP zona Internet - DMZ



Fuente: Autoría Propia

Figura 47. Conexiones zona Internet – DMZ HTTP y FTP

Fuente: Autoría Propia

Después de configurar las redirecciones de puertos y permitir los servicios HTTP y FTP entre las distintas zonas, se procede a verificar que las reglas correspondientes se hayan creado correctamente en el apartado de Tráfico entre zonas del firewall.

Figura 48. Trafico Inter - Zona

Fuente: Autoría Propia

En la imagen se visualizan las reglas creadas, donde se permite explícitamente el tráfico entre las zonas VERDE, NARANJA y ROJA (Internet). Estas reglas incluyen la habilitación de HTTP y FTP desde la LAN (Verde) hacia la DMZ (Naranja), y desde la DMZ hacia la WAN, así como tráfico proveniente de la zona ROJA hacia la DMZ.

La verificación de las reglas es fundamental para confirmar que las configuraciones de acceso han sido implementadas correctamente y que la política de seguridad de red se está aplicando de acuerdo con los requisitos del entorno.

Una vez creadas las reglas necesarias en el firewall, se procede a comprobar su funcionamiento. Desde un navegador

web en un equipo dentro de la red LAN, se realizaron las siguientes pruebas:

Acceso HTTP desde LAN hacia DMZ: Se intentó acceder a un servicio web alojado en la zona DMZ. La conexión fue exitosa, lo que confirma que la regla creada para permitir el tráfico HTTP en el puerto 80 está funcionando correctamente.

Figura 49. HTTP desde LAN hacia DMZ

Fuente: Autoría Propia

Acceso HTTP desde LAN hacia Internet (WAN): Se accedió a un sitio web público (Google) para validar la salida HTTP desde la LAN hacia la WAN. El acceso también fue exitoso.

Figura 50. HTTP desde LAN hacia WAN

Fuente: Autoría Propia

2.5 IMPLEMENTACIÓN DE PROXY (NO TRANSPARENTE) CON POLITIXAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Un proxy HTTP no transparente es un intermediario entre los clientes y los servidores web que requieren una configuración manual en los navegadores. A diferencia de los proxys transparentes, este tipo permite implementar políticas de autenticación más estrictas y registrar el tráfico de manera individualizada.

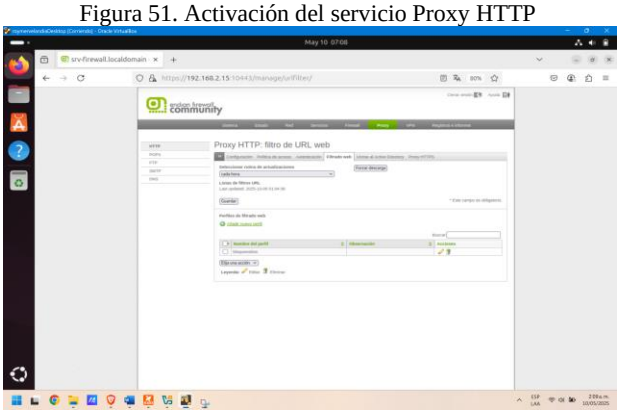
Endian Firewall es una solución de código abierto que integra herramientas como Squid, ClamAV y DansGuardian, facilitando la implementación de proxy, cortafuegos, antivirus perimetral y sistema de detección de intrusos. Su interfaz web simplifica la administración, aunque también permite el acceso mediante consola.

El entorno implementado en VirtualBox y se compone de:

- Un servidor Endian Firewall con tres interfaces de red virtual: RED (WAN), GREE (LAN) y ORANGE (DMZ).
- Una estación de trabajo Ubuntu Desktop en la red GREEN.
- Un servidor web en la red ORANGE simulando la DMZ.

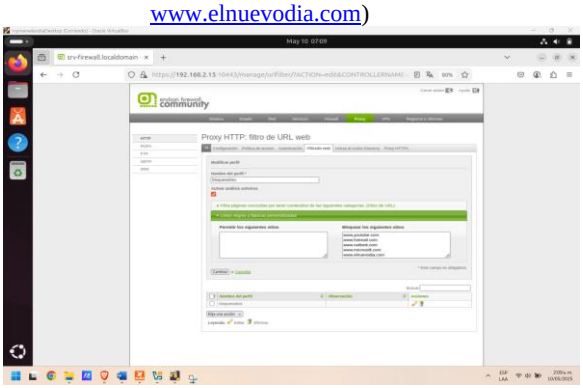
Pasos implementados partiendo de una instalación previa del Endian Firewall funcional, se procedió con la configuración del proxy HTTP no transparente.

Figura 51. Activación del servicio Proxy HTTP



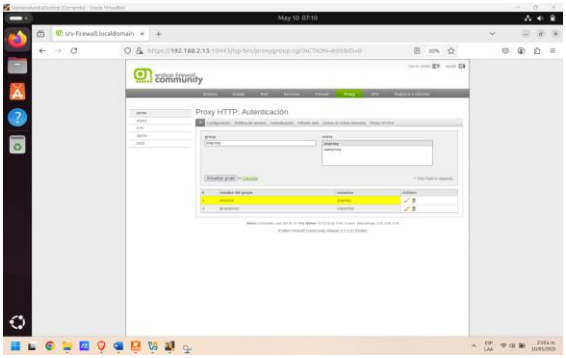
Fuente. Autoría Propia

Figura 52. Creación de lista negra bloqueando (www.hotmail.com, www.youtube.com y www.elnuevodia.com)



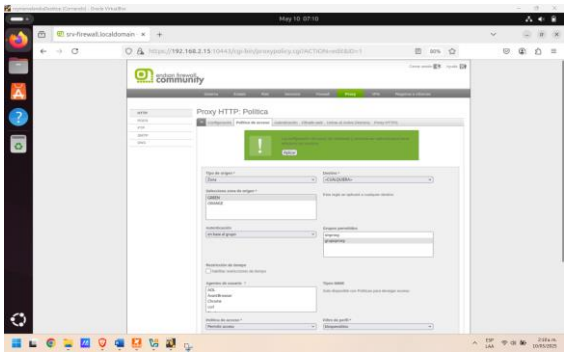
Fuente. Autoría Propia

Figura 53. Creación de usuarios y grupos para autenticación.



Fuente. Autoría Propia.

Figura 54. Asociación de una política de acceso al grupo definido.



Fuente. Autoría Propia.

Figura 55. Pruebas de navegación desde la estación de trabajo GREEN verificando bloqueo y autenticación.

Durante las pruebas, se comprobó que el proxy solicitaba autenticación antes de permitir la navegación. Al ingresar credenciales válidas, se permitió el acceso a sitios web no bloqueados y se restringió correctamente el acceso a los sitios de la lista negra. La configuración fue persistente tras reinicios del sistema y los registros mostraron la actividad por usuario, lo que permite una auditoría efectiva.

El uso de proxy no transparente con autenticación en Endian permite un control detallado del tráfico web, lo que mejora la seguridad y el cumplimiento de políticas organizacionales. Aunque la implementación en entornos virtualizados introduce ciertas limitaciones de rendimiento, representa un escenario válido para capacitación y pruebas. Futuras implementaciones podrían incluir integración con LDAP para una gestión centralizada de usuarios.

3. Conclusiones.

- Se elaboró el diagrama de red para las zonas verde, naranja y roja, lo que permitió definir el direccionamiento y la comunicación entre ellas. Posteriormente, se llevó a cabo la instalación del firewall Endian con la configuración inicial del direccionamiento, logrando establecer la conectividad y segmentación adecuada entre las zonas de la red.

- La correcta configuración de las interfaces de red en VirtualBox y la segmentación de zonas (verde, roja y naranja) en Endian permiten simular un entorno de red seguro y funcional, replicando escenarios reales de redes corporativas.

- La instalación efectiva de Endian y su integración con las máquinas virtuales proporciona una base sólida para aplicar políticas de seguridad perimetral y realizar prácticas de firewalling de manera controlada y educativa.

- La implementación de reglas NAT en Endian es esencial para permitir el acceso de dispositivos internos hacia redes externas, garantizando la comunicación controlada entre zonas sin comprometer la seguridad.

- La verificación exitosa del enrutamiento mediante NAT demuestra la capacidad de Endian para gestionar la traducción de direcciones IP de forma eficiente, permitiendo conectividad sin exponer directamente los recursos internos.

- La habilitación controlada de servicios como HTTP y FTP en la zona DMZ permite ofrecer servicios públicos desde una red aislada, minimizando los riesgos hacia la red interna.

- La restricción del protocolo ICMP refuerza la política de seguridad, evitando que dispositivos no autorizados realicen escaneos o diagnósticos de red, y demostrando la capacidad de Endian para aplicar reglas específicas por protocolo.

- La definición precisa de reglas de acceso entre zonas permite controlar el flujo de tráfico según las necesidades de cada segmento de red, asegurando la disponibilidad de servicios y la protección de recursos sensibles.

- Las pruebas funcionales desde navegadores y consolas confirman la efectividad de las políticas aplicadas, validando que el firewall cumple su función de filtrado entre zonas de manera precisa y confiable.

- La implementación de un proxy HTTP no transparente con políticas de autenticación mejora el control sobre la navegación web, permitiendo aplicar restricciones basadas en usuarios y grupos.

- El uso de listas negras y políticas de acceso personalizadas demuestra cómo Endian puede actuar como un filtro de contenido efectivo, alineado con las políticas internas de uso aceptable en entornos corporativos o educativos.

3 REFERENCIAS

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

[2] Debianian. (2023). *El manual del administrador de Debian 12.5.0*. Debian. https://www.debian.org/releases/stable/amd64/index.es.html.
[3] Endian. (2016). *Endian UTM 3.2 Manual referencia*. Endian. http://docs.endian.com/3.2/utm/index.html.
[4] La Croix, J. (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.
[5]*Oracle. (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/.*
[6] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/
[7] Jay 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