Arquitectura de Seguridad con Servicios en Endian Firewall

Javier Enrique Ángel Quevedo
e-mail: jeangelq@unadvirtual.edu.co
Cristian Camilo Bohórquez Molano
e-mail: ccbohorquezm@unadvirtual.edu.co
Brayan Alberto Acosta Rodríguez
e-mail: baacostar@unadvirtual.edu.co
Franklin Alberto Jiménez Latorre
e-mail: Fajimenezl@unadvirtual.edu.co
Carlos Mauricio Suarez Gutiérrez
e-mail: cmsuarezgut@unadvirtual.edu.co

RESUMEN: *Se detalla el proceso de fortalecimiento de la seguridad cibernética en un entorno simulado utilizando el firewall Endian Firewall sobre una arquitectura GNU/Linux. El trabajo se dividió en cinco temáticas siendo estas; la Configuración de la Instancia zonas con LAN, DMZ y WAN, la Configuración NAT que es la traducción de direcciones de red, la habilitación de Servicios en la DMZ por FTP/HTTP, la aplicación de Reglas de Acceso y la implementación de un Proxy HTTP no transparente. Las configuraciones se verificaron mediante consola y pruebas de conectividad, confirmando el aislamiento de las zonas internas, la traducción para el acceso a Internet y el filtrado granular de tráfico conforme al principio de mínimo privilegio. Los resultados validan la capacidad del sistema para segregar el tráfico y proteger los activos internos, cumpliendo con los estándares de seguridad requeridos para entornos de producción.*

PALABRAS CLAVE: DMZ, Endian Firewall, Red, NAT, Proxy.

1 INTRODUCCIÓN

La seguridad de la red es muy importante en la defensa de los activos organizacionales contra amenazas externas e internas, y la correcta implementación es prioridad en cualquier infraestructura de Tecnologías de la Información. Este artículo documenta el desarrollo práctico de un modelo de seguridad perimetral fuerte y segmentado, basado en la plataforma de firewall Endian, corriendo sobre un sistema operativo Linux. El proyecto aborda la necesidad de establecer políticas de tráfico granulares y defensivas que controlen el flujo de datos entre las zonas de confianza.

2 MARCO TEORICO

El proyecto se sustenta en principios de seguridad de redes y sistemas operativos de código abierto. La plataforma elegida, Endian Firewall, se basa en GNU/Linux y opera como un appliance unificado de gestión de amenazas UTM, utilizando el framework Netfilter del kernel para la manipulación de paquetes.

2.1 SEGMENTACIÓN Y ARQUITECTURA DE ZONAS

La segmentación de red es una estrategia de seguridad que divide la red en subredes aisladas. En este proyecto se utiliza el modelo de tres zonas:

- **Zona Verde (Green / LAN):** Red de confianza interna, con acceso irrestricto a todas las demás zonas.
- **Zona Naranja (Orange / DMZ):** Zona Desmilitarizada. Actúa como un *buffer* para servidores públicos (web, FTP) que deben ser accesibles desde la WAN, aislando al mismo tiempo la LAN de estos riesgos.
- **Zona Roja (Red / WAN):** La interfaz de riesgo, conectada a la red simulada de Internet, donde residen las amenazas externas.

2.2 Traducción de Direcciones de Red y Filtrado

La NAT es un mecanismo que permite a múltiples dispositivos en redes privadas compartir una única dirección IP pública WAN para comunicarse con Internet.

- **Source NAT:** La técnica traduce la IP de origen privada a la IP pública del firewall al salir a Internet. Esto garantiza la comunicación saliente de LAN y DMZ.
- **Destination NAT:** Utilizado para permitir que el tráfico de la WAN que llega a un puerto específico del firewall sea redirigido a un servidor específico dentro de la DMZ.

El filtrado de paquetes se gestiona mediante reglas a través de la capa de gestión de Endian, aplicando el Principio de Menor Privilegio, que dicta que solo el tráfico explícitamente permitido debe pasar entre las zonas.

2.3 Proxy a Nivel de Aplicación

A diferencia del firewall de paquetes que opera en Capas 3 y 4, el Proxy HTTP No Transparente opera a nivel de aplicación en Capa 7. Esto permite:

- **Inspección Profunda:** Analizar el contenido real de la petición HTTP y no solo la cabecera del paquete.

- **Listas de Control:** Aplicar políticas detalladas, como listas negras y la autenticación obligatoria de usuarios, independientemente de la dirección IP de origen.

3 METODOLOGÍA

La metodología implementada siguió un enfoque de diseño, configuración, y verificación en modo consola, garantizando que cada política de seguridad fuera funcional y trazable. El entorno se construyó sobre máquinas virtuales que simulan la topología de red de un firewall perimetral y sus zonas de influencia.

3.1 Temática 1: Configuración de Linux Endian en VirtualBox

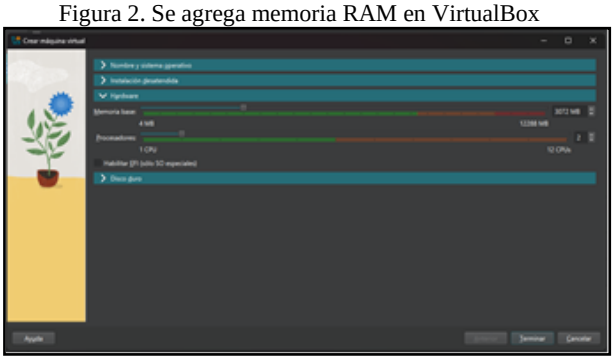
Se instala e implementa Endian, por tal motivo se accede a este enlace para su descarga: https://www.endian.com/en/community/. En VirtualBox se añade una nueva máquina virtual, la cual se le asigna un nombre, un sistema operativo y una versión como se observa en la figura 1.

Figura 1. Asignación en VirtualBox

Fuente: Autoría Propia

Luego, se procede a agregar la memoria base y la cantidad de procesadores, para este caso se usa 3072MB de memoria y 2 procesadores como se observa en la figura 2.

Figura 2. Se agrega memoria RAM en VirtualBox



Fuente: Autoría Propia

Para avanzar se realiza la asignación del archivo .iso que se descargó con anterioridad, esto se logra añadiendo ese archivo como un dispositivo secundario en la unidad óptica como se observa en la figura 3.

Figura 3. Asignación unidad óptica

Fuente: Autoría Propia

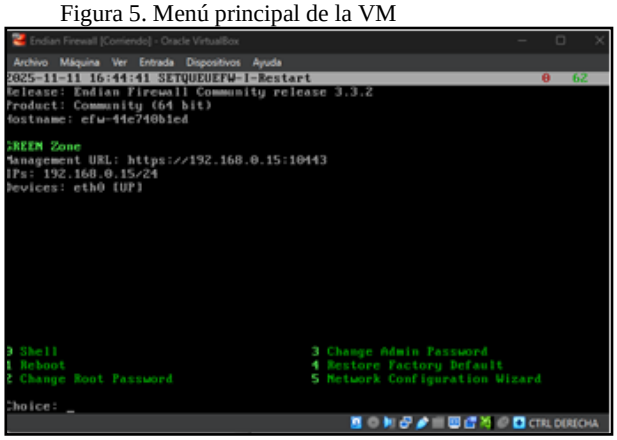
Uno de los pasos importante durante el inicio de la máquina virtual es la asignación de la IP de esta como se observa en la figura 4.

Figura 4. Asignación de IP de la máquina virtual

Fuente: Autoría Propia

Una vez instalado y configurado el entorno virtual se observa que se puede configurar por medio del siguiente menú como se observa en la figura 5.

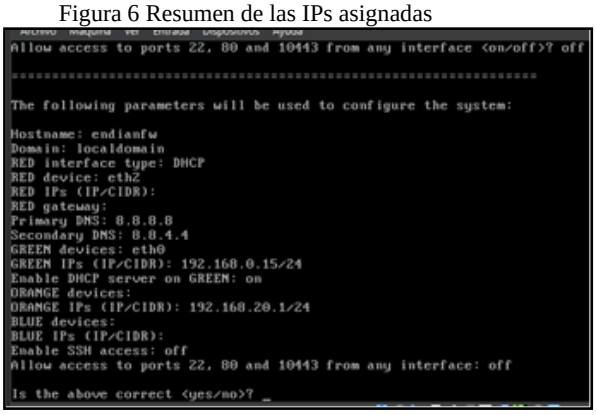
Figura 5. Menú principal de la VM



Fuente: Autoría Propia

Con la ayuda de la opción 5 se puede configurar las 3 redes solicitadas, en las cuales se puede asignar direcciones Ip, cuando este proceso finaliza se puede observar un resumen de lo realizado como se observa en la figura 6.

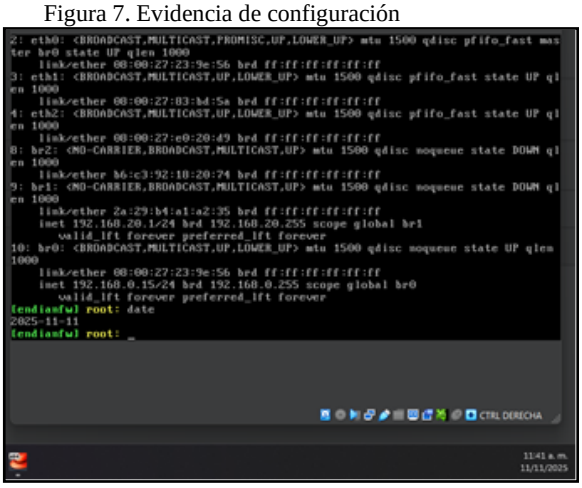
Figura 6 Resumen de las IPs asignadas



Fuente: Autoría Propia

Esto confirma que todo está configurado de manera correcta, por lo que se puede evidenciar que todo es correcto cuando en el Shell se ejecutar el comando ip addr que permite ver las ip asignadas como se observa en la figura 7.

Figura 7. Evidencia de configuración

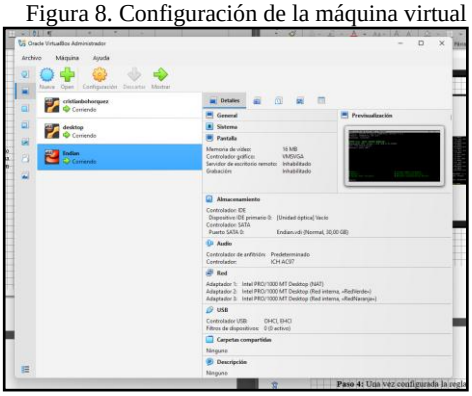


Fuente: Autoría Propia

3.2 Temática 2: Configuración NAT

Se configura la máquina virtual donde estará alojado Endian, se crean las redes internas Verde y Naranja y se asigna la correspondiente al desktop y al servidor como se observa en la figura 8.

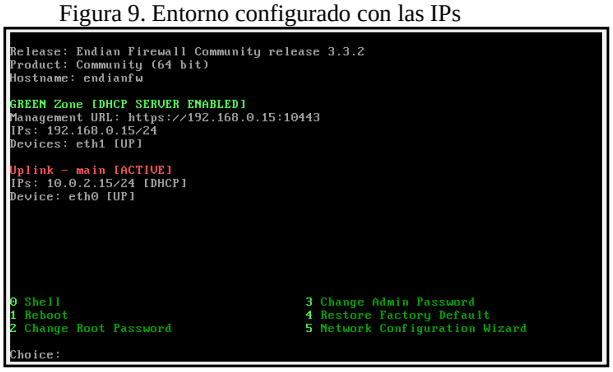
Figura 8. Configuración de la máquina virtual



Fuente: Autoría Propia

Se instala Endian Linux y se asignan las IPs de la temática 1, con ello se asigna los adaptadores de red y se genera conexión al desktop y al servidor como se observa en la figura 9.

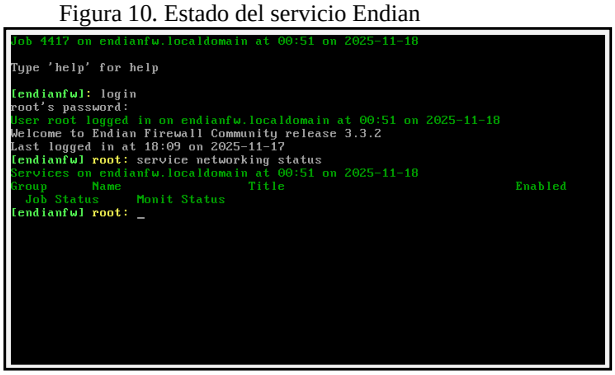
Figura 9. Entorno configurado con las IPs



Fuente: Autoría Propia

En la consola de comandos se va a ver el estatus del servicio como se observa en la figura 10.

Figura 10. Estado del servicio Endian



Fuente: Autoría Propia

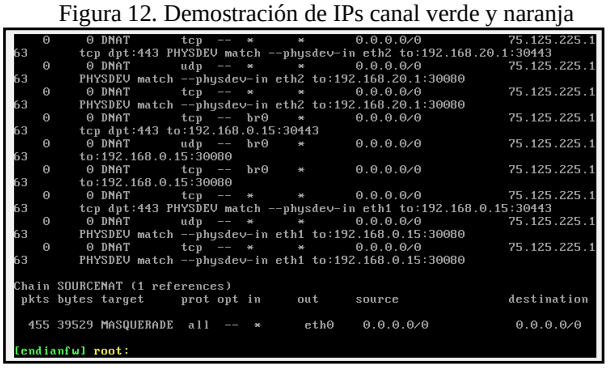
Inicio de la configuración de la regla de NAT - Traducción de Direcciones de Red mediante la interfaz gráfica del Cliente como se observa en la figura 11.

Figura 11. Interfaz gráfica de la regla NAT

Fuente: Autoría Propia

Demostración del establecimiento de la comunicación desde la LAN hacia la WAN - Red simulada de Internet como se observa en la figura 12.

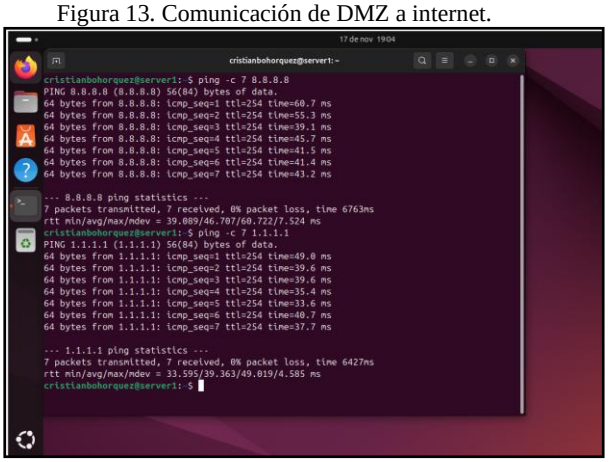
Figura 12. Demostración de IPs canal verde y naranja



Fuente: Autoría Propia

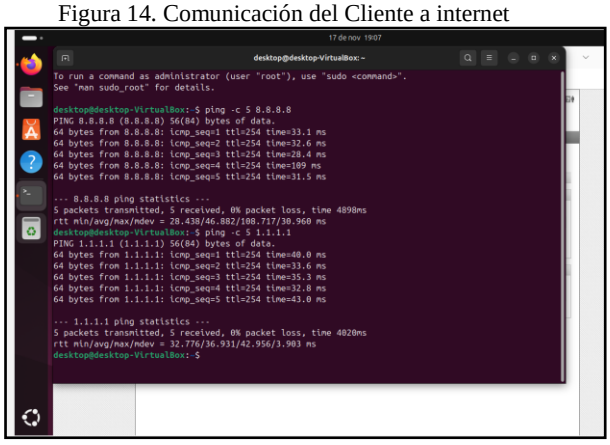
Una vez configurada la regla y demostrado el establecimiento de la comunicación desde la LAN hacia la WAN, se demostrará el establecimiento de la comunicación de la Zona DMZ y cliente hacia la Internet como se observa en las figuras 13 y 14 respectivamente.

Figura 13. Comunicación de DMZ a internet.



Fuente: Autoría Propia

Figura 14. Comunicación del Cliente a internet

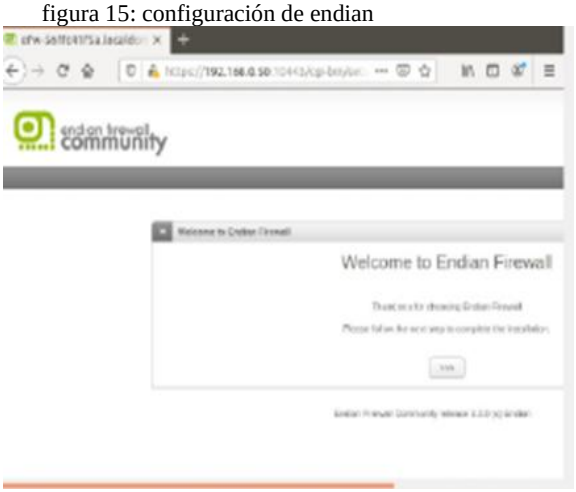


Fuente: Autoría Propia

3.3 Temática 3: Permitir servicios de la Zona DMZ para la red.

El usuario abrió su navegador web y accedió a la interfaz de administración del Endian Firewall mediante la dirección IP segura https://192.168.0.50:10443. Allí visualizó la ventana de bienvenida que confirmaba la conexión correcta. Luego seleccionó OK para iniciar el asistente y avanzar con la configuración del firewall.

figura 15: configuración de endian



Fuente: autoría propia

A continuación, ingresó al Asistente de configuración de red del Endian Firewall. Seleccionó el modo de red “Enrutamiento”, ya que este permite proteger la red interna (GREEN) y habilitar servicios a través de la DMZ (ORANGE). Como tipo de enlace eligió “Ethernet por DHCP” para obtener la configuración de red de forma automática. Posteriormente, presionó Siguiente.

figura 16 configuración de la zona roja

Fuente: autoría propia

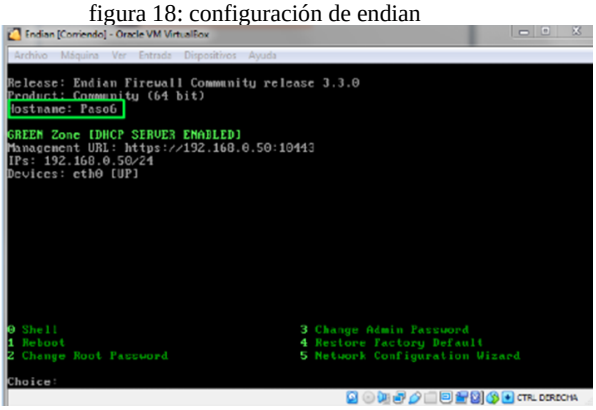
Posteriormente, configuró la interfaz VERDE (RED local). Activó el servicio DHCP para que el firewall asignara direcciones IP automáticamente a los equipos internos. Verificó que la IP de la interfaz fuera 192.168.0.50 con máscara /24 (255.255.255.0). También confirmó que la interfaz ena1 estuviera clasificada como GREEN y continuó con el asistente.

figura 17: configuración de la zona verde

Fuente: autoría propia

Después del reinicio y la configuración inicial, revisó la consola de Endian Firewall. Allí confirmó que la instalación de la versión 3.3.0 concluyó sin inconvenientes y verificó el nombre de host asignado, Fase6. Observó que la zona GREEN se encontraba activa con DHCP, que la IP seguía siendo 192.168.0.50/24 y que la URL de administración permanecía disponible. En este punto, podría modificar las contraseñas si fuera necesario.

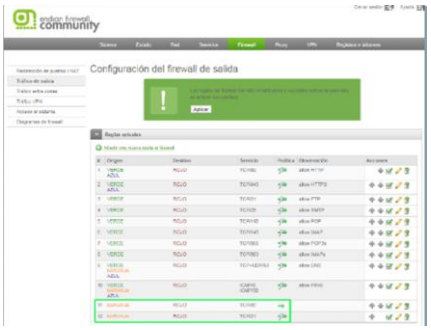
figura 18: configuración de endian



Fuente: autoría propia

Luego ingresó a la sección de configuración del firewall de salida para revisar las reglas predeterminadas. Confirmó que las redes GREEN y RED tenían permitido el tráfico a Internet para servicios comunes como HTTP (80) y HTTPS (443). También verificó la lista de reglas para asegurarse de que el tráfico saliente estuviera correctamente definido antes de crear las reglas internas.

figura 19: permisos de http con puerto 80 y FTP con puerto 21



fuente. autoría propia

Posteriormente accedió a la configuración de las reglas inter-zona y creó una nueva regla de tráfico. Como origen estableció la zona VERDE (Red Local) y como destino la zona NARANJA (DMZ). Seleccionó el servicio ICMP (Ping) y definió la política como DROP (denegada), tal como se requería en el producto esperado de la práctica.

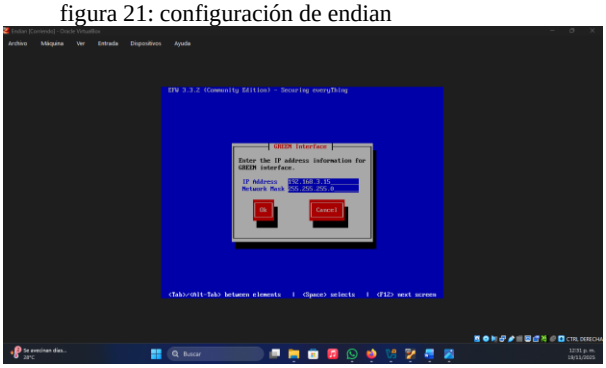
figura 20: bloqueo de protocolo ICMP PARA TIPO 8 Y 30

Fuente: autoría propia

3.4 Temática 4: Reglas de acceso para permitir o denegar el tráfico.

Para iniciar la configuración, se establece la interfaz GREEN dentro de la red local asignándole una dirección IP estática y su respectiva máscara de subred. Esta dirección actuará como la puerta de enlace interna. Dado que la zona GREEN representa el segmento más confiable de la red, su correcta parametrización es fundamental para que Endian pueda gestionar adecuadamente el enrutamiento hacia la DMZ (zona Naranja) y hacia la red externa (zona Roja).

figura 21: configuración de endian



Fuente: autoría propia

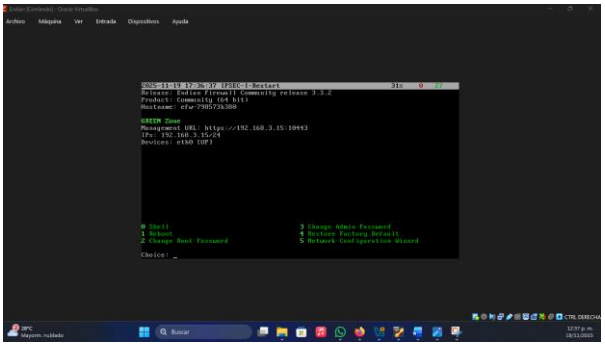
Después de completar la instalación del EFW (Endian Firewall), se retira el medio utilizado para la instalación. A partir de ese momento, la configuración inicial se continúa desde otro equipo mediante la interfaz web. Para acceder a ella, se ingresa a través de un navegador a las direcciones: http://192.168.3.15o https://192.168.3.15:10443

figura 22 Instalación EFW Completada Acceso Web

Fuente: autoría propia

La consola del sistema muestra el menú principal de Endian Firewall, indicando que el servicio ya está en funcionamiento. En esta interfaz se presenta también la URL para acceder a la WebGUI (https://192.168.3.15:10443) y se ofrecen opciones para reiniciar el dispositivo, apagarlo, modificar contraseñas o iniciar el asistente de configuración de red.

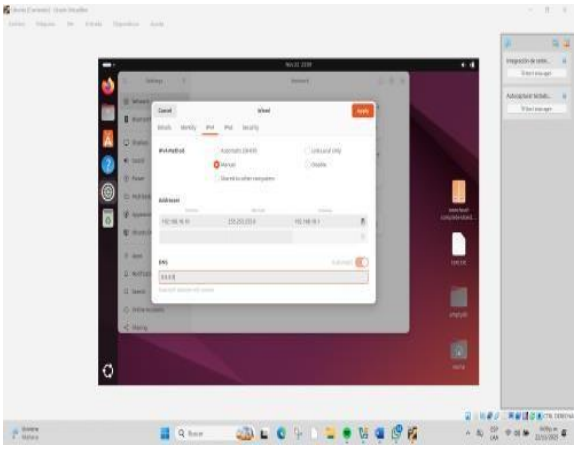
figura 23: Menú Principal Endian Firewall Consola



Fuente: autoría propia

En el sistema Ubuntu se realizó la configuración manual de red, asignando una IP estática, la máscara de subred correspondiente, la puerta de enlace y el servidor DNS (8.8.8.8). Esto garantiza que el equipo mantenga una dirección fija para su comunicación.

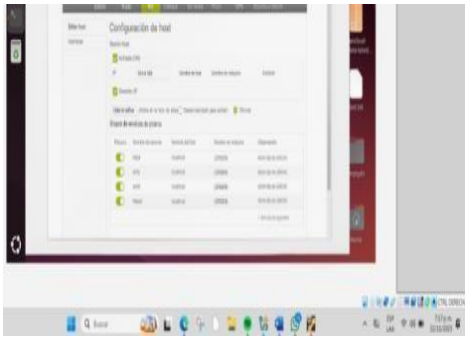
figura 24: Configuración IP estática en Ubuntu.



Fuente: autoría propia

Posteriormente, se accedió al apartado de Configuración del Host, donde se observan los perfiles de red y las interfaces disponibles, incluyendo las zonas GREEN y ORANGE. Esta sección permite verificar que cada zona esté correctamente asociada a su respectiva interfaz física o virtual.

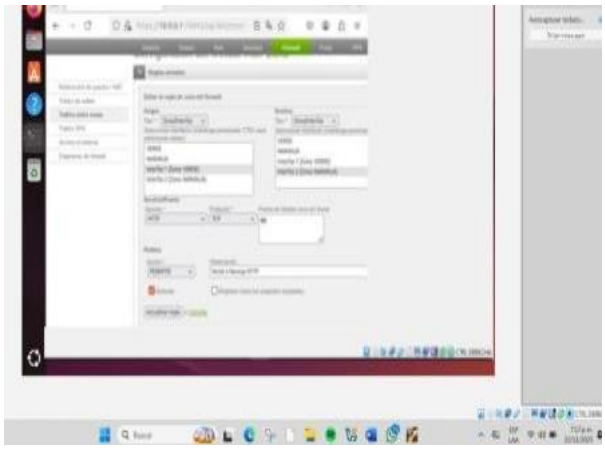
figura 25: Gestión y perfiles de red Host.



Fuente: autoría propia

En el cortafuegos se creó una regla de reenvío de puertos, definiendo el origen del tráfico, el destino dentro de la zona GREEN, el protocolo (por ejemplo, TCP) y el puerto correspondiente. El propósito es redirigir el tráfico externo hacia un servidor localizado en la red interna.

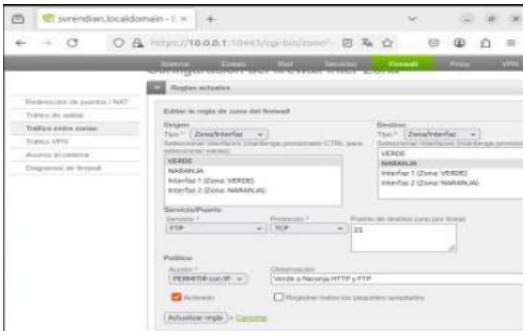
figura 26: Creación regla reenvío de puertos.



Fuente: autoría propia

También se configuró una regla específica de comunicación entre zonas, autorizando el servicio FTP (puerto 21 TCP) desde la zona Verde (confiable) hacia la zona Naranja (DMZ). Esta configuración habilita la transferencia de archivos entre ambas zonas.

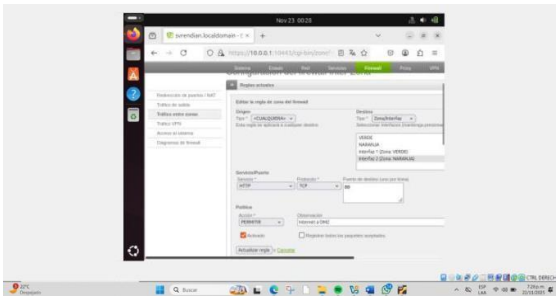
figura 27: Regla de tráfico VERDE a NARANJA.



Fuente: autoría propia

Otra regla añadida fue “Internet a DMZ”, destinada al tráfico entre zonas. Esta política permite el acceso mediante HTTP (puerto 80 TCP) desde la zona Roja (Internet/WAN) hacia la zona Naranja (DMZ), garantizando que los usuarios externos puedan acceder al servidor ubicado en dicha zona.

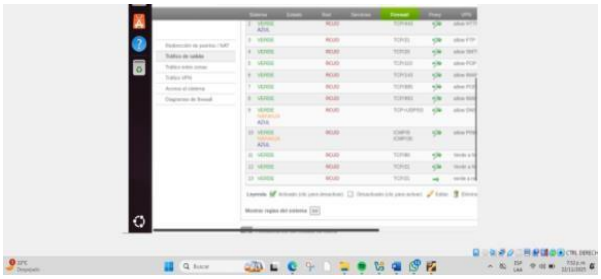
figura 28: Regla de acceso RED a DMZ.



Fuente: autoría propia

Desde la sección Seguridad > Firewall > Registros, se revisó la actividad generada por el tráfico saliente. Esta vista proporciona información detallada sobre la comunicación entre zonas, facilitando la supervisión y control de los flujos de datos.

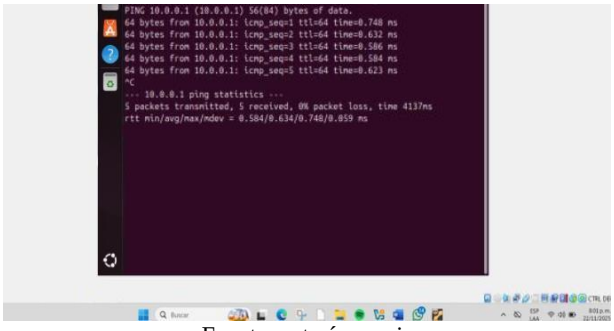
figura 29: Registros del tráfico entre zonas.



Fuente: autoría propia

Para verificar la conectividad, se ejecutó un comando PING hacia la dirección 10.0.0.1. La prueba confirmó la comunicación con el host al recibir la totalidad de los paquetes enviados, sin registrar pérdida alguna.

figura 30: Prueba de conectividad PING exitosa.

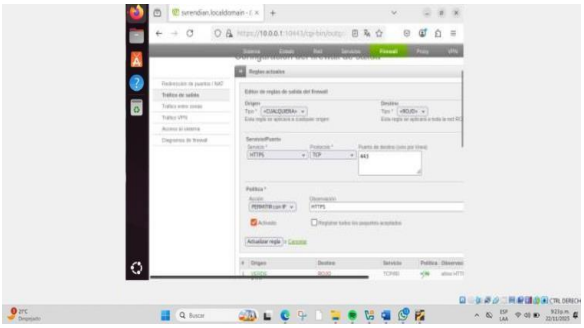


Fuente: autoría propia

Finalmente, se editó una regla de tráfico saliente (Outbound Traffic) para permitir el uso del servicio HTTPS (puerto 443 TCP) desde la zona Verde hacia la zona Roja. Con

ello, los usuarios internos pueden acceder de manera segura y cifrada a los servicios externos.

figura 31: Regla de salida HTTPS a RED.



Fuente: autoría propia

3.5 Temática 5: Implementar un Proxy HTTP No transparente con políticas de autenticación para navegación en Internet.

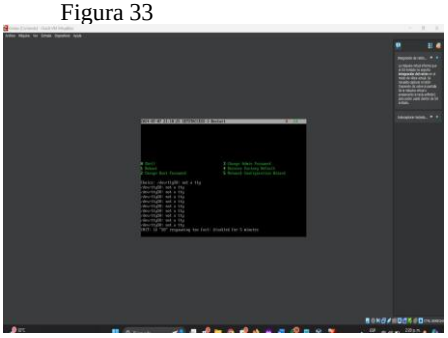
En esta figura se observa el instalador inicial de Endian. La interfaz muestra las primeras opciones de configuración, entre ellas la selección del idioma en el que se desarrollará la instalación. Esta pantalla es fundamental, pues garantiza que el usuario pueda comprender cada paso durante la preparación del sistema.

Figura 32

Fuente: autoría propia

Finalizada la instalación, Endian presenta su interfaz principal. En esta imagen se aprecia la vista inicial del sistema, desde la cual es posible acceder posteriormente a la consola web mediante la dirección IP asignada durante la instalación.

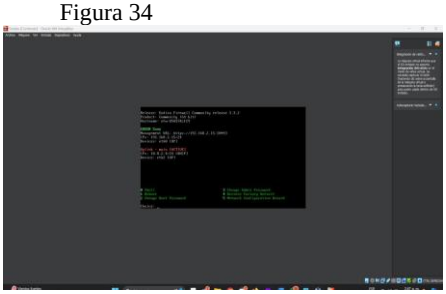
Figura 33



Fuente: autoría propia

Aquí se evidencia el reconocimiento automático que realiza Endian cuando el servidor inicia. En la imagen se distinguen claramente la red verde y la red roja, cada una con su rol específico dentro del esquema de seguridad del firewall.

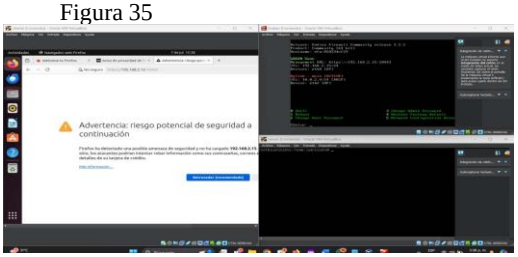
Figura 34



Fuente: autoría propia

La captura muestra el ingreso desde el cliente hacia la interfaz web de Endian mediante la IP configurada. También aparece el mensaje de advertencia generado por el navegador, indicando posibles riesgos de seguridad debido al uso de certificados autofirmados.

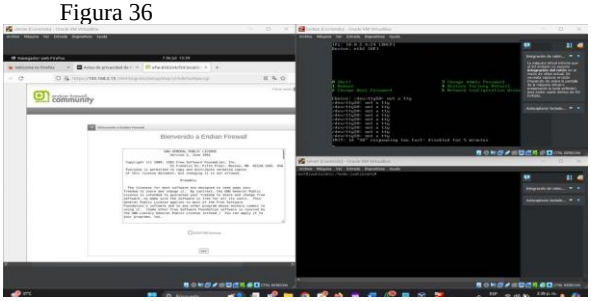
Figura 35



Fuente: autoría propia

Se presenta la ventana donde se deben aceptar los términos y condiciones de uso. Este paso es imprescindible para continuar con la administración del sistema desde su interfaz web.

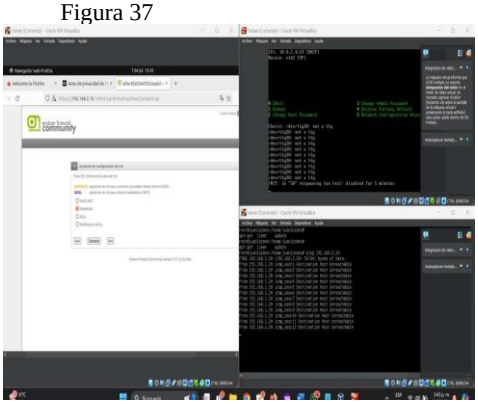
Figura 36



Fuente: autoría propia

En esta figura se observa el proceso de configuración de la red naranja, una red utilizada generalmente para dispositivos ubicados en zonas semiprotegidas o DMZ. La interfaz permite introducir los parámetros necesarios para su funcionamiento.

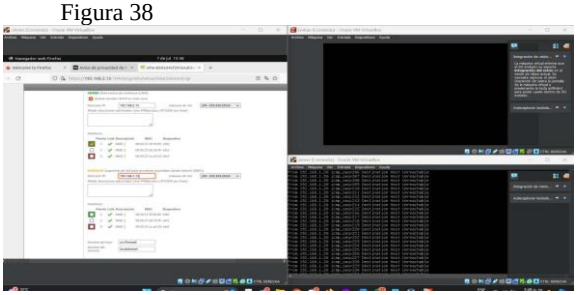
Figura 37



Fuente: autoría propia

Aquí se muestra la introducción de la dirección IP correspondiente a la red naranja, junto con la dirección hacia donde se dirigirán los paquetes. Esta configuración es clave para habilitar la segmentación correcta del tráfico.

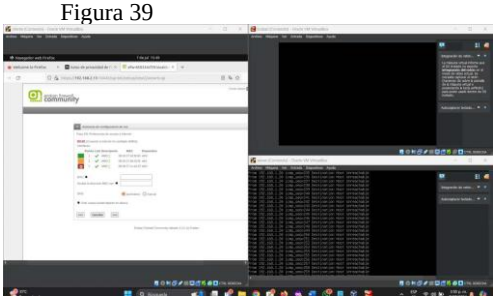
Figura 38



Fuente: autoría propia

La imagen confirma la correcta configuración de las tres redes: verde, roja y naranja. Esta estructura multilayer permite que el firewall cumpla adecuadamente su función de seguridad y filtrado.

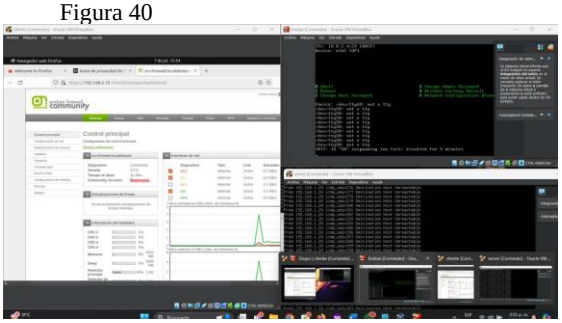
Figura 39



Fuente: autoría propia

Se observa la interfaz web de Endian ya operativa. Dentro de esta vista se encuentran múltiples menús que permiten ajustar parámetros del sistema, realizar configuraciones de red, políticas de filtrado, certificados, usuarios y más.

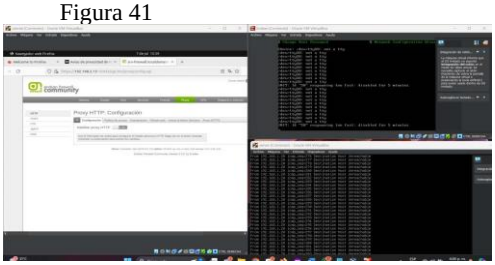
Figura 40



Fuente: autoría propia

La figura muestra la pestaña Proxy, desde donde se accede a las distintas configuraciones relacionadas con el servicio de intermediación de tráfico HTTP.

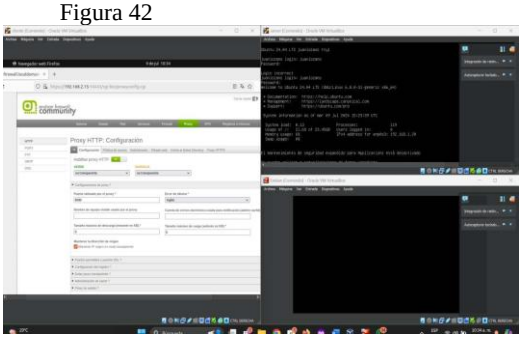
Figura 41



Fuente: autoría propia

En la configuración del Proxy HTTP, se selecciona la modalidad no transparente, que exige que los navegadores sean configurados manualmente para usar el proxy. Esta opción es ideal para escenarios donde se necesita control de autenticación.

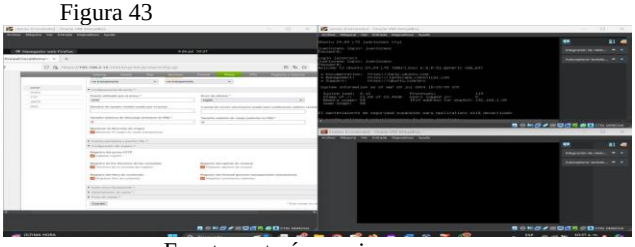
Figura 42



Fuente: autoría propia

Aquí se observa la sección que permite modificar parámetros como el puerto del proxy, el registro de actividad y otros ajustes esenciales. Esta configuración garantiza que el sistema lleve logs y supervise de forma constante el tráfico.

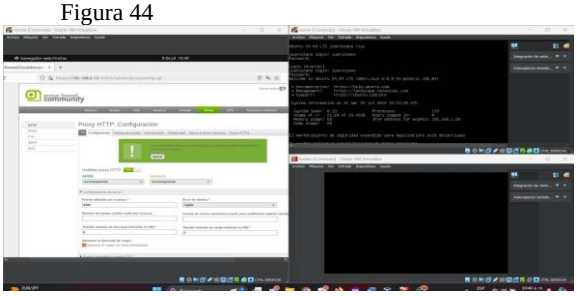
Figura 43



Fuente: autoría propia

La figura evidencia el guardado y aplicación de los cambios. Cada modificación requiere confirmación para activarse en el sistema.

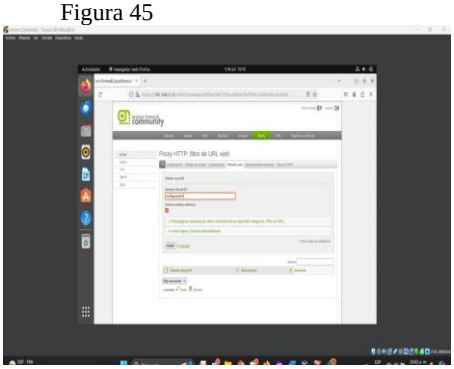
Figura 44



Fuente: autoría propia

Desde la pestaña Filtrado web, se inicia la creación de una nueva política. En la imagen se aprecia el formulario donde se definen las características de dicha política.

Figura 45



Fuente: autoría propia

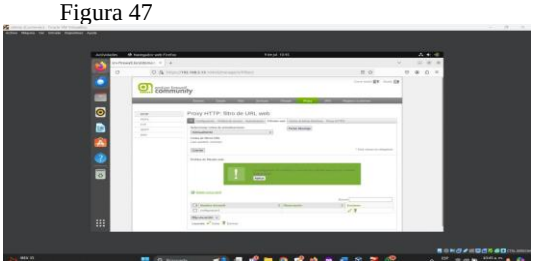
La captura muestra la selección de categorías de contenido que pueden bloquearse. Alternativamente, se accede a las listas blanca y negra para añadir manualmente las URL que se desean restringir. En este caso se agregan los sitios mencionados en la guía.

Figura 46

Fuente: autoría propia

Luego de ingresar las direcciones, se guardan y aplican los cambios. Este paso garantiza que la política quede registrada dentro del sistema.

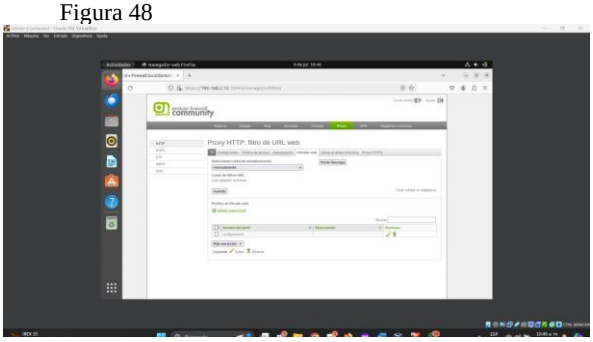
Figura 47



Fuente: autoría propia

Se visualiza la nueva política creada, la cual se encuentra lista para ser vinculada a la política de acceso y a la autenticación de usuarios.

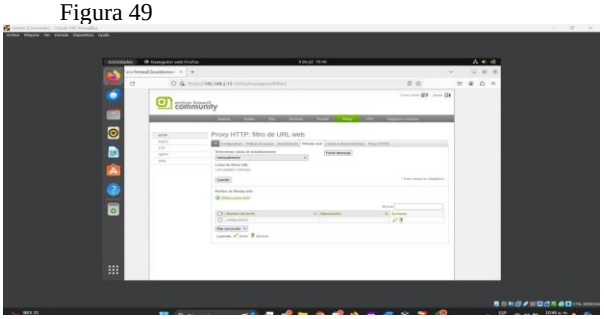
Figura 48



Fuente: autoría propia

Desde la pestaña Política de acceso, se procede a editar o generar una nueva política que determine cómo los usuarios interactuarán con el proxy y las restricciones aplicadas.

Figura 49



Fuente: autoría propia

Dado que el tráfico hacia muchos sitios se realiza mediante HTTPS, se requiere generar un certificado e instalarlo en el navegador del cliente. La figura refleja la ruta de ajustes necesaria para cargar dicho certificado.

Figura 50

Fuente: autoría propia

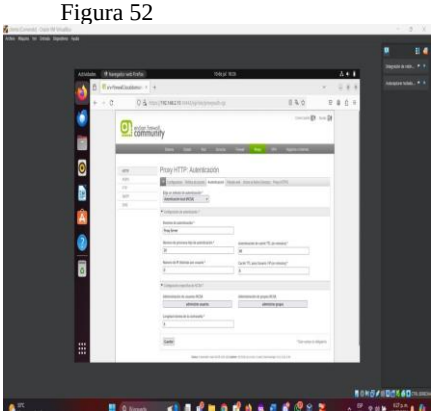
En esta imagen se aprecia el certificado previamente descargado y listo para ser importado al navegador. Esto permite que el proxy pueda inspeccionar tráfico cifrado sin generar alertas constantes.

Figura 51

Fuente: autoría propia

La figura muestra la pestaña de Autenticación, desde la cual se gestionan usuarios y grupos para el control de acceso.

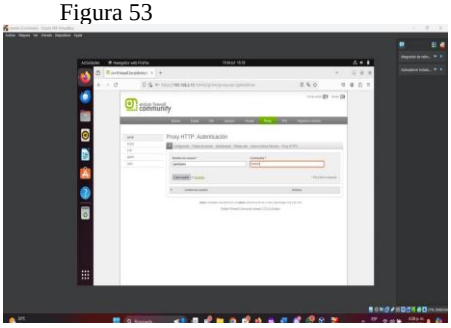
Figura 52



Fuente: autoría propia

Aquí se presenta el proceso de creación de un nuevo usuario, quien posteriormente será asociado a la política creada y al proxy.

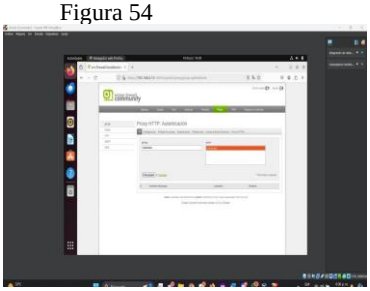
Figura 53



Fuente: autoría propia

Tras crear el usuario, se genera un grupo y se vincula dicho usuario al mismo. Este paso es importante para estructurar permisos y políticas más organizadas.

Figura 54



Fuente: autoría propia

Finalmente, se evidencia el intento de acceso a una de las páginas bloqueadas. El sistema muestra el mensaje de acceso restringido, confirmando que la política y las listas negras funcionan correctamente.

Figura 55

Fuente: autoría propia

4 ANALISIS DE RESULTADOS

La segmentación demostró un funcionamiento estable al verificar que las interfaces estaban correctamente distribuidas entre GREEN, ORANGE y RED. La implementación de NAT permitió comunicación eficiente sin exponer direcciones internas. La DMZ logró publicar servicios sin comprometer LAN, confirmando su eficacia como zona intermedia. Las reglas de acceso cumplieron con el principio de mínimo privilegio y garantizaron un flujo controlado. Finalmente, el proxy demostró capacidad para inspeccionar tráfico y aplicar políticas de autenticación.

5 CONCLUSIONES

La preparación del entorno virtual evidenció que una correcta instalación y parametrización inicial de Endian en VirtualBox es la base para cualquier arquitectura de seguridad funcional. La asignación adecuada de recursos, la definición precisa de las interfaces y la verificación mediante consola permitieron asegurar que el sistema contara con una configuración estable y coherente para las etapas posteriores, garantizando la disponibilidad de las zonas LAN, DMZ y WAN necesarias para el modelo perimetral.

La implementación de NAT demostró ser fundamental para habilitar la comunicación controlada entre las máquinas internas y la red externa. La validación del tráfico desde la LAN y la DMZ hacia la WAN confirmó que la traducción de direcciones opera de manera eficiente, permitiendo el acceso a servicios externos sin comprometer la estructura interna. Este mecanismo constituye un pilar clave para preservar la privacidad de los equipos locales y mantener un flujo seguro hacia Internet.

Se completó la configuración inicial y el ajuste de las reglas del Endian Firewall para cumplir con la Temática 3. El proceso comenzó con el asistente de configuración, donde se definió el modo de enrutamiento y la red GREEN. Posteriormente, se revisó la configuración del firewall de salida. Finalmente, la acción crucial fue crear una regla de tráfico para denegar el protocolo ICMP (ping) desde la red VERDE hacia la DMZ (NARANJA), asegurando el cumplimiento de la política de seguridad requerida en la práctica.

La definición de reglas de acceso entre zonas permitió establecer un control detallado sobre el flujo de información. El uso de políticas basadas en protocolos, puertos y direcciones reforzó el principio de mínimo privilegio, asegurando que solo el tráfico autorizado pudiera transitar entre LAN, DMZ y WAN. La verificación mediante registros y pruebas de conectividad confirma que un filtrado bien estructurado constituye la defensa más efectiva contra accesos no deseados y eventos de riesgo.

6 RECOMENDACIONES

Implementar monitoreo constante de tráfico y registros. La revisión periódica de los logs del firewall y del comportamiento de las interfaces es esencial para detectar patrones anómalos, intentos de acceso no autorizado o fallas de servicio. Integrar herramientas de monitoreo adicionales puede mejorar la capacidad de respuesta ante incidentes.

Realizar pruebas de penetración internas y externas. Una vez configuradas las zonas LAN, DMZ y WAN, es importante ejecutar pruebas controladas que evalúen la solidez de las reglas de acceso y la robustez de los servicios desplegados. Esto ayuda a validar que la segmentación realmente mitigue ataques y que los servicios públicos no expongan recursos sensibles.

Optimizar el uso del Proxy HTTP con políticas más restrictivas. Para fortalecer el control de navegación, se recomienda ampliar las listas de filtrado, habilitar autenticación obligatoria y aplicar supervisión de contenido en el proxy. Este enfoque permite asegurar un acceso a Internet más controlado y reduce riesgos por descargas no seguras o sitios maliciosos.

Actualizar periódicamente el sistema y los servicios. Mantener Endian Firewall y las máquinas que interactúan con él actualizadas es clave para evitar vulnerabilidades conocidas. Las actualizaciones corrigen fallos críticos y mejoran el rendimiento general del entorno.

Capacitar al personal encargado del mantenimiento. La administración de un firewall perimetral requiere conocimientos técnicos sólidos. Por ello, se recomienda que los responsables del sistema reciban formación continua sobre gestión de redes, seguridad, análisis de logs y mejores prácticas de administración.

Implementar copias de seguridad de la configuración. Realizar backups frecuentes de las reglas, perfiles de red y ajustes del sistema permite recuperar rápidamente la operación ante fallos inesperados, pérdidas de configuración o cambios erróneos durante pruebas.

7 REFERENCIAS

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

[2] 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.

[3] Cervelión, Á. J. (2023). Instalación de Nagios Core 4.4 en Ubuntu 22.04. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230.

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

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

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

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

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

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

[10] Essentials., L. L. (2022). Tema 1: La Comunidad Linux y una . https://learning.lpi.org/es/learning-materials/010-160/1/.