OPTIMIZACIÓN DE LA SEGURIDAD EN GNU/LINUX A TRAVÉS DE LA CONFIGURACIÓN ADMINISTRATIVA DE INTERFACES GRÁFICAS Y SERVICIOS DEL SISTEMA

Anyi Katerine Ipuz Lopez
e-mail: akipuzl@unadvirtual.edu.co
Jonathan Orlando Bolívar Santana
e-mail: jobolivars@unadvirtual.edu.co
Jorge Andrés Castiblanco Lozano
e-mail: jacastiblancol@unadvirtual.edu.co
Julián Steven Cifuentes Llanos
e-mail: jscifuentesll@unadvirtual.edu.co
Karen Yulieth González Garzón
e-mail: kygonzalezga@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la instalación y configuración de la distribución GNU/Linux Endian Firewall Community 3.3.2 en un entorno virtualizado mediante VirtualBox. Se detallan las etapas necesarias para establecer una red segura segmentada en tres zonas: VERDE (LAN), ROJA (WAN) y NARANJA (DMZ), simulando un entorno corporativo básico. La implementación incluyó la conexión y comunicación con un cliente en la red, así como con distintos servicios distribuidos en la misma. El objetivo principal fue fortalecer la seguridad perimetral y comprender la segmentación de redes en un entorno simulado, destacando la importancia de la seguridad de redes como pilar fundamental en infraestructuras modernas.*

PALABRAS CLAVE: Endian, Firewall, GNU/Linux, VirtualBox.

1 INTRODUCCIÓN

La seguridad en sistemas GNU/Linux es esencial para proteger las redes y los servicios frente a amenazas crecientes. Este artículo presenta la implementación y configuración de Endian Firewall Community en un entorno virtualizado con VirtualBox, como solución para optimizar la seguridad mediante la administración de interfaces gráficas y servicios del sistema. La infraestructura ha sido pensada para segmentación en tres zonas (Verde, Naranja y Roja), permitiendo un control granular del tráfico mediante reglas de acceso, NAT, y servicios como HTTP, FTP e ICMP. Además, se configura un proxy HTTP no transparente con autenticación, orientado al control de navegación y al uso eficiente del ancho de banda. La propuesta se fundamenta en herramientas de código abierto y prácticas educativas, simulando entornos reales para validar el fortalecimiento del perímetro de seguridad y la gestión administrativa en sistemas GNU/Linux.

2 PRERREQUSITOS

2.1 PREPARACIÓN ENTORNO VIRTUAL

Se utilizó VirtualBox como hipervisor para simular una red compuesta por un firewall (Endian) y una estación de trabajo cliente (Ubuntu). Se descargó la imagen ISO de Endian Firewall Community 3.3.2 desde el sitio oficial y se creó una máquina virtual con las siguientes características.

- Memoria RAM: 1024 MB
- Disco Duro: 10 GB (asignación dinámica)
- Arquitectura de S.O. Linux 64-bits

2.2 CONFIGURACIÓN DE INTERFACES

Se debe activar tres adaptadores de red en la VM de Endian.

- **Adaptador 1:** Red interna llamada “Redlan” para la zona VERDE (LAN).
- **Adaptador 2:** Adaptador en modo puente, correspondiente a la zona ROJA (acceso a internet).
- **Adaptador 3:** Red interna separada, nombrada “DMZ”, para la zona NARANJA (servidores).

Estas interfaces se asignaron de la siguiente manera:

- **eth0:** Zona VERDE, IP estática 192.168.0.1/24
- **eth1:** Zona ROJA, configurada por DHCP
- **eth2:** Zona NARANJA, IP estática 192.168.10.1/24

2.3 INSTALACIÓN Y CONFIGURACIÓN DE ENDIAN

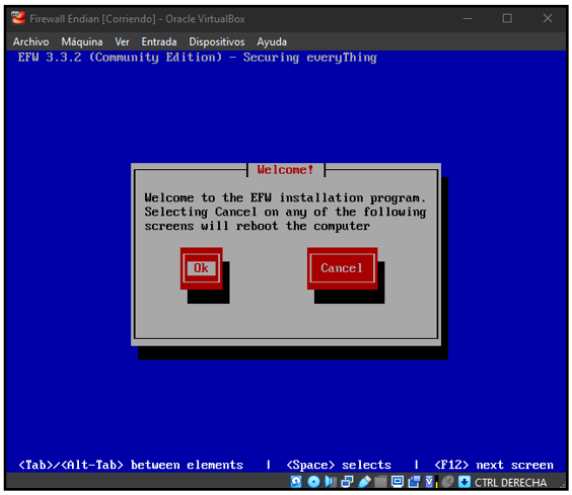
Endian, tal como refiere la documentación oficial , es un S.O. basado en IPCop (otra distribución de Linux), enfocado en hacer las funciones de un cortafuegos o firewall empleando muy poco recurso de hardware y optimizando las funciones a

lo netamente necesario para la configuración e interacción transaccional de redes (Endian, 2016) [1].

Una vez iniciada la VM con la ISO montada, se siguió el instalador en modo texto. Se estableció el nombre del host como “endianfw” y el dominio “dominio.local”. En el asistente de configuración de red se asignaron las zonas a las interfaces correspondientes. Como muestra la Figura 1, se verificó que cada interfaz tuviera el estado [UP] y la dirección IP correcta de acuerdo con lo siguiente.

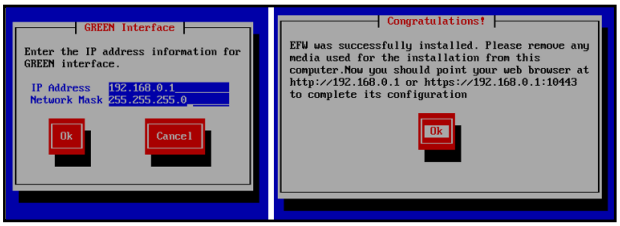
- Adaptador 1: Red interna “Redlan” (Zona VERDE)
- Adaptador 2: Adaptador puente (Zona ROJA)
- Adaptador 3: Red interna “DMZ” (Zona NARANJA)

Figura 1. Arranque de instalación Endian.



Fuente: Autoría propia.

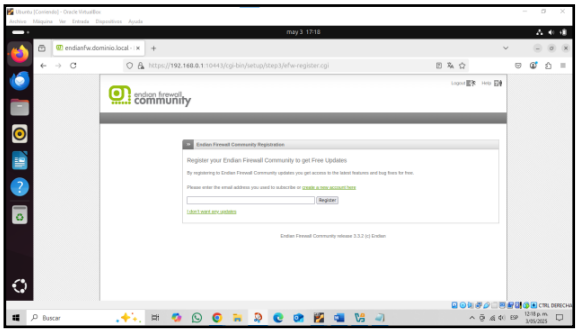
Figura 2. Finalización de instalación Endian.



Fuente: Autoría propia

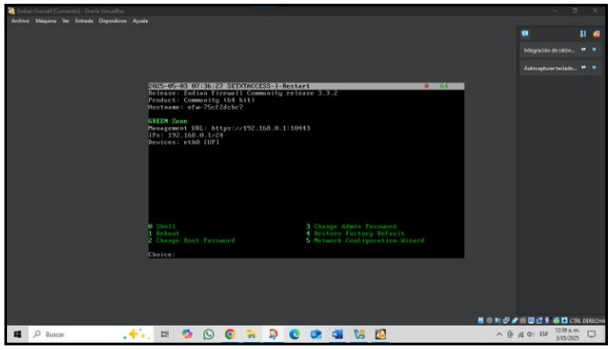
Esta instalación de Endian permite verificar la funcionalidad de las tres zonas de red. Desde el cliente Ubuntu se logra hacer ping a la IP del firewall (192.168.0.1) y acceder a la consola web de administración. En la Figura 3 se observa la interfaz de bienvenida para registrar la instalación. La Figura 4 confirma que la interfaz eth0 está activa en la zona VERDE, funcionando como puerta de enlace para la LAN.

Figura 3. Acceso desde el cliente Ubuntu a Endian web



Fuente: Autoría propia.

Figura 4. Consola Endian confirmando IP y zona VERDE.



Fuente: Autoría propia.

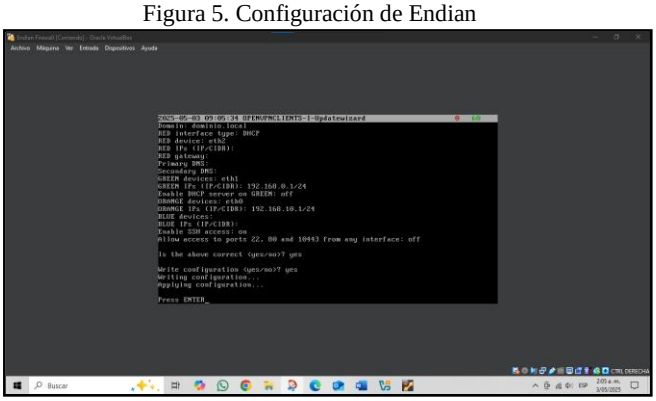
3 DESARROLLO

3.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

Se siguió un procedimiento estándar de acuerdo con el paso a paso descrito a continuación.

- Se descargó Endian Firewall Community 3.3.2 ISO.
- Se creó una máquina virtual con 1024 MB de RAM y disco de 10 GB.
- Se asignaron interfaces: eth0 (VERDE), eth1 (ROJA), eth2 (NARANJA).
- Se configuró IP estática 192.168.0.1/24 para la zona VERDE.
- El cliente Ubuntu se configuró con IP 192.168.0.10 en la misma red interna, según lineamientos de implementación de servidores Ubuntu en entornos virtualizados [2].

Figura 5. Configuración de Endian

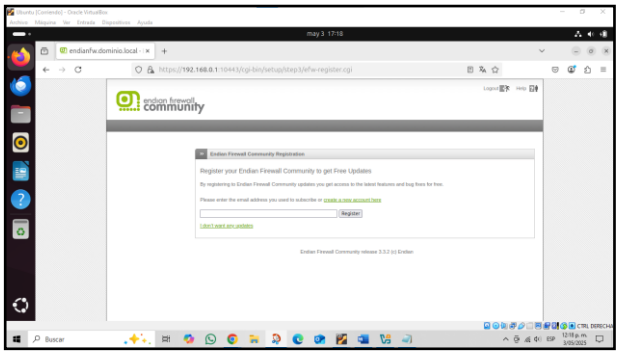


Fuente: Autoría propia.

De este ejercicio inicial, obtenemos que Endian responde exitosamente a la IP configurada, en este caso la 192.168.0.1. Y dado lo anterior, el cliente Ubuntu logra acceder a la interfaz web a través de https://192.168.0.1:10443.

Además, se logra probar la conectividad por medio de la consola en el cliente haciendo ping a la interfaz verde sin ninguna novedad por lo cual se confirma, por este medio también, el funcionamiento de cada adaptador en Endian.

Figura 6. Funcionamiento de Endian



Fuente: Autoría propia.

3.2 CONFIGURACIÓN NAT

Para esta sección, hay que tener en cuenta que "Endian Firewall crea automáticamente una regla NAT para cada zona para cada regla de reenvío de puerto configurada con el fin de permitir el acceso a ORANGE no solo desde RED sino también desde cada una de las otras zonas" (Endian, 2024) [3].

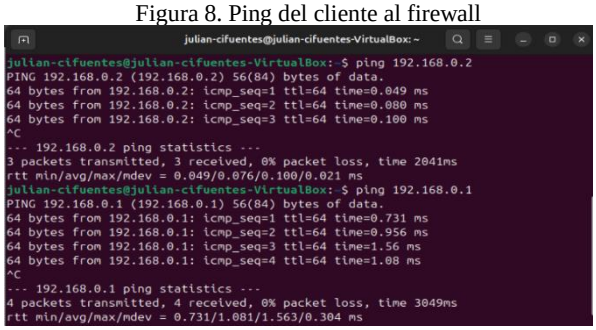
Entonces, una vez configurados los adaptadores en el firewall, se debe tener en cuenta también la configuración en el cliente de manera que tome la red interna creada.

Figura 7. Red Verde Cliente

Fuente: Autoría propia.

Luego, se logra también comprobar que no hay pérdida de paquetes al ejecutar ping sobre la puerta de enlace configurada.

Figura 8. Ping del cliente al firewall



Fuente: Autoría propia.

Ahora bien, con el fin de demostrar el establecimiento de la comunicación de la Zona DMZ hacia la Internet, se debe verificar el re-envío de puertos / NAT en función de la creación de las reglas.

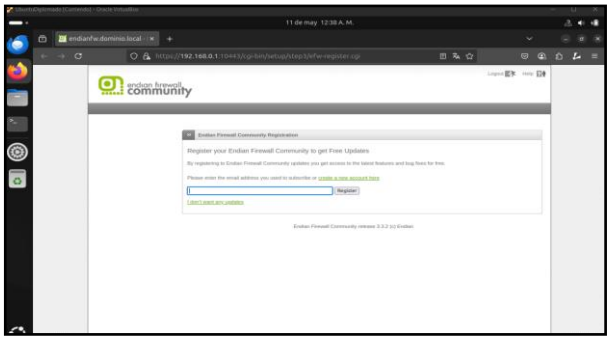
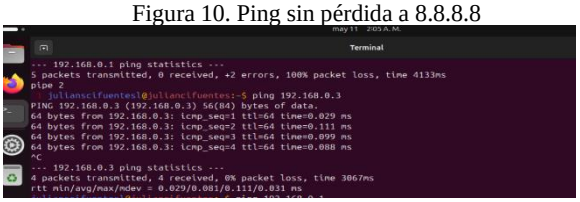


Figura 9. Visualización web Endian.
Fuente: Autoría propia.

Por lo que, desde el servidor, se debe tener no solo enrutamiento hacia el firewall sino también a internet estableciendo así una identificación de comunicación en la zona naranja.

Figura 10. Ping sin pérdida a 8.8.8.8



Fuente: Autoría propia.

Resulta necesario recordar que el sistema de manera "predeterminada divide la red en varias "zonas", diferenciadas por un código claro de colores", lo cual concede a cada zona una serie de reglas especiales de comportamiento (Hartek, 2016) [4].

3.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

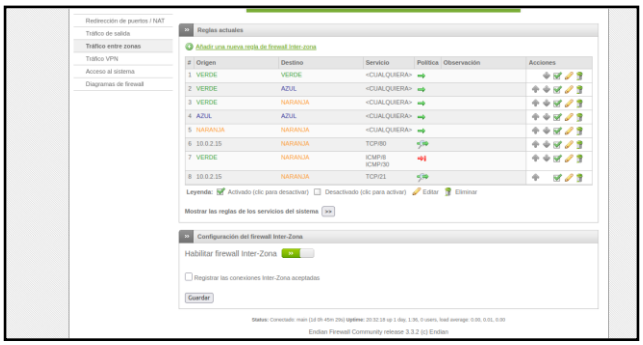
El tema principal de esta temática se enfocó en permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde el servidor web bajo Ubuntu Server, así como en denegar el protocolo ICMP (puertos 8 y 30) para evitar la ejecución de comandos de tipo "ping" en la red interna.

La implementación se realizó mediante la creación de una máquina virtual con Endian Firewall como sistema de seguridad, configurando tres interfaces de red, interfaz verde (LAN), naranja (DMZ) y roja (Internet vía NAT). Se asignaron direcciones IP estáticas a las interfaces verde (192.168.0.15) y Naranja para permitir la segmentación de servicios.

Durante la instalación y configuración inicial, se accedió a la consola web del firewall a través de https://192.168.0.15:10443, donde se definieron parámetros como zona horaria, contraseñas administrativas, y ajustes de red para cada interfaz. En la interfaz de configuración se crearon reglas de tráfico entre zonas para permitir el tráfico HTTP y FTP entre las zonas verde y naranja. Estas reglas también fueron replicadas en la sección de NAT, siguiendo buenas prácticas descritas en la gestión de firewalls bajo Linux [5]. para asegurar la redirección correcta hacia el servidor en la DMZ.

Posteriormente, se implementó una regla de denegación para los paquetes ICMP, bloqueando el tráfico de ping desde la zona verde hacia la zona naranja. Las pruebas realizadas desde una terminal confirmaron la efectividad de la regla, al no obtener respuesta al ejecutar el comando ping hacia direcciones IP dentro de la red del servidor.

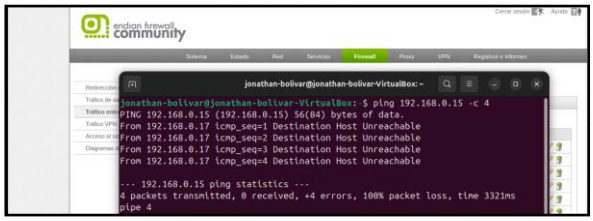
Figura 11. Reglas de la zona DMZ.



Fuente: Autoría propia.

Con todas las reglas aplicadas, se llevó a cabo una validación integral del funcionamiento de la red. Se verificó el acceso correcto al servidor web desde un navegador ubicado en la red verde, y se estableció una conexión FTP con éxito. Simultáneamente, la prueba de ping fallida confirmó la efectividad del bloqueo de ICMP. Estas pruebas demostraron que la DMZ estaba correctamente configurada, permitiendo únicamente los servicios deseados y restringiendo el resto del tráfico no autorizado.

Figura 12. Ping a 192.168.0.15 no responde



Fuente: Autoría propia.

3.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En un entorno digital cada vez más expuesto a amenazas y vulnerabilidades, la implementación de mecanismos de seguridad perimetral se vuelve fundamental para proteger los activos críticos, alineado con los lineamientos del estándar ISO/IEC 27001 [6]. la integridad, confidencialidad y disponibilidad de los recursos en una red. Esta temática se enfoca en diseñar y configurar una arquitectura de red segmentada mediante la herramienta Endian UTM, una solución de gestión unificada de amenazas (Unified Threat Management) de código abierto, a través de la creación de zonas de seguridad diferenciadas Verde (LAN), Naranja (DMZ) e Internet y la aplicación de reglas de firewall específicas, se busca controlar el tráfico de red y garantizar una comunicación segura entre los distintos segmentos.

También se integran funcionalidades como el enrutamiento, la redirección de puertos y la gestión de servicios HTTP y FTP, con el fin de simular un entorno de red real y evaluar el comportamiento de las políticas de acceso configuradas, como se observa a continuación.

Configuración de las reglas de acceso en el firewall Endian para los servicios HTTP y FTP en las zonas Verde, Naranja y Roja:

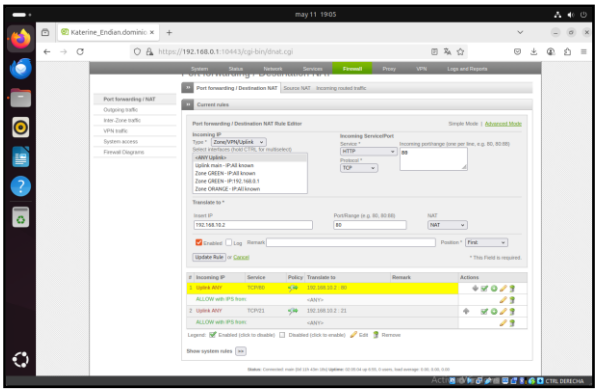
Primero, se listó las reglas para comunicar la Zona WAN (Roja) hacia la zona DMZ (Naranja) desde la interfaz de direccionamiento de puertos (Port forwarding) y permitir el acceso parametrizado a los servicios del host asignado en la zona DMZ:

Figura 13. Lista de reglas WAN hacia DMZ

Fuente: Autoría propia.

Para ellos, se asignó el enrutamiento HTTP al host en la Zona DMZ (Naranja) con la IP 192.168.10.2 que tiene el servidor web expuesto en el puerto 80:

Figura 14. Enrutamiento HTTP zona naranja puerto 80

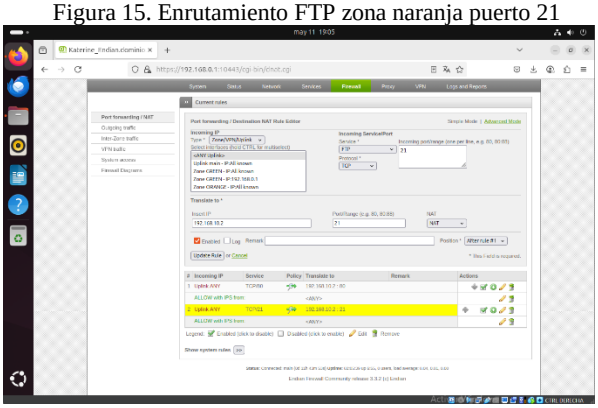


Fuente: Autoría propia.

Con lo anterior, las peticiones HTTP desde la zona WAN dirigen hacia el servidor web en la zona DMZ.

A continuación, se asignó el enrutamiento FTP al host 192.168.10.2 en la Zona DMZ (Naranja) con el servidor de FTP expuesto el puerto 21:

Figura 15. Enrutamiento FTP zona naranja puerto 21



Fuente: Autoría propia.

Igualmente que en con el protocolo HTTP, lo anterior permite el acceso al servidor FTP en la zona DMZ desde la zona WAN.

Con las zonas WAN y DMZ comunicadas, se listó las reglas del firewall para comunicar las Zonas LAN (Verde) y DMZ (Naranja) hacia la zona WAN (Roja) en la interfaz de Trafico saliente en el protocolo HTTP y HTTPS, permitiendo el acceso con las políticas establecidas:

Figura 16. Reglas comunicación LAN-DMZ hacia WAN

Fuente: Autoría propia.

Para ello, se asignó la regla de acceso HTTP entre la Zona DMZ (Naranja) y la Zona WAN (Roja) con los siguientes parámetros:

Figura 17. Regla HTTP entre DMZ.WAN

Fuente: Autoría propia.

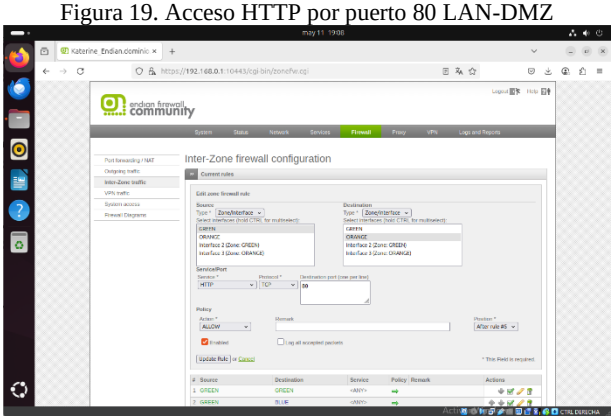
Luego, se asignó la regla de acceso HTTPS entre la Zona DMZ (Naranja) y la Zona WAN (Roja), así como la lista de reglas para comunicar la Zona LAN (Verde) hacia la Zona DMZ (Naranja) en la interfaz de Inter-Zone en los protocolos HTTP y FTP.

Figura 18. Comunicación LAN a DMZ por HTTP y FTP

Fuente: Autoría propia.

Se asigna la regla de acceso HTTP de la Zona LAN (Verde) a la Zona DMZ (Naranja) expuesto en el puerto 80.

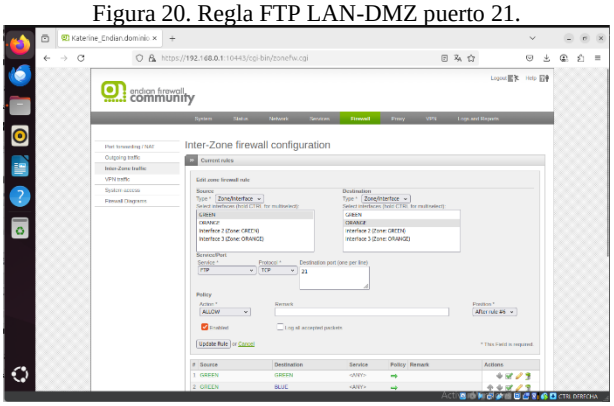
Figura 19. Acceso HTTP por puerto 80 LAN-DMZ



Fuente: Autoría propia.

Finalmente, se asignó la regla de acceso FTP de la Zona LAN (Verde) a la Zona DMZ (Naranja) expuesto en el puerto 21.

Figura 20. Regla FTP LAN-DMZ puerto 21.



Fuente: Autoría propia.

Con lo anterior se establecen las reglas del firewall en Endian UTM para permitir o denegar el acceso a protocolos entre las diferentes zonas, y así, se permitir un acceso controlado y seguro a las diferentes interfaces de red y sus servicios, o así mismo, denegarlo o restringirlo.

3.5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Un Proxy (No transparente) con autenticación, busca controlar, supervisar y proteger el acceso a internet desde una red local por medio de un firewall, en este caso Endian. La finalidad de esto es controlar quién accede a internet por medio de la autenticación obligatoria, usuario y contraseña, donde solo los usuarios autorizados pueden navegar, impidiendo que los usuarios no identificados puedan usar la red. También aplican las políticas de seguridad, en donde estas establecen los parámetros que se deben tener y así proteger de ingresos no autorizados del acceso a internet, en este sentido, se pueden definir reglas como los sitios que están permitidos o bloqueados, limitar las horas de navegación y restringir el acceso por grupos de usuarios, evitando el mal uso de internet, como lo expusieron Montoya y Tenesaca Gómez (2012) en su trabajo sobre el Hospital Santa Inés. Se puede monitorear y registrar la navegación, porque el proxy puede tener el registro del tráfico web, y también esta trazabilidad es útil para las auditorías o el análisis de incidentes. También se puede optimizar el uso de ancho de banda, con el *caching* mejora la velocidad de carga y reduce el tráfico hacia internet ayudando a que más usuarios puedan navegar eficientemente [7].

Dentro del contexto del diplomado, se llevó a cabo la implementación de un Proxy HTTP no transparente por medio del Endian Firewall Community, previamente instalado según la documentación de Endian (Endian.com, s.f.), esta actividad tenía como objetivo configurar un sistema de seguridad el cual debe regular el acceso a través de una lista negra, para esto, se hizo uso de una máquina virtual con EFW y Ubuntu. A continuación, se procede con la demostración a detalle de lo ejecutado [8].

3.5.1 CONFIGURACIÓN ENDIAN

Se crea una máquina virtual en donde se instaló Endian Firewall, en la parte inicial se configuran tres adaptadores de red en modo Red interna y Adaptador puente. En el primer arranque de EFW, se accede a la interfaz tipo Shell que muestra información sobre la red verde y el hostname que se asignó. Se ingresa a Ubuntu Desktop en la misma red interna y en el navegador web se ingresa a la URL http://192.168.0.15:10443, aquí se completaron los siguientes pasos para la configuración de red, como se indica en la guía de instalación de Endian en VirtualBox (Kifarunix.com, 2019) [9].

- Se selecciona el modo de operación en enrutamiento.
- Se activa la zona naranja para definir el segmento para servidores accesibles desde internet.
- Se asigna la IP 192.168.0.15 para la zona verde (LAN) y la IP 172.16.0.1 para la zona naranja (DMZ), también se asignaron los dispositivos eth0

en la zona verde, el eth1 para la zona naranja y el eth2 para la zona roja.

- También se definen los accesos a internet por medio de la interfaz roja usando DHCP, y se especifican los DNS de forma manual.
- Se omite el correo como administrador y también se confirmó la configuración completando el asistente.

3.5.2 CONFIGURACIÓN DEL PROXY HTTP (NO TRANPARENTE)

Se ingresa a la interfaz web de Endian, con el usuario y contraseña que se había creado, y desde el menú superior, en la sección Proxy > HTTP, se realiza la siguiente configuración:

- Se activa el modo No Transparente para la zona verde
- También se activa el Proxy y se selecciona el puerto 8080

Figura 21. Activación de modo no transparente web Endian.

Fuente: Autoría propia.

3.5.3 SE CREA EL PERFIL DE FILTRO DE CONTENIDO - LA LISTA NEGRA

En la pestaña Perfiles de filtro, se crea un perfil que para este caso se llamó Diplomado_UNAD, estando aquí se realizó lo siguiente:

- Activación del filtro de contenido
- Se habilita la opción de Lista Negra
- Estando aquí, se ingresa a los sitios solicitados para bloqueo de acuerdo con la necesidad: www.hotmail.com, www.youtube.com, www.elnuevodia.com.co
- Se guarda y se aplica la configuración

3.5.4 ACTIVACIÓN DE AUTENTICACIÓN DE USUARIO

Pasando a la pestaña Autenticación, se selecciona el método de autenticación Local (NCSA), después en Administración de usuario NCSA, se crea un usuario llamado admin2 y se asigna a un grupo llamado Linux_UNAD.

3.5.5 CREACIÓN DE POLÍTICA DE ACCESO CON AUTENTICACIÓN

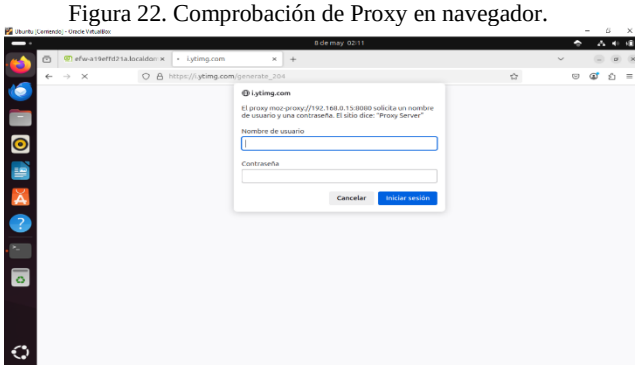
Estando en la pestaña de Políticas de acceso, se crea una regla con las opciones:

- Origen: <CUALQUIERA>
- Destino: <CUALQUIERA>
- Autenticación: En base al grupo
- Grupos permitidos: Linux_UNAD
- Restricción de tiempo: (sin activar)
- Agentes de usuario: Firefox
- Política de acceso: Permitir acceso
- Filtro de perfil: Diplomado_UNAD (para aplicar la lista negra)
- Posición: Primera posición
- Se dejó activa la opción "Permitir reglas de Política"

3.5.6 PRUEBA DESDE UBUNTU DESKTOP

Ahora se abre el navegador Firefox y se configuran los proxy HTTP de forma manual, escribiendo la IP de la máquina Endian 192.168.0.15 con el puerto 8080, al ingresar a alguna de las URL de la lista negra se solicitan las credenciales del usuario admin2 creado anteriormente, concluyendo que la configuración realizada se comporta de acuerdo con lo planeado.

Figura 22. Comprobación de Proxy en navegador.



Fuente: Autoría propia.

4 CONCLUSIONES

Se comprobó que el firewall respondía correctamente en cada interfaz, y que los servicios estaban en ejecución tras reiniciar. Esto valida que el sistema puede actuar como plataforma para continuar con las otras temáticas del diplomado: configuración de NAT, reglas de acceso, publicación de servicios desde la DMZ y configuración de proxy.

Una correcta configuración inicial permite tener claridad respecto a la infraestructura de red en corporaciones o proyectos internos de trabajo, lo que a su vez permite la prevención de amenazas de redes externas y el control de gestión de la información que se maneje a nivel interno.

La implementación de una red segmentada con una zona

desmilitarizada (DMZ) permitió evidenciar cómo una arquitectura correctamente estructurada puede ofrecer altos niveles de seguridad sin comprometer la funcionalidad de los servicios. Por medio de la configuración precisa del firewall y la asignación de roles a cada zona (verde, naranja y roja), se logró un equilibrio entre accesibilidad y protección. La habilitación controlada de servicios como HTTP y FTP, junto con el bloqueo del protocolo ICMP, demuestra la importancia de aplicar políticas de tráfico estrictas bajo el principio de mínimo privilegio. Enfoque que concuerda con las recomendaciones del NIST sobre políticas de firewall en entornos corporativos [10]. Este ejercicio no solo fortaleció los conocimientos técnicos en la gestión de redes y servicios en Linux, sino que también reafirmó la necesidad de aplicar buenas prácticas en seguridad informática dentro de infraestructuras reales.

A través de la implementación de Endian UTM se logró establecer una estructura de red segmentada que permite gestionar y controlar de forma eficiente el tráfico entre las distintas zonas de seguridad: Verde, Naranja, DMZ e Internet; Donde la configuración de reglas específicas para los protocolos HTTP y FTP evidenció la funcionalidad del firewall interzonal y la capacidad del sistema para aplicar políticas de acceso según los requerimientos de seguridad. Además, la incorporación de mecanismos como el enrutamiento y el port forwarding permitió validar la conectividad entre zonas bajo condiciones controladas, demostrando la utilidad de las soluciones UTM de código abierto como herramientas efectivas para la protección perimetral de redes, y refuerza el conocimiento práctico en administración de infraestructuras seguras.

La configuración de un Proxy HTTP no transparente con autenticación en Endian Firewall permitió establecer un control eficaz acerca del acceso a internet, realizado desde una red local, y así se garantizó que solo los usuarios que tengan los permisos puedan navegar utilizando credenciales. Implementando esta solución se pudo fortalecer la seguridad al aplicar filtros por medio de listas negras y se limitó el acceso según los grupos. En la actividad, se configuraron las zonas de red, el servicio proxy, la autenticación local siguiendo estructuras administrativas propuestas en entornos GNU/Linux [11]. y también las políticas de acceso, y así se pudo validar el funcionamiento desde el Ubuntu Desktop, por lo que se puede decir que se evidenció como una correcta configuración de proxy ayuda a mejorar la seguridad, optimiza los recursos y garantiza que se utilice responsablemente el internet.

5 REFERENCIAS

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

[2] J. LaCroix, (2020). Mastering Ubuntu Server, 2nd ed., Packt Publishing.

[3] Endian (2024). Port Forwarding Administrative Web Page, Chapter 6. Firewall Menu. https://docs.endian.com/archive/2.1/efw.firewall.port_forwarding.html#:~:text=Endian%20Firewall%20automatically%20creates%20a,each%20of%20the%20other%20zones

[4] Hartek. (2016). Unified Threat Managers e IPCOP. Follow The White Rabbit (blog). Recuperado de https://fwhibbit.es/unified-threat-managers-e-ipcop

[5] M. Rash, (2021). Linux Firewalls: Enhancing Security with nftables and Beyond, No Starch Press.

[6] ISO/IEC, (2013). 27001:2013 – Information Security Management Systems – Requirements, International Organization for Standardization.

[7] Narváez Montoya, M. S., & Tenesaca Gómez, R. L. (2012). Implementación de un sistema proxy con seguridad para la navegación de médicos y pacientes en el Hospital Santa Inés (Bachelor's thesis, Universidad del Azuay).

[8] Endian, (2022). How to Set Up The HTTPS Proxy. Recuperado de https://help.endian.com/hc/en-us/articles/115006253507-How-to-Set-Up-The-HTTPS-Proxy

[9] Kifarunix, (2024). Install and configure Endian Firewall on VirtualBox. (2024). Kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/

[10] National Institute of Standards and Technology (NIST), (2009). SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy.

[11] Linux Professional Institute, (2022) LPIC-1 Exam 101: Tema 102: Comandos GNU y Unix. https://learning.lpi.org/es/learning-materials/101-500/102/