INTEGRACIÓN DE SERVICIOS GNU/LINUX Y SEGURIDAD DE RED MEDIANTE ENDIAN FIREWALL

Sebastián Calderón Hoyos
scalderonh@unadvirtual.edu.co

RESUMEN: *Este escrito detalla el proceso seguido para instalar, afinar y validar un dispositivo de protección de frontera que emplea GNU/Linux Endian Firewall, implementado dentro de una simulación con VirtualBox. Se establecieron las zonas llamadas Verde (red local), Roja (internet) y Naranja (zona desmilitarizada), logrando una separación lógica apropiada. Se ajustaron los parámetros de traducción de direcciones de red para posibilitar el intercambio regulado entre la red local y la zona desmilitarizada hacia la red externa simulada. De igual forma, se pusieron en marcha los servicios web y de transferencia de archivos en la zona desmilitarizada, imponiendo límites al protocolo de mensajes de control para reforzar la protección. Se diseñaron directrices para la comunicación entre estos espacios con el objetivo de autorizar o prohibir el paso de datos según se requiriera, revisando su funcionamiento mediante chequeos de conexión y monitoreo de flujos. Finalmente, se configuró un intermediario web no visible que requiere usuario y contraseñas y que incluye filtros para sitios web no deseados, valorando su desempeño desde la red local. Las conclusiones confirman que Endian Firewall funciona bien para filtrar y administrar datos en redes divididas.*

PALABRAS CLAVE: Firewall, Endian, NAT, DMZ,

1 INTRODUCCIÓN

Debido a que los peligros digitales crecen, es necesario implementar redes fuertes que incorporen defensas en sus perímetros. Con esto en mente, alternativas de seguridad libres como GNU/Linux Endian ofrecen capacidades sofisticadas para separar, examinar y manejar el flujo de datos en compañías y escuelas. Usarlas en espacios virtuales resulta ser un método bueno para aprender de forma práctica las bases de la protección de redes.

Este trabajo se enfoca en diseñar una arquitectura dividida que emplee las zonas Verde, Roja y Naranja, además de configurar reglas NAT y pautas de entrada para asegurar intercambios protegidos y regulados. Las evaluaciones comprendieron prender servicios en la DMZ, restringir protocolos, reenviar puertos y chequear el movimiento entre zonas, lo cual ayuda a ver cómo responde el cortafuegos a distintas clases de datos.

También, se implementó un servidor proxy HTTP que no se nota, con validación y filtrado a través de listas de sitios vetados, fortaleciendo las normas de navegación y la supervisión de usuarios. Al integrar estos componentes, se puede medir la capacidad de Endian Firewall como una opción integral para administrar el acceso y salvaguardar el límite en redes que han sido separadas.

2 DESARROLLO DE LAS TEMÁTICAS

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

Durante la etapa inicial, luego de bajar la imagen ISO de Endian Firewall, empezamos por definir qué tarjetas de red irán destinadas a las zonas Verde, Roja y Naranja, viendo que queden bien repartidas antes de arrancar con la instalación del programa. Esta puesta a punto técnica es clave para asegurar que el firewall ande bien y que las distintas áreas operen separadas y bajo control desde el inicio.

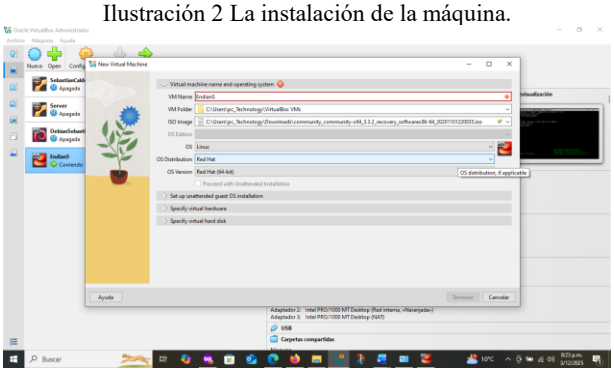
Previo a instalar la ISO, tenemos que preparar las conexiones de red para las redes roja, verde y naranja. Empezaremos por la roja, que es la que tendrá salida a internet; por eso mismo, la dejamos configurada en un adaptador NAT con DHCP, lo cual hará que las computadoras que se conecten obtengan sus direcciones IP solas.

Ilustración 1Configuracion interfaz de red roja

Fuente: Autoría Propia

Dividir la red correctamente resulta fundamental para asegurar el ambiente. En este caso particular, se configuraron tres conexiones de red virtuales en el aparato EFW, cada una representando un área de seguridad distinta. El siguiente cuadro detalla la configuración que se implementó:

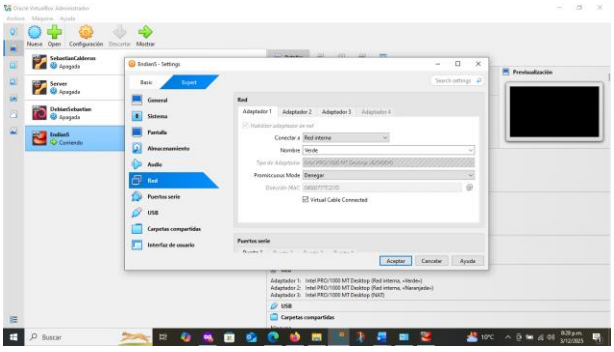
Ilustración 2 La instalación de la máquina.



Fuente: Autoría Propia

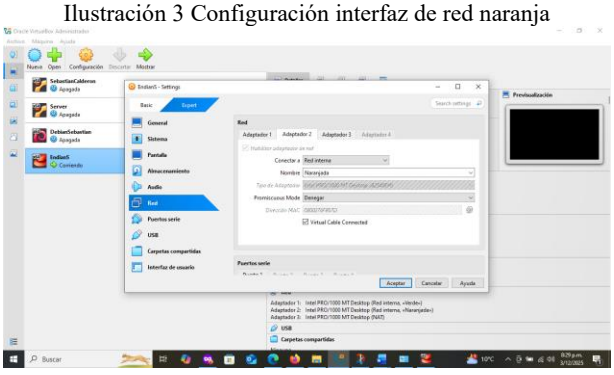
Ilustración 3 Configuración interfaz de red naranja

Para las redes que llamaremos Verde y Naranja, emplearemos sistemas internos, dándoles el nombre de sus colores respectivos.



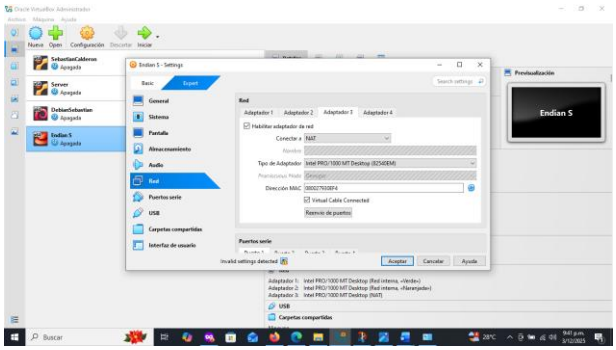
Fuente: Autoría Propia

Ilustración 3 Configuración interfaz de red naranja



Fuente: Autoría Propia

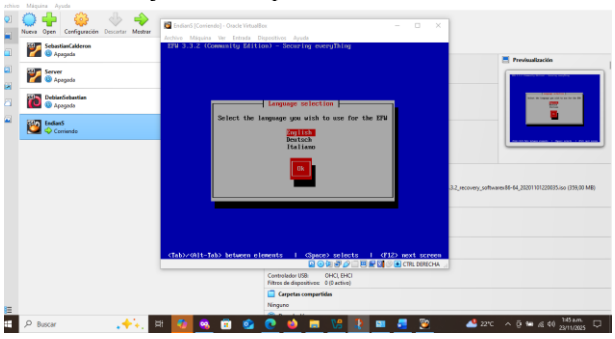
Ilustración 4 red NAT



Fuente: Autoría Propia

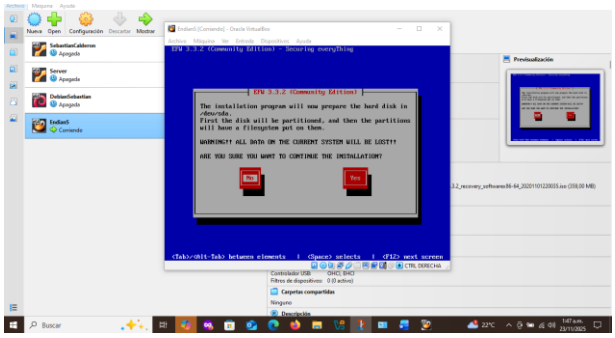
Tras modificar las conexiones de red, procedimos a montar la computadora virtual para Endian, habilitando los tres adaptadores asignados a cada una de las redes. Después, se ejecuta la instalación siguiendo las pautas que presenta el menú de opciones.

Ilustración 6 Selección del idioma con el que vamos a trabajar en la maquina Endian.



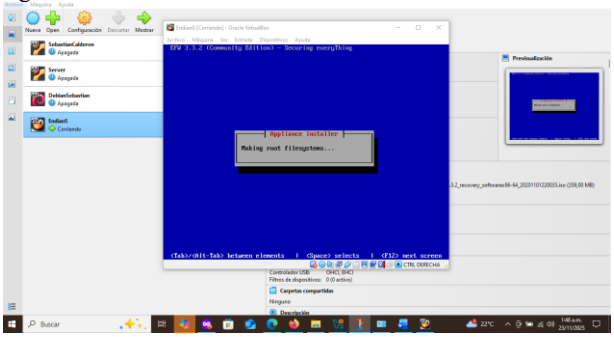
Fuente: Autoría Propia

Ilustración 7 Después nos aparecerá una advertencia, la cual especifica que proceso de instalación borrará todos los datos que contenga el disco duro, si deseamos continuar seleccionamos YES



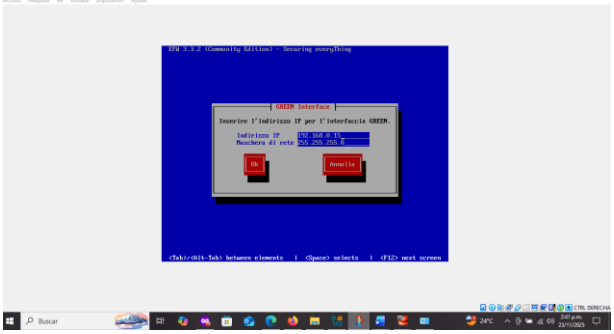
Fuente: Autoría Propia

Ilustración 8 Ahora comienza instalarse en nuestro disco duro, y podemos ver que nos irán saliendo mensajes como los siguientes.



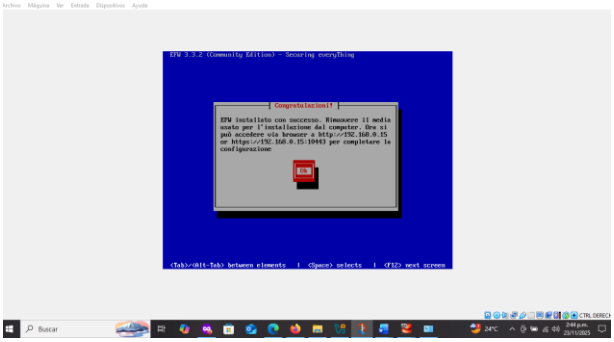
Fuente: Autoría Propia

Ilustración 2 Configuración de la dirección IP de la interfaz de red interna verde para posteriores configuraciones en navegador web.



Fuente: Autoría Propia

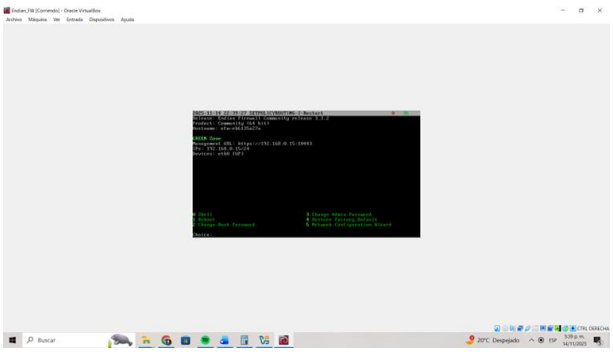
Ilustración 10 Después nos aparecerá una advertencia, la cual especifica que proceso de instalación borrará todos los datos que contenga el disco duro, si deseamos continuar seleccionamos OK



Fuente: Autoría Propia

Al terminar, se reiniciará y podremos ver la consola de Endian donde nos indica la ip para realizar la conexión por navegador web para la administración y opciones como cambiar la contraseña de administración, por defecto la contraseña es "endian" para este caso la cambié por "12345678"; el siguiente paso es configurar nuestras redes a través de la consola de endian.

Ilustración Consola Endian Firewall



Fuente: Autoría Propia

En esta interfaz podemos configurar las diferentes redes que vamos a utilizar a través de la opción No. 5; para la red Roja una red NAT con DCHP, para la red Verde una red interna con rango de ip 192.168.20.1/24 y para la red naranja de igual manera red interna con rango 192.168.10.5/24.

Ilustración 7 Configuración IP de las redes

Fuente: Autoría Propia

Iniciamos la máquina virtual cliente conectada a la zona Roja y verificamos que obtiene correctamente una dirección IP asignada por el servicio DHCP del adaptador NAT de VirtualBox, que actúa como la red simulada de Internet. Esta máquina cuenta únicamente con una interfaz de red configurada en modo NAT, lo que permite que funcione como un equipo externo al firewall. Finalmente, comprobamos la conectividad hacia Internet desde esta red simulada, confirmando que la comunicación opera sin inconvenientes.

Ilustración Verificación conexión a internet

Ponemos en marcha un equipo cliente nuevo que enlazamos a la Red Verde y empezamos a modificar su fichero yaml usando el segmento de red destinado en Endian. En este caso, la dirección IP que le toca es 192. 168. 20. 5. Tras aplicar las modificaciones con la orden netplan apply, comprobamos que el equipo ya tiene la IP puesta. Después, chequeamos la comunicación con el cortafuegos y, finalmente, entramos al portal web de manejo mediante la dirección 192. 168. 20. 1:10443, lugar donde reside el ajuste central de Endian.

Seguimos con el equipo cliente enlazado a la Red_Naranja y, al igual que en la computadora previa, ajustamos su archivo. yaml con el segmento de red que se ha asignado en Endian. En esta ocasión, la dirección IP configurada es 192. 168. 10. 10. Después de implementar los cambios utilizando el comando netplan apply, comprobamos que el equipo haya adquirido la IP correspondiente y, a continuación, corroboramos la conexión con el firewall.

Para terminar, cuando ya hayamos ajustado todos los parámetros de conexión, ponemos en marcha todas las computadoras virtuales y verificamos que todo marche bien. La que enlaza con la Red_Verde puede entrar sin dificultad a la parte visual de Endian usando la dirección que se muestra en la pantalla. Por otro lado, la que se une a la Red_Naranja mantiene una conexión fija con su red, y aunque ahora no navega por la web, podríamos darle acceso si se requiriera. A modo de cierre, la máquina vinculada a la Red_Roja navega por internet gracias a la dirección IP que le dio el sistema DHCP del componente NAT de VirtualBox, el cual imita una red externa.

Como evidencia, constatamos la conexión HTTP exitosa desde Linux Mint hacia el dominio externo zona roja; este hallazgo valida la normativa del firewall de salida para el tráfico HTTP..

Tomando en cuenta las comprobaciones previas que salieron bien, podemos confirmar que el firewall está eligiendo y dejando pasar solo lo que se necesita; esto incluye la comunicación interna entre las PCs de oficina (Zona verde) y el servidor (Zona naranja), además del acceso a la web (Zona roja) para sus tareas específicas. Este manejo ayuda a reducir las amenazas de ataques y garantiza que todos los sistemas vitales funcionen adecuadamente.

3 CONCLUSIONES

Se logra dominar la forma de armar la estructura del sistema operativo GNU/Linux, poniendo e manejando las distintas partes, usando tanto instrucciones escritas como las interfaces visuales. Se consigue montar una estructura de red dividida usando la versión GNU/Linux Endian, configurando el área segura (LAN), la externa (WAN) y la intermedia (DMZ), con el fin de mejorar la protección de una red; logrando administrar el paso de información de red, de forma medida y segura entre los aparatos dentro, los servidores y la entrada a internet de los sistemas operativos usados durante todo esto.

El trabajo con el tema dos sirvió para obtener un entendimiento mayor acerca de cómo ajustar cortafuegos, NAT y normas de protección en redes, usando Endian Firewall como herramienta principal. Durante este camino, se aprendió a poner reglas de control para asegurar las áreas LAN, DMZ y WAN, y se vio lo vital que es separar las redes bien para cuidar lo de adentro y asegurar una conexión segura hacia afuera. Poner en práctica SNAT y DNAT fue esencial para dar entrada controlada a servicios internos y asegurar que lo de afuera se pudiera usar correctamente, sin poner en riesgo la protección de la red interior. Las pruebas hechas demostraron que los ajustes hechos logran las metas de conexión y resguardo, resaltando qué tan bien funcionan las normas de seguridad aplicadas, lo cual mejoró el saber en cómo montar redes y cortafuegos y dejó ver la relevancia de aplicar defensas de seguridad apropiadas en lugares de trabajo o de operación.

3.1 TEMATICA 1

El empezar a usar GNU/Linux Endian dentro de un entorno simulado con VirtualBox nos sirvió mucho para ver en la práctica cómo se arma una barrera de seguridad que divide la red en partes. Poniendo bien las tarjetas de red y después de instalar todo, pudimos notar las tres partes esenciales: el área verde, que es como nuestra red interna segura (la LAN), el área roja que conecta con el exterior (el internet o WAN), y el área naranja donde se guardan los servidores en la zona desmilitarizada (DMZ). Este proceso no solo recalcó lo crucial que es dividir bien la red para protegerla y manejar el flujo de datos, sino que también resaltó lo útiles que son programas como Endian para manejar la infraestructura de red de forma segura y sin líos. Al final, esta tarea ayudó a afianzar conceptos clave sobre manejo de redes, simulación y seguridad digital.

4 REFERENCIAS

[1] «What Is Network Address Translation (NAT)?», Cisco. Accedido: 23 de noviembre de 2025. [En línea]. Disponible en: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-address-translation-nat.html

[2] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

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

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

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

[7] Arsys. (s.f.). *Protocolos de Internet: HTTP y FTP*. Recuperado de https://www.arsys.es/blog/protocolos-de-internet-http-y-ftp

[8] cyberleon95. (s.f.). *Instalación y configuración de Firewall Endian* [Presentación en SlideShare]. SlideShare.

https://es.slideshare.net/slideshow/instalacin-y-configurcin-firewall-endian/39219423

[9] Endian Team. (s.f.). *Endian Firewall Community (Versión 3.3.2) [Software de código abierto]*. SourceForge. https://sourceforge.net/projects/efw/

[10] *Outbound NAT | PFSense Documentation*. (s. f.). https://docs.netgate.com/pfsense/en/latest/nat/outbound.html

[11] *Port forwarding / NAT — Endian UTM 3.2 Reference Manual*. (s. f.). https://docs.endian.com/3.2/utm/firewall/dnat.html