“SEGURIDAD DE ALTO NIVEL CON ENDIAN FIREWALL“

Ruth Caicedo Aguiño
e-mail: rcaicedoag@unadvirtual.edu.co
Eider Fernando Gonzalez Fory
e-mail: efgonzalezfor@unadvirtual.edu.co
David Camilo Mejía
e-mail: dcmejiaz@unadvirtual.edu.co

RESUMEN: *En el siguiente se describe el proceso de instalación y configuración del sistema GNU/Linux Endian Firewall (EFW) en una máquina virtual utilizando VirtualBox, orientado a la creación de un entorno de red seguro. Se implementa una arquitectura que incluye tres zonas principales: verde (LAN interna), naranja (DMZ o zona de servidores) y roja (WAN o conexión a Internet). A lo largo del proceso, se detalla la configuración de las interfaces de red, la asignación de direcciones IP, y la verificación de la conectividad entre las zonas mediante pruebas de comunicación.*

Además, se realiza la configuración inicial del sistema, incluyendo la asignación de contraseñas con la validación de las zonas de seguridad. De esta forma mostramos una guía completa para desplegar Endian Firewall como una solución efectiva de enrutamiento, filtrado y protección perimetral.

PALABRAS CLAVE: Cortafuegos, Endian, VirtualBox, Zonas de red, Enrutamiento, GNU/Linux, Seguridad perimetral.

1 INTRODUCCIÓN

Con el uso masivo de las tecnologías de información se han acrecentado los ataques para acceder a información digital y causar daño a las infraestructuras de las compañías por lo que se hace necesario que como estudiantes de Ingeniería de Sistemas conozcamos las herramientas en entrono Linux que permitirán mitigar los riesgos asociados a la seguridad de la red. En este artículo se detallará el uso de Endian como Firewall para instalar seguridad perimetral en una red Local conformada por equipos Linux permitiendo la comunicación a una red Externa de forma controlada y segura, creando distintas zonas y aplicando reglas en cada una de ellas con el fin de controlar el ingreso y exposición de los equipos hacias las distintas redes. Esto con el fin de dar solución a la problemática presentada durante el diplomado sobre la implementación de una red.

En el contexto actual, donde las infraestructuras tecnológicas se encuentran expuestas a ciberataques cada vez más sofisticados —como intrusiones, malware, ataques de denegación de servicio, exfiltración de datos o accesos no autorizados—, resulta imprescindible que los futuros profesionales en Ingeniería de Sistemas desarrollen competencias prácticas en la implementación de soluciones de seguridad perimetral. Una de estas herramientas es Endian Firewall (EFW), una distribución basada en GNU/Linux que integra funciones avanzadas de protección, monitoreo y gestión del tráfico de red.

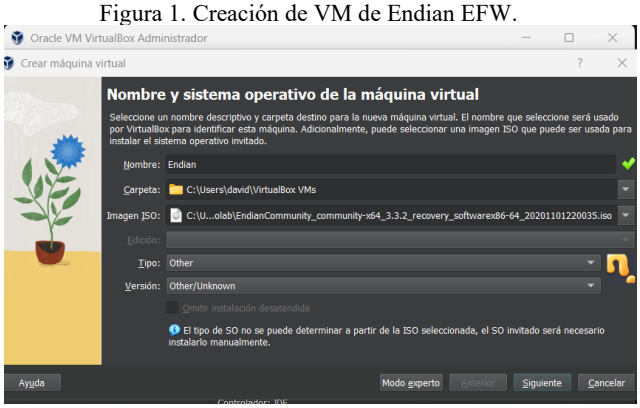
El presente artículo profundiza en la instalación, configuración y uso de Endian dentro de un entorno virtualizado con VirtualBox, permitiendo replicar escenarios reales de segmentación de red mediante zonas claramente definidas: Verde (LAN interna confiable), Naranja (DMZ para servidores expuestos) y Roja (WAN o Internet). A través de este laboratorio, el estudiante comprende la importancia de aislar servicios críticos, definir reglas de acceso específicas entre zonas, habilitar mecanismos de autenticación y aplicar políticas de filtrado que fortalezcan la seguridad.

2 CONFIGURACIÓN ENDIAN EN VIRTUAL BOX

Una vez descargado el ISO de la página oficial damos click en el botón iniciar máquina virtual y comenzamos a hacer la instalación simplemente dando en el botón *ok* y listo [1].

En la Figura 1 se evidencia la instalación de la máquina virtual con Endian.

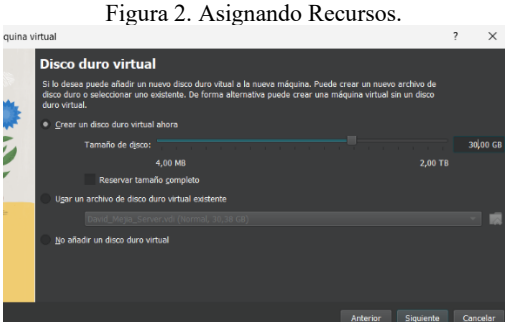
Figura 1. Creación de VM de Endian EFW.



Fuente: Autoría Propia.

En la Figura 2 se observa la configuración del disco duro virtual

Figura 2. Asignando Recursos.



Fuente: Autoría Propia.

En la Figura 3 se evidencia el global de la configuración

Figura 3. Resumen de la instalación.

Fuente: Autoría Propia.

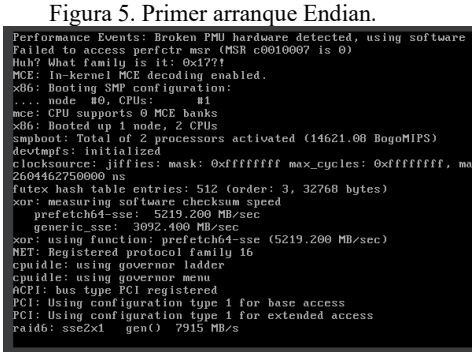
En la Figura 4 se observa la configuración de la sección de red

Figura 4. Definición de las 3 redes: dmz, naranja y verde.

Fuente: Autoría Propia.

En la Figura 5 se evidencia que todo fue instalado correctamente en los pasos anteriores

Figura 5. Primer arranque Endian.



Fuente: Autoría Propia.

En la Figura 6 se inicia seteando los primeros parámetros

Figura 6. Selección de lenguaje.

Fuente: Autoría Propia.

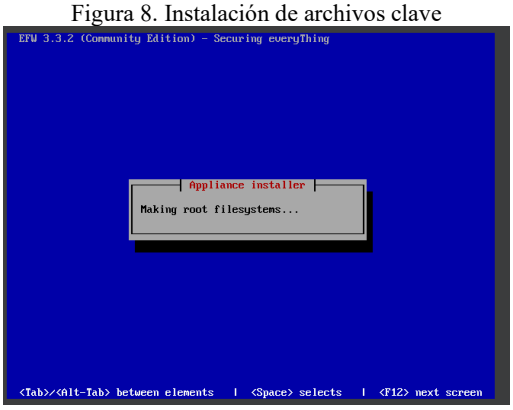
En la Figura 7 se puede evidenciar que se va a hacer una instalación limpia formateando

Figura 7. Advertencia formateo

Fuente: Autoría Propia.

En la Figura 8 se están creando los archivos raíz

Figura 8. Instalación de archivos clave



Fuente: Autoría Propia.

3 DESARROLLO DE LAS TEMATICAS

3.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED)

La configuración de las redes y las interfaces de red que dan servicio a las zonas es rápida y sencilla con este asistente de 8 pasos. Es posible navegar libremente hacia adelante y hacia atrás entre los pasos mediante botones siguiente y atrás e incluso cancelar en cualquier momento las acciones realizadas hasta el momento. [2]

Distribución de IPs según la zona:

- Naranja Servidor: 192.168.1.30
- Puerta de enlace: 192.168.1.25
- Verde Endian: 192.168.0.25
- Roja DHCP

En la Figura 9 se observa la asignación de ip para la zona verde

Figura 9. Configuración de la interfaz verde Endian

Fuente: Autoría Propia.

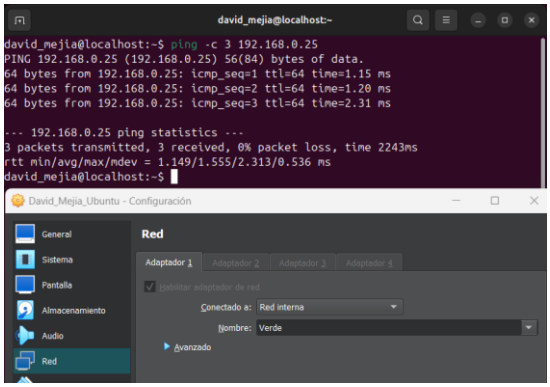
En la Figura 10 se ve la consola de comandos dentro de la zona verde

Figura 10. Zona verde

Fuente: Autoría Propia.

En la Figura 11 se ve la consola de comandos dentro de Ubuntu desktop

Figura 11. Se hace ping desde Ubuntu para probar la zona verde exitosamente



Fuente: Autoría Propia.

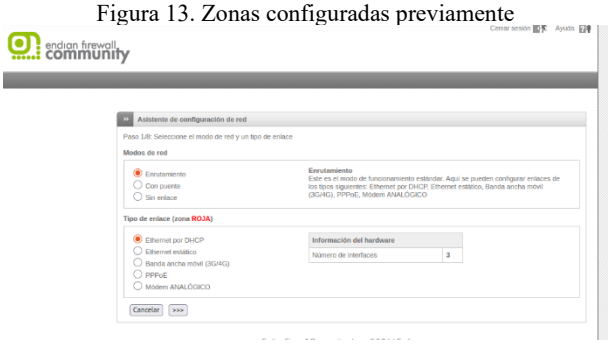
En la Figura 12 se observa el Mozilla Firefox accediendo a la ip de la zona verde

Figura 12. Entramos a la configuración de Endian

Fuente: Autoría Propia.

En la Figura 13 se observa el inicio del proceso de enrutamiento

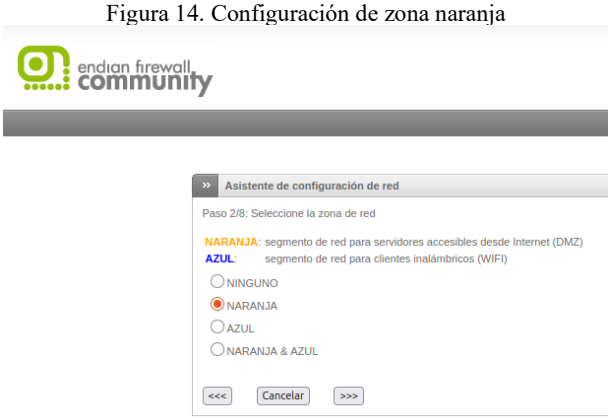
Figura 13. Zonas configuradas previamente



Fuente: Autoría Propia.

En la Figura 14 se ve el asistente de configuración de red

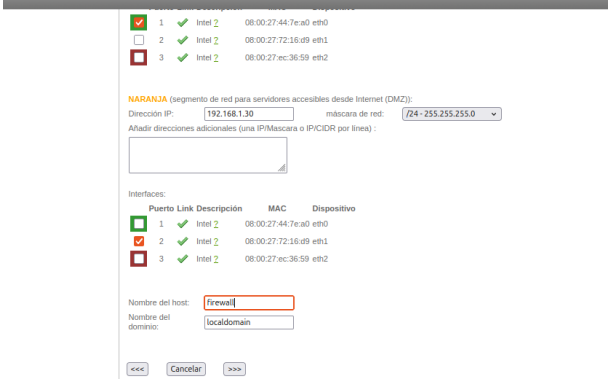
Figura 14. Configuración de zona naranja



Fuente: Autoría Propia.

En la Figura 15 se evidencia los distintos parámetros y dispositivos con los que cuenta el asistente de configuración de red

Figura 15. Se pone la ip asignada para la naranja



Fuente: Autoría Propia.

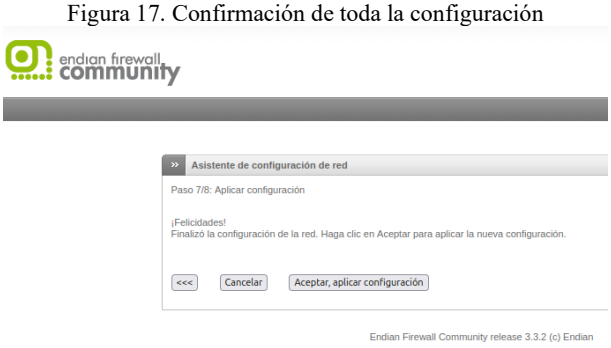
En la Figura 16 se evidencian las diversas zonas con sus dispositivos, y las direcciones MAC

Figura 16. Confirmación de zona roja

Fuente: Autoría Propia.

En la Figura 17 se pregunta si está seguro de que lo anterior está bien hecho para aplicarlo

Figura 17. Confirmación de toda la configuración



Fuente: Autoría Propia.

En la Figura 18 se ve el inicio de sesión con usuario en Endian después de aplicada configuración a las 3 zonas exitosamente

Figura 18. Menú principal de Endian

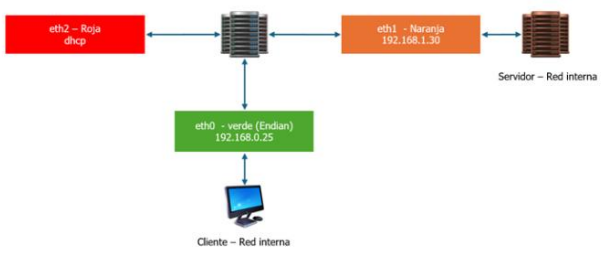
Fuente: Autoría Propia.

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

En la resolución de la temática, se plantea la siguiente configuración de red:

En la Figura 19 se ve el esquema general de las tres redes

Figura 19. Diseño de red temática



Fuente: Autoría Propia.

Donde se tiene lo siguiente:

- Zona Verde: Equipo Debian Desktop que se conectará a Endian por eth0. Conocido como el cliente.
- Zona Naranja: Equipo Ubuntu Server que se conectará a Endian por eth1. Conocido como el DMZ.
- Zona Roja: Equipo Endian que estará por eth2. Conocido como DHCP

Se accede desde Debian Desktop a la Interfaz de Endian mediante el enlace https://192.168.0.25:10443 y se realiza lo siguiente:

3.2.1 Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

En la Figura 20 se revisan los diversos parámetros de configuración.

Figura 20. Configuración protocolo HTTP puerto 80

Fuente: Autoría Propia.

En la Figura 21 se ajusta todo relacionado con la zona del firewall y FTP

Figura 21. Configuración protocolo FTP puerto 21

Fuente: Autoría Propia.

3.2.2 Comunicar la zona Internet con la zona DMZ

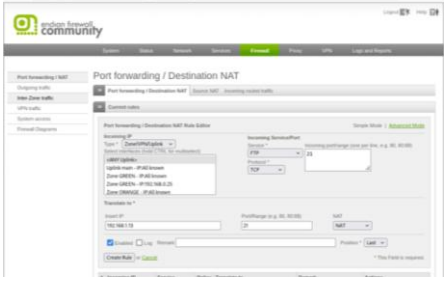
En la Figura 22 está la parte de los puertos y NAT con sus diversas opciones

Figura 22. Configuración desde la Zona ROJA al Puerto 80

Fuente: Autoría Propia.

En la Figura 23 se continua en la misma pantalla de la configuración de la anterior

Figura 23. Configuración desde la Zona ROJA al Puerto 21



Fuente: Autoría Propia.

3.2.3 Verificar en el tráfico Inter - Zona, la creación de las reglas.

En la Figura 24 se observa aplicación de las reglas configuradas en los números 5 y 6

Figura 24. Verificación de reglas aplicadas

Fuente: Autoría Propia.

3.2.4 Probar desde un navegador Web, las siguientes directivas:

3.2.4.1 El ingreso del servicio HTTP desde la LAN hacia la zona DMZ.

En la Figura 25 Se evidencia correcto cargue del Moodle desarrollado en la Actividad No. 6

Figura 25. Testeo desde la Zona Verde (Debian Desktop) hacia la Zona Naranja (Ubuntu Server)

Fuente: Autoría Propia.

3.2.4.2 El ingreso del servicio HTTP desde la LAN hacia la WAN.

En la Figura 26 se encuentra página de prueba para confirmar que la configuración HTTP está correcta

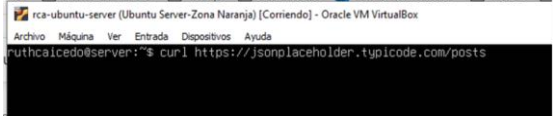
Figura 26. Testeo desde la Zona Verde (Debian Desktop)

Fuente: Autoría Propia.

3.2.4.3 El ingreso del servicio HTTP desde la zona DMZ hacia la WAN.

En la Figura 27 está la consola de la zona naranja para diversas pruebas

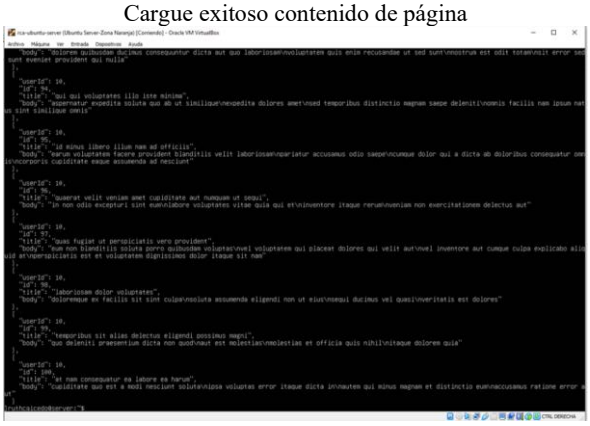
Figura 27. Testeo desde la Zona Naranja (Ubuntu Server)



Fuente: Autoría Propia.

En la Figura 28 se evidencia el resultado al ejecutar comandos en la consola a través de la zona naranja

Figura 28. Testeo desde la Zona Naranja (Ubuntu Server): Cargue exitoso contenido de página

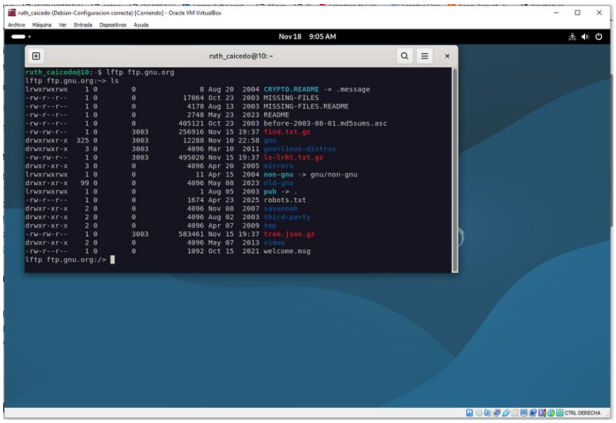


Fuente: Autoría Propia.

3.2.4.4 El ingreso del servicio FTP desde la LAN hacia la WAN.

En la Figura 29 corre Debian con la consola abierta para hacer pruebas en la zona verde

Figura 29. Testeo desde la Zona Verde (Debian Desktop) hacia FTP de la WAN



Fuente: Autoría Propia.

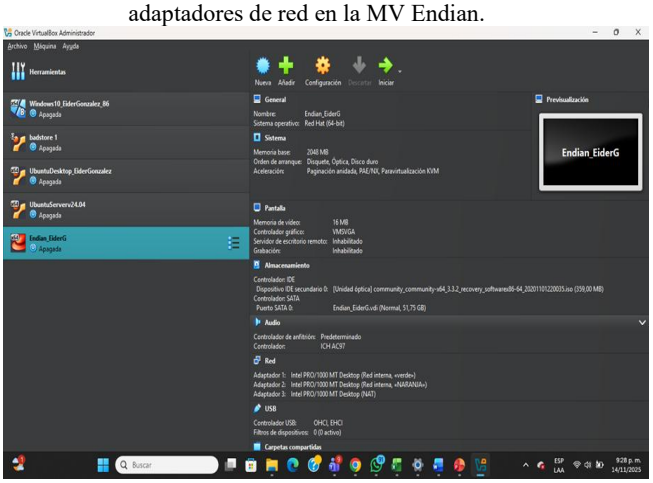
3.3 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

3.5.1. Implementación de GNU/Linux Endian, zonas verde, naranja y roja.

- Descarga de la ISO de Endian Community x64 3.3.2
- Creación de la máquina virtual con tres adaptadores de red:
  Adaptador 1: Red interna (verde)
  Adaptador 2: Red interna (Naranja)
  Adaptador 3: NAT (Roja)

En la Figura 30 se ve el VirtualBox listo para lanzar Endian

Figura 30: Imagen que evidencia la configuración de los adaptadores de red en la MV Endian.



Fuente: Autoría Propia

3.5.2. Configuración de Ubuntu Server (Zona verde)

- ADDRESS: 192.168.0.26
- GATEWAY: 192.168.0.25
- DNS: 8.8.8.8

En la Figura 31 la consola de comandos se hace ping a la ip para evaluar su funcionamiento

Figura 31: Evidencia de conexión de la Zona Verde haciendo uso del comando ping

Fuente: Autoría propia

3.5.3. Configuración de Ubuntu DesKtop (Zona Naranja)

- ADDRESS: 192.168.1.31
- GATEWAY: 192.168.1.30
- DNS: 8.8.8.8

En la Figura 32 se esta verificando el ping pero esta vez desde Ubuntu

Figura 32: Evidencia de conexión de la Zona Verde haciendo uso del comando ping

Fuente: Autoría propia

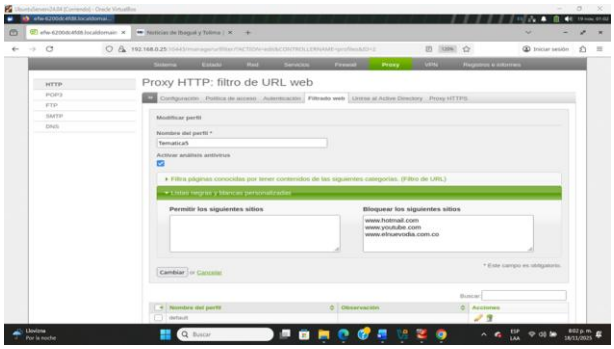
3.5.4. Implementación del Proxy

3.5.4.1 Crear un perfil y establecer una lista negra.

- Creación del perfil: Se creo el perfil dentro de las opciones de configuración del proxy HTTP en Endian con el nombre de Temática 5.
- Creación de la Lista Negra: En la configuración del perfil recientemente creado, se añadió los siguientes sitios a la lista negra para bloquear el acceso:
  - www.hotmail.com
  - www.youyube.com
  - www.elnuevodia.com.co

En la Figura 33 se visualiza los filtros de url web para las listas negras

Figura 33: Configuración del perfil y la lista negra en la GUI de Endian.



Fuente: Autoría propia

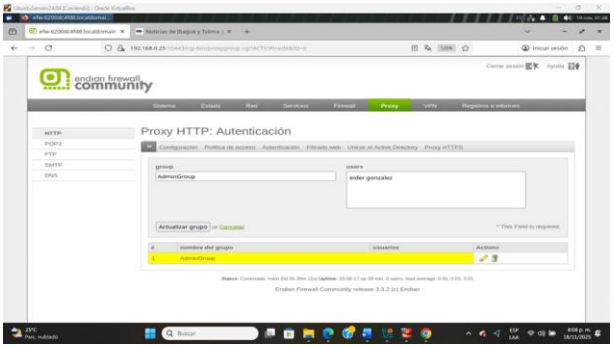
3.5.4.2. Configuración de autenticación por usuario y políticas de acceso.

- Crear usuario y asociarlo a un grupo: Utilizando la opción del proxy, se creó el usuario (eider gonzalez) y posteriormente se asoció este usuario al nuevo grupo (AdminGrup)
- Establecer una política de acceso y vincularla al perfil: Se creo una política de acceso y posteriormente

se vinculó el perfil de la lista negra creado en el primer paso y relacione la política con el mecanismo de autenticación por usuario o grupo, para nuestro caso se creó con la opción grupo.

En la Figura 34 se evidencia el panel principal de la autenticación en Endian

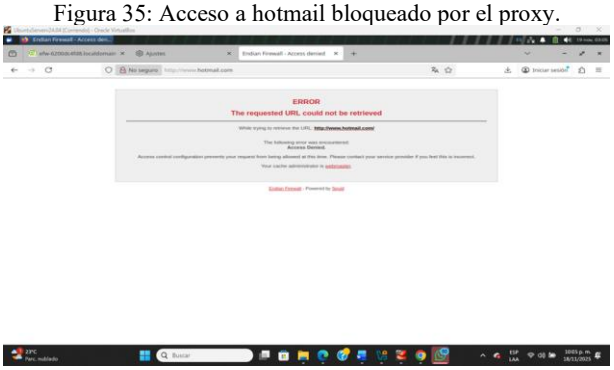
Figura 34: Configuración de las políticas de acceso en la interfaz de Endian.



Fuente: Autoría propia.

3.5.4.3. Pruebas de acceso: Intentos de acceso a los portales referenciados en la lista negra

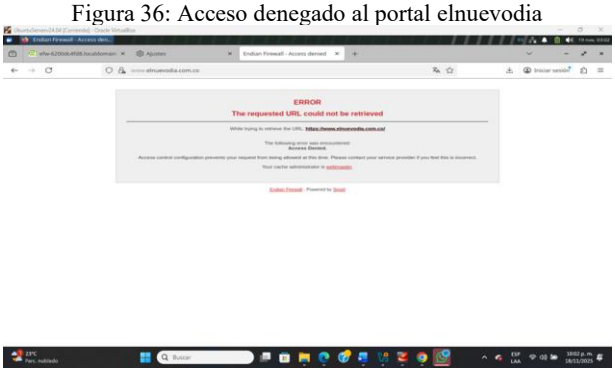
Figura 35: Acceso a hotmail bloqueado por el proxy.



Fuente: Autoría propia

En la Figura 36 se ve el resultado de intentar navegar a elnuevodia con la lista negra configurada

Figura 36: Acceso denegado al portal elnuevodia



Fuente: Autoría propia

4 CONCLUSIONES.

- En la temática 1, a medida que se van configurando las distintas redes como la naranja, roja y verde en Endian, es necesario ir haciendo ping desde la VM de Endian y desde Ubuntu Desktop para verificar que la configuración de cada una tenga conexión entre ellas; además, este proceso permite identificar rápidamente posibles errores de direccionamiento o reglas mal aplicadas, asegurando que los servicios de seguridad funcionen como se espera antes de avanzar con configuraciones más complejas.

- En la temática 4 se evidencia que Endian es un Firewall de distribución Linux que permite la configuración de una red LAN y controla el acceso hacia la red WAN y viceversa. Cuenta con una interfaz gráfica que facilita la administración de comunicación entre dispositivos y redes. En ésta, se evidencia la debida configuración de los puertos 80 para HTTP y 21 para FTP entre las zonas Roja definida para Endian DHCP, Verde definida para Cliente, continuando con el proceso de aprendizaje se definió la utilización de Debian Desktop y Naranja para el DMZ usando el servidor Ubuntu creado para dar cumplimiento en las actividades 4 y 5, teniendo este ya implementado un Moodle. En Endian Interfaz Gráfica, se configura la zona Roja hacia las zonas Verdes y Naranja mediante la opción Firewall > Port Forwarding NAT, y la configuración entre zonas Verde y Naranja se realizó mediante la opción Inter-Zone Traffic.

- Para la temática 5 implementación del Proxy HTTP No Transparente en GNU/Linux Endian (EFW) fue fundamental para establecer un control de acceso estricto a la WAN, logrando el doble objetivo de reforzar la seguridad perimetral mediante la autenticación obligatoria de usuarios para la navegación y la aplicación de políticas de filtrado de contenido (lista negra), lo cual garantiza la integridad de los recursos de la red LAN, cumpliendo de manera efectiva con los requisitos de seguridad planteados.

5 REFERENCIAS

[1] Carlos Serrano. Instalación Firewall Endian | Parte 1, (3 de agosto de 2020). Accedido el 13 de noviembre de 2025. [Video en línea]. Disponible: https://www.youtube.com/watch?v=kaolmNWyFiU

[2] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. Accedido el 13 de noviembre de 2025. Disponible: https://docs.endian.com/3.2/utm/system.html#network-configuration

[3] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix. Accedido el 13 de noviembre de 2025. Disponible: https://learning.lpi.org/es/learning-materials/101-500/102

[4] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. Accedido el 13 de noviembre de 2025. Disponible: https://help.ubuntu.com/20.04/ubuntu-help/index.htm

[5] Oracle (2020). Manual de usuario VirtualBox. VirtualBox. Accedido el 13 de noviembre de 2025. Disponible: https://www.virtualbox.org/manual

[6] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. Accedido el 13 de noviembre de 2025. Disponible: http://docs.endian.com/3.2/utm/index.htm

[7] Endian. (s.f.). Endian Firewall Community. Endian. Accedido el 13 de noviembre de 2025. Disponible: https://www.endian.com/community

[8] Endian. (2013). Endian Firewall Reference Manual. Endian. Accedido el 13 de noviembre de 2025. Disponible: https://www.endian.com/community/download

[9] Red Hat. (2023). Using iptables to configure NAT. Red Hat Documentation. Accedido el 13 de noviembre de 2025. Disponible: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10

[10] Cisco Systems. (2020). Network Address Translation (NAT) Configuration Guide. Cisco. Accedido el 13 de noviembre de 2025. Disponible: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat