“LABORATORIO DE REDES SEGURAS CON ENDIAN FIREWALL: DMZ, NAT Y PROXY AUTENTICADO”

Diego Andrés Grajales Rodríguez
e-mail: dagrajalesro@unadvirtual.edu.co
Derly Alejandra Ardila Barrera
e-mail: daardilaba@unadvirtual.edu.co
Wendy Carolina Murillo Pinzón
wcmurillop@unadvirtual.edu.co
Annie Yorley Lopez Duque
aylopezd@unadvirtual.edu.co
Daniel Sebastián Salamandra Perea
dssalamandrap@unadvirtual.edu.co

RESUMEN**:** *Este documento ofrece una guía detallada para instalar, configurar y verificar la seguridad de una instancia de Endian Firewall en un entorno virtual creado con VirtualBox. A lo largo del contenido se explican aspectos fundamentales como la asignación de interfaces de red, la creación de reglas NAT para permitir el acceso a Internet desde la LAN y la DMZ, la definición de políticas de seguridad entre zonas, la activación de servicios controlados dentro de la DMZ y la configuración de un proxy HTTP con funciones de autenticación y filtrado de contenidos. Esta propuesta emula una arquitectura de red empresarial enfocada en la seguridad perimetral mediante segmentación de tráfico y control de accesos entre zonas.*

PALABRAS CLAVE: DMZ, Firewall, HTTP, LAN, NAT.

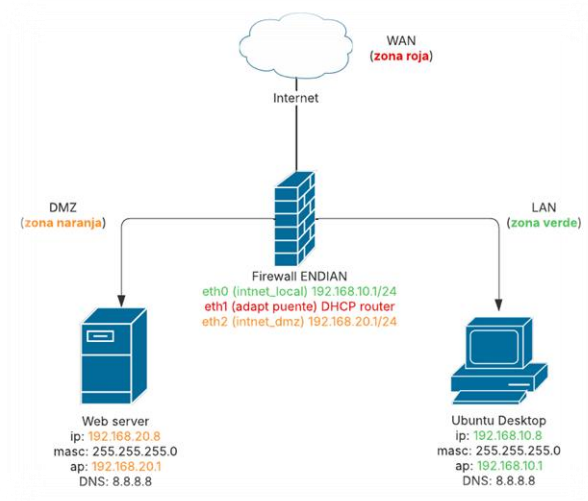
1 INTRODUCCIÓN

En una red, la protección y seguridad son fundamentales para resguardar la integridad de los datos. Endian Firewall se presenta como una solución de código abierto que permite implementar funciones avanzadas de seguridad en infraestructuras segmentadas. Este artículo tiene como objetivo guiar, paso a paso, la instalación y configuración de Endian Firewall en un entorno virtualizado con VirtualBox, replicando un escenario empresarial con zonas perimetrales donde se implementará, a través de la segmentación y políticas de acceso, una postura de seguridad robusta para cualquier organización.

2 PROPUESTA DE RED

Se propone la siguiente segmentación de red para la implementación de las zonas: Verde (LAN), Roja (WAN) y Naranja (DMZ). Ver **Figura 1.**

Figura 1. Segmentación de red



Fuente: Elaboración propia

2.1 CONFIGURACIÓN DE ENDIAN

Crear una VM en VirtualBox con los siguientes requerimientos:

- 3 GB de RAM.
- 8 GB de disco.
- mínimo 4CPU.

Posteriormente, cargar la imagen ISO del sistema operativo Endian descargada del repositorio: https://sourceforge.net/projects/efw/. Antes de iniciar la VM, se deben configurar las tarjetas de red con los parámetros que se proponen en la **Tabla 1**.

Tabla 1. Tarjetas de red Endian

# Tarjeta de red	Tipo	Zona designada
1	Adaptador puente	Zona roja
2	Red interna	Zona verde
3	Red interna	Zona Naranja

Fuente: Elaboración propia

Al iniciar la VM Endian, la primera opción de configuración que solicita el SO será asignar la IP para la zona

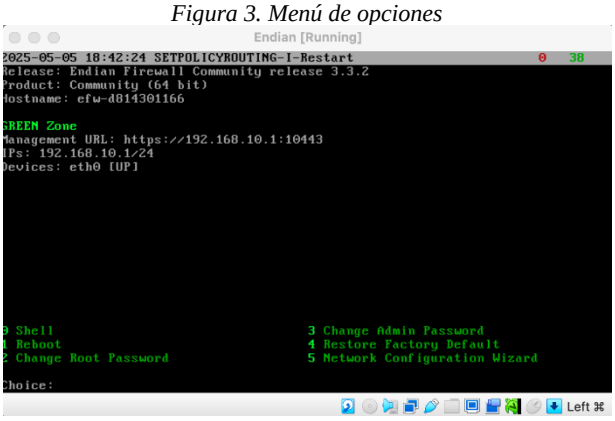
verde, que corresponde a la IP 192.168.10.1 y máscara de red 255.255.255.0 de acuerdo con la propuesta de red **Figura 1**.

Figura 2. Zona verde

Fuente: Elaboración propia

Por consiguiente, Endian arroja la pantalla de opciones **Figura 3**. Donde se debe elegir la opción número 5 (Network Configuration Wizard). Allí, solicitará los datos necesarios de parametrización para las tarjetas asignadas en las zonas (roja y naranja). Una vez se finalice la configuración, se mostrarán un resumen de la información de configuración para confirmar. En este punto, Endian se encuentra listo para recibir peticiones y puede ser accedido por medio de la interfaz de administración con la url: https://192.168.10.1:10443 desde cualquier navegador en la VM Ubuntu Desktop.

Figura 3. Menú de opciones



Fuente: Elaboración propia

2.2 CONFIGURACIÓN VM'S HOST

Para este ejercicio, se trabajará con 2 VM previamente creadas, que corresponden a un Ubuntu Desktop (maquina host trabajando en la zona verde) y un WebServer (maquina host trabajando en la zona naranja). Estas 2 máquinas deben ser configuradas según la segmentación de red **Figura 1**.

2.3 PRUEBAS DE COMUNICACIÓN

En el panel de administración de Endian, /firewall/Inter-Zone traffic, revisar que todas las reglas de comunicación se encuentren creadas y activas, de lo contrario, se deben crear como se muestra en la **Figura 4**.

Figura 4. Reglas de comunicación Endian

Fuente: Elaboración propia

Una vez se configuren las reglas, en el menú "Status" en la sección ARP table entries (entradas de la tabla de Protocolo de Resolución de Direcciones), se puede validar que las maquinas VM de las zonas verde y naranja se encuentren detectadas **Figura 5**.

Figura 5. Table entries

Fuente: Elaboración propia

Por último, ejecutar las siguientes pruebas de comunicación desde cada una de las VM:

Ubuntu Desktop:

- Ejecutar un ping hacia la puerta de enlace 192.168.10.1 (Endian).
- Ejecutar un ping hacía la IP 192.168.20.8 (VM web Server).
- Navegar a cualquier sitio web para confirmar salida a internet.

Web Server:

- Ejecutar un ping hacia la puerta de enlace 192.168.20.1 (Endian).
- Ejecutar un ping hacía la IP 192.168.10.8 (VM Ubuntu Desktop).
- Ping a cualquier URL, por ejemplo https://apple.com

Si las pruebas son exitosas, la configuración de Endian, ha finalizado, de lo contrario, repasar la segmentación de red **Figura 1**.

3 CONFIGURACIÓN NAT

La Traducción de Direcciones de Red (NAT, por sus siglas en inglés) es una técnica que permite a múltiples dispositivos en una red privada acceder a redes públicas, como Internet, utilizando una única dirección IP pública. En el contexto de Endian Firewall Community 3.3.2, la configuración de NAT se realiza principalmente a través de la sección "**Firewall > Outgoing Traffic",** donde se definen las reglas que permiten o

restringen el tráfico saliente desde las diferentes zonas de la red hacia la Zona Roja (Internet).

3.1 CONFIGURACIÓN DE REGLAS DE TRÁFICO SALIENTE

Para habilitar el acceso a Internet desde la red LAN (Zona Verde), se deben seguir los siguientes pasos:

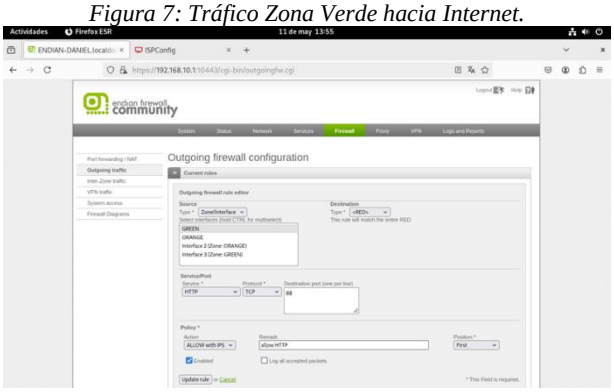
Acceder a la interfaz web de administración de Endian Firewall a través de un navegador ver **Figura 6**, utilizando la dirección IP asignada a la interfaz de la Zona Verde, https://192.168.10.1:10443**.** Ver **Figura 7.**

Figura 6: Interfaz Endian Firewall

Fuente: Elaboración propia

Navegar a la sección "Firewall" y seleccionar "Outgoing Traffic"

Figura 7: Tráfico Zona Verde hacia Internet.



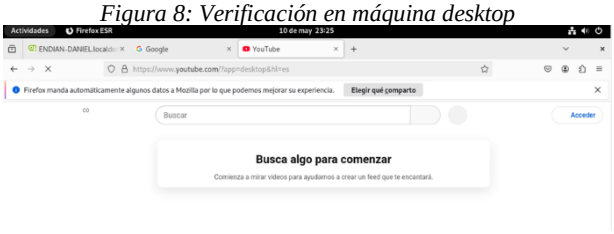
Fuente: Elaboración propia

Agregar una nueva regla de tráfico saliente con los siguientes parámetros:

- Origen: Zona Verde.
- Destino: Zona Roja.
- Servicios: HTTP (puerto 80) y HTTPS (puerto 443).
- Acción: Permitir (Allow).

Se guarda la regla y se aplican los cambios. Ver **Figura 8**. Esta configuración permite que los dispositivos en la red LAN accedan a servicios web en Internet, manteniendo un control sobre los protocolos permitidos y reforzando la seguridad de la red interna.

Figura 8: Verificación en máquina desktop



Fuente: Elaboración propia

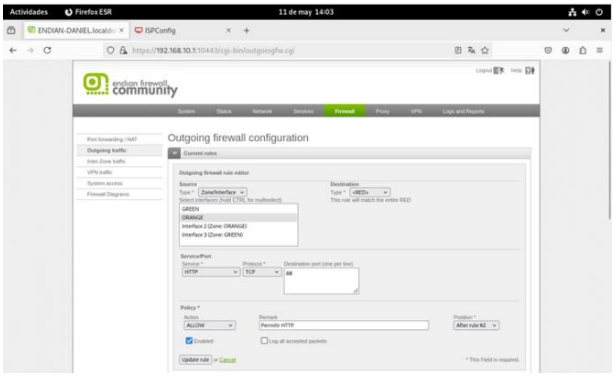
3.2 CONFIGURACIÓN DE REGLAS DE TRÁFICO SALIENTE PARA LA ZONA NARANJA (DMZ)

Para habilitar el acceso a Internet desde la red DMZ (Zona Naranja), se deben seguir pasos similares a los descritos anteriormente:

Acceder a la interfaz web de administración de Endian Firewall. Navegar a la sección "Firewall" y seleccionar "Outgoing Traffic". Agregar una nueva regla de tráfico saliente (ver **Figura 9**) con los siguientes parámetros:

- Origen: Zona Naranja.
- Destino: Zona Roja.
- Servicios: HTTP (puerto 80) y HTTPS (puerto 443).
- Acción: Permitir (Allow).

Figura 9: Configuración de salida para la Zona Naranja hacia la WAN.



Fuente: Elaboración propia

Crear la regla y aplicar los cambios realizados. Esta configuración permite que los servidores ubicados en la DMZ accedan a Internet para, por ejemplo, actualizar paquetes o sincronizar servicios, manteniendo un control sobre los protocolos permitidos y reforzando la seguridad de la red interna. Se evidencia la conectividad a Internet desde el servidor en la DMZ como se observa en la **Figura 10**.

Figura 10: Conectividad a Internet desde el servidor en la DMZ.

Fuente: Elaboración propia

3.3 CONFIGURACIÓN DE REGLAS DE TRÁFICO ENTRE ZONAS (INTER-ZONE TRAFFIC)

Además de controlar el acceso a Internet, es fundamental gestionar el tráfico entre las diferentes zonas de la red para mantener una arquitectura segura y funcional. En Endian Firewall, esto se realiza a través de la sección "Firewall > Inter-Zone Traffic", cómo se muestra en la **Figura 11**, donde se pueden definir reglas específicas para permitir o restringir la comunicación entre zonas internas, como la Zona Verde (LAN) y la Zona Naranja (DMZ).

Para permitir el acceso desde la Zona Verde a servicios específicos en la Zona Naranja, se deben seguir los siguientes pasos.

Figura 11: Creación de reglas para tráfico.

Fuente: Elaboración propia

Acceder a la interfaz web de administración de Endian Firewall. Navegar a la sección "Firewall" y seleccionar "Inter-Zone Traffic". Agregar una nueva regla de tráfico interzonal con los siguientes parámetros:

- Origen: Zona Verde.
- Destino: Zona Naranja.
- Servicios: Especificar los servicios necesarios, como HTTP, HTTPS, FTP, etc.
- Acción: Permitir (Allow).

Guardar la regla y aplicar. Estas configuraciones aseguran que los dispositivos en la LAN puedan acceder a los servicios necesarios en la DMZ, mientras que se previene el acceso no autorizado desde la DMZ hacia la LAN, manteniendo una estructura de red segura y controlada. Ver **Figura 12**.

Figura 12: Acceso desde la LAN hacia la DMZ

Fuente: Elaboración propia

4 PERMITIR SERVICIOS EN LA ZONA DESMILITARIZADA (DMZ)

Es posible realizar la configuración para permitir servicios en la zona desmilitarizada o DMZ, para efectos de este artículo se trabajará con los servicios HTTP permitiendo el uso del puerto 80 y FTP usando el puerto 21. También se realizará la demostración para denegar un servicio, en esta ocasión será ICMP usando el puerto 8 y 30.

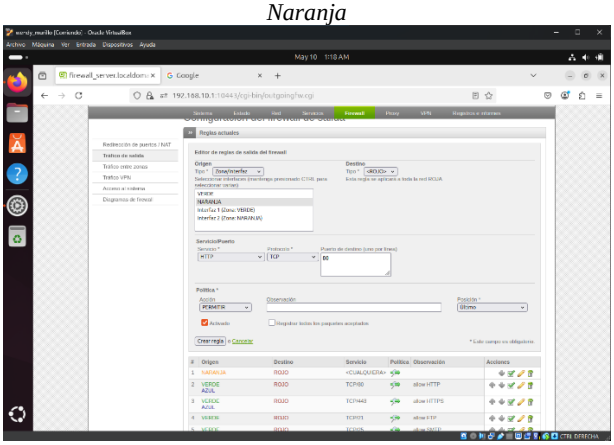
4.1 PERMITIR HTTP (PUERTO 80)

Para permitir el servicio HTTP por el puerto 80 ingresaremos a la administración de Endian desde el cliente desktop por medio de la url: 192.168.10.1:10443. Una vez se ha realizado el proceso de login, dirigirse al menú “Firewall” y seleccionar la opción “Trafico de salida”, ver **Figura 13**. Allí realizaremos las siguientes configuraciones para crear una regla nueva:

- Origen - Tipo: Zona/Interfaz
- Zona: Naranja
- Destino – Tipo: Rojo
- Servicio: HTTP
- Protocolo: TCP
- Puerto de destino: 80
- Política – Acción: Permitir
- Marcar la casilla “Activado”

Los demás campos se dejarán como vienen por defecto. Tal como se observa en la imagen a continuación:

Figura 13. Habilitar el protocolo HTTP desde la zona Naranja



Fuente: Elaboración propia

Una vez realizada la configuración, guardar los cambios y reiniciar el servidor Endian.

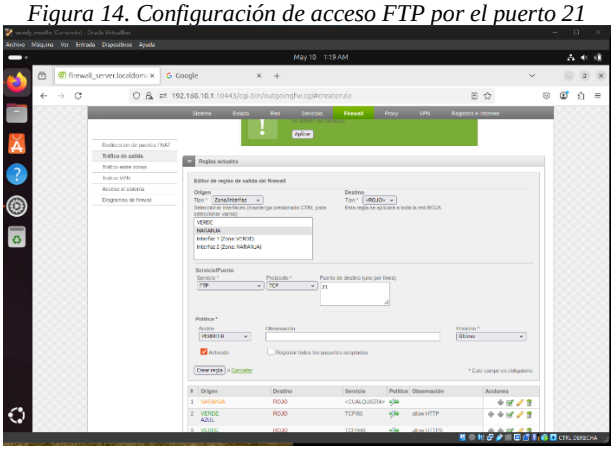
4.2 PERMITIR FTP (PUERTO 21)

Para realizar la configuración que permita el servicio FTP por el puerto 21, se debe permanecer en el menú "Firewall" y en la opción "Trafico de salida" seleccionada anteriormente en la administración de Endian. Seleccionar "Crear una nueva regla y realizar las siguientes configuraciones":

- Origen - Tipo: Zona/Interfaz
- Zona: Naranja
- Destino – Tipo: Rojo
- Servicio: FTP
- Protocolo: TCP
- Puerto de destino: 21
- Política – Acción: Permitir
- Marcar la casilla "Activado"

Los demás campos se dejarán por defecto como se aprecia en la **Figura 14**.

Figura 14. Configuración de acceso FTP por el puerto 21



Fuente: Elaboración propia

Una vez realizada la configuración, guardar los cambios y reiniciar el servidor Endian.

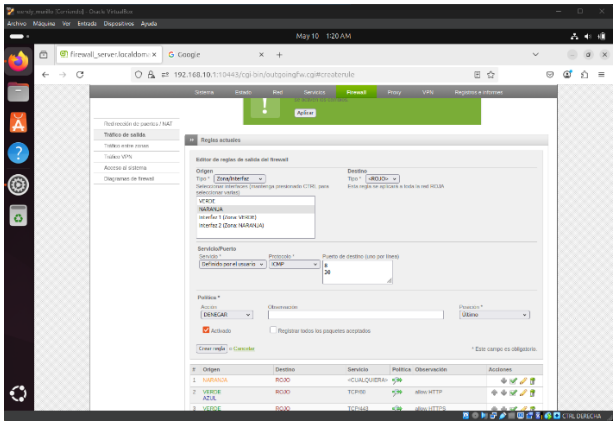
4.3 DENEGAR ICMP (PUERTO 8 y 30)

Para denegar el servicio ICMP por el puerto 8 y el puerto 30 es necesario regresar a la administración de Endian, dirigirse al menú "Firewall" y bajo la opción "Trafico de salida" (ver **Figura 15**) crear una nueva regla con las siguientes configuraciones:

- Origen - Tipo: Zona/Interfaz
- Zona: Naranja
- Destino – Tipo: Rojo
- Servicio: Definido por el usuario
- Protocolo: ICMP
- Puerto de destino (uno por línea): 8 y 30
- Política – Acción: Denegar
- Marcar la casilla "Activado"

Los demás campos se guardan con su valor por defecto. Así:

Figura 15. Configuración para denegar tráfico ICMP desde la DMZ



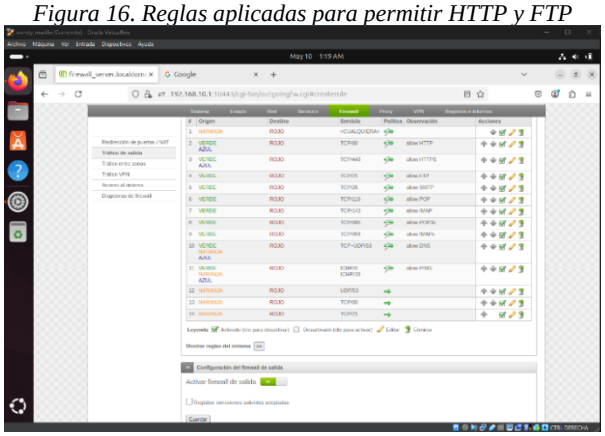
Fuente: Elaboración propia

Una vez realizada la configuración, guardar los cambios y reiniciar el servidor Endian.

4.4 COMPROBACIÓN EN EL TRAFICO DE SALIDA

En la **Figura 16** y **Figura 17** se observa la creación de las reglas en el tráfico de salida:

Figura 16. Reglas aplicadas para permitir HTTP y FTP



Fuente: Elaboración propia

Figura 17. Regla que bloquea el protocolo ICMP

Fuente: Elaboración propia

4.5 PRUEBAS DESDE EL SERVIDOR EN LA ZONA DMZ

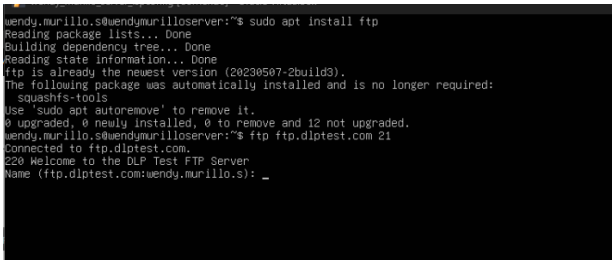
Para probar el protocolo http se usa el comando "curl http://google.com" (ver **Figura 18**) o también se puede comprobar el acceso con el comando "sudo apt update":

Figura 18. Prueba exitosa de HTTP mediante curl

Fuente: Elaboración propia

Ahora bien, para probar FTP realizamos la instalación con el comando "sudo apt ftp" y ejecutamos una prueba a un servidor FTP público por el puerto 21. Si el servidor responde quiere decir que la regla está funcionando correctamente cómo se confirma en la **Figura 19**.

Figura 19. Ejecución de prueba de conexión a un servidor FTP



Fuente: Elaboración propia

Finalmente, Para probar que ICMP está denegando correctamente se puede intentar hacemos un ping y se confirma el bloqueo de tráfico.

Figura 20. Bloqueo de tráfico ICMP desde el servidor DMZ

Fuente: Elaboración propia

Se puede observar en la **Figura 20** que el ping no logro conectarse, por lo que fue denegado el servicio correctamente.

5 CONFIGURACIÓN DE ACCESO ENTRE ZONAS Y PRUEBAS DE SERVICIOS

Esta temática del laboratorio se centra en el establecimiento de políticas de seguridad entre zonas, específicamente en la creación de reglas para permitir o restringir el tráfico de servicios HTTP y FTP entre la LAN, la DMZ y la WAN. Este proceso incluye tanto la configuración de reglas de firewall como la validación funcional de los accesos.

5.1 REGLAS DE ACCESO ENTRE ZONAS

Desde la consola de administración de Endian, en el módulo Firewall, Tráfico entre Zonas (Inter-Zone Firewall), se configuraron reglas para permitir el tráfico desde la zona verde (LAN) hacia la zona naranja (DMZ) mediante los servicios HTTP (puerto 80) y FTP (puerto 21). Asimismo, se habilitó el tráfico desde la zona WAN hacia la DMZ utilizando redirección de puertos (DNAT).

Para ello, se creó una regla de NAT que redirige las solicitudes recibidas en la interfaz WAN de Endian (IP: 192.168.1.23) al servidor web en la DMZ (192.168.20.8) a través del puerto 80. De igual forma, se configuró una segunda regla para redirigir el puerto 21 hacia el mismo servidor, permitiendo conexiones FTP externas. Estas reglas fueron verificadas en el panel de tráfico inter-zona, donde se confirmó su activación y correcta aplicación.

5.2 VERIFICACIÓN DE REGLAS Y CONECTIVIDAD ENTRE ZONAS

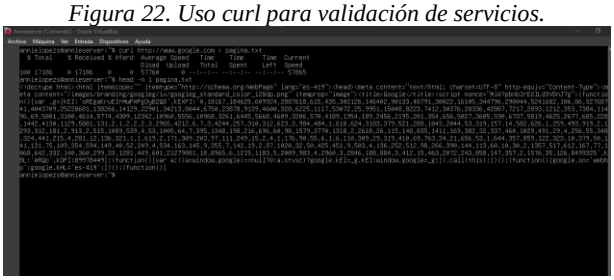
A continuación, se realizaron pruebas específicas de conectividad (ver **Figura 21**) y acceso a servicios para cada uno de los flujos de tráfico requeridos.

Figura 21. verifica visualmente la activación de reglas en el tráfico entre zonas

Fuente: Elaboración propia

Para las pruebas se emplearon herramientas como curl, navegadores web y el comando ftp desde diferentes dispositivos. En todos los casos, se logró una comunicación efectiva, cómo se demuestra en la **Figura 22** la correcta implementación de las políticas de seguridad.

Figura 22. Uso curl para validación de servicios.

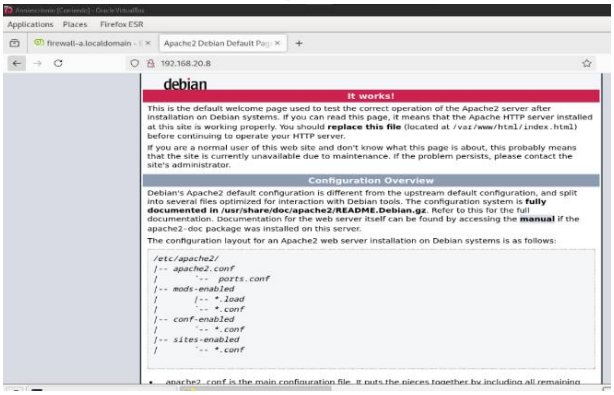


Fuente: Elaboración propia

5.3 EVIDENCIAS FUNCIONALES

Se accedió exitosamente al servidor web desde el escritorio ubicado en la zona verde mediante http://192.168.20.8. Ver **Figura 23**.

Figura 23. Acceso HTTP desde la zona Verde al servidor de la DMZ



Fuente: Elaboración propia

6 IMPLEMENTACIÓN DE UN PROXY HTTP CON POLÍTICAS DE AUTENTICACIÓN

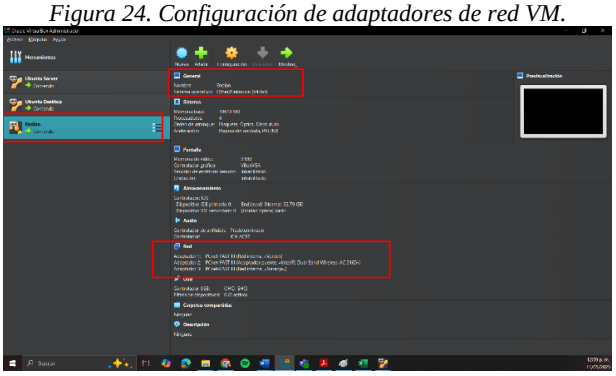
En el marco del presente trabajo, se llevó a cabo la implementación de un servidor proxy HTTP (no transparente) con políticas de autenticación para controlar la navegación en Internet, utilizando la plataforma de firewall Endian. Este proceso se desarrolló en un entorno de red virtualizado, conformado por tres máquinas virtuales gestionadas mediante Oracle VirtualBox: Ubuntu Server, Ubuntu Desktop y Endian Firewall.

6.2 CONFIGURACIÓN DEL ENTORNO VIRTUAL

Cada máquina fue configurada con interfaces de red específicas (ver **Figura 24**), estableciendo una topología controlada para pruebas:

- **Interfaz GREEN** (Red interna segura): 192.168.10.1/24 – asignada al firewall Endian.
- **Interfaz RED** (Conexión a Internet): configurada como adaptador en modo puente.
- **Interfaz ORANGE** (Zona desmilitarizada - DMZ): 192.168.20.1/24.

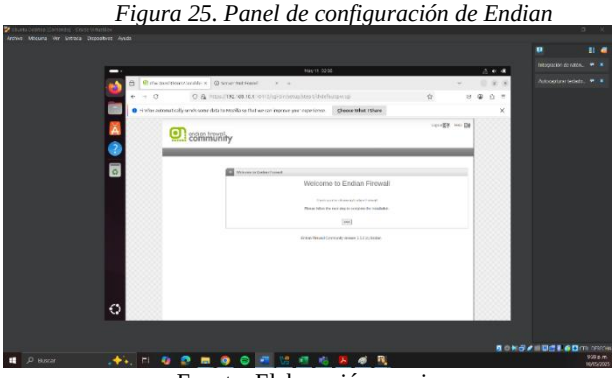
Figura 24. Configuración de adaptadores de red VM.



Fuente: Elaboración propia

La instalación de Endian se completó accediendo a su interfaz web mediante la dirección https://192.168.10.1:10443 (ver **Figura 25**), desde la estación de trabajo Ubuntu Desktop. Una vez dentro del sistema, se validaron las direcciones MAC asignadas, hostname y credenciales de acceso configuradas previamente.

Figura 25. Panel de configuración de Endian



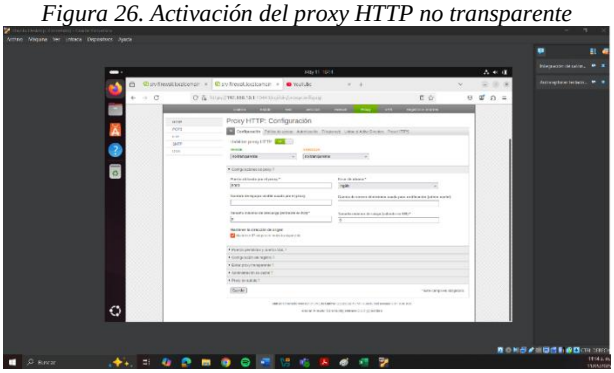
Fuente: Elaboración propia

6.3 HABILITACIÓN DEL PROXY Y CREACIÓN DE POLÍTICAS

Se activó el servicio de **proxy HTTP en modo no transparente** (ver **Figura 26**), permitiendo la interceptación de tráfico saliente mediante configuración explícita en los clientes. En el proxy se definió un perfil de filtrado web denominado *BloqueoSitios*, el cual restringía el acceso a los siguientes dominios: www.hotmail.com , www.youtube.com y www.elnuevodia.com.co.

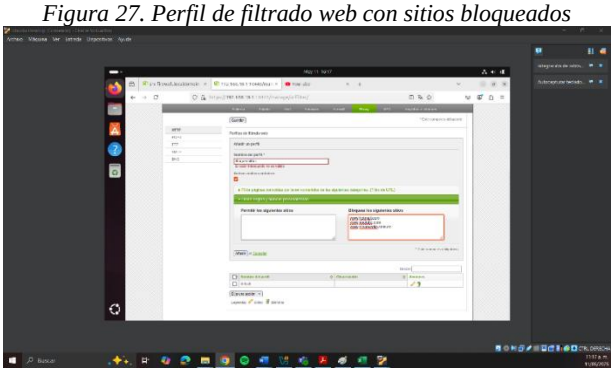
Adicionalmente, se configuró un sistema de autenticación basado en grupos y usuarios. Se creó el grupo grupo1 y el usuario usuario1, cómo se observa en la **Figura 27** y **Figura 28**, aplicando una política de control de acceso vinculada al perfil de filtrado, habilitada únicamente bajo autenticación.

Figura 26. Activación del proxy HTTP no transparente



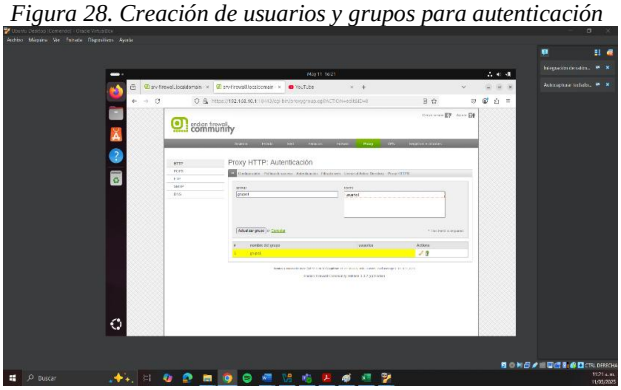
Fuente: Elaboración propia

Figura 27. Perfil de filtrado web con sitios bloqueados



Fuente: Elaboración propia

Figura 28. Creación de usuarios y grupos para autenticación



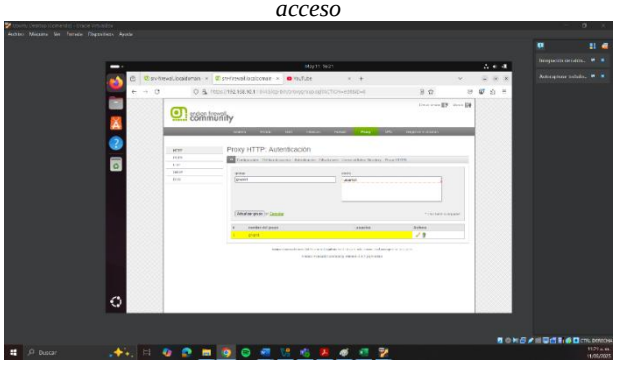
Fuente: Elaboración propia

6.4 VALIDACIÓN DE POLÍTICAS EN EL CLIENTE

Desde la estación Ubuntu Desktop, se configuró el navegador Mozilla Firefox para utilizar el proxy HTTP definido. Al intentar acceder a servicios web, se solicitó la autenticación del usuario previamente creado, confirmando la correcta aplicación de las políticas. Ver **Figura 29** y **Figura 30**.

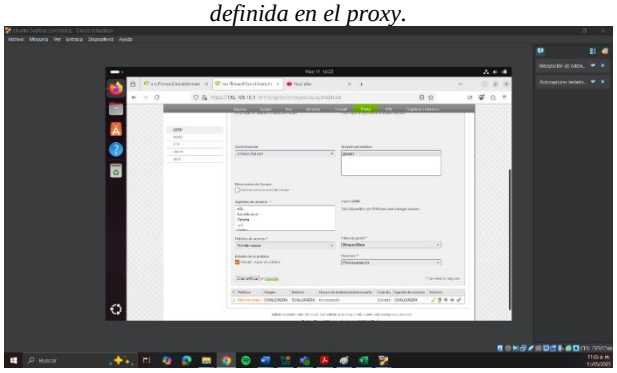
Las pruebas de validación demostraron que las páginas listadas en el perfil de filtrado fueron efectivamente bloqueadas, mientras que el resto del tráfico web se mantuvo accesible, garantizando así la funcionalidad del sistema proxy con control de autenticación por usuario.

Figura 29. Configuración de usuarios para el control de acceso



Fuente: Elaboración propia

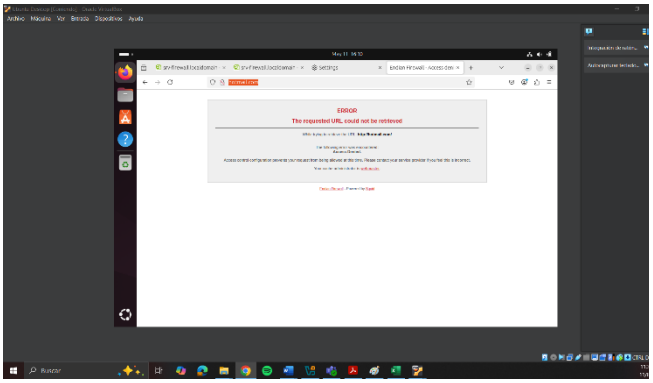
Figura 30. Política de acceso basada en autenticación definida en el proxy.



Fuente: Elaboración propia

La implementación del proxy HTTP con autenticación en un entorno virtualizado evidenció la viabilidad de controlar el acceso a contenidos en Internet mediante políticas centralizadas, sin afectar la experiencia general de navegación para los usuarios autorizados, cómo se muestra en la **Figura 31**. Este tipo de soluciones resulta especialmente útil para entornos académicos o corporativos donde se requiere restringir el acceso a ciertos contenidos sin comprometer la conectividad global.

Figura 31. Resultado exitoso del bloqueo de sitios web no autorizados.



Fuente: Elaboración propia

7 CONCLUSIONES

1. La implementación de las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ) en Endian Firewall permitió comprender la importancia de la segmentación de redes como mecanismo fundamental para el control del tráfico y la mitigación de riesgos de seguridad. Esta arquitectura facilita la aplicación de políticas diferenciadas para cada zona, mejorando la postura defensiva del sistema.
2. La configuración de reglas NAT demostró cómo es posible traducir direcciones privadas a públicas y viceversa, habilitando la comunicación controlada entre zonas internas y externas. Asimismo, el reenvío de puertos permitió exponer servicios específicos de la DMZ a Internet de forma segura y controlada.
3. A través de la creación de reglas de acceso, se evidenció cómo Endian Firewall permite permitir o denegar el tráfico entre zonas según protocolos, direcciones IP y puertos. Esta capacidad refuerza el principio de mínimo privilegio y permite limitar la superficie de exposición de servicios críticos.
4. La configuración de un proxy HTTP no transparente con autenticación por usuario permitió implementar filtros de contenido y políticas de navegación específicas. Esta práctica facilitó la comprensión de herramientas modernas de administración del uso de Internet, orientadas tanto a la seguridad como al cumplimiento de políticas organizacionales.
5. Las distintas pruebas realizadas, como el bloqueo de sitios web, la denegación de ICMP y el acceso controlado entre zonas, reforzaron la importancia de verificar constantemente la efectividad de las políticas de red. El monitoreo del tráfico en tiempo real validó el correcto funcionamiento de las reglas configuradas, lo cual es esencial en entornos de producción.

8 CITAS Y/O REFERENCIAS

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

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

[3] Endian. (s.f.). *Proxy Configuration Guide*. https://docs.endian.com/3.3/utm/proxy.html

[4] Endian. (s.f.). *The Firewall Menu - Endian UTM 3.2 Reference Manual*. https://docs.endian.com/3.2/utm/firewall.html

[5] Guijarro, A. Jiménez, J. Tapia, J. Viteri, X. Zambrano, J. (2018, enero). *Guía de prácticas de Endian*. Compas. http://142.93.18.15:8080/jspui/bitstream/123456789/55/1/Guia%20practicas%20endian.compressed.pdf

[6] Koromicha. (2024, julio 25). *Install and Configure Endian Firewall on VirtualBox*. Kifarunix. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/

[7] Jiménez, J. (2024, octubre 3). *Qué es NAT y cómo actúa en nuestra red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

[8] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server*. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[9] Linux Professional Institute. (s.f.). *LPIC-1 Exam 101*. https://learning.lpi.org/es/learning-materials/101-500/

[10] Linux Professional Institute. (2022). *Tema 102: Comandos GNU y Unix*. https://learning.lpi.org/es/learning-materials/101-500/102/

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

[12] Squid-cache.org. (s.f.). Squid: Configuration Guide – Authentication. https://wiki.squid-cache.org/ConfigExamples/Authenticate