IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE ENDIAN FIREWALL

Anderson Estiven Muñoz Chindioy
e-mail: anderson.munozc@unad.edu.co
Hector Fabio Cruz Perez
e-mail: hfcruzp@unadvirtual.edu.co
Anamaria Valencia Carabali
e-mail: avalenciacarb@unadvirtual.edu.co
Hernan Santiago Duque Orejuela
e-mail: hsduqueo@unadvirtual.edu.co
Oscar Julian Roman Rosero
e-mail: ojromanr@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de una solución de seguridad perimetral en GNU/Linux mediante Endian Firewall Community, desarrollada en un entorno virtualizado con VirtualBox. El trabajo integra cinco temáticas: la instalación de Endian y configuración de interfaces para las zonas Verde, Roja y Naranja; la configuración NAT para permitir comunicación desde LAN y DMZ hacia Internet; la habilitación de servicios HTTP y FTP en la DMZ; la creación de reglas de acceso entre zonas para permitir o denegar tráfico; y la implementación de un proxy HTTP no transparente con autenticación y filtrado de sitios. La validación se realizó mediante pruebas de conectividad, navegación, acceso a servicios, revisión de reglas y comandos de consola. Como resultado, se obtuvo una infraestructura segmentada, funcional y administrable, capaz de controlar el tráfico, proteger los servicios internos y fortalecer la seguridad perimetral en entornos GNU/Linux*

PALABRAS CLAVE: DMZ, Endian Firewall, GNU/Linux, NAT, Seguridad perimetral.

1 INTRODUCCIÓN

La seguridad perimetral en sistemas GNU/Linux permite proteger, segmentar y controlar el tráfico entre diferentes zonas de red, especialmente cuando existen equipos internos, servidores publicados y acceso hacia Internet. En este artículo se presenta el desarrollo de una infraestructura virtualizada basada en Endian Firewall Community, implementada sobre VirtualBox, con el propósito de aplicar controles de seguridad en una red dividida en zona Verde o LAN, zona Roja o WAN y zona Naranja o DMZ.

El trabajo integra las cinco temáticas propuestas para la Etapa 7. En la primera temática se aborda la instalación de GNU/Linux Endian en VirtualBox y la configuración inicial de sus tarjetas de red para separar correctamente las zonas Verde, Roja y Naranja. En la segunda temática se configura NAT para permitir la comunicación de la LAN y de la DMZ hacia la red externa, además de validar reglas de reenvío de puertos. En la tercera temática se habilitan servicios en la zona DMZ, principalmente HTTP y FTP, y se aplican restricciones al tráfico ICMP para controlar las pruebas de ping. En la cuarta temática se definen reglas de acceso entre zonas, permitiendo o denegando tráfico según los servicios requeridos, como HTTP y FTP desde LAN, WAN y DMZ. Finalmente, en la quinta temática se implementa un proxy HTTP no transparente con autenticación de usuarios, grupos, políticas de acceso y bloqueo de sitios específicos.

La metodología utilizada se basa en la configuración práctica de máquinas virtuales, asignación de direcciones IP, creación de reglas de firewall, validación de servicios, pruebas de conectividad y revisión de resultados mediante consola. Esta implementación permite evidenciar el funcionamiento de una arquitectura de seguridad perimetral completa, en la cual Endian actúa como firewall central para administrar la comunicación entre zonas, controlar la salida hacia Internet, proteger los servidores de la DMZ y aplicar políticas de navegación. De esta manera, el artículo consolida los resultados de las cinco temáticas y muestra cómo una solución GNU/Linux puede contribuir a la administración segura de redes en entornos académicos o empresariales.

2 OBJETIVOS DEL PROYECTO

2.1 OBJETIVO GENERAL

Implementar una solución de seguridad perimetral basada en GNU/Linux Endian Firewall Community en un entorno virtualizado, configurando zonas de red, NAT, servicios en DMZ, reglas de acceso y proxy HTTP, con el fin de controlar el tráfico entre LAN, WAN y DMZ, proteger los servicios internos y validar el funcionamiento de la infraestructura mediante pruebas técnicas.

2.2 OBJETIVOS ESPECIFICOS

- Configurar la instancia de GNU/Linux Endian en VirtualBox, asignando correctamente las interfaces de red para las zonas Verde, Roja y Naranja.
- Implementar reglas NAT que permitan la comunicación desde la red LAN hacia la WAN y desde la zona DMZ hacia Internet.
- Habilitar y validar servicios en la zona DMZ, como HTTP y FTP, garantizando su funcionamiento desde los segmentos autorizados.

- Configurar reglas de acceso entre zonas para permitir o denegar tráfico según los protocolos y puertos requeridos en la actividad.
- Aplicar restricciones de tráfico, incluyendo el control del protocolo ICMP, para validar políticas de bloqueo y seguridad en la red.
- Implementar un proxy HTTP no transparente con autenticación de usuarios y políticas de filtrado para controlar la navegación web.
- Verificar el funcionamiento de la infraestructura mediante pruebas de conectividad, navegación, acceso a servicios y revisión de reglas desde la consola de Endian.

3 METODOLOGÍA

La metodología se desarrolló mediante un laboratorio virtual en VirtualBox, utilizando GNU/Linux Endian Firewall Community como plataforma de seguridad perimetral. El procedimiento se organizó según las cinco temáticas propuestas en la actividad.

En la Temática 1, se realizó la instalación de Endian en VirtualBox y la configuración de sus tarjetas de red, asignando una interfaz para la zona Verde o LAN, una para la zona Roja o WAN y una para la zona Naranja o DMZ. Esta fase permitió establecer la base de la infraestructura de red.

En la Temática 2, se configuró NAT para permitir la comunicación desde la LAN hacia Internet y desde la DMZ hacia la red externa. También se validó el reenvío de puertos mediante reglas de Destination NAT hacia un servidor ubicado en la zona DMZ.

En la Temática 3, se habilitaron servicios en la DMZ, principalmente HTTP y FTP, y se aplicaron restricciones al protocolo ICMP para comprobar el bloqueo de tráfico no permitido dentro de la red.

En la Temática 4, se crearon reglas de acceso entre zonas para permitir o denegar tráfico según el origen, destino, protocolo y puerto, validando la comunicación entre LAN, WAN y DMZ de forma controlada.

En la Temática 5, se implementó un proxy HTTP no transparente con autenticación de usuarios, grupos y políticas de filtrado, incluyendo el bloqueo de sitios web definidos en la actividad.

Finalmente, se realizaron pruebas de conectividad, navegación, acceso a servicios y validación de reglas mediante herramientas como ping, curl, systemctl e iptables, con el fin de comprobar el correcto funcionamiento de la infraestructura implementada.

4 DESARROLLO DEL CONTENIDO

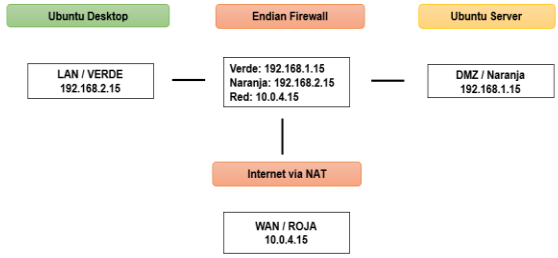
4.1 TEMATICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJEDAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

La seguridad perimetral permite proteger las redes internas mediante el uso de firewalls y zonas segmentadas como LAN, WAN y DMZ. En esta práctica se implementó GNU/Linux Endian sobre VirtualBox para controlar el tráfico y proteger los servicios alojados en un servidor GNU/Linux

4.1.1 ARQUITECTURA DEL SISTEMA

La arquitectura propuesta se basa en el modelo de defensa en profundidad. Se utiliza una topología de "brazo triple" donde el firewall actúa como el vértice de comunicación entre el mundo exterior e interior.

Figura 1.
Esquema de segmentación de red implementado.



Fuente: Autoría Propia

Se definen tres áreas críticas: 1) Zona Verde (LAN) con el más alto nivel de confianza. 2) Zona Roja (WAN) que representa a Internet, sin confianza alguna. 3) Zona Naranja (DMZ) con confianza parcial para servidores públicos.

4.1.2 CONFIGURACIÓN EN VIRTUALBOX

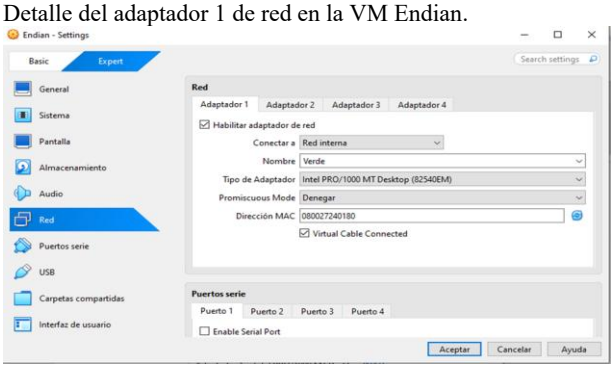
El éxito de la implementación depende de la correcta asignación de interfaces en el hipervisor. Se configuraron tres adaptadores para la VM de Endian.

Tabla 1.
Configuración de las tarjetas de red.

Adaptador	Tipo de Red	Propósito
Adaptador 1	Red interna: Verde	LAN y Gestión
Adaptador 2	Red interna: Naranja	DMZ Servidores
Adaptador 3	NAT	WAN Salida

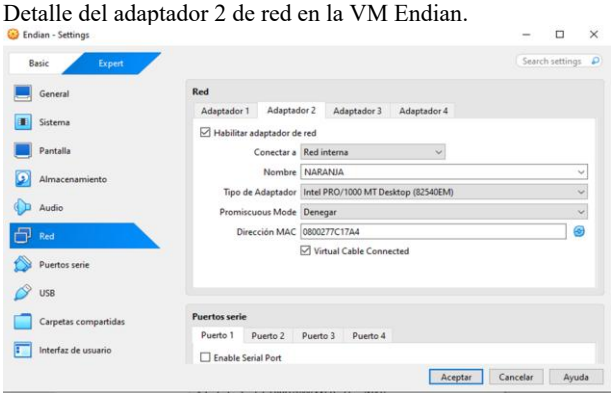
Fuente: Autoría propia

Figura 2.
Detalle del adaptador 1 de red en la VM Endian.



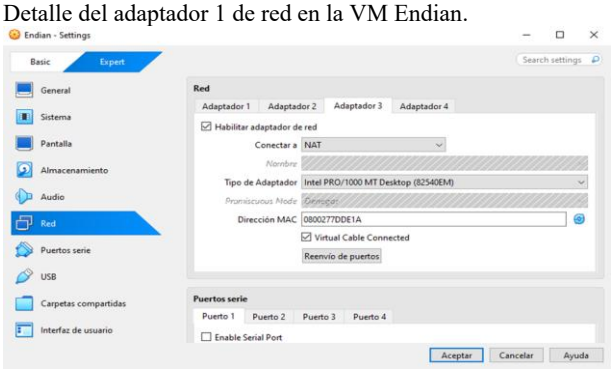
Fuente: Autoría Propia

Figura 3.
Detalle del adaptador 2 de red en la VM Endian.



Fuente: Autoría Propia

Figura 4.
Detalle del adaptador 1 de red en la VM Endian.



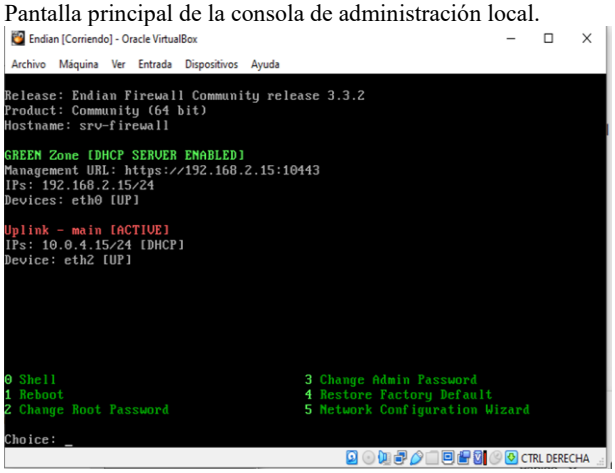
Fuente: Autoría Propia

4.1.3 INSTALACIÓN DE ENDIAN

El proceso de instalación inició con el booteo de la ISO 3.3.2. Durante la fase de configuración de consola, se asignó la dirección IP estática 192.168.2.15 a la interfaz Green.

Es vital destacar que el sistema formatea el disco virtual en sistemas de archivos específicos de Linux, asegurando la integridad de los logs y reportes que se generarán en fases posteriores.

Figura 5.
Pantalla principal de la consola de administración local.



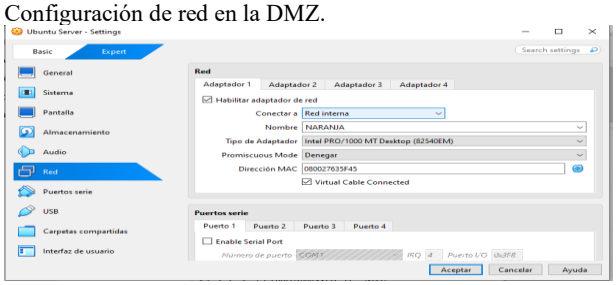
Fuente: Autoría Propia

4.1.4 CONFIGURACIÓN DE SERVICIO Y CIENTES FINALES

DMZ (UBUNTU SERVER)

Se desplegó un servidor Ubuntu con una configuración de red estática. El archivo Netplan fue editado para apuntar al firewall como puerta de enlace predeterminada, asegurando que todo el tráfico sea inspeccionado.

Figura 6.
Configuración de red en la DMZ.

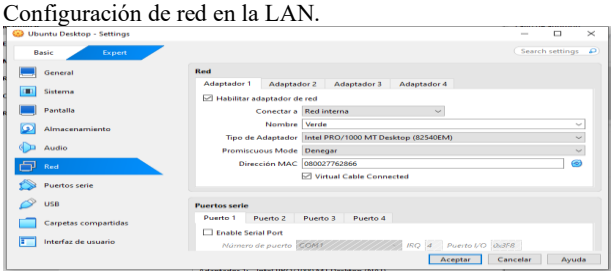


Fuente: Autoría Propia

DMZ (UBUNTU DESKTOP)

Se desplegó un servidor Ubuntu con una configuración de red estática. Conectado a la red Verde. Estación cliente detrás del Endian con acceso controlado a internet, asegurando que todo el tráfico sea inspeccionado.

Figura 7.
Configuración de red en la LAN.



Fuente: Autoría Propia

4.1.5 PRUEBAS Y VALIDACIÓN

Se realizaron pruebas de 'ping' cruzado. Se verificó que el Cliente LAN puede navegar (resolución DNS a través de Endian) y que el Servidor DMZ puede actualizar paquetes desde los repositorios oficiales mediante NAT.

Figura 8.
Evidencia de conectividad hacia la zona roja.

```
anamariavalencia@anamariavalencia-VirtualBox:~$ ping 10.0.4.15
PING 10.0.4.15 (10.0.4.15) 56(84) bytes of data.
From 192.168.2.15 icmp_seq=1 Destination Net Unreachable
From 192.168.2.15 icmp_seq=2 Destination Net Unreachable
From 192.168.2.15 icmp_seq=3 Destination Net Unreachable
From 192.168.2.15 icmp_seq=4 Destination Net Unreachable
```

Fuente: Autoría Propia

Figura 9.
Evidencia de conectividad hacia la zona Verde.

```
anamariavalencia@anamariavalencia-VirtualBox:~$ ping -c4 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
From 192.168.2.16 icmp_seq=1 Destination Host Unreachable
From 192.168.2.16 icmp_seq=2 Destination Host Unreachable
From 192.168.2.16 icmp_seq=3 Destination Host Unreachable
From 192.168.2.16 icmp_seq=4 Destination Host Unreachable
```

Fuente: Autoría Propia

Figura 10.
Evidencia de conectividad hacia la zona Naranja.

```
anamariavalencia@anamariavalencia-VirtualBox:~$ ping -c4 192.168.1.15
PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
64 bytes from 192.168.1.15: icmp_seq=1 ttl=64 time=0.879 ms
64 bytes from 192.168.1.15: icmp_seq=2 ttl=64 time=0.543 ms
64 bytes from 192.168.1.15: icmp_seq=3 ttl=64 time=0.756 ms
64 bytes from 192.168.1.15: icmp_seq=4 ttl=64 time=0.625 ms
```

Fuente: Autoría Propia

4.1.6 PRUEBAS Y VALIDACIÓN

Mediante el protocolo HTTPS en el puerto 10443, se accedió al panel principal. Desde aquí se monitorea el uso de CPU, RAM y el estado de las interfaces de red en tiempo real

Figura 11.
Interfaz gráfica de usuario para la gestión UTM.

Fuente: Autoría Propia

4.2 TEMATICA 2: CONFIGURACIÓN DE NAT Y VALIDACIÓN DE SERVICIOS EN ENDIAN UTM

La práctica se desarrolló en Oracle VirtualBox con tres máquinas: Endian Firewall, Ubuntu Desktop en la LAN y Ubuntu Server en la DMZ. Esta segmentación permite publicar servicios desde la DMZ sin exponer directamente la red interna, aplicando reglas de salida y de redireccionamiento controladas desde Endian.

4.2.1 ARQUITECTURA IMPLEMENTADA

Tabla 2.
Direccionamiento usado en la Temática 2.

Zona	Dirección / uso
GREEN	192.168.2.15 / LAN
ORANGE	192.168.1.15 / DMZ
RED	10.0.4.15 / WAN

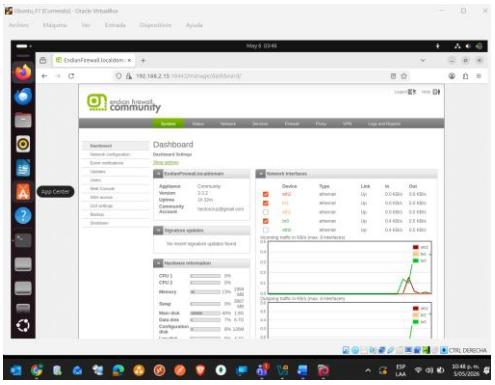
Fuente: Autoría propia.

Endian quedó configurado con GREEN en 192.168.2.15/24, ORANGE en 192.168.1.15/24 y RED en 10.0.4.15/24 por DHCP. En VirtualBox, la LAN se conectó a red_verde, la DMZ a red_naranja y la WAN mediante NAT.

4.2.2 CONFIGURACIÓN Y ACCESO A ENDIAN

En Ubuntu Desktop se configuró IP manual, puerta de enlace 192.168.2.15 y DNS públicos. Con ello se validó la comunicación con la interfaz web de Endian mediante HTTPS en el puerto 10443. El ingreso al panel permitió revisar el estado de las interfaces, las cuales quedaron activas para GREEN, ORANGE y RED.

Figura 12.
Panel de Endian con interfaces activas.



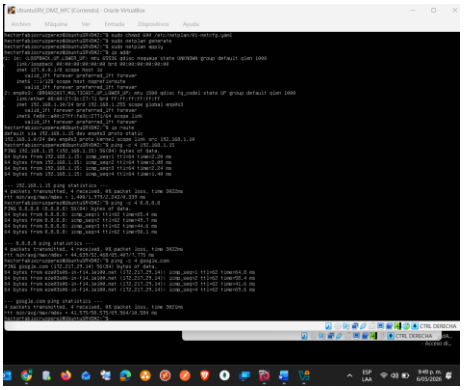
Fuente: Autoría Propia

La salida a Internet desde la LAN se validó mediante ping a 8.8.8.8 y curl hacia google.com. Esta prueba confirmó el funcionamiento del flujo LAN → Endian → RED → Internet.

4.2.3 CONFIGURACIÓN Y ACCESO A ENDIAN

En Ubuntu Server se creó una configuración estática con IP 192.168.1.10/24, puerta de enlace 192.168.1.15 y DNS 8.8.8.8. Inicialmente se validó conectividad con Endian ORANGE y salida por ICMP hacia Internet. La respuesta correcta confirmó el flujo básico desde la DMZ.

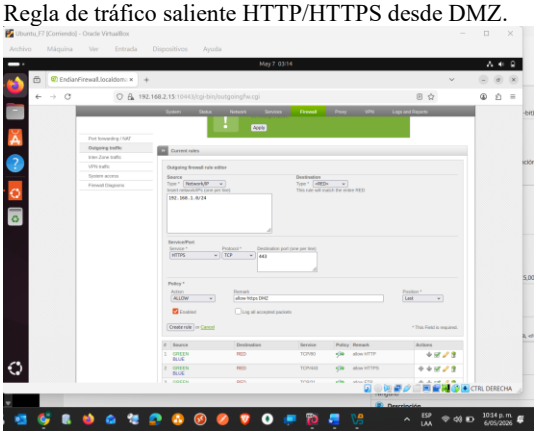
Figura 13.
Pruebas de conectividad desde Ubuntu Server DMZ.



Fuente: Autoría Propia.

Al ejecutar curl hacia google.com se evidenció bloqueo del puerto HTTP desde la zona Naranja. Por ello se crearon reglas de tráfico saliente permitiendo TCP/80 y TCP/443 desde la red 192.168.1.0/24 hacia RED.

Figura 14.
Regla de tráfico saliente HTTP/HTTPS desde DMZ.



Fuente: Autoría Propia

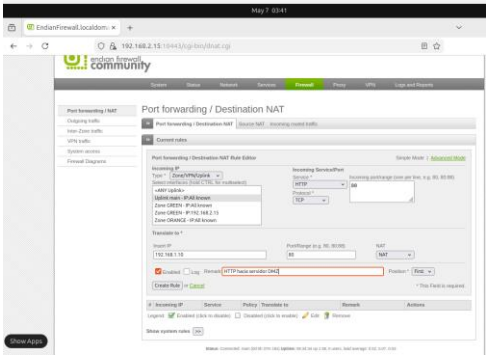
Después de aplicar las reglas, curl respondió correctamente tanto para HTTP como para HTTPS, demostrando que la DMZ podía salir a Internet de forma controlada mediante Endian.

4.2.4 SERVICIO WEB Y PORT FORWARDING

Se instaló Apache2 en el servidor DMZ y se comprobó su estado con systemctl. La prueba local con curl a localhost respondió HTTP/1.1 200 OK, evidenciando que el servicio web estaba activo antes de publicarlo mediante NAT.

Luego se creó una regla de Destination NAT para redirigir el tráfico TCP recibido en la IP RED 10.0.4.15 por el puerto 80 hacia el servidor 192.168.1.10:80. Esta regla permitió publicar el servicio web de la DMZ de manera controlada.

Figura 15.
Port forwarding TCP/80 hacia el servidor DMZ.



Fuente: Autoría Propia

La validación se realizó desde Ubuntu Desktop con curl hacia 192.168.1.10 y hacia 10.0.4.15. Ambas solicitudes respondieron 200 OK, confirmando acceso directo LAN-DMZ y reenvío correcto por la IP RED.

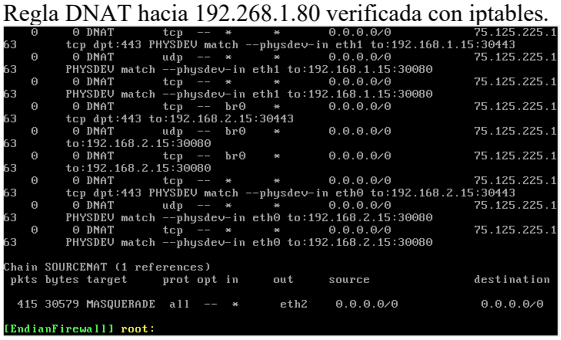
Figura 16.
Respuesta 200 OK desde el servidor DMZ y la IP RED.

Fuente: Autoría Propia.

4.2.5 VERIFICACIÓN DE NAT

Finalmente, en la consola de Endian se ejecutó iptables -t nat -L -n -v. La salida mostró MASQUERADE hacia eth2, interfaz correspondiente a la zona RED, lo que valida el Source NAT para salida a Internet. También se filtró la regla DNAT hacia 192.168.1.10, evidenciando la redirección del puerto 80 hacia Apache en la DMZ.

Figura 17.
Regla DNAT hacia 192.268.1.80 verificada con iptables.



Fuente: Autoría Propia.

4.3 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Actualmente las organizaciones requieren mecanismos de seguridad que permitan proteger la información y los servicios publicados en internet frente a accesos no autorizados y posibles amenazas externas. Una de las estrategias más utilizadas consiste en implementar zonas DMZ (Demilitarized Zone), las cuales permiten aislar servidores públicos de la red interna de la organización.

En esta actividad se implementó un entorno de seguridad perimetral utilizando GNU/Linux Endian como firewall y Ubuntu Server como servidor ubicado en la zona DMZ. El propósito principal fue habilitar los servicios HTTP y FTP dentro de la red, permitiendo el acceso controlado a dichos servicios y restringiendo el protocolo ICMP para evitar respuestas a solicitudes de ping.

4.3.1 CONFIGURACIÓN DE LA INFRAESTRUCTURA

Para el desarrollo de la práctica se utilizó VirtualBox como plataforma de virtualización y un servidor Ubuntu Server físico conectado a la zona ORANGE (DMZ). Se implementó GNU/Linux Endian como firewall principal para administrar el tráfico entre las diferentes redes.

Las direcciones IP utilizadas fueron las siguientes:

Tabla 3.
Direcciones IP utilizadas

Zona	Dirección IP
RED/WAN	DHCP
GREEN/LAN	192.168.2.15
ORANGE/DMZ	192.168.10.1
Ubuntu Server	192.168.10.104

Nota. Esta tabla muestra el direccionamiento IP utilizado para la configuración de la infraestructura en las diferentes zonas utilizadas. Fuente. Autoría Propia

4.3.2 INSTALACIÓN DE APACHE2

Para habilitar el servicio HTTP se instaló Apache2 en Ubuntu Server mediante los siguientes comandos:

```
sudo apt update
sudo apt install apache2 -y
```

Posteriormente se verificó el estado del servicio:

```
sudo systemctl status apache2
```

También se realizaron pruebas de administración del servicio utilizando los comandos:

```
sudo systemctl stop apache2
sudo systemctl start apache2
sudo systemctl restart apache2
```

Finalmente se comprobó que Apache estuviera escuchando en el puerto 80 mediante:

```
sudo ss -tulpn
```

4.3.3 INSTALACIÓN DEL SERVICIO FTP

El servicio FTP fue implementado utilizando VSFTPD. La instalación se realizó con el siguiente comando:

sudo apt install vsftpd -y

Posteriormente se verificó el estado del servicio:

sudo systemctl status vsftpd

También se realizaron pruebas de administración:

sudo systemctl stop vsftpd
sudo systemctl start vsftpd
sudo systemctl restart vsftpd

La verificación del puerto 21 se realizó utilizando:

sudo ss -tulpn

4.3.4 CONFIGURACIÓN DE SEGURIDAD Y BLOQUEO ICMP

Se configuraron reglas de seguridad con el objetivo de permitir los servicios HTTP y FTP y bloquear el protocolo ICMP.

sudo ufw allow 80/tcp
sudo ufw allow 21/tcp

Posteriormente se habilitó el firewall:

sudo ufw enable

Para bloquear solicitudes ICMP se utilizó la siguiente regla:

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

4.3.5 VERIFICACIÓN DE FUNCIONAMIENTO

Se realizaron diferentes pruebas para validar el correcto funcionamiento de la infraestructura implementada.

Desde el navegador web se accedió a:

http://192.168.10.104

En este punto se visualiza correctamente la página de apache2.

Se verificó el funcionamiento del servicio FTP utilizando:

ftp 192.168.10.104

La conexión se establece de manera correcta con el servidor.

Se realizaron pruebas mediante el comando ping:

ping 192.168.10.104

Como resultado, el servidor no respondió a las solicitudes ICMP debido a las reglas de bloqueo implementadas.

4.3.6 RESULTADOS

La implementación permitió establecer correctamente una infraestructura básica de seguridad perimetral utilizando GNU/Linux Endian y Ubuntu Server. Los servicios HTTP y FTP fueron publicados correctamente dentro de la zona DMZ, permitiendo el acceso controlado desde la red.

Las reglas de seguridad implementadas lograron bloquear satisfactoriamente el protocolo ICMP, incrementando la protección del servidor frente a solicitudes externas y las pruebas realizadas permitieron comprobar el correcto funcionamiento de los servicios y la efectividad de las políticas de seguridad configuradas.

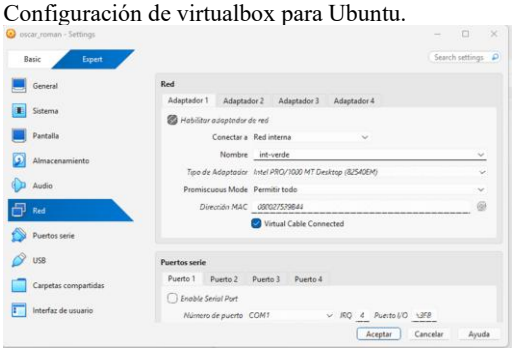
4.4 TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Se espera del laboratorio:

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

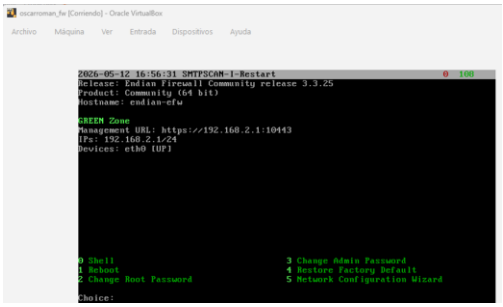
Comunicar la zona Internet con la zona DMZ.

Figura 18.
Configuración de virtualbox para Ubuntu.



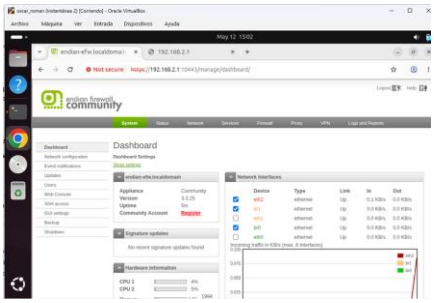
Fuente: Autoría Propia.

Figura 19.
Acceso a Endian mediante 192.168.2.1.



Fuente: Autoría Propia.

Figura 20.
Interfaz de administración.

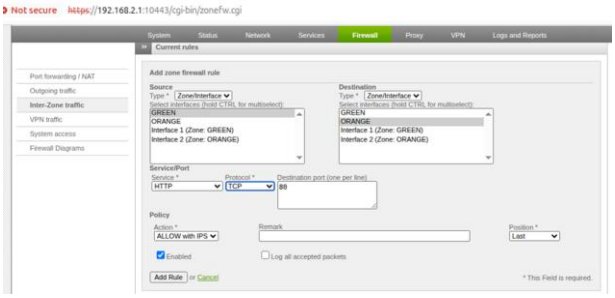


Fuente: Autoría Propia.

4.4.1 PASO A PASO

Comunicar zona verde con naranja (HTTP), mediante la siguiente regla:

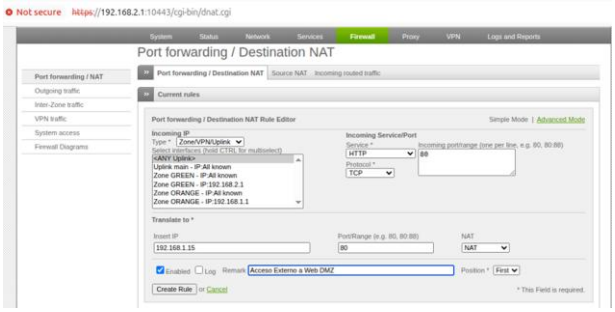
Figura 21.
Regla de comunicación verde a naranja.



Fuente: Autoría Propia.

Comunicar zona roja (internet) con DMZ:

Figura 22.
Regla de comunicación zona roja a DMZ.



Fuente: Autoría Propia.

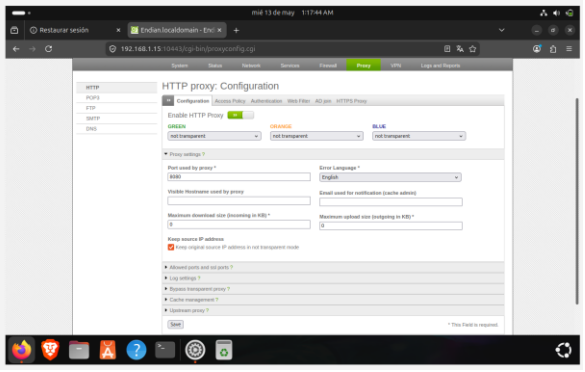
4.5 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLITICAS DE ATENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

4.5.1 IMPLEMENTACIÓN

Para el desarrollo de esta temática se implementó un Proxy HTTP no transparente utilizando GNU/Linux Endian como firewall principal. El objetivo de la práctica consistió en controlar la navegación de los usuarios dentro de la red LAN mediante políticas de autenticación y listas de restricción de contenido.

Inicialmente se habilitó el servicio Proxy HTTP desde la interfaz administrativa de Endian, configurando el modo no transparente para obligar a los usuarios a autenticarse antes de acceder a internet.

Figura 23.
Proxy HTTP No transparente

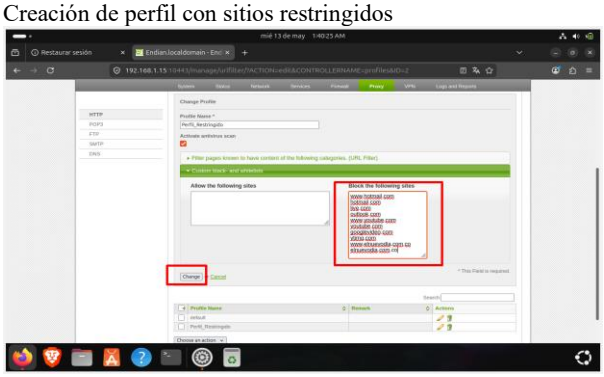


Fuente: Autoría Propia.

Posteriormente se creó un perfil de filtrado web incluyendo una lista negra de sitios restringidos. Los dominios bloqueados fueron los siguientes:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

Figura 24.
Creación de perfil con sitios restringidos



Fuente: Autoría Propia.

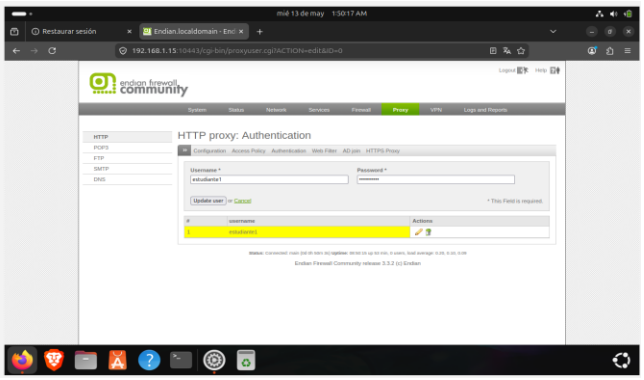
4.5.2 CREACIÓN DE USUARIOS Y POLITICAS DE AUTENTICACIÓN

Con el fin de controlar el acceso a internet, se implementó autenticación por usuario mediante las herramientas administrativas de Endian.

Se creó un usuario asociado a un grupo específico dentro del sistema de autenticación del proxy. Posteriormente se estableció una política de acceso vinculando:

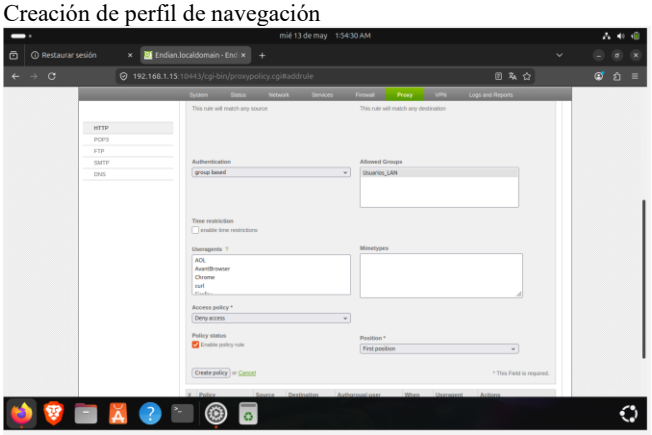
- Grupo de usuarios,
- Perfil de navegación,
- Lista negra configurada anteriormente.

Figura 25.
Creación de usuario local



Fuente: Autoría Propia.

Figura 26.
Creación de perfil de navegación

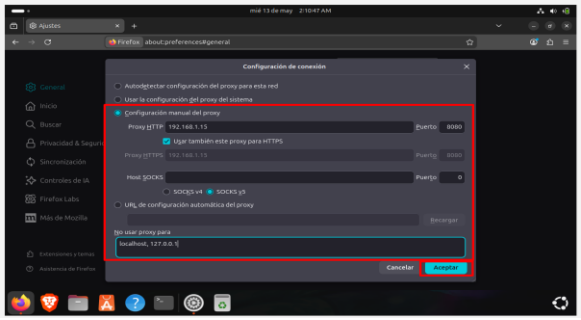


Fuente: Autoría Propia.

4.5.3 VERIFICACIÓN DE FUNCIONAMIENTO

Las pruebas se realizaron desde equipos ubicados en la red LAN utilizando navegadores web configurados para trabajar con el proxy HTTP implementado. Durante las pruebas se verificó el correcto funcionamiento del proceso de autenticación, la solicitud de credenciales para navegar, y el bloqueo de los sitios incluidos dentro de la lista negra.

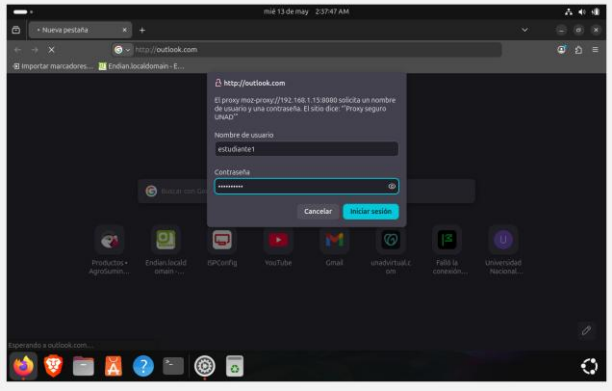
Figura 27.
Configuración del proxy en el navegador



Fuente: Autoría Propia.

Al intentar acceder a los dominios restringidos el sistema bloqueó satisfactoriamente la navegación, demostrando el correcto funcionamiento de las políticas de seguridad implementadas.

Figura 28.
Autenticación con usuario local



Fuente: Autoría Propia.

Figura 29.
Bloqueo del Proxy

Fuente: Autoría Propia.

4.5.4 RESULTADOS OBTENIDOS

La implementación del Proxy HTTP permitió controlar el acceso a internet dentro de la red LAN mediante autenticación de usuarios y políticas de filtrado web.

Las reglas configuradas en GNU/Linux Endian permitieron restringir sitios web específicos, administrar permisos de navegación, y fortalecer la seguridad perimetral de la infraestructura implementada.

Las pruebas realizadas evidenciaron el correcto funcionamiento del proxy y la efectividad de las políticas de acceso establecidas.

5 CONCLUSIONES

El laboratorio permitió desarrollar de manera integral las cinco temáticas propuestas para la implementación de seguridad perimetral en GNU/Linux mediante Endian Firewall Community. En la Temática 1, se estableció la base de la infraestructura al instalar Endian en VirtualBox y configurar correctamente las interfaces de red para las zonas Verde, Roja y Naranja, permitiendo separar la LAN, la WAN y la DMZ.

En la Temática 2, se configuró NAT para permitir la salida controlada hacia Internet desde la LAN y desde la DMZ, además de validar el redireccionamiento de puertos hacia un servidor ubicado en la zona Naranja. Esto evidenció la importancia de la traducción de direcciones para controlar la comunicación entre redes internas y externas.

En la Temática 3, la habilitación de servicios como HTTP y FTP en la DMZ permitió comprobar cómo los servidores pueden publicarse de forma controlada sin exponer directamente la red interna. Además, la restricción de ICMP demostró la utilidad de bloquear tráfico no requerido para reducir riesgos de exploración o reconocimiento de red.

En la Temática 4, la creación de reglas de acceso entre zonas permitió definir qué comunicaciones estaban autorizadas entre LAN, WAN y DMZ, reforzando el principio de mínimo privilegio y garantizando que solo los servicios necesarios fueran permitidos.

En la Temática 5, la implementación del proxy HTTP no transparente con autenticación permitió controlar la navegación de los usuarios desde la red interna. Mediante la creación de usuarios, grupos, perfiles de acceso y listas negras, se logró restringir el acceso a sitios específicos y aplicar políticas de navegación más seguras. Esta temática evidenció que el firewall no solo cumple funciones de filtrado de red, sino que también puede actuar como una herramienta de control de acceso web, auditoría y administración del uso de Internet.

6 REFERENCIAS

[1] Linux Professional Institute, *"Tema 102: Comandos GNU y Unix"*, LPI Learning Materials 101-500, 2022. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Debian Project, *"El manual del administrador de Debian 12.5.0"*, Debian Documentation, 2023. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[3] Oracle Corporation, *"VirtualBox User Manual"*, Oracle VM VirtualBox Documentation, 2020. Disponible en: https://www.virtualbox.org/manual/

[4] Canonical Ltd., *"Ubuntu Server Documentation"*, Help Ubuntu, 2023. Disponible en: https://help.ubuntu.com/

[5] Endian, *"Endian UTM 3.2 Reference Manual"*, Endian Documentation, 2016. Disponible en: http://docs.endian.com/3.2/utm/index.html

[6] J. LaCroix, *"Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server"*, Packt Publishing, Birmingham, UK, 2020. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952