Diseño e Implementación de un Proxy HTTP No Transparente en GNU/Linux utilizando Endian Firewall Community

Daniel Alejandro Herrera Mejía
e-mail: daherreramej@unadvirtual.edu.co

Angie Daniela Reyes Parra
e-mail: adreyespa@unadvirtual.edu.co

Jarlin Duván González
e-mail: jdgonzalezcues@unadvirtual.edu.co

Manuel Läuft
e-mail: mlauft@unadvirtual.edu.co

RESUMEN: *El siguiente artículo tiene como objetivo ofrecer una visión general clara y bien documentada de la implementación de un proxy HTTP no transparente con autenticación de usuarios utilizando un servidor Endian Firewall Community 3.2.5 ejecutado en una máquina virtual creada con VirtualBox. Para llevar a cabo esta tarea, se configuraron tres máquinas virtuales, cada una con una función específica: la primera máquina, Endian EFW, actuaba como cortafuegos configurado con tres zonas (LAN, DMZ y WAN); la segunda máquina, un servidor Ubuntu, se configuró con la IP estática 192.168.20.10 para la DMZ, y la tercera máquina, un Ubuntu Desktop, se destinó a la zona LAN y se configuró con la IP estática 192.168.10.20. Mediante el panel de control de Endian, se asignó el 3128 como puerto de proxy, se creó una lista negra para bloquear diversos sitios web y se configuraron las políticas de autenticación de usuarios y de acceso. A continuación, se llevaron a cabo varias pruebas que confirmaron que los sitios web restringidos quedaban efectivamente bloqueados y que se solicitaban las credenciales antes de permitir el acceso a Internet.*

Index Terms—GNU/Linux, Endian, Firewall, autenticación, lista negra, Proxy HTTP, seguridad perimetral, DMZ, LAN, WAN, VirtualBox.

1 INTRODUCCIÓN

El siguiente artículo se ha escrito para documentar el desarrollo de un proxy HTTP no transparente con políticas de autenticación de usuarios. Se implementó un servidor firewall utilizando la herramienta "Endian Firewall Community 3.2.5" [1], junto con un entorno de prueba que consta de tres máquinas virtuales creadas con VirtualBox [2], ejecutándose como instancias GNU/Linux. La primera máquina fue el servidor Endian EFW, importado a través de un archivo OVA y preconfigurado según las instrucciones del Tema 1; actuó como firewall central utilizando tres zonas de red (zona LAN verde, zona DMZ naranja y zona WAN roja). La segunda máquina, que ejecutaba Ubuntu Server 22.04 [3], se desplegó para el uso exclusivo de la zona DMZ naranja y se le asignó una dirección IP estática; Finalmente, la tercera máquina, que ejecutaba Ubuntu Desktop 22.04 [4], se dedicó exclusivamente a la zona LAN verde y también se le configuró con una dirección IP estática; Se utilizó para acceder al panel de control de administración web de Endian, donde el proxy HTTP estaba habilitado en modo no transparente y se le asignó el puerto 3128; se configuró un perfil de lista negra para bloquear el acceso a varios sitios web (hotmail.com, youtube.com y elnuevodia.com.co); y la cuenta de usuario se configuró con políticas de acceso basadas en grupos, con las validaciones correspondientes realizadas desde el cliente en la LAN. Al implementar este proyecto, logramos un control efectivo sobre la navegación web del usuario por perímetro, ya que el proxy requiere autenticación antes de permitir cualquier tráfico HTTP o HTTPS saliente.

El desarrollo de soluciones de este tipo es una práctica fundamental en la administración de sistemas GNU/Linux [5], ya que permite a las organizaciones establecer controles de acceso y priorizar el tráfico de Internet mediante protocolos de autenticación de usuarios, garantizando así la supervisión del tráfico de red y la seguridad perimetral en las redes corporativas [6].

2 INFRAESTRUCTURA Y CONFIGURACIÓN PREVIA

2.1 MÁQUINAS VIRTUALES UTILIZADAS

Este proyecto se desarrolló utilizando la herramienta Oracle VirtualBox, con la que se crearon tres máquinas virtuales que se ejecutaron simultáneamente en el mismo equipo físico:

Tabla 1. Máquinas virtuales del laboratorio.

VM	Sistema Operativo	Zona	Ip Asignada
Endian EFW	Endian Firewall Community 3.2.5	Firewall (3 NICs)	GREEN: 192.168.10.1 ORANGE: 192.168.20.1 RED: DHCP NAT

Ubuntu Desktop 22.04 LTS	Ubuntu Desktop 22.04	LAN (Zona Verde)	192.168.10.20/24 GW: 192.168.10.1
Ubuntu Server 22.04 LTS	Ubuntu Server 22.04	DMZ (Zona Naranja)	192.168.20.10/24 GW:192.168.20.1

Nota. Esta tabla muestra la distribución y la información detallada de cada una de las tres máquinas virtuales utilizadas durante el desarrollo.

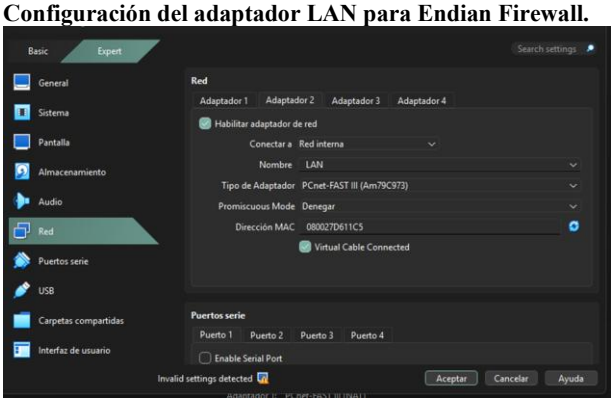
2.2 INSTALACIÓN Y CONFIGURACIÓN DE LA MÁQUINA VIRTUAL ENDIAN.

La instalación de la máquina se llevó a cabo configurando 3 adaptadores en la máquina Endian, para garantizar la conectividad entre las partes del ejercicio, así:

Figura 1.
Configuración del adaptador NAT para Endian Firewall.

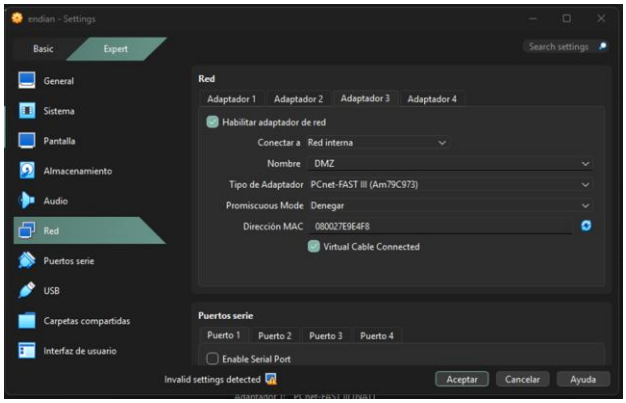
Fuente: Autoría propia

Figura 2.
Configuración del adaptador LAN para Endian Firewall.



Fuente: Autoría propia

Figura 3.
Configuración del adaptador DMZ para Endian Firewall.

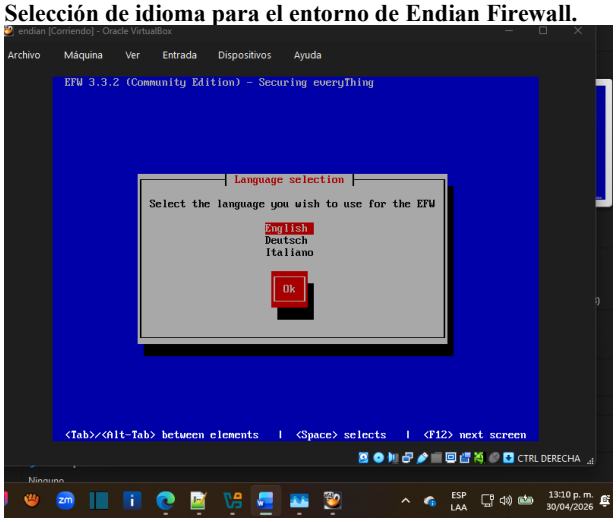


Fuente: Autoría propia

2.2.1 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DEL FIREWALL ENDIAN

Se realizó la configuración del firewall siguiendo los pasos del asistente de instalación.

Figura 4.
Selección de idioma para el entorno de Endian Firewall.



Fuente: Autoría propia

Figura 5.
Habilitar consola para Endian Firewall.

Fuente: Autoría propia
Nota**.** Se selecciona la opción NO debido a que no se está realizando una conexión física sino una virtualización.

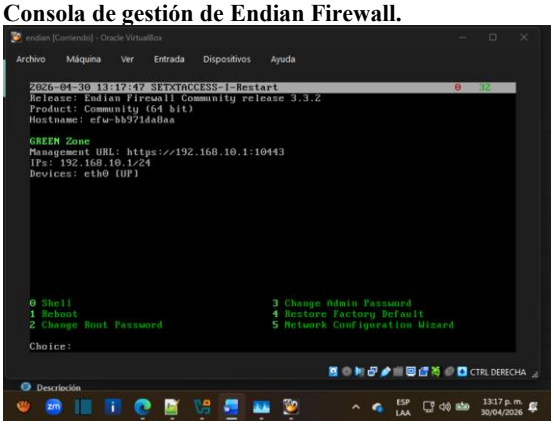
Figura 6.
Configuración de la Zona Green para Endian Firewall.

Fuente: Autoría propia
Nota**.** Se creó como opción de instalación la zona Green, en la cual se asignó la ip 192.168.10.1.

Figura 7.
Confirmación de la instalación de Endian Firewall.

Fuente: Autoría propia

Figura 8.
Consola de gestión de Endian Firewall.



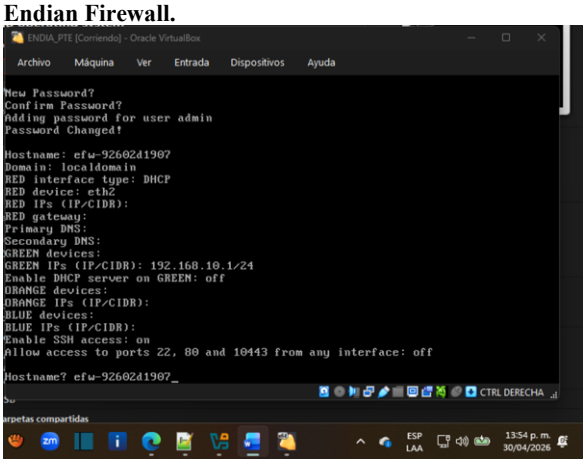
Fuente: Autoría propia

Nota**.** La consola muestra la Zona Green configurada dentro del proceso de instalación.

2.2.2 CONFIGURACIÓN DE LAS ZONAS RED Y ORANGE

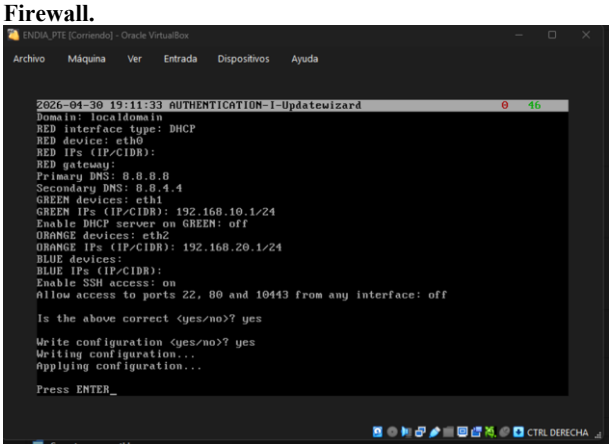
Con la herramienta ya instalada se realizó la configuración de las Zonas Red y Orange. Ingresando por la opción 5 “Network Configuration Wizard”. En la primera interacción Endian solicita el cambio de la contraseña del usuario *root,* dicha contraseña por defecto es “endian”, y se realizó el cambio por una de la elección del usuario, unad2026.

Figura 9.
Asignación de parámetros a las Zonas Orange y Red en Endian Firewall.



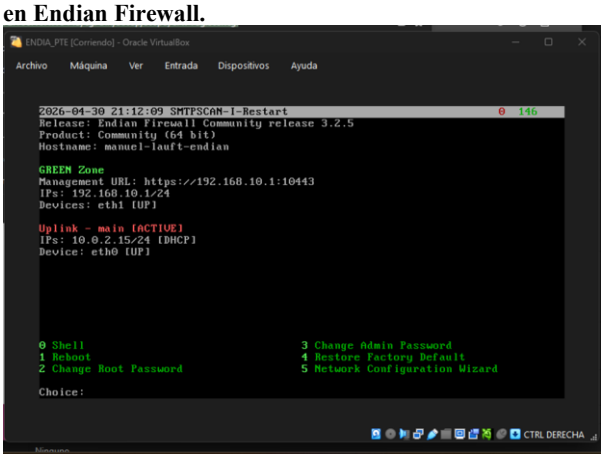
Fuente: Autoría propia

Figura 10.
Validación de los parámetros en la consola de Endian Firewall.



Fuente: Autoría propia

Figura 11.
Confirmación en la consola de la creación de la Zona Roja en Endian Firewall.



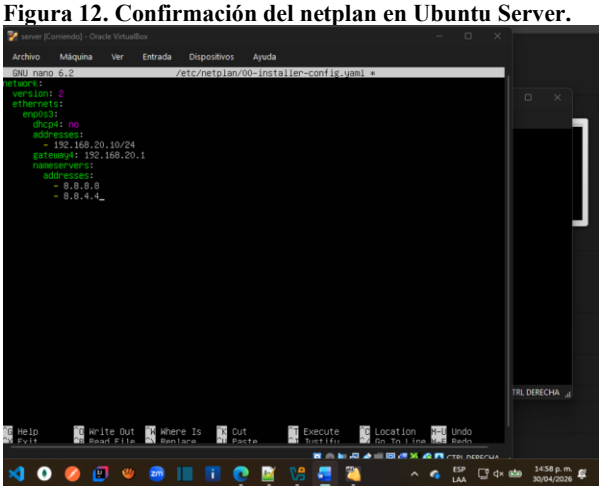
Fuente: Autoría propia

2.3 PRUEBA DE CONEXIÓN DE LA RED DMZ Y LAN EN LAS DISTRIBUCIONES UBUNTU SERVER Y UBUNTU DESKTOP.

2.3.1 CONFIGURACIÓN Y PRUEBA DE CONEXIÓN EN DMZ (UBUNTU SERVER)

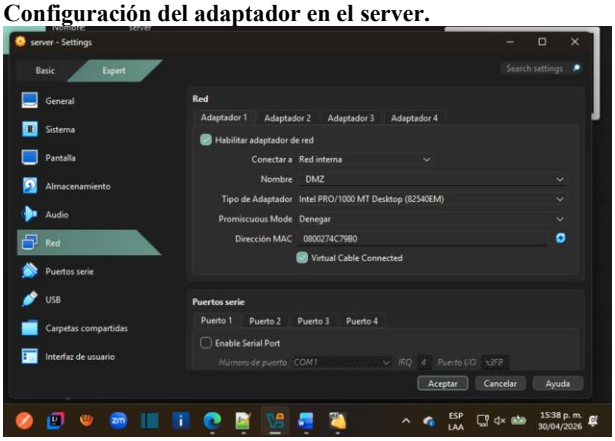
Se realizan las configuraciones en la máquina virtual de Ubuntu Server para realizar la prueba de conexión DMZ, haciendo configuraciones para obtener conexión mediante la edición del Netplan en el Server, así como un cambio de configuración en el adaptador de la máquina virtual. Se validan dichas conexiones mediante pruebas de ping de exposición de dicha conexión configurada.

Figura 12. Confirmación del netplan en Ubuntu Server.



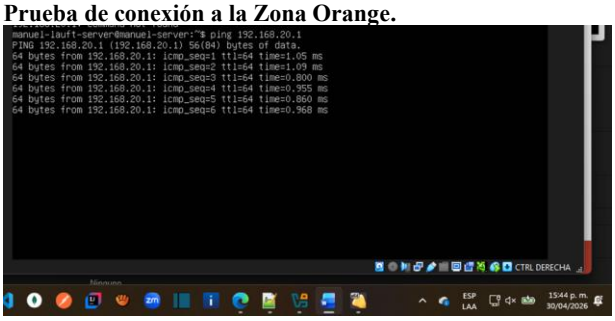
Fuente: Autoría propia
Nota. Configuración del archivo *config.yaml, para habilitar las direcciones y el Gateway del DMZ.

Figura 13.
Configuración del adaptador en el server.



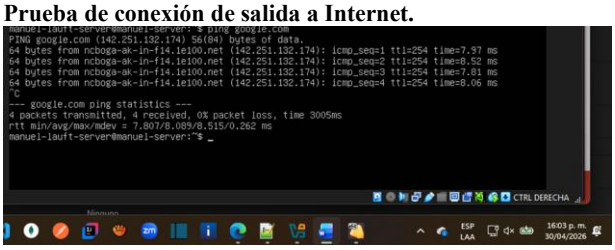
Fuente: Autoría propia

Figura 14.
Prueba de conexión a la Zona Orange.



Fuente: Autoría propia

Figura 15.
Prueba de conexión de salida a Internet.

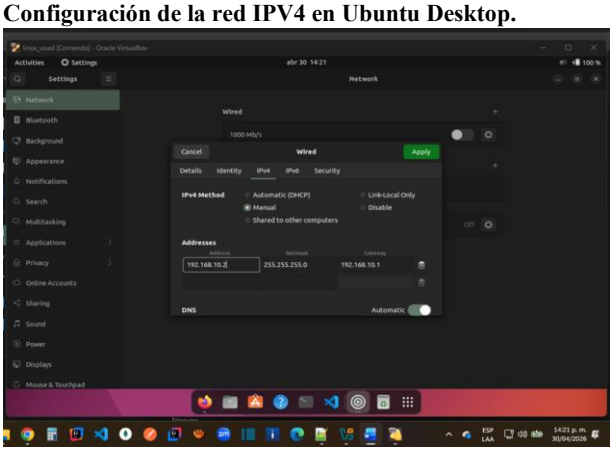


Fuente: Autoría propia

2.3.2 CONFIGURACIÓN Y PRUEBA DE CONEXIÓN LAN (UBUNTU DESKTOP)

Se realizan las configuraciones en la máquina virtual de Ubuntu Desktop para realizar la prueba de conexión LAN, siguiendo una implementación similar a la hecha en el Server, incluyendo una edición del Netplan, configuración de la dirección de red y pruebas de conexión.

Figura 16.
Configuración de la red IPV4 en Ubuntu Desktop.

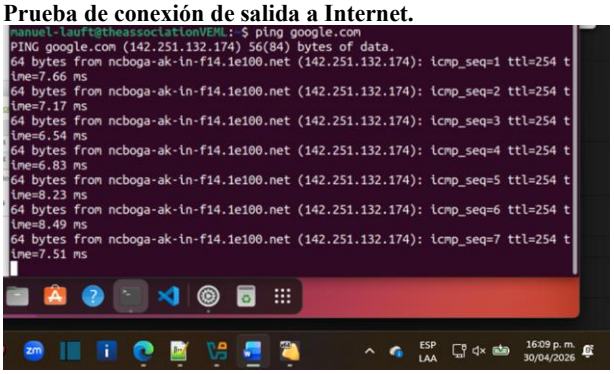


Fuente: Autoría propia

Figura 17.
Configuración de Netplan en Ubuntu Desktop.

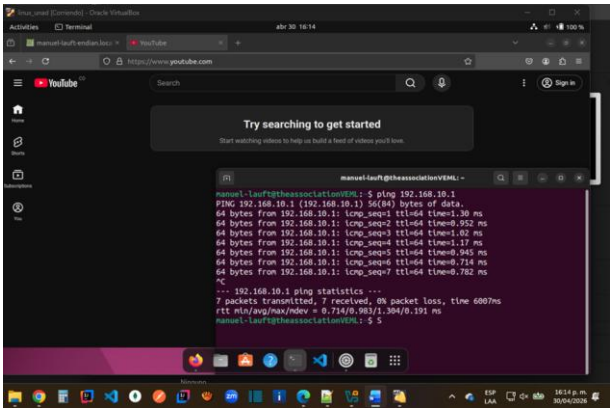
Fuente: Autoría propia

Figura 18.
Prueba de conexión de salida a Internet.



Fuente: Autoría propia

Figura 19.
Prueba de conexión de navegación en Internet desde el navegador.



Fuente: Autoría propia

2.4 IMPORTACIÓN DEL ARCHIVO. OVA

La máquina virtual que ejecuta el sistema operativo Endian Firewall Community 3.2.5, utilizada para implementar el proxy HTTP no transparente, es la misma que se creó en la lección 1; simplemente importamos el archivo. ova, ajustamos los adaptadores de red y verificamos la configuración de las direcciones IP asignadas por zona.

- Adaptador 1: NAT para zona roja WAN (salida a Internet)
- Adaptador 2: Red interna "LAN" para zona verde (red interna Desktop)
- Adaptador 3: Red interna "DMZ" para zona naranja (servidores)

2.5 VERIFICACIÓN DE ZONAS EN ENDIAN

Al iniciar el equipo que ejecuta el sistema operativo Endian Firewall Community 3.2.5, de forma predeterminada solo se mostrará la zona verde en la pantalla de la consola. Por lo tanto, si desea ver la configuración interna, debe acceder al Shell mediante la opción de menú 0, escribir 'login' para iniciar sesión como root con la contraseña unad2026 y, por último, se deben ejecutar los siguientes comandos:

Tabla 2. Comandos de verificación de zonas

Comando	Descripción
cat /var/efw/ethernet/settings	presenta el archivo de configuración de la red endian
ip link show	muestra todas las tarjetas de red disponibles en el sistema y las que están activas las tarjetas de red que presentaran son (eth0, eth1 y eth2)

Al ejecutar los comandos de la tabla anterior, se comprueba que las zonas estén configuradas correctamente de la siguiente manera: GREEN_ADDRESS=192.168.10.1 y ORANGE_ADDRESS=192.168.20.1, y que sus respectivos adaptadores de red estén activos y asignados de la siguiente manera: eth0 (RED), eth1 (GREEN) y eth2 (ORANGE)

2.6 CONFIGURACIÓN DE RED EN UBUNTU SERVER

El adaptador de red de esta máquina se configuró como una red DMZ interna. Dentro de la máquina virtual, configuramos el archivo netplan para asignarle una dirección IP estática de 192.168.20.10/24. Se ejecutan las siguientes instrucciones en la ventana de comandos de Ubuntu:

- Identificamos el archivo que hay que configurar mediante el comando 'ls /etc/netplan/'; esto nos mostrará el archivo 00-installer-config.yaml.
- Ahora editamos el archivo de netplan utilizando el editor de texto nano con el siguiente comando: 'sudo nano /etc/netplan/00-installer-config.yaml' ajustamos los parámetros exactamente como indica la tabla "Configuración net plan Ubuntu Server.".
- Después de realizar los cambios, aplícalos con el siguiente comando: '*sudo netplan apply'*, según la documentación oficial de Netplan [7].
- Comprueba que la dirección IP se ha asignado correctamente mediante el comando 'ip a'.

Tabla 3. Configuración netplan Ubuntu Server.

Parámetro	Valor
Interface	enp0s3
dhcp4	no
address	192.168.20.10/24
gateway4	192.168.20.1
DNS	8.8.8.8 / 8.8.4.4

Nota: la siguiente tabla ofrece información más detallada sobre los parámetros adecuados para ajustar el archivo netplan

Tras realizar el ajuste anterior, se verificó y confirmó que la asignación de la dirección IP 192.168.20.10/24 se había realizado correctamente.

2.7 CONFIGURACIÓN DE RED EN UBUNTU DESKTOP

Para configurar esta máquina virtual, seguimos el mismo procedimiento que utilizamos para la máquina con Ubuntu Server, con la única diferencia de que la tarjeta de red de se configuró como una LAN interna. Dentro de la máquina virtual, configuramos el archivo netplan para asignarle una dirección IP estática de 192.168.10.20/24 y una puerta de enlace de 192.168.10.1. Tras realizar este ajuste, verificamos y confirmamos que la dirección IP 192.168.10.20/24 se había asignado correctamente.

3 IMPLEMENTACIÓN DE SERVICIOS EN DMZ Y VALIDACIÓN DE SEGURIDAD

Durante el desarrollo de la temática número 3 se realizó la implementación de servicios HTTP y FTP dentro de la zona DMZ utilizando una máquina virtual Ubuntu Server 22.04 configurada con dirección IP estática 192.168.20.10/24 y puerta de enlace 192.168.20.1. La infraestructura fue integrada al entorno de Endian Firewall Community mediante la interfaz ORANGE, permitiendo la segmentación de la red y el aislamiento de los servicios publicados.

Posteriormente, se realizó la habilitación y verificación de los servicios Apache2 [8] y VSFTPD [9] dentro del servidor Ubuntu, permitiendo el acceso controlado a través de los puertos 80 y 21 respectivamente. Para ello, desde el apartado Firewall > Port Forwarding/NAT de Endian, se configuraron las reglas necesarias para permitir el tráfico hacia los servicios implementados en la zona DMZ.

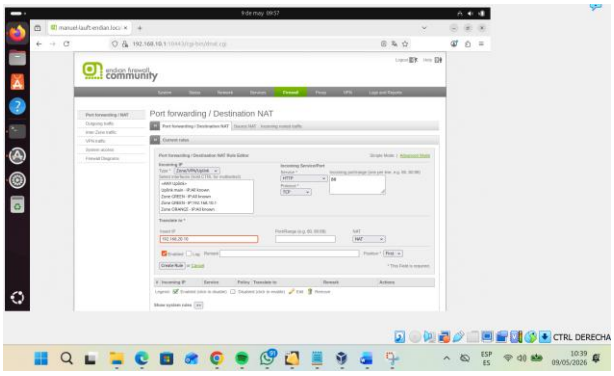
Adicionalmente, se implementó una política de seguridad para bloquear el protocolo ICMP entre zonas, con el propósito de evitar respuestas a solicitudes ping hacia el servidor. Esta validación permitió comprobar el correcto funcionamiento de las políticas de filtrado y seguridad perimetral implementadas sobre la infraestructura GNU/Linux.

Finalmente, se realizaron pruebas de funcionamiento mediante acceso HTTP desde navegador web, validación de los servicios activos mediante comandos systemctl status apache2 y systemctl status vsftpd, así como pruebas de conectividad ICMP, evidenciando que los servicios configurados funcionaban correctamente mientras el protocolo ping permanecía restringido por las políticas del firewall.

Tabla 4. Validación de servicios en DMZ

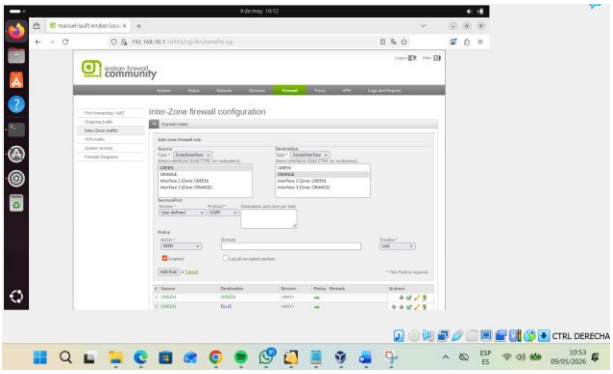
Prueba realizada	Resultado esperado	Estado
Acceso HTTP al servidor DMZ	Página Apache visible	PASS
Servicio FTP activo	Servicio VSFTPD funcionando	PASS
Bloqueo ICMP	Ping denegado	PASS
Verificación Apache2	Servicio activo	PASS
Verificación VSFTPD	Servicio activo	PASS

Figura 20.
Configuración de regla NAT para el servicio HTTP en Endian Firewall.



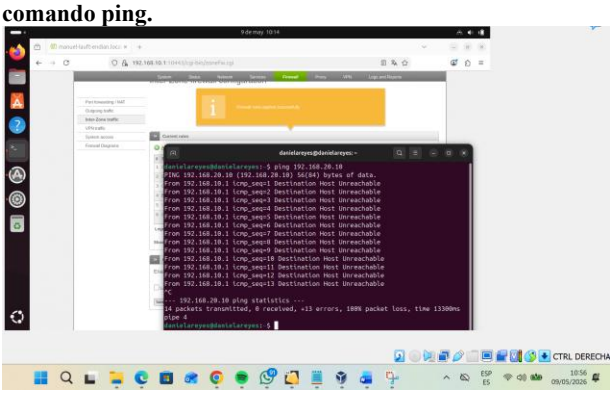
Fuente: Autoría propia
Nota**.** Regla NAT configurada en Endian Firewall Community para permitir el acceso al servicio HTTP (puerto 80) hacia el servidor Ubuntu ubicado en la zona DMZ.

Figura 21.
Configuración de regla de denegación para protocolo ICMP en Endian Firewall.



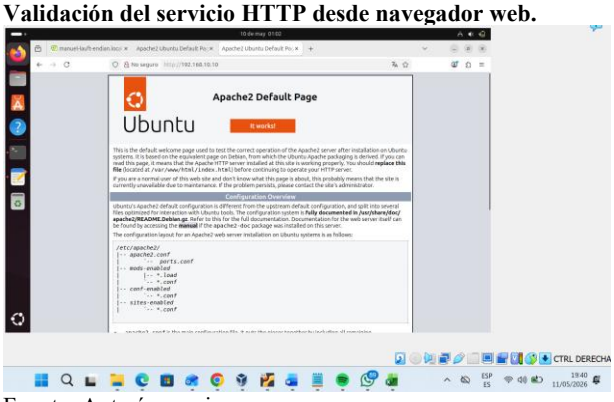
Fuente: Autoría propia
Nota. Regla configurada en Endian Firewall Community para denegar solicitudes ICMP entre zonas de red y restringir respuestas ping hacia el servidor ubicado en la zona DMZ.

Figura 22.
Validación de bloqueo de solicitudes ICMP mediante comando ping.



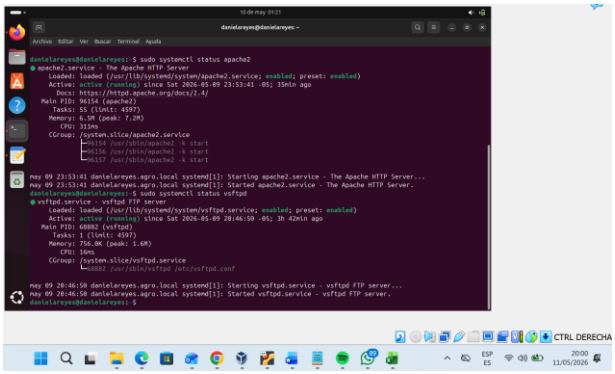
Fuente: Autoría propia
Nota**.** Se evidencia el bloqueo de respuestas ICMP hacia el servidor ubicado en la zona DMZ, mostrando pérdida total de paquetes durante la ejecución del comando ping.

Figura 23.
Validación del servicio HTTP desde navegador web.



Fuente: Autoría propia
Nota**.** Se evidencia el correcto funcionamiento del servicio Apache2 mediante acceso HTTP desde navegador web utilizando el servidor Ubuntu configurado en la zona DMZ.

Figura 24.
Verificación del estado de los servicios Apache2 y VSFTPD en Ubuntu Server.



Fuente: Autoría propia
Nota**.** Se evidencia que los servicios Apache2 y VSFTPD se encuentran activos y en ejecución dentro del servidor Ubuntu Server configurado en la zona DMZ.

4 CONFIGURACIÓN DEL PROXY Y AUTENTICACIÓN

4.1 ACCESO AL PANEL DE ADMINISTRACIÓN DE ENDIAN

Desde la máquina Ubuntu Desktop y utilizando el navegador Firefox, se accede al administrador de Endian en la siguiente dirección: "https://192.168.10.1:10443". El sistema mostrará una advertencia de seguridad debido al certificado auto firmado y pedirá las credenciales de inicio de sesión establecidas durante la configuración inicial del servidor Endian, con el nombre de usuario: admin y la contraseña: unad2026

4.2 ACTIVACIÓN DEL PROXY HTTP NO TRANSPARENTE [10]

Una vez se ha accedido al módulo de administración de Endian debemos configurar y activar el proxy http no transparente, para ello es necesario acceder al menú del proxy > http y allí se configuran los parámetros, según la siguiente tabla:

Tabla 5. Configuración del proxy HTTP

Parámetro	Valor
Enable HTTP Proxy	Activado (toggle verde)
Modo GREEN	not transparent
Modo ORANGE	not transparent
Puerto proxy	3128
Keep source IP	Habilitado

Nota: la siguiente tabla ofrece información más detallada sobre los parámetros adecuados para ajustar el proxy http no transparente

4.3 CREACIÓN DEL PERFIL CON LISTA NEGRA

En el apartado de Proxy > HTTP > Filtro web > Add new Profile Hemos creado el siguiente perfil, denominado "Restricted_Profile". A continuación, en la sección "black- and whitelists", se han añadido los siguientes dominios al campo " Block the following sites":

- hotmail.com
- youtube.com
- elnuevodia.com.co

Debe colocarse un punto antes del nombre de dominio para garantizar que tanto el dominio principal como cualquier subdominio queden bloqueados por el cortafuegos

4.4 CREACIÓN DE USUARIO Y POLÍTICAS DE ACCESO

En el apartado de Proxy > HTTP > Authentication > manage users hemos creado el usuario daniel con la contraseña unad2026, luego en Access Policy, se configuraron dos políticas en el siguiente orden:

Tabla 6. Políticas de acceso configuradas.

Política	Auth	Usuario	Accion
access denied	user based	daniel	Deny access
filter using Restricted_Profile	user based	daniel	Allow access + filtro

Nota: la siguiente tabla se presenta información detallada de las políticas de acceso configuradas

4.5 CONFIGURACIÓN DEL NAVEGADOR EN EL CLIENTE

En Ubuntu Desktop, hemos configurado el navegador para usar el proxy manualmente, mediante la siguiente ruta Menú > Configuración > Red > Configuración manual del proxy, posteriormente se ingresa la IP 192.168.10.1 en el campo Proxy HTTP con puerto 3128 y marcamos la opción 'Usar también este proxy para HTTPS'.

4.6 RESULTADOS Y VALIDACIÓN

Al ingresar a cualquier sitio web desde el navegador Firefox con el proxy configurado, el sistema nos solicita credenciales de autenticación con el siguiente mensaje 'El proxy 192.168.10.1:3128 solicita un nombre de usuario y una contraseña'. luego de ingresar el usuario daniel y la contraseña unad2026, realizamos las siguientes pruebas

Tabla 7. Resultados de las pruebas de validación.

Prueba realizada	Resultado esperado	Estado
Acceso a www.youtube.com	Bloqueado por lista negra	PASS
Acceso a www.hotmail.com	Bloqueado por lista negra	PASS
Acceso a www.elnuevodia.com.co	Bloqueado por lista negra	PASS
Autenticación proxy requerida	Solicita usuario/contraseña	PASS
Sitio no bloqueado (debian.org) [11]	Acceso concedido tras auth	PASS
Navegación sin proxy configurado	Tráfico directo sin filtro	VERIFICADO

Nota: la siguiente tabla ofrece información más detallada sobre las validaciones y resultados del proxy

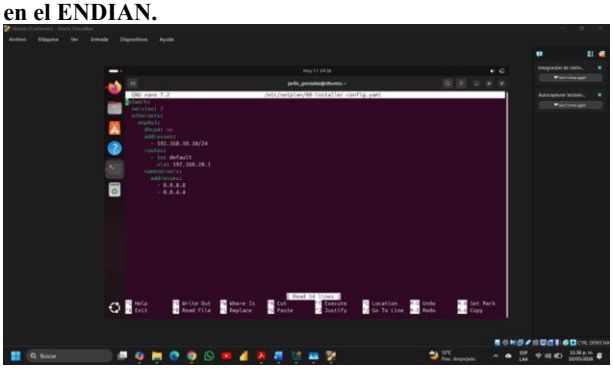
Los sitios incluidos en la lista negra mostraron una página de error de proxy en la que se indicaba que la conexión había sido rechazada, lo que confirma que el filtrado funciona correctamente; los sitios que no figuraban en la lista se cargaron con normalidad tras la autenticación de nuestro usuario.

5 REGLAS DE ACCESO PARA PERMITIR O DENEGAR TRÁFICO

5.1 CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES

Se realiza configuración de los adaptadores de red para cada una de las máquinas y posterior se agrega configuración en el archivo netplan.

Figura 25.
Configuración de las IP's de acuerdo con las configuradas en el ENDIAN.



Fuente: Autoría propia

Figura 26.
Configuración del Server

Fuente: Autoría propia

Figura 27.
Conexión a la interfaz del Endian Firewall Community

Fuente: Autoría propia Nota. Se realiza conexión desde el Desktop desde el navegador web a la ip 192.168.10.1 al puerto 10443.

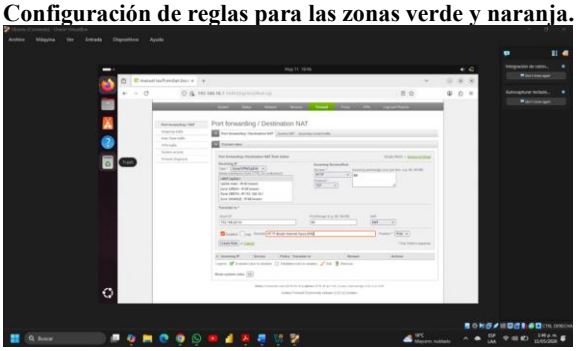
5.1 COMUNICACIÓN ENTRE LA ZONA VERDE Y NARANJA PROTOCOLO HTTP Y FTP

Se realiza configuración desde la interfaz ENDIAN en la ruta Firewall-Inter-Zona traffic, donde se define el protocolo HTTP y FTP para las dos zonas.

Tabla 8. Parámetros de reglas en el firewall

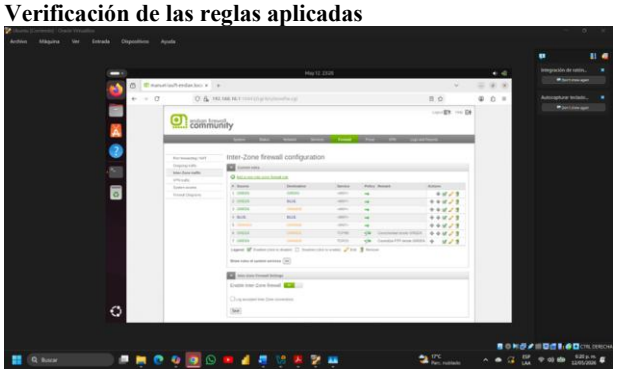
Source	Destino	Service	Politica
GREEN	**ORANGE**	HTTP (TCP/80)	ACCEPT
GREEN	ORANGE	FTP (TCP/21)	ACCEPT

Figura 28.
Configuración de reglas para las zonas verde y naranja.



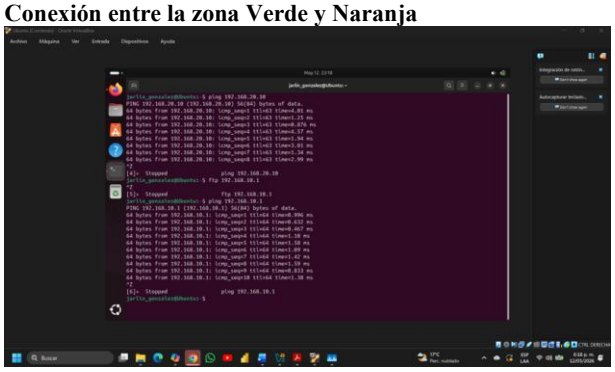
Fuente: Autoría propia
Nota. Se configura IP origen y destino desde la zona verde a la naranja bajo el servicio HTTP y protocolo TCP al puerto 80.

Figura 29.
Verificación de las reglas aplicadas



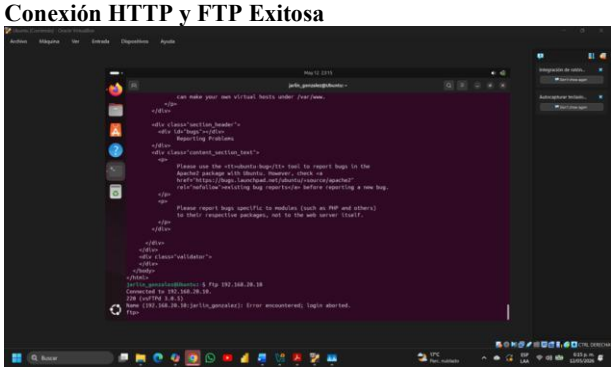
Fuente: Autoría propia
Nota. Se observa el registro de las dos reglas para permitir conexión entre las dos zonas.

Figura 30.
Conexión entre la zona Verde y Naranja



Fuente: Autoría propia
Nota. Se evidencia que desde el Desktop zona verde responde el ping a las IP's 192.168.20.10 zona naranja. Adicional responde a la IP 192.168.10.1

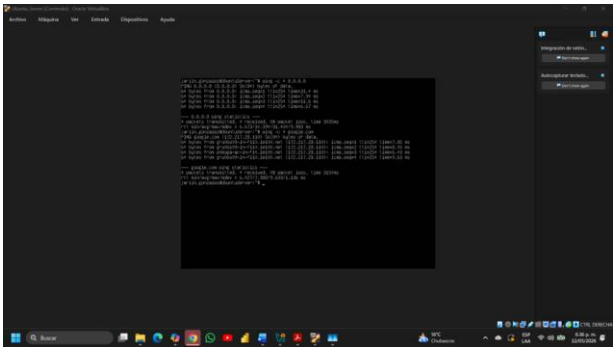
Figura 31.
Conexión HTTP y FTP Exitosa



Fuente: Autoría propia
Nota. Desde el Desktop la zona verde se verifica conexión vía HTTP y FTP a la ip 192.168.20.10, la cual es exitosa.

5.2 COMUNICACIÓN ZONA INTERNET CON ZONA DMZ

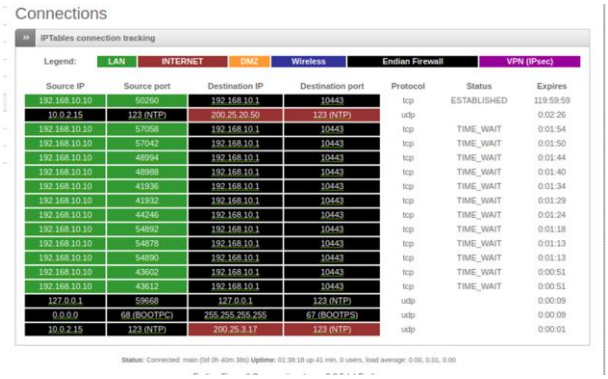
Figura 32.
Conexión zona internet a DMZ



Fuente: Autoría propia
Nota. Se configuró la comunicación entre la zona ORANGE y la RED (Internet). Las reglas de firewall permiten tráfico HTTP, HTTPS, FTP, DNS e ICMP saliente.

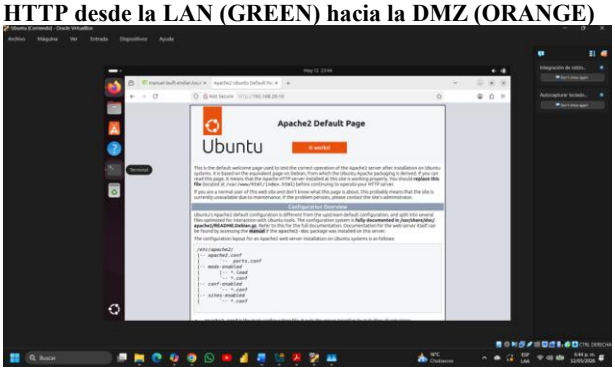
5.3 VERIFICACIÓN DE TRÁFICO INTER - ZONA

Figura 33.
Tráfico inter – zona



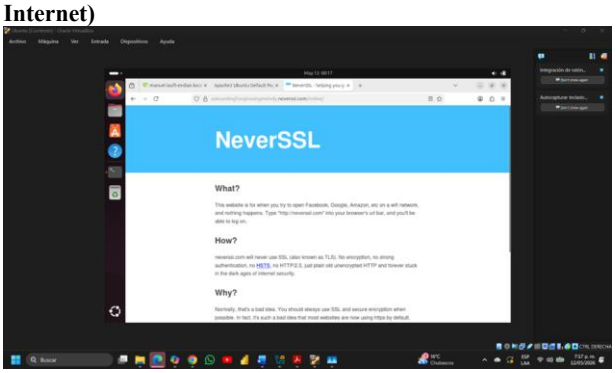
Fuente: Autoría propia
Nota. Las entradas muestran un origen en la IP 192.168.10.10 (LAN) hacia la 192.168.10.1 (el Firewall) por el puerto 10443. Este puerto suele utilizarse para la interfaz de administración web segura (HTTPS).

Figura 34.
HTTP desde la LAN (GREEN) hacia la DMZ (ORANGE)



Fuente: Autoría propia
Nota. Ingreso desde el servicio HTTP desde la LAN hacia la zona DMZ.

Figura 35.
HTTP desde la LAN (GREEN) hacia la WAN (RED / Internet)



Fuente: Autoría propia
Nota. HTTP desde la LAN (GREEN) hacia la WAN (RED / Internet)

6 CONCLUSIONES

La implementación de un proxy HTTP no transparente utilizando Endian como cortafuegos ofrece la posibilidad de controlar con gran detalle el tráfico de Internet de los usuarios de la LAN, ya que nos permite vincular políticas de filtrado a varios usuarios específicos para garantizar una conexión mejor controlada. Dado que varios dominios figuran en una lista negra y están configurados en el perfil de filtrado, esto actúa como un mecanismo eficaz y fácil de gestionar para denegar el acceso a sitios web no deseados, sin que se requieran conocimientos técnicos complejos ni ajustes en las reglas del cortafuegos.

Dado que la arquitectura se basa en zonas Endian (verde, naranja y roja), esto facilita la división correcta de la red en LAN, DMZ y WAN. Esto proporcionó una base sólida para la implementación de políticas de seguridad perimetral en dispositivos con GNU/Linux. Además, la autenticación de proxy basada en el usuario garantiza un mayor nivel de seguridad, ya que se solicitan datos de inicio de sesión antes de autorizar cualquier tráfico de Internet, lo que permite supervisar el comportamiento de navegación, ya que se requiere una identidad específica.

La implementación de servicios HTTP y FTP dentro de la zona DMZ permitió comprobar el funcionamiento de políticas de segmentación de red mediante Endian Firewall Community, garantizando el acceso controlado a servicios publicados y aplicando restricciones de seguridad como el bloqueo ICMP entre zonas. Las pruebas realizadas evidenciaron el correcto funcionamiento de Apache2 y VSFTPD, así como la efectividad de las reglas NAT y de filtrado implementadas sobre la infraestructura GNU/Linux.

7 REFERENCIAS

[1] Endian, “Endian UTM 3.2 Reference Manual,” Endian Documentation, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

[2] Oracle Corporation, “Oracle VM VirtualBox User Manual,” VirtualBox Documentation, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[3] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Birmingham, U.K.: Packt Publishing, 2020.

[4] Canonical Ltd., “Ubuntu Documentation,” Ubuntu Help, 2023. [En línea]. Disponible en: https://help.ubuntu.com/

[5] Linux Professional Institute, “Tema 102: Comandos GNU y Unix,” LPIC-1 Exam 101, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[6] Red Hat Inc., “Introduction to Firewalls and Network Security,” Red Hat Documentation, 2023. [En línea]. Disponible en: https://www.redhat.com/en/topics/security/what-is-a-firewall

[7] Oracle Corporation, “Netplan Configuration Examples,” Ubuntu Server Documentation, 2023. [En línea]. Disponible en: https://netplan.io/examples

[8] Apache Software Foundation, “Apache HTTP Server Documentation,” 2024. [En línea]. Disponible en: https://httpd.apache.org/docs/

[9] VSFTPD Project, “Very Secure FTP Daemon Documentation,” 2024. [En línea]. Disponible en: https://security.appspot.com/vsftpd.html

[10] Squid Software Foundation, “Squid Proxy Server Documentation,” 2024. [En línea]. Disponible en: http://www.squid-cache.org/Doc/

[11] Debian Project, “Debian 12 Administrator’s Handbook,” Debian Documentation, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html