ENDIAN, UNA OPCIÓN EFICIENTE Y SENCILLA PARA LA IMPLEMENTACIÓN DE SEGURIDAD EN GNU/LINUX

Giovanny Alexander Rivera Rodríguez
e-mail: gariverarod@unadvirtual.edu.co
Henry Felipe Jerez Barreto
e-mail: hfjerezb@unadvirtual.edu.co
Cristian Camilo Garzón Triana
e-mail: ccgarzont@unadvirtual.edu.co
Mateo Rodriguez Rojas
e-mail: mrodriguezrojas@unadvirtual.edu.co
Steven Cubides Montañez
e-mail: bcubidesm@unadvirtual.edu.co

RESUMEN: *El proyecto desarrolla la implementación de una infraestructura de red segura mediante el uso de Endian Firewall Community en un entorno virtualizado con VirtualBox y sistemas GNU/Linux. Se diseñó una arquitectura segmentada en tres zonas de seguridad: GREEN (LAN), ORANGE (DMZ) y RED (WAN), permitiendo un control granular del tráfico y una defensa en profundidad. Se configuraron interfaces de red, direccionamiento IP estático, reglas de firewall y mecanismos de NAT (SNAT y DNAT) para facilitar tanto la salida a Internet como la publicación segura de servicios desde la DMZ. En el servidor Ubuntu se implementaron servicios HTTP, FTP y acceso remoto, verificando su funcionamiento mediante pruebas de conectividad y monitoreo. Adicionalmente, se configuró un proxy HTTP no transparente con autenticación de usuarios y listas negras para el control de navegación web. Las validaciones finales demostraron la correcta operación de la infraestructura, evidenciando una solución eficiente, controlada y segura para la administración perimetral de redes empresariales.*

PALABRAS CLAVE: Firewall, seguridad, reglas, endian

1 INTRODUCCIÓN

La administración y protección de infraestructuras de red constituye un elemento fundamental en los entornos empresariales modernos, debido a la necesidad de garantizar la seguridad, disponibilidad y control de los servicios informáticos. En este contexto, la implementación de firewalls, la segmentación de redes y el control del acceso a Internet permiten establecer mecanismos eficientes de protección frente a accesos no autorizados, así como optimizar la gestión del tráfico entre diferentes zonas de seguridad.

La presente actividad desarrolla la implementación de un laboratorio virtualizado utilizando VirtualBox, Endian Firewall Community y sistemas operativos GNU/Linux Ubuntu Server y Ubuntu Desktop, con el propósito de diseñar una arquitectura de red segmentada en zonas GREEN, ORANGE y RED. Estas zonas representan respectivamente la red local (LAN), la zona desmilitarizada (DMZ) destinada a la publicación controlada de servicios, y la conexión WAN hacia Internet.

Durante el desarrollo de la práctica se configuraron interfaces de red, direccionamiento IP estático, reglas de firewall, NAT y acceso remoto mediante SSH, actividades propias de la administración de sistemas GNU/Linux [1], permitiendo establecer políticas de comunicación y control de tráfico entre las diferentes zonas de seguridad. Asimismo, se implementaron servicios como Apache HTTP, FTP y acceso remoto, los cuales fueron publicados y verificados mediante pruebas de conectividad y acceso controlado desde la LAN y la WAN.

Adicionalmente, se incorporaron mecanismos de control de navegación mediante un proxy HTTP no transparente, aplicando autenticación de usuarios y listas de restricción para fortalecer la seguridad perimetral y regular el acceso a contenidos web. Finalmente, se realizaron validaciones utilizando herramientas de administración y monitoreo en GNU/Linux, evidenciando el correcto funcionamiento de la infraestructura, las reglas de seguridad implementadas y los mecanismos de protección de la red.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar una infraestructura de seguridad perimetral en GNU/Linux mediante el uso de Endian Firewall Community y entornos virtualizados en VirtualBox, con el fin de configurar y administrar zonas de red LAN, WAN y DMZ, aplicando reglas de firewall, NAT, control de acceso y servicios de red que garanticen la seguridad, conectividad y administración eficiente del tráfico en una red empresarial simulada.

2.2 OBJETIVO ESPECIFICOS

Configurar un entorno virtualizado utilizando GNU/Linux Endian, Ubuntu Server y Ubuntu Desktop, implementando las zonas GREEN, ORANGE y RED para segmentar la red en LAN, DMZ y WAN respectivamente.

Implementar reglas NAT y políticas de firewall que permitan controlar la comunicación entre las diferentes zonas de

red, verificando el acceso seguro desde la LAN y la DMZ hacia Internet.

Habilitar y administrar servicios de red como HTTP, FTP y SSH en la zona DMZ, permitiendo el acceso controlado desde la red interna y externa mediante reglas de filtrado y publicación de servicios.

Aplicar reglas de acceso y restricciones de tráfico entre las zonas LAN, WAN y DMZ, validando la comunicación permitida y denegando protocolos no autorizados como ICMP para fortalecer la seguridad perimetral.

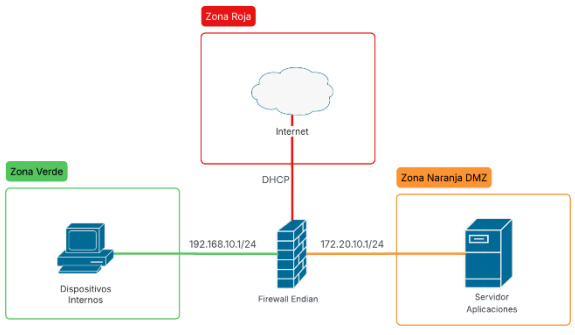
Configurar un proxy HTTP no transparente con políticas de autenticación y listas negras, con el propósito de controlar el acceso a contenidos web y reforzar las políticas de seguridad y navegación dentro de la red empresarial.

3 CONFIGURACIÓN E INSTALACIÓN DE ENDIAN EN VIRTUALBOX

Se implementó una infraestructura de red segmentada utilizando Endian Firewall Community 3.3.2 sobre VirtualBox, configurando tres zonas de seguridad: GREEN (LAN), RED (WAN) y ORANGE (DMZ), de acuerdo con el modelo de zonas de seguridad utilizado por Endian [2]. Se integraron máquinas virtuales Ubuntu Desktop y Ubuntu Server como cliente y servidor respectivamente, estableciendo direccionamiento IP estático, servicios de red y reglas de firewall para controlar el tráfico entre zonas. La validación final confirmó la conectividad entre todas las zonas y la publicación controlada de servicios desde la DMZ hacia la WAN.

La segmentación de redes mediante zonas de seguridad permite aplicar un enfoque de defensa en profundidad, reduciendo la exposición directa de la red interna frente a amenazas externas [3].

Figura 1.
Segmentación de la red



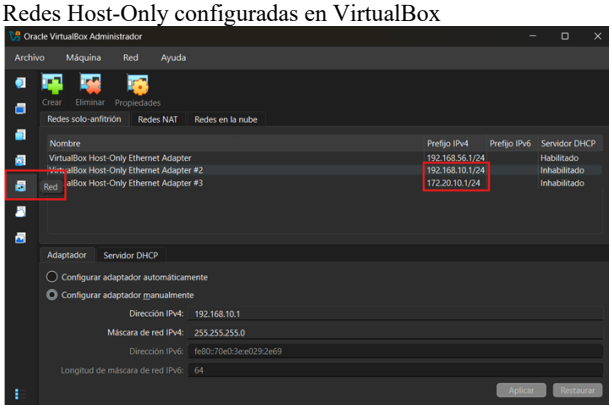
Fuente: Autoría Propia

3.1 INSTALACIÓN Y CONFIGURACIÓN ENDIAN

Se crearon las redes Host-Only en VirtualBox, se configuraron los tres adaptadores de red de la VM y se ejecutó la instalación de Endian, utilizando las funciones de virtualización y configuración de red disponibles en Oracle VirtualBox [4]. Al finalizar se establecieron las credenciales de acceso y se verificó el enrutamiento entre zonas mediante consola.

Se muestran las redes virtuales Host-Only creadas para la segmentación — 192.168.10.0/24 para GREEN y 172.20.10.0/24 para ORANGE — ambas con DHCP deshabilitado, junto con la configuración de los tres adaptadores de red de la VM Endian: Adaptador 1 Host-Only (LAN), Adaptador 2 NAT (WAN) y Adaptador 3 Host-Only (DMZ).

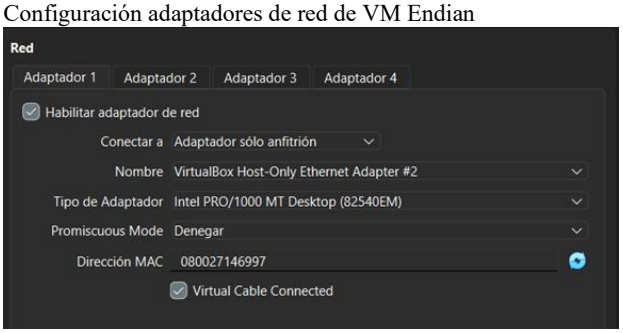
Figura 2.
Redes Host-Only configuradas en VirtualBox



Fuente: Autoría Propia

Se aprecian los adaptadores de red asignados a la VM: Adaptador 1 Host-Only (LAN), Adaptador 2 NAT (WAN) y Adaptador 3 Host-Only (DMZ), estableciendo la segmentación requerida por el firewall.

Figura 3.
Configuración adaptadores de red de VM Endian



Fuente: Autoría Propia

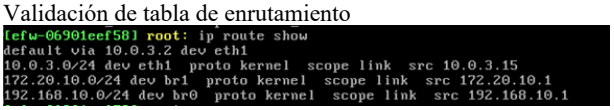
Se presenta el menú de consola de Endian versión 3.3.2 mostrando la zona GREEN activa con su dirección IP y la URL de acceso a la interfaz web de administración.

Figura 4.
Consola de Endian tras la Configuración

Fuente: Autoría Propia

Se confirma la tabla de enrutamiento con ip route show, verificando las rutas hacia las redes internas y la salida a Internet a través de la interfaz WAN.

Figura 5.
Validación de tabla de enrutamiento



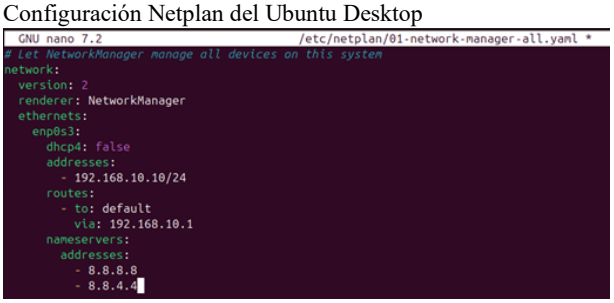
Fuente: Autoría Propia

3.2 CONFIGURACIÓN HOST ZONA VERDE (GREEN)

Se configuró el Ubuntu Desktop con IP estática mediante Netplan, deshabilitando cloud-init para evitar conflictos, siguiendo lineamientos generales de administración y configuración de sistemas Ubuntu [5]. Se validó la conectividad bidireccional con Endian y se accedió al Dashboard web confirmando las tres interfaces operativas.

Se observa el archivo Netplan con IP estática 192.168.10.10/24, gateway 192.168.10.1 y DNS configurados para el cliente de la zona GREEN.

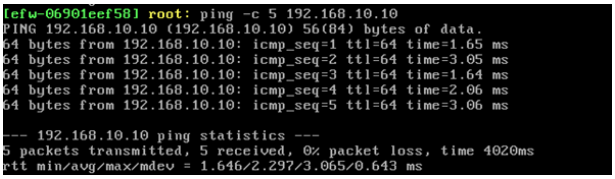
Figura 6.
Configuración Netplan del Ubuntu Desktop



Fuente: Autoría Propia

Se refleja el ping exitoso desde Endian hacia el Ubuntu Desktop confirmando la comunicación bidireccional entre el firewall y el cliente LAN.

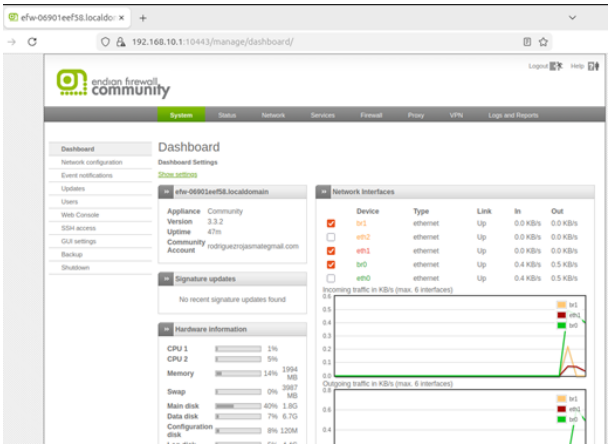
Figura 7.
Validación conectividad zona Green - Endian



Fuente: Autoría Propia

Se presenta el Dashboard de Endian accedido desde el Ubuntu Desktop, mostrando el estado UP de las interfaces GREEN, RED y ORANGE en tiempo real.

Figura 8.
Dashboard de Endian accedido desde zona GREEN



Fuente: Autoría Propia

3.3 CONFIGURACIÓN HOST 2 ZONA NARANJA (ORANGE)

Se integró el Ubuntu Server a la zona DMZ asignando IP estática mediante Netplan. Se validó la conectividad del servidor hacia Internet, hacia Endian y desde Endian hacia el servidor.

Se aprecia el archivo Netplan del servidor con IP estática 172.20.10.10/24 y gateway 172.20.10.1, estableciendo el direccionamiento de la zona DMZ.

Figura 9.
Configuración Netplan Ubuntu Server

```
 GNU nano 7.2
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 172.20.10.10/24
      gateway4: 172.20.10.1
      nameservers:
        addresses:
          - 8.8.8.8
```

Fuente: Autoría Propia

Se confirma el ping exitoso desde Endian hacia el servidor de la zona ORANGE, verificando la correcta comunicación entre el firewall y la DMZ.

Figura 10.
Comunicación entre Endian y el servidor DMZ

```
[efw-06901eef58] root: ping -c 5 172.20.10.10
PING 172.20.10.10 (172.20.10.10) 56(84) bytes of data.
64 bytes from 172.20.10.10: icmp_seq=1 ttl=64 time=0.694 ms
64 bytes from 172.20.10.10: icmp_seq=2 ttl=64 time=1.81 ms
64 bytes from 172.20.10.10: icmp_seq=3 ttl=64 time=2.23 ms
64 bytes from 172.20.10.10: icmp_seq=4 ttl=64 time=2.49 ms
64 bytes from 172.20.10.10: icmp_seq=5 ttl=64 time=1.53 ms

--- 172.20.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4020ms
rtt min/avg/max/mdev = 0.694/1.755/2.493/0.626 ms
```

Fuente: Autoría Propia

3.4 VALIDACIÓN E IMPLEMENTACIÓN SERVICIOS EN LA DMZ

Se verificó el estado activo de los servicios Apache, FTP y SSH en el servidor DMZ y se comprobó el acceso a cada uno desde el Ubuntu Desktop en la zona GREEN, aplicando procedimientos habituales de administración y validación de servicios en Ubuntu Server [6].

Figura 11.
Servicios activos en el servidor DMZ

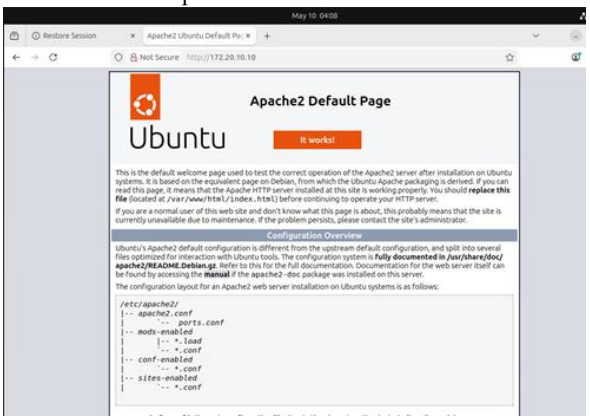
```
     Active: active (running) since Sun 2026-05-10 03:06:12 UTC; 46min ago
       Docs: https://httpd.apache.org/docs/2.4/
      Tasks: 31 (limit: 3943)
     Memory: 50.3M (peak: 51.2M)
        CPU: 1.992s
     CGroup: /system.slice/apache2.service
             ├─1411 /usr/sbin/apache2 -k start
             ├─1413 /usr/sbin/apache2 -k start
             ├─1417 "Passenger watchdog"
             ├─1425 "Passenger core"
             ├─1485 /usr/sbin/apache2 -k start
             ├─1486 /usr/sbin/apache2 -k start
             ├─1487 /usr/sbin/apache2 -k start
             ├─1488 /usr/sbin/apache2 -k start
             └─1489 /usr/sbin/apache2 -k start

May 10 03:06:11 unadserver.unad.com systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 10 03:06:12 unadserver.unad.com systemd[1]: Started apache2.service - The Apache HTTP Server.
mateoserver@unadserver:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2026-05-10 03:04:12 UTC; 48min ago
   Main PID: 636 (vsftpd)
      Tasks: 1 (limit: 3943)
     Memory: 932.0K (peak: 1.5M)
        CPU: 113ms
     CGroup: /system.slice/vsftpd.service
             └─636 /usr/sbin/vsftpd /etc/vsftpd.conf

May 10 03:04:11 unadserver.unad.com systemd[1]: Starting vsftpd.service - vsftpd FTP server...
May 10 03:04:12 unadserver.unad.com systemd[1]: Started vsftpd.service - vsftpd FTP server.
mateoserver@unadserver:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sun 2026-05-10 03:06:11 UTC; 47min ago
TriggeredBy: ● ssh.socket
```

Fuente: Autoria Propia

Se despliega el estado activo de Apache, vsftpd y SSH verificado con systemctl status, confirmando la disponibilidad de los servicios en la zona ORANGE.

Se muestra la página por defecto de Apache visualizada desde el navegador del Ubuntu Desktop, confirmando el acceso HTTP controlado desde la zona GREEN hacia la DMZ.

Figura 12.
Acceso servidor Apache en la zona GREEN



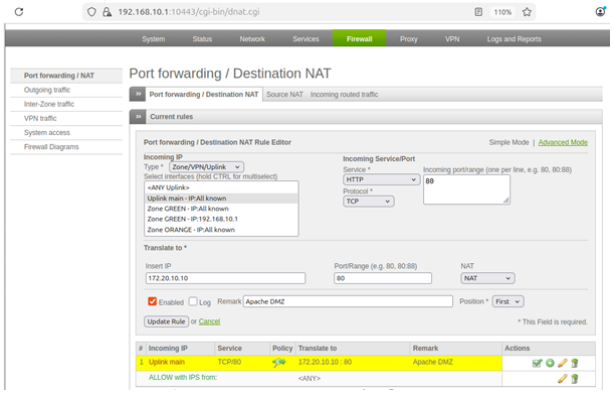
Fuente: Autoría Propia

3.5 CONFIGURACIÓN DE REGLAS FIREWALL EN ENDIAN

Se configuró una regla de Port Forwarding en Endian para redirigir el tráfico HTTP entrante por la WAN hacia el servidor Apache en la DMZ, validando la publicación del servicio desde la interfaz RED.

Se observa la regla de Destination NAT configurada en Endian redireccionando el tráfico HTTP entrante hacia el servidor Apache en la zona ORANGE, validando la publicación controlada del servicio desde la WAN.

Figura 13.
Regla Port Forwarding en Endian



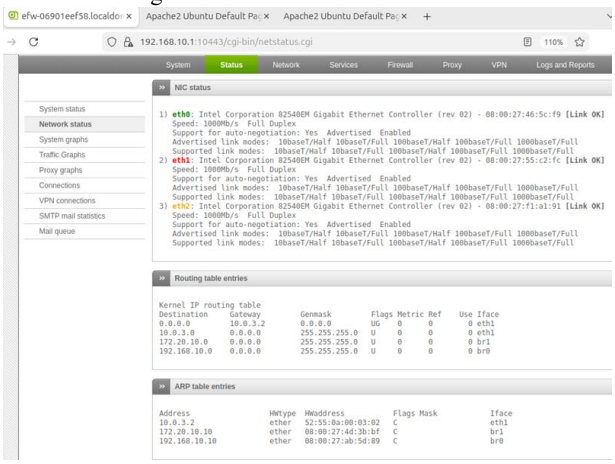
Fuente: Autoría Propia

3.6 VALIDACIONES FINALES

Se realizaron pruebas de conectividad desde todas las zonas y se verificó desde la interfaz web de Endian el estado operativo de las tres interfaces con sus tablas de enrutamiento y ARP.

Se presenta el estado UP de las tres interfaces, la tabla de enrutamiento del kernel y la tabla ARP desde la interfaz web de Endian, confirmando el funcionamiento completo de la infraestructura implementada.

Figura 14.
Validación integral de la infraestructura



Fuente: Autoría Propia

4 CONFIGURACION NAT

Para el desarrollo de la configuración NAT, es de gran importancia el reconocimiento de los conceptos básicos que esta la componen.

NAT es una tecnología fundamental en el ámbito de las redes que permite la traducción de direcciones IP dentro de una red privada a una dirección IP pública, facilitando la comunicación entre redes internas e Internet [7].

SNAT: (Source NAT / Masquerading): Cambia la IP origen, este es usado para configurar la salida de la red privada a internet.

DNAT: (Destination NAT / Port Forwarding): Cambia la IP destino, se usa para la publicación de aplicaciones privadas a internet, es decir, que alguien externo puedo acceso a la aplicación por medio de la traducción de la IP publica a la IP privada donde se aloja la aplicación o servicio.

El funcionamiento de NAT se fundamenta en la modificación de direcciones IP de origen o destino dentro del proceso de comunicación TCP/IP, permitiendo la interconexión entre redes privadas y redes externas [8].

La configuración de la red de cada uno de los equipos tienen una función muy importante, normalmente configuramos una IP estática con el comando ip addr add, sin embargo en varias distribuciones esta configuración solo aplica de manera temporal ya que esta se almacena en RAM, por lo que cuando la maquina es reiniciada pierde la conexión, es por esto que se implementa el uso de archivos YAML por medio del comando **sudo vim /etc/netplan/00-installer-config.yaml**, con este se asigna la IP estática de manera que con el reinicio esta no se desconfigure.

Figura 15.
Configuración archivo YAML

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 172.20.10.2/24
      routes:
        - to: default
          via: 172.20.10.1
      nameservers:
        addresses:
          - 8.8.8.8
```

Fuente: Autoría Propia

Una vez guardado el archivo cambiamos los permisos a 600 y se ejecuta **sudo netplan apply**, esto con el fin de cargar la configuración del archivo YAML.

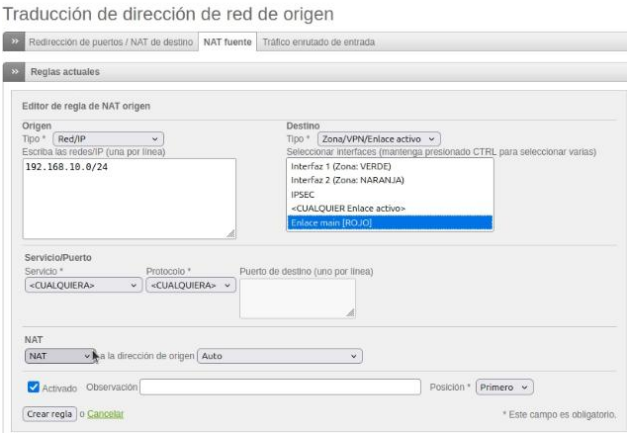
4.1 CONFIGURACIÓN DE NAT ZONA VERDE Y NARANJA

Desde el equipo cliente, ingresamos por el navegador web a https://192.168.10.1:10443/ e iniciamos sesión, donde veremos el dashboard inicial y el estado del Firewall.

En este nos dirigiríamos a la pestaña Firewall, luego en Redirección de puertos NAT seleccionamos la pestaña NAT Fuente, donde podremos distinguir las reglas NAT configuradas tanto propias poco las del sistema dando clic en Mostrar reglas del sistema.

Añadimos la nueva regla NAT origen, em el campo origen seleccionamos el tipo Red/Ip en el cual digitamos el direccionamiento de nuestra red verde 192.168.10.0/24, en el destino dejamos el Tipo Zona/VPN/Enlace activo y seleccionamos Enlace main (ROJO), la cual corresponde a nuestra zona roja WAN. Dejamos todos los puertos y protocolos y en tipo de NAT la dejamos de manera automática. Una vez se diligencian los campos, creamos la regla.

Figura 16.
Creación de regla SNAT para zona verde



Fuente: Autoría Propia

Igual que la regla anterior, aplicamos la misma configuración, solo que esta el origen será el direccionamiento que se ha asignado a nuestra zona naranja, es decir, 172.20.10.0/24. Se crea y aplica los cambios. Con estos verificamos en pantalla la creación de las dos reglas.

Figura 17.
Listado de reglas SNAT

Fuente: Autoría Propia

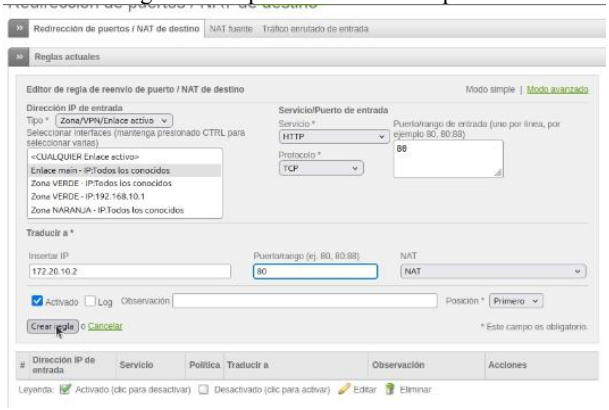
4.2 CONFIGURAR DNAT / PORT FORWARDING

Desde el equipo cliente, ingresamos por el navegador web a https://192.168.10.1:10443/ e iniciamos sesión, donde veremos el dashboard inicial y el estado del Firewall. En este nos dirigimos a la opción Firewall donde selecciona Redirección de puertos y posteriormente NAT de destino.

Para la creación de la regla DNAT para el acceso desde internet a nuestra aplicación web seleccionamos el acceso a Agregar nueva regla de reenvió de puertos / NAT de destino.

En dirección de IP de Entrada, se selecciona el tipo Zona/VPN/Enlace activo, en el cual selecciona Enlace main (ROJO) correspondiente a la WAN, seleccionamos el protocolo el cual será TCP, y en puertos digitamos 80, el cual es el puerto donde está expuesta la aplicación en apache, al digitar el puerto distinguirá el servicio de puerto de entrada el cual en este caso es HTTP. En traducir a digitamos la IP de nuestro servidor de aplicaciones ubicado en nuestra zona naranja DMZ, es decir, 172.20.10.2, así mismo el puerto por el que la aplicación es visible. La activamos y creamos la regla.

Figura 18.
Creación de regla DNAT para el servidor de aplicaciones



Fuente: Autoría Propia

Se procede a hacer el mismo proceso, pero con el puerto 21 para exponer a internet el servidor de FTP. Posteriormente podremos notar las reglas creadas.

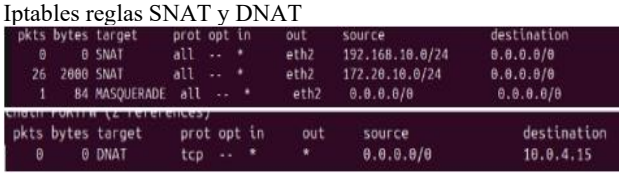
Figura 19.
Listado de reglas DNAT

Fuente: Autoría Propia

4.3 VERIFICACIÓN DE REGLAS

Para la verificación de pruebas nos conectamos por ssh al firewall Endian con las credenciales anteriormente asignadas por medio del comando **ssh root@192.168.10.1**. Verificamos la creación de las reglas con **iptables -t nat -L -n -v**. En los resultados mostrados verificamos la creación de las 4 creadas tanto las SNAT como las DNAT.

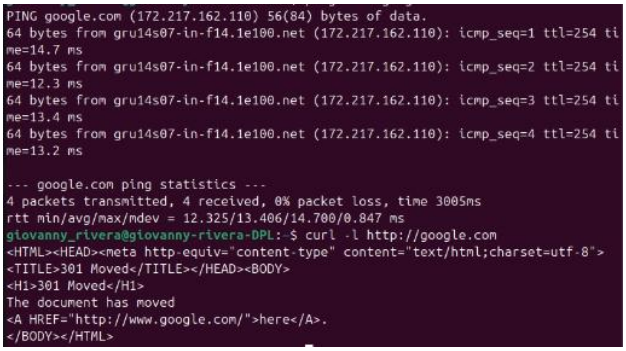
Figura 20.
Iptables reglas SNAT y DNAT



Fuente: Autoría Propia

En la regla DNAT podemos distinguir la ip de destino la cual será traducida hacia el servidor de aplicación. Así mismo, validamos la salida a internet de las zonas haciendo un ping a la ip 8.8.8.8 y curl a Google.com (**curl -l http://google.com**)

Figura 21.
Prueba de comunicación de salida



Fuente: Autoría Propia

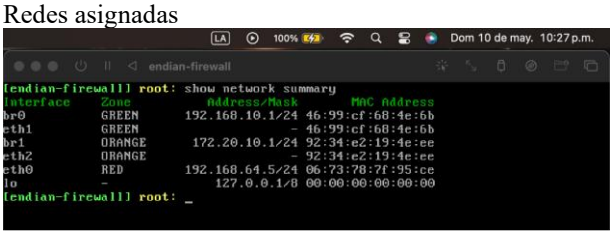
5 SERVICIOS DE LA ZONA DMZ

En esta sección se describe el proceso realizado para la implementación y configuración de Endian Firewall y Ubuntu Server dentro de una zona DMZ. Durante la práctica se verificó la conectividad entre equipos, se habilitaron los servicios HTTP y FTP y posteriormente se aplicaron reglas de firewall para controlar el tráfico de red y bloquear el protocolo ICMP.

5.1 VERIFICACIÓN DE ENDIAN FIREWALL

En esta primera isntanacia se verificó que Endian Firewall reconociera correctamente las tres zonas de red configuradas dentro de la infraestructura virtualizada: GREEN para la red interna, ORANGE para la DMZ y RED para la salida hacia Internet. Esta segmentación permite tener organizado el tráfico de manera más segura, separando los servicios públicos de los equipos internos y reduciendo riesgos de acceso no autorizado. Además, se comprobó que cada interfaz estuviera activa y funcionando correctamente antes de continuar con la implementación de los servicios de red.

Figura 22.
Redes asignadas



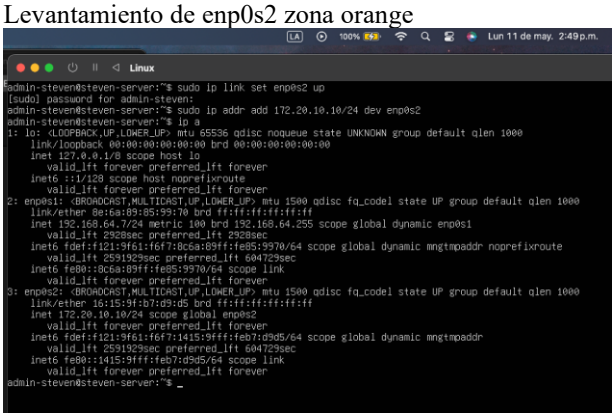
Fuente: Autoría Propia

La validación realizada desde la consola de Endian permitió identificar las direcciones IP asignadas a cada zona y confirmar que el firewall estaba gestionando adecuadamente la comunicación entre las diferentes redes.

5.2 CONFIGURACIÓN DE UBUNTU SERVER EN LA DMZ

Posteriormente se realizó la configuración del servidor Ubuntu dentro de la zona DMZ, asignándole una dirección IP estática mediante el comando ip addr add. Esta configuración permite mantener una conectividad estable y permanente dentro de la infraestructura, evitando cambios de direccionamiento después de reinicios del sistema. Con esta interfaz asociada a la zona ORANGE se habilita el propósito de alojar los servicios que serían publicados y controlados por el firewall.

Figura 23.
Levantamiento de enp0s2 zona orange



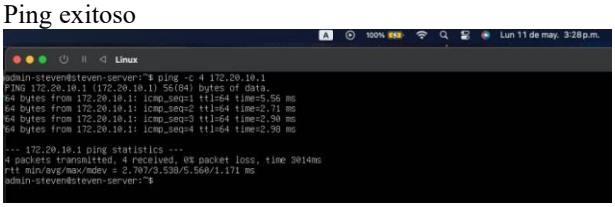
Fuente: Autoría Propia

Una vez habilitada la interfaz de red, se verificó que el servidor reconociera correctamente la puerta de enlace configurada en Endian Firewall y que existiera comunicación con las demás zonas autorizadas.

5.3 VERIFICACIÓN DE CONECTIVIDAD

Después de configurar la red del servidor, se realizaron pruebas de conectividad utilizando el comando ping entre Ubuntu Server y Endian Firewall. Con esto se valida que no existan errores en el direccionamiento IP, la máscara de red o la puerta de enlace configurada en la DMZ.

Figura 24.
Ping exitoso



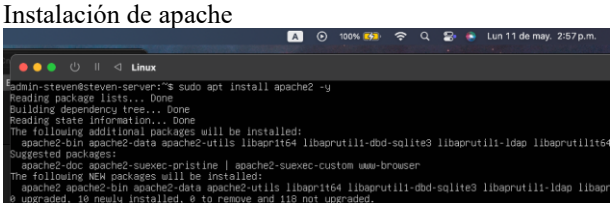
Fuente: Autoría Propia

Con una respuesta satisfactoria de los paquetes ICMP confirmó que la comunicación entre el firewall y el servidor se encontraba operativa. Por lo que se garantiza la estabilidad en la comunicación dentro de la infraestructura segmentada.

5.4 INSTALACIÓN DE SERVICIOS HTTP Y FTP

Se procede con la instalación y habilitación de los servicios Apache y VSFTPD para permitir servicios web y FTP dentro de la zona DMZ.

Figura 25.
Instalación de apache

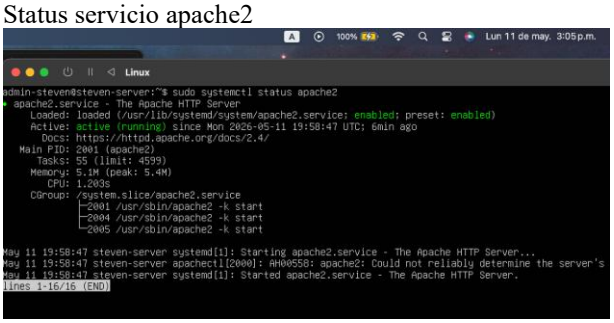


Fuente: Autoría Propia

Aplicando la instalación del servicio Apache2 utilizando el gestor de paquetes de Ubuntu Server, permitiendo implementar un servidor web dentro de la zona DMZ. Este servicio fue configurado para atender solicitudes HTTP sobre el puerto 80, posibilitando posteriormente el acceso desde la red LAN y desde la WAN mediante las reglas configuradas en Endian Firewall.

Con la verificación del estado de Apache se permite confirmar que el servicio web se encontraba activo y funcionando correctamente. Mediante el comando systemctl status apache2, donde se validó que el servidor iniciara automáticamente junto con el sistema operativo y permaneciera disponible para atender conexiones entrantes.

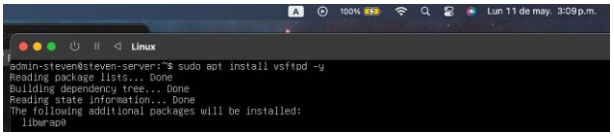
Figura 26.
Status servicio apache2



Fuente: Autoría Propia

Posteriormente se instaló el servicio VSFTPD, utilizado para la transferencia de archivos mediante el protocolo FTP. Este servicio fue implementado dentro de la DMZ con el objetivo de permitir el intercambio controlado de información entre usuarios autorizados y el servidor.

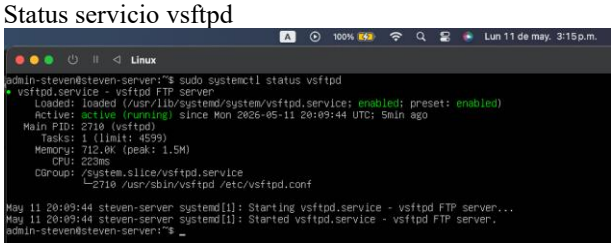
Figura 27.
Instalación VSFTPD



Fuente: Autoría Propia

Igual que el servicio Apache2, procedemos con la validación del servicio VSFTPD permitió comprobar que el servidor FTP se encontraba activo y escuchando conexiones sobre el puerto 21. Además, se verificó que el servicio estuviera habilitado para iniciar automáticamente, asegurando disponibilidad continua dentro de la infraestructura.

Figura 28.
Status servicio vsftpd

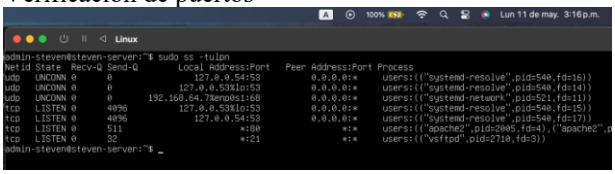


Fuente: Autoría Propia

5.5 VERIFICACIÓN DE PUERTOS ABIERTOS

Con los servicios instalados, se verifica que los puertos correspondientes a HTTP (80) y FTP (21) se encontraran habilitados y en estado LISTEN.

Figura 29.
Verificación de puertos



Fuente: Autoría Propia

Con estos resultados se permite identificar que los puertos 80 y 21 se encontraban en estado LISTEN, indicando que los servicios HTTP y FTP estaban disponibles dentro de la DMZ y listos para ser accedidos según las reglas definidas en el firewall.

5.6 CONFIGURACIÓN DE REGLAS EN ENDIAN

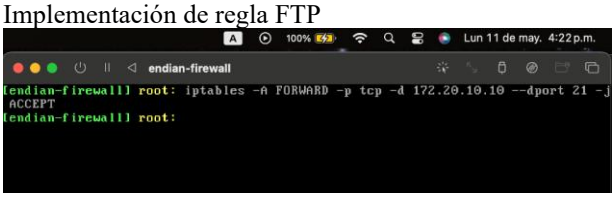
Se configuraron reglas en Endian Firewall para permitir tráfico HTTP y FTP hacia el servidor Ubuntu ubicado en la DMZ. Esta política permite controlar el acceso al servicio web desde otras zonas de red de manera segura y organizada.

Figura 31.
Implementación de regla HTTP

Fuente: Autoría Propia

De igual forma, se creó una regla para habilitar el tráfico FTP hacia el servidor Ubuntu. Esta configuración permite controlar el acceso al servicio de transferencia de archivos, asegurando que únicamente el tráfico autorizado pudiera establecer conexión con el servidor.

Figura 31.
Implementación de regla FTP

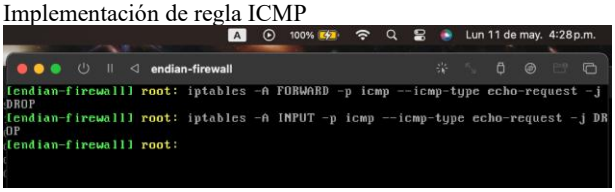


Fuente: Autoría Propia

5.7 BLOQUEO DEL PROTOCOLO ICMP

Finalmente se implementan las reglas para bloquear solicitudes ICMP tipo echo-request con el fin de impedir respuestas a ping. Esta restricción ayuda a reducir tareas de reconocimiento de red realizadas desde equipos externos mediante el uso de ping.

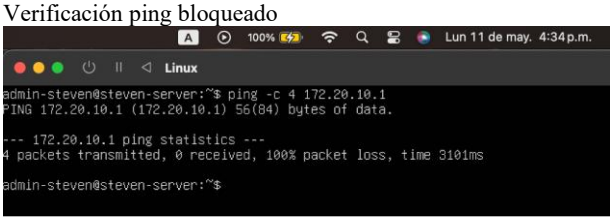
Figura 32.
Implementación de regla ICMP



Fuente: Autoría Propia

Tras realizar las pruebas se demuestra que las solicitudes ICMP eran rechazadas correctamente por el firewall. A pesar del bloqueo del protocolo ping, los servicios HTTP y FTP continuaron funcionando con normalidad, evidenciando que las políticas aplicadas no afectaron la disponibilidad de los servicios autorizados.

Figura 33.
Verificación ping bloqueado

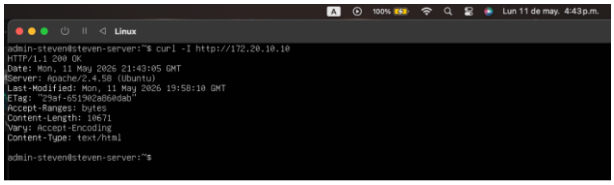


Fuente: Autoría Propia

5.8 VALIDACION FINAL

Finalmente, se realizaron pruebas generales de funcionamiento para verificar que los servicios publicados en la DMZ continuaran accesibles después de aplicar las reglas de seguridad en Endian Firewall. Por lo tanto, posteriormente a aplicar el bloqueo ICMP, se verificó que el servicio HTTP continuara funcionando correctamente.

Figura 34.
Verificación funcionamiento HTTP



Fuente: Autoría Propia

Con estas validaciones se confirma que la infraestructura segmentada funcionaba correctamente, permitiendo únicamente el tráfico autorizado entre las diferentes zonas de red. De esta manera, se logró implementar un entorno más seguro, controlado y estable para la publicación de servicios dentro de la DMZ.

6 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO. PRODUCTO ESPERADO

6.1 ARQUITECTURA DE RED Y SEGMENTACIÓN DE ZONAS DE SEGURIDAD

La base del proyecto fue el diseño de una arquitectura de red perimetral utilizando el sistema Endian Firewall Community. La segmentación se realizó bajo un modelo de defensa en profundidad, categorizando el tráfico en tres zonas de seguridad distintas:

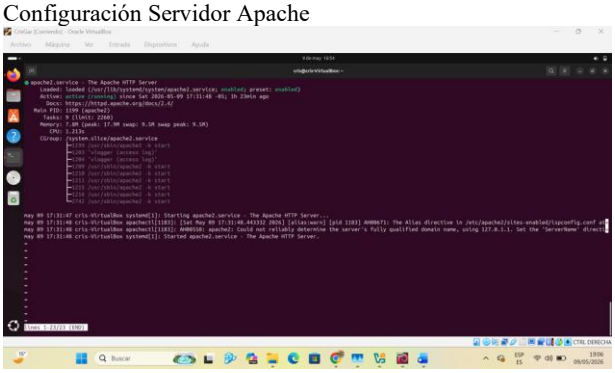
1. Zona Verde (LAN): Segmento de confianza donde reside el cliente (Ubuntu Desktop) con la IP 10.0.2.15.
2. Zona Naranja (DMZ): Zona de servicios donde se alojó el servidor Ubuntu Server (IP 10.0.3.15), encargado de los servicios críticos de Apache y FTP.
3. Zona Roja (WAN): Interfaz conectada a la red externa, simulando el acceso desde internet para las pruebas de penetración y disponibilidad.

Este esquema de segmentación es vital en la administración de sistemas Open Source, ya que permite que, en caso de que un servicio en la DMZ sea comprometido, el atacante no tenga una ruta directa hacia la red interna (LAN).

6.2 CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR UBUNTU (DMZ)

Previo a la implementación de las reglas, se procedió a la optimización de los servicios en el nodo de la DMZ. Se instaló el servidor web Apache2, verificando su estado mediante systemctl status apache2. Para el intercambio de archivos, se configuró vsftpd, ajustando el archivo de configuración /etc/vsftpd.conf para permitir el acceso a usuarios locales y asegurar que el servicio operara en los puertos estándar. La comunicación entre nodos se validó mediante el protocolo ICMP para asegurar la visibilidad básica antes de aplicar las restricciones del firewall.

Figura 35.
Configuración Servidor Apache



Fuente: Autoría Propia

6.3 GESTIÓN DE REGLAS INTER-ZONA Y POLÍTICAS DE ACCESO

El núcleo técnico se desarrolló en el módulo Inter-Zone Traffic. Se aplicó una política de denegación por defecto (Default Drop), abriendo únicamente los flujos necesarios:

- LAN → DMZ (HTTP/FTP): Se habilitó el acceso para que los administradores y usuarios internos pudieran gestionar el contenido web y cargar archivos al servidor.
- DMZ → WAN: Se permitió la salida del servidor hacia internet exclusivamente para la actualización de paquetes y repositorios mediante los puertos 80 y 443, restringiendo cualquier otro tipo de tráfico no iniciado por el servidor.

Figura 36.
Resumen de Reglas Inter-Zone traffic

Fuente: Autoría Propia

6.4 IMPLEMENTACIÓN DE NAT Y PORT FORWARDING (ACCESO DESDE LA WAN)

Para la publicación de los servicios hacia la red externa (WAN), se configuraron reglas de DNAT (Destination NAT) en el apartado de Port Forwarding. Esta configuración permite que las peticiones que llegan a la IP de la Zona Roja en los puertos 80 y 21 sean redirigidas de forma segura a la IP 10.0.3.15 de la DMZ. Este proceso oculta la estructura de direccionamiento interno de la organización, proporcionando una capa adicional de seguridad conocida como "seguridad por oscuridad", donde el atacante externo solo conoce la IP del firewall y no la del servidor real.

Figura 37.
Resumen de Reglas Port forwarding / NAT

Fuente: Autoría Propia

6.5 VERIFICACIÓN TÉCNICA Y AUDITORÍA DE TRÁFIC

La validación de reglas mediante iptables permite inspeccionar cadenas, políticas y contadores de paquetes asociados al filtrado y traducción de tráfico en sistemas GNU/Linux [9].

La validación de la seguridad se ejecutó en tres niveles técnicos:

- La comprobación de la infraestructura se realizó mediante pruebas de conectividad cruzada:
- Validación HTTP: Se utilizó el comando curl -I http://10.0.2.15 (o la IP correspondiente) desde una terminal externa para analizar el código de estado devuelto por el servidor. La obtención de un encabezado HTTP/1.1 200 OK confirmó que el firewall estaba permitiendo y redireccionando correctamente el tráfico web.
- Validación FTP: Se ejecutó el comando ftp seguido de la IP pública, logrando una autenticación exitosa. Se verificó que el firewall gestionara correctamente el paso de los comandos de control y la apertura dinámica de puertos para la transferencia de datos.
- Inspección de Iptables: Se accedió por SSH a la consola de Endian para ejecutar el comando iptables -L -n -v. Esta acción permitió observar los contadores de paquetes, confirmando de manera empírica que el tráfico estaba "macheando" con las reglas configuradas.

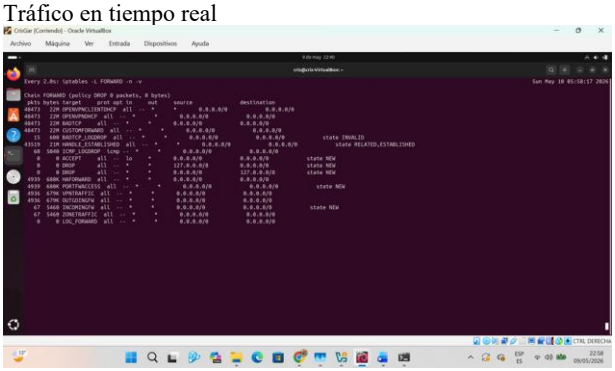
Figura 38.
Revisión de salida esperad HTTP/1.1 200 OK.

Fuente: Autoría Propia

6.6 MONITOREO Y GESTIÓN DE TRÁFICO EN TIEMPO REAL

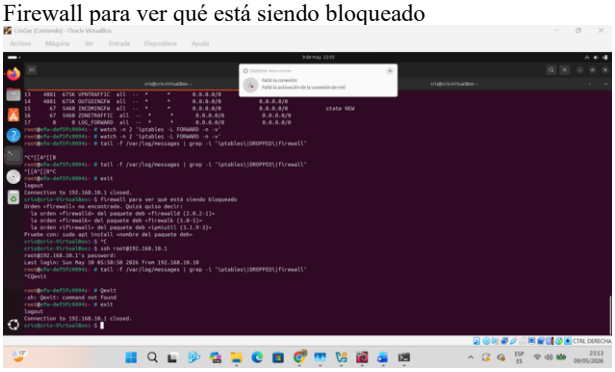
Como fase final, se utilizó el monitor de tráfico de Endian para supervisar el ancho de banda consumido durante las pruebas. Se prestó especial atención al Firewall Log, el cual permitió identificar y analizar paquetes bloqueados. Esta capacidad de auditoría es esencial para un administrador de sistemas, ya que permite diferenciar entre un fallo de configuración y un intento legítimo de escaneo de puertos por parte de terceros.

Figura 39.
Tráfico en tiempo real



Fuente: Autoría Propia

Figura 40.
Firewall para ver qué está siendo bloqueado



Fuente: Autoría Propia

7 IMPLEMENTACION DE PROXY HTTP

En los entornos de red empresariales, el control del acceso a Internet es un componente esencial de la seguridad perimetral. El uso de un proxy HTTP permite regular la navegación de los usuarios, aplicar políticas de autenticación y restringir el acceso a contenidos no autorizados, reduciendo riesgos de seguridad y mejorando el control administrativo.

En esta temática se describe la implementación conceptual y funcional de un proxy HTTP no transparente utilizando la plataforma Endian Firewall Community, haciendo énfasis en la autenticación de usuarios y el uso de listas negras para el control de acceso a sitios web desde la red LAN hacia Internet.

7.1 IMPLEMENTACIÓN PROXY HTTP NO TRANSPARENTE

El proxy HTTP fue implementado utilizando el módulo nativo de Proxy HTTP de Endian Firewall Community, el cual gestiona internamente el servicio Squid desde su panel de administración Web.

El uso de un proxy HTTP como Squid permite centralizar el control de navegación, aplicar autenticación de usuarios y establecer políticas de filtrado de contenido web [10].

Características principales del proxy configurado:

- Tipo de proxy: No transparente (explícito).
- Puerto de escucha: 3128.
- Modo de operación: Autenticado.

Acceso controlado mediante políticas por usuario y grupo.
La activación del proxy se realizó desde la interfaz administrativa segura de Endian, accesible únicamente desde la zona LAN.

Figura 41.
Implementación de proxy HTTP

Fuente: Autoría Propia

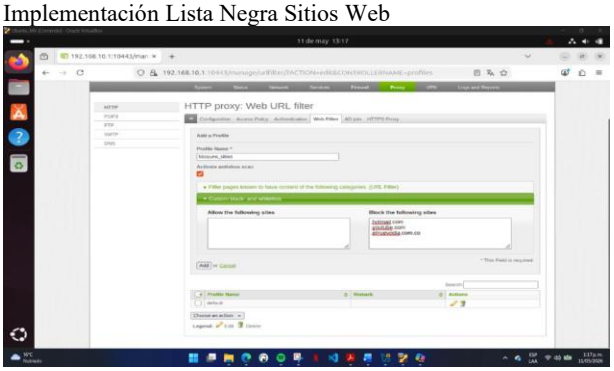
7.2 LISTA NEGRA SITIOS WEB

Como parte del control de navegación, se creó una lista negra con los siguientes dominios, los cuales deben ser bloqueados para los usuarios autenticados:

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

Estas restricciones permiten demostrar la efectividad del proxy en la aplicación de políticas de filtrado de contenido, impidiendo el acceso a sitios no permitidos desde la red interna.

Figura 42.
Implementación Lista Negra Sitios Web



Fuente: Autoría Propia

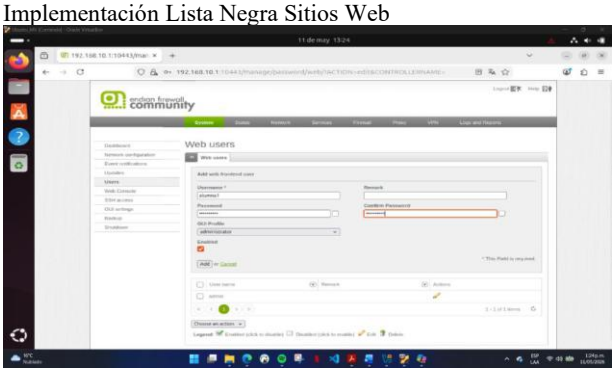
7.3 AUTENTICACIÓN USUARIOS DE GRUPO

Se implementó autenticación por usuario, creando usuarios específicos asociados a un grupo de navegación. La política de acceso al proxy fue configurada de forma que:

- Solo usuarios autenticados pueden navegar por Internet.
- Las políticas de filtrado se aplican en función del grupo asignado.
- El acceso es denegado automáticamente cuando se intenta acceder a un sitio contenido en la lista negra.

Este mecanismo garantiza trazabilidad, control individual de acceso y mayor seguridad perimetral.

Figura 43.
Implementación Lista Negra Sitios Web



Fuente: Autoría Propia

8 CONCLUSIONES

La implementación de Endian Firewall Community permitió comprender y aplicar los principios de seguridad perimetral en entornos GNU/Linux, integrando una infraestructura segmentada mediante las zonas GREEN, RED y ORANGE para controlar el tráfico de red y proteger los servicios implementados dentro de la LAN, la WAN y la DMZ.

La configuración de reglas NAT, Port Forwarding y políticas de acceso facilitó el control de las comunicaciones entre las diferentes zonas de red, permitiendo tanto la salida segura hacia Internet como la publicación controlada de servicios empresariales alojados en la DMZ, fortaleciendo así la administración y protección de la infraestructura virtualizada.

La implementación y validación de servicios como HTTP, FTP y SSH evidenció el correcto funcionamiento de los mecanismos de seguridad y segmentación de red, permitiendo establecer comunicaciones autorizadas entre la LAN, la WAN y la DMZ, mientras se restringieron protocolos y accesos no permitidos para mejorar la seguridad del entorno.

La configuración del proxy HTTP no transparente y las políticas de autenticación demostraron la importancia del control de navegación y filtrado de contenidos dentro de una red empresarial, permitiendo restringir el acceso a sitios web definidos mediante listas negras y reforzando las políticas de seguridad informática.

El desarrollo de la práctica fortaleció los conocimientos técnicos relacionados con virtualización, administración de sistemas GNU/Linux, configuración de firewalls y monitoreo de tráfico mediante herramientas como iptables, consolidando habilidades prácticas para la implementación de soluciones seguras y eficientes en infraestructuras de red empresariales.

9 REFERENCIAS

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

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

[3] W. R. Cheswick, S. M. Bellovin y A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2003.

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

[5] Canonical (2023). *Help Ubuntu. Ubuntu*. https://help.ubuntu.com/

[6] Jay LaCroix. (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

[7] OpenWebinars. (s. f.). *NAT: qué es y para qué sirve*. Recuperado el 9 de mayo de 2026, de https://openwebinars.net/blog/nat-que-es-y-para-que-sirve/.

[8] R. W. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols.* Boston, MA, USA: Addison-Wesley, 1994.

[9] Netfilter Project, “netfilter/iptables project,” Netfilter. [En línea]. Disponible en: https://www.netfilter.org/. [Accedido: 12-may-2026].

[10] Squid Software Foundation, “Squid: Optimising Web Delivery,” Squid-cache.org. [En línea]. Disponible en: https://www.squid-cache.org/. [Accedido: 12-may-2026].