Implementando seguridad en GNU/Linux

Edwin Montoya Romero
e-mail: emontoyar@unadvirtual.edu.co
Anderson Amaya Ortiz
e-mail: integrante2@institución (quitar hipervínculo)
José Luis Peña Peña
e-mail: integrante3@institución (quitar hipervínculo)
William Andrés Rincon Rodríguez
e-mail: warinconro@unadvirtual.edu.co
Ronny Alexander Almeida Barbosa
e-mail: raalmeidab@unadvirtual.edu.co

RESUMEN: *El presente documento describe la implementación integral de un entorno de red segmentado mediante firewall Endian Community Edition, sobre el cual se desplegaron servicios de hosting con Ispconfig y aplicaciones web como WordPress, PrestaShop, Moodle y OwnCloud. Se configuraron las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), estableciendo reglas de firewall, NAT, Proxy autenticado y políticas de seguridad. El objetivo fue demostrar la administración de servicios de red bajo GNU/Linux, evidenciando la comunicación controlada entre zonas y el acceso a internet con restricciones.*

ABSTRACT: This document describes the comprehensive implementation of a segmented network environment using Endian Community Edition firewall, on which hosting services were deployed with Ispconfig and web applications such as WordPress, PrestaShop, Moodle, and OwnCloud. The Green (LAN), Red (WAN), and Orange (DMZ) zones were configured, establishing firewall rules, NAT, authenticated proxy, and security policies. The objective was to demonstrate the administration of network services under GNU/Linux, evidencing controlled communication between zones and internet access with restrictions.

PALABRAS CLAVE: Endian, firewall, NAT, DMZ, proxy, Ispconfig, WordPress, PrestaShop, Moodle, OwnCloud.

1. INTRODUCCIÓN

La administración de redes y servicios en entornos Linux requiere comprender la segmentación, el control de tráfico y la publicación segura de servicios. Este proyecto aborda la configuración de un firewall Endian con tres zonas funcionales (Verde, Roja y Naranja), la implementación de un panel de hosting (Ispconfig) y el despliegue de aplicaciones web (WordPress, PrestaShop, Moodle, OwnCloud) que cumplen funciones empresariales, comerciales, educativas y de almacenamiento. El documento se organiza en cinco temáticas principales, cada una con su respectivo desarrollo, evidencias y verificación de resultados.

2. OBJETIVOS

Objetivo general

Configurar interfaces de usuario y escritorio a través de tareas administrativas con los servicios esenciales dándole un óptimo nivel de seguridad al sistema operativo GNU Linux

Objetivos específicos

- Implementar el sistema operativo GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).
- Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).
- Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia Internet. Verificar en el reenvío de puertos / NAT, la creación de las reglas.
- Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.
- Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red.
- Implementar y validar reglas de acceso en un firewall que permitan, en primer lugar, la comunicación entre la zona Verde y la zona Naranja usando los protocolos HTTP (puerto TCP/80) y FTP (puertos TCP/20 y TCP/21); en segundo lugar, habilitar la comunicación desde la zona Internet hacia la zona DMZ; y finalmente, verificar mediante la generación y análisis de tráfico interzona, así como pruebas prácticas desde un navegador web, el correcto funcionamiento de las siguientes directivas: ingreso del servicio HTTP desde la LAN hacia la DMZ, desde la LAN hacia la WAN, desde la DMZ hacia la WAN, desde la WAN hacia la DMZ, así como el ingreso del servicio FTP desde la LAN hacia la WAN y desde la WAN hacia la DMZ, comprobando que las reglas creadas permitan o denieguen el tráfico según lo especificado.
- Implementar un proxy HTTP no transparente en el gateway de la red local, configurando políticas de

autenticación por usuario y grupo que permitan controlar el acceso a Internet; para ello, se debe crear un perfil de filtrado con una lista negra que bloquee el acceso a los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, posteriormente crear un usuario asociado a un grupo específico dentro del proxy, establecer una política de acceso que vincule dicho grupo con el perfil de lista negra y la autenticación requerida, y finalmente probar desde un navegador web en la zona LAN verificando que el acceso a los tres portales mencionados sea efectivamente denegado mientras que la navegación a otros sitios no bloqueados permanezca habilitada.

3. ENTORNO DE IMPLEMENTACIÓN

VirtualBox

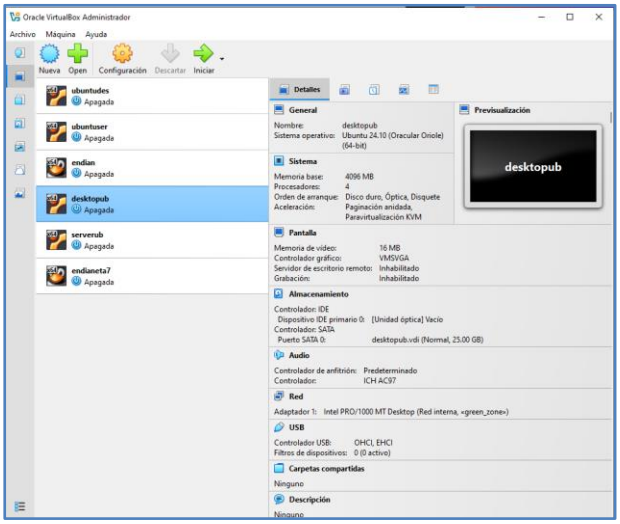

Figura 1 Software VirtualBox Fuente: Autoría propia

Configuración de red

Zona	Dirección IP	Descripción
Verde (LAN)	192.168.2.20	Cliente
	192.168.2.15	Ruta
Naranja (DMZ)	192.168.1.20	Cliente
	192.168.1.15	ruta
Roja	DHCP	WAN

Tabla 1. Segmentación de red Fuente: Autoría propia

3.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX – ENDIAN EN VIRTUAL BOX E INSTALACIÓN EFECTIVA DEL MISMO

En el paso 1 se instalaron las máquinas virtuales correspondientes al servidor, al cliente desktop y al firewall Endian.

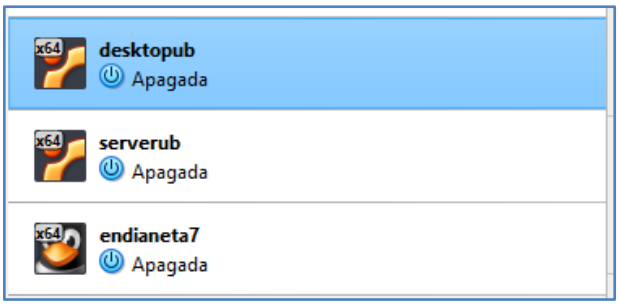

Figura 2. Máquinas virtuales instaladas Fuente: Autoría propia

En al paso 2 se configuraron los adaptadores de red en la VM Endian así:

Adaptador 1 green_zone
Adaptador 2 orange_zone
Adaptador 3 NAT.

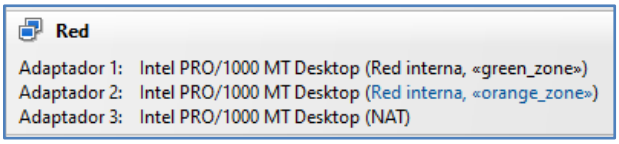

Figura 3. Configuración adaptadores 1 Fuente: Autoría propia

En el paso 3 se configuró la VM Endian en el Desktop Ubuntu

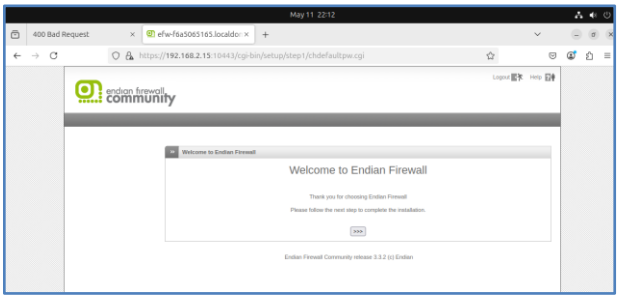

Figura 4. Configuración Endian en VM 1 Fuente: Autoría propia

En el paso 4 se realizó la configuración en la consola de la VM Endian.

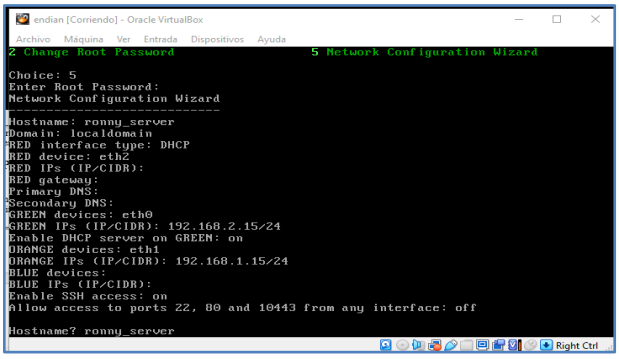

Figura 5. Configuración consola Endian 1 Fuente: Autoría propia

En el quinto paso se configuro las direcciones IP fijas para el servidor y el desktop

```
ronny_almeida@localhost:~$ sudo ip addr add 192.168.2.20/24 dev enp0s3
[sudo] password for ronny_almeida:
ronny_almeida@localhost:~$ sudo ip link set enp0s3 up
ronny_almeida@localhost:~$ sudo ip route add default via 192.168.2.15
ronny_almeida@localhost:~$
```

Figura 6. Configuración IP Desktop 1 Fuente: Autoría propia

```
ronny_server@serverub:~$ sudo ip addr add 192.168.1.20/24 dev enp0s3
ronny_server@serverub:~$ sudo ip link set enp0s3 up
ronny_server@serverub:~$ sudo ip route add default via 192.168.1.15
ronny_server@serverub:~$
```

Figura 7. Configuración IP Server 1 Fuente: Autoría propia

En el sexto paso se verificó conexión entre el servidor y el cliente desktop

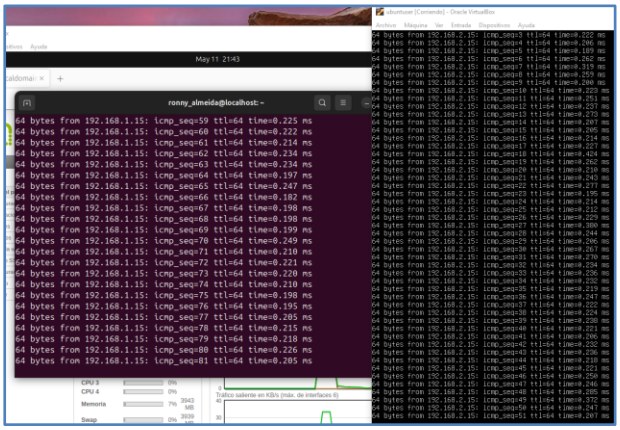

Figura 8. Conexión Desktop y Server 1 Fuente: Autoría propia

Finalmente, en el séptimo paso se verificó la conexión en el Dashboard de Endian ejecutado remotamente en el desktop.

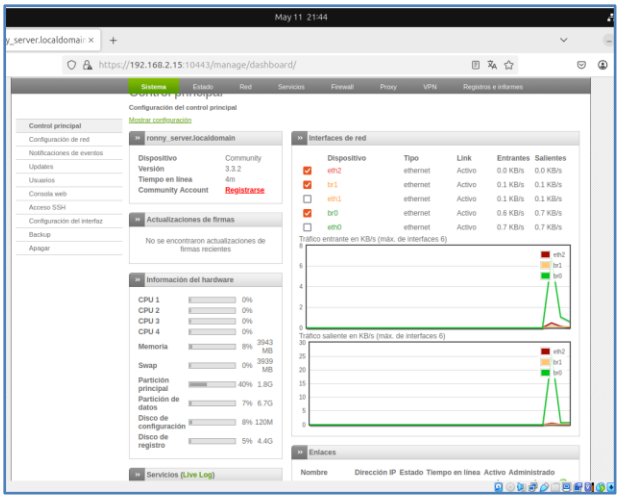

Figura 9. Verificar conexión Dashboard 1 Fuente: Autoría propia

3.2 CONFIGURACIÓN NAT

La segmentación de red mediante zonas permite controlar el flujo de información entre los diferentes segmentos que conforman la infraestructura. En este proyecto, se implementó Endian Firewall Community como dispositivo de seguridad perimetral, definiendo tres zonas claramente diferenciadas: zona verde (LAN) para los equipos de usuario final con direccionamiento 192.168.100.0/24, zona naranja (DMZ) para los servidores públicos con direccionamiento 192.168.200.0/24 y zona roja (WAN) como interfaz de salida a Internet mediante DHCP. Uno de los mecanismos fundamentales para garantizar la conectividad controlada entre estas zonas es la traducción de direcciones de red (NAT). A continuación, se describen las configuraciones realizadas para establecer comunicación desde la LAN hacia la WAN, desde la DMZ hacia Internet y el reenvío de puertos hacia los servicios alojados en la zona DMZ.

Reglas NAT implementadas

Se crearon dos reglas de tipo Source NAT dentro de la interfaz web de Endian Firewall, accediendo a la ruta Firewall → Port forwarding / NAT → Source NAT. La primera regla permite que todos los equipos de la red LAN puedan alcanzar recursos externos, mientras que la segunda regla habilita la salida a Internet desde los servidores ubicados en la DMZ.

Tipo de NAT	Origen	Destino
Comunicación LAN → WAN	192.168.100.0/24	0.0.0.0/0
Comunicación DMZ → Internet	192.168.200.0/24	0.0.0.0/0
Reenvío de puertos (WAN → DMZ)	WAN (puerto 8080)	192.168.200.2 (puerto 80)

Tabla 2. Reglas NAT configuradas en Endian Firewall Fuente: Autoría propia

En la siguiente imagen se evidencia la creación de la regla Source NAT correspondiente a la red LAN, donde se especifica la red de origen, el destino cualquier dirección y la habilitación de la regla.

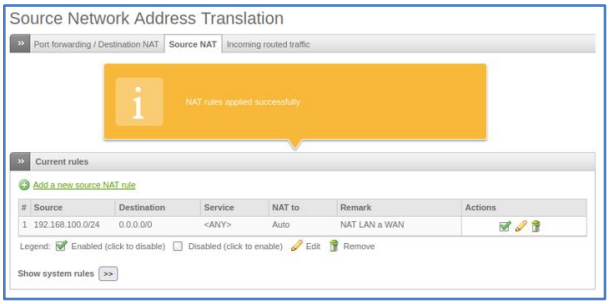

Figura 10. Regla Source NAT com. LAN -> WAN Fuente: Autoría propia

Posteriormente, se agregó una segunda regla Source NAT destinada a la zona DMZ, manteniendo el mismo destino

cualquier dirección para permitir la navegación y actualizaciones desde los servidores alojados en este segmento.

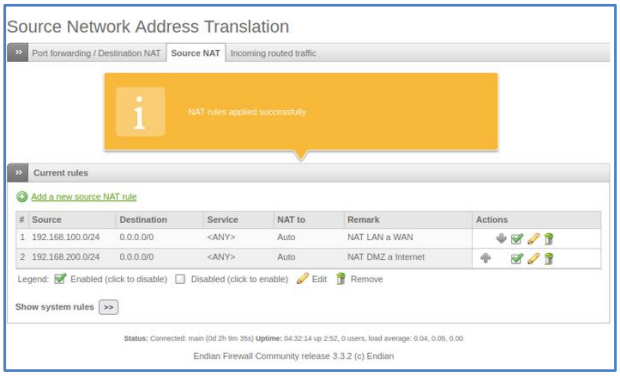

Figura 11. Regla Source NAT activas para LAN y DMZ Fuente: Autoría propia

Verificación de conectividad desde la LAN hacia Internet

Para comprobar el correcto funcionamiento de la regla NAT que permite la salida desde la red LAN hacia la WAN, se utilizó la máquina virtual correspondiente al cliente ubicado en la zona verde con dirección IP 192.168.100.2. Desde su terminal se ejecutó el comando date con el fin de registrar la fecha y hora exacta de la prueba, seguido del comando ping 8.8.8.8.

3.2.5 La respuesta obtenida muestra paquetes ICMP con tiempos de respuesta, confirmando que el equipo logra comunicarse con servidores externos a través del firewall, lo cual valida la correcta traducción de direcciones implementada.

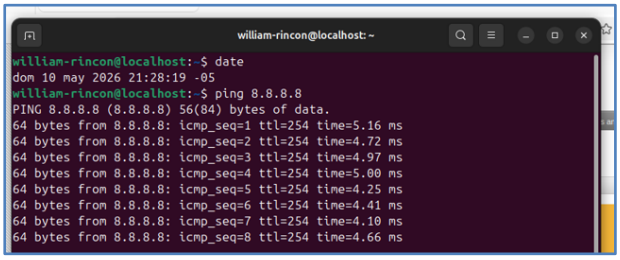

Figura 12. Prueba de conectividad cliente LAN - Internet Fuente: Autoría propia

3.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

El objetivo principal fue configurar una red virtualizada donde un servidor Ubuntu Server ubicado en la zona DMZ ofreciera los servicios HTTP y FTP, permitiendo el acceso desde un cliente Ubuntu ubicado en la LAN. Adicionalmente, se configuró una regla para denegar tráfico ICMP Echo Request, evitando que el servidor DMZ respondiera a solicitudes de ping desde la red interna.

Arquitectura de Red Propuesta

La topología implementada se compuso de tres máquinas virtuales:

Equipo	Función	Zona
Endian Firewall	Firewall y enrutador principal	RED, GREEN, ORANGE
Ubuntu Cliente	Cliente de red interna	GREEN / LAN
Ubuntu Server	Servidor HTTP y FTP	ORANGE / DMZ

Tabla 3. Segmentación red Fuente: Autoría propia

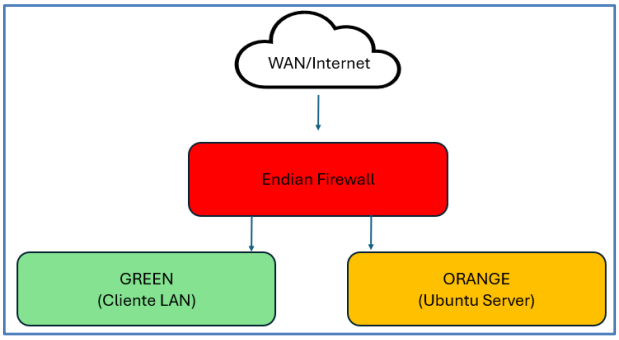

Figura 13. Segmentación red Fuente: Autoría propia

La segmentación por zonas permite separar los niveles de exposición de los equipos. La zona GREEN representa la red interna confiable, la zona ORANGE corresponde a la DMZ donde se alojan servidores publicados o semipúblicos, y la zona RED se utiliza como conexión hacia la WAN o Internet.

Zona	Equipo / Interfaz	Dirección IP	Función
GREEN	Endian br0	192.168.0.1/24	Gateway LAN
GREEN	Ubuntu Cliente	192.168.0.16/24	Cliente de prueba
ORANGE	Endian DMZ	192.168.10.1/24	Gateway DMZ
ORANGE	Ubuntu Server	192.168.10.10/24	Servidor HTTP/FTP
RED	Endian WAN	DHCP / NAT	Salida WAN

Tabla 4. Direccionamiento IP Fuente: Autoría propia

En Ubuntu Server se configuró una dirección estática mediante Netplan. Ubuntu Server utiliza Netplan para definir configuraciones de red como direcciones estáticas, rutas por defecto y servidores DNS, aplicando los cambios mediante el comando netplan apply.

La configuración lógica del servidor DMZ fue:

```
network:
 version: 2
 ethernets:
   enp0s3:
     dhcp4: false
     dhcp6: false
     addresses:
       - 192.168.10.10/24
     routes:
       - to: default
         via: 192.168.10.1
     nameservers:
       addresses:
         - 8.8.8.8
         - 1.1.1.1
```

Implementación de Servicios en Ubuntu Server
En el servidor Ubuntu ubicado en la DMZ se implementaron los servicios requeridos:

A. Servicio HTTP
Se habilitó un servicio web en el puerto TCP 80. Para fines de laboratorio, el servicio HTTP puede implementarse mediante Apache, Nginx o un servidor HTTP temporal con Python. La validación se realizó verificando que el puerto 80 estuviera en estado de escucha:

sudo ss -tulnp | grep ':80'
El resultado esperado fue:

tcp LISTEN 0 511 *:80 *:*
Esto confirmó que el servidor aceptaba conexiones entrantes en el puerto 80.

B. Servicio FTP
Para el servicio FTP se utilizó el puerto TCP 21. La validación se realizó mediante:

sudo ss -tulnp | grep ':21'
El objetivo fue permitir que el cliente ubicado en la red GREEN pudiera establecer conexión con el servidor FTP en la DMZ.

Configuración de Reglas en Endian Firewall
Endian organiza el control del tráfico en módulos específicos. Para esta práctica se utilizó principalmente Firewall → Inter-Zone traffic, ya que las reglas requeridas correspondían a tráfico entre la zona GREEN y la zona ORANGE. La documentación de Endian indica que esta sección permite definir cómo fluye el tráfico entre zonas internas distintas de RED.

Se crearon tres reglas principales.

A. Regla 1: Permitir HTTP desde LAN hacia DMZ

Campo	Valor
Source	GREEN
Destination	ORANGE
IP destino	192.168.10.10
Servicio	HTTP
Protocolo	TCP
Puerto	80
Política	Allow / Accept

Tabla 5. Regla 1 Fuente: Autoría propia

Esta regla permite que el cliente Ubuntu en la LAN accediera al servidor web ubicado en la DMZ.

Prueba realizada desde Ubuntu Cliente:

curl http://192.168.10.10

Resultado esperado:

Servidor Web DMZ funcionando

B. Regla 2: Permitir FTP desde LAN hacia DMZ

Campo	Valor
Source	GREEN
Destination	ORANGE
IP destino	192.168.10.10
Servicio	FTP
Protocolo	TCP
Puerto	21
Política	Allow / Accept

Tabla 6. Regla 2 Fuente: Autoría propia

Esta regla permitió la conexión hacia el servicio FTP del servidor DMZ.

Prueba desde Ubuntu Cliente:

ftp 192.168.10.10
o:
nc -vz 192.168.10.10 21

Resultado esperado:
Connection to 192.168.10.10 21 port [tcp/ftp] succeeded

C. Regla 3: Denegar ICMP hacia DMZ

Campo	Valor
Source	GREEN
Destination	ORANGE
IP destino	192.168.10.10
Servicio	ICMP / Echo Request
Tipo ICMP	8
Política	Deny / Drop / Reject

Tabla 7. Regla 3 Fuente: Autoría propia

El protocolo ICMP no utiliza puertos TCP o UDP. Para bloquear ping, se deniega específicamente ICMP Echo Request, correspondiente al tipo 8.

Prueba desde Ubuntu Cliente:
ping 192.168.10.10

Resultado esperado:
100% packet loss
o:
Destination Host Unreachable

Orden de las Reglas
El orden de las reglas es fundamental. La regla de denegación ICMP debe ubicarse por encima de cualquier regla general que permita tráfico de GREEN hacia ORANGE.

Orden recomendado:
Debido a que permitirían tráfico no requerido y reducirían la efectividad de la segmentación.

Pruebas y Resultados
Las pruebas realizadas permitieron validar el comportamiento esperado de la arquitectura.

Orden	Source	Destination	Servicio	Política
1	GREEN	ORANGE	ICMP Echo Request	Deny
2	GREEN	ORANGE	HTTP TCP 80	Allow
3	GREEN	ORANGE	FTP TCP 21	Allow

Tabla 8. Orden reglas Fuente: Autoría propia

Adicionalmente, se recomienda eliminar o desactivar reglas generales como:
GREEN → ORANGE → ANY → Allow

Prueba	Comando	Resultado esperado
Conectividad LAN a firewall	ping 192.168.0.1	Responde
Conectividad DMZ a firewall	ping 192.168.10.1	Responde
HTTP LAN hacia DMZ	curl http://192.168.10.10	Permitido
FTP LAN hacia DMZ	ftp 192.168.10.10	Permitido
ICMP LAN hacia DMZ	ping 192.168.10.10	Denegado

Tabla 9. Pruebas Fuente: Autoría propia

Durante la implementación se identificaron problemas asociados a rutas duplicadas en Ubuntu Server, causadas por configuraciones DHCP residuales. El servidor DMZ tenía simultáneamente una ruta por 192.168.10.1 y otra por 192.168.0.1, lo que afectaba el retorno del tráfico HTTP. La solución consistió en dejar el servidor con IP estática en la red DMZ y con un único gateway hacia 192.168.10.1.

También se verificó que el servidor HTTP escuchaba correctamente en el puerto 80 mediante:

sudo ss -tulnp | grep ':80'
y que el cliente LAN lograba establecer conexión TCP hacia el servidor mediante:

curl -v http://192.168.10.10

3.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Con el objetivo de garantizar la protección de los servidores que conforman la intranet y la extranet institucional, se implementó una arquitectura de seguridad perimetral basada en Endian Firewall Community como firewall principal, permitiendo segmentar el tráfico mediante una zona desmilitarizada (DMZ) y controlar el acceso entre redes internas y externas.

La infraestructura fue desplegada en un entorno virtualizado mediante Oracle VM VirtualBox, utilizando una estación GNU/Linux como cliente de la red LAN y un servidor GNU/Linux ubicado en la zona DMZ. El firewall fue configurado con tres interfaces principales: GREEN para la red interna con direccionamiento 192.168.10.0/24, ORANGE para la zona DMZ con direccionamiento 192.168.20.0/24 y RED como interfaz de acceso WAN.

Posteriormente, sobre el servidor ubicado en la zona ORANGE se habilitaron los servicios Apache HTTP Server y vsftpd, destinados a validar la publicación segura de aplicaciones y recursos hacia redes externas sin comprometer la integridad de la infraestructura interna.

Para dar solución específica a la temática 4, se implementaron reglas de acceso que permitieron la comunicación entre la zona GREEN y la zona ORANGE utilizando los protocolos HTTP y FTP sobre los puertos 80 y 21 respectivamente. Estas políticas garantizaron acceso controlado desde la red interna hacia los servicios alojados en la DMZ.

Adicionalmente, se configuraron reglas NAT y Port Forwarding para permitir comunicación controlada desde la zona WAN hacia la zona DMZ, logrando la publicación segura de los servicios implementados sin exposición directa de la red LAN.

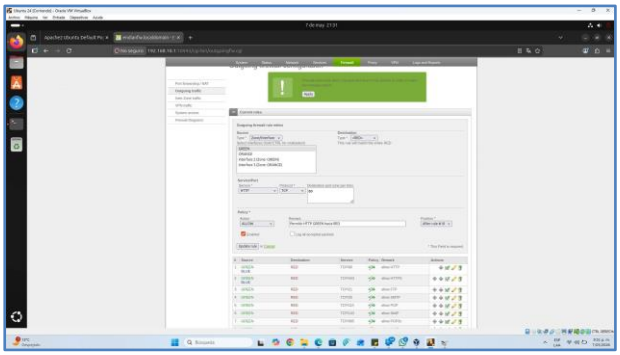

Figura 14. Endian Fuente: Autoría propia

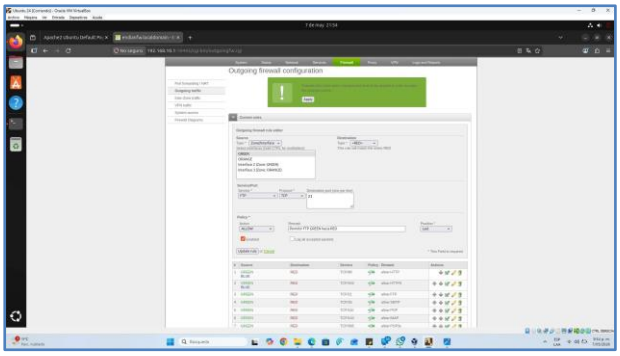

Figura 15. Endian Fuente: Autoría propia

Con las políticas aplicadas se realizaron pruebas funcionales de navegación HTTP y acceso FTP desde diferentes zonas de red, verificando la disponibilidad de los servicios y el comportamiento esperado de las reglas de seguridad configuradas.

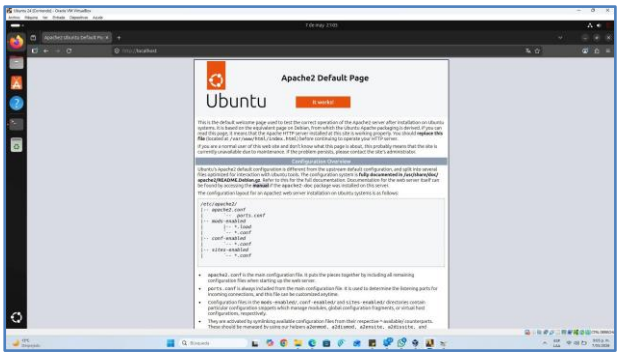

Figura 16. Navegación HTTP Fuente: Autoría propia

Desde la consola GNU/Linux también se verificó el estado operativo de los servicios mediante comandos de administración del sistema, validando el correcto funcionamiento de Apache y VSFTPD con evidencia de fecha y hora de ejecución, conforme a los requerimientos de la guía de actividades.

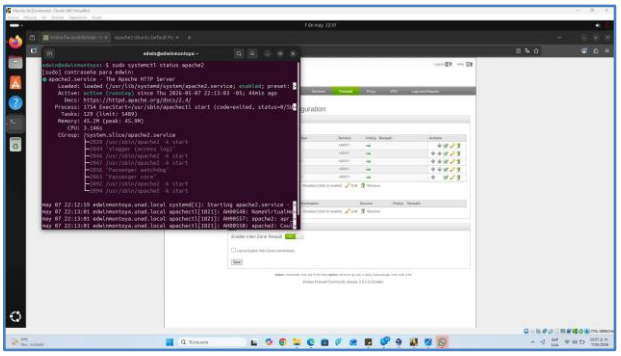

Figura 17. Servidor Apache Fuente: Autoría propia

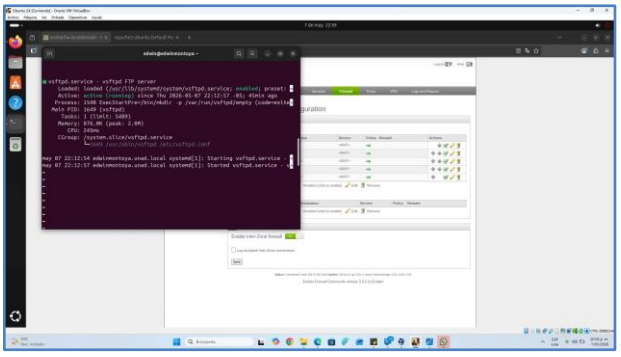

Figura 18. Servidor Apache Fuente: Autoría propia

Los resultados obtenidos permitieron comprobar que la segmentación mediante DMZ constituye un mecanismo efectivo para proteger bases de datos, aplicaciones y servicios empresariales, asegurando control granular del tráfico y reduciendo riesgos de acceso no autorizado desde redes externas.

3.5 IMPLEMENTAR UN PROXI HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICIDAD PARA LA NAVEGACIÓN EN INTERNET

Una vez finalizada la configuración inicial del firewall y establecida la segmentación de red en zonas (Verde–LAN, Roja–WAN y Naranja–DMZ), se procedió a habilitar el servicio de Proxy HTTP.

Ingreso a dashboard Endian firewall

Se accedió a la interfaz de administración del firewall.

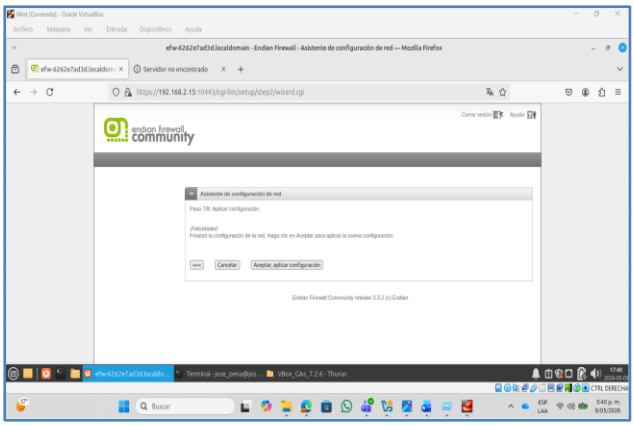

Figura 19. Ingreso dashboard de Endian firewall Fuente: Autoría propia

Habilitar proxy firewall

Se ingresó al menú Proxy → HTTP → Configuración. y se habilitó la opción Habilitar Proxy HTTP, se configuró el modo **No Transparente** para la zona VERDE, Se estableció el puerto 8080 como puerto de escucha del proxy, Se guardaron los cambios.
El modo no transparente fue seleccionado con el fin de forzar la autenticación de usuarios mediante configuración manual del proxy en el navegador

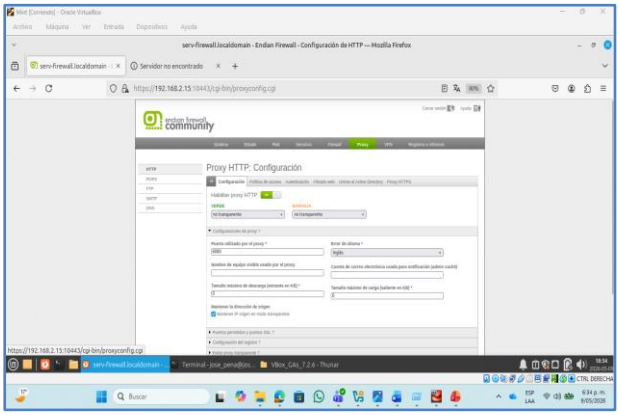

Figura 20. Configuración de proxy Fuente: Autoría propia

Configuración de autenticación
Para implementar control de acceso basado en usuario, se configuró autenticación local tipo NCSA
Se accedió a Proxy → HTTP → Autenticación. Se seleccionó el método Autenticación local (NCSA), se configuró el dominio de autenticación, se estableció el tiempo de caché TTL de autenticación en 60 minutos, se crearon usuarios mediante la opción Administrar usuarios, se creó un grupo denominado, por ejemplo, grupo_proxy, se asoció el usuario creado al grupo correspondiente

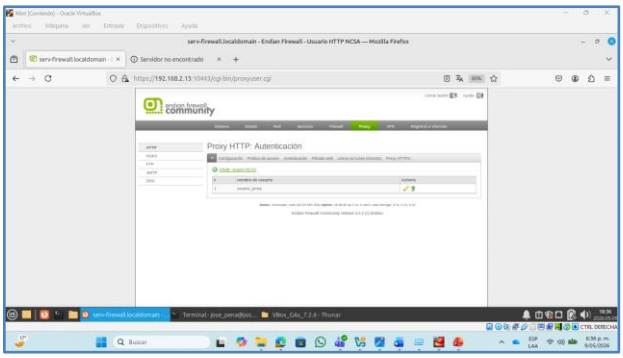

Figura 21. Configuración de autenticación Fuente: Autoría propia

Esta configuración permite aplicar políticas diferenciadas basadas en pertenencia a grupos.

Creación del perfil de filtrado Web (lista negra)

Se implementó un perfil de filtrado web para bloquear dominios específicos

Se accedió a Proxy → HTTP → Filtrado Web.
Se seleccionó la opción Añadir nuevo perfil, se creó un perfil denominado, por ejemplo, perfil bloqueo, se configuró una lista negra (Blacklist) incluyendo los siguientes dominios:

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

Se guardó el perfil de filtrado

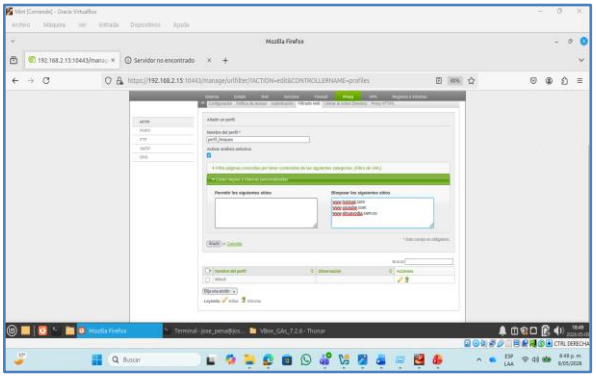

Figura 22. Configuración de perfil filtrado web Fuente: Autoría propia

Creación de política de acceso

Posteriormente, se configuró la política que vincula autenticación y perfil de filtrado.
Se accedió a Proxy → HTTP → Política de Acceso, se definió el tipo de origen como CUALQUIERA (Zona Verde) se estableció el destino como CUALQUIERA, en la sección Autenticación, se seleccionó En base a grupo se agregó el grupo previamente creado (grupo_proxy) como grupo permitido. Se configuró la política de acceso como Permitir acceso, se vinculó el perfil de filtrado creado en el punto anterior se habilitó la

política y se ubicó en la primera posición para garantizar prioridad. se guardó la configuración.

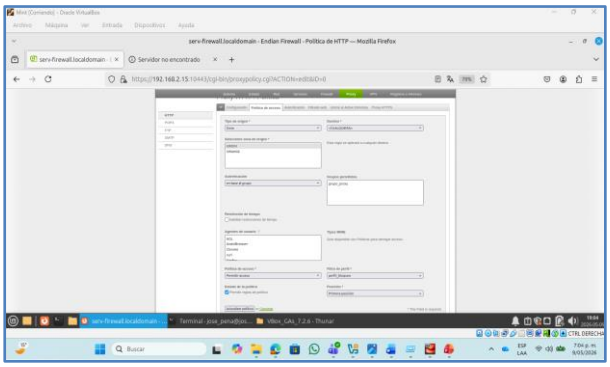

Figura 23. Configuración de Política de acceso Fuente: Autoría propia

Configuración del navegador cliente

En un equipo de la Zona Verde (LAN):
Se accedió a la configuración de red del navegador web. Se configuró el proxy manual indicando:

- Dirección IP del firewall (Zona Verde 192.168.2.15).
- Puerto 8080.

Se guardaron los cambios.

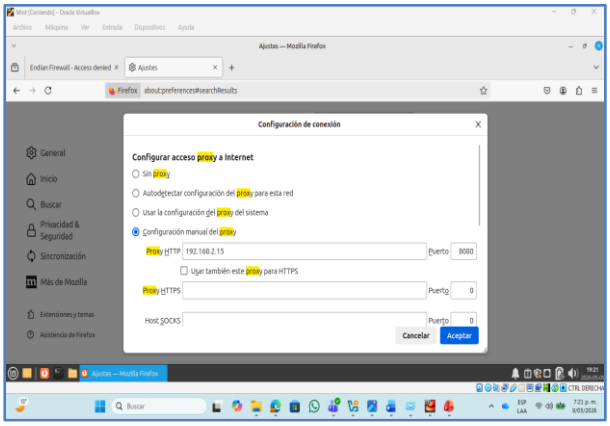

Figura 24. Configuración de navegador web al ser tipo no transparente Fuente: Autoría propia

Pruebas de funcionamiento

Finalmente, se realizaron pruebas de validación:

Se intentó acceder a los dominios configurados en la lista negra, el sistema solicita autenticación de usuario. Una vez autenticado, el acceso a los sitios bloqueados fue denegado, se verificó el registro de eventos en los logs del firewall.

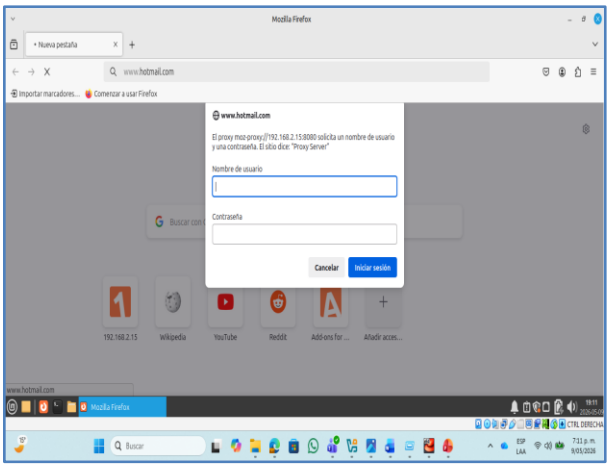

Figura 25. Prueba de autenticación Fuente: Autoría propia

Los resultados confirmaron el correcto funcionamiento del proxy HTTP con autenticación y filtrado web basado en políticas.

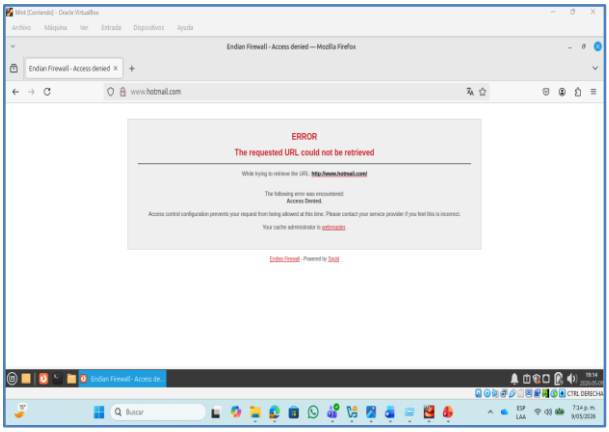

Figura 26. Validación de mensaje de error al tratar de ingresar a sitio bloqueado Fuente: Autoría propia

CONCLUSIONES

El desarrollo integral de las cinco temáticas permitió consolidar un entorno funcional de seguridad perimetral sobre plataformas GNU/Linux, evidenciando que la implementación de arquitecturas segmentadas mediante Endian Firewall Community constituye una solución robusta para el control, monitoreo y protección del tráfico entre redes internas, externas y zonas desmilitarizadas.

La instalación y configuración inicial del firewall, junto con la correcta asignación de interfaces para las zonas LAN, WAN y DMZ, demostró la importancia de una adecuada planificación del direccionamiento IP y de la segmentación lógica como base para garantizar comunicaciones seguras y administrables dentro de una infraestructura empresarial.

La configuración de políticas NAT y Port Forwarding permitió establecer comunicación controlada entre redes privadas y externas, validando mecanismos fundamentales de traducción

de direcciones que posibilitan tanto el acceso seguro a Internet desde segmentos internos como la publicación controlada de servicios alojados en la DMZ sin exponer directamente la red corporativa.

La habilitación y validación de servicios HTTP y FTP sobre servidores GNU/Linux ubicados en la zona desmilitarizada confirmó la eficacia del modelo de aislamiento perimetral, permitiendo exponer servicios específicos mientras se restringen accesos innecesarios mediante reglas precisas de filtrado y control de protocolos.

La implementación de reglas Inter-Zone permitió comprobar que el firewall puede aplicar políticas granulares para permitir o denegar tráfico según origen, destino, protocolo y puerto, garantizando que únicamente los servicios autorizados puedan establecer comunicación entre segmentos, fortaleciendo así la integridad y disponibilidad de los recursos protegidos.

La configuración de un proxy HTTP no transparente con autenticación basada en usuarios y grupos, complementado con listas negras y políticas de filtrado web, evidenció la capacidad de Endian para aplicar controles avanzados de navegación, autenticación y restricción de contenido, fortaleciendo la administración centralizada del acceso a Internet en entornos organizacionales.

Finalmente, el desarrollo práctico de estas actividades permitió fortalecer competencias esenciales en virtualización, administración de sistemas GNU/Linux, seguridad perimetral, gestión de servicios de red y aplicación de políticas de ciberseguridad, demostrando que la integración de herramientas de código abierto representa una alternativa técnica viable, escalable y altamente efectiva para la protección de infraestructuras tecnológicas modernas.

REFERENCIAS

LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware.
https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu.
https://help.ubuntu.com/

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

Oracle (2020), Manual de usuario VirtualBox. VirtualBox.
https://www.virtualbox.org/manual/

Endian (2016), Endian UTM 3.2 Manual referencia. Endian.
http://docs.endian.com/3.2/utm/index.html