IMPLEMENTACIÓN DE SEGURIDAD EN ENTORNOS GNU/LINUX

Erika Daniela Moreno Riveros
e-mail: edmorenori@unadvirtual.edu.co
Rosember Erminson Huertas Buitrago
e-mail: rehuertasb@unadvirtual.edu.co
Juan Sebastián Bocachica Pinzon
e-mail: jsbocachicap@unadvirtual.edu.co
Sara Daniela Rincon Medina
e-mail: sdrinconme@ unadvirtual.edu.co
Jessica Liliana Torres Salcedo
e-mail: jltorressa@unadvirtual.edu.co

RESUMEN

La protección de servidores en redes internas (LAN) y externas (WAN) requiere soluciones de seguridad perimetral que aseguren la integridad de aplicaciones y bases de datos. Este trabajo presenta la implementación de una zona desmilitarizada (DMZ) mediante la distribución GNU/Linux Endian Firewall (EFW), configurada en entornos virtualizados para delimitar y controlar el tráfico entre las distintas zonas de la infraestructura. De manera colaborativa, se desarrollaron temáticas específicas: configuración de instancias y tarjetas de red, reglas de NAT, habilitación de servicios en la DMZ, control de acceso interzonas y establecimiento de un proxy HTTP con autenticación. Las pruebas incluyeron la verificación de servicios web y FTP, la restricción de protocolos como ICMP y la validación de reglas de seguridad en consola. Los resultados evidencian que la planificación conjunta y el uso de EFW fortalecen la seguridad perimetral y garantizan la disponibilidad de servicios en entornos LAN, WAN y DMZ.

ABSTRACT

The protection of servers in internal (LAN) and external (WAN) networks requires perimeter security solutions to ensure the integrity of applications and databases. This paper presents the implementation of a demilitarized zone (DMZ) using the GNU/Linux Endian Firewall (EFW) distribution, configured in virtualized environments to delimit and control traffic between different network zones. Collaborative work was carried out through specific topics: instance and network card configuration, NAT rules, DMZ service enablement, inter-zone access control, and the establishment of an HTTP proxy with authentication. Tests included verification of web and FTP services, restriction of ICMP protocols, and validation of security rules through console evidence. The results show that coordinated planning and the use of EFW strengthen perimeter security and ensure service availability in LAN, WAN, and DMZ environments.

PALABRAS CLAVE: GNU/Linux, Endian Firewall, DMZ, NAT, HTTP Proxy.

1. INTRODUCCIÓN

La creciente interconexión de sistemas informáticos y el uso intensivo de aplicaciones web han incrementado la necesidad de implementar mecanismos de seguridad que garanticen la protección de servidores y bases de datos en entornos corporativos y educativos. En este contexto, resulta fundamental delimitar las redes internas (LAN) y externas (WAN) mediante la creación de una zona (DMZ), que actúe como capa intermedia de defensa frente a posibles amenazas.

El presente trabajo aborda la configuración de un entorno seguro bajo plataformas GNU/Linux, utilizando la distribución Endian Firewall como herramienta principal para la gestión del tráfico y la implementación de políticas de acceso. La metodología se desarrolla en un entorno virtualizado, donde se definen las zonas verdes (LAN), roja (WAN) y naranja (DMZ), permitiendo la segmentación y control de servicios críticos como HTTP y FTP, así como la restricción de protocolos susceptibles de explotación, como ICMP.

De manera colaborativa, los integrantes del grupo ejecutan actividades específicas que incluyen la configuración de reglas de NAT, la habilitación de servicios en la DMZ, la definición de políticas de acceso interzonas y la implementación de un proxy HTTP con autenticación. Este enfoque permite validar la efectividad de las medidas de seguridad aplicadas y analizar las ventajas, limitaciones e inconsistencias encontradas durante el proceso.

2. METODOLOGIA

2.1 Temática 1: Configuración de la Instancia para GNU/Linux Endian en VirtualBox (Tarjetas de Red) e Instalación

Para el desarrollo de esta actividad se configuró un entorno virtualizado en VirtualBox utilizando Endian Firewall 3.3 como sistema principal de seguridad y administración de red. Además, se implementaron dos máquinas virtuales adicionales: Ubuntu Desktop, utilizado como equipo cliente dentro de la red local, y Ubuntu Server, ubicado en la zona DMZ para simular un servidor dentro de la infraestructura.

El escenario de red se organizó en tres segmentos principales, cada uno con una función específica dentro de la arquitectura implementada:

Figura 1. Configuración de zonas de red y direccionamiento IP en Endian Firewall.

Zona	Propósito	Interfaz (Endian)	IP del Endian	Máscara	Rango de Hosts / DHCP	Tipo de dispositivos
ROJA (WAN)	Conexión a Internet	eth2	DHCP (asignada por red externa)	—	—	Router, ISP, enlace WAN
NARANJA (DMZ)	Servidores públicos (aislados)	eth1	172.20.30.1	255.255.255.0	172.20.30.10 – 172.20.30.99 (IP fija)	Servidores web, FTP, BD, correo
VERDE (LAN)	Red interna de usuarios	eth0	192.168.90.1	255.255.255.0	DHCP: 192.168.90.50 – 192.168.90.200	PCs, laptops, impresora

Fuente: Autoría Propia

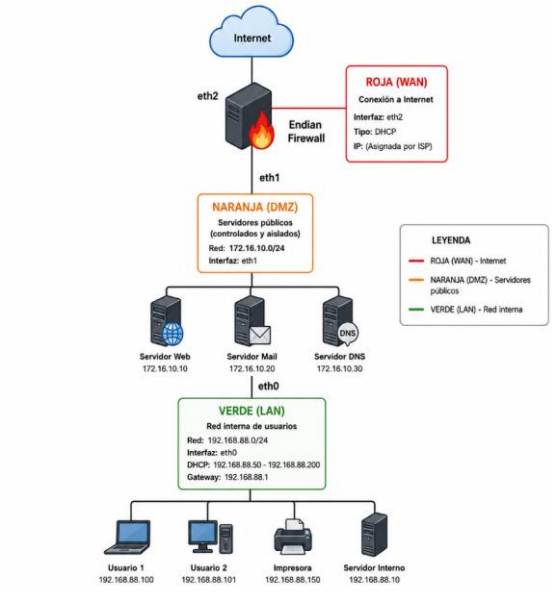
• **Red Verde (LAN):** configurada con el segmento 192.168.90.0/24, utilizada para la red interna de usuarios. En esta zona se encuentra el equipo cliente Ubuntu Desktop, el cual obtiene conectividad a través del firewall.

• **Red Naranja (DMZ):** destinada a los servicios y equipos que requieren estar más expuestos dentro de la infraestructura. En esta zona se configuró Ubuntu Server con direccionamiento estático para simular un servidor dentro de la DMZ.

• **Red Roja (WAN):** utilizada como interfaz de salida hacia Internet, conectada mediante NAT al equipo host donde se ejecutan las máquinas virtuales en VirtualBox.

Este escenario permitió recrear una arquitectura básica de seguridad perimetral, separando las diferentes zonas de red mediante Endian Firewall y facilitando la administración y el control del tráfico entre ellas.

Figura 2. Topología de red implementada con Endian Firewall y segmentación de zonas WAN, DMZ y LAN.



Fuente: Autoría Propia

2.1.1 Preparación del Entorno e Instalación de Sistemas Operativos

El desarrollo de la práctica inició con la descarga de Endian Firewall 3.3 desde su repositorio oficial en SourceForge. Posteriormente, se realizó la creación y configuración de las máquinas virtuales necesarias para el laboratorio en VirtualBox: Ubuntu Desktop como equipo cliente, Ubuntu Server como servidor en la DMZ y Endian como firewall encargado de la administración y segmentación de la red.

Con el fin de separar correctamente cada zona de la infraestructura, se configuraron las interfaces de red de Endian de la siguiente manera:

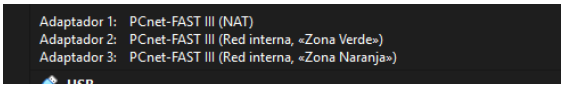
• **Adaptador 1:** configurado en modo red interna para la **Red Verde (LAN)**, permitiendo la comunicación con el equipo cliente Ubuntu Desktop.

• **Adaptador 2:** configurado en modo red interna para la **Red Naranja (DMZ)**, donde se encuentra Ubuntu Server.

• **Adaptador 3:** configurado en modo NAT para la **Red Roja (WAN)**, proporcionando acceso a Internet desde el firewall hacia el exterior.

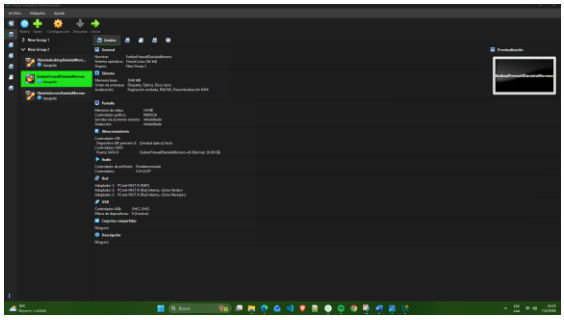
Esta configuración permitió simular un entorno de red segmentado, donde cada zona cumple una función específica y se encuentra controlada mediante el firewall Endian.

Figura 3. Configuración de adaptadores de red en VirtualBox para Endian Firewall.



Fuente: Autoría Propia

Figura 4. Creación y configuración de la máquina virtual Endian Firewall en VirtualBox.



Fuente: Autoría Propia

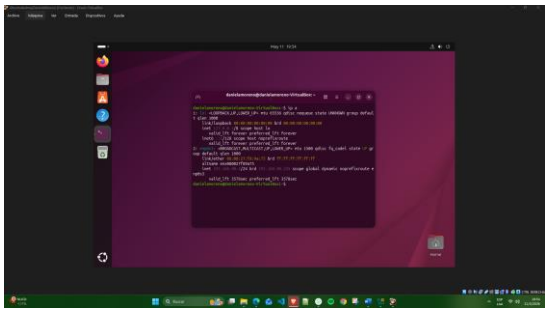
2.1.2 Configuración de Tarjetas de Red en los Sistemas Operativos Cliente y Servidor

Una vez configurada la estructura principal del firewall, se realizaron las asignaciones de red correspondientes a las máquinas virtuales que interactúan dentro de la arquitectura implementada:

2.1.3 Ubuntu Desktop (Cliente Red Verde)

El equipo Ubuntu Desktop fue configurado con un adaptador de red en modo red interna, asociado al segmento correspondiente a la Red Verde (LAN).

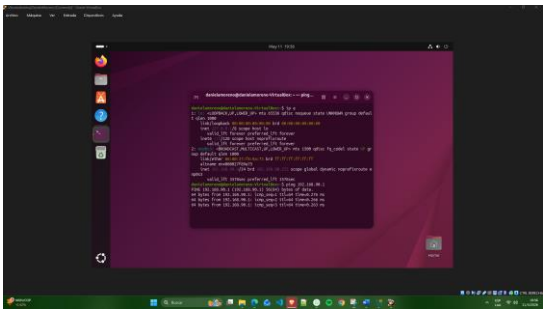
Figura 5. Verificación de configuración de red en Ubuntu Desktop mediante el comando ip.



Fuente: Autoría Propia

Gracias a esta configuración, la máquina cliente puede comunicarse directamente con Endian Firewall y operar como estación de trabajo dentro de la red local, obteniendo conectividad mediante el servicio DHCP configurado en el firewall.

Figura 6. Prueba de conectividad desde Ubuntu Desktop hacia la puerta de enlace 192.168.90.1.

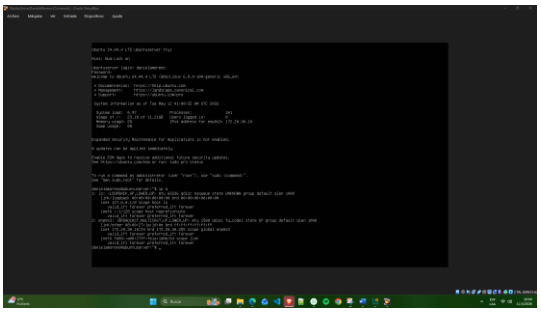


Fuente: Autoría Propia

2.1.4 Ubuntu Server (Servidor – Red Naranja)

Para Ubuntu Server se configuró un adaptador de red en modo red interna vinculado a la Red Naranja (DMZ).

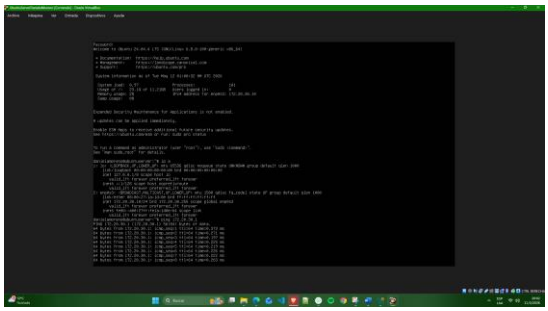
Figura 7. Verificación de configuración IP en Ubuntu Server mediante consola de comandos.



Fuente: Autoría Propia

De esta manera, el servidor permanece aislado de la red local y todo el tráfico hacia otras zonas debe pasar obligatoriamente por el firewall, permitiendo un mayor control y seguridad sobre los servicios alojados en esta área, se puede comprobar conectividad con ping a la dmz.

Figura 8. Configuración IP de Ubuntu Server en la zona DMZ.



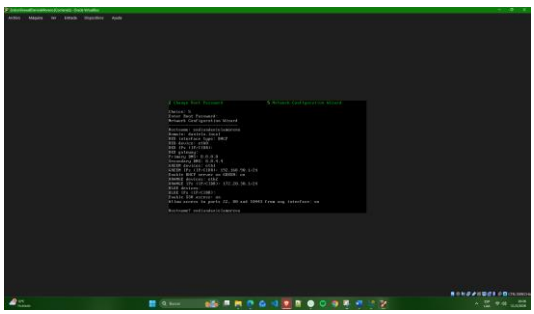
Fuente: Autoría Propia

2.1.5 Instalación de los Sistemas Operativos

Con las interfaces de red previamente definidas, se procedió a la instalación de los sistemas operativos utilizados en la práctica. Tanto Ubuntu Desktop como Ubuntu Server fueron instalados siguiendo el procedimiento estándar de instalación proporcionado por Ubuntu.

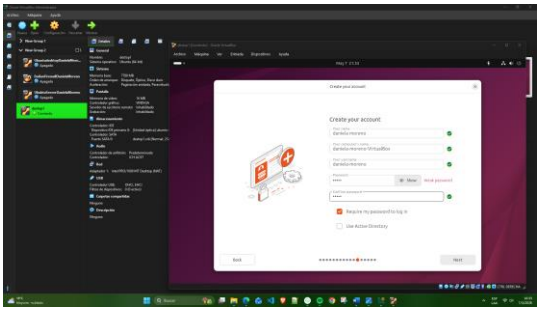
En el caso de Endian Firewall 3.3, el proceso de instalación permitió realizar la configuración inicial de las zonas de red, la asignación de interfaces y la activación de los servicios básicos necesarios para el funcionamiento del firewall y la segmentación de la infraestructura virtualizada.

Figura 8. Configuración de segmentos de red en Endian Firewall



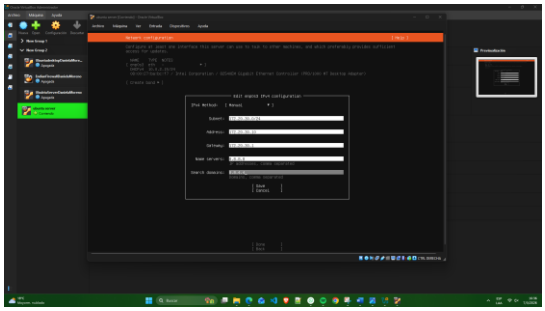
Fuente: Autoría Propia

Figura 9. Instalación de Ubuntu Desktop (Cliente)



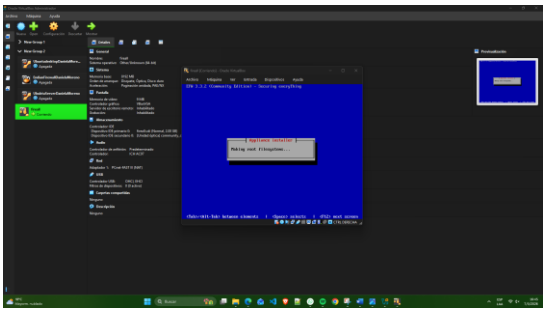
Fuente: Autoría Propia

Figura 10. Instalación de Ubuntu Server (Servidor)



Fuente: Autoría Propia

Figura 11. Proceso de instalación de Endian Firewall 3.3

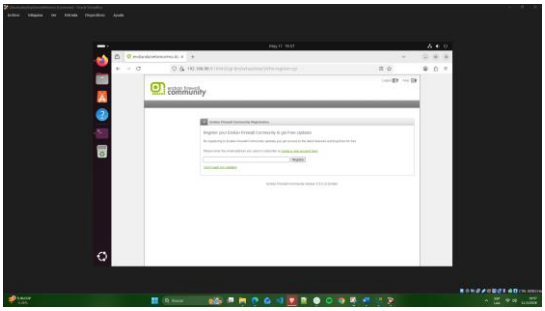


Fuente: Autoría Propia

2.1.6 Verificación de la Instalación de Endian

Una vez finalizada la instalación y configuración inicial de Endian Firewall, el sistema mostró su interfaz principal de administración.

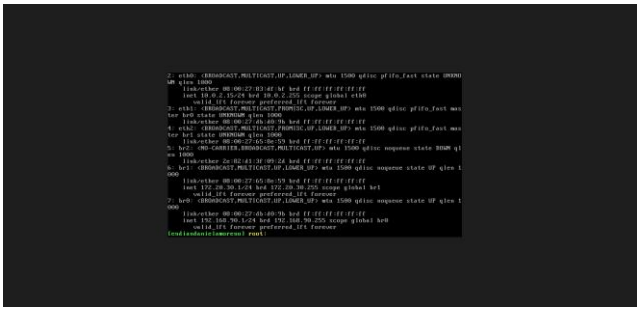
Figura 12. Acceso a la interfaz web de administración de Endian Firewall.



Fuente: Autoría Propia

Esta validación permitió comprobar que las interfaces de red fueron asignadas adecuadamente y que la segmentación de la infraestructura quedó operativa, dejando preparado el entorno para realizar pruebas de conectividad, administración del tráfico y aplicación de políticas de seguridad dentro del laboratorio virtualizado.

Figura 13. Vista general zonas de firewall

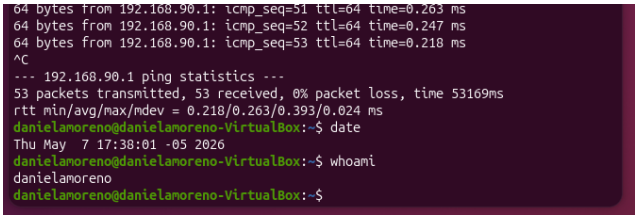


Fuente: Autoría Propia

2.1.7 Conectividad

Realizamos las pruebas finales de conectividad, ping a 192.168.90.1

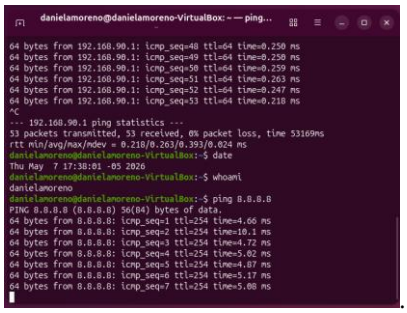
Figura 14. Prueba de conectividad.



Fuente: Autoría Propia

Se realiza la ejecución de comandos date, whoami y ping a 8.8.8.8.

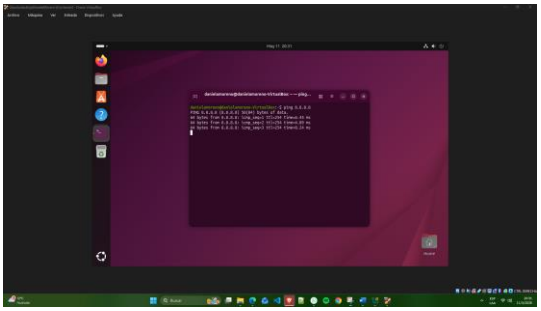
Figura 15. Ejecución de comandos.



Fuente: Autoría Propia

ping a 8.8.8.8. desde Ubuntu desktop (cliente)

Figura 16. Prueba de conectividad.



Fuente: Autoría Propia

2.1.8 Análisis

La implementación de Endian Firewall permitió evidenciar la importancia de la segmentación de redes dentro de una infraestructura informática. La separación entre las zonas VERDE, NARANJA y ROJA facilitó el control del tráfico y mejoró la seguridad entre los diferentes dispositivos conectados al entorno virtual.

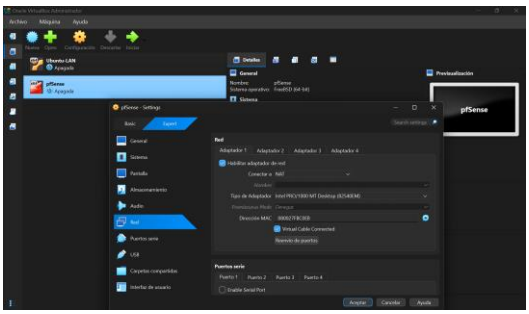
Las pruebas de conectividad demostraron que la configuración de las interfaces de red fue realizada correctamente, permitiendo la comunicación controlada entre los equipos y el acceso a servicios externos. Asimismo, el uso de VirtualBox facilitó la simulación de un escenario real de administración de redes sin necesidad de hardware físico adicional.

2.2 Temática 2: Configuración NAT.

Para el desarrollo de la práctica se utilizó Oracle VirtualBox para crear un entorno virtualizado compuesto por dos máquinas virtuales: pfSense como firewall/router y Ubuntu como cliente de la red LAN.

Se configuró una interfaz WAN conectada a NAT de VirtualBox para simular el acceso a Internet y una interfaz LAN mediante red interna para permitir la comunicación entre pfSense y Ubuntu.

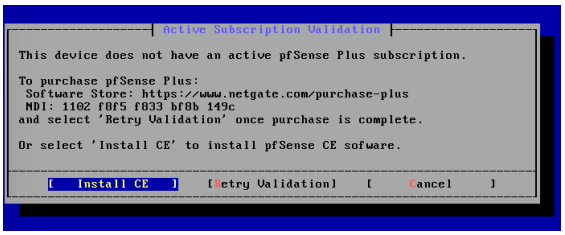
Figura 17. Interfaz VirtualBox



Fuente: Autoría Propia

Configuración de red de la máquina virtual pfSense en Oracle VirtualBox. Se observa el adaptador 1 configurado en modo NAT para simular la conexión WAN hacia Internet, permitiendo posteriormente la implementación de reglas NAT y comunicación entre la red LAN y la WAN.

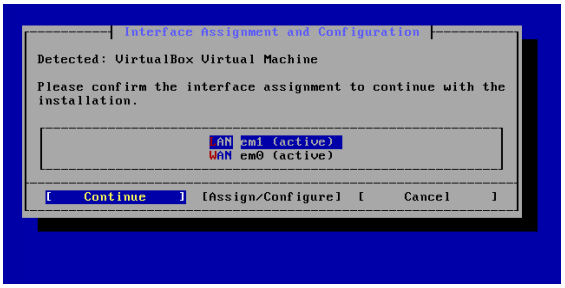
Figura 18. Configuración LAN - WAN



Fuente: Autoría Propia

Selección de instalación de pfSense Community Edition durante el proceso inicial de configuración. En esta etapa se eligió la versión gratuita CE para implementar el firewall y las funcionalidades NAT requeridas en la práctica.

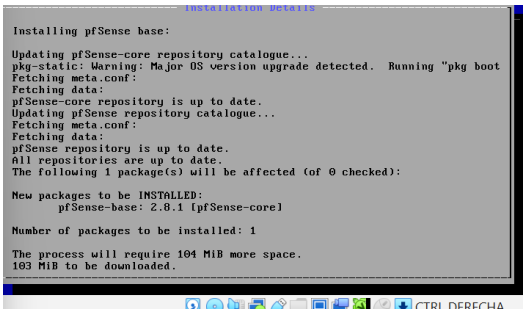
Figura 19. Funcionalidades de NAT



Fuente: Autoría Propia

Asignación y verificación de interfaces de red en pfSense. Se configuró la interfaz WAN asociada a la salida hacia Internet y la interfaz LAN destinada a la red interna utilizada por el cliente Ubuntu.

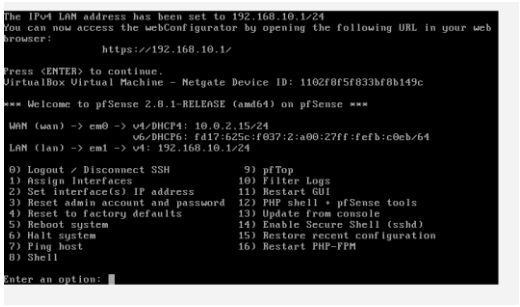
Figura 20. Verificación interfaz de red



Fuente: Autoría Propia

Proceso de instalación y descarga de paquetes base de pfSense Community Edition. El sistema realiza la instalación automática de componentes necesarios para el funcionamiento del firewall, NAT y servicios de red.

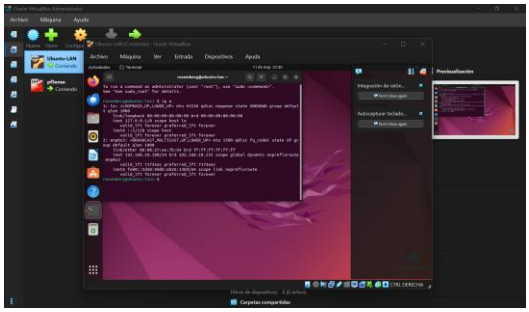
Figura 21. Funcionamiento del Firewall



Fuente: Autoría Propia

Consola principal de pfSense una vez finalizada la instalación y configuración inicial. Se evidencia la asignación de las interfaces WAN y LAN, así como la dirección IP 192.168.10.1/24 configurada para la red interna, permitiendo posteriormente la implementación y validación de NAT.

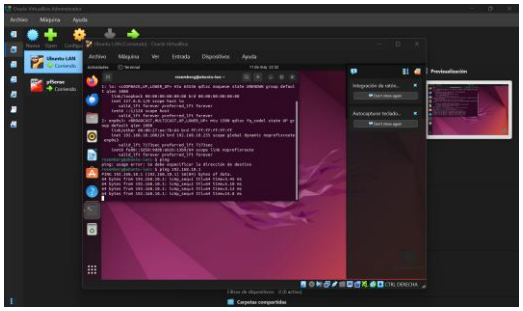
Figura 22. Implementación de variación NAT



Fuente: Autoría Propia

Verificación de la configuración de red del cliente Ubuntu mediante el comando ip a. Se evidencia que el equipo obtuvo la dirección IP 192.168.10.10/24 dentro de la red LAN administrada por pfSense.

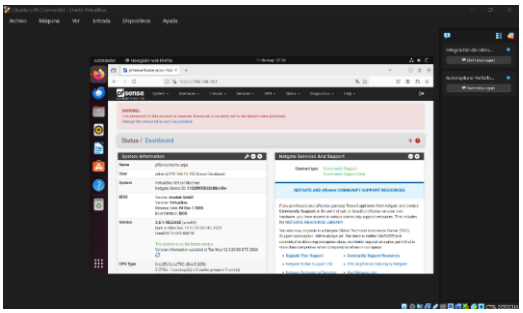
Figura 23. Red LAN administrada por pfSense



Fuente: Autoría Propia

Prueba de conectividad entre el cliente Ubuntu y el firewall pfSense mediante el comando ping 192.168.10.1. La respuesta satisfactoria confirma la correcta comunicación entre la LAN y la puerta de enlace configurada en pfSense.

Figura 24. Configuración en pfSense



Fuente: Autoría Propia

Acceso exitoso al panel de administración web de pfSense desde el navegador Firefox en Ubuntu. Esta conexión confirma el correcto funcionamiento de la red LAN y la administración centralizada del firewall mediante interfaz gráfica web.

2.2.1 Análisis

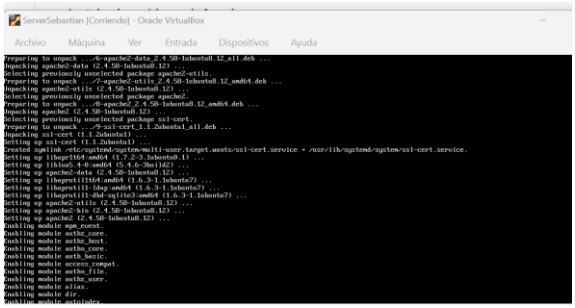
Mediante el desarrollo de esta práctica se logró implementar correctamente un esquema NAT utilizando pfSense en un entorno GNU/Linux virtualizado. La configuración permitió la comunicación entre la red LAN y la WAN, validando el acceso a Internet desde el cliente Ubuntu mediante reglas NAT automáticas.

Asimismo, se verificó el funcionamiento del servicio DHCP, la asignación de direcciones IP y el acceso al panel administrativo del firewall. Estas configuraciones permiten comprender la importancia de NAT en la administración y seguridad de redes empresariales y académicas.

2.3 Temática 3: Permitir servicios de la Zona DMZ para la red.

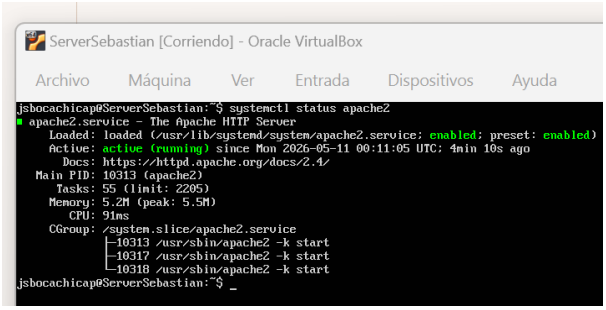
Para garantizar la correcta ejecución de los servicios, en el servidor se procede con la instalación de Apache, el cual provee el servicio web a través del puerto 80 (HTTP).

Figura 25. Instalación Apache



Fuente: Autoría Propia

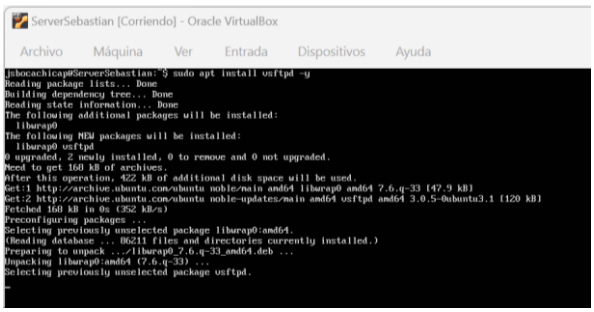
Figura 26. Verificación estado apache



Fuente: Autoría Propia

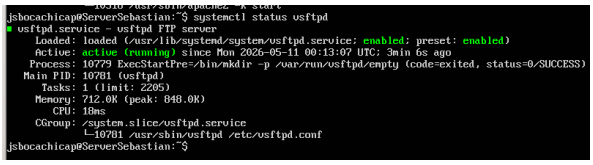
De igual manera, se procede con la instalación de vsftpd, dado que este servicio habilita el protocolo FTP en el puerto 21, permitiendo realizar pruebas de conectividad y transferencia de archivos en el entorno configurado.

Figura 27. Instalación FTP



Fuente: Autoría Propia

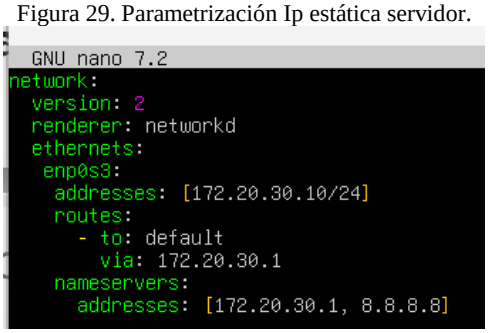
Figura 28. Verificación estado FTP



Fuente: Autoría Propia

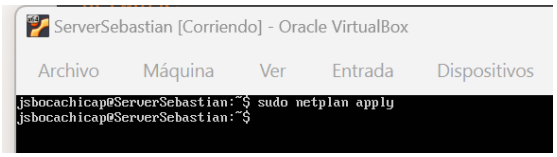
En el seguimiento de la práctica se debe garantizar que la dirección IP del servidor cumpla con los criterios definidos inicialmente, asegurando la correcta pertenencia al rango establecido para la zona correspondiente y la coherencia con la planificación de la infraestructura de red.

Figura 29. Parametrización Ip estática servidor.



Fuente: Autoría Propia

Figura 30. Aplicación de cambios.



Fuente: Autoría Propia

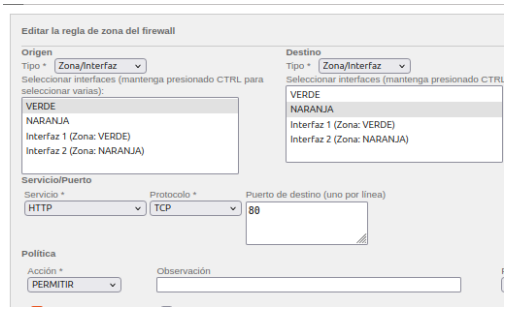
Posteriormente vamos a configurar las reglas en Endian Firewall para que el cliente LAN pueda acceder al servidor DMZ por HTTP y FTP, y al mismo tiempo bloquear ICMP (ping).

Vamos al panel web del cliente en el menú firewall, apartado reglas y establecemos las siguientes condiciones:

- Crear regla para HTTP

Zona origen: Green (LAN).
Zona destino: Orange (DMZ).
Servicio: HTTP (TCP/80).

Figura 31. Creación regla HTTP

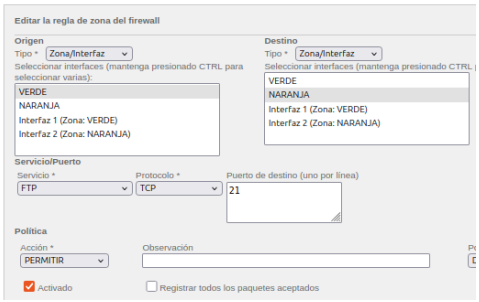


Fuente: Autoría Propia

- Crear regla para FTP

Zona origen: Green (LAN).
Zona destino: Orange (DMZ).
Servicio: FTP (TCP/21).

Figura 32. Creación regla FTP

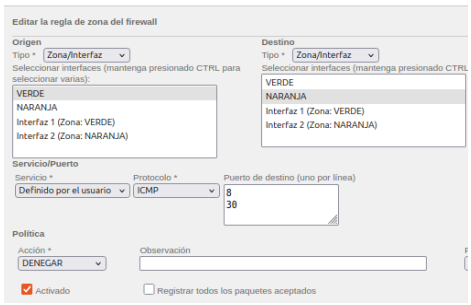


Fuente: Autoría Propia

- Bloquear ICMP

Zona origen: Green (LAN).
Zona destino: Orange (DMZ).
Servicio: ICMP (ping).

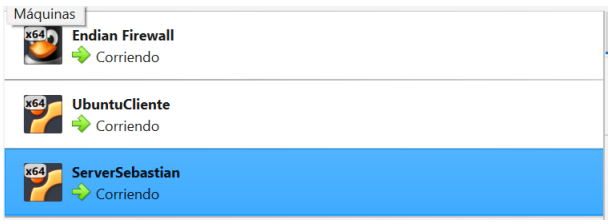
Figura 33. Creación regla de bloqueo ICMP



Fuente: Autoría Propia

Posterior a la configuración y creación de las reglas requeridas para la actividad, se procede a validar que los servicios estén activos y accesibles desde el cliente en la red LAN. Para garantizar la correcta comunicación, es indispensable que las tres máquinas virtuales (Endian Firewall, servidor Ubuntu en la DMZ y cliente Ubuntu en la LAN) se encuentren en ejecución simultánea. Bajo estas condiciones se verifican los tres casos definidos: acceso al servicio HTTP, acceso al servicio FTP y la restricción del protocolo ICMP.

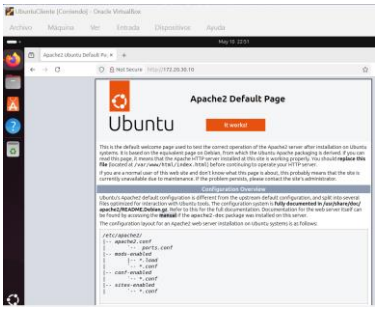
Figura 34. Ejecución máquinas virtuales



Fuente: Autoría Propia

- Probar HTTP: Desde cliente LAN abre http://172.20.30.10, debe cargar la página por defecto de Apache.

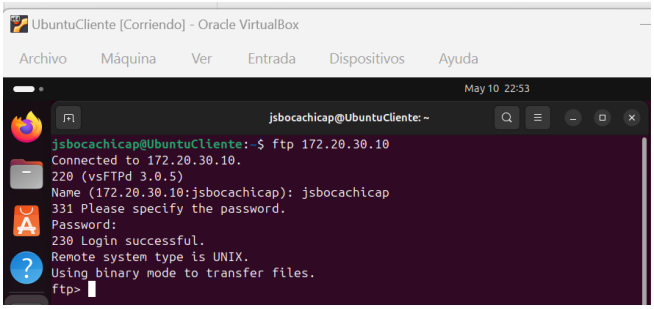
Figura 35. Prueba HTTP



Fuente: Autoría Propia

- Probar FTP: En el cliente desde la terminal ejecutamos ftp 172.20.30.10 debe responder el banner de vsftpd y pedir usuario/contraseña.

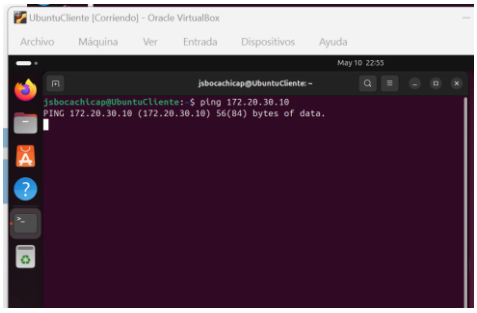
Figura 36. Prueba FTP



Fuente: Autoría Propia

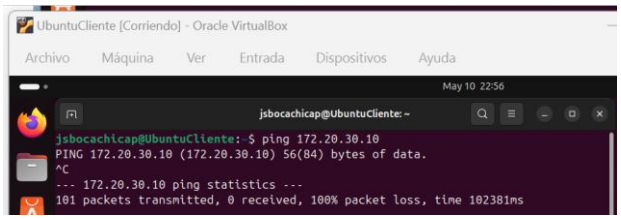
- Probar ICMP: Ejecutamos desde la terminal cliente ping 172.20.30.10 debe fallar, demostrando que la regla de bloqueo ICMP funciona.

Figura 37. Prueba Bloqueo Ping



Fuente: Autoría Propia

Figura 38. Prueba cierre de prueba ping



Fuente: Autoría Propia

2.3.1 Análisis

La implementación de reglas de firewall en la zona DMZ permitió habilitar servicios esenciales como HTTP y FTP, garantizando la disponibilidad de aplicaciones web y transferencia de archivos desde el servidor Ubuntu. Este resultado confirma la correcta comunicación entre la red interna y el servidor perimetral, cumpliendo con los objetivos de accesibilidad.

Por otro lado, la restricción del protocolo ICMP evidenció un control efectivo sobre intentos de diagnóstico y reconocimiento de red, reduciendo la exposición a ataques de tipo ping. La denegación de ICMP, verificada mediante pruebas en consola, refuerza la seguridad al limitar la visibilidad de la infraestructura hacia actores externos.

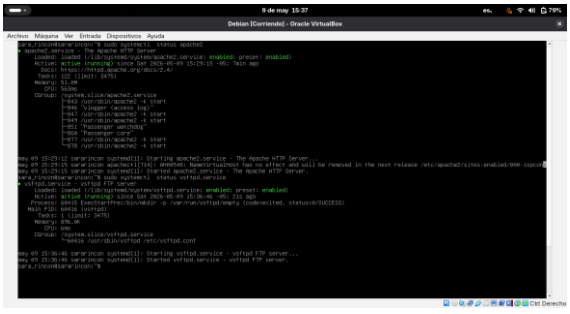
Sin embargo, se identificaron ventajas y limitaciones:

- Ventajas: mayor control del tráfico, segmentación clara entre LAN, WAN y DMZ, y cumplimiento de políticas de seguridad perimetral.
- Limitaciones: la restricción de ICMP puede dificultar tareas de administración y monitoreo legítimo, lo que obliga a definir excepciones controladas para administradores.
- Inconsistencias: la configuración inicial requirió ajustes en la definición de servicios personalizados (como ICMP) dentro de Endian Firewall, lo que generó complejidad adicional en la gestión.

2.4 Temática 4: Reglas De Acceso Para Permitir O Denegar El Tráfico

Primero verificamos que los servicios tanto como HTTP y FTP, estén instalado en nuestro servidor.

Figura 39. Servicios HTTP y FTP corriendo en el servidor.

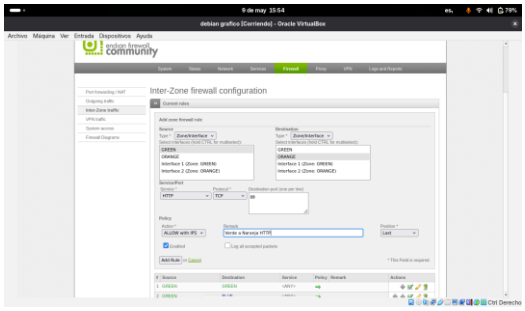


Fuente: Autoría Propia

2.4.1 Comunicar La Zona Verde Con La Zona Naranja Con El Protocolo HTTP Y FTP Con Sus Respectivos Puertos

Esta regla se creó en la sección Inter-Zone traffic del Endian para permitir la comunicación entre la zona VERDE (LAN) y la zona NARANJA (DMZ). Se configuró el servicio HTTP sobre el puerto 80 con protocolo TCP, lo cual permite que los usuarios de la red interna accedan al servidor web alojado en la DMZ desde sus navegadores.

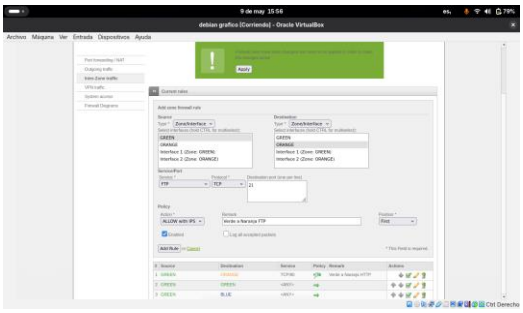
Figura 40. Creación de la regla de Inter zonas para HTTP.



Fuente: Autoría Propia

Esta regla se creó también en la sección Inter-Zone traffic para permitir la comunicación FTP entre la zona VERDE y la zona NARANJA. Se configuró sobre el puerto 21 con protocolo TCP, permitiendo la transferencia de archivos desde la LAN hacia el servidor FTP ubicado en la DMZ.

Figura 41. Creación de la regla de inter zonas FTP.

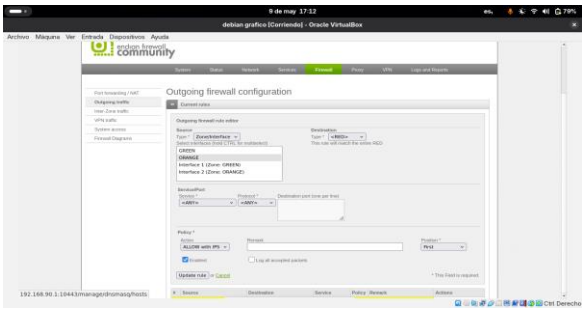


Fuente: Autoría Propia

2.4.2 Comunicar la zona Internet con la zona DMZ

Esta regla permite que todo el tráfico originado en la zona NARANJA (DMZ) tenga salida hacia Internet a través de la interfaz RED del Endian. Se configuró con servicio y protocolo ANY para no restringir ningún tipo de comunicación, garantizando que los servidores de la DMZ puedan acceder a recursos externos como actualizaciones o consultas a Internet.

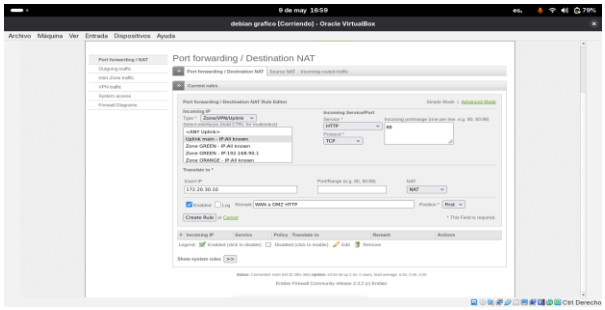
Figura 42. Creación de la regla que permite la comunicación de la DMZ con la red.



Fuente: Autoría Propia

Esta regla permite que las peticiones HTTP que llegan desde Internet a la interfaz RED del Endian sean redirigidas al servidor Debian ubicado en la DMZ (172.20.30.10). Se configuró sobre el puerto 80 con protocolo TCP, utilizando NAT de destino para evitar exponer directamente el servidor.

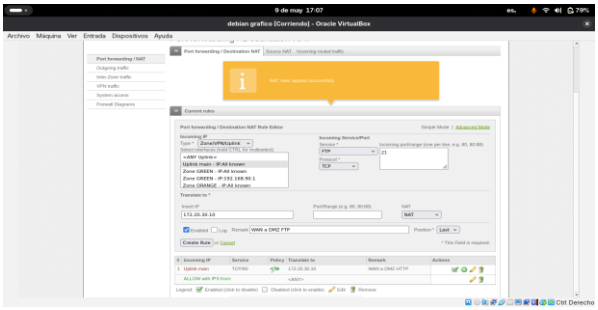
Figura 42. Creación de la regla que permite la comunicación del servicio HTTP.



Fuente: Autoría Propia

Esta regla permite que las peticiones FTP que llegan desde Internet a la interfaz RED del Endian sean redirigidas al servidor Debian ubicado en la DMZ (172.20.30.10). Se configuró sobre el puerto 21 con protocolo TCP, utilizando NAT de destino para evitar exponer directamente el servidor.

Figura 43. Creación de la regla que permite la comunicación del servicio FTP.

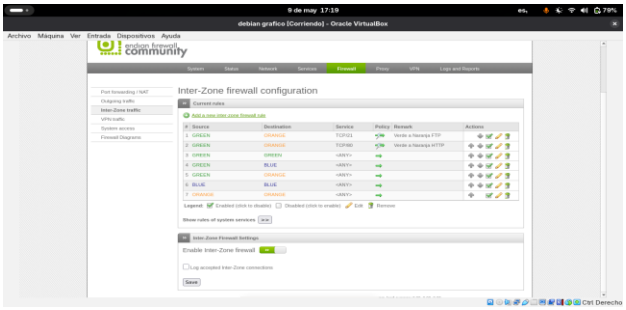


Fuente: Autoría Propia

2.4.3 Verificar En El Tráfico Inter - Zona, La Creación De Las Reglas

En la sección Inter-Zone traffic se verificaron las reglas creadas para la comunicación entre la zona VERDE y NARANJA. Se observa que el Endian ya incluye reglas predefinidas que permiten todo el tráfico entre estas zonas, sin embargo, se añadieron reglas específicas para HTTP (puerto 80) y FTP (puerto 21) con el fin de tener un control más granular sobre los servicios permitidos y documentar puntualmente cada protocolo habilitado.

Figura 44. Verificación de las reglas de inter zonas.



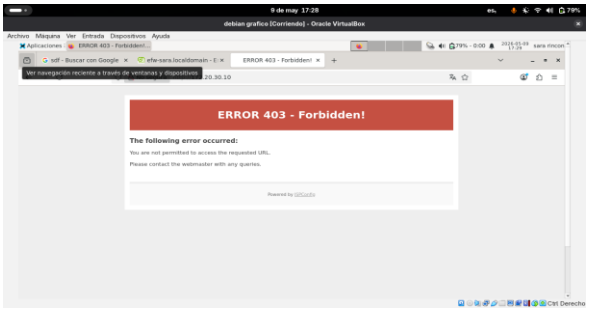
Fuente: Autoría Propia

2.4.4 Probar Desde Un Navegador Web, Las Siguientes Directivas

El Ingreso Del Servicio HTTP Desde La LAN Hacia La Zona DMZ.

Al ingresar a http://172.20.30.10 desde la zona VERDE, el servidor respondió con un error 403 del panel ISPConfig. Esto confirma que la regla Inter-Zone HTTP está funcionando correctamente, ya que la petición atravesó el firewall y fue respondida por el servidor web en la DMZ.

Figura 45. Prueba realizada desde el cliente accediendo a la página web.

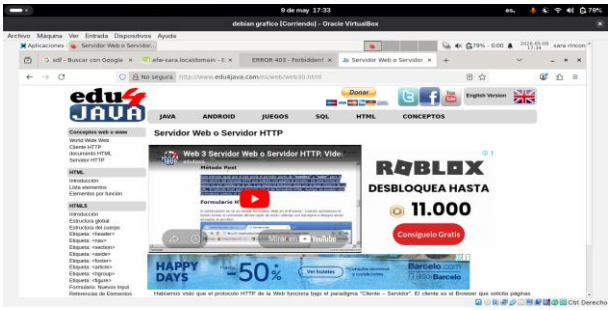


Fuente: Autoría Propia

2.4.5 El Ingreso Del Servicio HTTP Desde La LAN Hacia La WAN.

Se verificó el acceso HTTP desde la zona VERDE hacia Internet (WAN). Al ingresar a un sitio web externo, el navegador mostró el aviso "No seguro", característico de las páginas que utilizan el protocolo HTTP sin cifrado. La página cargó correctamente, confirmando que la LAN tiene salida a Internet a través del Endian.

Figura 46. Accediendo a una página HTTP alojada en la red.

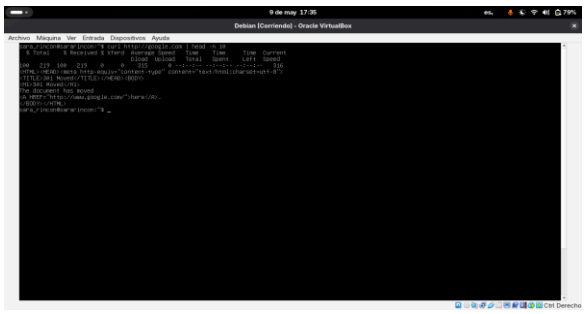


Fuente: Autoría Propia

2.4.6El Ingreso Del Servicio HTTP Desde La Zona DMZ Hacia La WAN.

Desde el servidor ubicado en la zona DMZ se ejecutó el comando curl http://google.com, obteniendo una respuesta HTTP 301. Esto confirma que el tráfico desde la DMZ hacia Internet (WAN) está permitido y que la regla de salida configurada en el Endian funciona correctamente.

Figura 47. Acceso a una página http desde la DMZ.

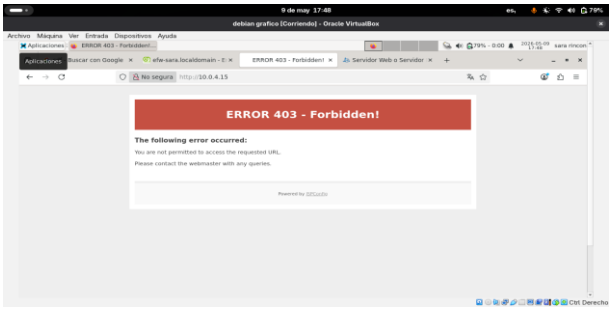


Fuente: Autoría Propia

2.4.7El Ingreso Del Servicio HTTP Desde La WAN Hacia La Zona DMZ.

Se probó el acceso HTTP desde la WAN hacia la DMZ ingresando a http://10.0.4.15 (IP de la interfaz RED del Endian). La petición fue redirigida correctamente al servidor ubicado en la zona NARANJA, el cual respondió con el panel de ISPConfig. Esto confirma que la regla de Port Forwarding para el puerto 80 está funcionando.

Figura 48. Acceso a la página alojada en el servidor a través de la IP pública.

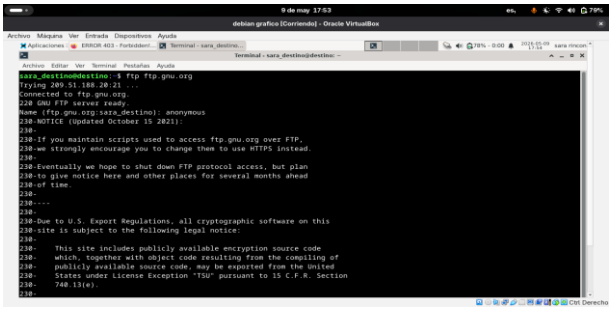


Fuente: Autoría Propia

2.4.8El Ingreso Del Servicio FTP Desde La LAN Hacia La WAN.

Se probó el acceso FTP desde la zona VERDE hacia Internet (WAN) utilizando el comando ftp ftp.gnu.org. La conexión fue exitosa y se realizó el inicio de sesión con usuario anónimo, comprobando que el Endian permite el tráfico FTP saliente desde la LAN hacia la WAN.

Figura 49. Acceso a un servicio FTP alojado en internet desde el cliente.

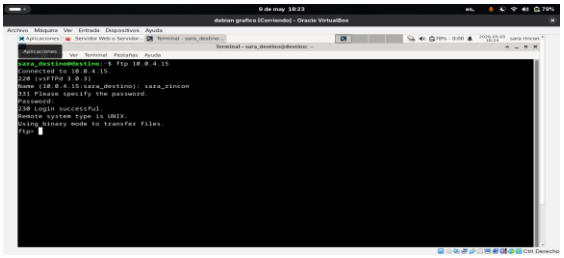


Fuente: Autoría Propia

2.4.9El Ingreso Del Servicio FTP Desde La WAN Hacia La Zona DMZ.

Se realizó la prueba de acceso FTP desde la WAN hacia la DMZ utilizando el comando ftp 10.0.4.15 (IP de la interfaz RED del Endian). La conexión fue redirigida correctamente al servidor FTP ubicado en la zona NARANJA, permitiendo el inicio de sesión exitoso con usuario y contraseña. Esto confirma que la regla de Port Forwarding para el puerto 21 está operativa.

Figura 50. Acceso al servicio FTP alojado en el servidor a través de la IP pública.



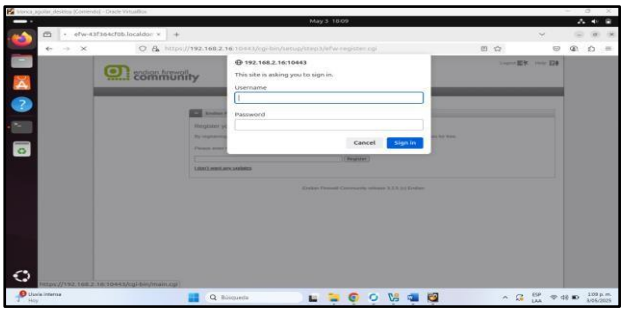
Fuente: Autoría Propia

2.5 Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Se debe configurar un perfil de navegación que incluya una lista negra para bloquear el acceso a páginas como www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. También se debe activar la autenticación por usuario, creando un usuario específico y asignándolo a un grupo. A este grupo se le aplicará una política de acceso, la cual se asociará al perfil previamente creado. Como prueba final, se verificará desde la red LAN que el navegador no permita ingresar a los sitios bloqueados.

Una vez configuradas las zonas, se procede a acceder al Endian Firewall desde el navegador de Ubuntu Desktop: a través de 192.168.90.1, e ingresamos las credenciales previamente asignadas.

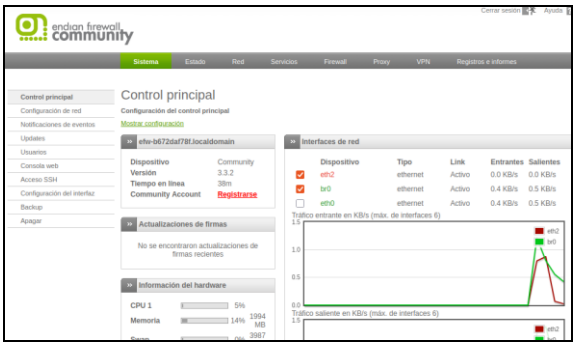
Figura 51. Login en Endian firewall, Ubuntu Desktop.



Fuente: Autoría propia.

Una vez realizado el Login correctamente, se accede a Endian Firewall, como se evidencia en la figura 51.

Figura 52. Entorno de trabajo Endian Firewall Comunnity, Ubuntu Desktop.



Fuente: Autoría propia.

Para iniciar con el cumplimiento de la temática 5, se trabaja sobre el módulo de Network configuration y se procede a realizar la configuración inicial de Endian Firewall Community se seleccionó el modo de red enrutamiento para permitir la comunicación segura entre las zonas LAN, DMZ y WAN. Posteriormente, se configuró la zona RED mediante DHCP con el fin de obtener automáticamente la conexión a Internet desde VirtualBox.

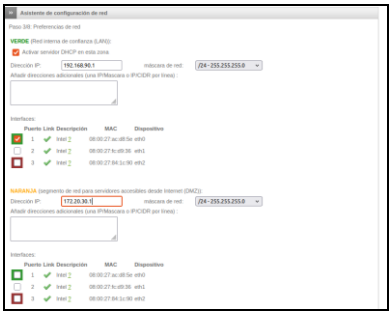
Figura 53. Configuración de red Endian, zona roja de manera DHCP.

Fuente: Autoría propia.

En la información de hardware se definieron tres interfaces de red correspondientes a las zonas GREEN, ORANGE y RED, permitiendo establecer la segmentación de la infraestructura de seguridad perimetral.

En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado naranja para definir el segmento de red que será accesible desde Internet (DMZ).

Figura 54. Configuración del tipo de red para las zonas del firewall.

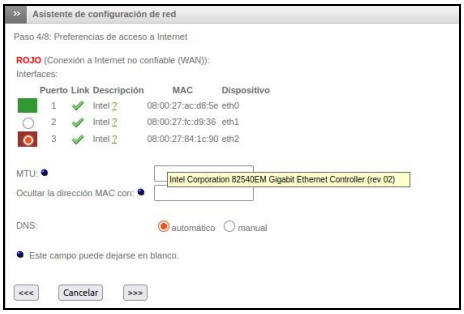


Fuente: Autoría propia.

Se verifican las ip de verde 192.168.90.1 y naranja 172.20.30.1

La configuración DNS se estableció de manera automática mediante DHCP, permitiendo que el firewall obtuviera dinámicamente los parámetros de conectividad necesarios para el acceso a Internet y la resolución de nombres de dominio.

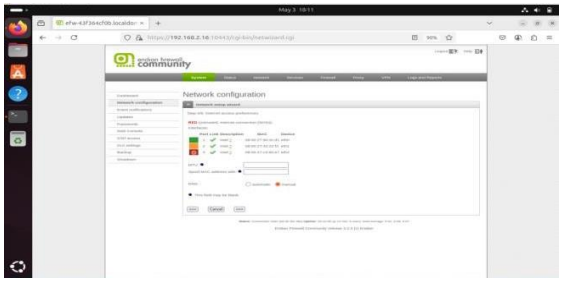
Figura 55. Configuración DNS automática



Fuente: Autoría propia.

De igual forma se confirma la zona roja DHCP.

Figura 56. Zona roja DHCP.



Fuente: Autoría propia.

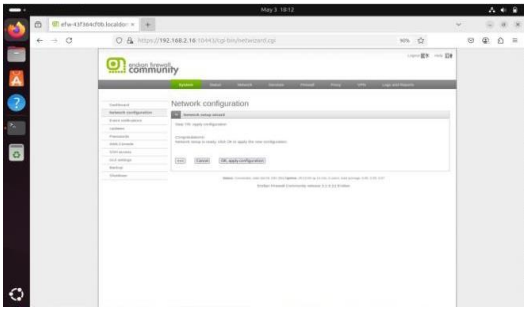
Se procede a verificar o ajustar los DNS 8.8.8.8 y 4.4.4.4.

Figura 57. DNS 8.8.8.8 y 4.4.4.4.

Fuente: Autoría propia.

Se pregunta si se desean aplicar los cambios, a lo cual se responde positivamente.

Figura 58. Configuraciones de Endian Firewall.



Fuente: Autoría propia.

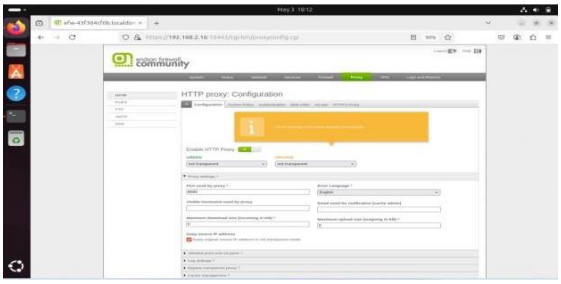
Figura 59. Mensaje de configuración exitosa de Endian Firewall.

Fuente: Autoría propia.

La figura 60, evidenció el mensaje de aplicación exitosa.

Al continuar con el proceso, se habilita el servicio de proxy.

Figura 61. Servicio proxy.



Fuente: Autoría propia.

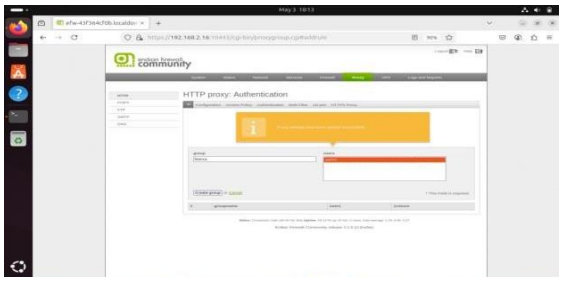
Se crea el usuario en el módulo de autenticación.

Figura 62. Creación de usuario en el módulo de autenticación.

Fuente: Autoría propia.

Una vez creado el usuario admin, se crea el grupo llamado blanca y se asocia a dicho grupo.

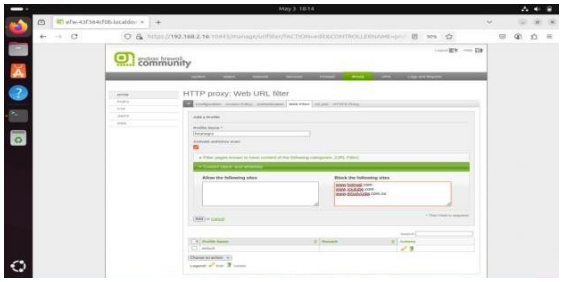
Figura 63. Creación de grupo en el módulo de autenticación.



Fuente: Autoría propia.

Una vez asociado el usuario admin, al grupo blanca; se crea un nuevo filtro con el nombre lista negra, donde se bloquean las 3 páginas sugeridas en la temática: www.hotmail.com, www.youtube.com, www.elnuevodia.com.co, se aplican y se guardan los cambios.

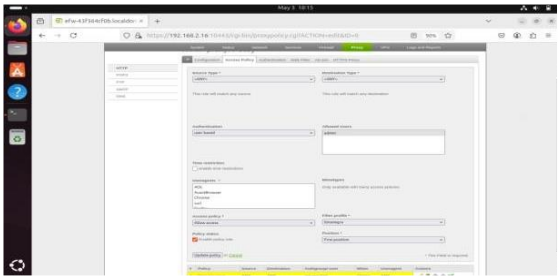
Figura 64. Creación de filtro.



Fuente: Autoría propia.

Se procede a crear una política de acceso donde se asocia el usuario admin, y se admite que apruebe la regla que se creó llamada lista negra.

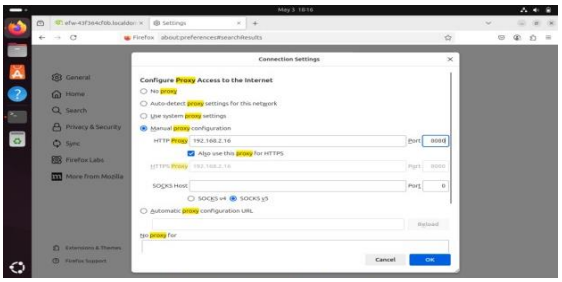
Figura 65. Creación de política de acceso.



Fuente: Autoría propia.

Finalmente, en la configuración de proxy del buscador Firefox (Ubuntu Desktop), se configura manualmente el Proxy donde se agrega 192.168.90.1 y adicional se habilita que use el mismo proxy en HTTPS.

Figura 66. Configuración de manual del proxy en el navegador.



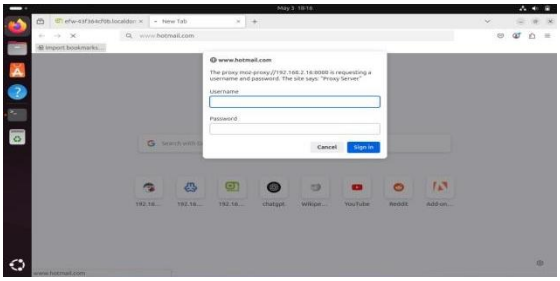
Fuente: Autoría propia.

La implementación permitió validar el correcto funcionamiento del Proxy HTTP no transparente, evidenciando autenticación obligatoria para los usuarios antes de acceder a Internet. Los sitios permitidos funcionaron normalmente, mientras que las páginas incluidas en la lista negra fueron bloqueadas exitosamente mediante políticas de filtrado web.

Asimismo, se verificó la administración del servicio Squid desde consola GNU/Linux mediante comandos de inicio, detención y reinicio del servicio, confirmando la operatividad del sistema de seguridad implementado

Para cerrar con broche de oro se verifica el éxito de las configuraciones, intentando ingresar a las páginas bloqueadas a través de la lista creada, por tanto, se accede desde el buscador Firefox a las siguientes páginas: Hotmail, YouTube y Nuevo Día, respectivamente, a los cual solicita autenticación de usuario, como se observa en la figura 17.

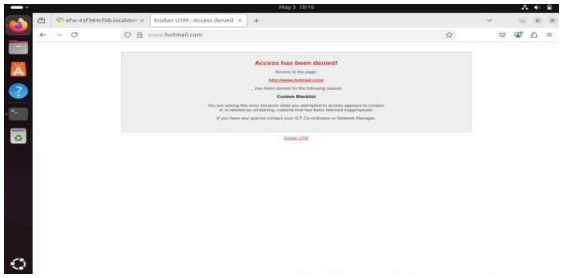
Figura 67. Autenticación de usuario.



Fuente: Autoría propia.

Luego de ingresar la autenticación, se evidencia el acceso denegado en Hotmail.

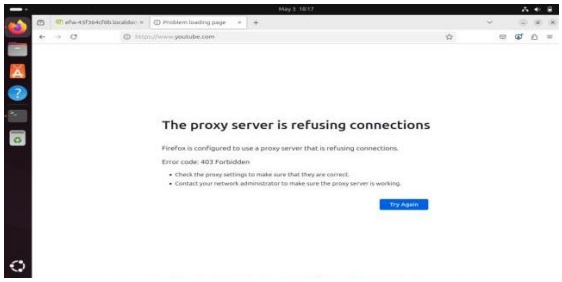
Figura 68. Acceso a Hotmail a través de Firefox.



Fuente: Autoría propia.

Respectivamente se intenta acceder a www.youtube.com y se evidencia el mismo mensaje.

Figura 69. Acceso a YouTube a través de Firefox.
Fuente: Autoría propia.



Y por último, se intenta ingresar a www.elnuevodia.com.co y el acceso es denegado, evidenciando el cumplimiento al objetivo deseado.

Figura 70. Acceso a El Nuevo Día a través de Firefox.

Fuente: Autoría propia.

2.5.1 Analisis

Se establecieron reglas para permitir o denegar acceso a servicio http y ftp, así como el bloqueo de ping entre todos los equipos de la red. El permitir los servicios HTTP y FTP es una estrategia clave para la administración de seguridad en redes. El bloqueo de ping (puertos 8 y 30) evita exploraciones no autorizadas y posibles ataques de reconocimiento, reforzando la privacidad de los servidores y dispositivos dentro de la red. Por otro lado, la habilitación de HTTP y FTP garantiza la accesibilidad a servicios web y transferencia de archivos, asegurando la operatividad sin comprometer la seguridad.

La combinación de estas reglas permite un equilibrio entre control de tráfico y funcionalidad, adaptándose a distintas necesidades y entornos corporativos. el funcionamiento de cada regla, se evidenció el correcto aislamiento y la comunicación permitida entre las distintas zonas, cumpliendo los objetivos planteados en cuanto a seguridad y accesibililidad.

3. CONCLUSIONES

La implementación de una zona desmilitarizada (DMZ) bajo plataformas GNU/Linux utilizando Endian Firewall demostró ser una estrategia eficaz para delimitar las redes internas y externas, fortaleciendo la seguridad perimetral en entornos corporativos y educativos. La gestión del tráfico y la aplicación de políticas de acceso permitieron validar la protección de servicios críticos como HTTP y FTP, al tiempo que se restringieron protocolos susceptibles de explotación, como ICMP.

El trabajo colaborativo entre los integrantes del grupo resultó fundamental para la correcta configuración de reglas de NAT, la habilitación de servicios en la DMZ y la implementación de un proxy HTTP con autenticación, evidenciando la importancia de la distribución de tareas en proyectos de seguridad informática. Asimismo, el uso de entornos virtualizados facilitó la simulación de escenarios reales sin comprometer infraestructuras físicas, lo que permitió analizar ventajas, limitaciones e inconsistencias de manera controlada.

En conjunto, los resultados obtenidos confirman que la planificación conjunta y el uso de herramientas libres como Endian Firewall contribuyen significativamente al fortalecimiento de la seguridad perimetral y a la disponibilidad de servicios en redes LAN, WAN y DMZ, abriendo la posibilidad de futuras mejoras en la automatización de reglas y la integración de servicios adicionales.

4. REFERENCIAS

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

[2] Canonical, Help Ubuntu, Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/

[3] Debian, El manual del administrador de Debian 12.5.0, Debian, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle, Manual de usuario VirtualBox, VirtualBox, 2020. [En línea]. Disponible en: https://www.virtualbox.org/manual/

[5] Endian, Endian UTM 3.2 Manual de referencia, Endian, 2016. [En línea]. Disponible en: http://docs.endian.com/3.2/utm/index.html

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

[7] Á. J. Cervelión, Instalación de Nagios Core 4.4 en Ubuntu 22.04. Objeto virtual de información (OVI), Repositorio Institucional UNAD, 2023. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/54230