SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNO VIRTUALIZADO

Andrés Felipe Benavides Bastidas
e-mail: afbenavidesb@unadvirtual.edu.co
Yessica Liliana Cerón Muñoz
e-mail: ylceronm@unadvirtual.edu.co
Francisco Andrés Nupán Cabrera
e-mail: fanupanc@unadvirtual.edu.co
Daniel Andrés Ortega Velasco
e-mail: daortegave@unadvirtual.edu.co
Sofía Rosero Mora
e-mail: sroseromo@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el proceso de instalación y configuración de Endian Firewall en un entorno virtual creado con VirtualBox. Durante el desarrollo del trabajo se organizó la red en tres zonas: LAN, DMZ y WAN, y se configuraron reglas NAT, DNAT y permisos de acceso para controlar el tráfico entre ellas. También se realizaron pruebas de conectividad, navegación y verificación de servicios para confirmar que todo funcionara correctamente. El objetivo principal fue entender cómo funciona un firewall perimetral y cómo se pueden aplicar sus herramientas para mejorar la seguridad de una red de manera práctica.*

ABSTRACT: *This article presents the installation and configuration process of Endian Firewall in a virtual environment created with VirtualBox. During the process, the network was organized into three zones: LAN, DMZ, and WAN. NAT, DNAT, and access permissions were configured to control traffic between these zones. Connectivity, browsing, and service verification tests were also performed to confirm that everything was functioning correctly. The main objective was to understand how a perimeter firewall works and how its tools can be practically applied to improve network security.*

PALABRAS CLAVE: DMZ, Endian Firewall, Firewall, NAT, Seguridad de red, VirtualBox.

1 INTRODUCCIÓN

La seguridad en una red no depende solo de instalar un firewall, sino de entender cómo se comportan sus diferentes funciones y cómo cada una aporta a la protección general. Por eso, en este trabajo se realiza la implementación de Endian Firewall dentro de un entorno virtual creado con VirtualBox, con el propósito de practicar paso a paso varias temáticas relacionadas con la seguridad perimetral.

Primero, se hace la instalación y configuración básica del sistema, organizando la red en las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN). Luego, se trabaja en la creación de reglas NAT y DNAT para permitir la salida a Internet y el acceso a servicios internos según correspondiera. También se configuraron permisos específicos en el firewall para controlar el tráfico entre las distintas zonas y se validaron servicios implementados dentro de la DMZ.

Además de estas configuraciones iniciales, también se tienen en cuenta las temáticas relacionadas con la autenticación de usuarios, el manejo de políticas de contenido y el uso del proxy, ya que forman parte del proceso de asegurar el acceso y regular el uso de los servicios dentro de la red. Finalmente, se realizan pruebas de conexión, navegación y funcionamiento general para confirmar que cada ajuste se hubiera aplicado correctamente.

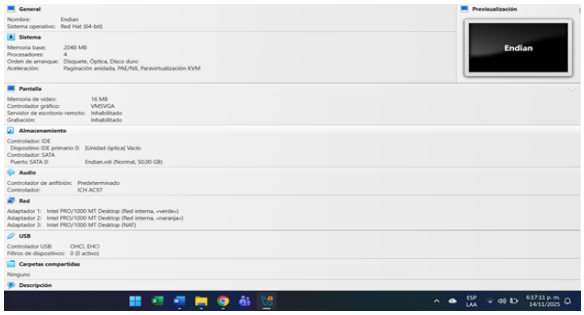
2 DESARROLLO TEMÁTICA 1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

La implementación de Endian Firewall Community como solución de seguridad perimetral requiere una configuración precisa de la infraestructura virtualizada que soporte la segmentación de red en zonas de seguridad diferenciadas. Este apartado detalla el proceso de instalación y configuración de GNU/Linux Endian en VirtualBox, estableciendo tres zonas de seguridad: verde (LAN), roja (WAN) y naranja (DMZ).

2.1 CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

El proceso de implementación inició con la creación de una máquina virtual en Oracle VirtualBox versión 7.0, asignando el nombre "Endian" al sistema. Se seleccionó la imagen ISO de Endian Firewall Community, distribución basada en Red Hat Enterprise Linux de 64 bits. Los recursos asignados comprendieron 2048 MB de memoria RAM, 4 núcleos de CPU y un disco duro virtual de 50 GB, parámetros suficientes para garantizar el funcionamiento óptimo del firewall en un entorno de pruebas. [5]

Figura 1. Configuración inicial de la máquina virtual Endian en VirtualBox

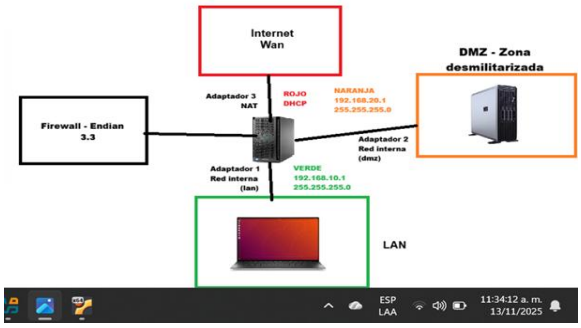


Fuente: Autoría Propia

2.2 ARQUITECTURA DE SEGMENTACIÓN DE RED

Antes de proceder con la configuración detallada de los adaptadores de red, resulta fundamental comprender la arquitectura completa de segmentación que se implementará. La topología diseñada sigue el modelo de seguridad perimetral basado en zonas diferenciadas, donde cada segmento de red opera con niveles de confianza y restricciones específicas [2].

Figura 2. Diagrama de arquitectura de segmentación de red implementada



Fuente: Autoría Propia

Como se observa en la Figura 2, la arquitectura implementada comprende los siguientes componentes interconectados:

2.2.1 ZONA VERDE (LAN - 192.168.10.0/24)

Representa la red de área local de confianza, conectada mediante el Adaptador 1 en modo red interna. Esta zona aloja los dispositivos cliente finales, tales como estaciones de trabajo de empleados, computadoras personales y dispositivos móviles corporativos. El direccionamiento asignado utiliza la subred 192.168.10.0/24 con máscara 255.255.255.0, donde la puerta de enlace predeterminada se establece en 192.168.10.1 (interfaz verde del firewall). El código de color verde simboliza el nivel de confianza más alto dentro de la infraestructura organizacional.

2.2.2 ZONA NARANJA (DMZ - 192.168.20.0/24)

Constituye la zona desmilitarizada o red perimetral, implementada mediante el Adaptador 2 en modo red interna. Esta zona intermedia hospeda servidores que proveen servicios accesibles desde Internet, tales como servidores web (HTTP/HTTPS), servidores de correo electrónico (SMTP), servidores FTP y servidores DNS públicos. El direccionamiento utiliza la subred 192.168.20.0/24 con máscara 255.255.255.0, estableciendo la puerta de enlace en 192.168.20.1 (interfaz naranja del firewall). El código de color naranja representa un nivel de confianza intermedio, requiriendo controles de seguridad más estrictos que la zona verde, pero permitiendo cierta exposición controlada hacia redes externas.

2.2.3 ZONA ROJA (WAN - DHCP)

Representa la conexión hacia Internet o redes externas no confiables, configurada mediante el Adaptador 3 en modo NAT. Esta zona opera con asignación dinámica de direcciones IP mediante protocolo DHCP, típicamente obteniendo direccionamiento del proveedor de servicios de Internet (ISP) o, en el caso del entorno virtualizado, del servidor DHCP de VirtualBox. El código rojo simboliza el nivel de confianza más bajo, considerándose toda comunicación de esta zona como potencialmente hostil hasta que se demuestre lo contrario.

2.2.4 FIREWALL ENDIAN 3.3

Actúa como elemento central de control y punto de aplicación de políticas de seguridad. Todas las comunicaciones inter-zona deben transitar obligatoriamente a través del firewall, donde son inspeccionadas, filtradas y registradas según las reglas establecidas. El firewall implementa funcionalidades de enrutamiento entre zonas, traducción de direcciones de red (NAT), filtrado de paquetes mediante reglas stateful, servicios de proxy HTTP/HTTPS, detección y prevención de intrusiones (IDS/IPS), y registro centralizado de eventos de seguridad.

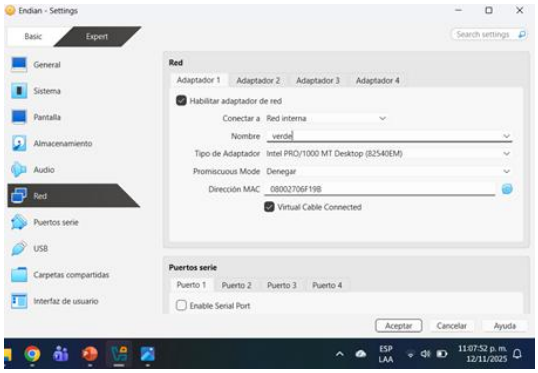
2.3 CONFIGURACIÓN DE ADAPTADORES DE RED

La segmentación de red se implementó mediante la configuración de tres adaptadores de red virtuales, cada uno asignado a una zona de seguridad específica según el modelo de seguridad perimetral de Endian [2].

2.3.1 ADAPTADOR 1 - ZONA VERDE (LAN)

Se configuró como red interna con el identificador "verde". Este adaptador gestiona la comunicación con los dispositivos de la red local de confianza, estableciendo la dirección MAC 08:00:27:06:F1:9B que posteriormente se vinculó con la interfaz de administración.

Figura 3. Configuración del adaptador de red para la zona verde

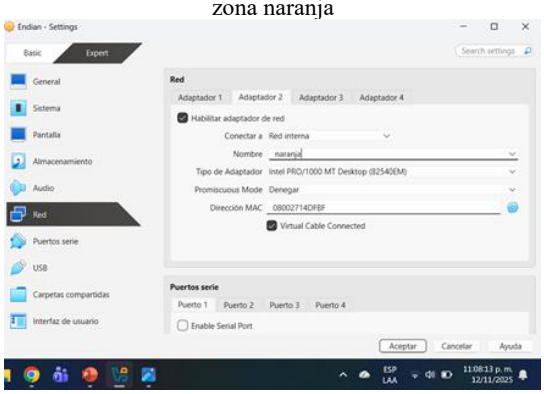


Fuente: Autoría Propia

2.3.2 ADAPTADOR 2 - ZONA NARANJA (DMZ)

Se estableció como red interna con identificador "naranja", destinado a alojar los servidores de servicios públicos. La dirección MAC asignada fue 08:00:27:14:DF:BF, permitiendo la separación lógica de los servicios expuestos hacia Internet.

Figura 4. Configuración del adaptador de red para la zona naranja

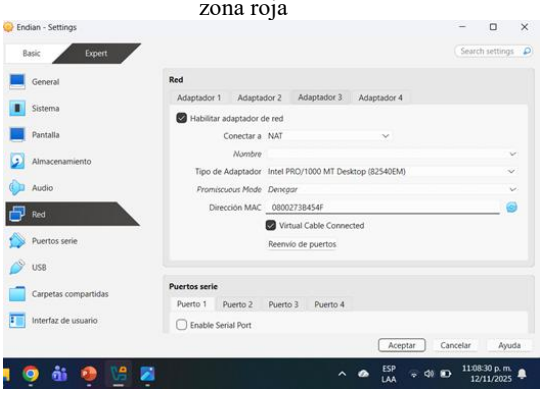


Fuente: Autoría Propia

2.3.3 ADAPTADOR 3 - ZONA ROJA (WAN)

Se configuró en modo NAT para proporcionar conectividad hacia Internet. Este adaptador opera con asignación dinámica de direcciones IP mediante DHCP, con dirección MAC 08:00:27:3B:45:4F.

Figura 5. Configuración del adaptador de red para la zona roja



Fuente: Autoría Propia

2.4 PROCESO DE INSTALACIÓN DEL SISTEMA OPERATIVO

La instalación de Endian Firewall se ejecutó mediante un proceso asistido que comprendió las siguientes etapas críticas:

2.4.1 SELECCIÓN DE IDIOMA E INICIO DE INSTALACIÓN

Se seleccionó el idioma inglés como predeterminado para el sistema, facilitando la compatibilidad con documentación técnica internacional [2].

2.4.2 PARTICIONAMIENTO DEL DISCO

Se optó por utilizar la totalidad del disco duro virtual de 50 GB, permitiendo al instalador crear automáticamente el esquema de particiones óptimo para el sistema operativo.

Figura 6. Proceso de particionamiento del disco duro

Fuente: Autoría Propia

2.4.3 INSTALACIÓN DE PAQUETES

El sistema procedió a instalar los componentes base del sistema operativo, incluyendo el kernel de Linux, herramientas de administración y módulos de firewall.

2.4.4 CONFIGURACIÓN DEL PUERTO SERIAL

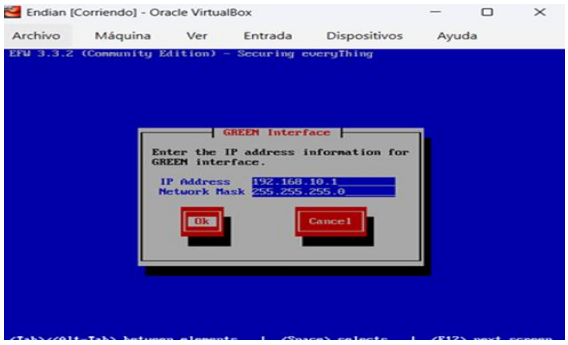
Se habilitó el soporte para puerto serial, funcionalidad que permite la administración remota mediante consola en caso de pérdida de conectividad de red.

2.5 CONFIGURACIÓN DE ZONAS DE SEGURIDAD

Durante la fase de configuración inicial post-instalación, se establecieron los parámetros de red para cada zona de seguridad:

Zona Verde (LAN): Se asignó la dirección IP 192.168.10.1/24 como puerta de enlace predeterminada, interfaz primaria de administración del firewall. Esta configuración permite que los dispositivos cliente en la red interna accedan a la interfaz web de gestión.

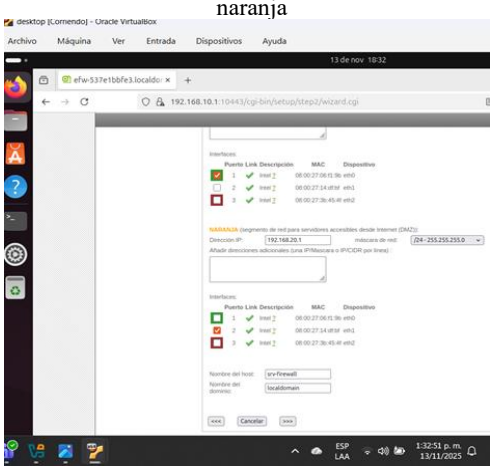
Figura 7. Configuración de la interfaz de red para la zona verde



Fuente: Autoría Propia

Zona Naranja (DMZ): Posterior a la instalación base, se configuró manualmente la dirección IP 192.168.20.1/24 para la zona desmilitarizada, estableciendo el host con nombre "srv-firewall".

Figura 8. Configuración de la interfaz de red para la zona naranja



Fuente: Autoría Propia

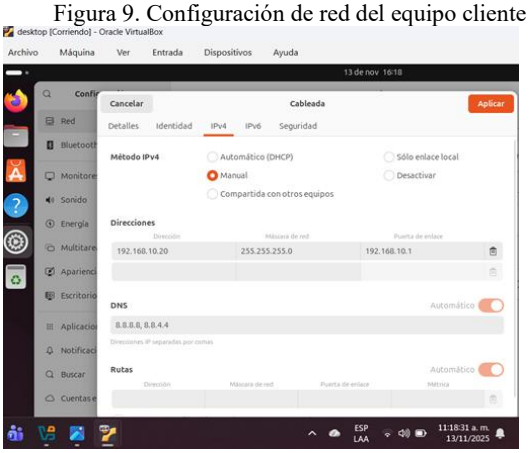
Zona Roja (WAN): Se mantuvo la configuración DHCP automática proporcionada por el adaptador NAT de VirtualBox, obteniendo dinámicamente la dirección IP 10.0.4.15/24 con puerta de enlace 10.0.2.2.

2.6 CONFIGURACIÓN DE EQUIPOS CLIENTE Y SERVIDOR

Para validar la correcta segmentación de red, se configuraron dos máquinas virtuales adicionales con Ubuntu Desktop 24.04 LTS [3]:

Cliente Desktop (Zona Verde): Se configuró con dirección IP estática 192.168.10.20/24, puerta de enlace 192.168.10.1 y servidor DNS 8.8.8.8. Esta máquina representa un dispositivo de usuario final en la red de confianza [1].

Figura 9. Configuración de red del equipo cliente



Fuente: Autoría Propia

Servidor Ubuntu (Zona Naranja): Se estableció con dirección IP 192.168.20.20/24, puerta de enlace 192.168.20.1 y DNS 8.8.8.8, preparando el entorno para alojar servicios web y de transferencia de archivos [1].

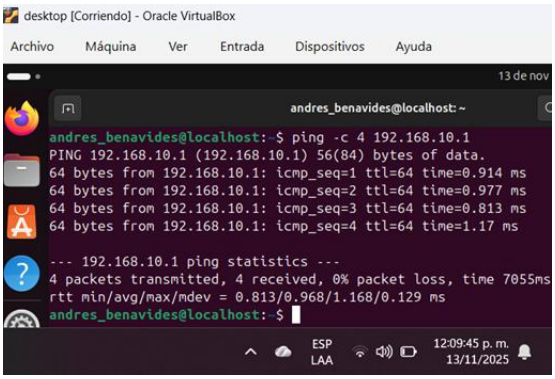
Figura 10. Configuración de red del servidor DMZ

Fuente: Autoría Propia

2.7 VERIFICACIÓN DE CONECTIVIDAD Y ACCESO A LA INTERFAZ WEB

Una vez completada la instalación y configuración, se procedió a verificar la conectividad entre las distintas zonas de seguridad. Desde el equipo cliente en la zona verde, se ejecutó el comando ping 192.168.10.1, obteniendo respuesta satisfactoria del firewall Endian [2].

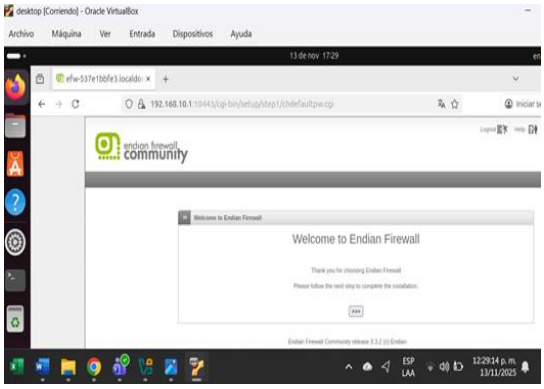
Figura 11. Prueba de conectividad desde el cliente hacia el firewall



Fuente: Autoría Propia

El acceso a la interfaz de administración web se realizó mediante navegador Firefox, ingresando a la URL https://192.168.10.1:10443. Tras aceptar el certificado auto firmado, se presentó la pantalla de bienvenida del asistente de configuración inicial.

Figura 12. Pantalla de bienvenida de la interfaz web de Endian



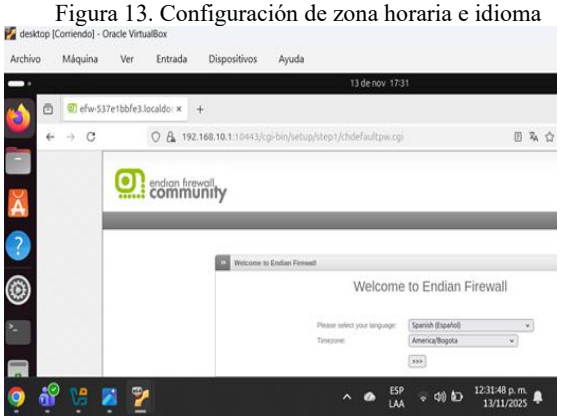
Fuente: Autoría Propia

2.8 CONFIGURACIÓN INICIAL DEL SISTEMA

El asistente de configuración inicial guio el proceso de parametrización del sistema, estableciendo [2].

- Idioma: español (España)
- Zona horaria: América/Bogotá (UTC-5)
- Contraseñas: Se establecieron credenciales seguras para los usuarios admin (administración web) y root (acceso SSH/consola)
- Modo de red: Enrutamiento (Routing mode)
- Tipo de enlace WAN: DHCP dinámico
- Número de interfaces: 3 adaptadores (Verde, Naranja, Roja)

Figura 13. Configuración de zona horaria e idioma



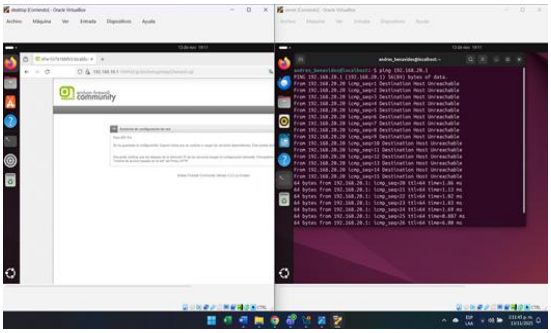
Fuente: Autoría Propia

Figura 14. Configuración de modos de red y adaptadores

Fuente: Autoría Propia

Una vez aplicadas las configuraciones, el sistema reinició los servicios de red, generando conectividad completa entre las tres zonas. Desde el servidor en la DMZ, se verificó exitosamente la conectividad hacia la puerta de enlace 192.168.20.1 [3].

Figura 15. Verificación de conectividad desde el servidor DMZ



Fuente: Autoría Propia

2.9 DASHBOARD DE ADMINISTRACIÓN Y MONITOREO

Finalmente, se accedió al panel de control principal de Endian, visualizando el estado de las tres interfaces de red configuradas [2]. El dashboard presentó información en tiempo real sobre el tráfico de red, estado de servicios y métricas de seguridad.

Figura 16. Panel de control principal de Endian Firewall

Fuente: Autoría Propia

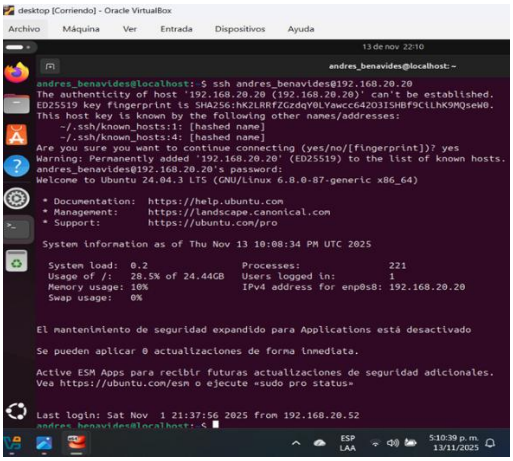
2.10 VERIFICACIÓN DE SERVICIOS Y CONECTIVIDAD SSH

Como validación final de la correcta configuración de la segmentación de red y las comunicaciones inter-zonas, se procedió a verificar la conectividad mediante el protocolo SSH (Secure Shell) desde el equipo cliente en la zona verde hacia el servidor ubicado en la zona naranja (DMZ).

Prueba de conectividad SSH hacia la DMZ: Desde el cliente Ubuntu Desktop en la zona verde (192.168.10.20), se estableció una conexión SSH hacia el servidor en la zona naranja (192.168.20.20) utilizando el comando ssh andres_benavides@192.168.20.20 [3]. Esta prueba válida que:

1. El enrutamiento entre la zona verde y la zona naranja está funcionando correctamente
2. El firewall Endian permite el tráfico SSH entre estas zonas
3. Los servicios de red en el servidor DMZ están operativos
4. La resolución de nombres y autenticación funcionan adecuadamente

Figura 17. Verificación del servicio SSH con conexión desde el cliente hacia el servidor DMZ



Fuente: Autoría Propia

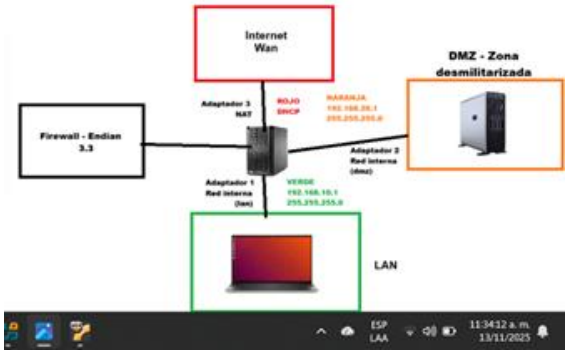
3 DESARROLLO TEMÁTICA 2 CONFIGURACIÓN NAT

En esta parte del trabajo se realizó la configuración de NAT en el firewall Endian. Esto permite a los equipos de la red interna salir a Internet sin que se vea su dirección IP real, ya que el firewall reemplaza esas direcciones por la que tiene configurada hacia la red WAN (la simulación de Internet).

En esta actividad se trabajó con tres zonas:

- Zona Verde (LAN): donde están los equipos internos (192.168.10.0/24).
- Zona Naranja (DMZ): donde se ubican posibles servidores que pueden publicar servicios (192.168.20.0/24).
- Zona Roja (WAN): conexión hacia Internet (IP por DHCP).

Figura 18. Topología utilizada con zonas Verde, Naranja y Roja.



Fuente: Autoría Propia

3.1 INGRESO A LA CONFIGURACIÓN NAT EN ENDIAN

Una vez que se completó la Temática 1, es decir, la instalación y la segmentación básica, Endian en la máquina virtual (configuración de interfaces Verde, Naranja y Roja, y la comprobación inicial de conectividad entre equipos), se procede a avanzar con la Temática 2. Con Endian ya instalado y las zonas creadas, la siguiente etapa consiste en habilitar y validar las reglas de NAT para permitir la salida controlada a Internet de la LAN y de la DMZ [2].

Figura 19. Panel de Endian

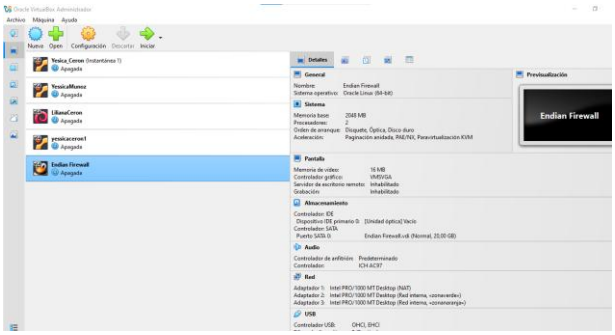
Fuente: Autoría Propia

3.2 VERIFICAR ESTADO DEL ENTORNO

En VirtualBox [5] se confirma que la VM “Endian” tiene 3 adaptadores:

- Adaptador 1: Red interna “verde”
- Adaptador 2: Red interna “naranja”
- Adaptador 3: NAT (o Bridge) “roja”

Figura 20. Adaptadores en VirtualBox para la VM Endian.



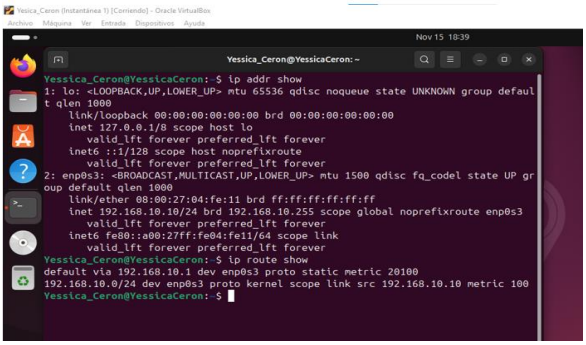
Fuente: Autoría Propia

Figura 21. Panel de interfaces en Endian

Fuente: Autoría Propia

Desde el cliente en la Zona Verde se confirmó la configuración de red ejecutando ip addr show y ip route show [3]. La salida mostró la dirección 192.168.10.10/24 y la ruta predeterminada vía 192.168.10.1, lo que verifica que el equipo está correctamente integrado al gateway administrado por Endian.

Figura 22. Salida de ip addr show y ip route show en cliente LAN.



Fuente: Autoría Propia

Para continuar con la configuración de la Temática 2, el primer paso consiste en ingresar a la interfaz administrativa del firewall Endian. Este acceso se realiza desde el navegador web del equipo ubicado en la Zona Verde (LAN), utilizando la dirección asignada a la interfaz verde del firewall.

Se debe abrir un navegador e ingresar la siguiente URL: https://192.168.10.1:10443

Al cargar la página, el sistema solicitará las credenciales del administrador. Una vez autenticado, se mostrará el panel principal de Endian, desde donde se gestionan las funciones del firewall.

Ingreso a la sección Firewall → NAT, dentro de esta sección se encuentran las herramientas para crear reglas.

Figura 23. Ingreso a Endian con las credenciales

Fuente: Autoría Propia

3.3 CREAR REGLA SNAT PARA LAN

El objetivo de este punto es que todos los equipos pertenecientes a la Zona Verde (LAN), con red 192.168.10.0/24, puedan acceder a Internet utilizando la dirección IP de la interfaz Roja (WAN) del firewall Endian. Para lograrlo, se crea una regla de Source NAT (SNAT) [2].

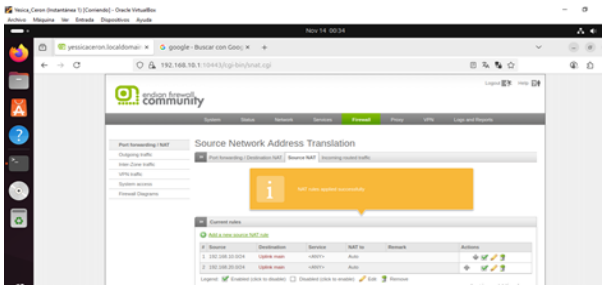
Figura 24. Acceso inicial al módulo NAT dentro de la interfaz gráfica de Endian

Fuente: Autoría Propia

En la opción Source NAT seleccionar "Agregar nueva regla", Completar los campos: Agregar mediante ip la zona de origen en este caso la zona verde, y la interfaz de salida en este caso la wan que es la roja y guardar cambios.

Con esta regla en funcionamiento, cualquier equipo dentro de la LAN podrá comunicarse con redes externas sin exponer su IP privada, incrementando la seguridad y facilitando la traducción de direcciones.

Figura 25. Creación de la regla SNAT para la red LAN dentro del módulo NAT de Endian.



Fuente: Autoría Propia

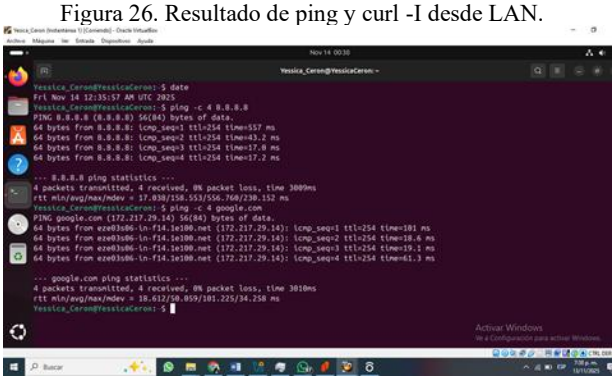
3.4 VERIFICAR SALIDA A INTERNET DESDE LAN

Desde el equipo cliente en la Zona Verde se ejecutaron pruebas de conectividad hacia Internet. El ping y la consulta HTTP (curl -I) confirmaron que la salida hacia Internet funciona correctamente a través de la regla SNAT aplicada [2].

Comandos de verificación

ping -c 4 8.8.8.8
curl -I http://example.com

Figura 26. Resultado de ping y curl -I desde LAN.



Fuente: Autoría Propia

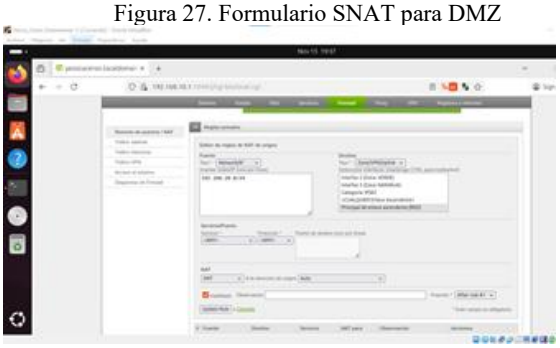
3.5 CREAR REGLA SNAT PARA DMZ

Después de comprobar la salida a Internet desde la Zona Verde, el siguiente paso es habilitar la traducción de direcciones para la Zona Naranja (DMZ), de manera que los servidores o servicios ubicados en dicha red puedan acceder a Internet sin exponer sus direcciones privadas.

La red utilizada para la DMZ en este escenario es 192.168.20.0/24, y al igual que en la LAN, se empleará una regla de Source NAT (SNAT), para que el tráfico saliente use la dirección IP configurada en la interfaz Roja (WAN) del firewall Endian.

En el mismo apartado de crear nueva regla, agrego los parámetros correspondientes, en este caso la zona de origen es la zona naranja y su interfaz de salida es zona Roja (WAN).

Figura 27. Formulario SNAT para DMZ

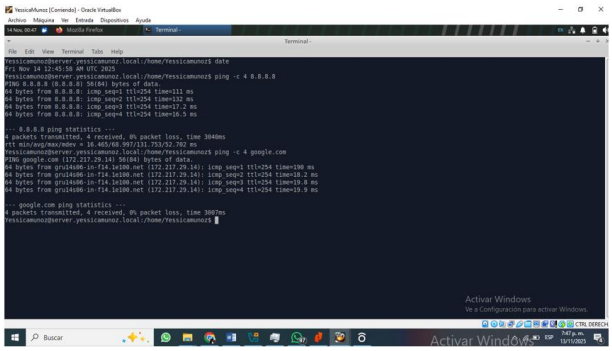


Fuente: Autoría Propia

3.6 VERIFICAR SALIDA A INTERNET DESDE DMZ

La prueba curl -I desde el servidor en la Zona Naranja devolvió cabeceras HTTP válidas, lo que confirma que la DMZ puede acceder a recursos externos mediante la regla SNAT configurada.

Figura 28. Resultado de ping y ping -c 4 google.com desde servidor DMZ.



Fuente: Autoría Propia

3.7 CONFIGURACIÓN DE DNAT / PORT FORWARDING EN ENDIAN

La regla DNAT o Port Forward en Endian Firewall se configura mediante su interfaz administrativa para permitir que un servicio alojado en la DMZ fuera accesible desde Internet. Se selecciona el servidor y el puerto del servicio (por ejemplo, HTTP en el puerto 80) y se crea la regla indicando la dirección IP pública del firewall, el puerto externo que recibiría las conexiones, la dirección IP interna del servidor y el puerto interno del servicio, junto con el protocolo correspondiente. Una vez activada la regla, se realizaron pruebas desde un host externo para verificar que el tráfico se redirigiera correctamente al servidor, confirmando que el servicio podía ser accedido de forma segura desde la red externa. [2].

Figura 29. DNAT con parámetros completados

Fuente: Autoría Propia

3.8 PROBAR ACCESO DESDE WAN

Para verificar la regla DNAT configurada, se utilizó una máquina host o una máquina virtual actuando como cliente externo. Desde este equipo se accedió a la dirección IP pública del firewall utilizando el puerto configurado, comprobando que las solicitudes se reenviaran correctamente al servidor en la DMZ y que el servicio respondiera según lo esperado [2].

Figura 30. Respuesta de máquina virtual externa

Fuente: Autoría Propia

En esta temática se llevó a cabo la configuración de las reglas de NAT y DNAT en Endian Firewall, asegurando la conectividad desde la LAN y la DMZ hacia la red externa simulada. Se implementaron reglas de traducción de direcciones y reenvío de puertos para publicar servicios específicos de manera segura. La correcta creación y activación de estas reglas se verificó mediante pruebas de conectividad interna y externa. Los resultados detallados de estas pruebas se presentan en la sección correspondiente de resultados del artículo.

4 DESARROLLO TEMÁTICA 3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

El siguiente procedimiento describe la implementación de reglas de firewall en Endian Firewall (EFW) para permitir selectivamente el tráfico de servicios esenciales (HTTP y FTP) desde la Zona Desmilitarizada (DMZ) y, simultáneamente, denegar el protocolo ICMP para aumentar la seguridad perimetral.

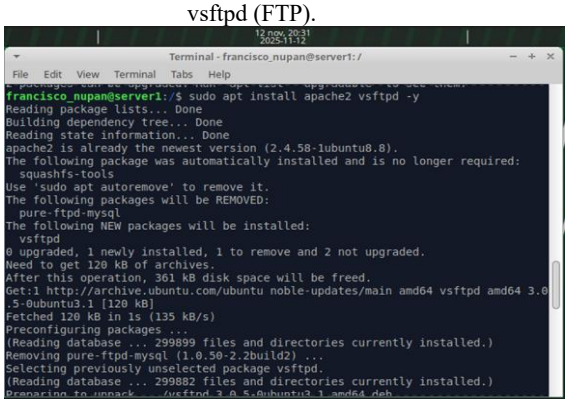
4.1 PREPARACIÓN DE SERVICIOS EN EL SERVIDOR DE LA ZONA DESMILITARIZADA (DMZ)

4.1.1 INSTALACIÓN DE SERVICIOS WEB Y DE TRANSFERENCIA DE ARCHIVOS

En el servidor GNU/Linux (Ubuntu Server) configurado dentro de la Zona Naranja (DMZ), se instalan los paquetes necesarios para proveer los servicios que serán expuestos a la red: Apache2 para el servicio HTTP y vsftpd para el servicio FTP. El proceso de instalación se inicia con la actualización de la lista de paquetes y la ejecución del comando de instalación [3].

Comando ejecutado en la consola del servidor DMZ: sudo apt update && sudo apt install apache2 vsftpd –y

Figura 31. Instalación de los servicios Apache (HTTP) y vsftpd (FTP).



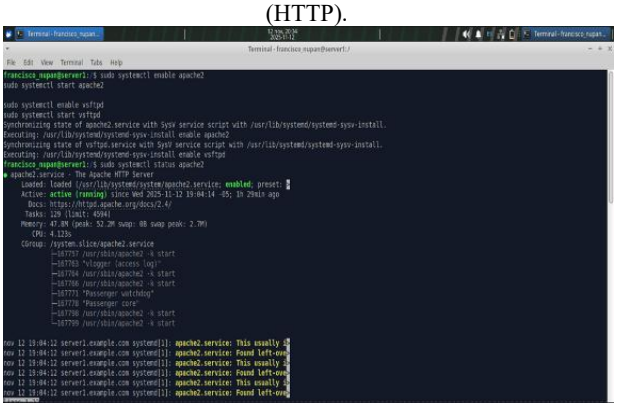
Fuente: Autoría Propia

4.1.2 VERIFICACIÓN DE LA OPERATIVIDAD DE LOS SERVICIOS

Una vez finalizada la instalación, se verifica el estado de los servicios recién instalados para confirmar su correcto arranque y disponibilidad [3]. El servicio Apache2 (HTTP) y el servicio vsftpd (FTP) deben mostrar un estado de active (running).

Comandos para la verificación: sudo systemctl status apache2 sudo systemctl status vsftpd

Figura 32. Verificación del estado del servicio Apache2 (HTTP).



Fuente: Autoría Propia

4.1.3 CONFIGURACIÓN DE REGLAS DE FIREWALL EN ENDIAN EFW (TRÁFICO DE SALIDA)

La configuración de las reglas de tráfico se realiza a través de la interfaz de administración web de Endian EFW, específicamente en la sección de control de tráfico de salida (Outbound traffic).

4.1.4 ACCESO A LA CONFIGURACIÓN DE TRÁFICO DE SALIDA

Se ingresa a la consola de administración de Endian y se navega a la sección Firewall -> Tráfico de salida para iniciar la creación de las reglas que controlarán el acceso desde la DMZ (Zona Naranja) hacia la WAN (Zona Roja/Internet).

Figura 33. Acceso a la sección de Tráfico de salida en Endian EFW.

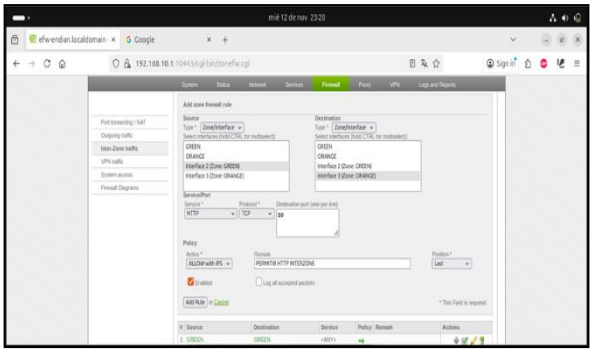
Fuente: Autoría Propia

4.1.5 CREACIÓN DE REGLA DE PERMISO PARA HTTP (PUERTO 80)

Se establece la primera regla para permitir el flujo de datos del servicio HTTP, esencial para la navegación web y la publicación del servidor. Los parámetros configurados son:

- Acción: Aceptar (ACCEPT).
- Zona de Origen: Naranja (DMZ), donde reside el servidor web.
- Destino: Cualquier, permitiendo la comunicación hacia la WAN.
- Servicio: HTTP (Puerto 80).

Figura 34. Creación de la regla de permiso HTTP desde DMZ a WAN.



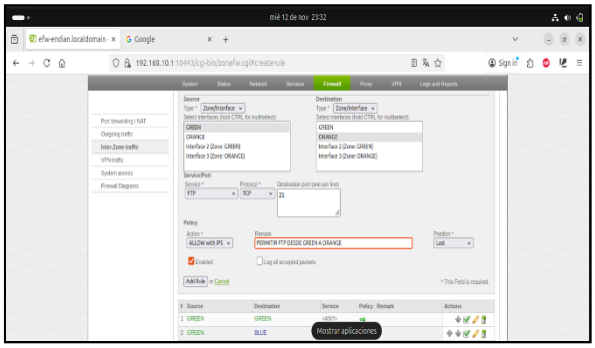
Fuente: Autoría Propia

4.1.6 CREACIÓN DE REGLA DE PERMISO PARA FTP (PUERTO 21)

De forma similar, se define una regla para autorizar la comunicación utilizando el protocolo FTP (puerto 21), permitiendo la transferencia de archivos desde el servidor DMZ hacia la WAN. Los parámetros se ajustan a:

- Acción: Aceptar (ACCEPT).
- Zona de Origen: Naranja (DMZ).
- Destino: Cualquier.
- Servicio: FTP (Puerto 21).

Figura 35. Creación de la regla de permiso FTP desde DMZ a WAN.

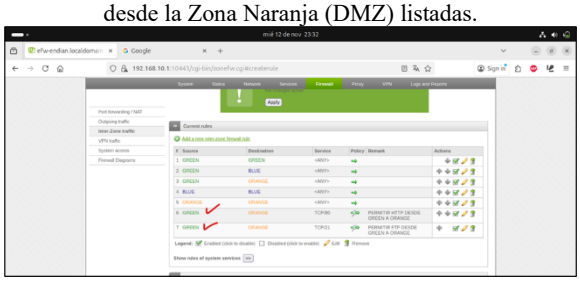


Fuente: Autoría Propia

4.1.7 VERIFICACIÓN DE REGLAS DE PERMISO

Se revisa la tabla de Tráfico de salida para constatar que las reglas de HTTP y FTP hayan sido registradas con la acción ACCEPT y las zonas de origen y destino correctas.

Figura 36. Reglas de tráfico de salida para HTTP y FTP desde la Zona Naranja (DMZ) listadas.



Fuente: Autoría Propia

4.1.8 CREACIÓN DE REGLA DE DENEGACIÓN PARA ICMP

Para cumplir con la política de seguridad que restringe el uso del comando ping en la red, se configura una regla para denegar el protocolo ICMP (Internet Control Message Protocol). Esta regla es crítica para evitar el escaneo de red básico.

Los parámetros establecidos son:

- Acción: Rechazar (DROP).
- Zona de Origen: Cualquier.
- Destino: Cualquier.
- Servicio: ICMP.

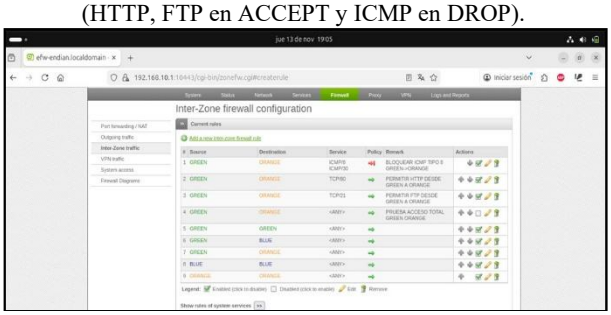
Figura 37. Creación de la regla de denegación para el protocolo ICMP.

Fuente: Autoría Propia

4.1.9 VERIFICACIÓN FINAL DE LAS POLÍTICAS IMPLEMENTADAS

Se realiza una inspección final de la lista de Tráfico de salida para confirmar que las reglas de permiso para HTTP y FTP se encuentren activas (ACCEPT) y que la regla de denegación para ICMP también esté activa (DROP), garantizando el cumplimiento de los requisitos de la temática.

Figura 38. Verificación de las reglas de Tráfico de salida (HTTP, FTP en ACCEPT y ICMP en DROP).



Fuente: Autoría Propia

4.2 PRUEBAS Y VERIFICACIÓN DE LA SEGURIDAD IMPLEMENTADA

Se realizaron pruebas de conectividad desde una estación de trabajo de la Zona Verde (LAN) hacia el servidor en la Zona Naranja (DMZ) para validar el comportamiento integrado de las políticas de seguridad (DROP) y de acceso a servicios (ACCEPT).

4.2.1 PRUEBA INTEGRADA DE SEGURIDAD Y SERVICIOS

La validación demostró que el firewall aplica correctamente las restricciones de seguridad mientras garantiza la disponibilidad operativa.

4.2.2 DENEGACIÓN (DROP ICMP)

La ejecución del comando ping 192.168.20.2 (dirigido a la DMZ) resultó en la denegación inmediata de la conexión, confirmando la pérdida del 100% de los paquetes. Esto válida la

regla de seguridad que bloquea el protocolo ICMP para mitigar el escaneo de red.

4.2.3 PERMISO (ACCEPT HTTP Y FTP)

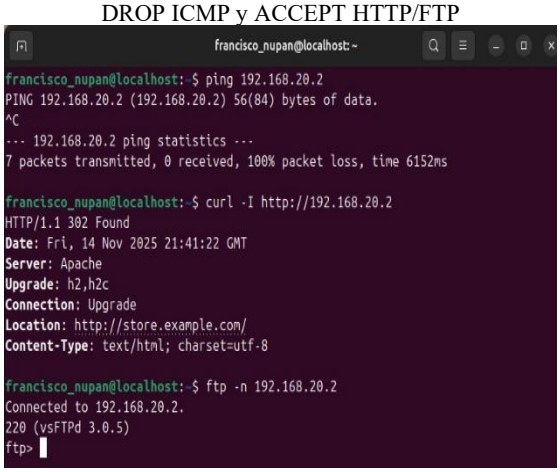
Para verificar la accesibilidad de los servicios esenciales:

La ejecución de curl -I http://192.168.20.2 confirmó la operatividad del servicio HTTP (puerto 80) al retornar exitosamente el código de respuesta HTTP 302 FOUND [3].

La prueba de acceso al servicio FTP (puerto 21) mediante el comando ftp -n 192.168.20.2 demostró la conexión directa al servidor sin requerir credenciales [3].

Estos resultados confirman que el firewall gestiona el tráfico de manera eficiente, permitiendo los flujos de datos esenciales (HTTP/FTP) mientras mantiene una postura de seguridad firme al denegar el protocolo ICMP.

Figura 39. Validación mediante consola de firewall: DROP ICMP y ACCEPT HTTP/FTP



Fuente: Autoría Propia

5 DESARROLLO TEMÁTICA 4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La temática 4 se llevó a cabo mediante la implementación de políticas de seguridad para administrar el flujo de tráfico interzonal y el control de accesos desde y hacia la zona roja.
Este proceso requirió la creación de reglas en el módulo firewall de Endian y configuraciones de traducción de direcciones de red, tanto de origen como de destino [2].

5.1 COMUNICACIÓN INTERZONAL Y TRÁFICO SALIENTE

Se configuraron reglas específicas en el módulo de firewall para asegurar que el tráfico entre las zonas LAN y DMZ se estableciera de manera controlada limitando la comunicación únicamente por medio de los protocolos autorizados. Se permitió la salida a internet para ambas zonas, mediante el uso de políticas de tráfico de salida y Nat de Origen, garantizado que tanto los clientes internos como los servidores pudieran acceder a recursos externos necesarios para su operación, sin comprometer la seguridad de la segmentación de la red interna.

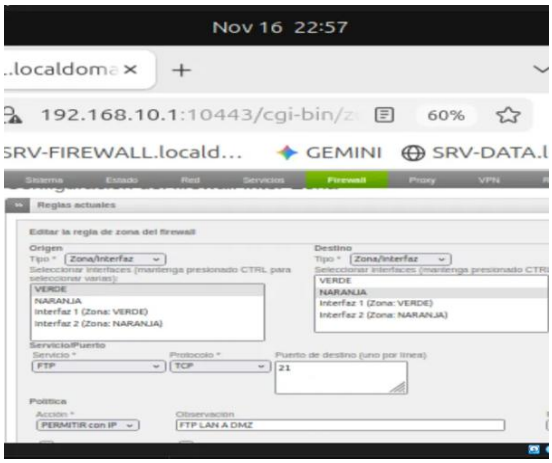
5.1.1 REGLAS DE LAN (ZONA VERDE) A DMZ (ZONA NARANJA)

Para cumplir con la directiva para la comunicación de servicios, se habilitaron reglas bidireccionales en el segmento verde a naranja.
En módulo firewall de Endian, en la sección Tráfico entre zonas, se permitió el protocolo HTTP (TCP/80) y FTP (TCP/21) entre las zonas verde 192.168.10.0/24 (LAN) y naranja 192.168.20.0/24 (DMZ).

Figura 40. Creación de Regla para HTTP (TCP/80

Fuente: Autoría Propia

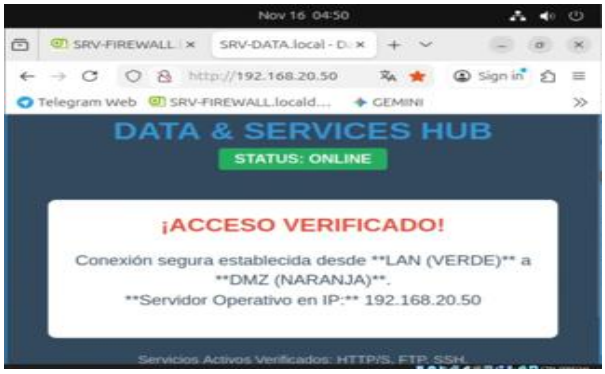
Figura 41. Creación de Regla FTP, puerto 21, protocolo TCP



Fuente: Autoría Propia

La conectividad mediante el protocolo HTTP fue probada con éxito validando la carga de la página web que se aloja en el servidor DMZ (192.168.20.50), desde el cliente LAN, una máquina virtual con Ubuntu Desktop como lo muestra la Figura 42 [1].

Figura 42. Ingreso del servicio HTTP desde la LAN a la zona DMZ, mediante el ingreso a una página creada en el servidor.



Fuente: Autoría Propia

La conectividad mediante FTP se llevó a cabo desde la máquina virtual cliente, ubicada en la zona verde por medio de la terminal ejecutando el comando ftp 192.168.20.50 (ip del servidor). En la Figura 43 podemos observar la conexión ftp correctamente establecida.

Figura 43. Conexión ftp al servidor mediante el usuario ftptestuser

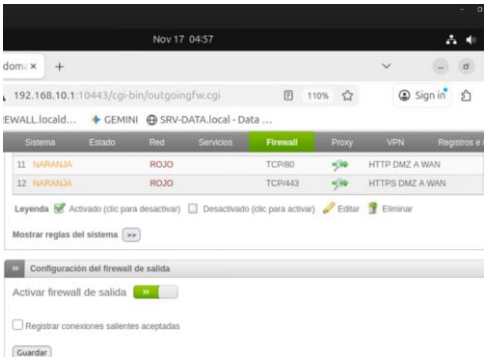
Fuente: Autoría Propia

5.1.2 REGLAS DE SALIDA A WAN

La conectividad hacia internet (WAN) para la zona DMZ se gestionó mediante la creación de reglas en la sección tráfico de salida, del módulo firewall. Las reglas que se crearon cumplen con la función de Filtrado de paquetes estas permiten pasar el tráfico saliente si cumplen con las condiciones de origen, destino y servicio.

La regla HTTP de DMZ a WAN permite que el servidor acceda a cualquier servidor de internet usando el puerto 80 y la regla HTTPS de DMZ a WAN permite que el servidor acceda a sitios web seguros en internet, que es lo más común hoy en día.

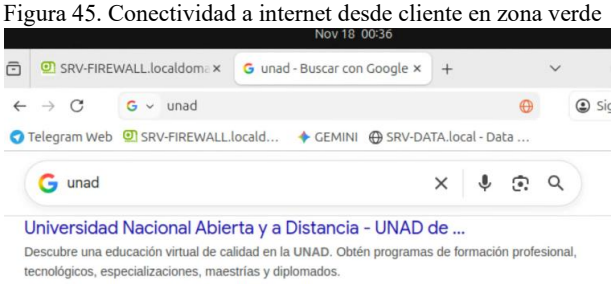
Figura 44. Creación de reglas para comunicar la zona Internet con la zona DMZ



Fuente: Autoría Propia

En cuanto a la conectividad LAN a Wan es importante destacar que, debido a la política de confianza predeterminada de Endian, la Zona VERDE (LAN) mantiene una conectividad inicial a Internet para servicios básicos (DNS, HTTP/S). Esta conectividad se debe a la aplicación automática del NAT de Origen (Masquerading) para el tráfico saliente desde la interfaz VERDE hacia la interfaz ROJA, lo cual es una característica inherente a la configuración de seguridad de la zona de confianza.

Figura 45. Conectividad a internet desde cliente en zona verde



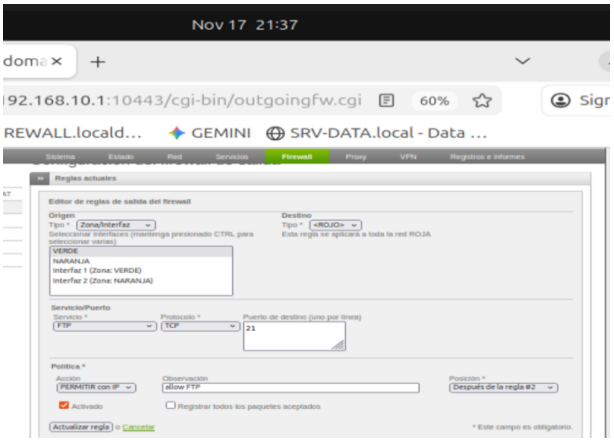
Fuente: Autoría Propia

5.2 INGRESO DEL SERVICIO FTP DESDE LAN HACIA WAN Y DE WAN HACIA LA ZONA DMZ

5.2.1 CONEXIÓN FTP LAN A WAN

Esta directiva verifica la conectividad de salida por FTP desde la zona de alta confianza (VERDE) hacia la red externa (WAN). Esta regla cumple con el requisito para la transferencia de archivos.

Figura 46. Creación regla en tráfico de salida del servicio FTP desde la LAN hacia la WAN



Fuente: Autoría Propia

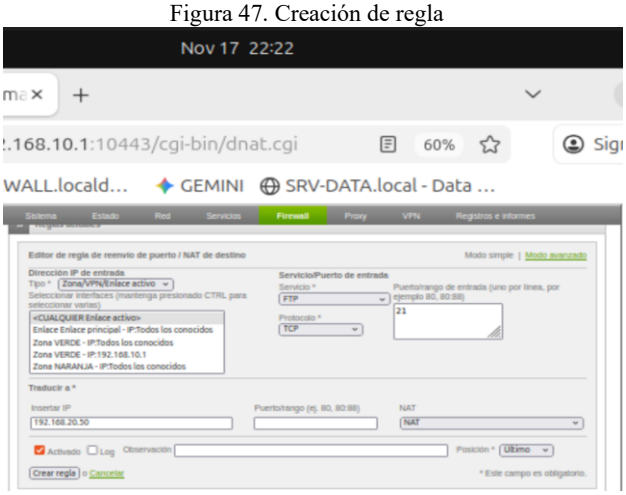
5.2.2 CONEXIÓN FTP WAN HACIA LA ZONA DMZ

Para permitir el acceso externo al servidor FTP alojado en la Zona Naranja (DMZ), se implementó una regla de Traducción de Direcciones de Red de Destino (NAT de Destino), también conocida como Port Forwarding.

Implementación: La regla redirige el tráfico entrante al puerto FTP (TCP/21) que llega a la interfaz de la Zona Roja (WAN) hacia la dirección IP privada del servidor en la DMZ (192.168.20.50).

Esta configuración es fundamental ya que el firewall actúa como un proxy de conexión, traduciendo la dirección pública a la dirección privada y asegurando que los usuarios de Internet puedan acceder al servicio sin conocer la topología interna de la red. [4]

Figura 47. Creación de regla



Fuente: Autoría Propia

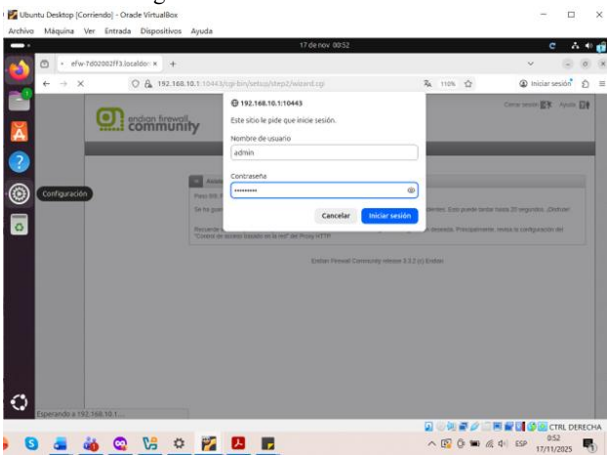
6 DESARROLLO TEMÁTICA 5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

En la temática 5 se pretende crear un perfil y establecer una lista negra para restringir el acceso a los sitios web www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Posteriormente crear un usuario y vincularlo a un grupo, establecer una política de acceso y asociar el perfil creado y relacionarlo con la política de autenticación. Por último, realizar pruebas desde la LAN por medio de un navegador web, probando el acceso a los sitios bloqueados.

6.1 INGRESO A LA INTERFAZ WEB ENDIAN

Se ingresa a la interfaz web de Endian escribiendo en el navegador la URL https://192.168.10.1:10443 y digitando el nombre de usuario y contraseña [2].

Figura 48. Autenticación de usuario

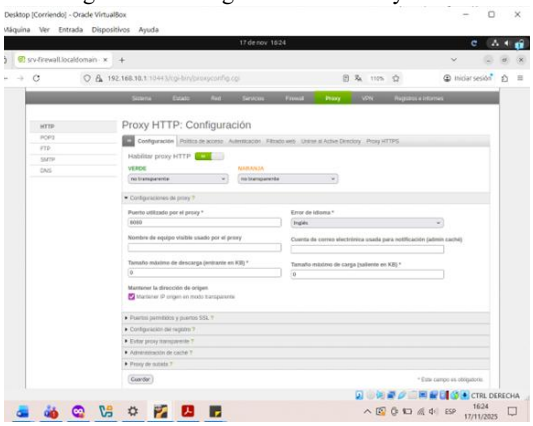


Fuente: Autoría Propia

6.2 CONFIGURACIÓN DEL PROXY HTTP (NO TRANSPARENTE)

En el módulo configuración se habilita el servicio de proxy HTTP, para que permita las solicitudes de HTTP y se deja la configuración por defecto en las zonas verde y naranja la opción no transparente y en el puerto utilizado por el proxy 8080 [2].

Figura 49. Configuración del Proxy HTTP

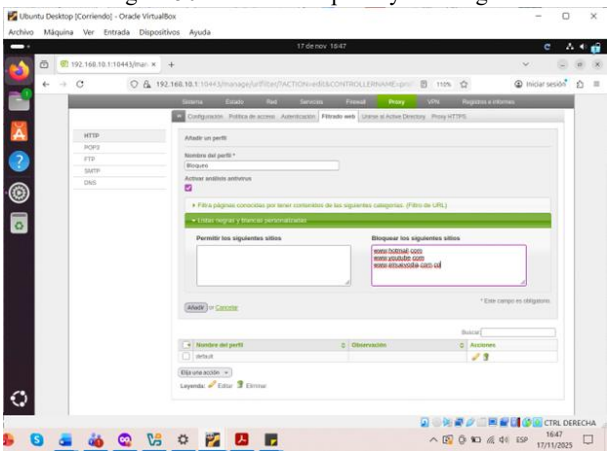


Fuente: Autoría Propia

6.3 CREACIÓN DE PERFIL Y LISTA NEGRA

En el módulo filtrado web, se crea un perfil asignándole el nombre Bloqueo y en la sección de listas negras y blancas personalizadas se ingresan las URL de los sitios que se requieren bloquear, los cuales son: www.hotmail.com, www.youtube.com y el www.elnuevodia.com.co [2].

Figura 50. Creación de perfil y lista negra

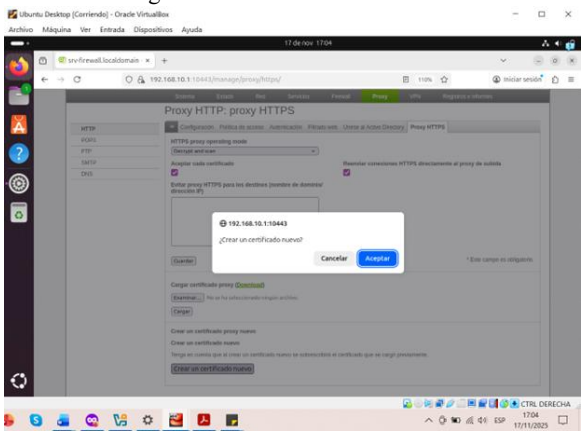


Fuente: Autoría Propia

6.4 GENERACIÓN DE CERTIFICADO PARA EL PROTOCOLO HTTPS

Teniendo en cuenta que las páginas que se desean bloquear se conectan mediante el protocolo https, se debe generar un certificado desde el módulo proxy HTTPS y cargarlo al navegador por medio de los ajustes de este.

Figura 51. Creación de certificado



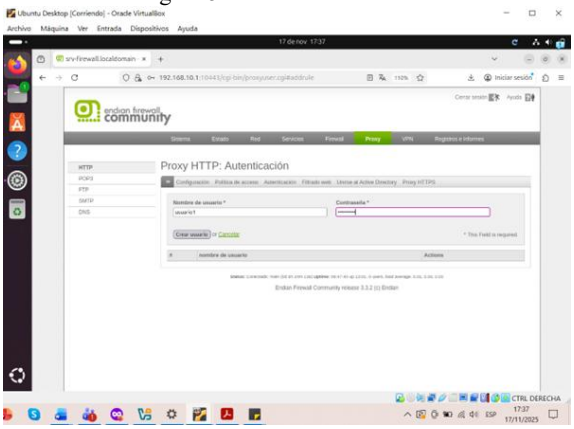
Fuente: Autoría Propia

6.5 AUTENTICACIÓN POR USUARIO

6.5.1 CREACIÓN DE USUARIO

Se crea un usuario en el módulo de autenticación, asignando usuario1 como nombre de usuario y una contraseña [2].

Figura 52. Creación de usuario

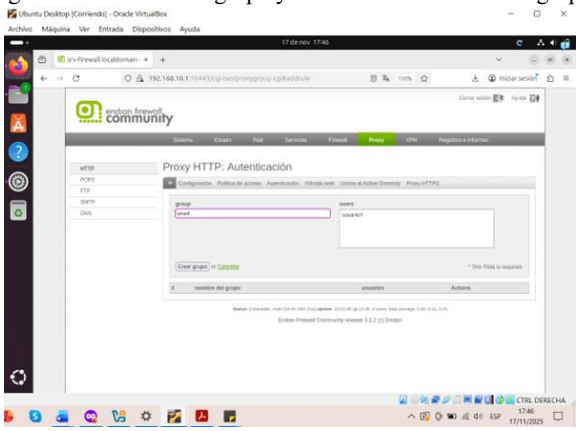


Fuente: Autoría Propia

6.5.2 CREACIÓN DE GRUPO Y ASOCIACIÓN DEL USUARIO AL GRUPO

En el mismo módulo de autenticación, se crea un grupo asignándole el nombre unad y se vincula a ese grupo el usuario creado anteriormente correspondiente a usuario1 [2].

Figura 53. Creación de grupo y asociación del usuario al grupo

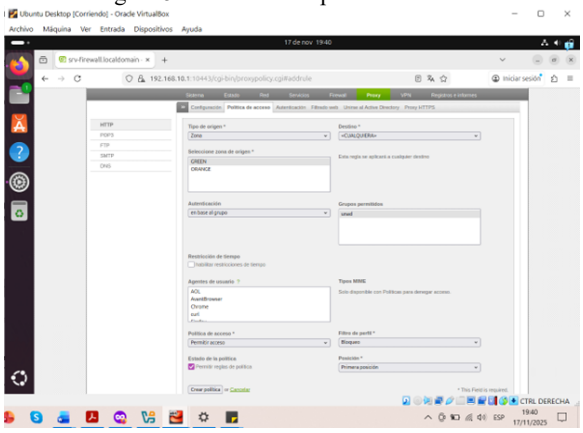


Fuente: Autoría Propia

6.5.3 POLÍTICA DE ACCESO

Se configura una política de acceso en el módulo denominado política de acceso, estableciendo los siguientes parámetros: el tipo de origen en zona; la zona de origen en green, correspondiente a la zona verde; la autenticación en base al grupo, porque se creó un usuario que se asoció a un grupo; en los grupos permitidos se selecciona el grupo que se creó llamado unad; en política de acceso debe seleccionarse permitir acceso; en filtro de perfil debe ir el filtro que se creó, el cual se denomina Bloqueo [2].

Figura 54. Creación de política de acceso

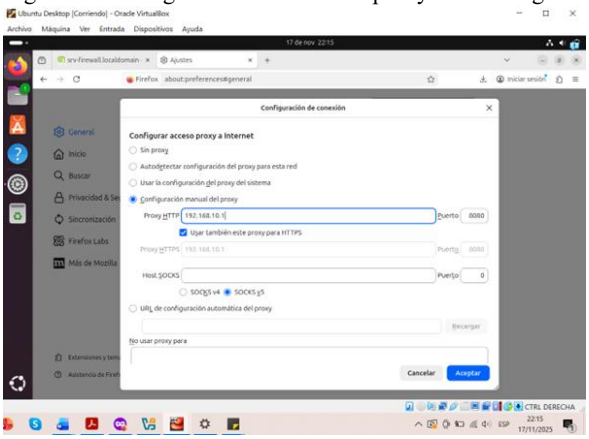


Fuente: Autoría Propia

6.6 CONFIRUACIÓN DEL SERVIDOR PROXY EN EL NAVEGADOR

Se configura el servidor proxy del navegador para que se bloqueen los sitios, seleccionando configuración manual del proxy, ingresando la dirección IP 192.168.10.1 que se asignó al servidor proxy para el tráfico HTTP, el puerto utilizado por el proxy que es 8080 y activando la opción usar también este proxy para HTTPS [2].

Figura 55. Configuración del servidor proxy en el navegador



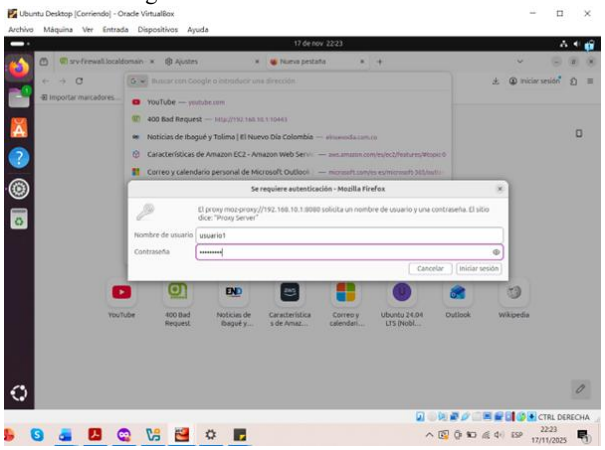
Fuente: Autoría Propia

6.7 COMPROBACIÓN DE FUNCIONAMIENTO

6.7.1 SOLICITUD DE AUTENTICACIÓN

Al ubicarse en la barra de direcciones para ingresar a un sitio, el navegador solicita autenticación y se ingresa el nombre de usuario y contraseña que se configuraron.

Figura 56. Solicitud de autenticación

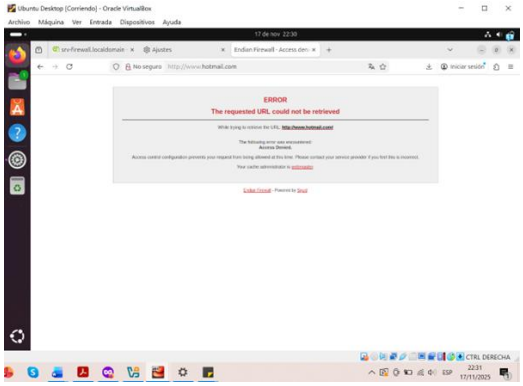


Fuente: Autoría Propia

6.7.2 BLOQUEO DE ACCESO AL SITIO DE HOTMAIL

Al intentar ingresar a la página web www.hotmail.com, aparece un mensaje de acceso denegado, lo cual indica que no se puede acceder al sitio.

Figura 57. Acceso denegado al sitio de Hotmail

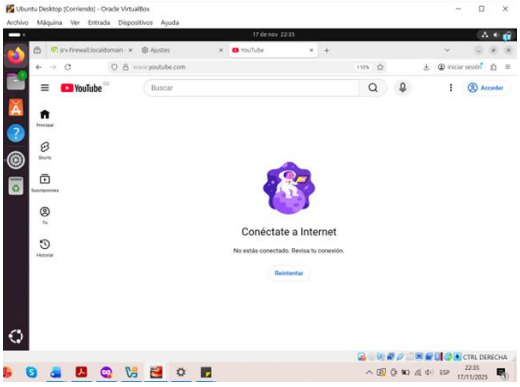


Fuente: Autoría Propia

6.7.3 BLOQUEO DE ACCESO AL SITIO DE YOUTUBE

Al intentar ingresar a la página web www.youtube.com, aparece un mensaje que indica conéctate a internet, por lo cual no permite acceder al sitio.

Figura 58. Acceso denegado al sitio de YouTube

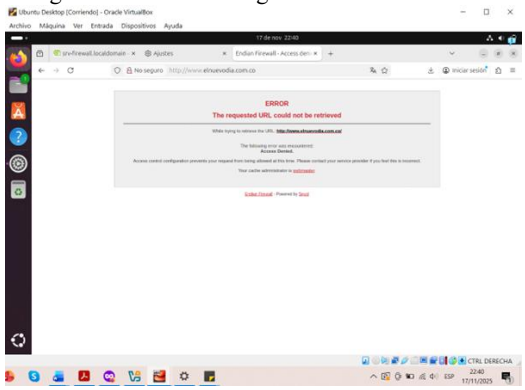


Fuente: Autoría Propia

6.7.4 BLOQUEO DE ACCESO AL SITIO EL NUEVO DÍA

Al intentar ingresar a la página web www.elnuevodia.com.co, aparece un mensaje de acceso denegado, por lo cual no se puede acceder al sitio.

Figura 59. Acceso denegado al sitio el nuevo día



Fuente: Autoría Propia

7 RESULTADOS

La implementación de Endian Firewall en un entorno virtualizado con VirtualBox, como parte de los resultados de la temática 1, permitió comprobar la correcta segmentación de la red en tres zonas diferenciadas: Verde (LAN), Naranja (DMZ) y Roja (WAN). Los resultados obtenidos evidencian que la configuración de los adaptadores de red y la instalación del sistema operativo se realizaron de manera efectiva, garantizando la comunicación controlada entre los distintos segmentos.

Los resultados en la temática 2 mostraron que la segmentación de red en las zonas Verde, Naranja y Roja funcionó correctamente. Las pruebas de conectividad confirmaron que tanto la LAN como la DMZ lograron salida a Internet mediante las reglas SNAT configuradas. Además, la regla DNAT permitió publicar el servicio web alojado en la DMZ, verificándose su acceso desde un equipo externo en la WAN. Todas las pruebas realizadas (ping, curl y acceso HTTP) validaron que las reglas de traducción de direcciones operaron de forma estable y sin errores.

Como resultado la temática 3 tenemos que a implementación de reglas de seguridad perimetral para la Zona Desmilitarizada (DMZ) en Endian Firewall (EFW) fue exitosa. La política de **Denegación (DROP) de ICMP** se validó con una pérdida del 100% de los paquetes en las pruebas de `ping`, asegurando la protección contra el escaneo de red básico. Simultáneamente, las políticas de **Permiso (ACCEPT)** para los servicios esenciales se confirmaron operativas. La conexión al servidor web en la DMZ, mediante el puerto 80, retornó un código **HTTP OK**, y la prueba de acceso al puerto 21 para FTP se estableció sin inconvenientes. Esto demuestra un control de tráfico eficiente, priorizando la seguridad sin comprometer la disponibilidad de servicios necesarios en la DMZ.

La implementación de la Temática 4 culminó con la correcta aplicación de políticas de seguridad basadas en el principio de mínimo privilegio. Se logró establecer una segmentación estricta entre la Zona Verde (LAN) y la Zona Naranja (DMZ), permitiendo únicamente los flujos esenciales (HTTP/FTP). Mediante la configuración de NAT de Destino (Port Forwarding), se expusieron los servicios de la DMZ a la WAN de manera controlada, validando así la función del Endian

Firewall como un perímetro de seguridad eficaz para garantizar la accesibilidad externa con protección interna.

La temática 5 consistió en implementar un sistema de control de acceso a internet por medio de un Proxy HTTP no transparente en Endian Firewall, con el objetivo de establecer políticas de filtrado, autenticación de usuarios y aplicación de restricciones de navegación según perfiles. Además, se realizaron pruebas que demostraron el funcionamiento adecuado del servicio de autenticación, la eficacia del filtrado basado en perfiles y un registro detallado que se lleva de cada solicitud HTTP en los logs del sistema.

8 DISCUSIÓN

Los resultados de la temática 1 demuestran que la virtualización con VirtualBox es una estrategia viable para implementar y probar soluciones de seguridad perimetral sin necesidad de infraestructura física dedicada. La segmentación en zonas permitió simular un entorno corporativo real, donde la LAN representa los usuarios internos, la DMZ los servicios expuestos y la WAN la conexión hacia Internet.

El desarrollo de la temática 2 permitió evidenciar la importancia de una correcta segmentación de red y del uso adecuado de reglas NAT dentro de un firewall. El ejercicio mostró que, al organizar el tráfico por zonas y aplicar políticas claras, la administración de la red se vuelve más controlada y segura. Aunque durante el proceso fue necesario ajustar interfaces y validar la conectividad, estas acciones reforzaron la comprensión del funcionamiento del firewall y la relevancia de una configuración precisa para evitar fallos y riesgos en la infraestructura.

La implementación demostró la exitosa segmentación de la red, el uso de NAT de Destino cumplió el objetivo de exponer servicios HTTP y FTP de la DMZ a la WAN de forma controlada, de esa forma se garantizó el ingreso externo, así como la configuración de reglas para comunicación a nivel de LAN y DMZ.

Al implementar el Proxy HTTP no transparente con autenticación y listas de control de acceso (ACL) en Endian Firewall, se evidenció lo esencial de utilizar mecanismos avanzados de filtrado. Esto es clave para gestionar correctamente la navegación de los usuarios en una red LAN.

9 CONCLUSIONES.

En la temática 1, se implementó la infraestructura virtualizada con segmentación de red en tres zonas establece la base para la aplicación de políticas de seguridad avanzadas, permitiendo el control granular del tráfico entre zonas y hacia Internet. Esta configuración sigue las mejores prácticas recomendadas por Endian (2016) para entornos de seguridad perimetral, garantizando la separación lógica entre redes de confianza, zonas desmilitarizadas y conexiones externas.

En la temática 2, la configuración NAT implementada en Endian permitió que tanto la LAN como la DMZ accedieran a Internet sin exponer sus direcciones privadas, y que un servicio interno pudiera publicarse de forma controlada mediante DNAT. Las pruebas realizadas (ping, curl, verificación de tablas iptables y logs) confirmaron la correcta operación de las reglas. Se recomienda auditar periódicamente las reglas publicadas y limitar el reenvío de puertos solo a los servicios estrictamente necesarios.

La temática 3 validó la implementación de una seguridad perimetral efectiva. Se logró establecer un control de tráfico granular en Endian Firewall.

La regla DROP para el protocolo ICMP fue verificada, bloqueando el comando ping y mitigando el escaneo de red, lo cual fortalece la postura de seguridad. Paralelamente, las reglas ACCEPT específicas garantizaron la disponibilidad de los servicios esenciales: HTTP (puerto 80) y FTP (puerto 21) se mantuvieron accesibles desde la red interna.

En síntesis, se cumplió el equilibrio requerido, demostrando la capacidad del firewall para denegar protocolos de bajo nivel sin comprometer la operatividad de los servicios expuestos en la DMZ.

La implementación de la temática 4 demostró correctamente la aplicación de mínimo privilegio y la segmentación estricta de Endian Firewall garantizando accesibilidad bidireccional de forma controlada entre zonas y salida a la WAN mediante directivas clave para el ingreso externo e interno a los servicios HTTP/FTP del servidor en la zona Naranja, se implementaron reglas de tráfico de salida para el permiso de navegación desde DMZ.

Una correcta configuración y manejo de la solución de seguridad perimetral que ofrece Endian Firewall, protege de manera efectiva los recursos internos, gestiona el tráfico externo y evita ataques y accesos no autorizados, garantizando así la integridad, confidencialidad y disponibilidad de los datos y servicios críticos en la red.

10 REFERENCIAS

[1] Canonical, «Help ubuntu,» Canonical, 2023. [En línea]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html. [Último acceso: 11 2025].

[2] Endian, «Endian Documentation,» Endian, 2016. [En línea]. Available: http://docs.endian.com/3.2/utm/index.html. [Último acceso: 11 2025].

[3] J,LaCroix, «Mastering Ubuntu Server», *Packt Publishing*, 2020. [En línea]. Available: https://international.scholarvox.com/book/88908267#. [Último acceso: 11 2025].

[4] L. P. I. (LPI), «LPI Learning,» LPI, 2022. [En línea]. Available: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/. [Último acceso: 2025].

[5] Oracle, «VirtualBox,» Oracle Corporation, 2020. [En línea]. Available: https://www.virtualbox.org/manual/. [Último acceso: 11 2025].