IMPLEMENTACIÓN Y CONFIGURACIÓN DE UN FIREWALL CON ENDIAN EN ENTORNOS VIRTUALES: NAT, DMZ, POLÍTICAS DE ACCESO Y PROXY HTTP

Ospinal Burbano, Mariana
e-mail: mospinalb@unadvirtual.edu.co
Salazar Morales, Diego Fernando
e-mail: dfsalazarmo@unadvirtual.edu.co
Londoño Escobar, Angie Paola
e-mail: aplondonoe@unadvirtual.edu.co
Gómez Holguín, Luisa María
e-mail: lmgomezhol@unadvirtual.edu.co
Giraldo Marín, Carlos Andrés
e-mail: cagiraldomo@unadvirtual.edu.co

RESUMEN: *En este artículo se describe el proceso de implementación de una infraestructura de seguridad perimetral utilizando la distribución GNU/Linux Endian Firewall (EFW) como solución central. El enfoque del proyecto se basó en la extensión de una red segmentada en zonas LAN, WAN y DMZ, cuyo objetivo es asegurar el acceso y la protección de los servicios críticos de la empresa. Se desarrollaron temáticas orientadas a la instalación y configuración de EFW, definición de reglas NAT, habilitación controlada de servicios en la DMZ, creación de políticas de acceso entre zonas y el establecimiento de un proxy HTTP con autenticación y restricciones de navegación. Cada solución fue desarrollada por medio de pruebas funcionales y comandos administrativos que permitieron validar la conectividad, seguridad y eficiencia del entorno. Este documento es el resultado de la configuración de interfaces de usuario y escritorio por medio de tareas administrativas que optimizan el sistema GNU/Linux.*

PALABRAS CLAVE: Autenticación proxy, Endian Firewall, DMZ, reglas de acceso.

1 INTRODUCCIÓN

En la actualidad la evolución constante de las amenazas cibernéticas obliga a las empresas a implementar estrategias sólidas de seguridad perimetral, las cuales contribuyen a la protección de sus infraestructuras tecnológicas. Asegurar las redes internas (LAN) y aislar los servicios críticos expuestos mediante una Zona Desmilitarizada (DMZ) se ha convertido en una práctica esencial para preservar la integridad, disponibilidad y confiabilidad de los datos empresariales. En este contexto, las soluciones basadas en sistemas GNU/Linux, como Endian Firewall (EFW), resultan ser una alternativa eficaz y versátil para gestionar Firewalls avanzados y controlar el tráfico de red.

Esta actividad propone la implementación y configuración de una solución de seguridad perimetral integral, en la cual se emplea la distribución GNU/Linux Endian Firewall. Por medio del enfoque práctico y colaborativo de esta actividad, se abordaron desafíos técnicos específicos relacionados con la segmentación de red, configurando las zonas por medio de colores (Zona Verde (LAN), Zona Naranja (DMZ), Zona Roja (WAN - Extranet), la configuración de reglas NAT, el control de acceso entre zonas y la implementación de un proxy HTTP con autenticación y filtrado de contenido. La infraestructura de la solución fue virtualizada en el entorno de Oracle VirtualBox, en la cual se crearon máquinas virtuales bajo las distribuciones de GNU/Linux como un servidor web en la DMZ, una desktop en la LAN y un Firewall como punto de control central. Permitiendo de esta manera, la experimentación y verificación de diferentes configuraciones de seguridad.

Los resultados obtenidos en esta implementación demuestran la efectividad de Endian Firewall en la creación de una arquitectura de red segura, segmentada, controlada y eficiente. La configuración de NAT facilitó dicha comunicación controlada entre las diferentes zonas de la red y la Internet simulada. Las reglas de acceso implementadas permitieron una precisión en el control del tráfico permitido o denegado entre la LAN, la DMZ y la WAN. Adicionalmente, la implementación de un proxy HTTP con autenticación y listas negras proporcionó una capa adicional de seguridad y control sobre la navegación web desde la red interna.

Esta experiencia aporta conocimientos sobre seguridad de redes al plantear un caso de estudio práctico de implementación de una solución de seguridad perimetral robusta, empleando GNU/Linux Endian Firewall como distribución especializada en el tema. Las configuraciones y pruebas realizadas brindan información valiosa para los estudiantes y profesionales interesados en el aprendizaje y aplicación de la protección de infraestructuras de red basadas en software libre.

A continuación, se detalla la arquitectura implementada, los procedimientos que se realizaron en cada temática y los resultados alcanzados para este caso de estudio.

2 INSTALACIÓN ENDIAN FIREWALL

Para iniciar con el desarrollo de las temáticas, se descargó la distribución de Endian Firewall Community de la página oficial https://www.endian.com/en/community/. Previo a esto, se instaló en la plataforma VirtualBox, la cual simula

computadores dentro de los diversos sistemas operativos por medio de la creación y ejecución de máquinas virtuales.

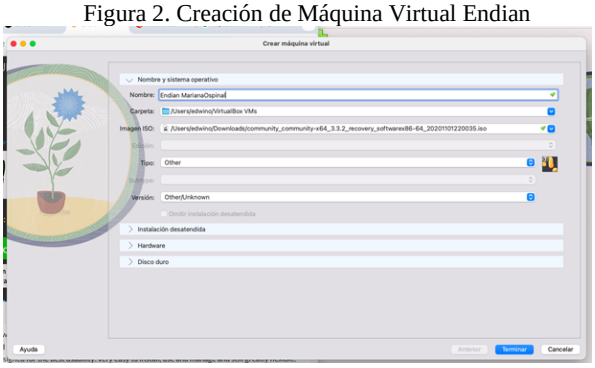
Endian es una distribución de OpenSource de Linux, el cual actúa como corta fuego o Firewall en esta actividad. Este Firewall protege y filtra cualquier servidor [1].

Figura 1. Descarga de Endian Firewall

Fuente: Autoría propia

Una vez se descargó Endian, se creó la máquina virtual y en la opción de "imagen ISO" se agregó la ISO descargada.

Figura 2. Creación de Máquina Virtual Endian

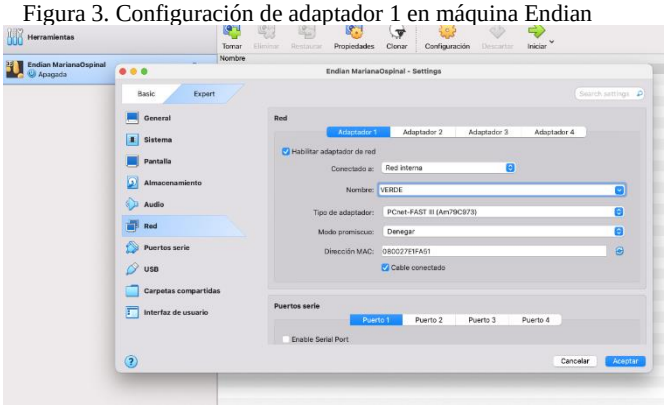


Fuente: Autoría propia

Luego se configuró las tarjetas de red de la siguiente manera:

Adaptador 1 > verde > red interna
Adaptador 2 > Naranja > red interna
Adaptador 3 > Puente (LAN) – salida a internet

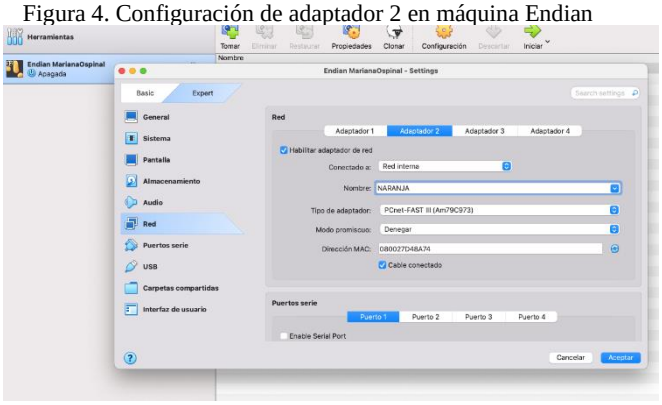
Figura 3. Configuración de adaptador 1 en máquina Endian



Fuente: Autoría propia

La primera configuración para el ENDIAN FIREWALL, es el adaptador 1 que corresponde a la Zona Verde.

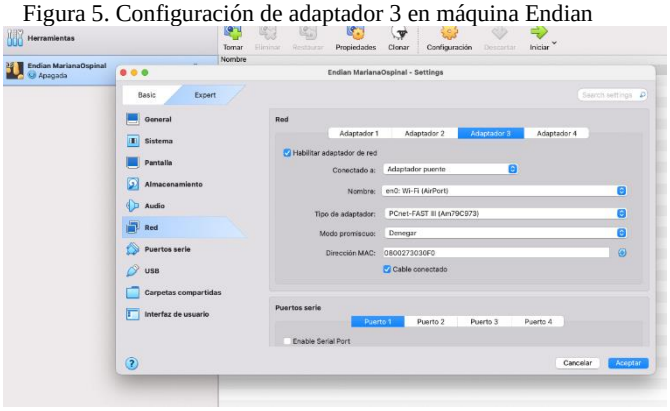
Figura 4. Configuración de adaptador 2 en máquina Endian



Fuente: Autoría propia

Adaptador 2 en ENDIAN FIREWALL, que corresponde a la zona naranja.

Figura 5. Configuración de adaptador 3 en máquina Endian



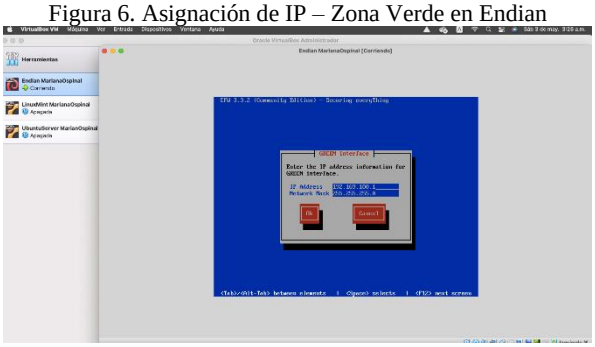
Fuente: Autoría propia

Adaptador 3 en ENDIAN FIREWALL - salida a interne por medio de Adaptador puente.

Después, se ejecuta la máquina virtual booteando desde la ISO, se escogió el idioma y se aceptó la creación de una partición e instalación de un disco. Seguido de esto, el sistema detectó la primera zona (verde), por lo que en este proceso de

instalación el sistema solicitó la ip y máscara de la red verde: 192.169.100.1 – 255.255.255.0.

Figura 6. Asignación de IP – Zona Verde en Endian



Fuente: Autoría propia

Luego de realizar y aceptar todos los cambios, se evidencia la correcta instalación de Endian donde muestra información de la Zona Verde, como la IP y el puerto de conexión.

Realizado esto, se seleccionó la opción 0 del menú (Figura 7) para acceder al Shell en la máquina Endian. Se inició sesión utilizando la contraseña predeterminada, que es endian. A continuación, el sistema informó que Endian había asignado automáticamente una dirección IP a la zona roja mediante DHCP. Esto ocurrió porque en la configuración del adaptador 3 de la máquina Endian Firewall se seleccionó el modo Adaptador puente, lo que indica al sistema que debe obtener una dirección IP pública de forma automática a través de DHCP. Esta configuración permite optimizar la conectividad a Internet, ya que facilita que múltiples dispositivos internos puedan acceder a la red externa compartiendo una única dirección IP asignada por el proveedor de servicios.

Las configuraciones siguientes del Endian se realizaron en una máquina con Linux Mint.

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

Objetivo: Se detalla el proceso de implementación y configuración de la distribución GNU/Linux Endian para segmentar la red en zonas segura (verde), pública (roja) y de servidores (naranja). La función principal de este Firewall es proteger y filtrar los servidores [1].

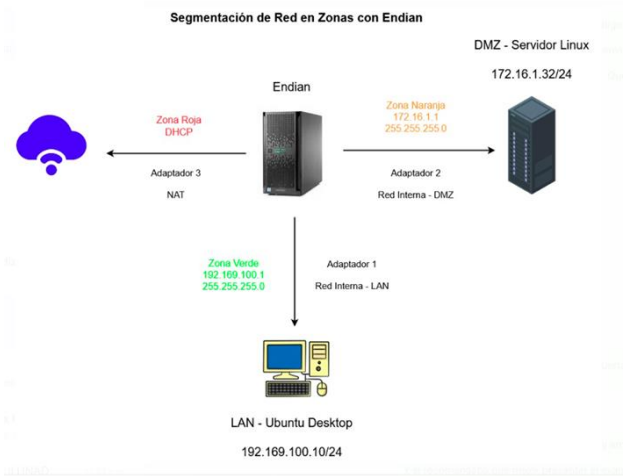
Acción: Crear una máquina virtual, asignar tres tarjetas de red (verde: interna, roja: Puente, naranja: interna separada), instalar Endian configurando cada interfaz en la zona correspondiente

Las Zonas de red son divisiones lógicas de la red que Endian Firewall utilizará para organizar y aplicar políticas de seguridad de forma diferente [5].

3.1 TOPOLOGÍA DE RED SEGMENTADA CON ENDIAN FIREWALL

Para dar inicio al desarrollo de las temáticas se diseñó la topología de segmentación de red para implementarse en cada máquina (desktop - server) y durante la instalación de Endian para que asigne a estas zonas las IP estipuladas en la topología. El objetivo principal de la segmentación de red es mejorar la seguridad y el control de todo el tráfico por medio de la separación de los dispositivos de acuerdo a su nivel de confianza y de la función crítica que tengan.

Figura 8. Topología de Segmentación de red



Fuente: Autoría propia

3.2 INSTALACIÓN Y CONFIGURACIÓN DE TARJETAS DE RED EN DISPOSITIVOS (DESKTOP - SERVER)

Para continuar con el proceso de implementación fue necesario crear las máquinas virtuales que se encontrarían en las redes internas verde (usuarios) y naranja (servidores). Este proceso consta de las siguientes etapas:

- Se crearon las máquinas virtuales para cada componente (escritorio y servidor).
- Se descargó Linux Mint y se instaló como escritorio para la red interna verde.
- Se descargó Ubuntu Server 24.04.2 y se instaló como servidor de la red interna naranja.
- Se asignaron recursos hardware como CPU, RAM, Almacenamiento.

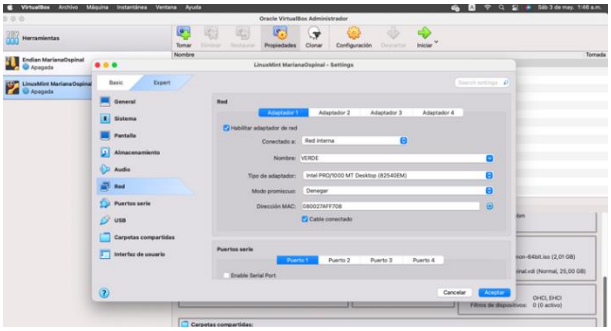
3.3 MÁQUINA VIRTUAL DESKTOP (LINUX MINT – ZONA VERDE / LAN)

Este dispositivo forma parte de la red interna segura (conocida como Zona Verde), conectada al firewall Endian.

La máquina virtual Linux Mint Desktop debe tener una sola tarjeta de red configurada en VirtualBox como "Red Interna" con el nombre VERDE, ya que forma parte de la zona verde de la topología. Dentro del sistema operativo, se le asigna la dirección IP 192.169.100.10 con máscara 255.255.255.0 y

como puerta de enlace la IP 192.169.100.1, que corresponde a la interfaz del Endian Firewall en la zona verde.

Figura 9. Instalación de Linux Mint escritorio en la red interna VERDE



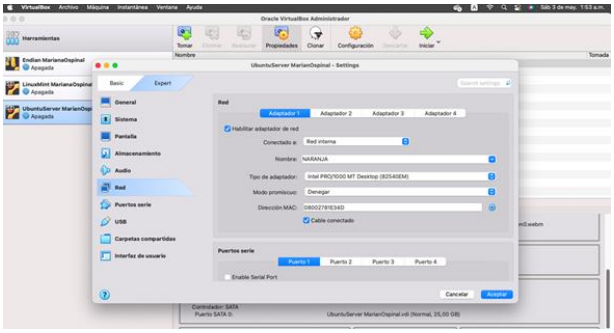
Fuente: Autoría propia

3.4 MÁQUINA VIRTUAL DEL SERVER (UBUNTU SERVER – ZONA NARANJA / DMZ)

Este dispositivo debe ubicarse en la DMZ (zona naranja - semisegura), la cual está conectada a Endian Firewall para ser accesible desde otras zonas bajo su control.

La máquina virtual Ubuntu Server debe tener también una sola tarjeta de red configurada como “Red interna” con el nombre NARANJA, ya que pertenece a la red Desmilitarizada. Para este servidor y de acuerdo a la topología se asigna la dirección IP 172.16.1.32 con máscara 255.255.255.0 y como puerta de enlace la IP 172.16.1.1, la cual corresponde a la interfaz del Endian Firewall en la zona naranja.

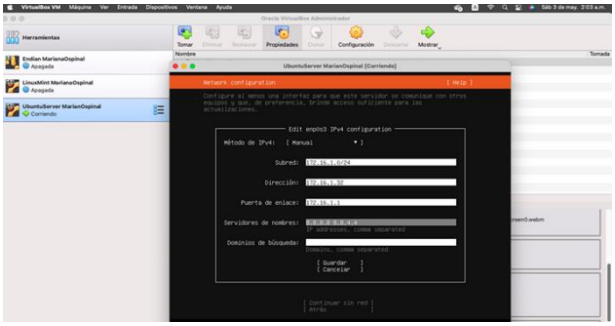
Figura 10. Instalación de Ubuntu Server en la red interna NARANJA



Fuente: Autoría propia

Continuando con el proceso de instalación del sistema operativo en el Ubuntu Server destinado a la zona naranja, se procedió a la configuración manual de la red, para lo cual fue necesario encender la máquina y continuar con ese proceso. En la (figura 11) se aprecia que se estableció una dirección IP estática con base en el esquema de segmentación previamente definido (figura 8). Se configuró la interfaz de red enp0s3 con los siguientes parámetros: dirección IP 172.16.1.32, máscara de subred /24, puerta de enlace 172.16.1.1 (corresponde a la interfaz del Firewall Endian en la zona naranja). Esta configuración garantiza que el servidor este correctamente integrado dentro de la DMZ, logrando una comunicación controlada con otras zonas por medio del Firewall, preparándolo además, para ofrecer servicios accesibles de manera segura a otras redes externas e internas.

Figura 11. Configuración de dirección IP y Gateway en Ubuntu Server



Fuente: Autoría propia

Hasta el momento solamente hay conexión entre la máquina desktop y el Endian Firewall por medio de la puerta de enlace de la zona verde (192.169.100.1). Para lograr comunicación con el Ubuntu Server se continuó con las configuraciones en el Endian pero esta vez desde el navegador de la máquina desktop.

3.5 CONFIGURACIÓN AVANZADA EN EL ENDIAN FIREWALL

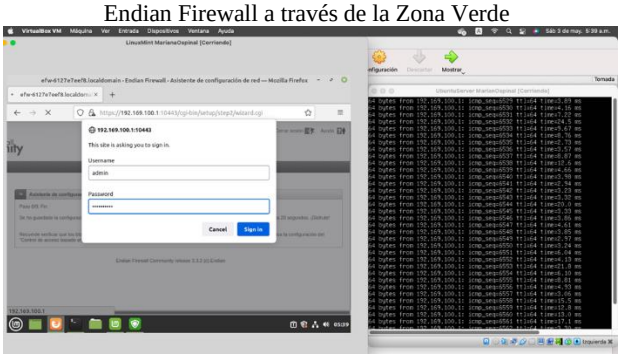
En la máquina desktop se accedió a la interfaz web de Endian Firewal usando la dirección 192.169.100.1 conectada al puerto 10443, en la cual se realizaron los siguientes pasos:

- Al ingresar a la página se eligió la configuración avanzada y se aceptó el riesgo de acceso.
- Se eligió el idioma para continuar con la instalación.
- Se aceptó la licencia de uso GNU.
- Se establecieron nuevas contraseñas para el acceso a la interfaz web (admin) y para el acceso SSH (root).
- El asistente detectó que la zona roja ya estaba configurada automáticamente mediante DHCP.
- Se verificó que tanto la zona verde (LAN) como la zona roja (WAN) estaban activas y funcionales.
- Se habilitó la zona naranja (DMZ) para alojar servidores accesibles desde Internet.
- Se seleccionó el adaptador de red disponible y se configuró la IP de la zona naranja como 172.16.1.1.
- Se asignó un nombre al host del firewall.
- Finalmente, se llegó al paso 8/8 del asistente, donde se aplicaron y guardaron todas las configuraciones realizadas.

3.6 PRUEBAS DE FUNCIONAMIENTO

Esta primera prueba se realizó desde el servidor Linux ubicado en la zona Naranja con el fin de verificar la conectividad hacia la zona verde, específicamente hacia el Firewall Endian, cuya IP en esa red interna es 192.169.100.1. Se pretende confirmar que el servidor tiene comunicación directa con el Firewall, lo cual es primordial para asegurar que la segmentación de red estuviera funcionando correctamente.

Figura 12. Comunicación exitosa entre Ubuntu Server y Endian Firewall a través de la Zona Verde

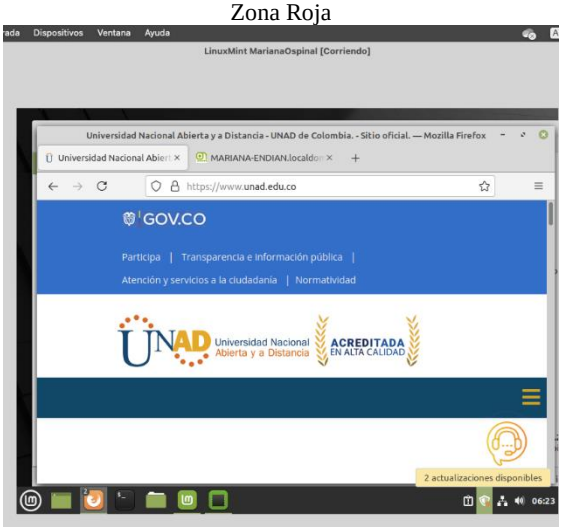


Fuente: Autoría propia

El resultado positivo del ping se refleja en el recibimiento de respuestas constantes que indican que no hay bloqueo en la red.

La siguiente prueba consistió en acceder desde la máquina desktop, ubicada en la zona verde a un sitio web externo mediante un navegador, con el fin de verificar la conexión a Internet. El acceso exitoso confirma que la máquina desktop tiene salida a Internet debido a la correcta configuración del Firewall Endian, que incluye el enrutamiento, NAT y la puerta de enlace.

Figura 13. Comunicación exitosa en Máquina de Zona Verde y Zona Roja



Fuente: Autoría propia

Esto demostró que la Zona Verde estaba operando y que estaba correctamente enlazada con la Zona Roja que es la que proporciona el Internet.

La última prueba se ejecutó en la máquina Desktop por medio del comando ping 192.169.100.**1** que corresponde a la IP de la interfaz verde del Firewall Endian. La respuesta exitosa confirma la conectividad entre la Desktop y el Endian, validando que la red interna esté operando adecuadamente.

4 TEMÁTICA 2: CONFIGURACIÓN NAT

En entornos de red donde se desea permitir la navegación hacia redes externas desde una red privada, la traducción de direcciones de Red (NAT) por sus siglas en inglés, es una técnica esencial. En este caso, se utilizó la plataforma de seguridad Endian Firewall para implementar reglas de NAT y control de tráfico, con el objetivo de facilitar la conectividad desde la red local (LAN) hacia una red externa simulada como Internet (WAN). Esta práctica es especialmente relevante en escenarios de laboratorio, pruebas o entornos corporativos, donde se requiere segmentar el tráfico y aplicar políticas específicas sin comprometer la seguridad de la red interna.

La principal motivación para aplicar NAT en este contexto es la necesidad de enmascarar las direcciones IP privadas de los dispositivos de la LAN, lo que impide su exposición directa a la red pública. De este modo, las solicitudes de salida se identifican con la dirección IP del firewall en la interfaz de salida, en este caso el enlace “Rojo” actuando como puerta de enlace y representante de la red local ante la WAN. Esta práctica garantiza no solo un direccionamiento adecuado, sino también un control eficaz del tráfico mediante las reglas del firewall [9].

4.1 CONFIGURACIÓN EN LA RED LAN

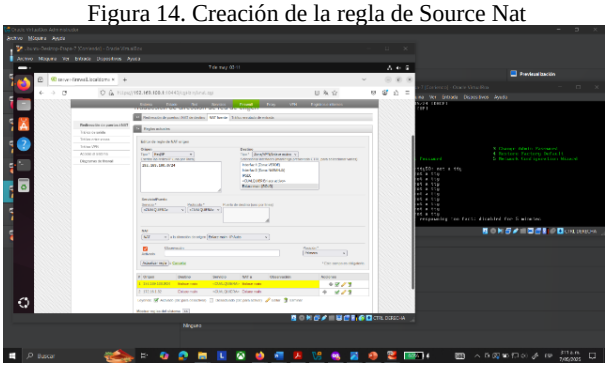
El procedimiento inicial consistió en la creación de una regla de NAT de origen (Source NAT) destinada a ocultar las direcciones IP privadas de la LAN [8]. Esta medida garantiza que las solicitudes de salida utilicen la dirección IP pública del firewall como identificador, habilitando así la navegación hacia el exterior. La configuración se llevó a cabo accediendo al apartado Firewall en la interfaz principal del sistema, seleccionando la opción “Redireccionamiento de puertos / NAT” y posteriormente “NAT de fuente” [12]

El procedimiento se inició accediendo al apartado Firewall de la interfaz de administración web del sistema Endian. Desde allí, se navegó hacia la sección “Redireccionamiento de puertos / NAT” y luego a la subsección “NAT de fuente”, donde fue posible definir una nueva regla que permita traducir las direcciones IP de origen.

En la figura 14 se ilustra la creación de esta regla, con los siguientes parámetros específicos:

- Origen: Red/IP — 192.169.100.0/24 (rango correspondiente a la red LAN).
- Destino: Zona/VPN/Enlace activo — Enlace Main [Rojo].
- Servicio/Puerto: configuración por defecto.
- NAT: Acción NAT — Dirección de origen: Enlace Main – IP.Auto.

Figura 14. Creación de la regla de Source Nat



Fuente: autoría propia

Esta configuración permite que cualquier dispositivo dentro del segmento LAN que intente acceder a recursos externos utilice como dirección fuente la IP pública del enlace Rojo. Tras definir estos parámetros, se seleccionaron las opciones “Crear regla” y “Aplicar” dejando activa la regla de NAT [7].

Una vez habilitada la salida a través de NAT se procedió a comprobar el funcionamiento del control de tráfico saliente, el cual es un componente crítico para gestionar el acceso de dispositivos específicos a la red WAN. Para ello, se diseñó una política de firewall orientada a bloquear el tráfico saliente desde una dirección IP determinada (192.169.100.3) perteneciente a un equipo cliente con Ubuntu Desktop [2].

En la sección Tráfico de salida del módulo Firewall, se creó una nueva regla con los siguientes valores:

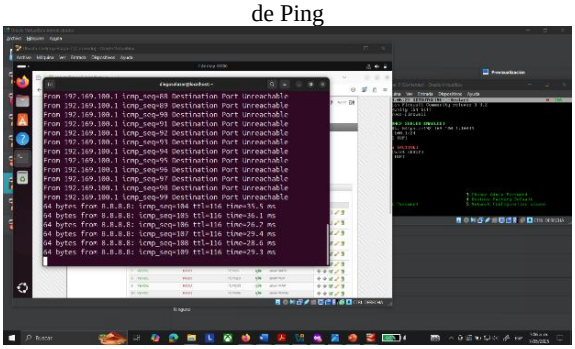
- Origen: Red/IP — 192.169.100.3.
- Destino: Zona Rojo.
- Servicio/Puerto: configuración por defecto.
- Política: Acción Rechazar.
- Observaciones: bloqueo de Internet para el Desktop.
- Posición: Primera en la lista de reglas.

Esta regla se activó utilizando las opciones Añadir regla y Aplicar, priorizándola por encima de cualquier otra configuración existente. De manera que, para validar la efectividad de la regla de bloqueo, se accedió a la terminal del equipo Ubuntu Desktop con dirección IP 192.169.100.3 y se ejecutó el comando: ping 8.8.8.8.

El resultado obtenido fue: From 192.169.100.1 icmp_seq=38 Destination Port Unreachable.

Tal como se muestra en la figura 15, esta respuesta evidencia que el firewall impidió el acceso a Internet desde el equipo bloqueado, confirmando el funcionamiento correcto de la política de denegación.

Figura 15. Verificación de la conectividad mediante pruebas de Ping



Fuente: autoría propia

Posteriormente, se desactivó la regla de bloqueo y se repitió la misma prueba, obteniendo una respuesta positiva: 64 bytes from 8.8.8.8: icmp_seq=134 ttl=116 time=25.6 ms

Este resultado validó que, al eliminar la restricción, se restableció la conectividad lo que demostró que las políticas configuradas son efectivas y reversibles.

Como comprobación adicional se accedió al navegador Firefox desde el mismo equipo bloqueado y se intentó abrir la página principal de Wikipedia. Tras desactivar la regla de bloqueo el acceso a la página fue exitoso y se confirmó que la navegación estaba plenamente habilitada.

4.2 CONFIGURACIÓN EN LA DMZ

Una vez verificada la correcta implementación de la NAT de origen y las políticas de control de tráfico saliente para permitir o restringir el acceso desde la red LAN hacia la red WAN se procedió a replicar un proceso similar en la zona DMZ. Esta etapa fue fundamental para extender las capacidades de seguridad y gestión del tráfico permitiendo controlar de manera precisa las comunicaciones entre dispositivos ubicados en segmentos expuestos de la red y la Internet pública [3].

Para establecer y gestionar la conectividad entre la zona desmilitarizada (DMZ) y la red pública (Internet) se procedió a la implementación de reglas de Traducción de Direcciones de Red (NAT) de tipo origen junto con políticas específicas de control de tráfico saliente utilizando el sistema de gestión de seguridad de red proporcionado por Endian Firewall. Estas acciones permiten mantener un nivel adecuado de protección en una zona crítica, comúnmente utilizada para alojar servicios que deben ser accesibles tanto desde redes internas como externas, sin comprometer la seguridad del resto de la infraestructura.

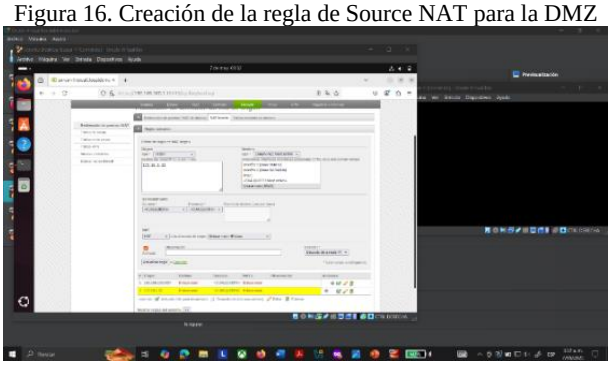
La configuración de la NAT tuvo como finalidad principal ocultar la dirección IP privada del dispositivo ubicado en la DMZ, de modo que todas las solicitudes de salida hacia la red WAN se presenten utilizando la IP pública del enlace identificado como “Rojo”. Esta técnica de enmascaramiento no solo permite cumplir con los requisitos de direccionamiento y enrutamiento a través de Internet, sino que también constituye una medida esencial para reducir la exposición directa de dispositivos internos a amenazas externas.

En la figura 16 se muerta el proceso de configuración que se realizó accediendo al apartado “Firewall” dentro del panel de

administración de Endian. Desde la sección "Redireccionamiento de puertos / NAT", se ingresó al módulo de "NAT de fuente", donde se añadió una nueva regla utilizando los siguientes parámetros:

- Origen: Tipo Red/IP — Dirección: 172.16.1.32 (dispositivo ubicado en la DMZ).
- Destino: Tipo Zona/VPN/Enlace activo — Interfaz: Enlace Main [Rojo].
- Servicio/Puerto: Configuración predeterminada.
- NAT: Acción: NAT — Dirección de origen: Enlace Main – IP.Auto.

Figura 16. Creación de la regla de Source NAT para la DMZ



Fuente: autoría propia

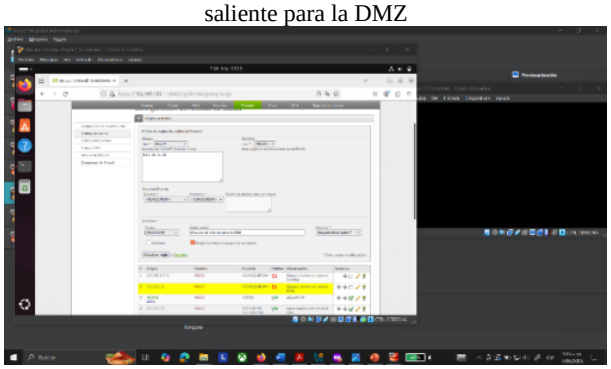
Una vez completada la configuración, se seleccionaron las opciones "Crear regla" y "Aplicar", quedando la regla activa y lista para su funcionamiento.

Adicionalmente, con el objetivo de validar la capacidad del sistema para gestionar el tráfico saliente desde la DMZ se definió una política específica de firewall orientada al bloqueo temporal de acceso a Internet para la dirección IP 172.16.1.32. Esta regla fue creada dentro de la sección "Tráfico de salida" y se configuró con los siguientes valores:

- Origen: Red/IP — Dirección: 172.16.1.32.
- Destino: Zona: Rojo.
- Servicio/Puerto: Configuración por defecto.
- Política: Acción: Rechazar.
- Observaciones: "Bloqueo de Internet para la DMZ".
- Posición: Después de la regla 1.

Como se puede ver en la figura 17.

Figura 17. Configuración de la regla de bloqueo de tráfico saliente para la DMZ



Fuente: autoría propia

La política fue incorporada al conjunto de reglas activas mediante las opciones "Añadir regla" y "Aplicar".

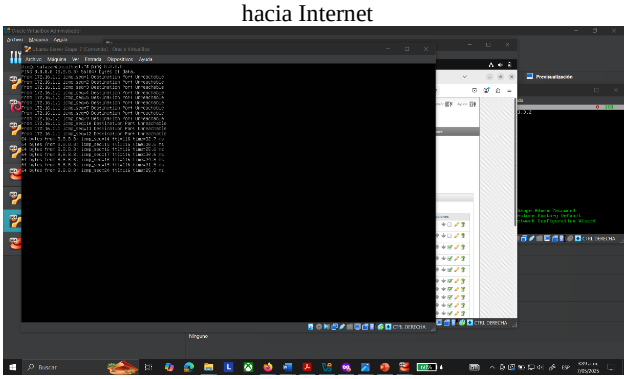
Para comprobar el correcto funcionamiento de la configuración se accedió a la terminal de un equipo ubicado dentro de la zona DMZ y se ejecutó el comando ping dirigido a la dirección IP 8.8.8.8 (servidor DNS público de Google). En la prueba inicial, con la regla de bloqueo activa, no se recibió respuesta alguna lo que confirmó que la salida hacia Internet se encontraba restringida. Posteriormente, al desactivar la regla de firewall, se repitió la prueba obteniendo la siguiente respuesta:

4 bytes from 8.8.8.8: icmp_seq=212 ttl=116 time=23.4 ms

Este resultado evidenció que al levantar la restricción de tráfico la comunicación entre la zona DMZ e Internet se restableció de manera efectiva. Por tanto, se concluye que tanto la regla de NAT de origen como la política de control de tráfico saliente cumplen adecuadamente con su función garantizando conectividad y seguridad bajo las condiciones definidas por el administrador del sistema.

Lo anterior se puede evidenciar en la figura 18.

Figura 18. Verificación de conectividad desde la Zona DMZ hacia Internet



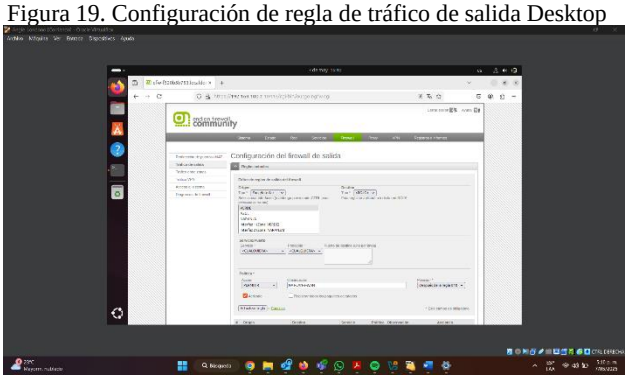
Fuente: autoría propia

5 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

Regla de NAT de salida (Masquerading):

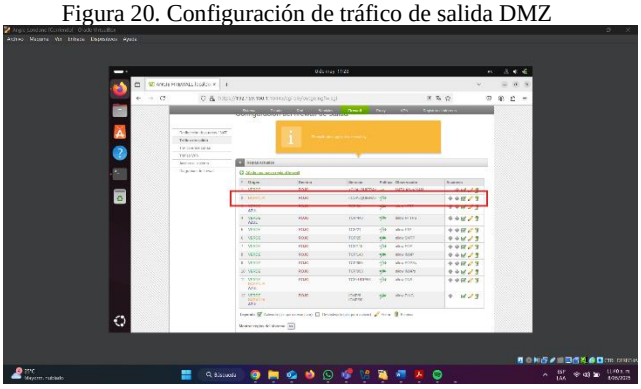
- Objetivo: Permitir la salida a Internet de los dispositivos en la zona Verde (LAN) y en la zona Naranja (DMZ).
- Acción: Traducción de direcciones privadas a la dirección pública asignada en la zona Roja (WAN)[11].

Figura 19. Configuración de regla de tráfico de salida Desktop



Fuente: Autoría propia

Figura 20. Configuración de tráfico de salida DMZ

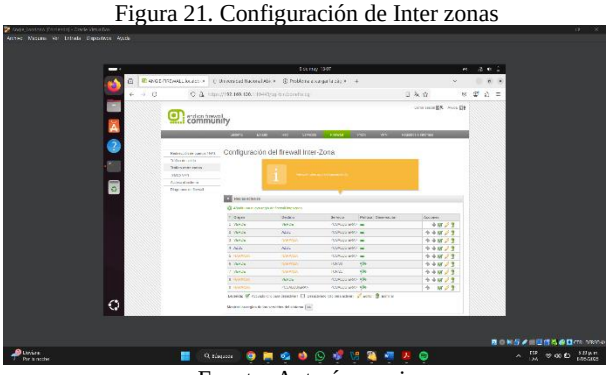


Fuente: Autoría propia

Regla de tráfico entre zonas (Green → Red):

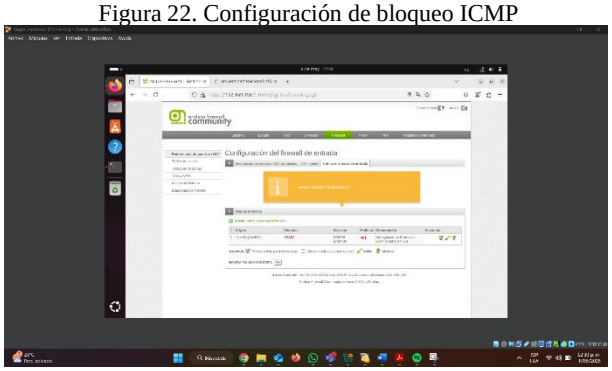
- Objetivo: Permitir la navegación web desde los equipos cliente en la LAN.
- Protocolos: HTTP, HTTPS, DNS y otros requeridos [4][10].
- Acción: Aceptar.

Figura 21. Configuración de Inter zonas



Fuente: Autoría propia

Figura 22. Configuración de bloqueo ICMP

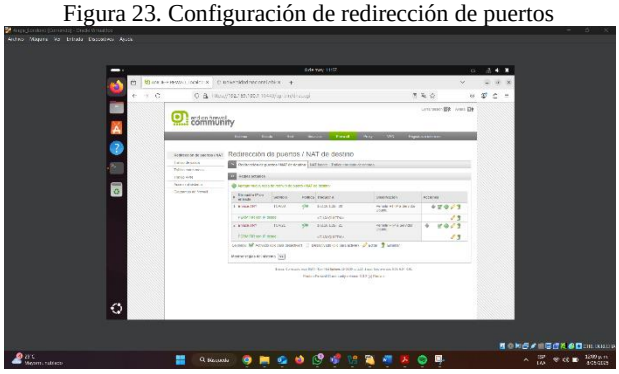


Fuente: Autoría propia

5.1 SERVICIOS HTTP Y FTP

En un servidor Ubuntu Server, se instalaron los paquetes apache2 para habilitar un servidor web y vsftpd para ofrecer servicios de transferencia de archivos. Posteriormente, se crearon reglas de redirección de puertos (Destination NAT) en Endian Firewall que permiten que las solicitudes externas recibidas por los puertos 80 (HTTP) y 21 (FTP) en la interfaz Red (WAN) sean redirigidas al servidor interno en la DMZ. Además, se establecieron reglas de firewall para permitir el acceso a dichos servicios desde la zona Green (LAN), garantizando el aislamiento y control de tráfico entre zonas según buenas prácticas de seguridad perimetral[6][10][11].

Figura 23. Configuración de redirección de puertos



Fuente: Autoría propia

6 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

6.1 CONFIGURACIÓN DE ZONAS DE RED

Basándose en la configuración definida en la Temática 1, se establecieron las siguientes zonas de red, gestionadas mediante el firewall Endian:

- Zona Verde (LAN): Administrada por el firewall. Contiene los equipos de los usuarios internos.
- Zona Naranja (Servidor): Reservada para servicios internos de uso público.
- Zona DMZ (zona desmilitarizada): Aloja servicios que pueden ser accedidos desde el exterior de la red.

- Zona WAN (Internet): Canal de comunicación con Internet.

6.2 CONFIGURACIÓN DE RED

A cada interfaz de red se le asignó una dirección IP y un gateway correspondiente, lo que permitió una correcta comunicación entre zonas. La configuración asegura que los paquetes se enruten de manera adecuada en cada segmento de la red.

6.3 REGLAS DE COMUNICACIÓN ENTRE ZONAS

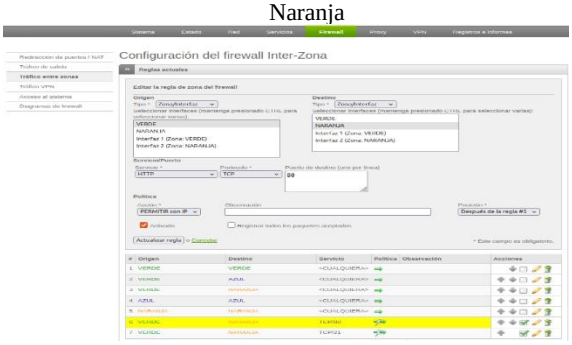
Comunicación entre la Zona Verde y la Zona Naranja:

Se configuraron reglas específicas en el firewall para permitir el tráfico desde la Zona Verde (LAN) hacia la Zona Naranja (Servidor) mediante los protocolos:

- HTTP (puerto 80).
- FTP (puerto 21).

Estas reglas aseguran que los usuarios puedan acceder a servicios web y transferencia de archivos ubicados en la zona de servidores.

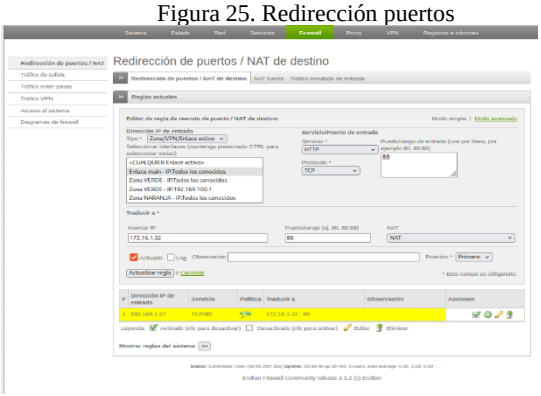
Figura 24. Comunicación Zona Verde con Zona Naranja mediante HTTP y comunicación FTP entre Zona Verde y Naranja



Fuente: Autoría propia

Para permitir el acceso desde Internet a servicios ubicados en la zona DMZ, se implementó redirección de puertos (port forwarding). Esta técnica permite que el firewall enrute el tráfico externo hacia los servidores definidos, sin comprometer la seguridad interna.

Figura 25. Redirección puertos



Fuente: Autoría propia

6.4 VERIFICACIÓN Y PRUEBAS

Validación de reglas inter-zona:

Para confirmar que las reglas fueron aplicadas correctamente, se monitoreó el tráfico en el módulo de administración del firewall. Las reglas creadas permitieron la comunicación deseada entre zonas, de forma controlada y segura.

Pruebas de acceso desde el navegador web:

Se realizaron pruebas de navegación desde equipos ubicados en distintas zonas para validar el acceso permitido por las reglas configuradas. Los resultados fueron los siguientes:

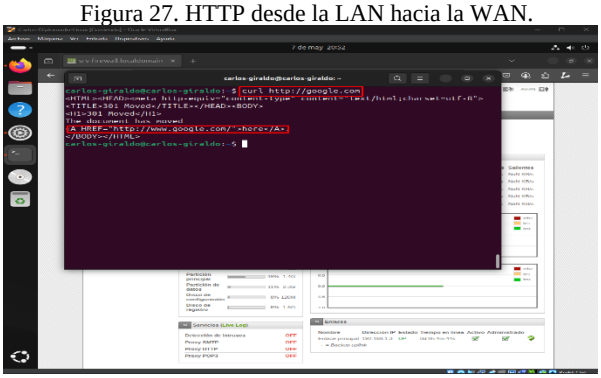
El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso del servicio HTTP desde la LAN hacia la WAN.

Origen	Destino	Protocolo	Estado
LAN (Zona Verde)	DMZ	HTTP	Permitido
LAN (Zona Verde)	WAN (Internet)	HTTP	Permitido
DMZ	WAN (Internet)	HTTP	Permitido
LAN (Zona Verde)	WAN (Internet)	FTP	Permitido
WAN (Internet)	DMZ	HTTP	Permitido

Figura 26. HTTP desde la LAN hacia la zona DMZ

Fuente: Autoría propia

Figura 27. HTTP desde la LAN hacia la WAN.



Fuente: Autoría propia

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN. El ingreso del servicio HTTP desde la WAN hacia la zona DMZ. El ingreso del servicio FTP desde la LAN hacia la WAN.

Figura 28. HTTP desde la zona DMZ hacia la WAN

Fuente: Autoría propia

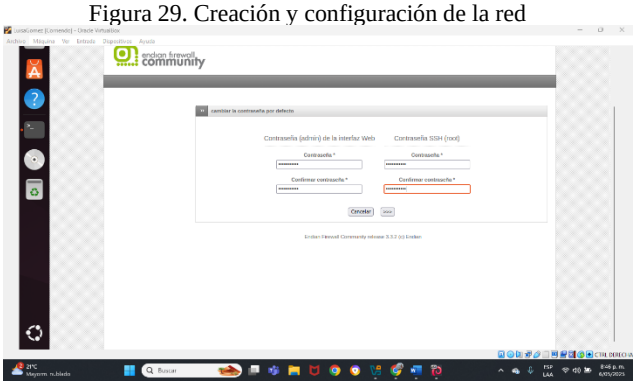
7 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

7.1 CREACION Y CONFIGURACIÓN DE USUARIO

De acuerdo con la arquitectura de red implementada, la cual se ha estructurado mediante una segmentación lógica y funcional del entorno en distintas zonas, damos inicio a la exploración de esta temática crucial. Esta estrategia de segmentación, que se detalla visualmente en la Figura 1 de este documento, constituye un elemento fundamental en la organización y la seguridad de nuestra infraestructura de red, permitiendo una gestión más eficiente de los recursos y la aplicación de políticas de seguridad específicas para cada dominio.

Posteriormente, se procede a la creación y validación de credenciales de usuario. Este proceso se inicia una vez que el usuario ha realizado el intento de ingreso al sistema a través de un navegador web, especificando la dirección IP del recurso al que desea acceder.

Figura 29. Creación y configuración de la red



Fuente: Autoría propia

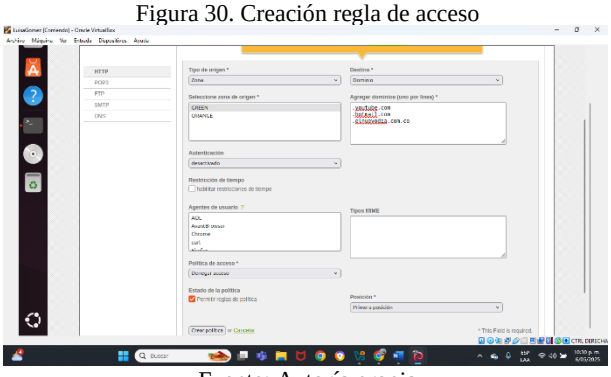
Luego procedemos a configurar cada una de las zonas y podemos percibir como por ejemplo el DNS se configura de manera automática.

7.2 BLOQUEO DE DOMINIOS ESPECÍFICOS

Para poder continuar con el primer paso fundamental del bloqueo de las páginas web específicas, tal como se ha solicitado en el ejercicio, se hace imprescindible habilitar la funcionalidad del proxy HTTP dentro de la configuración del sistema. Adicionalmente, resulta necesario modificar el puerto de comunicación predeterminado asociado a este servicio proxy, con el objetivo de optimizar la seguridad y el control del tráfico de red. Esta modificación del puerto por defecto añade una capa adicional de protección y puede dificultar intentos de acceso no autorizado.

Una vez configurado el proxy HTTP con el puerto deseado, se procede a la adición de una nueva regla de control de acceso. Esta regla tiene como propósito específico restringir el acceso a las páginas web concretas que se mencionan explícitamente en los requerimientos del ejercicio. Para implementar esta restricción de manera efectiva, se establece la "zona verde" de la red como el origen del tráfico al cual se aplicará la regla. Finalmente, se define la política de acceso para esta regla como "denegar servicio", lo que asegura que cualquier intento de acceso desde la zona verde hacia las páginas web listadas será bloqueado de manera sistemática por el sistema de control de acceso.

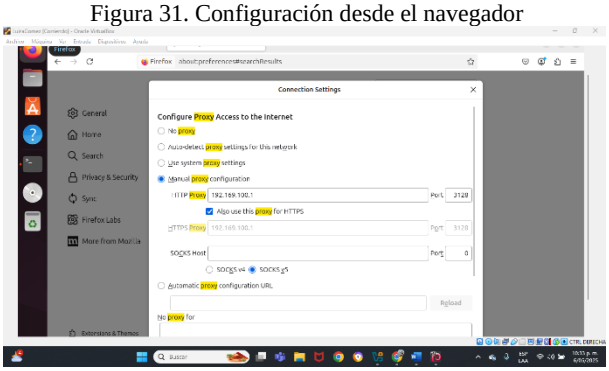
Figura 30. Creación regla de acceso



Fuente: Autoría propia

Nos dirigimos al navegador y en su configuración vamos a modificar la opción de proxy colocando la IP del Endian y el puerto correspondiente.

Figura 31. Configuración desde el navegador



Fuente: Autoría propia

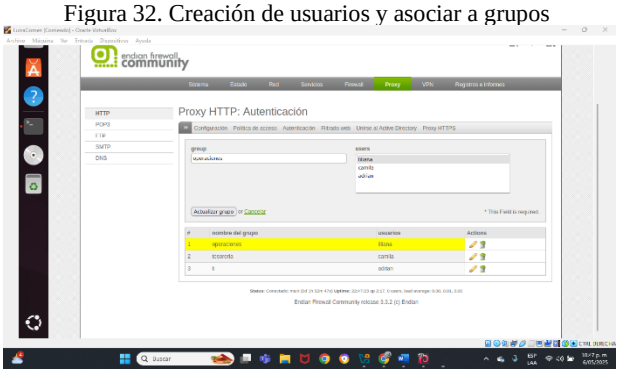
Aquí podemos evidenciar de manera clara y concluyente cómo los dominios web especificados han sido bloqueados exitosamente, demostrando la efectividad de las reglas de control de acceso implementadas previamente. Esta observación confirma la correcta configuración del proxy HTTP y la aplicación de la política de denegación de servicio, lo que impide el acceso a los recursos web restringidos desde la zona de red designada.

7.3 CREACIÓN DE USUARIOS Y GRUPOS

En lo concerniente a la implementación de la política de autenticación de usuarios, como una medida inicial y fundamental para establecer un control de acceso robusto y granular, se procede a la creación lógica de grupos de usuarios. Esta agrupación se realiza atendiendo a criterios específicos, tales como roles organizacionales, niveles de privilegio o necesidades de acceso a determinados recursos. La creación de estos grupos facilita la administración de permisos y la aplicación uniforme de políticas de seguridad a conjuntos de usuarios con características similares, simplificando la gestión y fortaleciendo la seguridad general del sistema.

De la misma manera creamos los usuarios y luego procedemos a asociar los usuarios a los grupos, creamos diferentes nombres y esto es lo que permitirá que cada usuario tenga que autenticar y a partir de ahí se le darán unos permisos y se debe tener en cuenta que se debe habilitar la autenticación por usuario desde las políticas de acceso.

Figura 32. Creación de usuarios y asociar a grupos



Fuente: Autoría propia

Se puede evidenciar de manera explícita cómo el servidor proxy, al intentar acceder a los dominios web que han sido previamente configurados para su bloqueo, solicita de forma activa la autenticación del usuario que intenta realizar la conexión. Este comportamiento confirma la correcta implementación de las políticas de seguridad y la funcionalidad del proxy como un punto de control de acceso, requiriendo la identificación y validación de las credenciales del usuario antes de permitir cualquier interacción con los recursos restringidos.

7.4 VERIFICACIÓN DE PERMISOS DE NAVEGACIÓN

Podemos verificar de forma detallada la manera en que se manifiestan los permisos de navegación para los diferentes usuarios o grupos dentro de la red. Esta verificación permite constatar la correcta aplicación de las políticas de acceso definidas, evidenciando qué recursos en línea son accesibles y cuáles se encuentran restringidos para cada entidad autenticada.

Figura 33. Verificación permisos

Fuente: Autoría propia

8 CONCLUSIONES

La implementación de Endian Firewall en una infraestructura virtual demuestra ser una solución eficaz y educativa para comprender los principios de segmentación de red, seguridad perimetral y configuración de servicios. El entorno creado permite simular el funcionamiento de una red empresarial segura, facilitando la comprensión de conceptos como NAT, DMZ, firewall rules y acceso controlado.

La implementación de reglas NAT y políticas de firewall en la plataforma Endian demostró ser una solución eficaz para gestionar la conectividad y seguridad entre diferentes zonas de red, particularmente desde la LAN y la DMZ hacia la WAN. A través de la configuración de reglas de Source NAT y controles de tráfico saliente, se logró enmascarar direcciones IP privadas y establecer filtros precisos que permitieron validar el funcionamiento del sistema tanto en escenarios de acceso permitido como restringido. Las pruebas realizadas confirmaron la flexibilidad y robustez de esta arquitectura, lo que la convierte en una opción viable para entornos de laboratorio, empresariales o educativos donde se requiera una segmentación clara del tráfico y un control granular de la salida hacia redes externas.

Se logró establecer una infraestructura de red virtualizada completamente funcional y segmentada mediante el uso de Endian Firewall Community. A continuación, se detallan los principales logros:

- Acceso exitoso a la interfaz web de Endian desde la zona Green.
- Conectividad a Internet confirmada desde la zona Green (Desktop) y zona Orange (Server).
- Acceso exitoso a la página web y servidor FTP alojado en Ubuntu Server desde clientes en la zona Green.
- Tráfico correctamente re - direccionado mediante reglas NAT.

La experiencia permitió afianzar conocimientos en redes, seguridad perimetral y uso de herramientas de virtualización para simulación de entornos reales.

La configuración de reglas de acceso que permiten la comunicación entre la zona Verde y la zona Naranja mediante los protocolos HTTP (puerto 80) y FTP (puertos 20 y 21) demuestra la capacidad de segmentar y controlar el tráfico de red, habilitando servicios específicos de forma segura entre distintas zonas.

9 REFERENCIAS

[1] Araque, D., Gonzalez, C. y Deossa, A. (2009). *Servidor firewall Endian* [Trabajo académico, SENA – Regional Antioquia, Programa de Administración de Redes de Computadores]. https://es.slideshare.net/slideshow/manual-endian/1360390

[2] Barbhuiya, F., Biswas, S. y Nandi, S. (2011). An Active Host-Based Intrusion Detection System for ARP-Related Attacks and its Verification. *International Journal of Network Security & Its Applications (IJNSA),* 3(3), 163-180. https://www.airccse.org/journal/nsa/0511ijnsa11.pdf

[3] Ciampa, M. (2018). *CompTIA Security+ Guide to Network Security Fundamentals.* (7ª ed.). Cengage Learning. https://unidel.edu.ng/focelibrary/books/A%202022%20Comptia%20Security%2B%20Guide%20to%20Network%20Security%20Fundamentals%20by%20Mark%20Ciampa%20%28z-lib.org%29.pdf

[4] Cisco Systems. (2020*). CCNA 200-301 official cert guide: Volume 2.* Cisco Press. https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-2-9780138214951

[5] Endian srl. (2008). *Manual de referencia del firewall Endian r. 2.2.1.9*. https://docs.endian.com/archive/2.2/efw.system.html

[6] Endian. (2021). *Endian firewall community manual.* https://wiki.endian.com/display/USERDOC/Endian+Firewall+Community+3.3

[7] Forouzan, B. (2007). *Data Communications and Networking.* (4ª ed.). McGraw-Hill. https://dpvipracollege.in/wp-content/uploads/2023/01/Data-Communications-and-Networking-By-Behrouz-A.Forouzan.pdf

[8] Jankowski, B., Mazurczyk, W. y Szczypiorski, K. (27-30 de Septiembre de 2010). *Information Hiding Using Improper Frame Padding.* Simposio Proceedings of 2010 14th International Telecommunications Network Strategy and Planning Symposium, Networks 2010. Warsaw, Poland. https://ieeexplore.ieee.org/document/5624901

[9] Kurose, J. y Ross, K. (2017). *Computer Networking: A Top-Down Approach*. (7ª ed.). Pearson. https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf

[10] Pérez, J. (2020). Implementación de zonas DMZ en redes seguras con software libre. Revista Tecnológica – *Universidad Técnica de Ambato*, 18(2), 77–85. https://doi.org/10.31243/rte.v18i2.607

[11] Red Hat. (2023). *How to configure firewalld zones and services.* Red Hat Customer Portal. https://access.redhat.com/solutions/221403

[12] Tanenbaum, A. y Wetherall, D. (2011). *Redes de Computadoras.* (5ª ed.). Pearson. https://bibliotecavirtualapure.wordpress.com/wp-content/uploads/2015/06/redes_de_computadoras-freelibros-org.pdf