IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN GNU/LINUX MEDIANTE ENDIAN FIREWALL: CONFIGURACIÓN DE DMZ, NAT, CONTROL DE ACCESO Y PROXY HTTP

Cristian Fernando Romero Villarreal
e-mail: cfromerov@unadvirtual.edu.co
Jeffrey Leonardo Muñoz Muñoz
e-mail: jlmunozmu@unadvirtual.edu.co
Juan Sebastián Urrego Arias
e-mail: jsurregoa@unadvirtual.edu.co
Kaleth Joseh Cristancho Alandette
e-mail: kjcristanchoa@unadvirtual.edu.co

RESUMEN: *El presente artículo describe la implementación de seguridad en infraestructuras bajo la plataforma GNU/LINUX, por medio del uso de la distribución Endian Firewall. Se establecen 5 temáticas fundamentales: la instalación y configuración inicial de Endian en VirtualBox con zonas LAN, WAN y DMZ; la configuración de NAT para la comunicación entre redes; la habilitación y restricción de servicios en la zona DMZ mediante reglas de tráfico; el control de acceso inter-zona con protocolos HTTP y FTP y la implementación de un proxy HTTP no transparente con autenticación de usuarios contra el helper NCSA y filtrado de URL mediante c-icap (protocolo ICAP), incluyendo el bloqueo de dominios específicos vía lista negra personalizada.*

PALABRAS CLAVE: GNU/Linux, Endian Firewall, Seguridad perimetral, Proxy HTTP.

1 INTRODUCCIÓN

La seguridad perimetral en las redes industriales es un componente esencial para garantizar la integridad, disponibilidad y confidencialidad de los servicios e información alojados en los diferentes servidores bajo el uso de sistemas GNU/LINUX. Los ambientes empresariales, actualmente se encuentran con mucha exposición a los servicios de internet, es por esto que se requiere de mecanismos de seguridad para delimitar las zonas de acceso a la información y gestionar el tráfico de la red.

Endian Firewall Community es una distribución GNU/Linux especializada en seguridad perimetral que permite administrar la red mediante zonas diferenciadas: verde para la red LAN interna, roja para la red WAN o salida a Internet y naranja para la red DMZ o segmento de servidores. Esta separación por zonas facilita la aplicación de políticas de seguridad distintas según el origen, destino y tipo de tráfico que atraviesa el firewall [1].

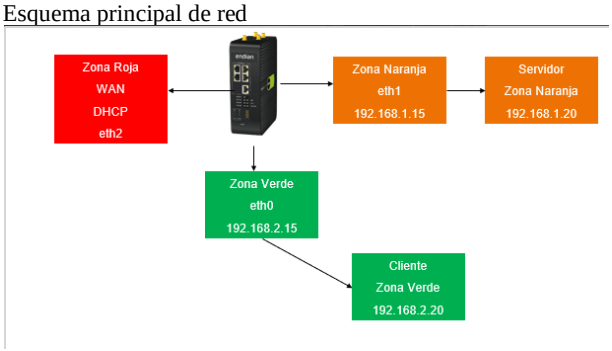
El presente trabajo documenta la implementación colaborativa de una infraestructura de seguridad perimetral utilizando Endian como plataforma central, tomando desde la configuración inicial de la instancia virtualizada hasta la implementación de un proxy HTTP con autenticación, pasando por reglas NAT, control de servicios en la DMZ y políticas de

acceso inter-zona y, finalmente, la inspección de tráfico web a nivel de aplicación mediante un proxy autenticado que combina identidad de usuario, pertenencia a grupo y filtrado por categoría/dominio.

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

Se lleva a cabo la distribución y asignación de direcciones IP para cada zona y los equipos asociados, garantizando una correcta organización y conectividad de la red.

Figura 1.
Esquema principal de red



Fuente: Autoría Propia

Se creó una máquina virtual en Oracle VM VirtualBox con el propósito de simular y administrar la infraestructura de red del proyecto. Para ello, se configuraron tres adaptadores de red con funciones específicas: el Adaptador 1 en modo NAT, destinado a la zona roja (WAN), permitiendo la conexión hacia redes externas e Internet; el Adaptador 2 en modo de red interna (LAN), asignado a la zona verde para la comunicación entre los equipos de la red local; y el Adaptador 3 también en modo de red interna, destinado a la zona naranja (DMZ-Servidor), con el

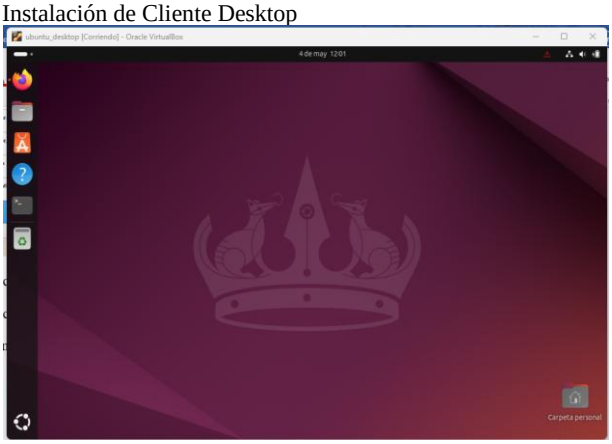
fin de aislar y gestionar los servicios dentro de la arquitectura implementada. Esta forma de instalación en VirtualBox permite validar Endian como firewall perimetral en un entorno de laboratorio con interfaces separadas por zona [2].

Figura 2.
Creación de máquinas virtuales

Fuente: Autoría Propia

Se realiza la creación y configuración del cliente desktop utilizando el sistema operativo Ubuntu, seleccionado debido a su estabilidad, seguridad y amplia compatibilidad con herramientas y servicios de red. Además, este sistema operativo ofrece un entorno completo y eficiente para la administración de recursos, la ejecución de aplicaciones y la realización de pruebas dentro de la infraestructura implementada, convirtiéndose en una opción adecuada para el desarrollo y funcionamiento del proyecto.

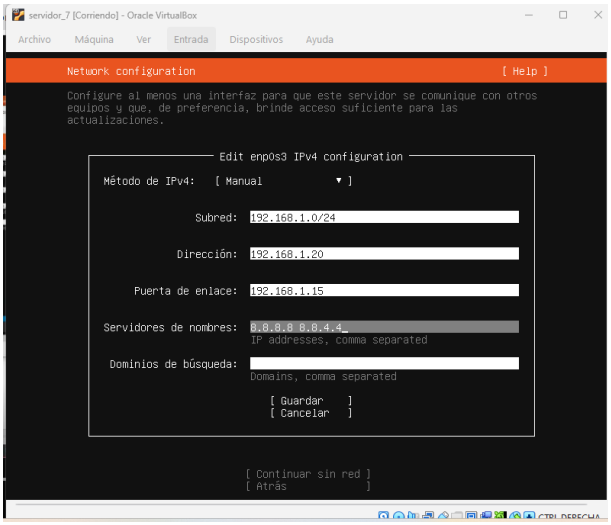
Figura 3.
Instalación de Cliente Desktop



Fuente: Autoría Propia

Se realiza la creación y configuración del servidor utilizando Ubuntu Server, seleccionado por su estabilidad, manejo eficiente de recursos y capacidad de administración en entornos de red. Durante el proceso de configuración, se habilita una dirección IP estática de acuerdo con la planificación establecida en el esquema inicial, lo que permite mantener una comunicación estable y permanente entre los dispositivos y servicios implementados dentro de la infraestructura. Ubuntu proporciona documentación de soporte para la administración del sistema y la configuración de servicios de red usados en este tipo de entornos.

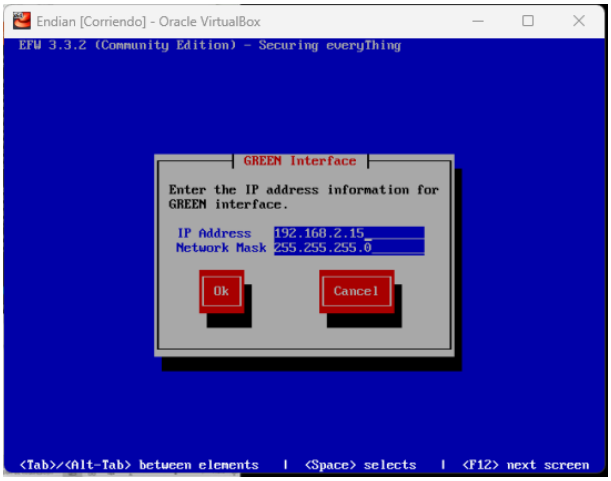
Figura 4.
Creación del servidor



Fuente: Autoría Propia

Instalación y configuración de Endian Firewall Community, asignando una dirección IP estática para la zona verde de la red (LAN). Este rango de direccionamiento será utilizado por todos los clientes y dispositivos que se conecten a dicha zona, permitiendo una administración organizada de la red, una correcta comunicación entre los equipos y un mejor control del tráfico interno dentro de la infraestructura implementada.

Figura 5.
Instalación de Endian Firewall



Fuente: Autoría Propia

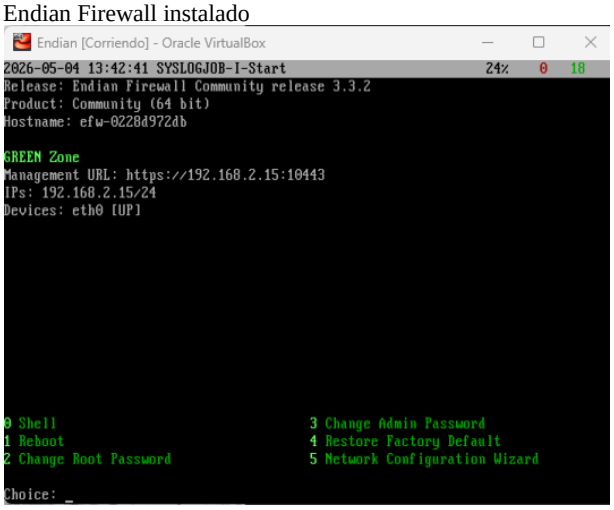
Se finaliza el proceso de instalación de Endian Firewall Community, dejando el sistema preparado para continuar con la habilitación y administración de los servicios a través del cliente web. Asimismo, se deja lista la plataforma para realizar las configuraciones correspondientes del servidor, permitiendo avanzar con la implementación y gestión de los diferentes servicios y políticas de red dentro de la infraestructura establecida [1].

Figura 6.
Asignación de URL de acceso WEB

Fuente: Autoría Propia

Interfaz de Endian Firewall Community inicializada correctamente, incorporando los módulos necesarios para el acceso, administración y configuración del sistema. Asimismo, se habilitan las herramientas de edición y gestión por medio de consola, permitiendo realizar ajustes avanzados, monitoreo de servicios y administración de la infraestructura de red de manera más eficiente y segura.

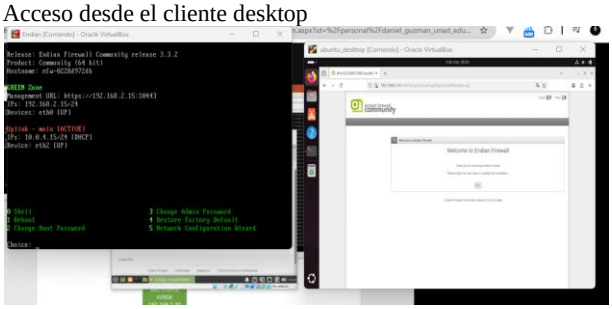
Figura 7.
Endian Firewall instalado



Fuente: Autoría Propia

Acceso al cliente desktop por medio de la URL que muestra Endian. Al ya haber configurado las tarjetas de red desde el inicio, el cliente toma una IP por DHCP dentro del mismo rango de la zona verde. Es por esto que el acceso a Endian desde el navegador es posible. Si se desea y se requiere mejor orden. Se configura una IP estática en el mismo rango de la zona verde

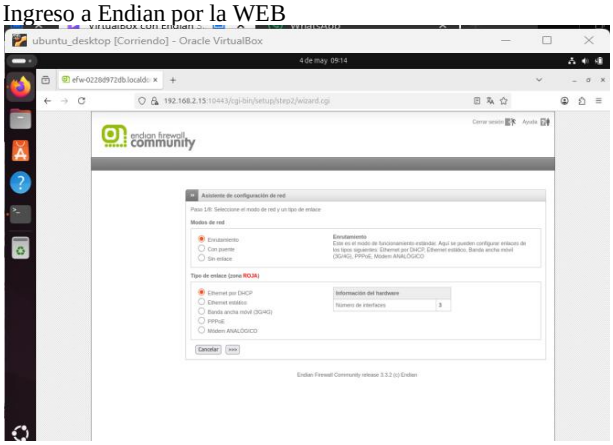
Figura 8.
Acceso desde el cliente desktop



Fuente: Autoría Propia

Se realiza el ingreso a la interfaz web de Endian Firewall Community para iniciar el proceso de configuración del sistema. En esta etapa, la plataforma solicita la asignación de contraseñas de acceso para la administración y seguridad del firewall; se establecen las credenciales deseadas y se continúa con el asistente de configuración. Posteriormente, se muestra la pantalla principal destinada a la configuración del enrutamiento de red, donde se definen las interfaces, zonas y parámetros necesarios para la correcta comunicación entre los diferentes segmentos de la infraestructura implementada.

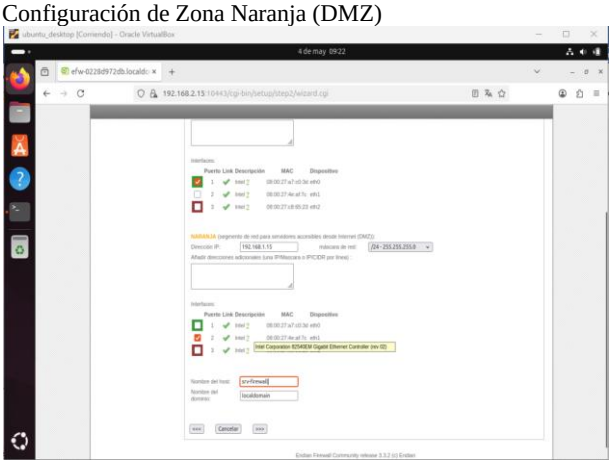
Figura 9.
Ingreso a Endian por la WEB



Fuente: Autoría Propia

Una vez configurada la red roja (WAN), encargada de proporcionar el acceso a internet, y la red verde (LAN), destinada a permitir la comunicación entre los diferentes equipos de la red interna, se procede con la instalación y configuración de la red naranja (DMZ). Esta zona será utilizada para establecer la conexión con el servidor, permitiendo aislar y administrar los servicios de manera más segura, además de facilitar el control del tráfico y la comunicación entre la red interna y los servicios alojados en el servidor [1].

Figura 10.
Configuración de Zona Naranja (DMZ)



Fuente: Autoría Propia

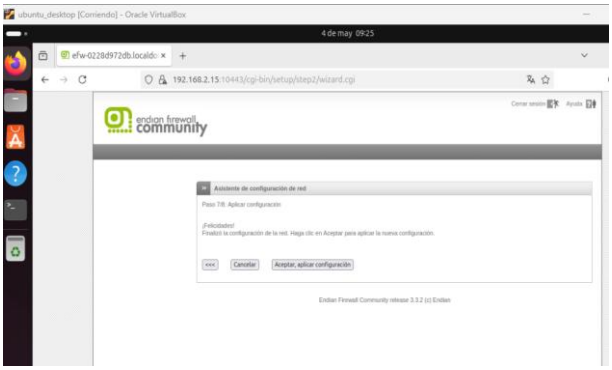
Se realiza la asignación de una dirección IP estática para la zona naranja (DMZ), configurándose de acuerdo con la dirección MAC correspondiente del servidor para garantizar una identificación y conexión permanente dentro de la red. Además, se asigna un nombre al servidor dentro de Endian Firewall Community, facilitando su administración, monitoreo y reconocimiento dentro de la infraestructura implementada.

Figura 11.
Asignación de IP y enrutamiento de zona naranja

Fuente: Autoría Propia

Al finalizar el proceso de configuración, se verifica que las tres zonas de red —roja (WAN), verde (LAN) y naranja (DMZ)— se encuentran correctamente configuradas y activadas dentro de Endian Firewall Community. Con esto, la infraestructura queda preparada para su implementación y operación, garantizando la comunicación adecuada entre las diferentes redes, el acceso a internet y la administración segura de los servicios y servidores configurados.

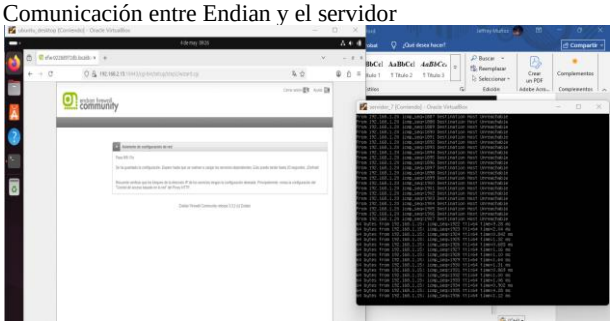
Figura 12.
Verificación de zonas activas



Fuente: Autoría Propia

Se realiza la verificación de conectividad entre el servidor y Endian Firewall Community mediante pruebas de comunicación utilizando el comando *ping* desde el servidor hacia la dirección IP asignada a Endian. Esta validación permite confirmar que la comunicación entre ambos dispositivos es correcta y que la configuración de red implementada se encuentra funcionando adecuadamente.

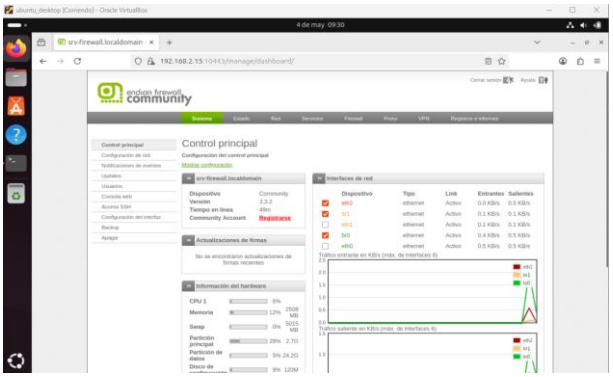
Figura 13.
Comunicación entre Endian y el servidor



Fuente: Autoría Propia

Después de verificar una conexión exitosa, se procede nuevamente al ingreso de Endian Firewall Community utilizando el usuario administrador (*admin*) y la contraseña configurada previamente. Posteriormente, se accede a la vista principal del Firewall, específicamente al panel *Dashboard*, donde se visualizan las diferentes conexiones activas, el estado de las interfaces de red y la información general del sistema mediante una interfaz gráfica funcional e intuitiva, facilitando así la administración y monitoreo de la infraestructura de red implementada.

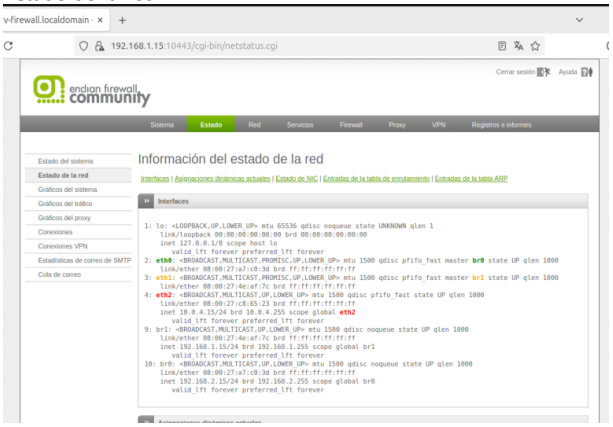
Figura 14.
Dashboard de Endian Firewall



Fuente: Autoría Propia

Verificación del estado de la red en la zona gráfica de Endian. En esto se puede visualizar las tres zonas conectadas y funcionales, la zona verde en donde se conecta el cliente. La zona naranja donde está conectado el servidor y la zona roja que es la conexión a internet desde el proveedor

Figura 15.
Estado de la red



Fuente: Autoría Propia

La instalación de Endian se realizó desde la imagen ISO oficial. Durante el proceso se configuraron las interfaces de red asignando eth0 a la zona verde (`192.168.2.15/24`), eth1 a la zona naranja (`192.168.1.15/24`) y eth2 a la zona roja. Se verificó el estado de los servicios desde consola y desde la interfaz web en la máquina del cliente.

La implementación resultó exitosa comprobando los accesos desde los diferentes servidores, tanto el cliente como el servidor Ubuntu, además de eso se verificó la accesibilidad desde la interfaz web con URL: (`https://192.168.2.15:10443`), en este último se observa el dashboard de Endian realizando procesos en toda la red.

3 CONFIGURACIÓN NAT.

En esta sección del trabajo, se realiza la implementación de configuración NAT, esto permite que cuando un dispositivo interno *(LAN)* salga a la red externa *(WAN)*, lo realice a través de una sola dirección IP, que puede estar siendo usada por varios dispositivos a la vez, esto permite un mayo anonimato y seguridad de la infraestructura tecnológica, así se tiene un mayor control del tráfico de información de salida y entrada, para la configuración exitosa requerimos una serie de pasos explicada a continuación, todo esto también permitiendo un análisis y filtrado de peticiones [3].

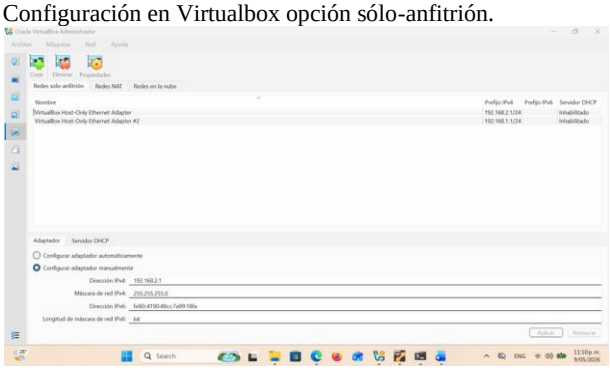
Para la aplicación de configuración NAT en firewall, se debe cumplir con los siguientes requisitos:

- Endian Firewall;
- Ubuntu Server (DMZ);
- Ubuntu Desktop (LAN).

3.1 Configuración redes sólo-anfitrión.

Se configura dos redes de tipo sólo-anfitrión, esto permitirá aislar por completo la red LAN, y red DMZ, así el tráfico solamente pasará por el firewall de Endian, dando una mayor seguridad, y cumpliendo con la finalidad de esta configuración, como podemos visualizar, la dirección IP es única en cada caso, y esta debe ser diferente a las predeterminadas de Endian, para que no exista conflicto en la ejecución [4].

Figura 16.
Configuración en Virtualbox opción sólo-anfitrión.



Fuente: Autoría Propia.

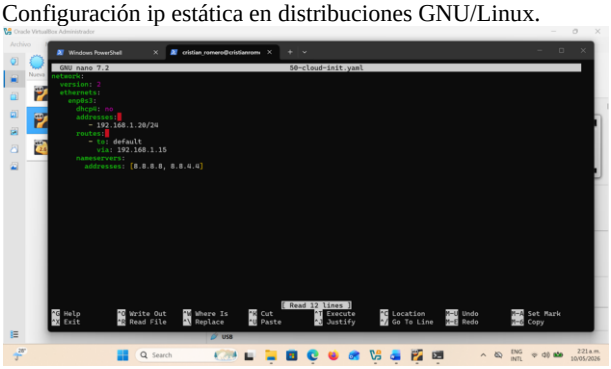
3.2 Configuración ip estática.

Este paso es muy importante, para el funcionamiento correcto de NAT, y el firewall en general, la configuración IP estática en el servidor DMZ, y en el cliente LAN permite diferenciar cada máquina, y que comportamiento en el tráfico de datos se realizará de acuerdo a las reglas posteriores, este paso se debe realizar manualmente, para tener un control muy detallado y estricto, en la montura de la presente infraestructura de ciberseguridad [4].

Para definir el direccionamiento estático en Ubuntu se editó el archivo de configuración de netplan mediante el comando sudo nano /etc/netplan/50-cloud-init.yaml. Esta configuración permite establecer la dirección IP, puerta de

enlace y servidores DNS de forma persistente, de acuerdo con la documentación de administración de red de Ubuntu [5].

Figura 17.
Configuración ip estática en distribuciones GNU/Linux.



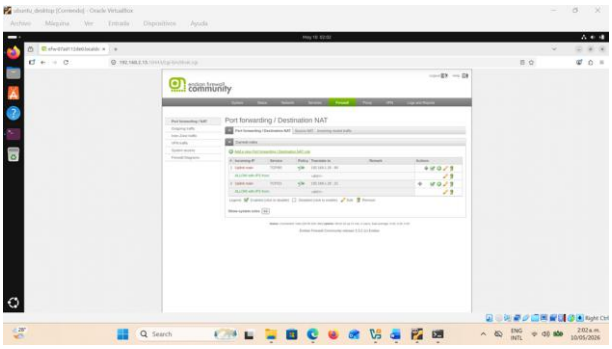
Fuente: Autoría Propia.

3.3 Configuración Port-forwarding

Como requisito previo, se debe tener Endian configurado de forma básica su dirección IP para acceso al panel de administración, luego, se dirige en el navegador a la dirección IP establecida, y se ingresan las credenciales configuradas en la instalación. Se visualiza el dashboard con las múltiples opciones, entre ellas, la que se usará en este paso, es Port Forwarding, que permitirá cuando una petición externa (WAN), necesite acceder a la red interna, se redirija a la zona desmilitarizada (DMZ), y pueda realizar la consulta, de acuerdo a los protocolos de seguridad vigentes [5].

En la pestaña de Port Forwarding, se agrega dos reglas, una para la dirección IP del DMZ con el puerto 80, y otra con el puerto 21, siendo esta última de utilidad cuando se quiera acceder vía SSH, desde el computador anfitrión Windows.

Figura 18.
Configuración Port Forwarding.

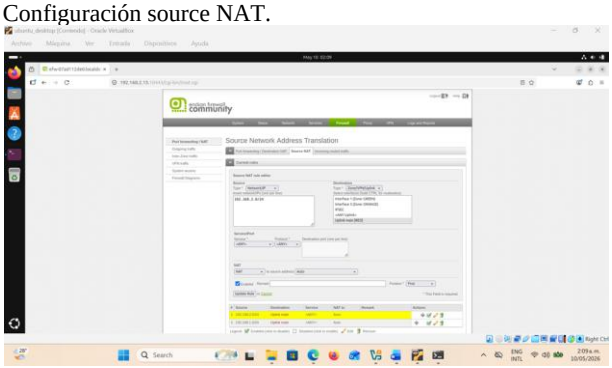


Fuente: Autoría Propia.

3.4 Configuración Source NAT

Siguiente paso, es la configuración de source NAT, esto permitirá que DMZ, y LAN puedan salir o conectarse a red externa (WAN), compartiendo la misma dirección IP, esto permite una mayor seguridad y anonimato en el sistema, la traducción de direcciones IP fue además un gran avance en el internet, permitiendo un mayor ahorros de direcciones IP, sobre todo en el caso específico de las direcciones IPv4, este es el principal objetivo de la presente temática, y una sección muy relevante en la configuración del Firewall [5]

Figura 19.
Configuración source NAT.



Fuente: Autoría Propia.

3.5 Configuración Outgoing traffic.

A continuación se realiza la configuración de las reglas Outgoing traffic, esto permitirá que el tráfico salga, y pueda establecer conexión externa, se procede a crear unas reglas de LAN a WAN, por unos puertos determinados, para seguir buenas prácticas de ciberseguridad, esta configuración es importante, sobre todo cuando en LAN se necesite actualizar paquetes, y los repositorios puedan descargarse de forma libre, pero manteniendo la seguridad de la red interna.

En principio se crean reglas con dirección green a red, y orange a red, por unos puertos establecidos, como se mencionó antes, para seguir manteniendo la seguridad pero a la vez facilitar el acceso a repositorios, y contenido de internet sin restricciones, dando una navegación completa y rápida, estas reglas se crean de manera sencilla seleccionando la interfaz requerida y su destino, como paso adicional se configura el tipo de puerto, y se da clic en guardar [5].

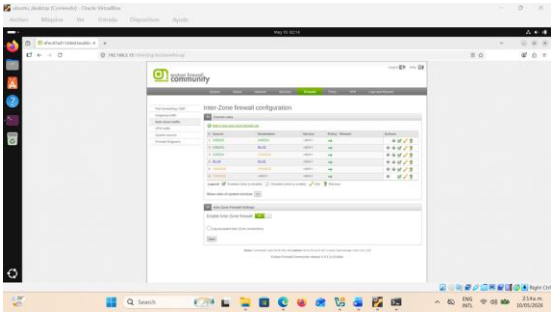
Figura 20.
Configuración reglas Outgoing traffic.

Fuente: Autoría Propia.

3.6 Configuración Inter-Zone Firewall.

A continuación se realizan las configuraciones Inter-Zone Firewall, este ajuste permite la comunicación dentro de la red, entre las distintas interfaces, es decir desde LAN a DMZ, DMZ a LAN, LAN a LAN, entre otras. Con esto se puede comunicar entre Ubuntu Desktop a Ubuntu Server, y realizar peticiones, accesos SSH, y establecer una comunicación segura sin salir a la red externa. La adición de reglas es muy sencilla, click en el botón "más", y escribimos la interfaz de origen, y la interfaz de destino, de forma opcional se selecciona el tipo de puerto, y se reinicia para aplicar cambios [5].

Figura 21.
Pantalla de Inter-Zone Firewall.



Fuente: Autoría Propia.

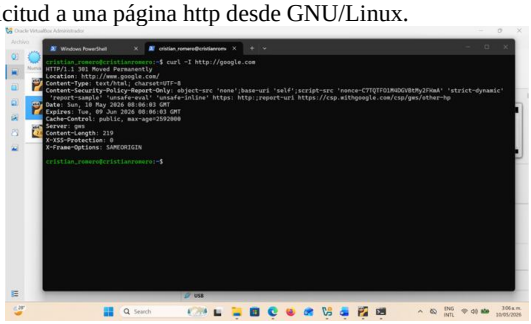
3.7 Pruebas peticiones Http, FTP en múltiples direcciones.

Se realizan pruebas para saber si la configuración fue correcta en los distintos escenarios, uno de ellos es en el servidor dentro de DMZ, que tiene instalado la distro Ubuntu Server, se comienza por realizar una solicitud a una página http, y visualizar su estado, debemos obtener un código 200, o 301, que nos indica una correcta carga de los paquetes. Como se puede visualizar, el código fue 301, que significa una carga exitosa, y al ser http, la página se redirige a https, culminando por correcta la configuración, los mismos comandos se ejecutan en Ubuntu Desktop que está alojado en LAN, y por consiguiente dió los mismos resultados.

El comando Curl, permite realizar peticiones, para verificar el adecuado funcionamiento del tráfico de datos, en este trabajo, se realiza de interno a externo, e interno a interno.

Es decir, LAN a WAN, DMZ a WAN, LAN a DMZ, y se obtuvo una comunicación exitosa [5].

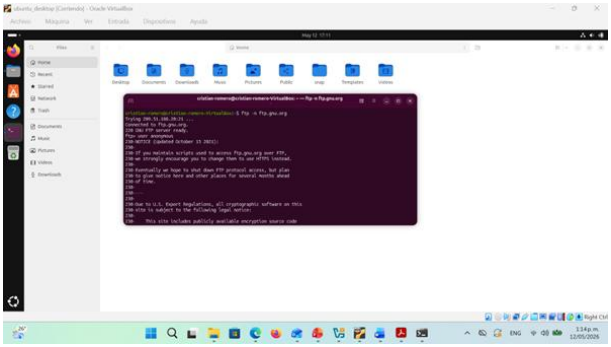
Figura 22.
Solicitud a una página http desde GNU/Linux.



Fuente: Autoría Propia.

A continuación se realiza la conexión a un servidor FTP público para ensayar un estado correcto en la salida WAN, se ejecuma el comando `ftp ftp.gnu.org`, y visualizamos la salida, si dice "Connected", la conexión fue exitosa, y al final de la consola, tendremos listo el login ftp, para realizar las peticiones que requerimos, podemos también visualizar los archivos en el servidor, y las características comunes de esta comunicación [5].

Figura 23.
Conexión a un servidor FTP público desde WAN.

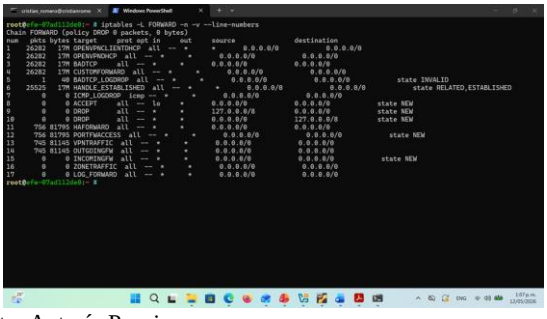


Fuente: Autoría Propia.

Entre otras pruebas, tenemos el conocer la dirección ip pública desde las distintas máquinas LAN, y DMZ, deben ser la misma, para dar por firmeza, que la configuración NAT se realizó, y está funcionando correctamente, para chequear esta sección ejecutamos el comando `curl ifconfig.me`, y comparamos la dirección IP entre las distintas máquinas de la infraestructura tecnológica; también debemos destacar la comprobación de la correcta instalación de Apache, para en posteriores temáticas los compañeros puedan brindar servicios, y la dirección de acceso, sea la ip pública que se visualizó en el comando.

Finalmente se realiza la comprobación de reglas de envío, y contadores en Endian Firewall, se ejecuta una serie de comandos para visualizar internamente las configuraciones realizadas, sin necesidad de interfaz gráfica, y de manera resumida, primero se ejecuta el comando `iptables -L FORWARD -n -v --line-numbers`, esta ejecución muestra los paquetes que entran y salen de cada regla establecida [6].

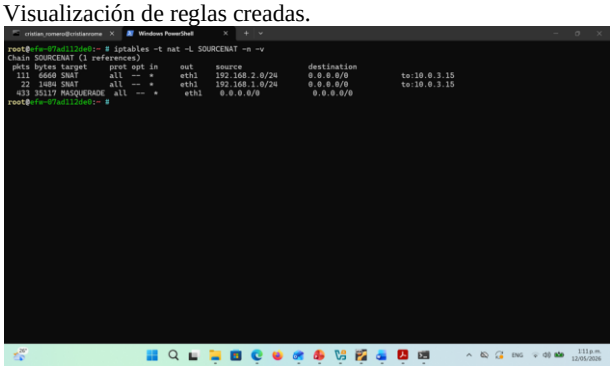
Figura 24.
Ejecución del comando.



Fuente: Autoría Propia.

Y si se ejecuta el comando `iptables -t nat -L SOURCENAT -n -v`, se puede verificar las IP tables, y redes configuradas en la cadena SOURCENAT, esto permite un análisis de las reglas creadas para NAT, es decir el camuflado de la ip pública para múltiples dispositivos a la vez, y en cuáles está realizando efecto [6].

Figura 25.
Visualización de reglas creadas.

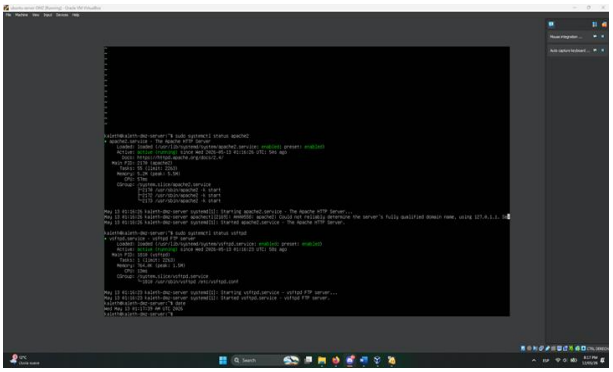


Fuente: Autoría Propia.

4 REGLAS DE ACCESO INTER-ZONA

Antes de gestionar las reglas de acceso Inter-Zona del sistema, debemos asegurarnos de cumplir con los requisitos previos entre los cuales están: servicios vsftpd y apache2 activo en servidor ubuntu, Ubuntu Desktop con navegador, acceso ssh a una computadora endian. Primero se debe verificar que los servicios estén activos y funcionales para satisfacer el prerrequisito del servidor. Nosotros usaremos principalmente los servicios apache2 y vsftpd, pero en este punto pueden configurarse más aspectos del servidor como usuarios y paquetes a utilizar [7].

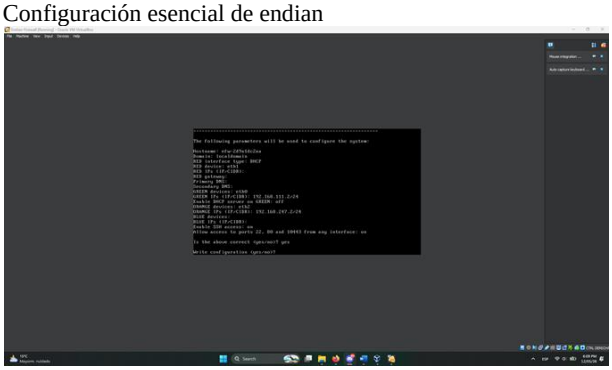
Figura 26.
Verificación de servicios en servidor - Tema 4



Fuente: Autoría Propia.

Ahora procedemos a corroborar la configuración de la computadora host donde se instalará el servicio de Endian para asegurarnos de que todo esté orden antes de iniciar el procedimiento. Cuando se empieza desde cero, es necesario descargar el ISO del sistema operativo desde el sitio web oficial de endian firewall y, en nuestro caso, cargarlo a una máquina virtual de VirtualBox para proceder con su instalación.

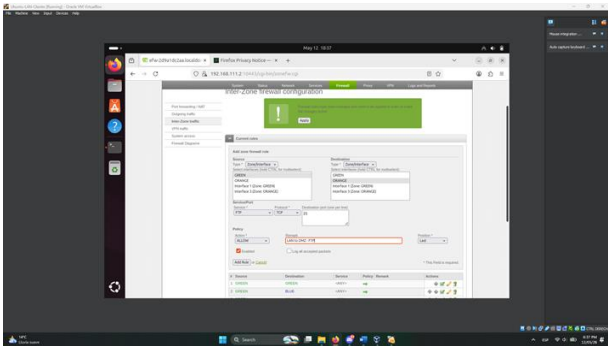
Figura 27.
Configuración esencial de endian



Fuente: Autoría Propia.

La imagen anterior nos muestra el setup preparado para nuestros casos de prueba, se pueden visualizar las distintas direcciones IPs para cada una de las pantallas, tanto verdes, rojas y naranjas. Una vez que todo esté en orden y configurado, procedemos a ingresar al portal web de endian firewall a través de la dirección https://192.168.111.2:10443. Esta puede hallarse en la ventana principal de endian firewall.

Figura 28.
Portal de tráfico Inter-Zona en endian firewall

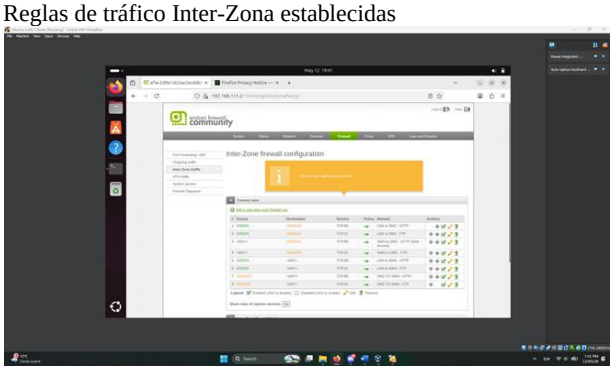


Fuente: Autoría Propia.

Ahora nos dirigimos al área de configuración de reglas de tráfico inter-zona dentro de la pestaña “firewall” del portal web para inicializar su configuración.

Lo que queremos lograr es permitir que cada computadora pueda conectarse a las demás a través de los puertos HTTP 80 y FTP 21 y así mismo, a la web; en la siguiente figura podremos visualizar estas reglas con mayor claridad, donde hallamos las reglas necesarias ya establecidas dentro del portal web de endian firewall.

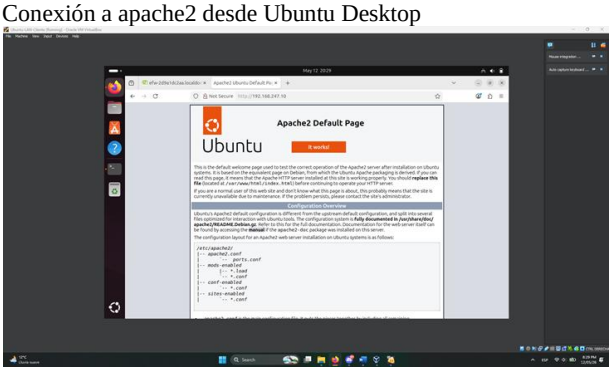
Figura 29.
Reglas de tráfico Inter-Zona establecidas



Fuente: Autoría Propia

Ahora se procede a corroborar la correcta implementación de las reglas de tráfico. Primeramente, verificamos que la computadora Ubuntu desktop pueda conectarse al servicio apache2 del servidor. Nótese que al ser un servicio web montado en un servidor, este puede configurarse según las necesidades pertinentes para cada caso de uso particular a través de la especificación de módulos específicos a cargar, los DNS y URLs, e incluso la asignación de virtual hosts [8]. Para nuestra finalidad, sólamente es necesario establecer un punto de acceso para verificar las reglas de red establecidas.

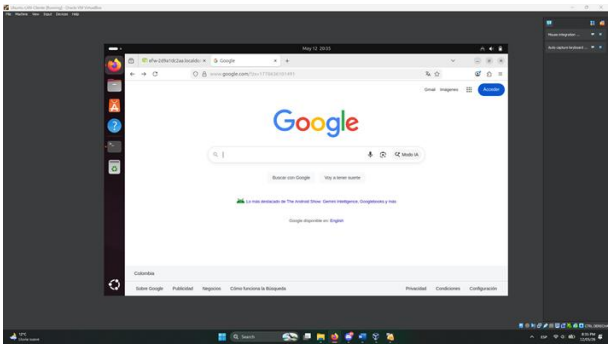
Figura 30.
Conexión a apache2 desde Ubuntu Desktop



Fuente: Autoría Propia

¡Éxito! Nuestra computadora desktop es capaz de conectarse al servicio web de apache2 configurado dentro de nuestro servidor, de forma local. Ahora comprobamos si esta computadora puede conectarse a la web o redes WAN ingresando a algún sitio web de acceso público como lo es el buscador www.google.com.

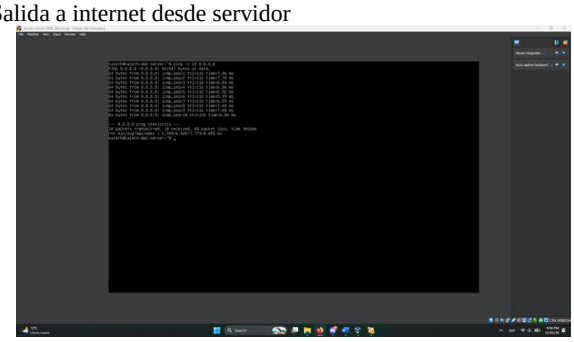
Figura 31.
Conexión a la web desde Ubuntu Desktop



Fuente: Autoría Propia

Se comprueba el acceso a la web o red WAN desde la computadora Ubuntu desktop de manera exitosa, lo cual es un indicio del correcto funcionamiento de nuestras reglas previamente establecidas. Ahora debemos verificar que nuestro servidor también tenga acceso a la red WAN haciendo ping al servidor DNS público de google a través de la ip 8.8.8.8.

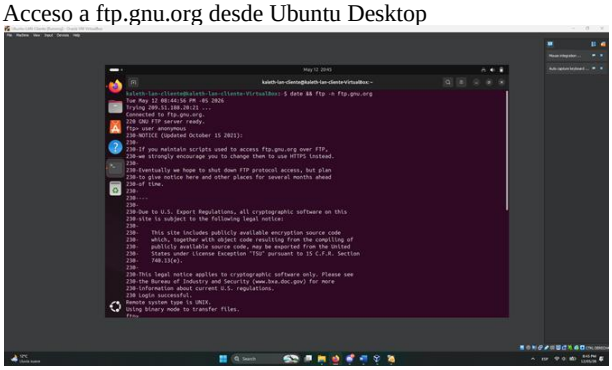
Figura 32.
Salida a internet desde servidor



Fuente: Autoría Propia

Y por último, ahora procedemos a verificar que tanto la computadora Ubuntu Desktop como la máquina de nuestro endian firewall puedan acceder al FTP del servidor, tal como lo establecimos anteriormente. Esto nos permitirá saber que las redes de nuestras computadoras sean capaces de enviar y recibir paquetes entre sí mismas, fundamental en configuración de sistemas de redes locales.

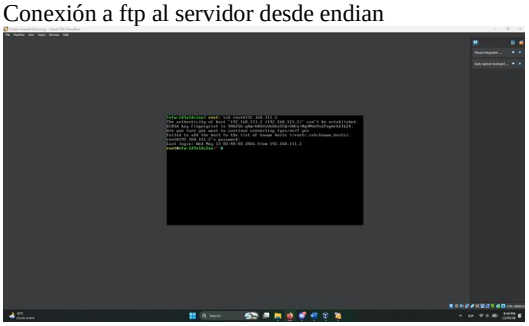
Figura 33.
Acceso a ftp.gnu.org desde Ubuntu Desktop



Fuente: Autoría Propia

Tras haber corroborado en nuestra máquina Ubuntu Desktop, ahora comprobaremos en la máquina host donde establecimos y configuramos nuestro endian firewall. Como nota adicional, es importante conocer que este tipo de verificaciones e incluso configuraciones de servicios pueden designarse y estructurarse dentro de las distintas etapas de arranque del sistema Linux a través de la asignación de niveles de RunLevel dentro de un administrador de servicios como lo es SysVinit [9].

Figura 34.
Conexión a ftp al servidor desde endian



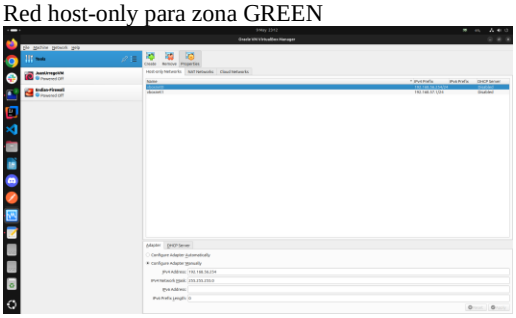
Fuente: Autoría Propia

Se comprueba que la implementación de las reglas de tráfico inter-zona fueron correctamente establecidas dentro de la red y sus computadoras. La gestión del tráfico dentro de una red nos permite manejar un índice de ciberseguridad mayor dentro de nuestros sistemas, puesto que únicamente se le brinda acceso a direcciones estrictamente necesarias a las computadoras, previniendo su uso indebido o innecesario.

5 PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN DE USUARIOS Y FILTRADO POR LISTA NEGRA

Un servidor proxy actúa como intermediario entre el usuario y los recursos de Internet, permitiendo centralizar las solicitudes web, aplicar controles de acceso y registrar la actividad de navegación [10]. En esta temática se implementa un proxy HTTP no transparente sobre Endian Firewall, de manera que el navegador debe declarar explícitamente el proxy, autenticarse con un usuario válido y quedar sujeto a una política de filtrado por lista negra.

Figura 35.
Red host-only para zona GREEN



Fuente: Autoría Propia

La red host-only vboxnet0 se configuró con direccionamiento 192.168.56.0/24 para representar la zona GREEN o red interna del laboratorio. Desde esta zona se realizan las pruebas de navegación del usuario cliente hacia Internet, obligando a que el tráfico pase por Endian antes de salir a la red externa. Esta configuración es la base para aplicar el proxy HTTP no transparente, ya que permite identificar el segmento desde el cual se originan las solicitudes web.

Figura 36.
Asignación de interfaces GREEN y ORANGE en Endian.

Fuente: Autoría Propia

En esta pantalla se evidencia la asignación de interfaces de red dentro del asistente de configuración de Endian. La zona GREEN queda asociada al segmento interno desde el cual se conectan los usuarios, mientras que la zona ORANGE permanece definida como parte de la segmentación del firewall. Esta separación de interfaces permite que Endian controle el tráfico entre zonas y aplique posteriormente las políticas del proxy HTTP sobre las solicitudes generadas desde la red interna.

Figura 37.
Verificación de conectividad entre el host y Endian.

Fuente: Autoría Propia

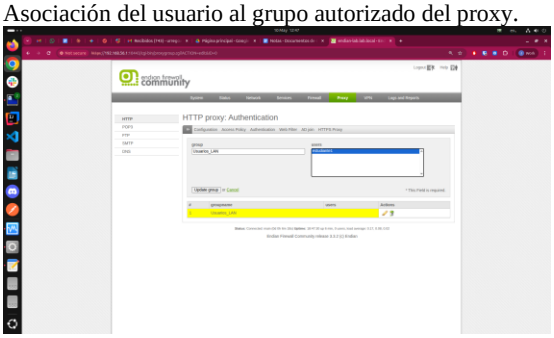
La prueba de conectividad confirma que el host ubicado en la zona GREEN alcanza correctamente la dirección de administración de Endian. Esta validación es necesaria antes de configurar el proxy en el navegador, porque demuestra que el equipo cliente tiene comunicación con el firewall y puede enviar sus solicitudes web para que sean autenticadas, filtradas y reenviadas según la política establecida.

Figura 38.
Configuración del proxy HTTP no transparente en Endian.

Fuente: Autoría Propia

El servicio de proxy HTTP se habilitó en modo no transparente sobre la zona GREEN y escuchando por el puerto 8080. Esta configuración obliga a que el navegador del usuario declare explícitamente la dirección del proxy antes de navegar. Gracias a este modo de operación, Endian puede solicitar credenciales de acceso, identificar al usuario y aplicar reglas de filtrado antes de permitir o denegar la salida hacia Internet.

Figura 39.
Asociación del usuario al grupo autorizado del proxy.



Fuente: Autoría Propia

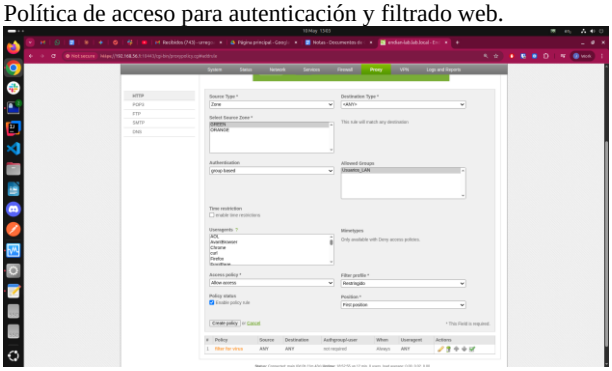
En esta configuración se confirma que el usuario estudiante1 quedó asociado al grupo Usuarios_LAN. Esta asociación permite que la política de acceso del proxy no dependa únicamente de la dirección IP del equipo, sino también de la identidad del usuario autenticado. De esta forma, Endian puede autorizar la navegación solo a usuarios registrados y aplicar reglas comunes al grupo definido.

Figura 40.
Perfil de filtrado con lista negra de dominios.

Fuente: Autoría Propia

Se crea el perfil 'Restringido', que contiene los dominios definidos en la lista negra. Esta lista se evalúa mediante el módulo de filtrado asociado a c-icap, apoyado en el protocolo ICAP, el cual permite integrar servicios externos para inspeccionar o adaptar tráfico HTTP antes de entregar la respuesta al cliente. Cuando el hostname de destino coincide con un dominio bloqueado, la petición es rechazada por la política de acceso configurada en Endian.

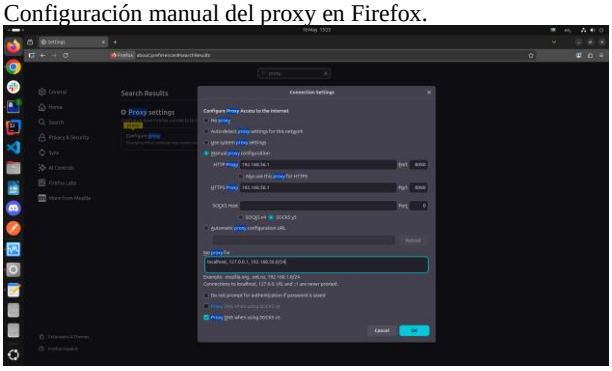
Figura 41.
Política de acceso para autenticación y filtrado web.



Fuente: Autoría Propia

La política de acceso vincula el grupo Usuarios_LAN, el requisito de autenticación y el perfil de filtrado Restringido. Esta regla define el flujo principal de la implementación: primero el usuario debe autenticarse, después el proxy valida su pertenencia al grupo autorizado y finalmente se aplica el filtro por lista negra. Con esta configuración se integran en una sola política el control de identidad y el bloqueo de dominios no permitidos.

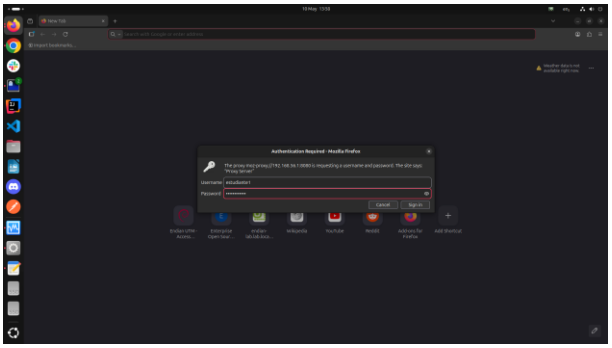
Figura 42.
Configuración manual del proxy en Firefox.



Fuente: Autoría Propia

El navegador Firefox se configuró manualmente para utilizar el proxy HTTP ubicado en 192.168.56.1:8080. Esta evidencia confirma que la implementación es no transparente, ya que el cliente debe indicar de forma explícita el servidor proxy que procesa sus solicitudes. A partir de esta configuración, toda navegación realizada desde el perfil de prueba pasa por Endian antes de llegar a Internet.

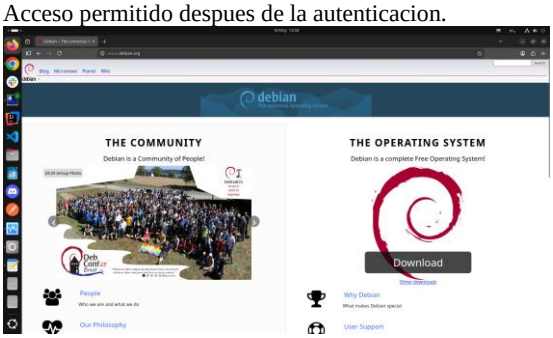
Figura 43.
Solicitud de credenciales del proxy en el navegador.



Fuente: Autoría Propia

Al intentar navegar, Firefox muestra una ventana de autenticación solicitada por el proxy. Este comportamiento confirma que Endian está exigiendo usuario y contraseña antes de permitir la salida del tráfico web. La autenticación es el primer control aplicado por la política, por lo que un usuario no registrado o con credenciales inválidas no debería poder continuar hacia los sitios solicitados.

Figura 44.
Acceso permitido despues de la autenticacion.



Fuente: Autoría Propia

Después de ingresar credenciales válidas, el usuario logra acceder correctamente a un sitio permitido. Esta prueba demuestra que el proxy no bloquea toda la navegación, sino que permite el acceso cuando el usuario está autenticado y el dominio solicitado no pertenece a la lista negra. Por tanto, la política funciona de manera selectiva, autorizando el tráfico válido y manteniendo el control sobre los destinos restringidos.

Figura 45.
Bloqueo de dominio incluido en la lista negra.

Fuente: Autoría Propia

El acceso a www.hotmail.com fue rechazado por el proxy debido a que el dominio coincide con la lista negra configurada en el perfil de filtrado. Esta prueba evidencia que la política también evalúa el destino solicitado antes de permitir la navegación. La respuesta de denegación confirma que el filtro web se encuentra activo y que el bloqueo por dominio funciona correctamente.

Figura 46.
Verificación de servicios del proxy en Endian.

Fuente: Autoría Propia

La verificación por consola confirma que Squid se encuentra activo, que el demonio c-icap atiende el puerto 1344 para apoyar la inspección de contenido mediante ICAP y que el archivo /var/efw/proxy/ncsausers contiene la credencial del usuario en formato hash APR1. Además, se valida que los archivos de ACL de Squid asociados a grupos fueron generados correctamente por la consola web de Endian, lo que confirma la aplicación de la política de autenticación y filtrado.

6 CONCLUSIONES

La instalación y configuración de GNU/Linux Endian Firewall en VirtualBox permitió establecer una infraestructura de seguridad perimetral funcional, segmentando la red en tres zonas claramente definidas: zona verde (LAN 192.168.2.0/24), zona roja (WAN) y zona naranja (DMZ 192.168.1.0/24). La correcta asignación de las interfaces de red a cada zona garantiza que el tráfico entre segmentos sea gestionado exclusivamente por el firewall, eliminando la comunicación directa entre la red interna y los servidores expuestos, lo que constituye el fundamento de cualquier arquitectura de seguridad perimetral robusta bajo plataformas GNU/Linux.

La elección de trabajar con Endian Firewall como opción preferida de GNU/Linux, permitió gracias a un entorno virtual, tener de forma estructurada, implementando NAT, aumentando la seguridad del tráfico de datos en los dispositivos conectados, así también la asignación correcta de la zona verde, y naranja, hizo que al realizar las pruebas dieron resultados adecuados.

La implementación del proxy HTTP no transparente sobre Endian Firewall demostró ser efectiva como mecanismo de control de navegación en redes locales, al combinar tres capas independientes de seguridad: clasificación por zona (capa 3), autenticación de usuario mediante NCSA (capa 7) y filtrado de URL por dominio mediante c-icap (capa 7). Esta arquitectura permite distinguir entre dispositivos pertenecientes a la red

interna y usuarios autorizados dentro de ella, aplicando políticas diferenciadas a cada combinación.

El uso de Endian Firewall es importante ya que actúa como un filtro de seguridad entre la red y el exterior, con esto se evitan amenazas, accesos no autorizados y tráfico malicioso que puede existir en la red de internet. Sin este control, la información queda expuesta a que cualquier dispositivo conectado a la red pueda realizar un ataque , robar información o detener los procesos de la empresa o entidad.

7 REFERENCIAS.

[1] Endian S.r.l., "Endian Firewall Community — Reference Manual", Endian Documentation, 2023. [En línea]. Disponible en: https://docs.endian.com/community/ (Consultado: 29 de abril de 2026).

[2] Koromicha, "Install and configure Endian firewall on VirtualBox", Kifarunix, 2024. [En línea]. Disponible en: https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/ (Consultado: 30 de abril de 2026).

[3] J. Elson y A. Cerpa, "Internet Content Adaptation Protocol (ICAP)", IETF RFC 3507, abr. 2003. [En línea]. Disponible en: https://www.rfc-editor.org/rfc/rfc3507 (Consultado: 2 de mayo de 2026).

[4] E. Limones, "NAT: Qué es y para qué sirve", OpenWebinars.net, 24 jun. 2022. [En línea]. Disponible en: https://openwebinars.net/blog/nat-que-es-y-para-que-sirve/. [Consultado: may. 2026].

[5] Canonical, "Help Ubuntu", Ubuntu, 2023. [En línea]. Disponible en: https://help.ubuntu.com/ (Consultado: 5 de mayo de 2026).

[6] Endian S.r.l., "The firewall menu — Endian UTM 3.2 Reference Manual", Endian Documentation, s.f. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/firewall.html (Consultado: 6 de mayo de 2026).

[7] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952 (Consultado: 12 de mayo de 2026).

[8] GoDaddy, "Apache2: configurar servidor web", GoDaddy, 2025. [En línea]. Disponible en: https://www.godaddy.com/resources/es/crearweb/apache2-configurar-servidor-web (Consultado: 9 de mayo de 2026).

[9] Linux Professional Institute, "LPIC-1 Exam 101 – Tema 101: Arquitectura del sistema", LPI, 2022. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/101/ (Consultado: 10 de mayo de 2026).

[10] D. Ghimiray, "¿Qué es un servidor proxy y cómo funciona?", AVG, 23 de marzo de 2023. [En línea]. Disponible en: https://www.avg.com/es/signal/proxy-server-definition (Consultado: 8 de mayo de 2026).