IMPLEMENTACIÓN DE SEGURIDAD EN GNU/LINUX MEDIANTE ENDIAN FIREWALL

Alvaro Africano Mejia
aafricanom@unadvirtual.edu.co
Elkin Octavio Araque Gallardo
eoaraqueg@unadvirtual.edu.co
Fran Yeiler Sagra Sanchez
fysanchezs@unadvirtual.edu.co
Jeydent Julieht Martínez Jiménez
jjmartinezji@unadvirtual.edu.co
Jesus Orlando Martinez
jomartinezd@unadvirtual.edu.co

RESUMEN—*Este artículo presenta la implementación de una infraestructura de seguridad en GNU/Linux mediante Endian Firewall, utilizando VirtualBox como entorno de virtualización. El desarrollo se organizó en cinco temáticas: configuración de la instancia GNU/Linux Endian en VirtualBox, configuración NAT, habilitación de servicios en la zona DMZ, implementación de reglas de filtrado inter-zona y configuración de un proxy HTTP no transparente. Para ello, se segmentó la red en tres zonas principales: verde o LAN, naranja o DMZ y roja o WAN, con el propósito de controlar el tráfico, reducir la exposición de los servicios internos y validar el comportamiento de las políticas de seguridad aplicadas. Los resultados evidencian que Endian Firewall permite administrar reglas de conectividad, traducción de direcciones, reenvío de puertos, autenticación de usuarios y filtrado de contenido web, fortaleciendo la seguridad perimetral en un entorno virtualizado.*

PALABRAS CLAVE—Endian Firewall, filtrado inter-zona, GNU/Linux, NAT.

1 INTRODUCCIÓN

La seguridad de una red no depende únicamente de conectar equipos y permitir la comunicación entre ellos, sino de definir con precisión qué tráfico puede circular, desde dónde puede hacerlo y en qué condiciones debe ser permitido o bloqueado. En los entornos actuales, donde la información representa un activo estratégico para las organizaciones, una configuración deficiente de la infraestructura puede facilitar accesos no autorizados, exposición de servicios internos y pérdida de control sobre los recursos tecnológicos.

En este contexto, los firewalls cumplen un papel esencial dentro de la seguridad perimetral, ya que permiten separar redes, controlar paquetes, aplicar reglas de acceso y reducir la superficie de exposición frente a amenazas externas o internas. Endian Firewall es una solución basada en GNU/Linux que permite implementar este tipo de controles mediante zonas de seguridad, reglas NAT, reenvío de puertos, filtrado inter-zona y servicios complementarios como proxy HTTP [1].

El presente artículo documenta la implementación de una infraestructura virtualizada con Endian Firewall, orientada a segmentar una red en tres zonas principales: LAN, DMZ y WAN. La zona verde representa la red interna o LAN; la zona naranja corresponde a la DMZ, donde se ubican servicios que pueden ser publicados de forma controlada; y la zona roja representa la red externa o WAN. Esta arquitectura permite simular un escenario de seguridad en el que los servicios internos no quedan expuestos directamente, sino protegidos mediante políticas de firewall.

El objetivo del artículo es describir la configuración y validación de Endian Firewall en un entorno GNU/Linux virtualizado, conservando el desarrollo en cinco temáticas: configuración inicial de la instancia, NAT, servicios DMZ, filtrado inter-zona y proxy HTTP no transparente. A partir de estas temáticas se analiza cómo la segmentación, las reglas de tráfico y las pruebas de conectividad permiten fortalecer la seguridad de una red controlada.

2 METODOLOGÍA DE IMPLEMENTACIÓN

La implementación se realizó en un entorno virtualizado mediante VirtualBox, utilizando Endian Firewall como sistema principal de seguridad perimetral y máquinas GNU/Linux como cliente y servidor. La infraestructura fue diseñada para representar una red segmentada en tres zonas: la zona verde, asociada a la LAN; la zona naranja, destinada a la DMZ; y la zona roja, correspondiente a la WAN. Esta división permitió establecer un escenario controlado para configurar reglas de conectividad, traducción de direcciones, publicación de servicios y filtrado de tráfico.

El procedimiento se organizó en cinco temáticas. En la primera, se configuró la instancia de GNU/Linux Endian en VirtualBox, incluyendo la creación de la máquina virtual, asignación de adaptadores de red, instalación del sistema y definición de las zonas verde, naranja y roja. En la segunda, se implementaron reglas NAT para permitir la salida de las redes internas hacia la WAN y el reenvío de puertos hacia servicios ubicados en la DMZ. En la tercera, se habilitaron servicios como HTTP y FTP sobre el servidor ubicado en la zona DMZ, con el propósito de validar el acceso controlado desde las zonas autorizadas.

En la cuarta temática, se configuraron reglas de filtrado inter-zona para definir explícitamente qué tráfico podía pasar entre LAN, DMZ y WAN. Esta fase incluyó pruebas de conectividad, acceso a servicios y

verificación mediante comandos del sistema como iptables. Finalmente, en la quinta temática se implementó un proxy HTTP no transparente, con autenticación local, grupos de usuarios, perfiles de filtrado y listas negras para controlar el acceso a determinados sitios web.

La validación de la infraestructura se llevó a cabo mediante pruebas de conectividad, acceso HTTP y FTP, comprobación de NAT, verificación de Port Forwarding, revisión de reglas activas en el kernel y prueba de bloqueo de navegación mediante proxy. Estas pruebas permitieron comprobar que las configuraciones aplicadas en Endian Firewall funcionaban de acuerdo con el diseño de seguridad planteado.

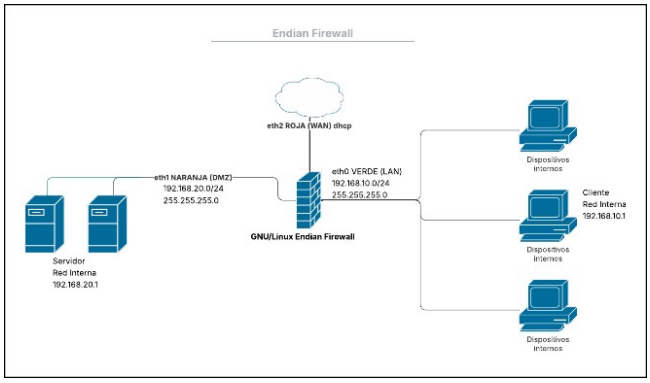
3 DESARROLLO DE LAS TEMÁTICAS

3.1 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX, TARJETAS DE RED E INSTALACIÓN EFECTIVA

La primera temática correspondió a la preparación del entorno virtualizado y la instalación de Endian Firewall. Para ello, se definió una arquitectura de red compuesta por tres zonas de seguridad: verde, naranja y roja. La zona verde fue asignada a la LAN, la zona naranja a la DMZ y la zona roja a la WAN. Esta organización permitió separar el tráfico interno, los servicios publicados y la comunicación hacia la red externa.

Figura 1.

Diagrama de red con Endian Firewall

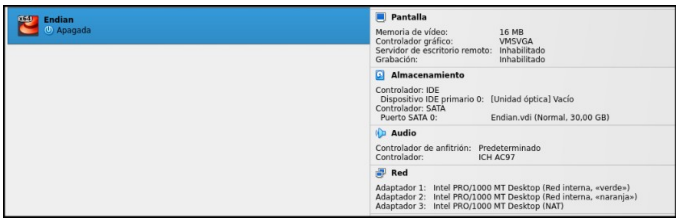


Fuente: Autoría propia

En VirtualBox se creó la máquina virtual correspondiente a Endian Firewall y se configuraron tres adaptadores de red. El primer adaptador se destinó a la zona verde, el segundo a la zona naranja y el tercero a la zona roja. La zona verde se configuró como red interna para conectar el cliente de la LAN; la zona naranja se configuró como red interna para alojar el servidor en la DMZ; y la zona roja se configuró mediante NAT para simular la salida hacia la WAN.

Figura 2.

Adaptadores de red configurados en Endian Firewall



Fuente: Autoría propia

Posteriormente, se configuraron los adaptadores de red de las máquinas GNU/Linux utilizadas como cliente y servidor. El equipo cliente fue asociado a la zona verde, mientras que el servidor fue asociado a la zona naranja. Esta configuración permitió que cada máquina virtual cumpliera un rol específico dentro de la infraestructura de red.

Figura 3.

Adaptador de red configurado para Debian Desktop

Fuente: Autoría propia

El adaptador para la zona NARANJA que es el Debian Server se especifica como red interna y se especifica que quede bien ajustada la zona para evitar inconvenientes más adelante. Es esencial que los nombres si son en mayúscula o en minúscula se escriban igual igualmente para evitar problemas y que los reconozca.

Figura 4.

Adaptador de red configurado para Debian Server

Fuente: Autoría propia

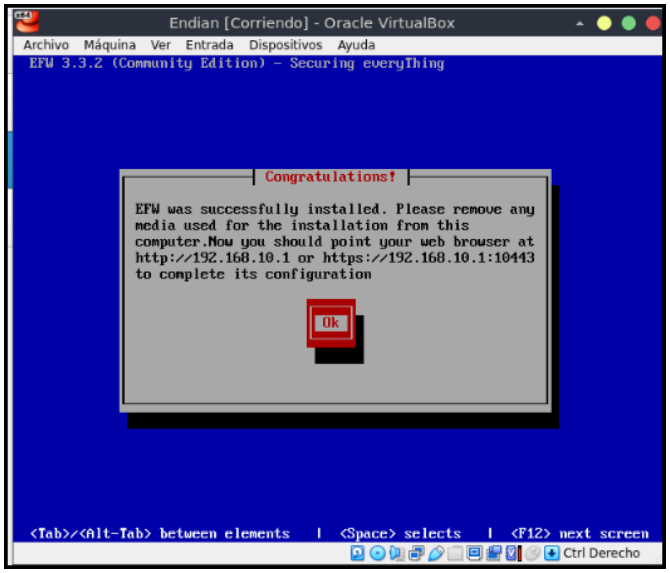
Durante la instalación de Endian Firewall se seleccionó el idioma disponible, se preparó el disco virtual y se definió la dirección IP de la zona verde. Para esta zona se asignó la dirección 192.168.10.1 con

máscara 255.255.255.0. Esta IP permitió posteriormente acceder a la interfaz web de administración desde el equipo cliente ubicado en la LAN.

Luego de la instalación, Endian Firewall mostró las zonas activas y la información de red configurada. Desde el navegador del cliente se accedió a la interfaz de administración mediante la dirección correspondiente a la zona verde. En el asistente inicial se aceptó la licencia, se omitió la restauración de copia de seguridad, se establecieron credenciales administrativas y se configuró el modo de red en enrutamiento.

Figura 5.

Proceso de instalación de Endian Firewall

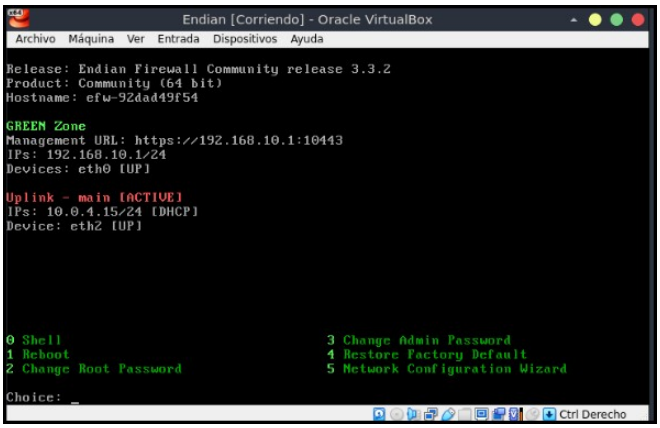


Fuente: Autoría propia

Una vez completado el asistente, la interfaz web de Endian Firewall quedó disponible para la administración de reglas, servicios, NAT, proxy y tráfico entre zonas. Como validación inicial, se realizaron pruebas de conectividad mediante el comando ping hacia las direcciones de las interfaces configuradas.

Figura 6.

Consola inicial de Endian Firewall

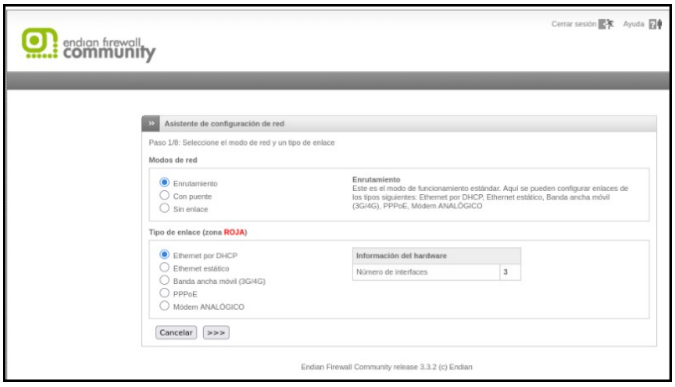


Fuente: Autoría propia

La zona ROJA que se configura como la WAN debe dejarse en DHCP, en la imagen se aprecia las diferentes opciones que hay pero se selecciona la primera, también se observa el número de interfaces que hay en el momento siendo un total de 3, una para cada una de las zonas que se están trabajando en el momento.

Figura 7.

Interfaz web de administración de Endian Firewall

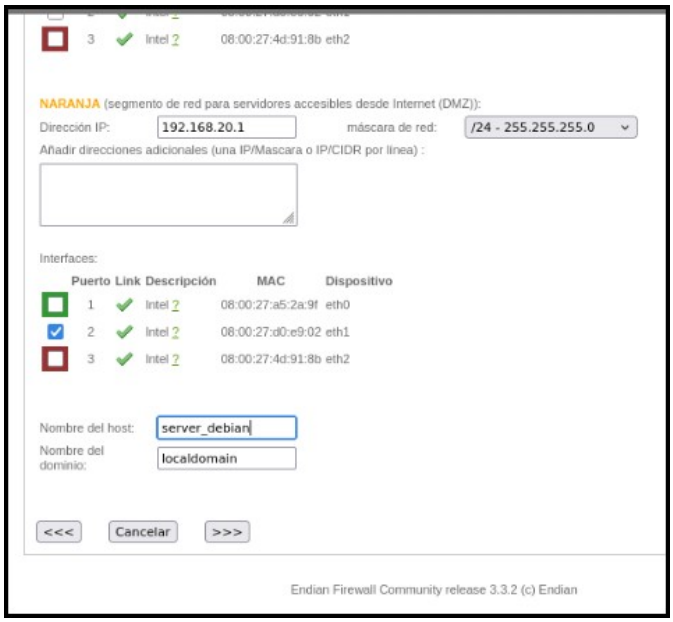


Fuente: Autoría propia

Posteriormente, se configuró la zona naranja o DMZ, asignando la dirección 192.168.20.1 con máscara 255.255.255.0. Esta zona fue utilizada para conectar el servidor GNU/Linux destinado a alojar servicios como HTTP y FTP. La zona roja se mantuvo mediante DHCP, asociada al adaptador NAT de VirtualBox, para simular la conectividad hacia la WAN.

Figura 8.

Configuración de la zona naranja en Endian Firewall

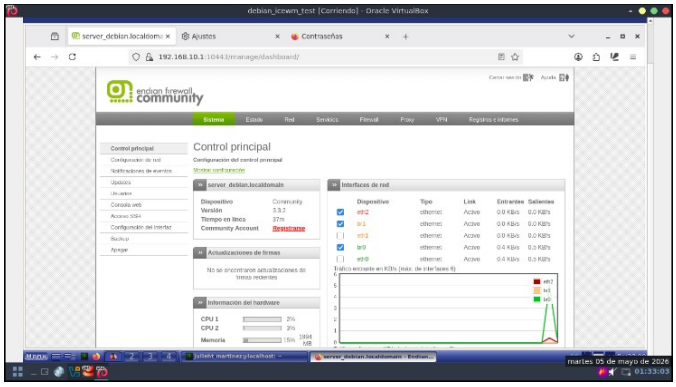


Fuente: Autoría propia

Una vez completado el asistente, la interfaz web de Endian Firewall quedó disponible para la administración de reglas, servicios, NAT, proxy y tráfico entre zonas. Como validación inicial, se realizaron pruebas de conectividad mediante el comando ping hacia las direcciones de las interfaces configuradas.

Figura 9.

Panel principal de Endian Firewall Community

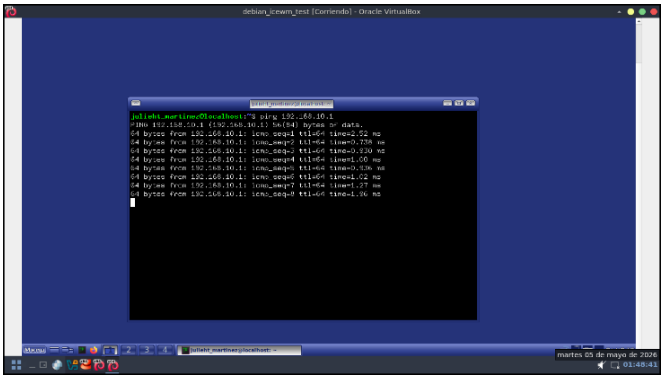


Fuente: Autoría propia

En el entorno gráfico que es Debian Desktop se hace mediante uso de la terminal o shell las pruebas con el comando ping y la IP a la que se hace el envió de los datos, en la imagen se aprecia que efectivamente funciona y hay envió, en dado caso que falle debe haber un error que pudo cometerse en los ajustes que se realizaron con anterioridad.

Figura 10.

Comprobación de conectividad hacia 192.168.10.1 desde Debian Desktop

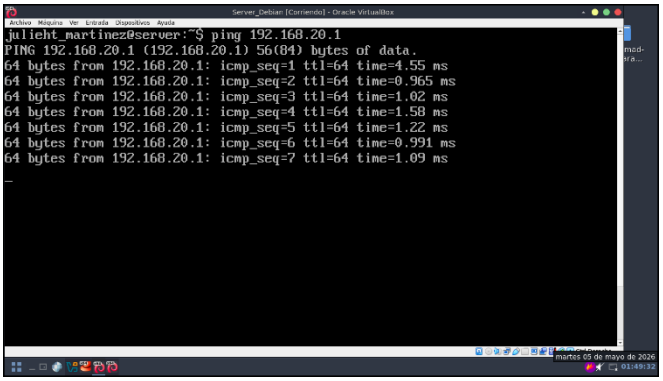


Fuente: Autoría propia

Igualmente para Debian Server con ayuda del comando ping y la IP en este caso 192.168.20.1 se observa que hay un envió de datos y que las conexiones y los ajustes realizados se hicieron de manera adecuada y todo funciona como se esperaba. Como en el servidor no hay entorno gráfico solo se inicia sesión y se ingresan los comandos que se necesiten.

Figura 11.

Comprobación de conectividad hacia 192.168.20.1 desde Debian Server



Fuente: Autoría propia

Esta primera temática permitió establecer la base de la infraestructura, dejando habilitadas las zonas necesarias para las configuraciones posteriores de NAT, servicios DMZ, filtrado inter-zona y proxy HTTP. El sistema operativo usado para la implementación es Debian GNU/Linux y Ubuntu, siguiendo la guía oficial de instalación para cada opción [2].

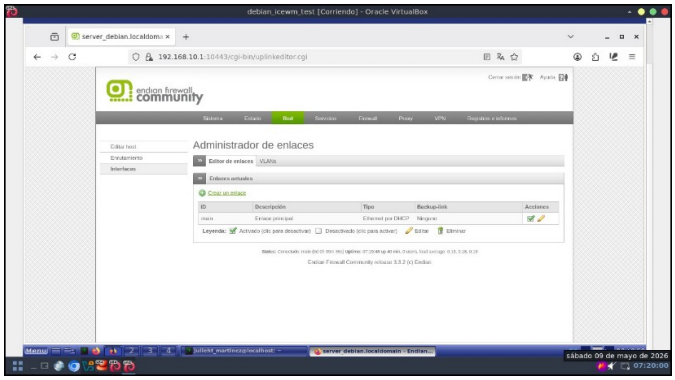
3.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La segunda temática consistió en la configuración de reglas NAT para permitir que las redes internas pudieran comunicarse con la zona externa de forma controlada. NAT, o Network Address Translation, permite traducir direcciones IP privadas para que los equipos ubicados

en redes internas puedan acceder a la WAN utilizando la interfaz externa del firewall.

Figura 12.

Estado de la interfaz WAN mediante DHCP en Endian Firewall



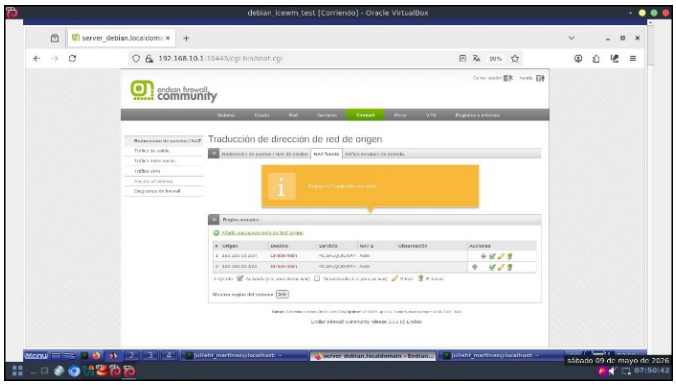
Fuente: Autoría propia

En primer lugar, se validó la configuración de NAT de salida desde la zona verde hacia la zona roja. Esta regla permite que los equipos de la LAN, pertenecientes a la red 192.168.10.0/24, puedan salir hacia la WAN mediante la dirección IP asignada a la interfaz roja de Endian Firewall. Este proceso corresponde al mecanismo de Source NAT o enmascaramiento.

También se revisó la salida desde la zona naranja hacia la zona roja. Esta configuración permite que los servidores ubicados en la DMZ puedan acceder a Internet para tareas como actualizaciones, sincronización o descarga de paquetes, sin quedar expuestos directamente a la red externa.

Figura 13.

Aplicación de políticas NAT de origen en Endian Firewall

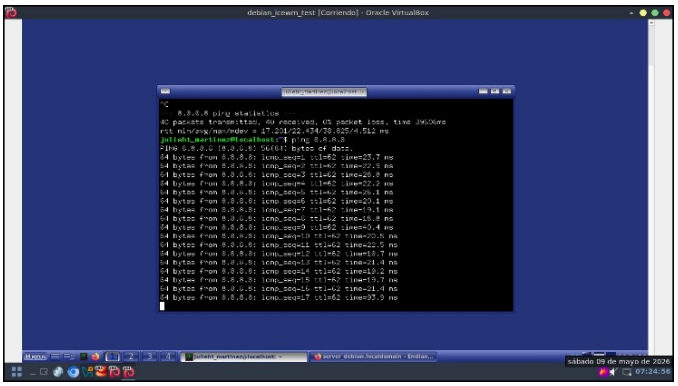


Fuente: Autoría propia

Además de la traducción de salida, se configuró Port Forwarding o Destination NAT para permitir el acceso controlado desde la WAN hacia servicios específicos alojados en la DMZ. En este caso, se consideraron servicios como HTTP en el puerto 80 y FTP en el puerto 21, redirigidos hacia el servidor ubicado en la zona naranja.

Figura 14.

Comprobación de navegación desde la zona verde hacia la WAN

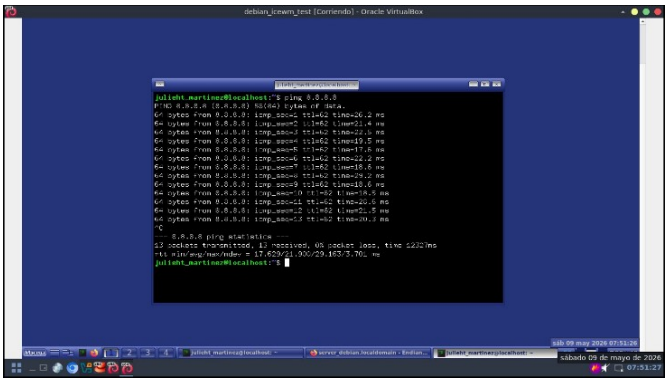


Fuente: Autoría propia

Si la regla configurada queda realizada de manera adecuada en la terminal se muestra el resultado al ingresar el comando ping 8.8.8.8 mostrando el envió correcto de datos, se puede apreciar desde la LAN hacia la WAN, siendo desde la zona VERDE a la zona ROJA. Al terminar el comando se muestra el total de paquetes enviados y si hay errores en el envió los muestra.

Figura 15.

Análisis de latencia y pérdida de paquetes en la comunicación LAN-WAN



Fuente: Autoría propia

En la tabla 1 se observan las reglas NAT configuradas y verificadas en el firewall, se incluyen las diferentes reglas de traducción de las direcciones SNAT para poder permitir la salida de las redes internas hacia el Internet y de las reglas DNAT usadas para el redireccionamiento de los puertos hacia los servicios que estan alojados en la DMZ.

Tabla 1.

REGLAS NAT VERIFICADAS

Origen	Destino	Tipo de regla	Estado
192.168.10.0/24	WAN, zona roja	SNAT, Masquerade	Activo
192.168.20.0/24	WAN, zona roja	SNAT, Masquerade	Activo
WAN	DMZ, puerto 80	Port Forwarding, DNAT	Verificado
WAN	DMZ, puerto 21	Port Forwarding, DNAT	Verificado

Nota. Esta tabla muestra cuales son las reglas NAT configuradas y las verificadas en la red, incluyen las reglas SNAT para poder permitir la salida de las diferentes subredes internas dirigidas hacia el Internet mediante el enmascaramiento. Fuente. Autoría Propia

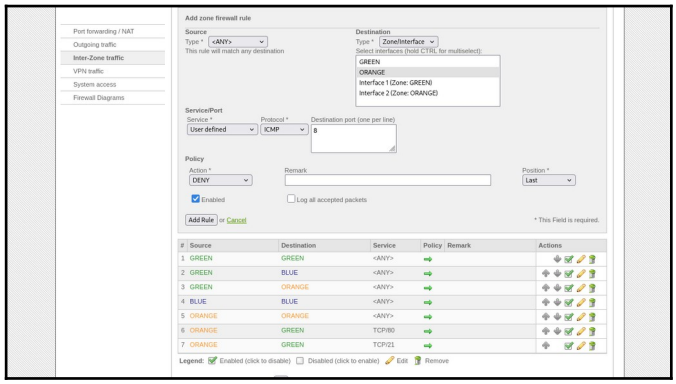
La configuración NAT permitió que la infraestructura interna conservara direcciones privadas, mientras Endian Firewall administraba la comunicación hacia la red externa. Asimismo, el reenvío de puertos permitió publicar servicios específicos sin exponer completamente la red interna. Esta temática fue fundamental para establecer conectividad controlada entre LAN, DMZ y WAN. Para realizar la configuración de las reglas NAT y el control de tráfico entre las zonas se realizó haciendo uso de la documentación oficial de Endian [1].

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

La tercera temática se orientó a documentar la configuración de servicios y reglas asociadas al tráfico entre la zona DMZ y la red interna. En este escenario, la zona naranja u ORANGE corresponde a la DMZ, mientras que la zona verde o GREEN corresponde a la LAN. Por esta razón, la configuración registrada en Endian Firewall permitió analizar el comportamiento del tráfico inter-zona, especialmente en relación con los servicios HTTP, FTP y el bloqueo de solicitudes ICMP.

Figura 16.

Configuración de regla ICMP con acción DENY

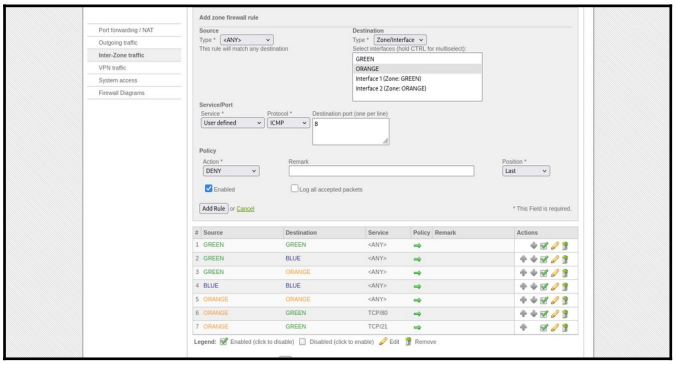


Fuente: Autoría propia

Se accedió a la sección Inter-Zone Traffic de Endian Firewall con el fin de revisar las reglas existentes y registrar las políticas aplicadas entre las zonas ORANGE y GREEN. En esta sección se configuraron reglas para permitir tráfico TCP asociado a los servicios HTTP y FTP, de acuerdo con la evidencia disponible en la tabla de reglas del firewall.

Figura 17.

Reglas HTTP y FTP configuradas entre zonas

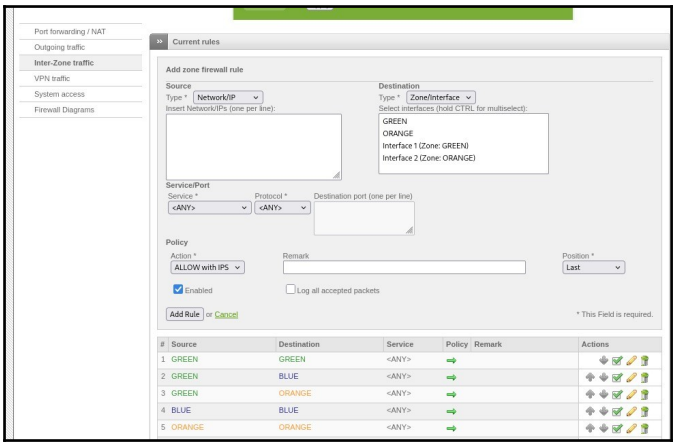


Fuente: Autoría propia

En la imagen se muestran las reglas personalizadas para la Inter-Zone Traffic mediante la interfaz web de Endian Direwall desde el entorno gráfico, dando una mejor visualización y comprensión de las mismas. Se observan las diferentes zonas, los destinatarios de estas.

Figura 18.

Tabla de reglas personalizadas en Inter-Zone Traffic

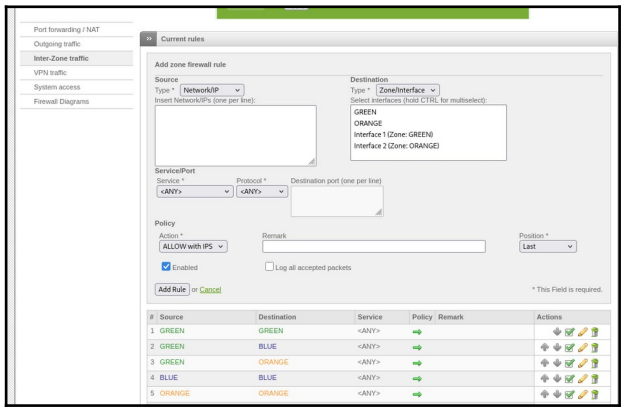


Fuente: Autoría propia

También se configuró una regla para denegar tráfico ICMP tipo 8, correspondiente a solicitudes echo request utilizadas por el comando ping. Esta medida permitió limitar el reconocimiento de equipos entre zonas y reducir la exposición de la infraestructura frente a pruebas de exploración innecesarias.

Figura 19.

Formulario para bloqueo de tráfico ICMP hacia la DMZ

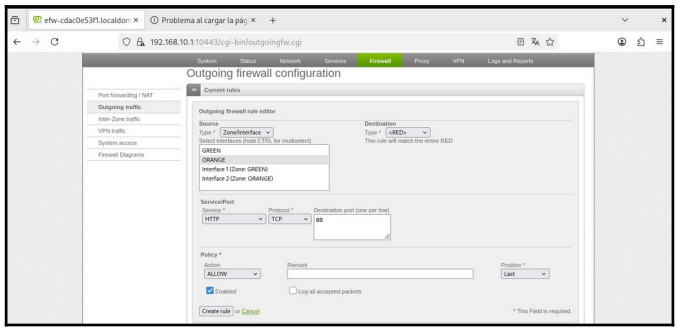


Fuente: Autoría propia

En la sección Outgoing Traffic se establecieron reglas de salida para permitir tráfico HTTP desde las zonas internas hacia la zona roja. Esta configuración complementó el acceso a servicios externos y permitió validar la navegación desde las máquinas autorizadas.

Figura 20.

Regla HTTP en Outgoing Traffic hacia la zona roja



Fuente: Autoría propia

En la Tabla 2 se presenta la configuración realizada de las reglas establecidas de tráfico entre las diferentes zonas (Inter-Zone Traffic) que se implementan en el firewall, tambíen mostrando los diferentes permisos y las restricciones que se establen para poder controlar la comunicación entre las diferentes zonas de la red y así poder mejorar la seguridad del sistema.

Tabla 2.

REGLAS CONFIGURADAS EN INTER-ZONE TRAFFIC

Regla	Origen	Destino	Servicio	Acción
1	ORANGE	GREEN	TCP/80, HTTP	ALLOW
2	ORANGE	GREEN	TCP/21, FTP	ALLOW
3	ANY	ORANGE	ICMP/8	DENY

Nota. Etabla muestra las reglas configuradas en el tráfico para las zonas de la red, permite el acceso de HTTP y FTP desde la zona ORANGE hacia la zona GREEN, mientras que se bloquean las solicitudes de ICMP que provienen de cualquier origen, hacia la zona ORANGE para poder reforzar la seguridad de la red.

De acuerdo con la evidencia disponible, las reglas registradas permitieron tráfico HTTP y FTP desde ORANGE hacia GREEN y bloquearon ICMP hacia ORANGE. Por tanto, esta temática no se presenta como una validación de acceso desde LAN hacia DMZ, sino como una documentación del sentido real del tráfico configurado en Endian Firewall. Esta precisión evita contradicciones entre el texto, las figuras y la tabla de reglas.

Figura 21.

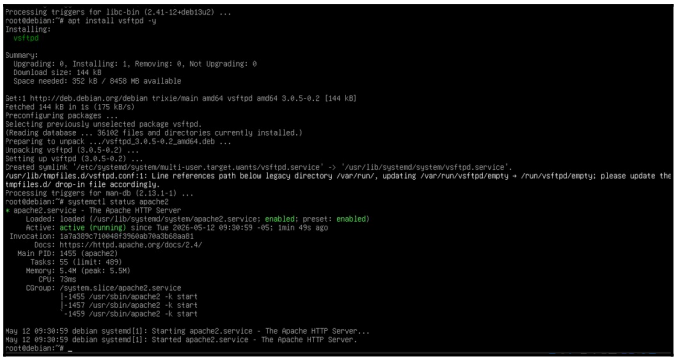
Instalación del servidor web Apache2 en Debian Server

Fuente: Autoría propia

Se aprecia en la figura 22 el proceso de la instalación del servicio FTP mediante el uso de vsftpd y luego la verificación de su adecuado funcionamiento en la zona DMZ, esto permite comprobar que haya la disponibilidad y el acceso a los servicios que se configuran en el servidor.

Figura 22.

Instalación de vsftpd y verificación de servicios en la DMZ

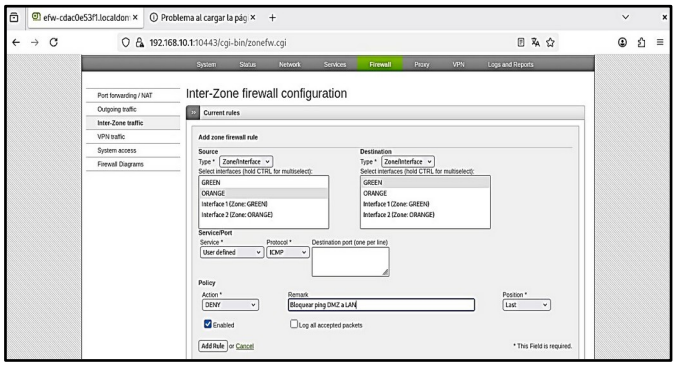


Fuente: Autoría propia

Finalmente, se verificó el bloqueo ICMP mediante pruebas de conectividad. La respuesta Destination Host Unreachable permitió comprobar que la política de denegación estaba afectando el tráfico correspondiente, según la regla configurada en Endian Firewall.

Figura 23.

Regla ICMP con comentario de bloqueo hacia la DMZ

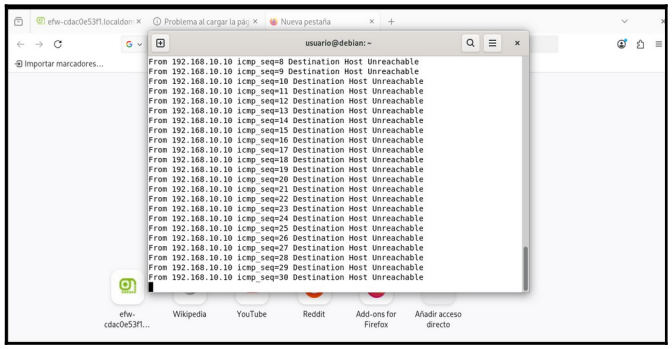


Fuente: Autoría propia

Se observa que hay prueba de conectividad mediante el uso del comando ping hacia la zona ORANGE, y se evidencia el bloqueo configurado en el firewall esto cuando muestra el mensaje “Destination Host Unreachable”, por lo que se confirma el funcionamiento adecuado de las reglas de seguridad que se implementaron.

Figura 24.

Prueba de ping bloqueado con respuesta Destination Host Unreachable



Fuente: Autoría propia

Esta temática permitió evidenciar que la seguridad de una DMZ no consiste solamente en alojar servicios, sino en definir con precisión qué protocolos se permiten y cuáles deben ser restringidos. La configuración y la verificación para los parámetros de hardware y red se hace con ayuda de los contenidos de certificación LPIC-1 [3].

3.4 TEMÁTICA 4: IMPLEMENTACIÓN DE REGLAS DE FILTRADO INTER-ZONA EN ENDIAN FIREWALL

La cuarta temática abordó la configuración de reglas de filtrado inter-zona en Endian Firewall. A diferencia de NAT, que se encarga de traducir direcciones IP, el filtrado inter-zona determina si un paquete puede cruzar de una zona a otra o si debe ser bloqueado. Por esta razón, esta etapa resulta crítica dentro de la seguridad perimetral, ya que establece el control efectivo del flujo de tráfico entre LAN, DMZ y WAN.

3.4.1 CREACIÓN DE REGLAS INTER-ZONE TRAFFIC

Desde la interfaz web de Endian Firewall se accedió a la sección Firewall y posteriormente a Tráfico entre zonas. Allí se revisaron las reglas existentes y se crearon políticas específicas para permitir los servicios necesarios hacia la zona naranja.

Figura 25.

Panel de Endian Firewall en la sección Tráfico entre zonas

Fuente: Autoría propia

La primera regla permitió tráfico HTTP desde la zona verde hacia la zona naranja, utilizando el puerto TCP/80. Esta regla permitió que el cliente ubicado en la LAN pudiera acceder al servidor web alojado en la DMZ.

Figura 26.

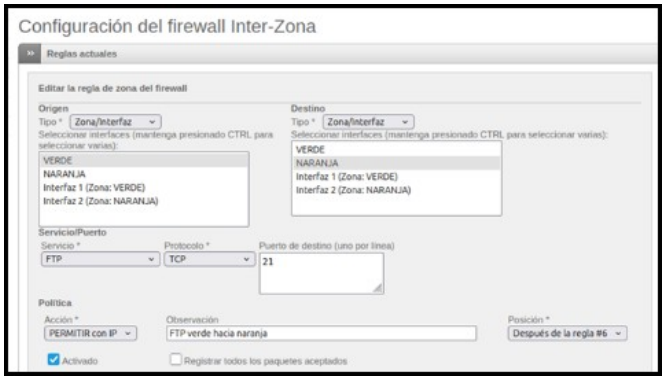
Configuración de la regla HTTP TCP/80 desde la zona verde hacia la zona naranja

Fuente: Autoría propia

La segunda regla permitió tráfico FTP desde la zona verde hacia la zona naranja mediante el puerto TCP/21. Esta política se utilizó para validar la conexión hacia el servicio FTP instalado en el servidor ubicado en la DMZ.

Figura 27.

Configuración de la regla FTP TCP/21 desde la zona verde hacia la zona naranja

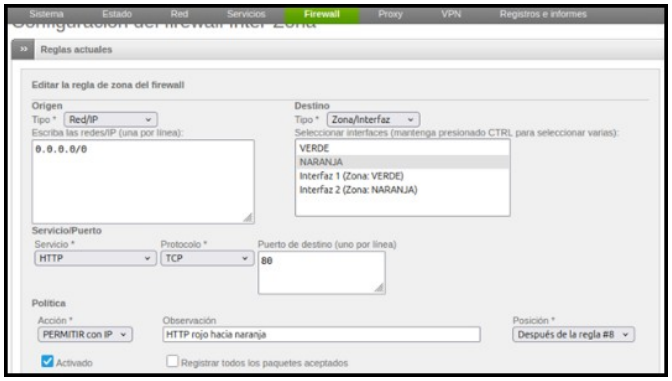


Fuente: Autoría propia

La tercera regla permitió tráfico HTTP desde cualquier origen hacia la zona naranja. Esta configuración trabajó en conjunto con el Port Forwarding definido en la temática NAT, permitiendo que las solicitudes dirigidas desde la WAN al puerto correspondiente fueran redirigidas hacia el servidor interno.

Figura 28.

Configuración de la regla HTTP desde cualquier origen hacia la zona naranja

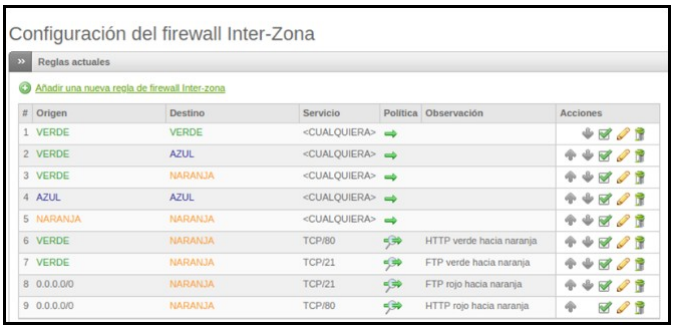


Fuente: Autoría propia

La cuarta regla permitió tráfico FTP desde cualquier origen hacia la zona naranja. Después de aplicar los cambios, Endian Firewall mostró la tabla de reglas activas, donde se evidenció que las políticas agregadas quedaron habilitadas para procesar tráfico entre zonas.

Figura 29.

Tabla de reglas inter-zona creadas y activas



Fuente: Autoría propia

3.4.2 PRUEBAS DE CONECTIVIDAD ENTRE ZONAS

Para comprobar el funcionamiento de las reglas, se realizaron pruebas de acceso a los servicios HTTP y FTP. Desde el Desktop ubicado en la zona verde se accedió al servidor de la DMZ mediante HTTP, obteniendo la página por defecto de Apache2. Esta prueba confirmó que el servicio web estaba disponible desde la zona autorizada.

Figura 30.

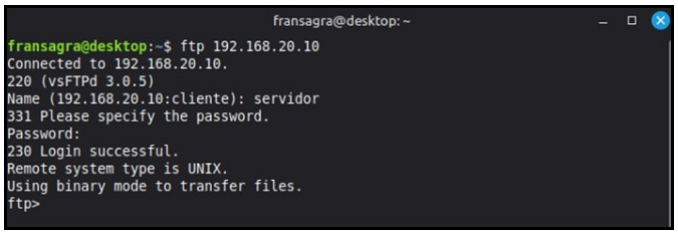
Navegador del Desktop mostrando Apache al acceder a 192.168.20.10

Fuente: Autoría propia

De igual manera, se verificó la conexión FTP hacia el servidor ubicado en la DMZ. La autenticación exitosa confirmó que la regla asociada al puerto TCP/21 permitía el acceso al servicio configurado.

Figura 31.

Terminal del Desktop con conexión FTP exitosa hacia 192.168.20.10

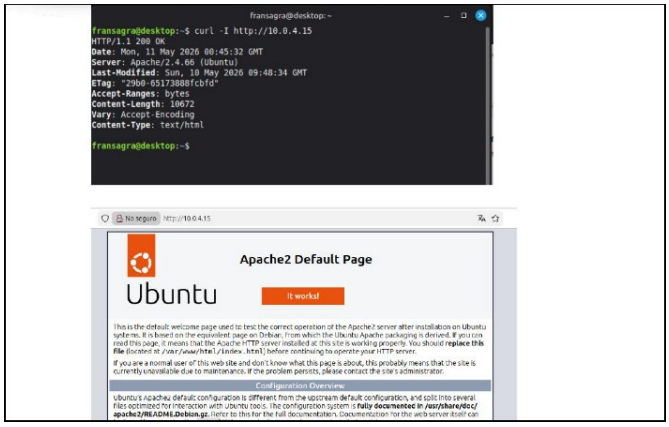


Fuente: Autoría propia

También se realizaron pruebas desde la zona roja hacia la DMZ mediante Port Forwarding. El acceso HTTP evidenció respuesta satisfactoria del servidor web interno, mientras que la prueba FTP confirmó la disponibilidad del servicio publicado desde la DMZ.

Figura 32.

Acceso HTTP desde la WAN hacia la DMZ mediante Port Forwarding

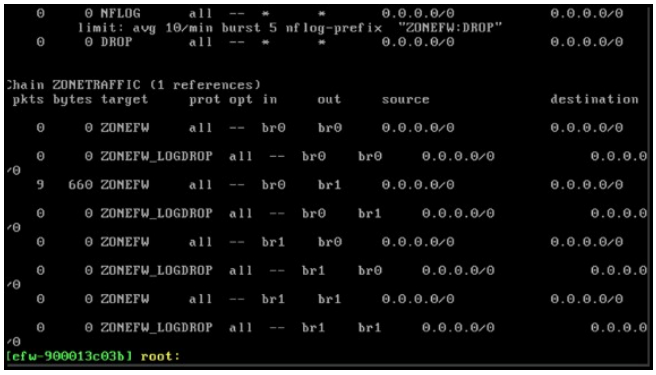


Fuente: Autoría propia

Se aprecia la imagen con la conexión FTP que se realiza desde la zona ROJA (WAN), hacia el servidor que se encuentra ubicado en la DMZ zona NARANJA, se verifica el funcionamiento de las reglas de redireccionamiento y el acceso configurado en el firewall.

Figura 33.

Conexión FTP entrante desde la zona roja hacia la DMZ



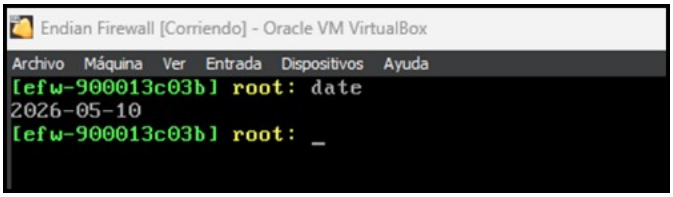
Fuente: Autoría propia

3.4.3 VERIFICACIÓN EN EL KERNEL CON IPTABLES

Para confirmar que las reglas creadas desde la interfaz gráfica se aplicaron en el sistema, se accedió al shell de Endian Firewall y se ejecutaron comandos de verificación. Primero se revisó la fecha del sistema para documentar el momento de la prueba.

Figura 34.

Fecha y hora del sistema Endian al momento de la verificación

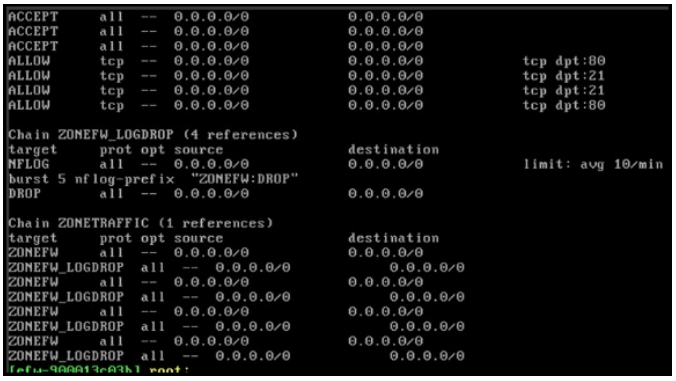


Fuente: Autoría propia

Posteriormente, se ejecutó iptables -L -n para observar las reglas activas en la cadena FORWARD. Allí se identificaron entradas asociadas a los puertos 80 y 21, lo que confirmó la existencia de políticas de reenvío para los servicios HTTP y FTP.

Figura 35.

Salida de iptables -L -n con las reglas FORWARD activas

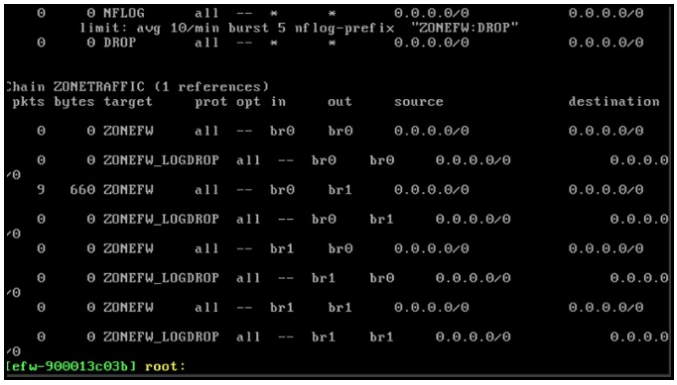


Fuente: Autoría propia

Finalmente, se ejecutó iptables -L -n -v para revisar los contadores de paquetes y bytes procesados. La presencia de contadores superiores a cero permitió comprobar que las reglas no solo estaban registradas, sino que habían procesado tráfico real durante las pruebas.

Figura 36.

Salida de iptables -L -n -v mostrando contadores de paquetes procesados



Fuente: Autoría propia

La verificación con iptables fortaleció la validez técnica de la implementación, ya que permitió comprobar que las políticas configuradas en la interfaz web se reflejaron en las reglas activas del sistema operativo.

3.5 TEMÁTICA 5: IMPLEMENTACIÓN DE PROXY HTTP NO TRANSPARENTE EN ENDIAN FIREWALL

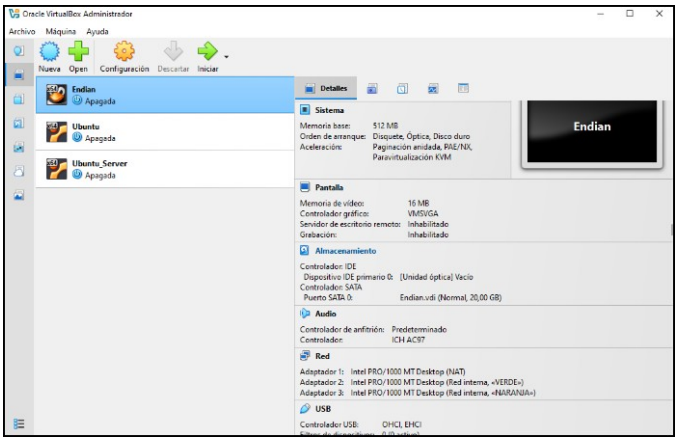
La quinta temática consistió en la implementación de un proxy HTTP no transparente en Endian Firewall. Esta configuración agregó una capa de control sobre la navegación web, permitiendo aplicar autenticación de usuarios, perfiles de filtrado y listas negras de sitios restringidos.

3.5.1 INFRAESTRUCTURA Y CONFIGURACIÓN INICIAL

La infraestructura utilizada mantuvo la organización de máquinas virtuales en VirtualBox, incluyendo Endian Firewall, un equipo Desktop y un servidor GNU/Linux. Los adaptadores de red se configuraron para representar las zonas roja, verde y naranja, de acuerdo con el esquema de segmentación utilizado durante el desarrollo del artículo.

Figura 37.

Máquinas virtuales configuradas en VirtualBox

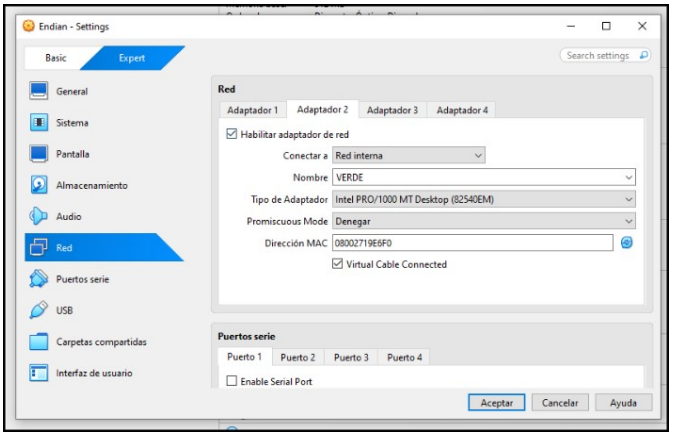


Fuente: Autoría propia

Se presenta la configuración para el adaptadore de red de la zona VERDE y la zona NARANJA en la VirtualBox, para permitir y establecer la adecuada comunicación entre las diferentes zonas para la red virtual implementada.

Figura 38.

Configuración de adaptadores VERDE y NARANJA en VirtualBox

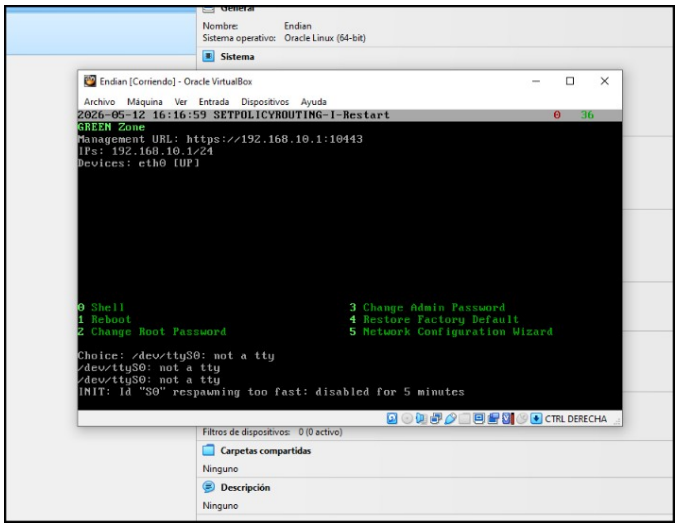


Fuente: Autoría propia

Al iniciar Endian Firewall se confirmó la disponibilidad de la zona verde con la dirección correspondiente para acceder al panel de administración. Desde el navegador del Desktop se ingresó a la interfaz web y se verificó la conectividad con el firewall.

Figura 39.

Consola de Endian con zona verde activa

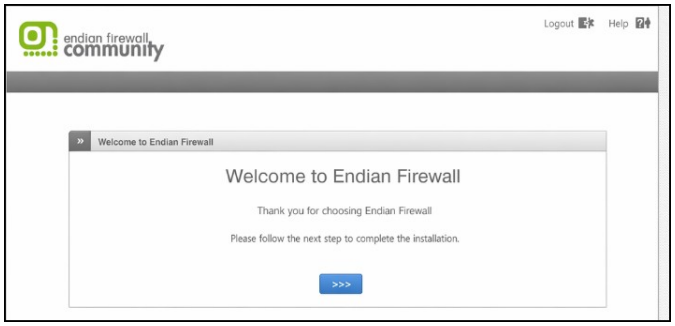


Fuente: Autoría propia

Se observa el panel de bienvenida de la interfaz web de Endian Firewall, posterior a la configuración e instalación, desde el cual se puede administrar las funciones de seguridad, la red y el monitoreo del firewall. Así como apreciar las demás opciones que brinda la interfaz para Endian.

Figura 40.

Panel de bienvenida de Endian Firewall Community

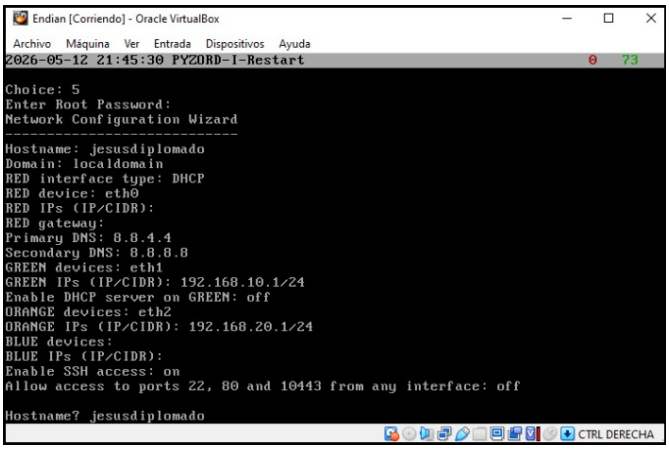


Fuente: Autoría propia

Se observa la configuración completa de la red desde la consola de Endian Firewall, se incluye la asignación de las interfaces y los parámetros que son necesarios para el funcionamiento adecuado de las zonas de la red y la comunicación entre estas.

Figura 41.

Configuración de red completa en la consola de Endian



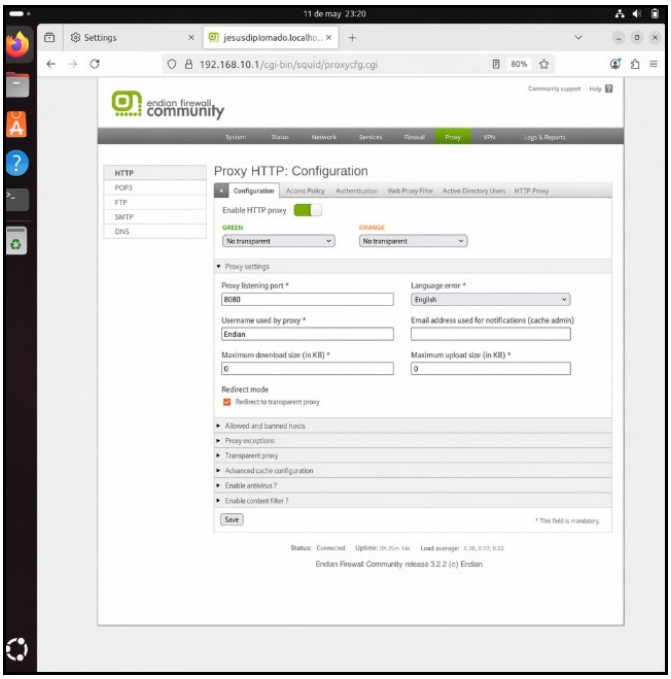
Fuente: Autoría propia

3.5.2 CONFIGURACIÓN DEL PROXY HTTP NO TRANSPARENTE

En el menú Proxy y luego HTTP se configuró el servicio en modo no transparente para las redes GREEN y ORANGE. Esta modalidad exige que los equipos clientes utilicen explícitamente el proxy para navegar, lo que permite aplicar autenticación y políticas de filtrado de manera controlada. El puerto de escucha configurado fue el 8080.

Figura 42.

Configuración del proxy HTTP en modo no transparente



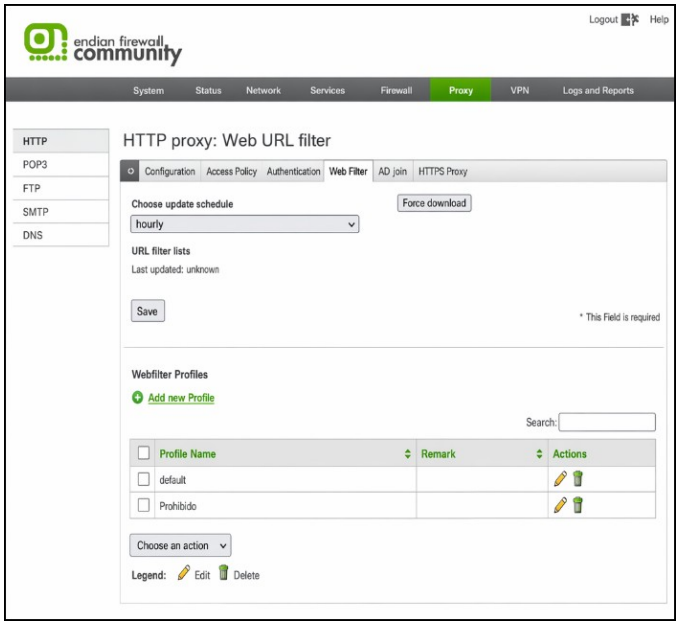
Fuente: Autoría propia

3.5.3 FILTRO WEB Y LISTA NEGRA

En la sección Web Filter se crearon perfiles de filtrado web. Dentro del perfil denominado Prohibido se activaron opciones de control y se incorporaron sitios web a una lista negra personalizada, con el fin de impedir su acceso desde los equipos sujetos a la política definida.

Figura 43.

Sección Webfilter Profiles con perfil Prohibido creado

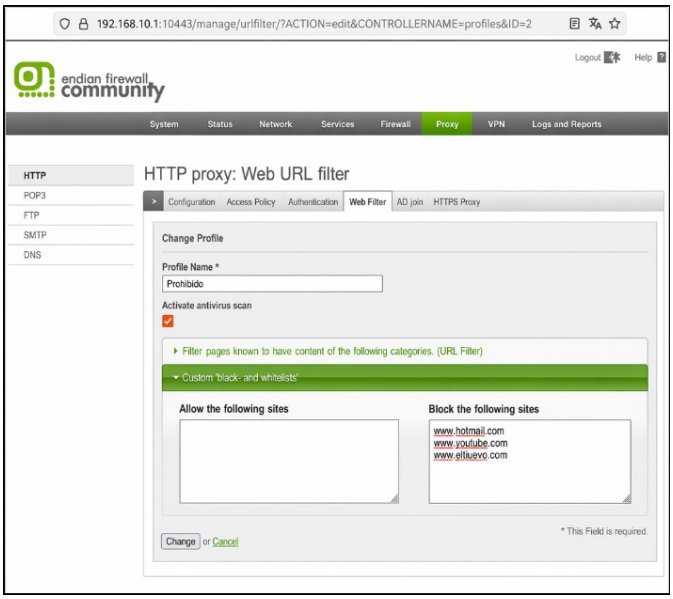


Fuente: Autoría propia

En la imagen se muestra la creación y la configuración del perfil “Prohibido” con la lista negra aplicada, se usa para la restricción del acceso a los sitios o a los servicios específicos como una parte de las políticas de seguridad y un buen control de navegación que se implementan en Endian Firewall.

Figura 44.

Perfil Prohibido con lista negra configurada



Fuente: Autoría propia

3.5.4 AUTENTICACIÓN DE USUARIOS Y GRUPOS

En la pestaña Authentication se creó un usuario local y se asoció a un grupo definido para la práctica. El método utilizado fue Local Authentication mediante NCSA, lo cual permitió gestionar credenciales directamente desde Endian Firewall sin depender de servicios externos de directorio.

Figura 45.

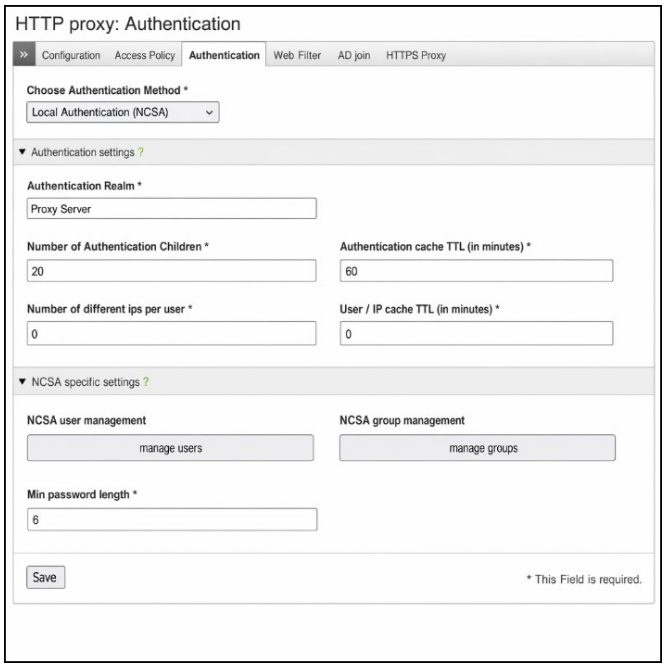
Creación de usuario y grupo para autenticación del proxy

Fuente: Autoría propia

La Figura 46 muestra la configuración para el método de autenticación NCSA en Endian Firewall, se usa para la gestion del acceso para los usuarios mediante las credenciales almacenadas de manera y poder reforzar el control de autenticación en la red.

Figura 46.

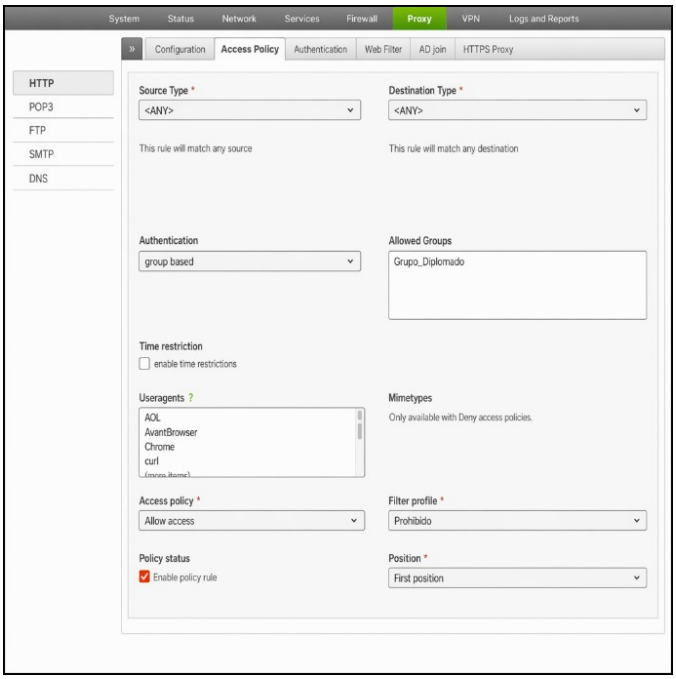
Método de autenticación NCSA configurado



Fuente: Autoría propia

Figura 47.

Política de acceso con grupo y perfil de filtrado Prohibido



Fuente: Autoría propia

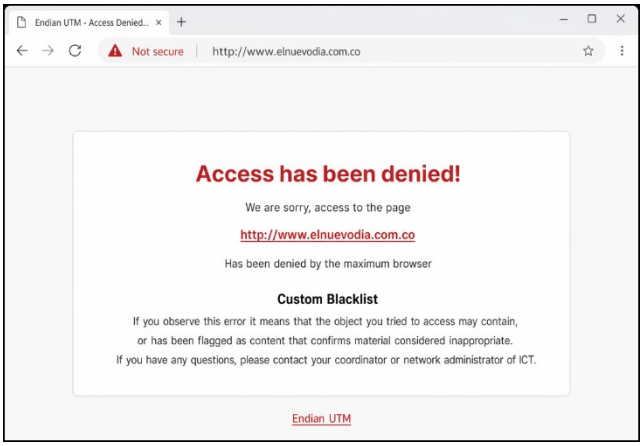
3.5.5 POLÍTICA DE ACCESO Y VERIFICACIÓN

En la sección Access Policy se creó una política que vinculó el grupo de usuarios con el perfil de filtrado configurado. Esta política permitió autorizar la navegación bajo condiciones definidas y aplicar simultáneamente el bloqueo de los sitios incluidos en la lista negra.

Como prueba final, se intentó acceder desde el Desktop a uno de los sitios incluidos en la lista negra. Endian Firewall respondió con una página de acceso denegado, confirmando que el proxy HTTP no transparente aplicó correctamente la política de filtrado configurada.

Figura 48.

Verificación de acceso denegado por lista negra del proxy



Fuente: Autoría propia

La implementación del proxy permitió demostrar que la seguridad perimetral no se limita al control de direcciones IP y puertos, sino que también puede extenderse al control de usuarios, grupos y contenido web.

4 RESULTADOS Y VALIDACIÓN

Los resultados obtenidos evidencian que la infraestructura virtualizada permitió segmentar correctamente la red en las zonas LAN, DMZ y WAN. La configuración inicial de Endian Firewall permitió el acceso a la interfaz web de administración desde el equipo cliente, así como la identificación de las interfaces correspondientes a cada zona de seguridad. Esto confirmó que la base de red quedó operativa para el desarrollo de las temáticas posteriores.

En relación con NAT, se verificó que las redes internas pudieron establecer comunicación hacia la zona WAN mediante reglas de traducción de direcciones. La configuración de Source NAT permitió que el tráfico originado desde la LAN y la DMZ saliera hacia Internet utilizando la interfaz roja de Endian Firewall. Asimismo, el reenvío de puertos permitió publicar servicios internos de la DMZ, especialmente HTTP y FTP, sin exponer de forma directa toda la red interna.

Las pruebas de servicios demostraron que el servidor ubicado en la DMZ respondió a solicitudes HTTP y FTP desde las zonas autorizadas. El acceso al servidor Apache y la autenticación FTP permitieron comprobar que las reglas aplicadas no solo estaban creadas en la interfaz gráfica, sino que funcionaban dentro del flujo real de tráfico entre las zonas de red.

La validación del filtrado inter-zona permitió confirmar que Endian Firewall controló el paso de paquetes entre LAN, DMZ y WAN según las reglas configuradas. La revisión mediante iptables mostró la existencia de reglas activas en la cadena de reenvío, mientras que los contadores de paquetes evidenciaron que dichas reglas procesaron tráfico real durante las pruebas. Esto resulta importante porque demuestra que la configuración no quedó únicamente registrada en la interfaz web, sino aplicada en el núcleo del sistema.

Finalmente, la configuración del proxy HTTP no transparente permitió aplicar control sobre la navegación web mediante autenticación local, grupos de usuarios, perfiles de filtrado y listas negras. La prueba de acceso denegado a un sitio incluido en la lista negra confirmó que el proxy aplicó correctamente la política definida, agregando una capa adicional de control sobre el uso de la red.

5 CONCLUSIONES

La implementación realizada demuestra que la seguridad perimetral no depende únicamente de instalar un firewall, sino de configurar de forma coherente las zonas de red, las reglas de traducción, los servicios publicados y los mecanismos de validación. Endian Firewall permitió representar una infraestructura segmentada en LAN, DMZ y WAN, lo que facilitó comprender cómo se puede aislar el tráfico interno, controlar el acceso a servicios y reducir la exposición directa de los recursos de red.

La configuración NAT cumplió un papel central en la comunicación entre redes privadas y la zona externa, ya que permitió que los equipos internos accedieran a la WAN sin revelar directamente sus direcciones privadas. A su vez, el Port Forwarding permitió publicar servicios ubicados en la DMZ de manera controlada, mostrando que la exposición de servicios debe realizarse mediante reglas específicas y no mediante permisos generales que comprometan la seguridad de toda la infraestructura.

El filtrado inter-zona evidenció la importancia de definir con precisión el sentido del tráfico, los protocolos autorizados y las zonas involucradas. Una regla mal orientada puede cambiar completamente el nivel de exposición de la red, especialmente cuando se permite tráfico desde la DMZ hacia la LAN. Por ello, la validación de reglas con pruebas reales e iptables resulta necesaria para comprobar que las políticas aplicadas en la interfaz gráfica corresponden al comportamiento efectivo del sistema.

La implementación del proxy HTTP no transparente amplió el enfoque de seguridad hacia el control de navegación, usuarios y contenido. Esta configuración permitió demostrar que una arquitectura segura no solo debe filtrar direcciones y puertos, sino también establecer políticas de acceso asociadas a perfiles, grupos y listas de sitios restringidos. En consecuencia, el proxy complementó las reglas de firewall con una capa de control más cercana al comportamiento del usuario.

En conjunto, las cinco temáticas permitieron construir una visión integral de la seguridad en GNU/Linux mediante Endian Firewall. La práctica evidenció que la protección de una red requiere diseño, configuración, pruebas y revisión constante. No basta con que los servicios funcionen; también es necesario comprobar que funcionan bajo las restricciones previstas y que cada regla responde al propósito de seguridad definido para la infraestructura.

6 REFERENCIAS

[1] Endian, “Endian UTM 3.2 Reference Manual,” 2016. [Online]. Available: http://docs.endian.com/3.2/utm/index.html. [Accessed: May 10, 2026].

[2] Debian, “Debian GNU/Linux Installation Guide,” 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html. [Accessed: May 10, 2026].

[3] Linux Professional Institute, “LPIC-1 Exam 101: Determine and configure hardware settings,” 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/101/101.1/ [Accessed: May 10, 2026].