DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN ENTORNOS GNU/LINUX MEDIANTE LA CONFIGURACIÓN DE NAT y FIREWAL EN ENDIAN

Deninson Alexander Chamorro Rueda
dachamorror@unadvirtual.edu.co
Juan Esteban Ortiz Fernández
jeortizf@unadvirtual.edu.co
Fredy Javier Morales Piamba
fjmoralesp@unadvirtual.edu.co
Luis Alexander Sanabria
lasanabriasa@unadvirtual.edu.co
Byron Eduardo Falla Suaza
befallas@unadvirtual.edu.co

RESUMEN: *Este articulo documenta la implementación de medidas de seguridad en un entorno GNU/Linux usando el Firewall Endian. Se detalla la configuración de la zona DMZ para permitir servicios como HTTP por el puerto 80 y FTP por el puerto 21, garantizando de igual manera la restricción de protocolos no esenciales como ICMP que permiten la integridad del servidor. La actividad de la Etapa 7 está enfocada en la implementación de medidas de seguridad en sistemas GNU/Linux, combinando teoría y práctica. Su objetivo principal es que el estudiante aprenda a proteger una infraestructura de red mediante la configuración de servicios y herramientas de seguridad.*

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

1 INTRODUCCIÓN

La administración y protección del tráfico de red constituye un aspecto fundamental en los entornos informáticos modernos, especialmente en infraestructuras que integran zonas LAN, WAN y DMZ. El presente reporte se enfoca en la gestión del tráfico hacia la zona desmilitarizada (DMZ), describiendo las actividades técnicas desarrolladas para fortalecer la seguridad de una infraestructura de red compuesta por las zonas Roja, Verde y Naranja, con el propósito de proteger los servicios alojados en sistemas GNU/Linux y herramientas Open Source. La segmentación de redes y el uso de firewalls permiten reducir riesgos de acceso no autorizado y mejorar el control del tráfico de datos dentro de las organizaciones [1].

Durante el desarrollo de la práctica se implementaron mecanismos de configuración y administración de servicios de red, permitiendo aplicar conocimientos relacionados con seguridad informática, direccionamiento IP, control de acceso y monitoreo del tráfico. Asimismo, se trabajó sobre un entorno virtualizado que integra una red local (LAN), conexión externa a internet (WAN) y una zona desmilitarizada (DMZ), con el fin de comprender la importancia de establecer políticas de seguridad y filtrado de paquetes para garantizar la disponibilidad y protección de los recursos compartidos. Los sistemas GNU/Linux ofrecen herramientas robustas y flexibles para la administración segura de servicios y redes empresariales [2].

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar y validar mecanismos de seguridad perimetral en entornos GNU/Linux mediante la configuración de Endian Firewall, reglas NAT, políticas de acceso y servicios de red en un entorno virtualizado.

2.2 OBJETIVOS ESPECÍFICOS

- Configurar un entorno de red virtualizado en VirtualBox mediante la implementación de las zonas WAN, LAN y DMZ utilizando Endian Firewall.
- Implementar y validar reglas NAT y DNAT para permitir la comunicación segura entre las diferentes zonas de red y el acceso a servicios externos.
- Configurar políticas de firewall para permitir y restringir el tráfico de red mediante servicios HTTP, FTP y reglas de control de acceso.
- Instalar y verificar servicios Apache2 y vsftpd en un servidor GNU/Linux ubicado en la zona DMZ, comprobando su funcionamiento mediante pruebas de conectividad y acceso.

3 DESARROLLO DE TEMATICAS

3.1 TEMATICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO.

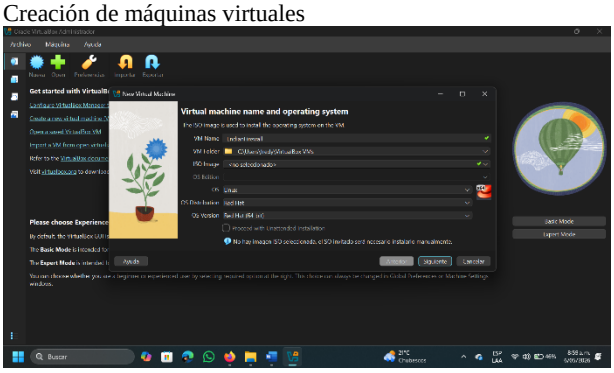
La temática tiene como objetivo la configuración inicial que permite el acceso a los servicios del sistema operativo Endian Firewall Community. Durante esta etapa se configuran las redes virtuales en la aplicación VirtualBox, permitiendo una comunicación segura entre un cliente de escritorio y un servidor mediante las zonas verde, roja y naranja correspondientes a las redes LAN, WAN y DMZ, respectivamente.

Configurar y validar reglas de acceso en un entorno de red virtualizado utilizando Endian Firewall, con el fin de controlar el tráfico entre las zonas WAN, LAN y DMZ, permitiendo la publicación y verificación segura de servicios HTTP y FTP mediante políticas de firewall, NAT y segmentación de red.

3.1.1 CONFIGURACIÓN VIRTUALBOX Y CREACIÓN DE MÁQUINAS VIRTUALES

Para iniciar la actividad práctica, se realizó la instalación de la aplicación Oracle VM VirtualBox con el propósito de aprovechar sus características y funcionalidades más recientes. La instalación se efectuó desde cero con el fin de evitar conflictos ocasionados por configuraciones previas, tanto en el entorno de VirtualBox como en las distribuciones instaladas en las máquinas virtuales. Este procedimiento permitió garantizar un entorno estable y adecuado para el desarrollo de las prácticas de virtualización y configuración de redes, permitiendo una administración eficiente de los recursos virtuales y del entorno de pruebas [3].

Figura 1.
Creación de máquinas virtuales

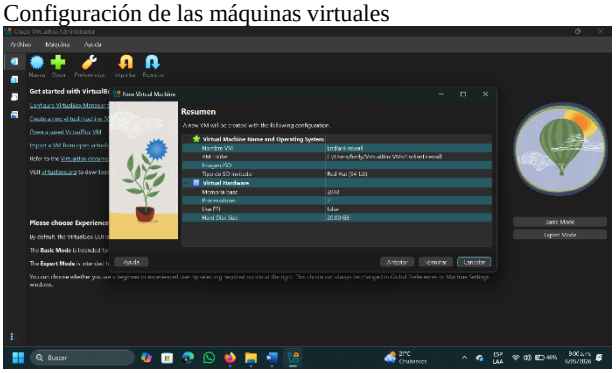


Fuente: Autoría Propia

Posteriormente, se llevó a cabo la creación y configuración de tres máquinas virtuales dentro del entorno de Oracle VM VirtualBox, destinadas a cumplir diferentes funciones dentro de la práctica de virtualización y administración de redes. La primera máquina virtual fue asignada al sistema Endian Firewall Community, encargado de la gestión y control del tráfico de red entre las distintas zonas configuradas. La segunda máquina virtual correspondió a Ubuntu Desktop, utilizada como equipo cliente para realizar pruebas de conectividad, acceso a servicios y validación de reglas de seguridad. Finalmente, la tercera máquina virtual fue destinada a Ubuntu Server, empleada para la implementación y administración de servicios de red dentro del entorno virtualizado.

Para garantizar un funcionamiento estable y adecuado de cada sistema operativo, se asignó a cada máquina virtual una configuración de hardware compuesta por 2 GB de memoria RAM, 2 núcleos de procesador y un disco duro virtual de 20 GB de capacidad. Esta configuración permitió disponer de los recursos mínimos necesarios para ejecutar correctamente los servicios, aplicaciones y procesos requeridos durante el desarrollo de la práctica.

Figura 2.
Configuración de las máquinas virtuales



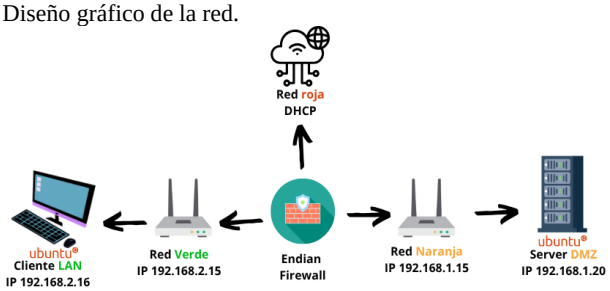
Fuente: Autoría propia

3.1.2 IMPLEMENTACIÓN DE REDES

Para la configuración de redes se activan en el sistema Endian Firewall Community tres adaptadores de red, destinados a cada una de las zonas. La zona verde se configura para la comunicación interna de la red LAN con una puerta de enlace 192.168.2.15; la zona naranja se destina a la DMZ para la comunicación con servidores de red interna mediante la puerta de enlace 192.168.1.15; y la zona roja se configura con NAT y DHCP habilitados para el acceso a internet.

En cuanto al cliente, se configura un adaptador de red interna enrutado hacia la zona verde de la red LAN con dirección IP estática 192.168.2.16. De igual manera, el servidor se configura con un adaptador de red interna enrutado hacia la zona naranja, utilizando la dirección IP estática 192.168.1.20.

Figura 3.
Diseño gráfico de la red.



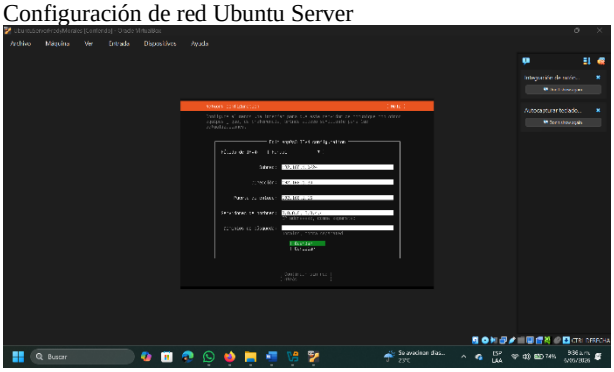
Fuente: Autoría propia mediante Canva

3.1.3 CONFIGURACIÓN DE RED CON IP ESTÁTICA EN EL CLIENTE Y SERVIDOR.

Con el propósito de garantizar una red estable y una comunicación adecuada entre los dispositivos virtualizados, se realizó la configuración de direccionamiento IP tanto en el equipo cliente como en el servidor, de acuerdo con el esquema de red previamente definido. La asignación de direcciones IP se implementó de manera estática, permitiendo mantener rutas de comunicación permanentes y evitando variaciones en la conectividad dentro del entorno virtualizado. Esta configuración facilitó la administración de la red y aseguró la correcta interacción entre los diferentes servicios y equipos utilizados durante la práctica.

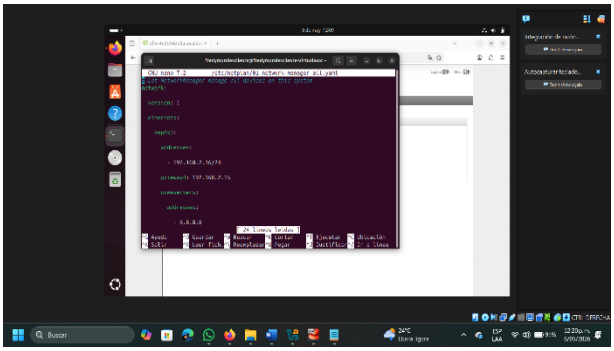
En el caso del servidor, la configuración de red fue realizada durante el proceso de instalación del sistema operativo, estableciendo de forma manual los parámetros correspondientes a dirección IP, máscara de subred, puerta de enlace y servidores DNS. Por otra parte, en el equipo cliente la configuración se efectuó mediante la modificación de los archivos de Netplan, herramienta utilizada por las versiones actuales de Ubuntu para la administración de interfaces de red. De esta manera, se logró mantener un entorno de comunicación controlado y estable para el desarrollo de las pruebas de conectividad y administración de red [4].

Figura 4.
Configuración de red Ubuntu Server



Fuente: Autoría Propia

Figura 5.
Configuración de red

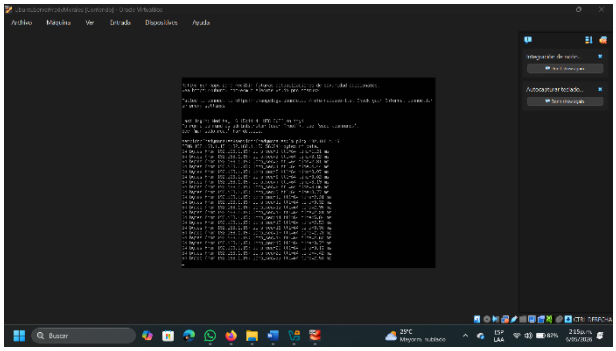


Fuente: Autoría propia

3.1.4 VERIFICACIÓN DEL PROCESO

Al finalizar el proceso de instalación y configuración, se obtiene como resultado un acceso seguro y controlado mediante un entorno de red que permite la comunicación desde el cliente y el servidor hacia el acceso web. Dicho funcionamiento se verifica mediante pruebas de comunicación realizadas entre las terminales y el firewall, así como mediante la validación del acceso a internet.

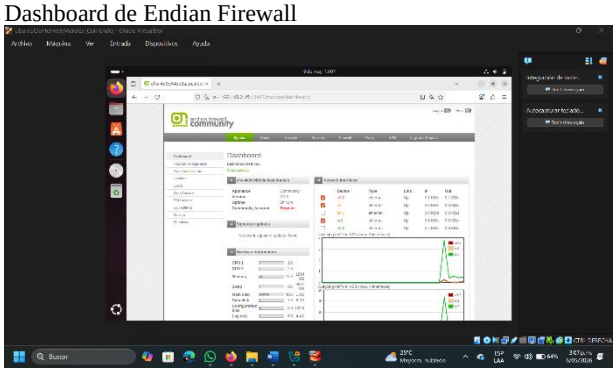
Figura 6.
Pruebas de comunicación



Fuente autoría Propia

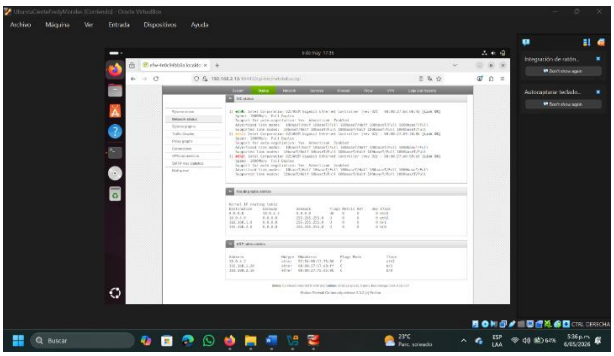
Por otra parte, como evidencia final se obtiene el acceso a la configuración del sistema Endian Firewall Community desde la terminal cliente a través de su entorno web, lo que permite verificar los servicios en funcionamiento y las reglas configurables para el uso seguro de la red.

Figura 7.
Dashboard de Endian Firewall



Fuente: Autoría Propia

Figura 8.
Validación de redes activas, interfaz web Endian Firewall



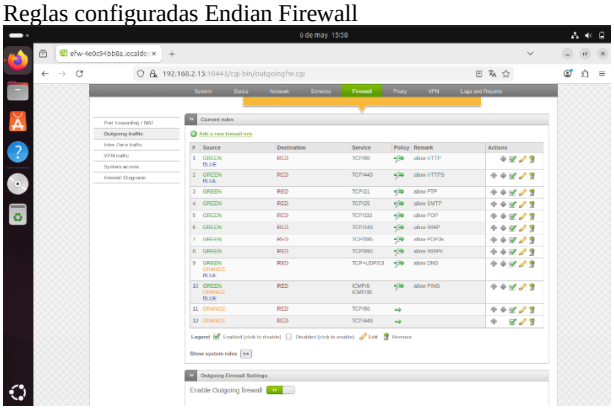
Fuente: Autoria propia.

3.1.5 DIFICULTADES EN EL PROCESO

Durante el proceso de verificación de los servicios se evidenció, en una primera instancia, que el servidor, aunque respondía satisfactoriamente a las pruebas de comunicación hacia la red Roja (WAN), no lograba establecer conexión con los repositorios al momento de realizar descargas de paquetes de actualización o instalaciones de software. Esta situación permitió identificar restricciones en las políticas de acceso configuradas en el firewall, afectando la comunicación hacia servicios externos.

Para solucionar el inconveniente identificado, fue necesario implementar dos reglas en el Firewall Endian orientadas a la red Naranja (DMZ), permitiendo la comunicación mediante los puertos TCP/80 y TCP/443. Con esta configuración se habilitó correctamente el acceso a servicios web y repositorios externos, logrando así una conectividad completa a internet desde el servidor. La implementación de políticas de filtrado y control de acceso en firewalls constituye una práctica esencial para proteger los servicios expuestos y garantizar una comunicación segura entre las diferentes zonas de red [5].

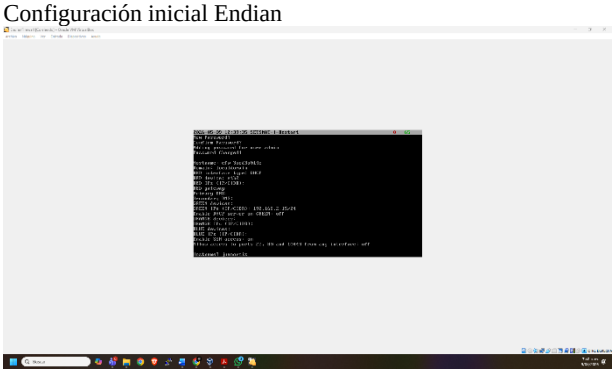
Figura 9.
Reglas configuradas Endian Firewall



Fuente: Autoría propia

3.2 TEMATICA 2: CONFIGURACION NAT

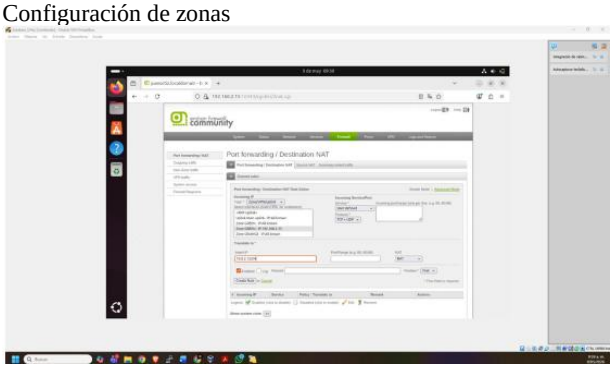
Figura 10.
Configuración inicial Endian



Fuente: Autoría Propia

En esta temática se realizó la configuración de NAT (Network Address Translation) en el Firewall Endian, con el propósito de permitir la comunicación entre la red local (LAN) y la red WAN simulada como Internet. Esta configuración fue importante para que los equipos de la red interna pudieran acceder a servicios externos utilizando una sola dirección IP pública, mejorando además la seguridad de la red.

Figura 11.
Configuración de zonas

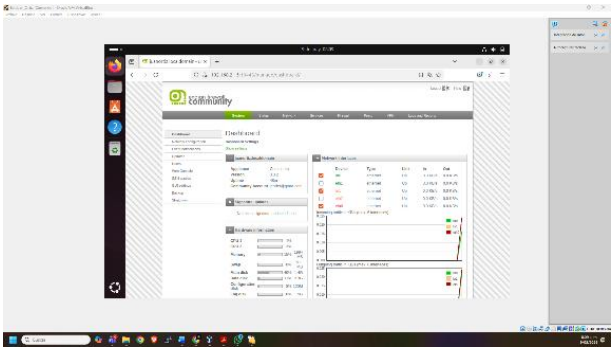


Fuente: Autoría Propia

3.2.1 CONFIGURACIÓN DE LA REGLA NAT

Para iniciar la práctica se ingresó a la interfaz administrativa de Endian Firewall desde la zona verde. Después se procedió a crear la regla NAT de salida, seleccionando como red de origen la LAN interna y habilitando la traducción automática de direcciones.

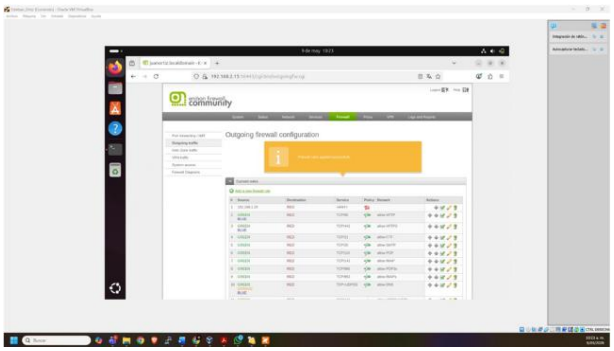
Figura 12.
Ingreso a la Consola de Endian



Fuente: Autoría Propia

Con esta configuración, los dispositivos conectados a la red privada lograron establecer comunicación con la red externa sin exponer directamente sus direcciones IP internas. La regla creada permitió el tráfico adecuado entre las diferentes zonas configuradas en el entorno de laboratorio.

Figura 13.
Configuración de Reglas

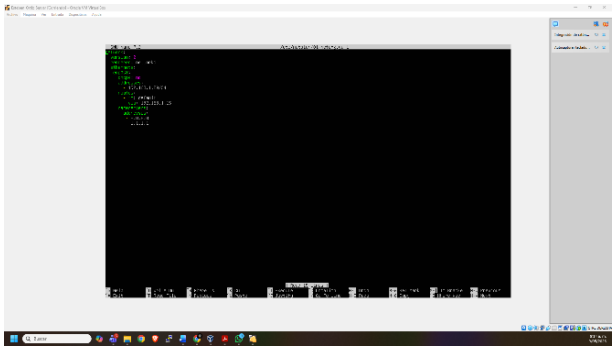


Fuente: Autoría Propia

3.2.2 VERIFICACIÓN DE CONECTIVIDAD

Una vez aplicada la configuración NAT, se realizaron diferentes pruebas para comprobar el correcto funcionamiento de la comunicación entre la LAN y la WAN. Para ello se utilizaron comandos básicos de conectividad como ping y traceroute desde los equipos de la red interna.

Figura 14.
Configuración Yalm en el servidor



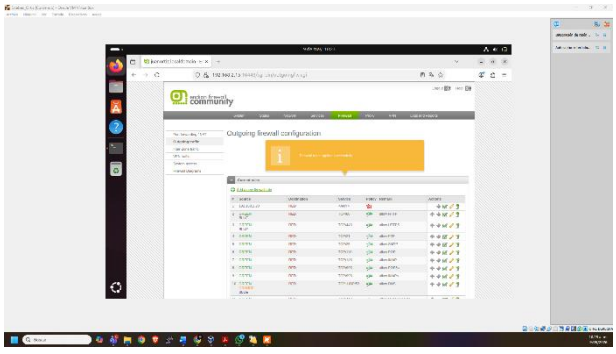
Fuente: Autoría Propia

Durante las verificaciones se observó que los paquetes enviados desde la LAN podían salir correctamente hacia la red externa, confirmando que la traducción de direcciones estaba funcionando de manera adecuada.

Adicionalmente, en el apartado de reglas NAT del Firewall Endian se comprobó que la configuración creada aparecía activa y habilitada dentro del sistema.

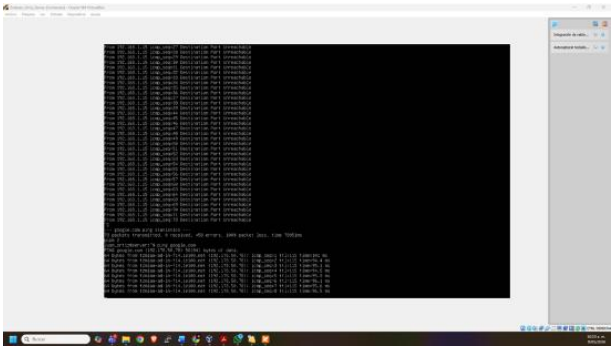
La ventana principal presenta la interfaz web de Endian Firewall Community, una solución de seguridad de red de código abierto. Se encuentra en la sección de configuración de firewall de salida (Outgoing firewall configuration), mostrando una lista de reglas de tráfico aplicadas con éxito.

Figura 15.
Regla de Bloqueo del servidor hacia internet



Fuente: Autoría Propia

Figura 16.
Pruebas de Conectividad



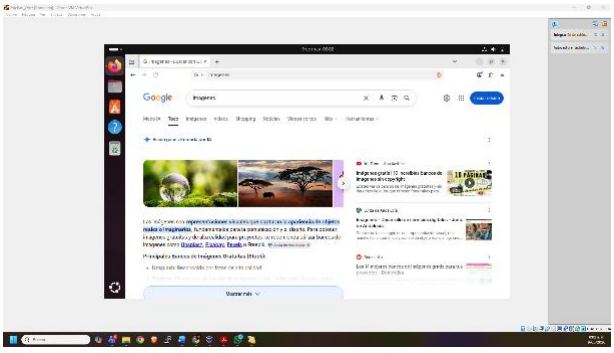
Fuente: Autoría Propia

3.2.3 RESULTADOS OBTENIDOS

Las pruebas realizadas permitieron evidenciar que la configuración NAT funcionó correctamente dentro del entorno de red implementado. Los equipos de la LAN lograron acceder a la WAN simulada sin inconvenientes y el firewall realizó la traducción de direcciones de manera automática.

La configuración de reglas NAT permitió establecer correctamente la comunicación entre las zonas LAN, DMZ y la red WAN, garantizando el acceso controlado hacia Internet desde los diferentes segmentos de red. Asimismo, las pruebas realizadas permitieron verificar el correcto funcionamiento del reenvío de puertos y las políticas configuradas en el firewall, fortaleciendo la administración y seguridad de la infraestructura de red [6].

Figura 17.
Prueba de conexión de Ubuntu desktop Con la IP



Fuente: Autoría Propia

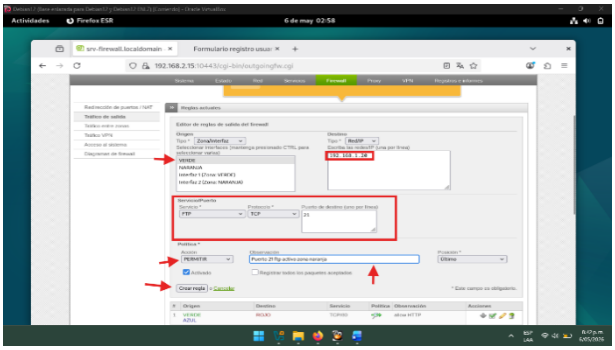
3.3 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ

Para esta temática se realizó la configuración de reglas de acceso en el Endian Firewall desde Debian 12 zona verde (DMZ) para el servidor Ubuntu Server ubicado en la zona naranja (DMZ)

3.3.1 HABILITACIÓN DE SERVICIOS HTTP Y FTP

Para la habilitación de los puertos se configuro Endian Firewall con la creación de reglas que permiten el tráfico por el puerto 80(HTTP) y el puerto 21 (FTP).

Figura 18.
Configuración de regla.

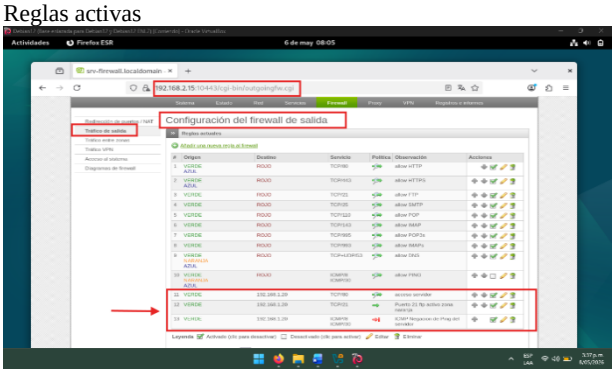


Fuente: Autoría Propia

3.3.2 NEGACIÓN DE PROTOCOLO ICMP

Para evitar respuestas de comando ping hacia la red se implementó la negación del protocolo ICMP puertos (8 y 30), dando como resultado la confirmación de la restricción exitosa del tráfico por medio de ping.

Figura 19.
Reglas activas



Fuente: Autoría Propia

La configuración de los servicios HTTP y FTP en la zona DMZ permitió validar el acceso controlado a los recursos publicados desde el servidor Ubuntu Server. Asimismo, el bloqueo del protocolo ICMP permitió restringir las respuestas a solicitudes

de ping, fortaleciendo las políticas de seguridad y control del tráfico implementadas en el firewall [5].

3.4 TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

3.4.1 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

La Temática 4 se enfocó en la configuración de reglas de acceso y control de tráfico utilizando Endian Firewall en un entorno de red virtualizado. Durante el desarrollo de la práctica se implementó la segmentación de redes mediante las zonas WAN (Roja), LAN (Verde) y DMZ (Anaranjada), permitiendo establecer políticas de seguridad para autorizar o restringir la comunicación entre dichas zonas.

3.4.2 CONFIGURACIÓN DE REGLAS DE FIREWALL Y NAT

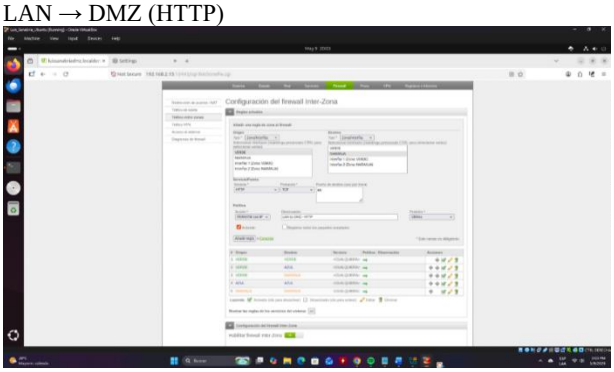
Se configuraron reglas de firewall, NAT y DNAT para habilitar servicios HTTP y FTP desde la WAN hacia la DMZ, así como reglas inter-zona para controlar la comunicación entre la red interna y el servidor ubicado en la zona DMZ.

3.4.3 REGLAS PARA VERDE (LAN) ↔ NARANJA (DMZ)

En la sección de tráfico entre zonas, se procede a crear y configurar las reglas necesarias para permitir la comunicación entre la red LAN y la zona DMZ, definiendo los servicios, protocolos y puertos autorizados para el intercambio de tráfico.[8]

Configuramos la regla inter-zona para permitir el tráfico HTTP desde la LAN hacia la DMZ mediante el puerto TCP/80.

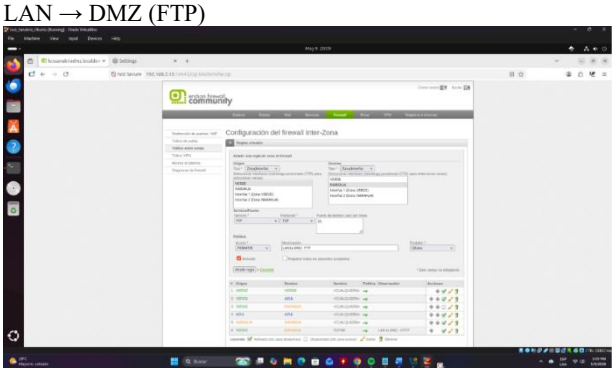
Figura 20.
LAN → DMZ (HTTP)



Fuente: Autoría Propia

Ahora configuramos la regla inter-zona para permitir el tráfico FTP desde la LAN hacia la DMZ mediante el puerto TCP/21.

Figura 21.
LAN → DMZ (FTP)



Fuente: Autoría Propia

3.4.4 REGLAS PARA INTERNET (WAN) ↔ DMZ

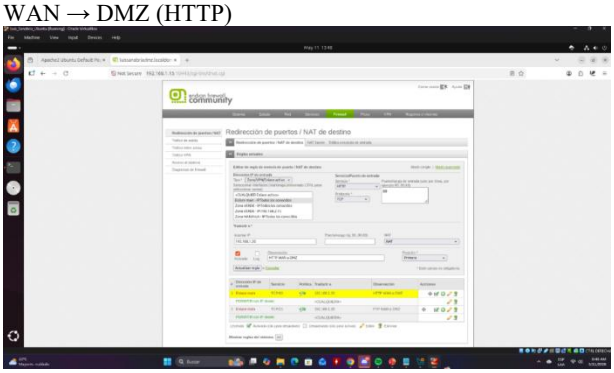
Para configurar las reglas de acceso desde la zona WAN hacia la zona DMZ, se accede a la sección de redireccionamiento de puertos (Port Forwarding/NAT), donde se definen las políticas necesarias para permitir el tráfico autorizado hacia los servicios publicados en la DMZ [7].

Figura 22.
Para el caso de endian 3.3.2 configuramos las reglas NAT para la redirección de WAN a DMZ

Fuente: Autoría Propia

Podemos ver la configuración de la regla DNAT en Endian Firewall para permitir el acceso al servicio HTTP desde la zona WAN hacia el servidor ubicado en la DMZ, mediante la redirección del tráfico entrante por el puerto TCP/80 hacia la dirección IP interna del servidor.

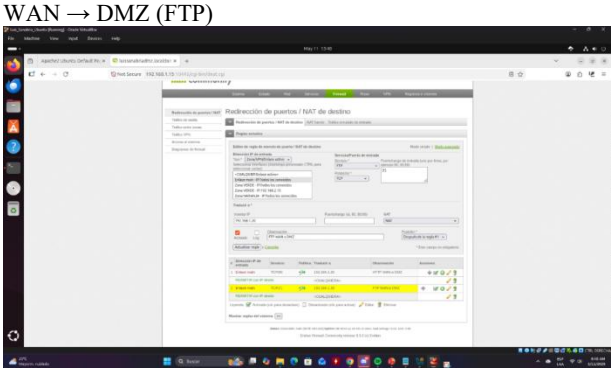
Figura 23.
WAN → DMZ (HTTP)



Fuente: Autoría Propia

A continuación, configuramos una regla de redirección NAT en Endian Firewall para permitir el acceso al servicio FTP desde la zona WAN hacia el servidor ubicado en la DMZ, habilitando la comunicación mediante el puerto TCP/21 hacia la dirección IP interna del servidor FTP.

Figura 24.
WAN → DMZ (FTP)



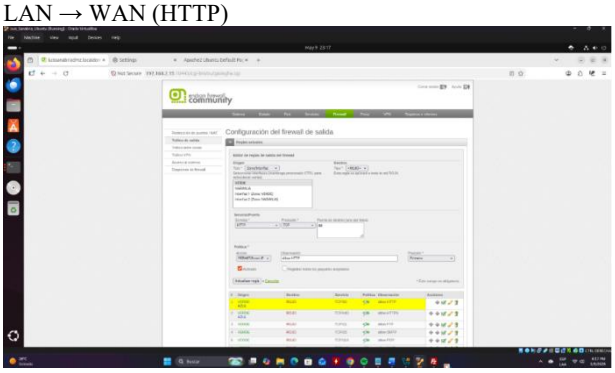
Fuente: Autoría Propia

3.4.5 REGLAS PARA LAN → WAN

Para configurar la comunicación desde la zona LAN hacia la WAN, se accede a la sección de tráfico de salida, donde se establecen las reglas y políticas que permiten controlar el acceso de la red interna hacia Internet. [8]

Configuramos una regla de firewall de salida en Endian Firewall para permitir la comunicación desde la red LAN hacia la WAN mediante el servicio HTTP, habilitando el tráfico por el puerto TCP/80 para el acceso a servicios web externos.

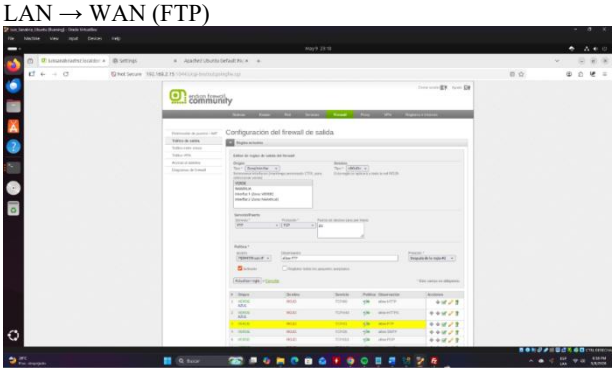
Figura 25.
LAN → WAN (HTTP)



Fuente: Autoría Propia

Configuramos una regla de firewall de salida en Endian Firewall para permitir la comunicación desde la red LAN hacia la WAN mediante el servicio FTP, habilitando el tráfico por el puerto TCP/21 para la transferencia de archivos y acceso a servicios FTP externos.

Figura 26.
LAN → WAN (FTP)



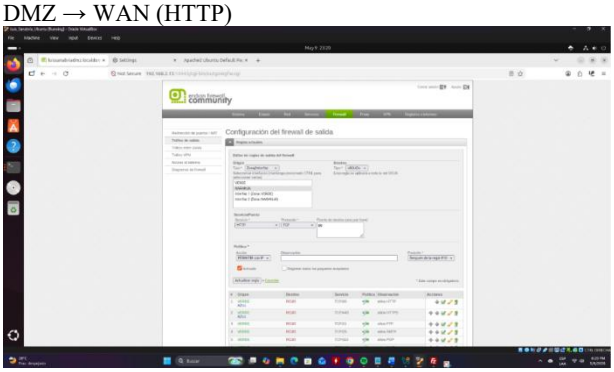
Fuente: Autoría Propia

3.4.6 REGLAS PARA DMZ → WAN

En la misma sección de tráfico de salida también se configuran las reglas necesarias para permitir la comunicación desde la zona DMZ hacia la WAN, definiendo los servicios y accesos autorizados hacia Internet. [9]

configuramos la regla de salida para permitir el tráfico HTTP desde la DMZ hacia la WAN mediante el puerto TCP/80.

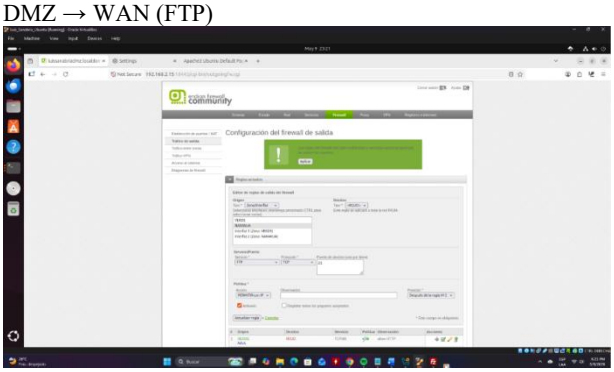
Figura 27.
DMZ → WAN (HTTP)



Fuente: Autoría Propia

Configuramos la regla de salida para permitir el tráfico FTP desde la DMZ hacia la WAN mediante el puerto TCP/21.

Figura 28.
DMZ → WAN (FTP)



Fuente: Autoría Propia

3.4.7 IMPLEMENTACIÓN DE SERVICIOS EN LA DMZ

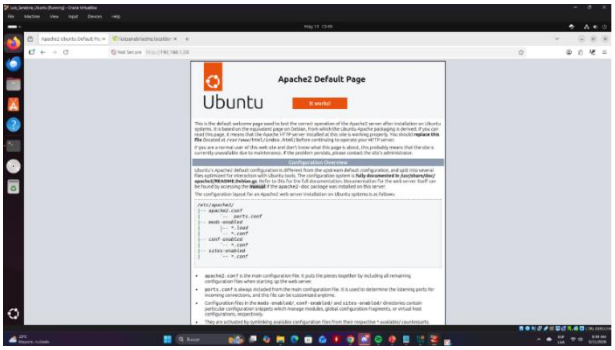
En el servidor Linux ubicado en la zona anaranjada se realizó la instalación y configuración de los servicios Apache2 y vsftpd, permitiendo la publicación de servicios HTTP y FTP. Adicionalmente, se configuraron usuarios y permisos para el acceso mediante FTP.

3.4.8 VERIFICACIÓN DE CONECTIVIDAD Y FUNCIONAMIENTO

Se llevaron a cabo pruebas de conectividad y validación de servicios utilizando herramientas como ping, curl, acceso HTTP y conexiones FTP, verificando el correcto funcionamiento del enrutamiento, las políticas de seguridad implementadas y la comunicación controlada entre las diferentes zonas de red. Realizando lo siguiente:

Para el acceso de conectividad de LAN hacia WAN se uso el navegador para acceder con la dirección IP del servidor DMZ.

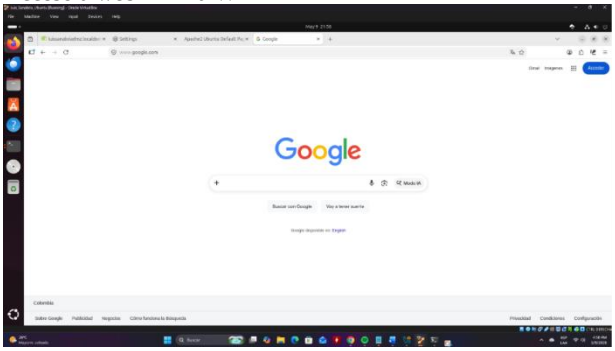
Figura 29.
Acceso a web LAN a DMZ



Fuente: Autoria propia.

Pudimos comprobar el Acceso a la red WAN desde el LAN accediendo a Google, lo que nos permite validar que si tenemos conexión a internet a través del firewall Endian.

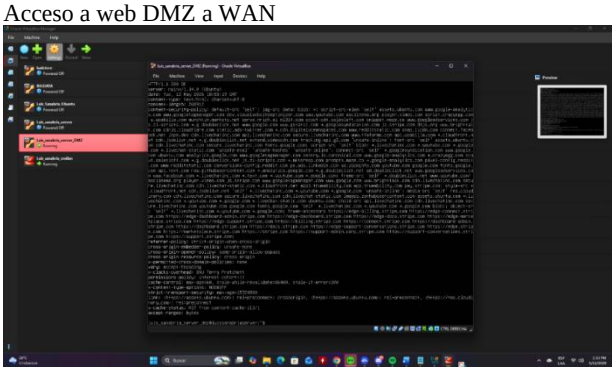
Figura 30.
Acceso a web LAN a WAN



Fuente: Autoria propia.

Se realizo la comprobación de el acceso a la red WAN desde el servidor DMZ usando el comando: date && curl -I https://www.ubuntu.com

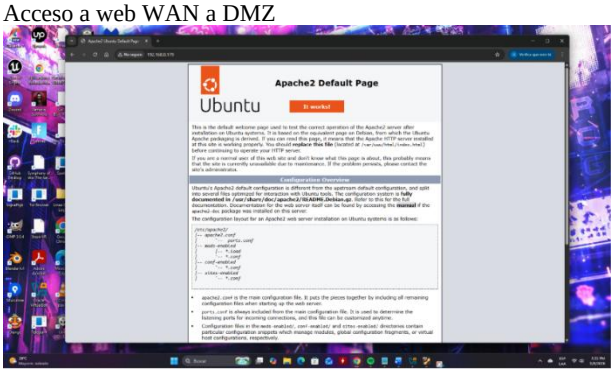
Figura 31.
Acceso a web DMZ a WAN



Fuente: Autoria propia.

Al momento de la validación de el acceso de la red WAN a el servidor DMZ se simulo accediendo desde fuera de las maquinas virtuales con la dirección IP de la maquina con el Firewall Endian para probar el enrutamiento correcto.

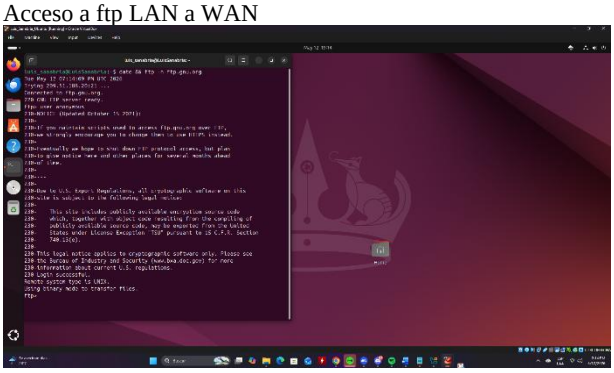
Figura 32.
Acceso a web WAN a DMZ



Fuente: Autoria propia.

Se comprobó el acceso a FTP desde LAN a WAN accediendo a un servidor FPT público en la web con el comando: *date && ftp -n ftp.gnu.org*

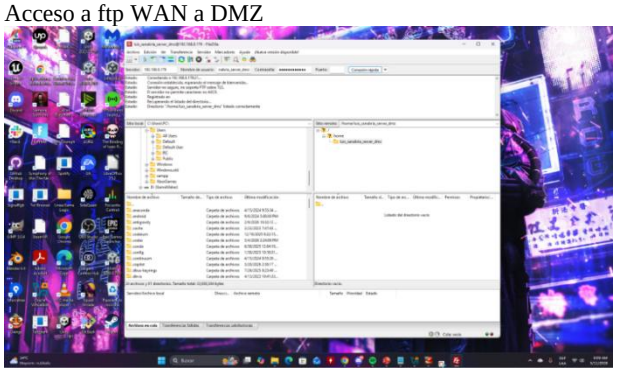
Figura 33.
Acceso a ftp LAN a WAN



Fuente: Autoria propia.

Se comprobó el acceso por FPT de WAN a DMZ usando un cliente FPT desde fuera de la red del firewall Endian, usando la IP de la maquina con firewall Endian.

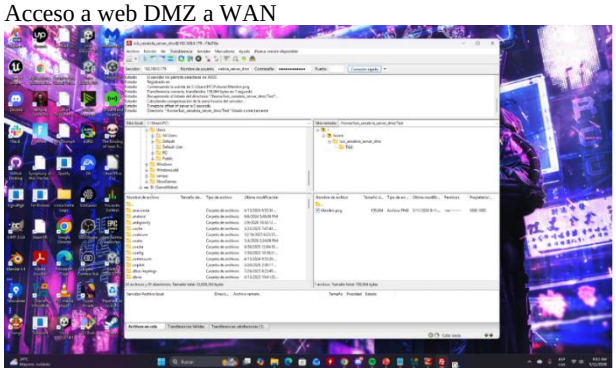
Figura 34.
Acceso a ftp WAN a DMZ



Fuente: Autoria propia.

Para probar la conexión correcta probamos subiendo un archivo dese el cliente FTP a la dirección conectada

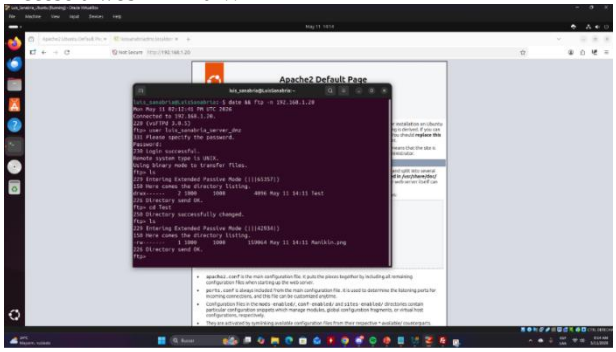
Figura 35.
Acceso a web DMZ a WAN



Fuente: Autoría propia.

Podemos hacer una prueba en terminal para comprobar que el archivo esta subido correctamente en el servidor y que la conexión de FTP desde WAN a DMZ fue exitosa, para esto accedemos por terminal desktop al servidor FTP en DMZ

Figura 36.
Acceso a web DMZ a WAN



Fuente: Autoría propia.

La implementación de reglas de acceso permitió controlar y administrar la comunicación entre las zonas Verde, Naranja y WAN mediante los servicios HTTP y FTP, garantizando un intercambio de información seguro y organizado. Las pruebas realizadas desde los diferentes segmentos de red permitieron verificar el correcto funcionamiento de las políticas de filtrado y control de tráfico configuradas en el firewall.

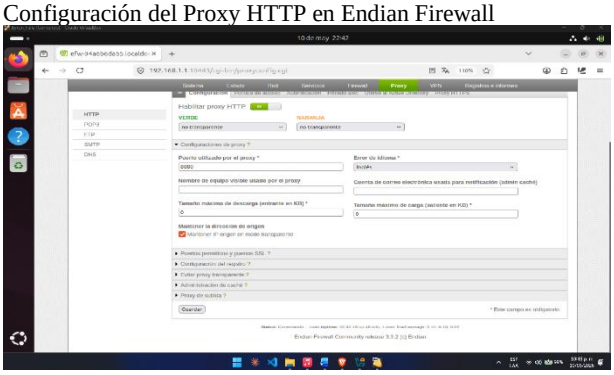
3.5 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

La Temática 5 consistió en la implementación de un proxy HTTP no transparente con políticas de autenticación para el control de la navegación en Internet desde la red interna (LAN), utilizando Endian Firewall Community 3.3.2 como plataforma de seguridad perimetral.

3.5.1 CONFIGURACIÓN DEL PROXY HTTP

Se accedió a la interfaz web de administración de Endian Firewall y se habilitó el servicio proxy HTTP desde el menú Proxy → HTTP. El proxy se configuró en modo no transparente tanto para la zona GREEN (LAN) como para la zona ORANGE (DMZ), con el puerto de escucha 8080. Esta configuración obliga a los usuarios a configurar manualmente el proxy en su navegador, lo que permite identificar y autenticar a cada usuario de forma individual antes de conceder acceso a Internet.

Figura 37.
Configuración del Proxy HTTP en Endian Firewall

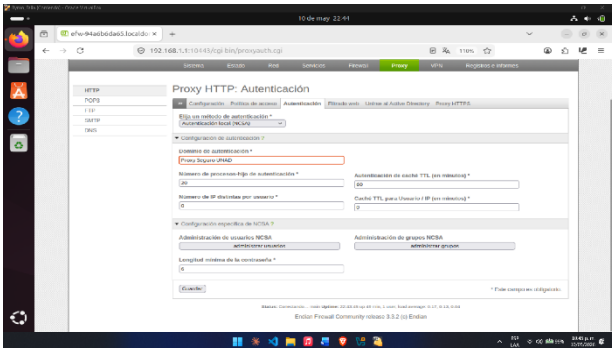


Fuente: Autoría propia.

3.5.2 AUTENTICACIÓN DE USUARIOS Y GRUPOS

Para la autenticación se seleccionó el método de autenticación local NCSA, configurando el dominio de autenticación como "Proxy Seguro UNAD". Posteriormente se creó el grupo Usuarios_LAN y el usuario estudiante1, asociando dicho usuario al grupo creado. Esta configuración permite que el proxy exija credenciales válidas antes de permitir cualquier navegación desde la red interna.

Figura 38.
Configuración de autenticación, grupo y usuario en Endian Firewall



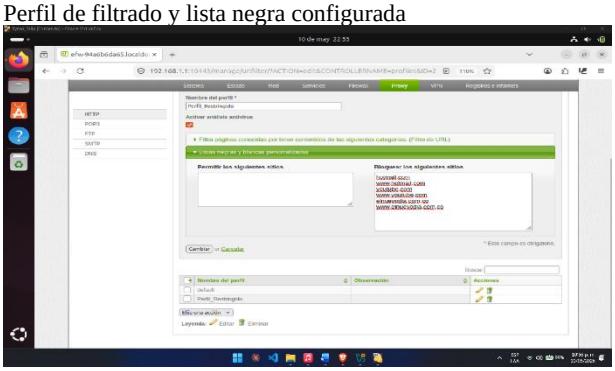
Fuente: Autoría propia.

3.5.3 CREACIÓN DE LISTA NEGRA Y PERFIL DE FILTRADO

Se creó el perfil de filtrado denominado Perfil_Restringido, dentro del cual se configuró una lista negra personalizada con los siguientes dominios bloqueados:

hotmail.com y www.hotmail.com
youtube.com y www.youtube.com
elnuevodia.com.co y www.elnuevodia.com.co

Figura 39.
Perfil de filtrado y lista negra configurada

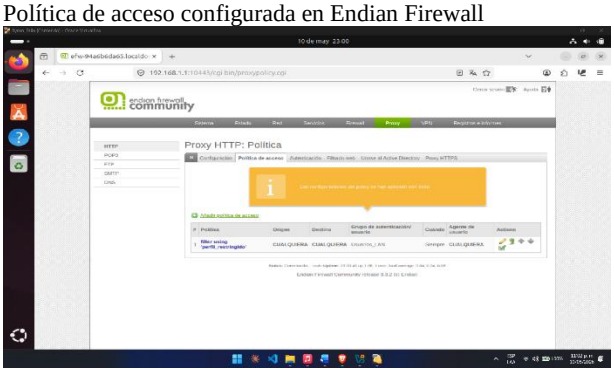


Fuente: Autoría propia.

3.5.4 POLÍTICA DE ACCESO

Se creó una política de acceso que vincula el grupo Usuarios_LAN con el Perfil_Restringido, estableciendo autenticación en base al grupo. Esta política garantiza que todo usuario de la red interna deba autenticarse con credenciales válidas y que el tráfico web sea filtrado según las reglas definidas en el perfil de filtrado.

Figura 40.
Política de acceso configurada en Endian Firewall



Fuente: Autoría propia.

3.5.5 VERIFICACIÓN DEL SERVICIO DESDE CONSOLA.

Desde la consola de Endian Firewall se verificó el estado del servicio Squid (motor del proxy) mediante los siguientes comandos, evidenciando la fecha y hora de ejecución tal como lo requiere la guía:

date && /etc/init.d/squid status
date && /etc/init.d/squid stop
date && /etc/init.d/squid start
date && /etc/init.d/squid restart

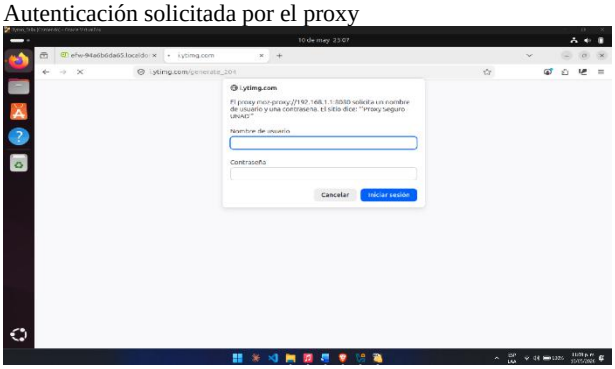
Figura 41.
Verificación del servicio Squid desde consola

Fuente: Autoría propia.

3.5.6 PRUEBAS DE NAVEGACIÓN DESDE EL CLIENTE LAN

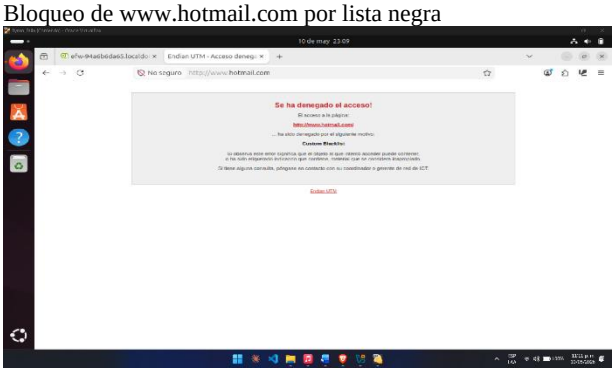
Desde la VM Ubuntu cliente se configuró Firefox con el proxy manual (192.168.1.1, puerto 8080). Al intentar navegar, el proxy solicitó autenticación mostrando el mensaje "Proxy Seguro UNAD". Tras ingresar las credenciales del usuario estudiante1, se verificó que los sitios incluidos en la lista negra fueron bloqueados correctamente por Endian Firewall, mostrando la página de error "Se ha denegado el acceso - Custom Blacklist".

Figura 42.
Autenticación solicitada por el proxy



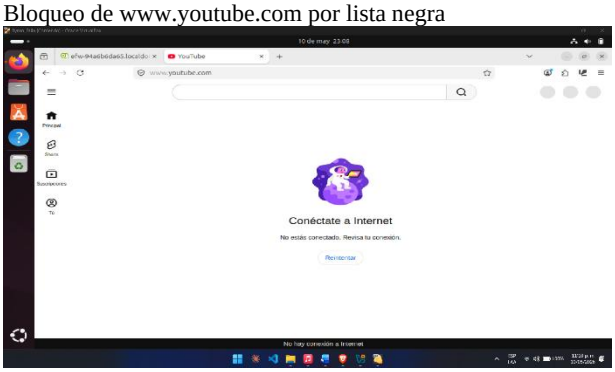
Fuente: Autoría propia.

Figura 43.
Bloqueo de www.hotmail.com por lista negra



Fuente: Autoría propia.

Figura 44.
Bloqueo de www.youtube.com por lista negra



Fuente: Autoría propia.

Figura 45.
Bloqueo de www.elnuevodia.com.co por lista negra

Fuente: Autoría propia.

4 CONCLUSIONES

La implementación de Endian Firewall en un entorno virtualizado permitió comprender la importancia de la segmentación de redes y la administración del tráfico mediante políticas de seguridad orientadas a la protección de los servicios y recursos de la infraestructura. A través de la configuración de las zonas WAN, LAN y DMZ, junto con la aplicación de reglas NAT, DNAT y filtrado de paquetes, fue posible establecer mecanismos de control de acceso que garantizaron una comunicación segura y organizada entre las diferentes redes, fortaleciendo así la seguridad del entorno implementado.

Asimismo, la configuración y puesta en funcionamiento de servicios HTTP y FTP en la zona desmilitarizada (DMZ) permitió validar el correcto comportamiento de los mecanismos de publicación de servicios y restricción de acceso, evidenciando la eficiencia de las herramientas GNU/Linux y de las soluciones Open Source para la administración, monitoreo y protección de infraestructuras de red empresariales. De igual manera, se logró identificar la relevancia de aplicar políticas adecuadas de seguridad para reducir vulnerabilidades y controlar el acceso a los recursos compartidos.

Finalmente, las pruebas de conectividad y verificación realizadas durante la práctica permitieron comprobar el correcto funcionamiento de las políticas de seguridad configuradas, evidenciando una comunicación adecuada entre las diferentes zonas de red y un acceso controlado a los servicios implementados. Los resultados obtenidos permitieron fortalecer los conocimientos relacionados con la administración de redes, configuración de firewalls y gestión segura de servicios en entornos GNU/Linux.

5 REFERENCIAS

W. Stallings, Network Security Essentials: *Applications and Standards*, 6th ed. Pearson, 2018.

Oracle Corporation. (2024). *Oracle VM VirtualBox*.

Canonical Ltd. (2024). *Network configuration with Netplan*.

E. Nemeth, G. Snyder, T. Hein, B. Whaley y D. Mackin, *UNIX and Linux System Administration Handbook*, 5th ed. Pearson, 2017.

A. S. Tanenbaum y D. J. Wetherall, *Computer Networks*, 5th ed. Pearson, 2011.

Endian, "*Port forwarding / NAT — Endian UTM 5.0 Reference Manual*," [Online]. Available: https://docs.endian.com/5.0/utm/firewall/dnat.html.

Endian Firewall, *"Outgoing traffic — Endian Firewall Reference Manual,"* [Online]. Available: https://docs.huihoo.com/endian-firewall/efw-reference-manual/2.2/efw.firewall.html

J. F. Kurose y K. W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed. Pearson, 2017.

R. W. Stevens y S. A. Rago, *Advanced Programming in the UNIX Environment*, 3rd ed. Addison-Wesley, 2013.

Wolf, G., & Halter, E. M. (2005). *Virtualization: From the desktop to the enterprise*. Apress.

Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.