IMPLEMENTACION DE REGLAS FIREWALL EN ENDIAN PARA HABILITAR SERVICIOS

Angie Leandry Almansa Tabares
alalmansat@unadvirtual.edu.co
Daniela Sánchez García
dsanchezgarcia@unadvirtual.edu.co
Liliana Amparo Viana Londoño
lavianalo@unadvirtual.edu.co
Miguel Ángel López Villada
malopezvil@unadvirtual.edu.co
Nicolas Santiago Mosquera Sánchez
nsmosqueras@unadvirtual.edu.co

RESUMEN: *La actividad consiste en la implementación de un entorno de seguridad en GNU/Linux mediante la distribución Endian firewall, con el fin de proteger la infraestructura de red actual, se realiza la configuración tres máquinas virtuales con sus respectivas interfaces de red, que permite segmentar las tres redes entre zonas (LAN,WAN y DMZ) facilitando así el monitoreo y revisión del tráfico.*
Posteriormente, Se implementa los direccionamientos de red (NAT) permitiendo la comunicación entre las redes internas y externas, habilitando el acceso controlado entre el servidor que se encuentra ubicado en la zona desmilitarizada hacia el cliente (Desktop).Además, se configuran las reglas de acceso que permiten o bloquean el tráfico entre las diferentes zonas red, de este modo se garantiza que se acceda a los servicios autorizados, finalmente, se realiza la implementación de un proxy HTTP con autentificación, el cual fortalece las políticas de acceso y bloqueo hacia los sitios web.

PALABRAS CLAVE: Firewall, NAT, Proxy, Seguridad

1 INTRODUCCIÓN

En la actualidad, la seguridad perimetral es un pilar fundamental para garantizar la integridad y disponibilidad de los recursos tecnológicos institucionales frente a amenazas externas [5], [6]. El presente artículo documenta la implementación colaborativa de una arquitectura de red segura fundamentada en sistemas operativos GNU/Linux [8], utilizando la distribución Endian Firewall [3] gestionada a través del entorno de virtualización VirtualBox [4]. El proyecto se desarrolla a través de cinco temáticas progresivas que garantizan el control absoluto del tráfico, desde la segmentación de la red hasta la validación de usuarios a nivel de aplicación.

Inicialmente, la infraestructura se divide en tres zonas de seguridad estrictamente aisladas: LAN (verde), DMZ (naranja) y WAN (roja) [7]. Sobre esta topología lógica, se establecen directivas de Traducción de Direcciones de Red (NAT) y reenvío de puertos, posibilitando la comunicación controlada entre las redes internas e Internet [9]. Posteriormente, se efectúa un endurecimiento del sistema (hardening) habilitando exclusivamente los servicios HTTP y FTP para los servidores alojados en la DMZ, mientras se deniega el tráfico de diagnóstico como el protocolo ICMP para prevenir la enumeración y el escaneo de vulnerabilidades [6].

Finalmente, el blindaje perimetral se fortalece mediante la creación de reglas de acceso inter-zona que administran el flujo de información bajo el principio de mínimo privilegio. Como medida definitiva de control de navegación, se implementa un servidor proxy HTTP en modalidad no transparente [3]. Este servicio exige la autenticación de los usuarios por grupos y aplica políticas de restricción mediante listas negras, garantizando la trazabilidad, optimización del ancho de banda y el cumplimiento normativo en el consumo de recursos web de toda la organización [5].

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

2.1 CREACIÓN DE MÁQUINAS VIRTUALES

La implementación se desarrolló utilizando el software de virtualización open Source llamado Oracle VirtualBox, debido a que esta herramienta permite crear entornos aislados para pruebas de seguridad informática sin afectar el sistema operativo anfitrión siendo esto ideal para realizar pruebas e implementaciones en entornos controlados. La infraestructura virtualizada estuvo compuesta por tres máquinas virtuales que representan los diferentes segmentos de una red perimetral empresarial.

La primera máquina virtual correspondió a GNU/Linux Endian Firewall, el cual fue configurado como dispositivo

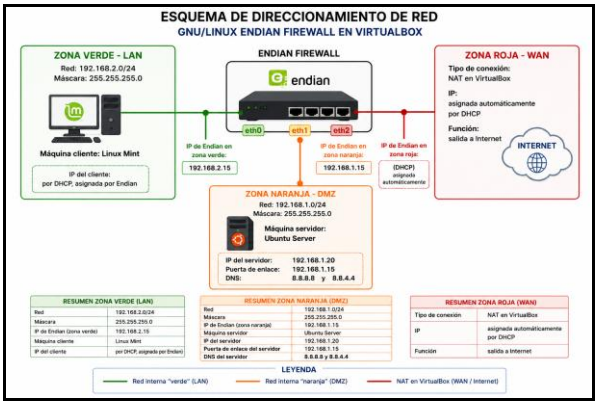
central de seguridad encargado del control de tráfico, administración de zonas y filtrado de paquetes entre las diferentes redes. Esta máquina se configuró con sistema operativo Linux de 64 bits, 2048 MB de memoria RAM y un disco duro virtual dinámico de 50 GB. La segunda máquina virtual fue Linux Mint, utilizada como cliente de la zona verde o LAN interna. Esta estación de trabajo permitió validar la asignación dinámica de direcciones IP mediante DHCP y comprobar la conectividad hacia el firewall y hacia Internet. La tercera máquina virtual correspondió a Ubuntu Server, implementada como servidor de la zona naranja o DMZ. La utilización de Ubuntu Server permitió simular un entorno empresarial donde los servicios críticos se encuentran aislados de la red interna con el fin de disminuir riesgos de acceso no autorizado.

Cada máquina virtual fue configurada con 2 GB de memoria RAM y un disco duro virtual dinámico de 50 GB. La asignación dinámica del almacenamiento permitió optimizar el uso de recursos del equipo anfitrión asegurando con ello que solo el espacio necesario sea ocupado, ya que el espacio físico únicamente aumenta conforme se almacenan datos dentro de las máquinas virtuales lo cual es una ventaja enorme en el tema de la optimización del uso de los recursos.

2.2 CONFIGURACIÓN DE ADAPTADORES DE RED

La configuración de los adaptadores de red representó una de las etapas más importantes de la implementación, debido a que de ella dependía el correcto funcionamiento de la segmentación de red y de las zonas de seguridad configuradas en Endian Firewall. Para la máquina virtual Endian se configuraron tres adaptadores de red independientes, siendo cada uno de estos asociados a una zona específica dentro de la infraestructura de red.

Figura 1.
Esquema de direccionamiento de la red



Fuente: Autoría Propia

El Adaptador 1 fue configurado como red interna con el nombre “verde”, permitiendo la comunicación entre Endian y la máquina Linux Mint. Esta red representa la LAN interna de la organización, donde se ubican los equipos cliente. El Adaptador 2 fue configurado igualmente como red interna, utilizando el nombre “naranja”. Esta interfaz permitió conectar Endian con Ubuntu Server, el cual se ubicó en la zona desmilitarizada o DMZ. La finalidad de esta segmentación consistió en aislar los servicios expuestos de la red interna principal. Finalmente, el Adaptador 3 fue configurado en modo NAT con el propósito de proporcionar acceso a Internet a través del sistema anfitrión. Esta interfaz simuló la zona roja o WAN de la infraestructura de red.

Linux Mint fue conectado únicamente a la red interna “verde”, mientras que Ubuntu Server se conectó exclusivamente a la red interna “naranja”. Esta segmentación permitió aislar el tráfico de cada zona y simular un entorno perimetral funcional similar al utilizado en escenarios reales de administración de redes y seguridad informática. Adicionalmente, se verificó que los nombres de las redes internas coincidieran exactamente entre las máquinas virtuales, debido a que VirtualBox diferencia entre mayúsculas y minúsculas. Un error en el nombre de la red interna impediría la comunicación entre los dispositivos virtualizados.

2.3 INSTALACIÓN DE GNU/LINUX ENDIAN

La instalación de GNU/Linux Endian Firewall se realizó mediante una imagen ISO montada desde la sección de almacenamiento de Oracle VirtualBox. Una vez iniciada la máquina virtual, el instalador presentó una interfaz en modo texto donde se seleccionó el idioma de instalación y se confirmó el uso completo del disco duro virtual. Durante el proceso de instalación se configuró inicialmente la interfaz correspondiente a la zona verde, asignando la dirección IP 192.168.2.15/24. Esta dirección fue utilizada posteriormente como puerta de enlace predeterminada para los equipos ubicados en la red LAN. Finalizada la copia de archivos y el reinicio del sistema, se accedió a la interfaz web de administración de Endian mediante el navegador Firefox desde Linux Mint. El acceso se realizó utilizando el protocolo HTTPS y el puerto 10443.

A través del asistente de configuración inicial se establecieron los parámetros principales del firewall. En primer lugar, se definió el modo de funcionamiento enrutado (Routing), permitiendo el tráfico entre las diferentes zonas de seguridad. Posteriormente, se habilitó la zona naranja correspondiente a la DMZ, configurando la dirección IP 192.168.1.15/24. La zona roja fue configurada automáticamente mediante DHCP utilizando la interfaz NAT proporcionada por VirtualBox.

Ubuntu Server fue configurado con dirección IP estática 192.168.1.20/24, debido a que los servidores requieren direcciones fijas para garantizar la disponibilidad de los servicios dentro de la red. Por otra parte, Linux Mint obtuvo direccionamiento dinámico mediante el servicio DHCP proporcionado por Endian Firewall en la zona verde. La configuración final permitió disponer de una arquitectura segmentada compuesta por una red LAN, una DMZ y una interfaz WAN virtualizada, estableciendo así una base adecuada para implementar políticas posteriores de seguridad y control de tráfico. Ubuntu Server fue configurado con dirección IP estática 192.168.1.20/24 y Linux Mint obtuvo direccionamiento dinámico mediante DHCP proporcionado por Endian.

2.4 RESULTADOS Y VERIFICACIÓN

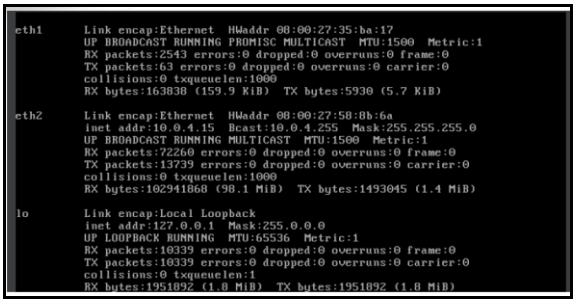
Las pruebas realizadas permitieron validar el correcto funcionamiento de la infraestructura virtualizada y confirmar que la segmentación de red implementada operaba adecuadamente en cada una de las zonas configuradas dentro de Endian Firewall. La primera verificación se realizó desde Ubuntu Server, ubicado en la zona naranja (DMZ). Desde la consola del sistema se ejecutó el comando ping 192.168.1.15, correspondiente a la interfaz naranja de Endian. Las respuestas obtenidas permitieron comprobar que el servidor podía comunicarse correctamente con el firewall a través de la red interna "naranja", confirmando que la configuración del adaptador de red y el direccionamiento IP eran correctos.

Posteriormente, desde Linux Mint se realizaron pruebas ICMP hacia la dirección IP 192.168.2.15 perteneciente a la interfaz verde de Endian Firewall. La recepción de respuestas exitosas confirmó el funcionamiento adecuado de la red LAN virtualizada y la correcta comunicación entre el cliente y el firewall. Además de las pruebas de conectividad, se verificó el direccionamiento IP asignado en cada máquina virtual utilizando el comando ip addr show. En Linux Mint se comprobó que el sistema recibió automáticamente una dirección IP dentro del rango 192.168.2.0/24 mediante el servicio DHCP proporcionado por Endian. Por otra parte, Ubuntu Server mantuvo correctamente la dirección IP estática 192.168.1.20/24 configurada durante la instalación.

Una de las verificaciones más importantes consistió en comprobar el acceso a Internet desde la zona verde. Para ello, desde Linux Mint se abrió el navegador web Firefox y se accedió correctamente a páginas externas como Google. La carga exitosa de los sitios web confirmó que Endian Firewall estaba direccionando adecuadamente el tráfico desde la zona verde hacia la zona roja mediante la interfaz NAT configurada en VirtualBox. Adicionalmente, se verificó desde el dashboard principal de Endian Firewall que las tres zonas de seguridad se encontraban activas y operativas. En el panel de administración fue posible visualizar la interfaz verde con la dirección IP 192.168.2.15, la interfaz naranja con la dirección IP 192.168.1.15 y la interfaz roja obteniendo direccionamiento automático mediante DHCP.

Las validaciones también incluyeron la administración de servicios desde la consola de Endian Firewall. Para ello, se accedió al Shell del sistema como usuario root y se ejecutaron diferentes comandos de administración y monitoreo. Inicialmente se utilizó el comando date con el fin de registrar la fecha y hora de ejecución de las verificaciones realizadas. Posteriormente, mediante el comando ifconfig se visualizaron todas las interfaces de red activas del firewall, permitiendo confirmar la correcta asignación de direcciones IP en cada zona.

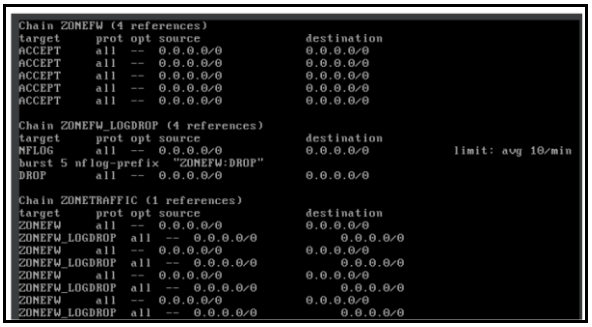
Figura 2.
Resultado del comando ifconfig



Fuente: Autoría Propia

Asimismo, se ejecutó el comando iptables -L -n para revisar las reglas activas del firewall configuradas automáticamente por Endian. Este comando permitió verificar las políticas de filtrado aplicadas sobre el tráfico entre las diferentes zonas de seguridad.

Figura 3.
Resultado del comando iptables -L -n



Fuente: Autoría Propia

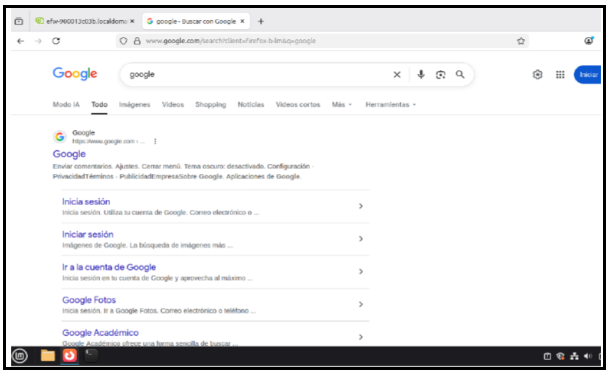
También se inspeccionaron los servicios disponibles dentro del sistema utilizando el comando ls /etc/init.d/, identificando servicios importantes como sshd, dhcp-server, dnsmasq y uplinksdaemon. Sobre estos servicios se realizaron operaciones de administración generando así buenas prácticas mediante comandos de estado y reinicio. Por ejemplo, se utilizaron instrucciones de administración de servicios tales como:

- /etc/init.d/sshd status
- /etc/init.d/sshd restart
- /etc/init.d/dhcp-server status
- /etc/init.d/dhcp-server restart
- /etc/init.d/dnsmasq status
- /etc/init.d/dnsmasq restart

La ejecución de estos comandos permitió verificar el funcionamiento de los servicios relacionados con administración remota, asignación dinámica de direcciones IP y resolución de nombres dentro de la infraestructura. En conjunto, las pruebas realizadas demostraron que la implementación de GNU/Linux Endian en VirtualBox funcionó correctamente, garantizando conectividad entre

zonas, acceso a Internet, administración de servicios y segmentación adecuada de la infraestructura virtualizada. Estos resultados proporcionan una base estable para la aplicación de configuraciones avanzadas relacionadas con reglas NAT, control de acceso, servicios de red y políticas de firewall.

Figura 4.
Linux Mint accediendo a Internet a través de Endian



Fuente: Autoría Propia

3 TEMÁTICA 2: CONFIGURACIÓN NAT EN ENDIAN FIREWALL

3.1 INFRAESTRUCTURA IMPLEMENTADA

La infraestructura virtualizada utilizada para la implementación estuvo compuesta por tres zonas de seguridad administradas mediante GNU/Linux Endian Firewall. La zona verde correspondió a la red LAN interna con direccionamiento 192.168.2.0/24. En esta red se ubicó la máquina Linux Mint utilizada como cliente para realizar pruebas de conectividad y navegación hacia Internet. La zona naranja correspondió a la DMZ con direccionamiento 192.168.1.0/24. Dentro de esta red se configuró un servidor Ubuntu Server con dirección IP estática 192.168.1.20, el cual fue utilizado para alojar servicios HTTP y FTP publicados mediante reglas NAT. Finalmente, la zona roja representó la conexión WAN hacia Internet utilizando el modo NAT proporcionado por Oracle VirtualBox. Las interfaces configuradas en Endian Firewall fueron las siguientes:

Figura 5.
Esquema general de la infraestructura implementada

Zona	Color	Red	IP de Endian	Máquina asociada	IP de la máquina
LAN	Verde	192.168.2.0/24	192.168.2.15	Linux Mint	DHCP
DMZ	Naranja	192.168.1.0/24	192.168.1.15	Ubuntu Server	192.168.1.20
WAN	Roja	NAT de VirtualBox	DHCP	Internet	No aplica

Fuente: Autoría Propia

3.2 CONFIGURACIÓN SOURCE NAT PARA LA ZONA VERDE

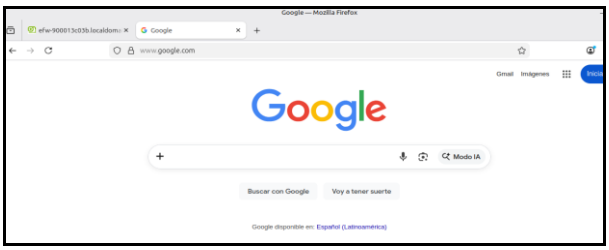
La primera configuración realizada correspondió a una regla Source NAT para permitir que los equipos ubicados en la red LAN pudieran acceder a Internet a través de la interfaz roja de Endian Firewall. La regla fue creada desde la sección NAT de la interfaz web administrativa de Endian. En esta configuración se definió como red origen la subred 192.168.2.0/24 perteneciente a la zona verde y como interfaz de salida la zona roja. El objetivo principal de esta regla consistió en traducir las direcciones privadas de la LAN hacia la dirección IP asignada dinámicamente en la zona WAN, permitiendo la navegación hacia Internet desde los equipos internos.

Figura 6.
Botón para agregar una nueva regla de Source NAT en Endian Firewall

Fuente: Autoría Propia

Posteriormente, desde Linux Mint se realizaron pruebas de conectividad utilizando comandos ICMP y navegación web, inicialmente se ejecutó el comando ping 8.8.8.8 y al ser la recepción de respuestas exitosas confirmó que la comunicación hacia internet estaba funcionando correctamente mediante NAT. De igual forma, se realizó una prueba adicional utilizando ping www.google.com, esta verificación permitió comprobar no solamente la conectividad externa, sino también el funcionamiento adecuado de la resolución DNS.

Figura 7.
Linux Mint accediendo a Internet mediante Endian Firewall

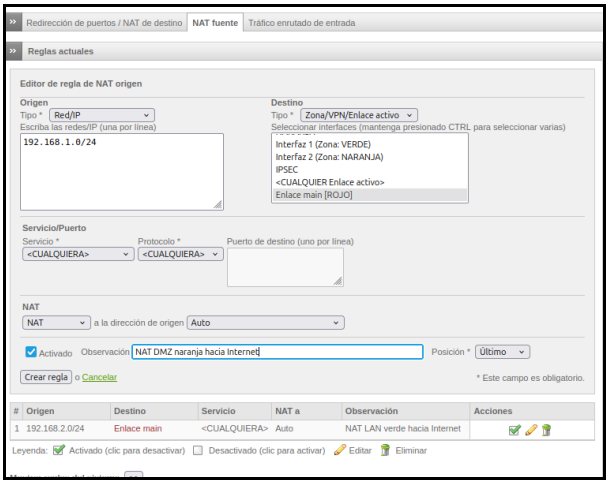


Fuente: Autoría Propia

3.3 CONFIGURACIÓN SOURCE NAT PARA LA ZONA NARANJA

Posteriormente se configuró una segunda regla Source NAT orientada a permitir el acceso a Internet desde la zona naranja o DMZ. La implementación de esta regla fue necesaria debido a que el servidor Ubuntu ubicado en la DMZ requería acceso externo para realizar actualizaciones, pruebas de conectividad y validación de servicios. La regla NAT fue configurada definiendo como origen la subred 192.168.1.0/24 y utilizando como interfaz de salida la zona roja del firewall.

Figura 8.
Configuración Source NAT para la zona naranja (DMZ)

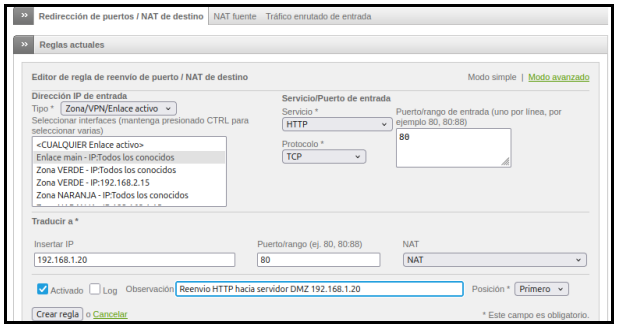


Fuente: Autoría Propia

3.4 CONFIGURACIÓN DE PORT FORWARDING

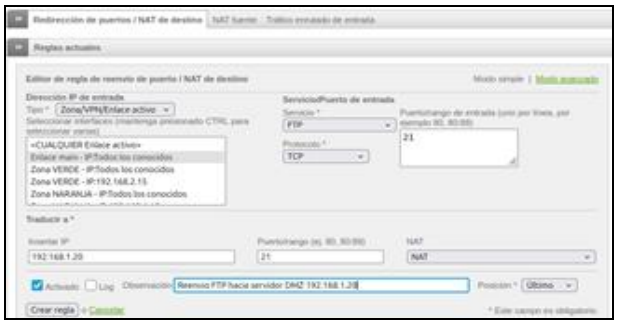
Una vez verificadas las reglas Source NAT, se procedió a implementar reglas de Port Forwarding o redirección de puertos. Estas reglas permitieron publicar servicios internos alojados en el servidor Ubuntu Server ubicado en la DMZ, facilitando el acceso externo desde la zona WAN. La primera regla configurada correspondió al servicio HTTP utilizando el puerto 80. Esta configuración permitió redirigir el tráfico entrante recibido en la interfaz roja hacia el servidor Ubuntu con dirección IP 192.168.1.20 (ver Fig. 9). Posteriormente, se configuró una segunda regla para el servicio FTP utilizando el puerto 21, redirigiendo igualmente el tráfico hacia el servidor ubicado en la DMZ. (ver Fig. 10). La implementación de estas reglas permitió simular un escenario empresarial donde los servicios públicos son publicados dentro de una zona desmilitarizada, manteniendo aislada la red LAN interna.

Figura 9.
Regla Port Forwarding para servicio HTTP



Fuente: Autoría Propia

Figura 10.
Regla Port Forwarding para servicios FTP



Fuente: Autoría Propia

3.5 PRUEBAS Y VERIFICACIÒN FINAL

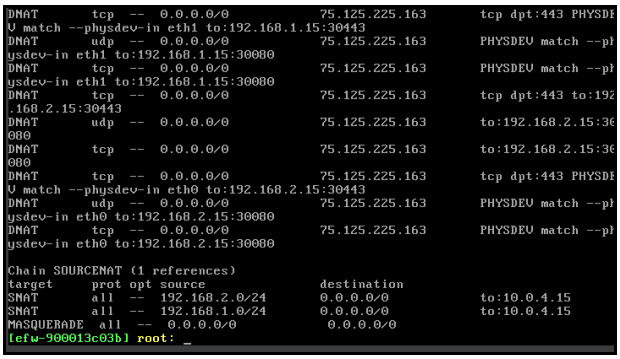
Con el propósito de validar el correcto funcionamiento de las reglas NAT implementadas, se realizaron diferentes pruebas desde las máquinas virtuales y desde la consola administrativa de Endian Firewall, desde Linux Mint se ejecutó el comando traceroute 8.8.8.8 y la salida obtenida mostró que el primer salto correspondía a la dirección IP 192.168.2.15, perteneciente a Endian Firewall, demostrando que el tráfico estaba siendo direccionado adecuadamente a través del firewall.

Figura 11.
Resultado del comando traceroute desde Linux Mint

Fuente: Autoría Propia

Adicionalmente, desde el Shell de Endian Firewall se verificaron las reglas activas con el fin de prevenir contingencias siendo esto una aplicación de buenas prácticas, para ello se utilizó el comando iptables -t nat -L -n, la salida permitió visualizar las reglas Source NAT y Port Forwarding configuradas previamente, confirmando que el firewall estaba aplicando correctamente las traducciones y redirecciones definidas.

Figura 12.
Verificación de reglas NAT mediante iptables



Fuente: Autoría Propia

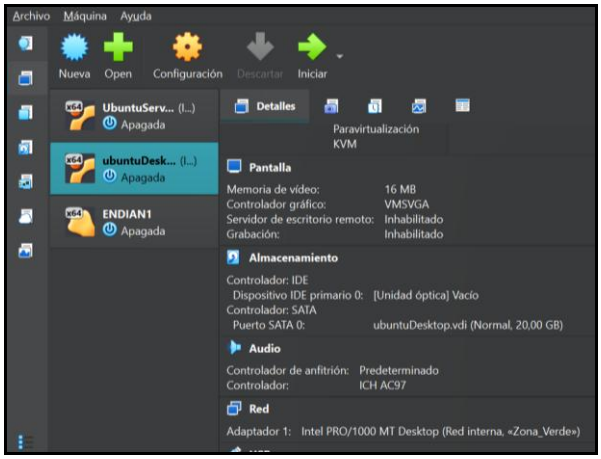
También se revisó la interfaz web de administración de Endian, observando que las reglas NAT aparecían activas y asociadas correctamente a las zonas correspondientes. En conjunto, las pruebas realizadas permitieron demostrar el correcto funcionamiento de las reglas NAT implementadas, garantizando acceso a Internet desde la LAN y la DMZ, así como la publicación controlada de servicios HTTP y FTP alojados dentro de la infraestructura virtualizada.

4 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

4.1 DISEÑO DE LA TOPOLOGIA

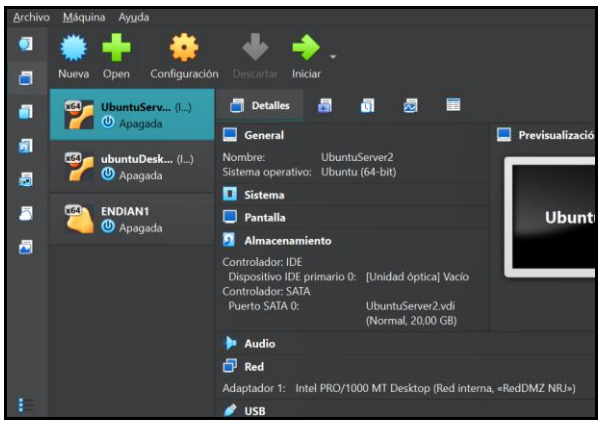
La topología de red se implementó mediante las tres zonas principales, [7] para la zona roja se configuró principalmente como la red para dar acceso al internet NAT, esta utilizada por Endian Firewall Community, para zona verde se configuró la máquina virtual Ubuntu desktop (Cliente) utilizada como la red LAN y finalmente para la zona naranja: la máquina virtual Ubuntu servidor destinado como DMZ. El Endian firewall Community funciona como un "sistema de gestión unificada de amenazas" (Endian, s.f.) tiene la capacidad de convertir equipos en gestores de acceso, por ende, se realiza la configuración de la zona de red mediante la información necesaria para cada uno de los tres adaptadores de red. [4], [6].

Figura 13.
Configuración adaptador 1 zona verde LAN Desktop



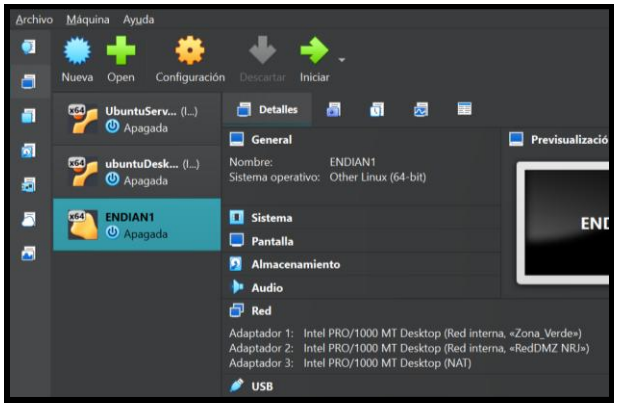
Fuente: Autoría Propia

Figura 14.
Configuración adaptador 2 zona naranja DMZ servidor



Fuente: Autoría Propia

Figura 15.
Configuración de adaptador 3 zona roja NAT Endian Firewall



Fuente: Autoría Propia

4.2 CONFIGURACION MAQUINA VIRTUAL

Se configuran las redes internas en el VirtualBox en donde La máquina desktop se relaciona a la red interna que corresponde a la zona verde y la máquina servidor se relaciona a la red interna destinada a la zona naranja (DMZ). Una vez que se ha instalado la máquina virtual Endian firewall Community, se accedió al asistente de red para crear el hostname, dominio y la interfaz correspondiente a cada zona de seguridad. [4], [6].

4.3 CONFIGURACIÓN DEL FIREWALL ENDIAN

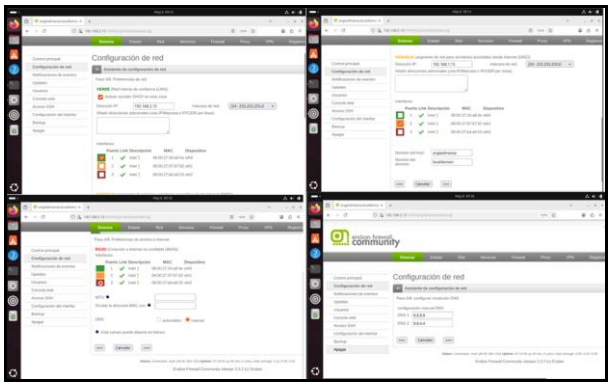
Desde el navegador de la máquina virtual desktop se accedió al panel del dashboard de Endian Firewall mediante la dirección https://192.168.2.15:10443 [3] la cual incluye la dirección asignada a Endian en la zona verde y el puerto de conexión 10443, pposteriormente, se verifico que el modo de red estuviera configurado y enrutado en la segmentación de las ip de cada zona de acuerdo con la topología de red definida previamente. [3], [8].

- Zona verde : 192.168.2.15
- Zona naranja: 192.168.1.15
- Zona DMZ: 192.168.1.20

También se configuraron los servidores del DNS:

- DNS1: 8.8.8.8
- DNS2: 8.8.4.4 (figura 4)

Figura 16.
Configuración de red en el Endian firewall.

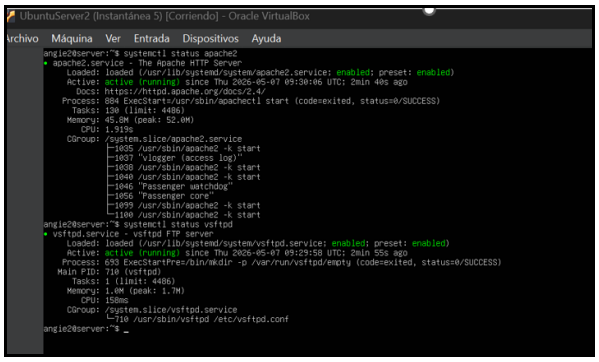


Fuente: Autoría Propia

4.4 IMPLEMENTACION DE SERVICIOS

Se realizaron las pruebas de conectividad desde el Ubuntu server utilizando los comandos ping hacia la IP de Endian con el ping 192.168.1.15 y a internet mediante el ping 8.8.8.8. Los resultados demostraron la comunicación correcta entre las zonas y el funcionamiento de la NAT. La instalación de los servicios HTTP y FTP, en el servidor Ubuntu se actualizan los servicios mediante el comando sudo apt update, posteriormente, se verifica que los servicios de apache2 (HTTP) y FTP estuvieran instalados y activos.

Figura 17.
Servicio de Apache2 (HTTP) y FTP activos.



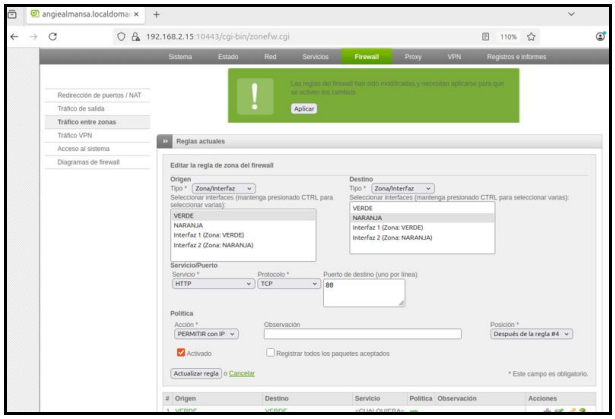
Fuente: Autoría Propia

Para dar acceso al servicio web alojado en la zona DMZ se procedió a realizar la configuración de la regla entre la zona verde asignada al cliente y la zona naranja asignada a los servidores, mediante el puerto 80. [3]. Para poder realizar la habilitación del servicio de HTTP, se creó una regla en Endian firewall desde su interfaz web ingresando en la opción Firewall – tráfico entre zonas, la configuración utilizada fue la siguiente:

- Origen: Zona verde
- Destino: Zona naranja
- Servicio: HTTP
- Puerto: 80
- Protocolo: TCP
- Acción: Permitir.

Después de guardar la regla se verifico la conectividad hacia el servidor mediante el puerto 80, comprobando el funcionamiento adecuado del servicio Apache2 (HTTP). [3].

Figura 18.
Configuración de HTTP Endian puerto 80.

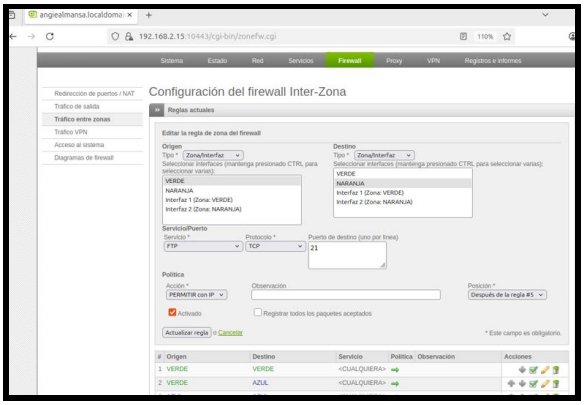


Fuente: Autoría Propia

La configuración de la regla FTP, se realizó de manera similar, creando una directiva que permitió el funcionamiento del servicio FTP entre la red LAN y la zona DMZ mediante la utilización del puerto21. [3]. Esta configuración posibilito la comunicación adecuada entre cliente y servidor para transferencia de los archivos. Las reglas fueron creadas utilizando el siguiente parámetro.

- Origen: Zona verde
- Destino: Zona naranja
- Servicio: FTP
- Puerto: 21
- Protocolo: TCP
- Acción: Permitir

Figura 19.
Configuración regla FTP puerto 21

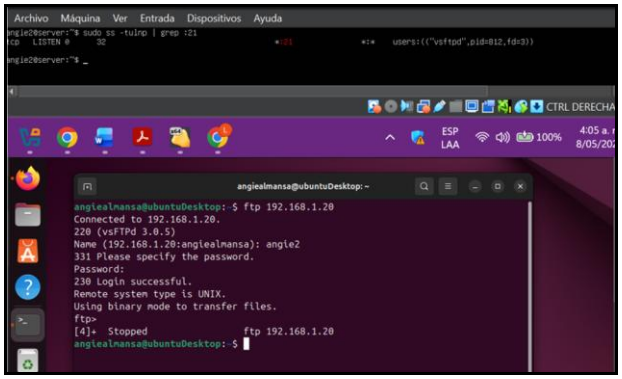


Fuente: Autoría Propia

Las pruebas realizadas desde la máquina virtual desktop, utilizada como cliente, y la máquina virtual configurada como servidor, permitieron comprobar el correcto funcionamiento del servicio FTP. Mediante las verificaciones realizadas se evidencio que el servidor se encontraba activo y respondiendo de manera adecuada a la solicitud realizada desde cliente. De este modo, se confirmó que la autentificación de usuario funciona mediante el ingreso de las credenciales configuradas previamente.

De igual forma, fue posible acceder al servicio de FTP sin inconvenientes, demostrando la comunicación efectiva entre ambas maquinas virtuales dentro de la red configurada. Estas pruebas permiten validar la disponibilidad, estabilidad y eficacia del servicio FTP implementado, garantizando el intercambio de información entre el cliente y servidor de manera satisfactoria (ver Fig.20).

Figura 20.
Prueba funcionamiento regla del puerto 21.



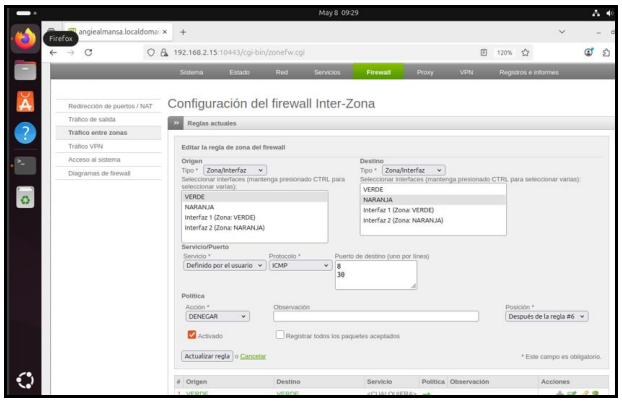
Fuente: Autoría Propia

4.5 BLOQUEO PROTOCOLO ICMP.

Con el objetivo de fortalecer la seguridad de la infraestructura de red, se implementó una regla que impidió las respuestas a solicitudes del protocolo ICMP, denegando de esta manera el uso del comando ping entre las diferentes zonas configuradas de la red [8], [10]. Esta configuración permitió restringir la detección y reconocimiento de equipos dentro de la infraestructura, aumentando el nivel de la protección frente a posibles accesos no autorizados, la solicitud de bloqueo ICMP se hace conforme a las políticas de seguridad establecidas. Las reglas fueron creadas utilizando el siguiente parámetro.

- Origen: Zona verde
- Destino: Zona naranja
- Servicio: ICMP echo reques
- Tipo ICMP: 8 y 30
- Acción: Denegar

Figura 21.
Configuración para denegar protocolo ICMP.

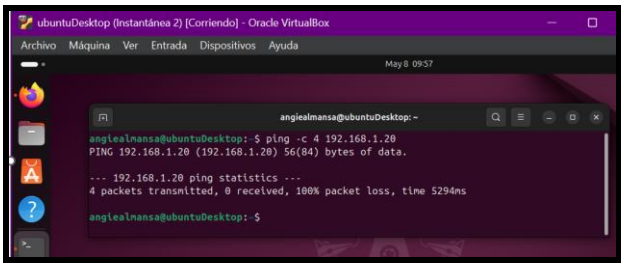


Fuente: Autoría Propia

Posteriormente, se realizaron las pruebas necesarias mediante consola utilizando el comando ping 192.168.1.20; como resultado, no se obtuvo respuesta desde el servidor en la zona DMZ, evidenciando el correcto funcionamiento del

bloqueo implementado [3]. De esta manera, se confirmo que las reglas de seguridad configuradas en firewall están operando de forma adecuada, impidiendo comunicación ICMP entre las zonas establecidas.

Figura 22.
Prueba de funcionamiento denegación del ping.



Fuente: Autoría Propia

4.5.1 RESULTADOS

Las pruebas efectuadas permiten verificar el adecuado funcionamiento de cada una de las reglas configuradas en Endian Firewall Community; también los servicios de HTTP y FTP fueron accesibles desde la red LAN al DMZ mediante el puerto 80 y 21. [3]. De igual manera, se bloqueó exitosamente el protocolo ICMP, evitando respuestas a solicitud mediante el uso de ping entre zona de configuración. [8], [10]. Por último, desde la sección de registro e informes en Endian firewall Community, fue posible analizar y verificar el tráfico que se generado en el proceso, dando paso a la correcta aplicación de la política de seguridad. [3].

5 TEMATICA 4: DESARROLLO E IMPLEMENTACION

5.1 REGLAS LAN → DMZ: HTTP y FTP

Desde la sección Firewall > Tráfico entre zonas, se establecieron dos reglas con origen VERDE y destino NARANJA, utilizando el protocolo TCP y la política PERMITIR CON IP: una para el puerto 80 (HTTP) y otra para el puerto 21 (FTP). La Fig. 1 ilustra la regla HTTP, que ya está listada y activa después de su implementación. La Fig. 2 presenta la tabla que incluye ambas reglas (HTTP TCP/80 y FTP TCP/21), confirmando así la creación exitosa de las dos directivas.

Figura 23.
Regla HTTP (TCP/80) de zona verde a zona naranja creada y activa en Endian Firewall

Fuente: Autoría Propia

Figura 24.
Tabla inter-zona con ambas reglas LAN→DMZ: HTTP (TCP/80) y FTP (TCP/21) activas.

Fuente: Autoría Propia

5.2 REGLAS WAN → DMZ: HTTP y FTP

Para permitir el acceso externo, se establecieron dos reglas adicionales con origen Red/IP 0.0.0.0/0 (zona roja) y destino NARANJA, manteniendo los mismos servicios y políticas. Estas reglas operan de manera complementaria al Port Forwarding (DNAT) previamente configurado: el DNAT especifica hacia dónde debe ser redirigido el tráfico; la regla inter-zona determina si se permite su paso. La Fig. 3 muestra la tabla completa con las nueve reglas activas, que incluyen las cuatro configuradas en este contexto (filas 6 a 9).

Figura 25.
Tabla completa del firewall inter-zona con las nueve reglas activas, incluyendo las cuatro de esta temática


El tercer punto solicita verificar en el tráfico inter-zona la creación de todas las reglas. Se ha accedido a la sección Firewall, Tráfico entre zonas y se ha capturado la tabla completa de reglas activas.

Figura 11

Tabla completa de reglas del firewall inter-zona mostrando todas las reglas creadas

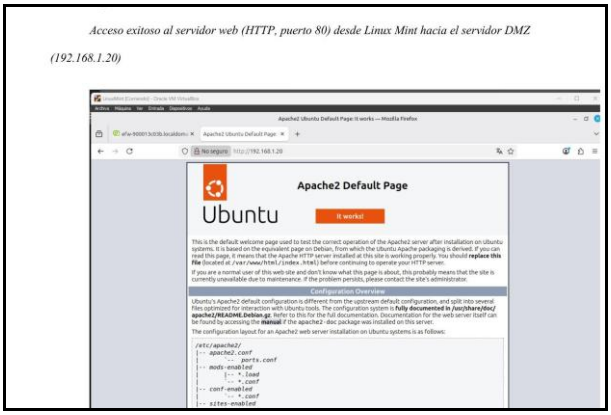
Fuente: Autoría Propia

5.3 PRUEBAS FUNCIONALES LAN HACIA DMZ

Se accedió a la dirección http://192.168.1.20 utilizando el navegador Firefox en el sistema operativo Linux Mint, la página predeterminada de Apache2 se cargó de manera correcta (ver Fig. 26), lo que confirma que el tráfico HTTP (TCP/80) desde la zona verde está permitido. El servicio FTP fue verificado mediante el comando ftp 192.168.1.20; la Fig.

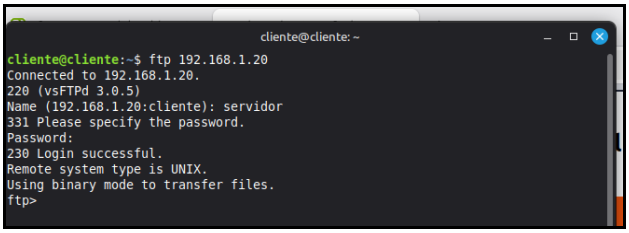
27 presenta el mensaje 230 Login successful de vsftpd 3.0.5 en el puerto 21, lo que confirma el acceso FTP desde la LAN.

Figura 26.
Acceso HTTP exitoso desde Linux Mint (LAN) al servidor Apache2 de la DMZ (192.168.1.20)



Fuente: Autoría Propia

Figura 27.
Conexión FTP exitosa desde Linux Mint (LAN) hacia el servidor vsftpd de la DMZ (puerto 21)



Fuente: Autoría Propia

5.4 WAN HACIA DMZ

Se accedió a la dirección IP de la zona roja (10.0.4.15:80) a través de HTTP. A través del reenvío de puertos, el tráfico fue redirigido a 192.168.1.20. La Fig. 6 ilustra la consola de Endian con las direcciones IP de la infraestructura y el navegador mostrando la página de Apache que se cargó exitosamente desde la zona roja, validando así la combinación de DNAT y la regla inter-zona. El acceso FTP desde la WAN también se verificó de manera similar utilizando ftp 10.0.4.15, siendo redirigido al servidor vsftpd en 192.168.1.20 mediante el Port Forwarding; la autenticación se completó con el mensaje 230 Login successful, confirmando el acceso FTP externo a la DMZ.

Con límites de servicio y puerto para reducir la superficie de ataque, en comparación con la autorización completa entre zonas y con una arquitectura LAN-DMZ-WAN en Endian Firewall es directamente aplicable a entornos reales, donde la DMZ actúa como una zona de transición, protegiendo la red interna, pero sin comprometer de forma práctica su correcta accesibilidad para servicios públicos establecidos y configurados.

6 IMPLEMENTACIÓN DE PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN

La consolidación de una arquitectura de seguridad perimetral segmentada en zonas de red (LAN, DMZ y WAN) demanda la integración de mecanismos robustos para el control de tráfico a nivel de aplicación [8]. En este contexto, el presente apartado detalla la configuración avanzada del sistema GNU/Linux Endian Firewall [3], [4], mediante la implementación de un proxy HTTP operando de manera estricta en modalidad no transparente. El propósito rector de esta directiva técnica es gobernar el flujo de paquetes hacia la red externa [5], restringiendo de forma categórica el acceso a dominios no corporativos mediante listas negras, e imponiendo un proceso obligatorio de validación de credenciales basado en grupos de seguridad [10]. De este modo, se complementa la infraestructura de red previamente cimentada sobre el entorno de virtualización [7], garantizando no solo la conectividad de los nodos internos gestionados como Ubuntu Desktop [1], sino también la trazabilidad, la integridad y el estricto cumplimiento de las políticas de seguridad y filtrado de la red.

6.1 DEFINICIÓN Y FUNCIONES DEL PROXY HTTP NO TRANSPARENTE

Un proxy HTTP no transparente opera como un nodo intermediario lógico situado entre la red de área local y la red externa, exigiendo una configuración manual y explícita en los equipos cliente para enrutar su tráfico web hacia el puerto de escucha designado en el cortafuegos [3], [5]. A diferencia de las implementaciones transparentes, esta topología de red imposibilita que un dispositivo no autorizado evada los controles perimetrales mediante el simple establecimiento de una conexión física a la infraestructura, otorgando a la administración un control absoluto sobre el flujo de la información [8]. Adicionalmente, este modelo arquitectónico constituye un requisito técnico indispensable para la integración de protocolos de validación de credenciales, lo cual habilita la aplicación granular de políticas de acceso, monitoreo de navegación y restricción basada en jerarquías o grupos de usuarios [10].

6.2 HABILITACIÓN Y CONFIGURACIÓN INICIAL DEL PROXY

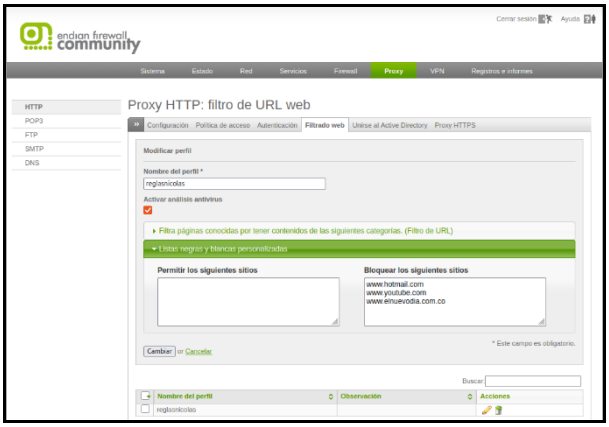
Para materializar el control de la navegación, se procedió a la activación del servicio de proxy HTTP sobre las interfaces correspondientes a las zonas LAN (verde) y DMZ (naranja), estableciendo su operatividad en modo no transparente a través del puerto lógico 8080 [4]. Esta directiva obliga a que toda petición HTTP proveniente de los terminales internos sea gestionada de forma exclusiva por el cortafuegos, sin posibilidad de evasión mediante configuraciones locales de red. La implementación inicial requiere la especificación del puerto de escucha y el modo operativo para habilitar la intercepción del tráfico (ver Fig. 28).

Figura 28.
Activación y configuración del proxy HTTP en Endian

Fuente: Autoría Propia

Posterior a la habilitación del servicio de intermediación, resulta imperativo establecer las reglas de restricción de contenido mediante un esquema de filtrado web [5]. Con este propósito, se estructuró un perfil de seguridad denominado “reglasnicolas”, orientado a denegar el tráfico hacia plataformas de entretenimiento y sistemas de mensajería no corporativos. Dentro de los parámetros estrictos de este perfil, se configuró una lista negra (blacklist) que incluye los dominios explícitos www.hotmail.com, www.youtube.com y www.elnuevodia.com.co [4]. La aplicación de este filtro bloquea de manera categórica la resolución y el acceso a dichos portales desde la red interna.

Figura 29.
Configuración del filtro de URL web o filtrado web



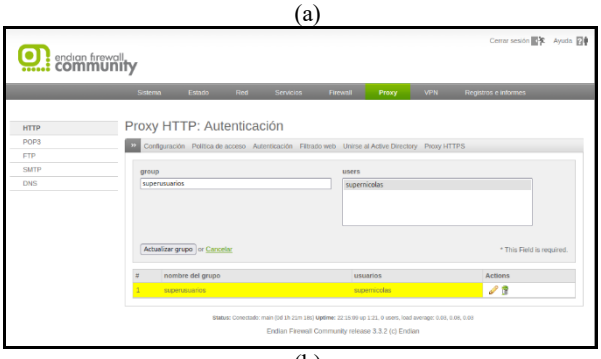
Fuente: Autoría Propia

6.3 AUTENTICACIÓN DE USUARIOS Y POLÍTICAS DE ACCESO

Para garantizar que únicamente el personal autorizado disponga de privilegios de conexión hacia la red externa, se implementó un mecanismo riguroso de control de identidades fundamentado en los principios de seguridad de la información [1]. A través del módulo de autenticación del servidor proxy gestionado por Endian Firewall [2], se efectuó la creación del usuario lógico “supernicolas”, el cual fue asociado de manera jerárquica al grupo de seguridad denominado “superusuarios”. Este procedimiento resulta vital para la administración de accesos, permitiendo establecer una auditoría precisa sobre los sujetos que consumen los recursos de ancho de banda en la infraestructura.

Figura 30.
Configuración para la autenticación mostrando (a) la creación del usuario "supernicolas" y (b) su asociación al grupo "superusuarios"

(a)

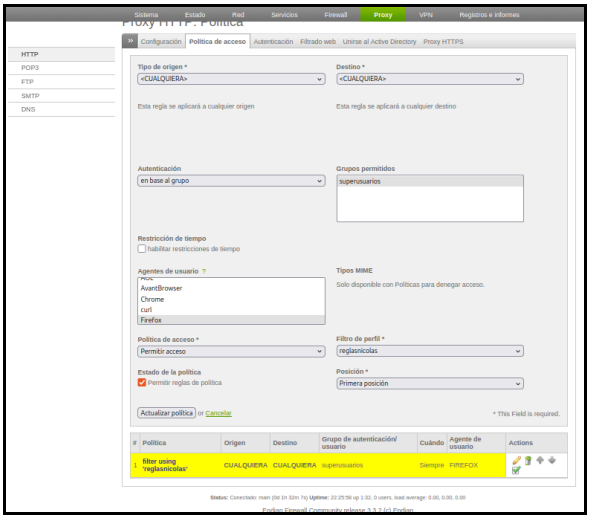


(b)

Fuente: Autoría Propia

Una vez estructuradas las identidades del sistema, se definió una política de acceso integral para gobernar el enrutamiento web. Esta directiva técnica se configuró con el propósito de interceptar el tráfico proveniente de cualquier origen hacia cualquier destino, condicionando la salida a Internet a una validación estricta de credenciales basada en el grupo “superusuarios”. De manera simultánea y complementaria, a esta directiva de autenticación se le vinculó el filtro de perfil “reglasnicolas” diseñado en la fase anterior [3]. Este enlace lógico y arquitectónico asegura que, aun cuando un usuario logre autenticarse exitosamente en el sistema perimetral, las restricciones impuestas por la lista negra prevalezcan de forma obligatoria, bloqueando la resolución de los dominios no corporativos (ver Fig. 31).

Figura 31.
Creación de política de acceso y vinculación al perfil creado

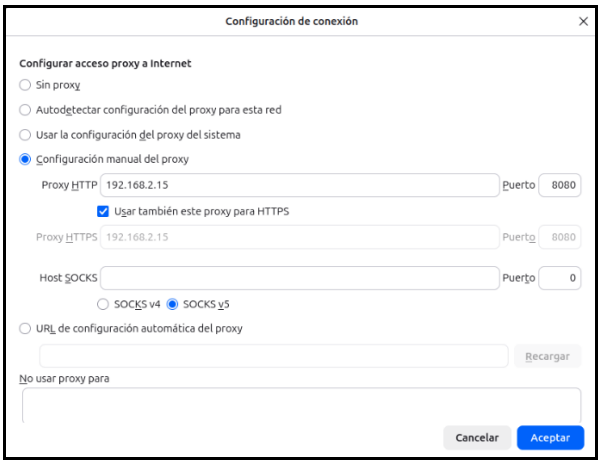


Fuente: Autoría Propia

6.4 APLICACIÓN Y VERIFICACIÓN EN LA RED LAN

Con la arquitectura de control desplegada en el firewall perimetral, la fase culminante consistió en la parametrización del nodo cliente (Ubuntu Desktop) alojado en la zona verde (LAN) [1]. En estricto cumplimiento del modelo no transparente, se procedió a configurar manualmente las propiedades de red del navegador web, enrutando todo el tráfico saliente de manera obligatoria hacia la dirección IP del proxy (192.168.2.15) a través del puerto 8080 [2], [3]. Este ajuste aísla las conexiones directas hacia la interfaz externa, obligando al cliente a someterse a las políticas de seguridad gestionadas por el firewall.

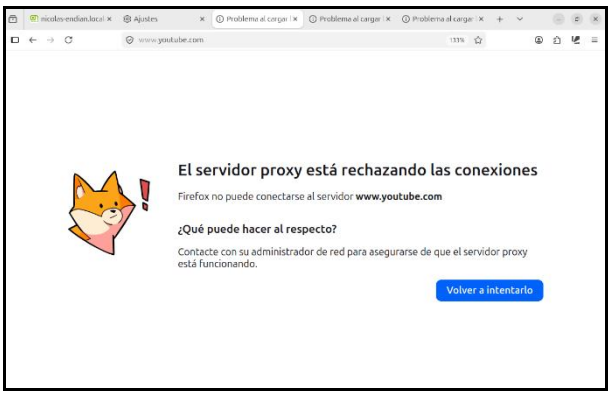
Figura 32.
Aplicación del proxy HTTP en el navegador del cliente



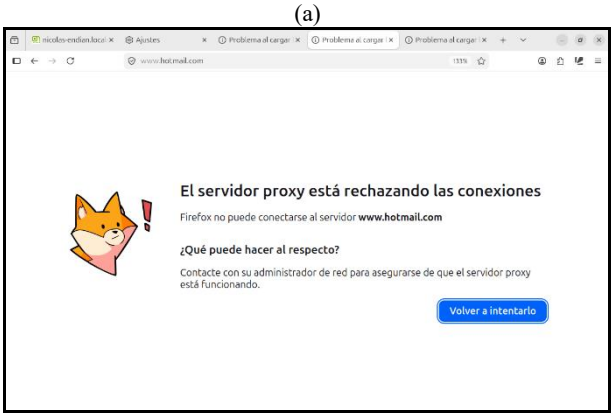
Fuente: Autoría Propia

La validación técnica de seguridad inició comprobando la efectividad del filtrado web. Al intentar establecer conexión con los dominios restringidos en la lista negra desde el navegador del cliente, el servidor proxy interceptó y denegó la resolución DNS y el tráfico HTTP de manera inmediata, arrojando un mensaje de conexión rechazada. Esta prueba empírica confirma la eficacia del perímetro frente a intentos de acceso a plataformas no autorizadas por la organización

Figura 33.
Aplicación efectiva de la lista negra en el proxy HTTPpara (a) YouTube, (b) Hotmail y (c) El Nuevo Día



(a)



(b)

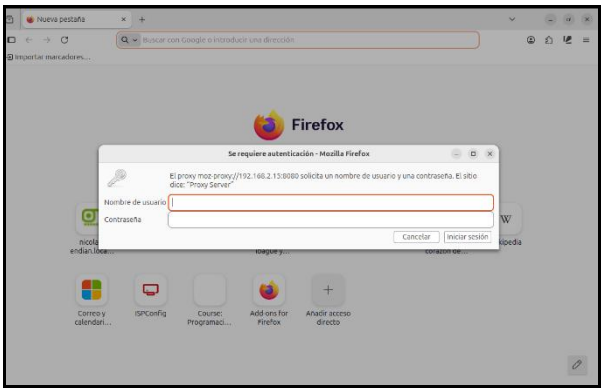
(c)

Fuente: Autoría Propia

Finalmente, para evaluar la directiva de control de acceso, se simuló una petición hacia un dominio no restringido. Como mecanismo de protección, el sistema

interrumpió la navegación para exigir la validación de identidad [4]. Tras suministrar las credenciales del usuario autorizado y validarse su pertenencia al grupo de seguridad, el proxy permitió el flujo de paquetes hacia la red externa. Este comportamiento demuestra que la navegación a Internet está condicionada ineludiblemente a la autenticación del usuario, cerrando el ciclo de seguridad y auditoría en la red LAN.

Figura 34.
Aplicación de las políticas de autenticación para acceso a Internet.



Fuente: Autoría Propia

7 CONCLUSIONES

La implementación de Endian Firewall en un entorno virtualizado permite concluir que la seguridad perimetral efectiva trasciende la mera instalación de software, fundamentándose en un diseño riguroso de la arquitectura de red y una segmentación funcional de zonas (Verde, Naranja y Roja). Esta estructura no solo organiza el tráfico según su nivel de exposición, sino que actúa como el prerrequisito técnico indispensable para la correcta aplicación de políticas de filtrado, reglas NAT y servicios de proxy. Se evidencia que la integridad del sistema depende críticamente de la configuración en la capa de virtualización, donde la precisión en la asignación de adaptadores y direccionamiento IP asegura la interoperabilidad y la coherencia en el trabajo colaborativo. Finalmente, la validación operativa mediante pruebas de conectividad y el aislamiento de servicios críticos en una Zona Desmilitarizada (DMZ) consolidan un modelo de administración centralizada que replica con exactitud los principios de protección de activos y control de tráfico exigidos en infraestructuras de red reales bajo estándares profesionales.

La implementación de reglas Source NAT en GNU/Linux Endian Firewall permitió garantizar el acceso a Internet desde las zonas LAN y DMZ, demostrando el correcto funcionamiento de la traducción de direcciones de red dentro de una infraestructura segmentada. Además, la implementación de Endian firewall Community funciona como sistemas de gestión unificada de amenazas [3] permitió administrar de forma eficaz y eficiente el tráfico de las zonas de red mediante las reglas de seguridad indicadas, configurar los servicios de HTTP y FTP en la zona DMZ demostrando la capacidad del firewall para controlar el acceso a recursos internos sin necesidad de comprometer la seguridad en la red LAN [5]. Las reglas de acceso entre zonas fueron correctamente creadas y configuradas en Endian Firewall, lo que llevó a la comunicación controlada de LAN, DMZ y WAN. Las pruebas funcionales confirmaron que HTTP y FTP funcionan exitosamente en cada una de las combinaciones necesarias en las zonas correspondientes.

La implementación de un proxy HTTP en modalidad no transparente a través de GNU/Linux Endian Firewall demostró ser una medida altamente efectiva para el control y la auditoría del tráfico web en la red de área local (LAN). Se evidenció que condicionar la salida a Internet a una configuración manual en el cliente elimina el riesgo de evasión de políticas perimetrales por conexiones no autorizadas, fortaleciendo el control de acceso en la infraestructura [2], [3]. Asimismo, la creación de directivas de filtrado web, materializadas mediante listas negras, permitió bloquear con éxito la resolución de dominios no corporativos específicos, mitigando el consumo innecesario de ancho de banda y reduciendo la exposición de la red interna [4]. Finalmente, la integración de políticas de acceso basadas en la autenticación obligatoria de grupos y usuarios garantizó que únicamente el personal validado pudiese establecer conexiones hacia la red externa [5], cumpliendo a cabalidad con los principios rectores de seguridad perimetral en arquitecturas modernas.

8 REFERENCIAS

[1] Canonical. (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

[2] Debian. (2023). El manual del administrador de Debian 12.5.0. Debian. https://www.debian.org/releases/stable/amd64/index.es.html

[3] Endian Firewall Community. (2016). Endian UTM 3.2 Manual referencia. Endian. http://docs.endian.com/3.2/utm/index.html

[4] GNU Project. (s.f.). GNU/Linux System Administration Documentation. Recuperado de: https://www.gnu.org

[5] Kurose, J., & Ross, K. (2017). Computer Networking: A Top-Down Approach. Pearson Education.

[6] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[7] Oracle Corporation. (2020). Oracle VM VirtualBox User Manual. Recuperado de: https://www.virtualbox.org/manual/

[8] Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.

[9] The Linux Documentation Project. (s.f.). iptables Tutorial. Recuperado de: https://www.linux.org

[10] Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.