IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Eider Andres Castilla Landinez
eacastillal@unadvirtual.edu.co
Yudith Paola Barrios Portilla
ypbarriosp@unadvirtual.edu.co
Heinner Chayanne Rojas Uribe
hcrojasu@unadvirtual.edu.co
Víctor Alfonso Pineda Torres
vapinedat@unadvirtual.edu.co
Roberto José Lázaro Sepulveda
rjlazaros@unadvirtual.edu.co

RESUMEN: *Este artículo documenta la implementación completa de una infraestructura de seguridad perimetral utilizando GNU/Linux Endian como firewall multipropósito. El desarrollo abarca desde la configuración inicial y segmentación de red en zonas verde, naranja y roja, hasta la implementación de reglas NAT para conectividad saliente y publicación de servicios. Se detalla el control granular aplicado a servicios HTTP y FTP junto con la restricción del protocolo ICMP, complementado con el establecimiento de reglas de firewall para comunicación inter-zonal. Finalmente, se despliega un proxy Squid con autenticación y políticas de filtrado para el control de navegación. Las pruebas de conectividad y los registros de tráfico confirmaron el funcionamiento efectivo de cada capa de seguridad, demostrando que Endian constituye una solución enterprise integral para la gestión de redes que combina filtrado avanzado, control de acceso y capacidades de proxy en una plataforma unificada de código abierto.*

PALABRAS CLAVE: Endian, Linux, Segmentación, Seguridad, DMZ, NAT, Proxy HTTP.

1 INTRODUCCIÓN

En un entorno digital donde las amenazas de ciberseguridad crecen de forma exponencial, la protección perimetral de las redes se ha convertido en una necesidad crítica para organizaciones de todos los tamaños. Los firewalls, como primera línea de defensa, no solo deben controlar el acceso a la red, sino también segmentar el tráfico, gestionar servicios y garantizar que las comunicaciones internas y externas se realicen de manera segura y eficiente. Este artículo presenta una implementación práctica del firewall GNU/Linux Endian, una solución de código abierto que combina robustez, flexibilidad y un amplio conjunto de herramientas para la administración avanzada de redes. A lo largo de esta guía, se detallan los pasos para configurar un entorno segmentado en zonas verdes (LAN), naranjas (DMZ) y rojas (WAN), implementar reglas NAT y de control de tráfico, y desplegar un proxy con autenticación mediante Squid. Cada temática está respaldada con evidencia práctica, configuraciones reales y pruebas de funcionamiento, ofreciendo así un marco replicable para administradores de sistemas, estudiantes de redes y profesionales de la seguridad que buscan fortalecer sus infraestructuras con herramientas accesibles y poderosas.

2 OBJETIVO GENERAL

Implementar en un entorno virtual una infraestructura de red segura apoyada en Endian Firewall, estableciendo las zonas LAN, DMZ y WAN y aplicando mecanismos de firewall, NAT y control de servicios que regulen el flujo de información entre cada segmento.

2.1 OBJETIVOS ESPECIFICOS

Desplegar y parametrizar la máquina virtual de Endian Firewall en VirtualBox, asignando adecuadamente las interfaces de red asociadas a las zonas VERDE (LAN), ROJA (WAN) y NARANJA (DMZ).

Diseñar e implementar reglas de traducción de direcciones (NAT) que habiliten una comunicación controlada entre las redes LAN, DMZ y WAN, garantizando el enrutamiento correcto del tráfico.

Publicar y asegurar servicios expuestos en la DMZ, como HTTP y FTP, aplicando restricciones específicas sobre los protocolos permitidos e impidiendo el uso de ICMP desde y hacia este segmento.

Definir políticas de filtrado inter-zona que regulen el flujo de paquetes entre LAN, DMZ y WAN, estableciendo reglas explícitas de permiso y denegación acorde con los criterios de seguridad planteados.

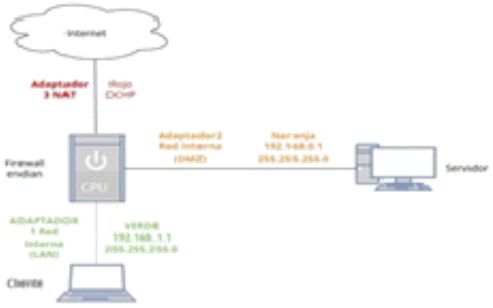
Configurar un proxy HTTP no transparente en Endian Firewall, incorporando mecanismos de autenticación de usuarios y listas negras de sitios para ejercer un control granular sobre la navegación web.

3 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

Para la temática 1 se aborda la instalación y configuración de Endian, una distribución GNU/Linux orientada a funcionar como firewall perimetral, cuyo propósito principal es controlar y proteger el tráfico que circula entre Internet y las distintas redes internas de la organización.

Como punto de partida, resulta fundamental definir la segmentación de red, ya que esta proporciona la estructura lógica sobre la cual se planifica la implementación de las zonas (LAN, DMZ y WAN) y se determinan las rutas y políticas de seguridad que será necesario aplicar..

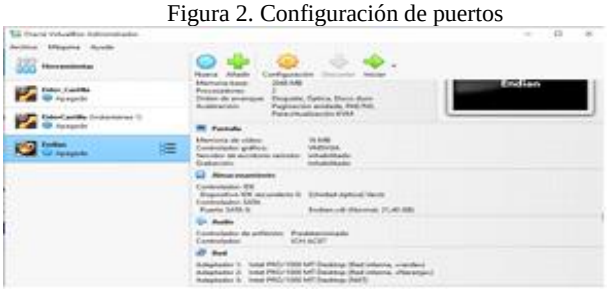
Figura 1. Segmentación de red



Fuente: Autoría Propia

Como segundo paso es necesario, la configuración de cada puerto tanto en los equipos clientes como en el firewall Endian, creando zonas como indica la segmentación de red.

Figura 2. Configuración de puertos



Fuente: Autoría Propia

Una vez configurados los puertos de cada una de las máquinas, se puede, proceder a la instalación del firewall Endian, en el transcurso de esta también queda configurada la zona verde.

Figura 3. Instalación de Linux Endian

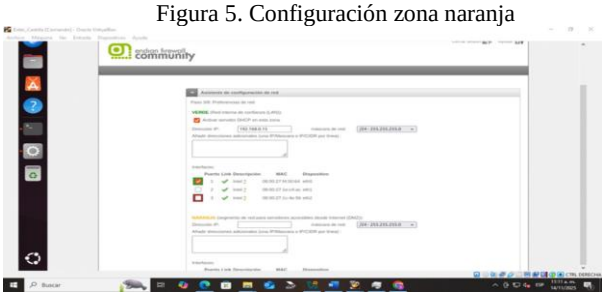
Fuente: Autoría Propia

Figura 4. Zona verde configurada

Fuente: Autoría Propia

En este punto ya podemos ingresar a un equipo cliente, desde la barra direcciones de un buscador y digitando la ip que se le asignó al firewall podemos entrar a su interfaz gráfica y configurar la zona naranja.

Figura 5. Configuración zona naranja



Fuente: Autoría Propia

Ya terminada la configuración de las zonas podemos apreciar su funcionamiento desde la interfaz del firewall.

Figura 6. Verificación configuración completa

Fuente: Autoría Propia

4 TEMÁTICA 2: CONFIGURACIÓN NAT

4.1 CONFIGURACIÓN DE NAT DESDE LA LAN HACIA LA WAN

Para validar la conectividad desde la LAN hacia Internet, se configuró una regla de tipo NAT que permite la traducción de múltiples direcciones privadas hacia una dirección pública mediante PAT. La prueba de navegación web desde la red interna confirma que el firewall está traduciendo correctamente el tráfico y permitiendo su salida hacia la WAN.

Figura 7. Configuración de NAT desde LAN hacia la WAN

Fuente: Autoría Propia

4.2 VERIFICACIÓN FUNCIONAL DEL NAT

Se ejecutaron pruebas de eco (ping) hacia dominios externos, verificando tanto la traducción de direcciones realizada por el firewall como la resolución de nombres a través de los servidores DNS configurados. Los resultados confirmaron el correcto funcionamiento del mecanismo de NAT y la comunicación entre las redes internas y la zona WAN..

Figura 8. Verificación funcional de la NAT

Fuente: Autoría Propia

4.3 CONFIGURACIÓN DE NAT PARA LA ZONA DMZ

Se implementó una regla NAT de destino (DNAT) para permitir la publicación de servicios alojados en la DMZ hacia Internet. Mediante reglas configuradas en el firewall, el tráfico entrante TCP y UDP es redirigido hacia la dirección privada del servidor en la DMZ, garantizando así de manera correcta el aislamiento y la seguridad de la red.

Figura 9. Configuración NAT para la zona DMZ

Fuente: Autoría Propia

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

Esta temática se centra en la implementación de reglas de control de tráfico en Endian Firewall, orientadas a publicar los servicios HTTP y FTP para su consumo desde Internet y, al mismo tiempo, restringir el uso del protocolo ICMP con el fin de fortalecer la postura de seguridad de la infraestructura.

5.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21) DESDE EL SERVIDOR WEB

Se configura una regla de redirección de puertos que permite exponer el servicio FTP de la DMZ a cualquier dirección IP de la red externa. De este modo, Endian recibe las conexiones entrantes, las redirige internamente hacia el servidor FTP y devuelve la respuesta al cliente que originó la solicitud.

Figura 10. Configuración de la regla FTP

Fuente: Autoría Propia

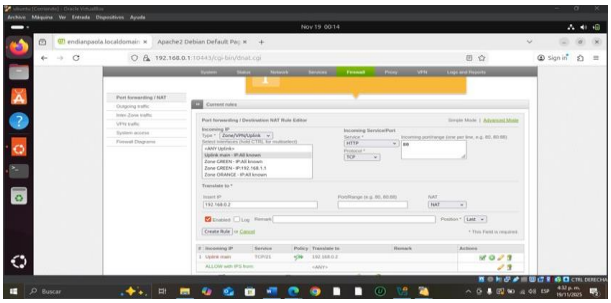
Para comprobar el correcto funcionamiento de la regla, se accedió al servicio FTP expuesto por el servidor de la DMZ identificado con la dirección IP 192.168.0.2. Desde la terminal del equipo cliente se ejecutó el comando ftp contra dicho servidor, tras lo cual el sistema solicitó las credenciales de usuario y contraseña; una vez autenticada la sesión, se obtuvo acceso al servicio, evidenciando que la publicación del FTP a través de Endian opera de manera adecuada.

Figura 11. Comprobación de la regla FTP

Fuente: Autoría Propia

Se replica el mismo proceso para la creación de la regla FTP, pero haciendo foco en el servicio HTTP.

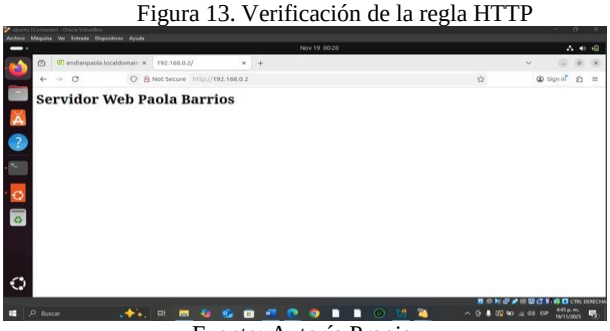
Figura 12. Configuración de la regla HTTP



Fuente: Autoría Propia

Para verificar el funcionamiento de la regla, se accedió desde el equipo cliente a la página web alojada en el servidor de la DMZ utilizando la dirección IP 192.168.0.2. Tal como se aprecia en la imagen, la carga correcta del sitio confirma que el acceso HTTP a través de Endian se realiza de forma adecuada.

Figura 13. Verificación de la regla HTTP

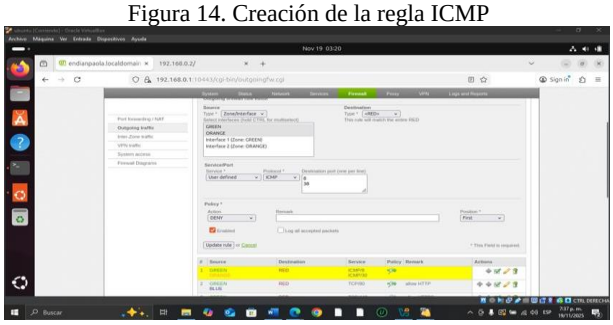


Fuente: Autoría Propia

5.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR HACER PING EN LA RED.

Se define una regla de firewall cuyo origen son las zonas VERDE y NARANJA y cuyo destino es la zona ROJA, con el objetivo de denegar el envío de paquetes ICMP hacia la red externa. En dicha regla se bloquean específicamente las solicitudes de eco (ICMP tipo 8) y otros tipos asociados, de modo que se impide la realización de ping hacia direcciones externas y se refuerza la seguridad al limitar la información expuesta sobre la infraestructura interna.

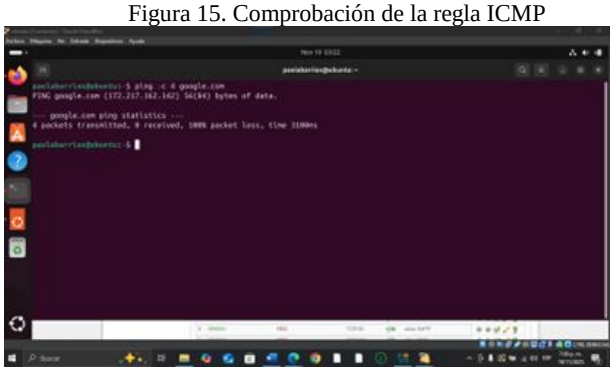
Figura 14. Creación de la regla ICMP



Fuente: Autoría Propia

En la imagen se observa que, al ejecutar el comando ping, no se recibe respuesta a los paquetes enviados; al finalizar, la salida solo indica el número de paquetes transmitidos, sin confirmación de recepción. Este comportamiento confirma que la regla de bloqueo ICMP se encuentra aplicada correctamente y está impidiendo las respuestas de eco desde la red de destino.

Figura 15. Comprobación de la regla ICMP



Fuente: Autoría Propia

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

La finalidad de esta temática busca configurar e implementar distintas reglas de firewall para los servicios HTTP y FTP, controlando cómo se comunican las zonas de red LAN (VERDE), DMZ (NARANJA) e Internet/WAN (ROJO).

Para ello se simulan clientes y servidores en cada zona, se aplican reglas de acceso y NAT, y se verifican las conexiones mediante pruebas prácticas y revisión de los registros de tráfico inter-zona.

6.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

Para permitir el acceso HTTP entre la zona VERDE (LAN) y la zona NARANJA (DMZ) se creó en Endian una regla específica de "tráfico entre zonas" que autoriza las conexiones HTTP TCP/80 desde el cliente Ubuntu Desktop (Zona Verde) hacia el servidor Ubuntu Server (Zona Naranja). Sobre este servidor se instaló y habilitó el servicio Apache2, de modo que la DMZ ofreciera un sitio web accesible solo a través del firewall.

Figura 16. Creación de la regla HTTP LAN - DMZ

Fuente: Autoría Propia

De forma análoga, para habilitar el servicio FTP entre la zona VERDE y la zona NARANJA se instaló el servidor vsftpd en la máquina de la DMZ (192.168.0.2) y se creó una regla de firewall que permite conexiones TCP/21 desde la LAN hacia dicha red. Esta configuración garantiza que cualquier cliente autorizado en la zona VERDE pueda autenticarse contra el servidor FTP de la DMZ, manteniendo siempre el control del flujo a través de Endian.

Figura 17. Creación de la regla FTP LAN - DMZ

Fuente: Autoría Propia

6.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Para comunicar la zona Internet con la DMZ mediante HTTP se configuraron reglas de "Redirección de puertos / NAT de destino" en Endian, de forma que todo el tráfico entrante por la interfaz ROJA al puerto 80/TCP se traduzca hacia el servidor web de la DMZ (192.168.0.2:80). Adicionalmente, en el adaptador NAT de la máquina virtual de Endian en VirtualBox se definió un reenvío de puertos desde el equipo anfitrión (127.0.0.1:8080) hacia el puerto 80 del cortafuegos, simulando así un cliente externo en Internet.

Figura 18. Creación de la regla HTTP WAN - DMZ

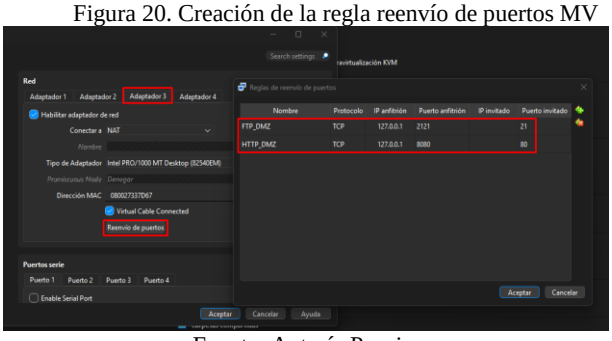
Fuente: Autoría Propi

De manera similar, para exponer el servicio FTP de la DMZ hacia la zona Internet se creó en Endian una regla de NAT de destino que redirige las conexiones entrantes al puerto 21/TCP de la interfaz ROJA hacia el servidor FTP (vsftpd) ubicado en 192.168.0.2. En VirtualBox se habilitó un segundo reenvío de puertos, mapeando el puerto 2121 del anfitrión a dicho puerto 21 de Endian, lo que permite simular clientes FTP externos conectándose a 127.0.0.1:2121.

Figura 19. Creación de la regla FTP WAN - DMZ

Fuente: Autoría Propia

Figura 20. Creación de la regla reenvío de puertos MV



Fuente: Autoría Propia

6.3 VERIFICAR EN EL TRÁFICO INTER ZONA, LA CREACIÓN DE LAS REGLAS.

Para verificar la correcta creación y funcionamiento de las reglas de firewall, se utilizó el módulo de registros de Endian en la sección de tráfico inter-zona.

Figura 21. Verificación regla tráfico inter-zona Endian

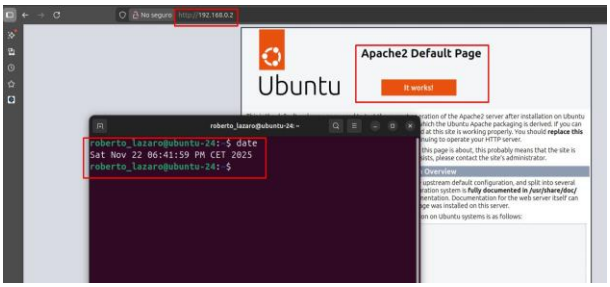
Fuente: Autoría Propia

6.4 PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS.

6.4.1 EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ:

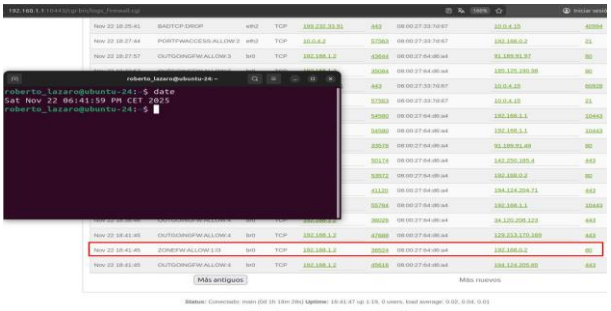
Para comprobar el ingreso del servicio HTTP desde la LAN hacia la zona DMZ se utilizó el equipo Ubuntu Desktop ubicado en la red VERDE. Desde su navegador web se accedió a la dirección http://192.168.0.2, correspondiente al servidor Apache alojado en la DMZ, verificando que la página por defecto de Apache2 se cargaba correctamente. Esta prueba confirmó que las reglas de tráfico entre zonas configuradas previamente permiten el acceso HTTP desde la LAN hacia la DMZ, lo cual se corroboró adicionalmente revisando los registros del firewall, donde se observaron entradas GREEN → ORANGE en el puerto 80/TCP con acción de aceptación.

Figura 22. Prueba ingreso servicio HTTP desde LAN a DMZ



Fuente: Autoría Propia

Figura 23. Verificación registros Endian servicio HTTP desde LAN a DMZ

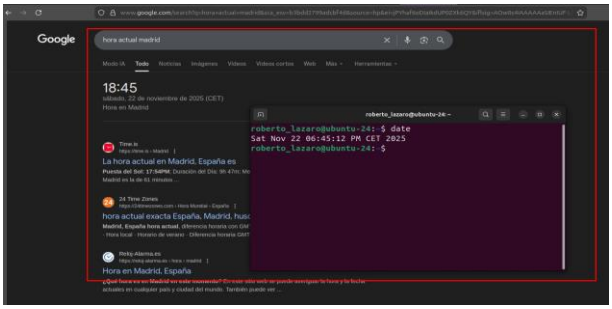


Fuente: Autoría Propia

6.4.2 EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA WAN:

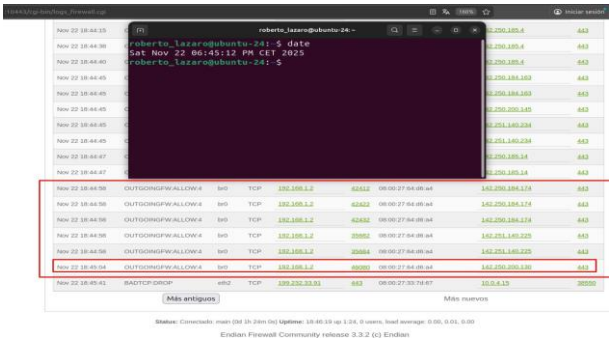
El ingreso del servicio HTTP desde la LAN hacia la WAN se validó accediendo, también desde el navegador del equipo en la zona VERDE, a sitios externos como http://www.google.com. La carga satisfactoria de la página, junto con la aparición en los logs de Endian de conexiones GREEN → RED hacia direcciones IP públicas en el puerto 80/TCP marcadas como OUTGOINGFW:ALLOW, evidenció que la LAN dispone de salida a Internet por HTTP a través del cortafuegos, respetando las políticas de tráfico de salida definidas.

Figura 24 Prueba ingreso servicio HTTP desde LAN a WAN



Fuente: Autoría Propia

Figura 25. Verificación registros Endian servicio HTTP desde LAN a WAN



Fuente: Autoría Propia

6.4.3 EL INGRESO DEL SERVICIO HTTP DESDE LA DMZ HACIA LA WAN:

Para el ingreso del servicio HTTP desde la zona DMZ hacia la WAN se ejecutaron peticiones web desde el servidor Ubuntu Server de la DMZ mediante la herramienta curl, apuntando igualmente a recursos externos. El éxito de estas solicitudes, unido a los registros ORANGE → RED en el puerto 80/TCP, confirmó que la DMZ puede acceder a Internet de forma controlada.

Figura 26 Prueba ingreso servicio HTTP desde DMZ a WAN

Fuente: Autoría Propia

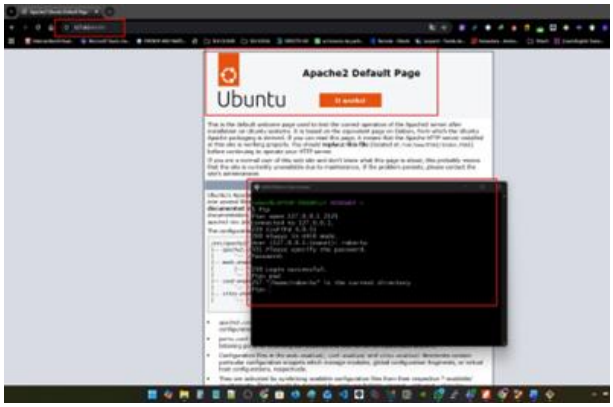
Figura 27 Verificación registros Endian servicio HTTP desde DMZ a WAN

Fuente: Autoría Propia

6.4.4 EL INGRESO DEL SERVICIO HTTP DESDE LA WAN HACIA LA ZONA DMZ:

Para el ingreso del servicio HTTP desde la WAN hacia la zona DMZ se comprobó simulando un cliente externo desde el equipo anfitrión Windows, accediendo en el navegador a http://127.0.0.1:8080. Gracias al reenvío de puertos en VirtualBox y a las reglas de NAT de destino en Endian, estas conexiones fueron traducidas hacia 192.168.0.2:80, mostrando la página de Apache de la DMZ y registrando tráfico RED → ORANGE aceptado en el firewall.

Figura 28 Prueba ingreso servicio HTTP desde WAN a DMZ



Fuente: Autoría Propia

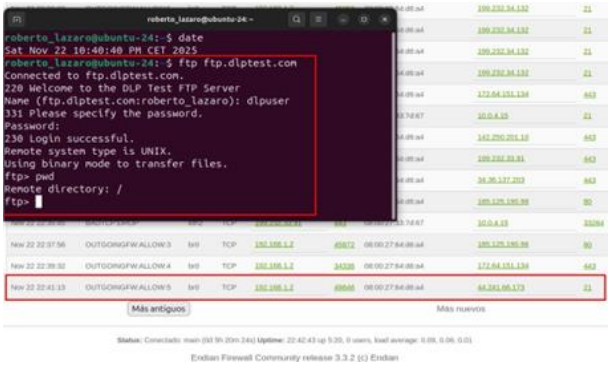
Figura 29 Verificación registros Endian servicio HTTP desde WAN a DMZ

Fuente: Autoría Propia

6.4.5 EL INGRESO DEL SERVICIO FTP DESDE LA LAN HACIA LA WAN:

En el caso del servicio FTP desde la LAN hacia la WAN, se utilizó el cliente FTP del equipo Ubuntu Desktop para intentar establecer conexiones contra servidores FTP públicos alojados en Internet. Para poder realizar una prueba más completa se hizo uso del servicio FTP público https://dlptest.com/ftp-test/, ejecutando así una prueba completa, en los registros del firewall se observaron intentos de salida GREEN → RED al puerto 21/TCP con acción permitida, lo que demuestra que el cortafuegos autoriza el tráfico FTP de la LAN hacia la WAN según lo configurado.

Figura 30 Prueba ingreso servicio FTP desde LAN a WAN y verificación registros Endian

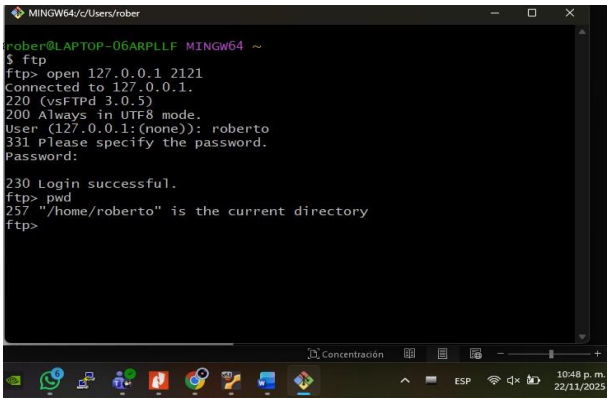


Fuente: Autoría Propia

6.4.6 EL INGRESO DEL SERVICIO FTP DESDE LA WAN HACIA LA ZONA DMZ:

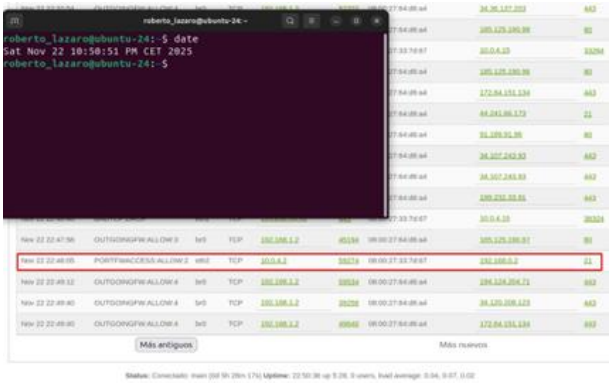
Finalmente, el ingreso del servicio FTP desde la WAN hacia la zona DMZ se probó desde el sistema Windows conectando mediante ftp 127.0.0.1 2121. Esta petición fue reenviada por VirtualBox al puerto 21 de Endian y posteriormente traducida a 192.168.0.2:21, donde se encuentra el servidor vsftpd. El inicio de sesión exitoso y la navegación por el directorio remoto, junto con las entradas RED → ORANGE en el puerto 21/TCP en los logs, confirmaron la correcta publicación del servicio FTP de la DMZ hacia la WAN.

Figura 31 Prueba ingreso servicio FTP desde WAN a DMZ



Fuente: Autoría Propia

Figura 32 Verificación registros Endian servicio FTP desde WAN a DMZ



Fuente: Autoría Propia

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

7.1 INSTALAR SQUID

Para la implementación del proxy HTTP se utilizó Squid, un servicio de caché y filtrado de contenido ampliamente empleado como proxy en entornos GNU/Linux. En el servidor basado en Ubuntu se procedió a instalarlo mediante el gestor de paquetes del sistema, utilizando el comando sudo apt install squid, el cual descarga e instala automáticamente todos los componentes necesarios. Esta instalación constituye la base sobre la cual se configurarán posteriormente las políticas de filtrado, las listas negras de sitios web y los mecanismos de autenticación de usuarios para controlar la navegación desde la red LAN.

Figura 33 Instalación de Squid

Fuente: Autoría Propia

7.2 CREAR UN PERFIL CON LISTA NEGRA (ACL)

Como parte de la configuración de control de acceso, se definió una lista negra de sitios web que serán bloqueados por el proxy. Para ello, en el servidor se creó el archivo /etc/squid/blacklist.txt mediante el comando sudo nano

/etc/squid/blacklist.txt, en el cual se añadieron las direcciones www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Este archivo será utilizado posteriormente por Squid como una ACL (Access Control List), permitiendo asociar dicha lista negra a un perfil de navegación y aplicar políticas de bloqueo sobre los dominios especificados desde la red LAN.

Figura 34 Creación de la lista negra

Fuente: Autoría Propia

7.3 CREAR ACL EN SQUID.CONF

A continuación, se procedió a editar el archivo de configuración principal de Squid mediante el comando sudo nano /etc/squid/squid.conf, con el fin de definir la lista de control de acceso (ACL) asociada a la lista negra. En este archivo se declaró una ACL denominada blacklist que utiliza como origen el fichero /etc/squid/blacklist.txt, donde se encuentran los dominios bloqueados, y se añadió posteriormente una regla http_access deny blacklist para negar el acceso a cualquier petición cuyo destino coincida con los sitios incluidos en dicha lista.

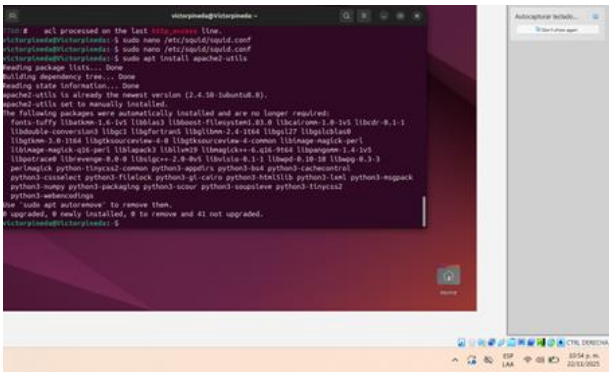
Figura 35 Creación de la lista de control de acceso

Fuente: Autoría Propia

7.4 CONFIGURAR AUTENTICACIÓN POR USUARIO

Para habilitar la autenticación por usuario en el proxy, se instaló el paquete apache2-utils mediante el comando sudo apt install apache2-utils. Este paquete proporciona la herramienta htpasswd, utilizada para crear y gestionar las credenciales de los usuarios que deberán autenticarse antes de iniciar la navegación a través de Squid. De esta manera, el proxy puede aplicar políticas de acceso basadas en usuarios y grupos definidos, reforzando el control sobre quién puede utilizar el servicio y bajo qué restricciones.

Figura 36 Configuración de la autenticación



Fuente: Autoría Propia

Una vez instalada la herramienta htpasswd, se procedió a crear el archivo de credenciales de usuarios para el proxy mediante el comando sudo htpasswd -c /etc/squid/users proxyuser. Con esta instrucción se genera el fichero /etc/squid/users y se define el usuario inicial proxyuser, al que se le asigna una contraseña. Este archivo será posteriormente referenciado en la configuración de Squid para validar la autenticación de los clientes antes de permitir el acceso a Internet.

Figura 37 Configuración del usuario

Fuente: Autoría Propia

7.5 ASOCIAR USUARIO AL GRUPO Y VINCULAR POLÍTICA

Para configurar el acceso de un usuario al proxy, primero se debe crear el archivo /etc/squid/group_profes.txt y agregar a este el nombre del usuario, por ejemplo, proxyuser. Posteriormente, en el archivo de configuración squid.conf, se define una lista de control de acceso (ACL) que apunta a dicho archivo y se concede el permiso correspondiente. Este procedimiento garantiza que solo los usuarios listados puedan utilizar el servicio.

Figura 38 Creación del grupo y vinculación del usuario

Fuente: Autoría Propia

Figura 39 Configuración de la política

Fuente: Autoría Propia

7.6 REINICIAR SQUID - SUDO SYSTEMCTL RESTART SQUID

Mediante este paso se aplican los cambios realizados en la configuración. Al reiniciar el servicio, Squid carga nuevamente el archivo squid.conf junto con las ACL, reglas y ajustes de autenticación.

Figura 40 Verificación del servicio Squid

Fuente: Autoría Propia

8 CONCLUSIONES

La implementación del firewall Endian permitió estructurar una arquitectura segura y segmentada, donde cada zona (verde, naranja y roja) fue configurada correctamente para garantizar control del tráfico y protección perimetral desde el inicio de la instalación.

La creación y verificación de reglas NAT y de acceso entre zonas demostró la importancia del control granular del tráfico, permitiendo habilitar servicios específicos como HTTP y FTP, asegurar la DMZ y validar la eficacia del filtrado revisando los registros inter-zona.

La configuración y verificación de las reglas de firewall para los servicios HTTP y FTP en la zona DMZ demostró la efectividad de Endian como solución de seguridad perimetral, permitiendo exponer servicios internos de manera controlada hacia Internet mientras se mantiene el aislamiento de la red interna. La implementación de reglas de NAT de destino (DNAT) y la posterior validación mediante pruebas de conectividad confirmaron que es posible publicar servicios de forma segura, al mismo tiempo que se fortalece la infraestructura mediante la restricción de protocolos no esenciales como ICMP, reduciendo así la superficie de ataque y mejorando la postura de seguridad general de la red.

La implementación de reglas de acceso granular entre las zonas VERDE, NARANJA y ROJA evidenció la flexibilidad del firewall Endian para controlar flujos de tráfico específicos según políticas de seguridad definidas. Mediante la creación de reglas de filtrado y NAT, se logró una comunicación segura y auditada entre segmentos, permitiendo acceso HTTP y FTP desde la LAN hacia la DMZ y WAN, mientras se garantizaba la publicación controlada de servicios hacia Internet. La verificación a través de registros de tráfico inter-zona confirmó el correcto funcionamiento de cada regla, validando el modelo de seguridad basado en zonas y el control exhaustivo del tráfico de red.

La integración del proxy Squid con ACL y autenticación reforzó las políticas de navegación, permitiendo restringir contenido, gestionar accesos por usuario y complementar el modelo de seguridad de red con controles de filtrado y monitoreo más avanzados.

9 REFERENCIAS

[1] Endian S.r.l., "Endian Firewall Community Documentation", Endian Network Security, 2023. [En línea]. Disponible: https://www.endian.com/community/documentation/

[2] R. Ziegler, "Linux Network Security", 2nd ed., Prentice Hall, NJ, pp. 145-180, 2018.

[3] D. P. Bovet y M. Cesati, "Understanding the Linux Kernel", 3rd ed., O'Reilly Media, pp. 673-720, 2020.

[4] W. R. Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley, pp. 223-285, 2019.

[5] M. G. Sobell, "A Practical Guide to Linux Networking", Prentice Hall, pp. 89-134, 2021.

[6] Squid Project, "Squid Proxy Cache Documentation", The Squid Software Foundation, 2022. [En línea]. Disponible: https://wiki.squid-cache.org/

[7] J. N. BLANk, "Network Address Translation (NAT) Concepts and Configuration", IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 345-367, 2020.

[8] L. Sánchez y R. Martínez, "DMZ Architecture and Security Policies", InterNATional Journal of Network Security, vol. 15, no. 2, pp. 78-95, 2021.

[9] K. S. Singh y A. Patel, "Firewall Rule Management Best Practices", IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 512-530, 2022.

[10] P. L. Ventura, "Proxy Server Implementation with Squid", Journal of Network Systems, vol. 29, no. 4, pp. 234-251, 2021.