DISEÑO DE UNA ARQUITECTURA DE RED SEGURA SEGMENTADA USANDO ENDIAN FIREWALL COMMUNITY

Fredy Aponte Ávila
e-mail: fapontea@unadvirtual.edu.co
Brayan Umba Chisaba
e-mail: buchisaba@unadvirtual.edu.co
Carlos Steven Fonseca Garces
e-mail: csfonsecag@unadvirtual.edu.co
Jorge Enrique Guerrero Ruiz
e-mail: jeguerreroru@unadvirtual.edu.co

RESUMEN: *Este articulo plantea una solución ante un constante crecimiento y desarrollo de amenazas y ataques cibernéticos y por consiguiente se implementará una estrategia de seguridad perimetral considerablemente elaborada. La implementación de una Zona Desmilitarizada (DMZ) surge a partir de una necesidad esencial buscando una defensa sólida y robusta de una infraestructura de red. El presente estudio documenta el proceso que conlleva dicha implementación desde el diseño hasta su implementación, todo esto utilizando la distribución de GNU/Linux Endian Firewall (EFW), una solución completa en el entorno de seguridad de código abierto. Su objetivo principal es establecer una barrera de protección sólida para que los servidores donde se almacenan aplicaciones y bases de datos que en su mayoría de casos es información crítica de forma parcial o completa, estén bajo el resguardo de plataformas GNU/Linux, segmentándolos de la red interna (LAN) y su exposición directa a la red externa (WAN). Se detalla la configuración estratégica de distintas zonas de red siendo estas la zona roja como punto de conexión a internet seguida de la zona verde como la red interna de confianza y por último la zona naranja como el enclave seguro para los servidores expuestos. Así mismo, se compartirá la verificación básica de la conectividad inicial, asegurando consigo la comunicación bidireccional controlada entre las zonas y la accesibilidad a la interfaz de administración centralizada del firewall.*

PALABRAS CLAVE: DMZ, Endian, Firewall, Seguridad, UTM.

1 INTRODUCCIÓN

Dado el panorama actual en la administración de sistemas, la seguridad de la infraestructura de red se ha convertido en una preocupación principal. El crecimiento de ataques dirigidos a la creciente criticidad de los datos almacenados en servidores hace que sea necesaria la implementación de medidas de protección proactivas y multicapa. Una de las arquitecturas de seguridad fundamentales en este contexto es la Zona Desmilitarizada.

En el presente trabajo, abordaremos la implementación de una DMZ haciendo uso de Endian Firewall (EFW), esta es una distribución de GNU/Linux que abarca un conjunto completo de herramientas de seguridad, este incluye servicios como firewall, sistema de prevención de instrucciones (IPS), filtrado de contenido, servicios de VPN entre otros. Su elección se basó en el diseño específico para la seguridad de redes, su flexibilidad y su gran adopción en entornos donde la robustez y la capacidad de configuración no solo son necesarias si no esenciales para proteger y resguardar infraestructuras basadas en GNU/Linux. El objetivo final es demostrar como EFW puede ser usado de forma eficaz estableciendo una DMZ que salvaguarde los activos críticos de una red.

2 METODOLOGIA

La implementación de la DMZ con Endian Firewall se basó en la segmentación lógica de la red en tres zonas de seguridad específicamente definidas, cada una de ellas con un objetivo específico asociado a un nivel de confianza:

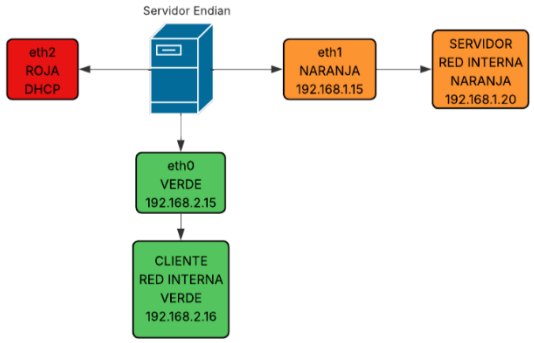
Zona Roja (Interfaz eth2): La puerta de enlace a la red externa (WAN). Esta interfaz representa la conexión física del firewall a un proveedor de servicios de internet. En su configuración inicial, se estableció que dicha interfaz obtenga su dirección IP de forma dinámica por medio del Protocolo de Configuración Dinámica de Host (DHCP), el método común para la asignación de direcciones en redes externas. Dicha configuración permite que tenga una fácil integración con la infraestructura del proveedor de internet sin la necesidad de configuraciones estáticas complejas en este punto.

Zona Verde (Interfaz eth0): Es la Red Interna de Confianza (LAN). Esta zona compete al segmento de red donde van a residir las estaciones de trabajo para los usuarios y otros sistemas internos que requieran un nivel de confianza elevado. Para su implementación se configuro una subred privada haciendo uso del rango de direcciones 192.168.2.0/24. Dentro de esta red se asignó una dirección IP estática a la interfaz eth0 del firewall (192.168.2.15) esta actúa como la puerta de enlace predeterminada para los dispositivos conectados a esta red. Así mismo se configuro una maquina cliente GNU/Linux con la dirección IP 192.168.2.16, dentro del mismo segmento de red esto para simular una estación de trabajo convencional.

Zona Naranja (Interfaz eth1): La Zona Desmilitarizada (DMZ) para uso de servidores expuestos. Esta zona intermedia se diseñó exclusivamente para contener los servidores que necesitan ser accesibles desde la red externa, un ejemplo de ellos

sería un servidor web o un servidor de aplicaciones. Se configuro adicionalmente una subred privada separada, usando el rango de direcciones 192.168.1.0/24. La interfaz eth1 del firewall se configuro con la dirección IP estática 192.168.1.15, funcionando como la puerta de enlace para los servidores ubicados en dicha zona. Se implemento también un servidor GNU/Linux dentro de la DMZ, asignándole la dirección IP estática 192.168.1.20, simulando así un servidor que podría contener diversa información sensible.

Figura 1. Diagrama de Red



Fuente: Autoría Propia

La configuración de las zonas previamente mencionadas en Endian Firewall permitirán un control del tráfico de red entre ellas, validando que tipo de comunicaciones están permitidas y hacía que dirección. Esta segmentación es necesaria para el propósito con el cual se implementa la DMZ que es contener cualquier posible penetración en los servidores que se encuentran expuestos sin que se propague el ataque directamente a la red interna.

3 RESULTADOS

Una vez implementada la configuración inicial de las zonas de red en Endian Firewall y su respectiva asignación de direcciones IP a las maquinas cliente y servidor, se procedió a realizar unas pruebas de verificación para cerciorarnos sobre la correcta comunicación dentro de cada zona, entre las zonas y el firewall.

En la máquina del cliente que se encuentra en la Zona Verde (192.168.2.16), se hace uso del comando ip a para confirmar que la interfaz de la red activa tenía asignada la dirección IP correcta validando también que la puerta de en lace predeterminada estaba configurada hacia la dirección IP de la interfaz verde del firewall (192.168.2.15). Posteriormente se ejecutó el comando ping 192.168.2.15 para validar que efectivamente existiera una comunicación bidireccional dentro de la red local (LAN) confirmando así que la máquina del cliente podía alcanzar la interfaz del firewall en su propia zona.

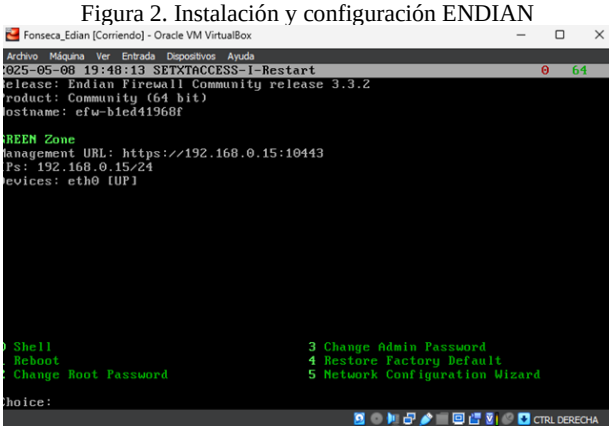
Se realiza el proceso de forma similar en el servidor ubicado en la Zona Naranja (192.168.1.20), haciendo uso del comando IP a para verificar la configuración de red, garantizando que la dirección IP y puerta de enlace (apuntando a la interfaz naranja del firewall, 192.168.1.15), fuesen correctas. La ejecución del comando ping 192.168.1.15 confirmo la comunicación entre el servidor DMZ y la interfaz del firewall en la zona naranja.

Concluyendo, se accedió a la interfaz de administración web de Endian Firewall desde el navegador en la maquina cliente (ubicada en la Zona Verde), usando la dirección HTTPS https://192.168.2.15:10443, estableciendo una conexión segura con el firewall. Al principio el navegador mostro una advertencia con relación al certificado de seguridad autoafirmado de Endian, dicho comportamiento es normal dadas implementaciones iniciales. Posterior a aceptar la excepción del certificado, se visualizó la página de inicio de sesión de la interfaz de administración web de Endian Firewall. El presente acceso exitoso desde la red interna (Zona Verde) dejo en evidencia la capacidad de gestionar centralizadamente la configuración y las políticas de seguridad que competen al firewall.

3.1 CONFIGURACION NAT

Se presentan escenarios específicos de comunicación entre una red local (LAN), una zona desmilitarizada (DMZ) y una red simulada de Internet (WAN). El objetivo principal es guiar al lector en la implementación práctica de reglas NAT, que faciliten el flujo de tráfico deseado entre estas áreas, asegurando al mismo tiempo la protección y el aislamiento requeridos.

Figura 2. Instalación y configuración ENDIAN



Fuente: Autoría Propia

Configuración de Network Address Translation (NAT) para Acceso LAN a WAN:

Para permitir que los dispositivos dentro de la red local (zona verde) accedan a la red externa (simulada como Internet), se configura una regla NAT de tipo "NAT Fuente"

Una vez que se elige el idioma de la interfaz y definido la ubicación, el siguiente paso crucial en la configuración inicial de Endian consiste en establecer las credenciales de acceso para los usuarios con privilegios administrativos: admin y root. En esta ventana de configuración, se encuentran los campos donde es necesario ingresar contraseñas seguras y únicas para cada uno de estos usuarios. El administrador, conocido como admin, generalmente cuenta con permisos para gestionar la interfaz web y realizar ajustes generales en el firewall, mientras que el usuario root tiene acceso total al sistema operativo subyacente a través de la línea de comandos.

Esta etapa es crucial, ya que estas contraseñas forman la primera línea de defensa contra accesos no autorizados a la

administración del firewall y al sistema operativo. Por ello, deben ser tratadas con la más estricta precaución y confidencialidad. Unas credenciales débiles o fácilmente adivinables podrían poner en riesgo la seguridad de toda la red protegida por el firewall Endian.

Figura 3. Establecer las claves de acceso de los usuarios admin y root.

Fuente: Autoría Propia

En la interfaz de configuración de la "NAT Fuente", el siguiente paso consiste en iniciar la creación de una nueva regla, haciendo clic en la opción correspondiente a "añadir regla". Al hacerlo, se abrirá un formulario en el que se deberán especificar los parámetros que determinarán cómo se traducirá el tráfico originado en la red local, comúnmente denominada como la zona "Verde", cuando salga hacia la red externa. Para permitir un acceso irrestricto a internet desde los dispositivos dentro de la LAN, que se ha identificado con la dirección IP 192. 168. 0. 15/24, se deben ajustar adecuadamente estos parámetros.

Es fundamental definir los siguientes parámetros en la regla NAT de origen: primero, la interfaz de salida, que se corresponde con la conexión WAN o "Roja"; en segundo lugar, la red o dirección IP de origen, que en este caso será la subred 192. 168. 0. 0/24, abarcando todos los dispositivos de la LAN; y, por último, el destino, que se configurará como "cualquiera" para facilitar la comunicación con cualquier servidor en internet.

Figura 4. Establecer las claves de acceso de los usuarios admin y root

Fuente: Autoría Propia

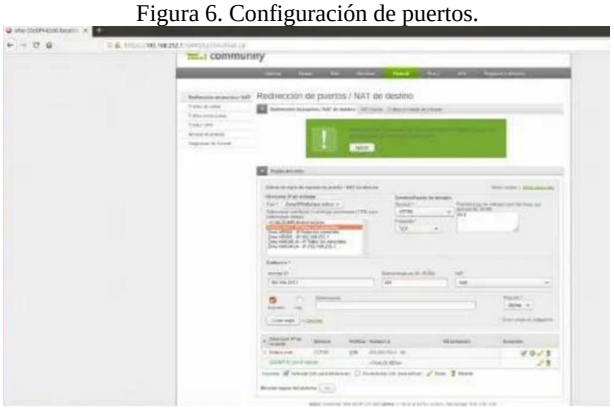
Es necesario establecer una regla de tráfico muy específica, pero esta vez en sentido opuesto. En lugar de indicarle al firewall cómo traducir las direcciones de salida, se define qué tráfico entrante desde el exterior no tiene permitido acceder a nuestra red. Esta regla se centra en el tráfico "enrutado de entrada", lo cual implica que se analizan las conexiones que intentan acceder a la red local desde la WAN. La idea principal es que, a menos que se habilite una puerta específica (como se realizara más adelante con el reenvío de puertos), ningún usuario de internet debería poder iniciar una comunicación directamente con los dispositivos de la red LAN.

Figura 5. Creación de nuestras reglas evitar el acceso WAN a LAN

Fuente: Autoría Propia

En esta sección, se detalla cómo permitir que las personas desde internet accedan a los servidores web. Para lograrlo, se crearán dos "servicios" que representan las formas más comunes de visualizar páginas web: el servicio estándar (HTTP) que opera en el puerto 80, y el servicio seguro (HTTPS) que utiliza el puerto 443. Al definir estos servicios con sus números de puerto correspondientes, se está indicando al firewall: "Si alguien desde internet solicita la a la puerta número 80, se debe redirigir a este lugar de nuestra red", y lo mismo se aplicara para la puerta número 443. Este paso es fundamental para garantizar que el sitio web sea accesible desde el exterior.

Figura 6. Configuración de puertos.



Fuente: Autoría Propia

Después de configurar, la interfaz de administración del firewall, Endian proporciona un resumen claro y conciso de las reglas de reenvío que se han configurado. En esta pantalla, se puede observar cada regla en detalle, incluyendo la interfaz de origen (la WAN), el puerto de destino en el firewall, el protocolo utilizado (en este caso, TCP), así como la dirección IP y el puerto del servidor interno al que se redirigirá el tráfico. Esta vista permite confirmar que las reglas se han establecido correctamente y que la configuración coincide con las intenciones definidas.

Endian ofrecerá un resumen general sobre los resultados de toda la configuración que se ha llevado a cabo hasta ahora. Esto incluirá las reglas NAT de origen para la comunicación entre la LAN y la WAN, la regla que bloquea el tráfico entrante de la WAN hacia la LAN, así como las reglas de redirección de puertos que se han definido recientemente. Esta pantalla final funciona como una confirmación visual de que todos los pasos

se han completado con éxito. De esta manera, el firewall Endian está debidamente configurado para permitir la comunicación saliente desde la LAN, bloquear el acceso no solicitado desde la WAN y redirigir el tráfico web entrante hacia los servidores designados.

Figura 7. Resultados obtenidos de la configuración de reglas

Fuente: Autoría Propia

3.2. CONFIGURACION DE SERVICIOS PERMITIDOS EN LA DMZ Y REGLAS DE CONTROL

Con el objetivo de garantizar una arquitectura de red segura y controlada, se procedió a permitir únicamente aquellos servicios esenciales entre la zona interna (verde) y la zona desmilitarizada (naranja). En este caso, se habilitaron los servicios HTTP (puerto 80) y FTP (puerto 21) para permitir el acceso controlado a un servidor web y un servidor de transferencia de archivos ubicado en la DMZ, ambos corriendo bajo Ubuntu Server.

Esta decisión se fundamenta en la necesidad de brindar servicios externos accesibles desde la red interna o pública, sin comprometer el resto de la infraestructura. El protocolo HTTP es el más común para la publicación de sitios web, mientras que FTP es útil para la gestión de archivos en servidores remotos. Ambos representan servicios legítimos que, si bien necesarios, pueden ser vectores de ataque si no se restringen adecuadamente mediante reglas de filtrado.

Las políticas de seguridad fueron configuradas en el módulo de firewall de Endian, estableciendo reglas explícitas que permiten el tráfico TCP entrante hacia los puertos mencionados, únicamente desde direcciones IP previamente definidas. Se aplicaron políticas restrictivas por defecto (deny all) y se habilitaron de forma selectiva los servicios requeridos.

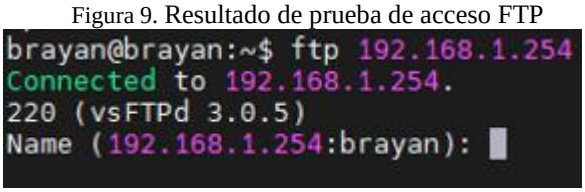
Figura 8. Reglas del firewall para permitir HTTP y FTP en zona naranja

Fuente: Autoría Propia

Adicionalmente, se estableció la denegación del protocolo ICMP (Internet Control Message Protocol), asociado al diagnóstico de red (como el comando ping). Esta decisión se justifica bajo el principio de minimización de superficie de ataque, ya que permitir ICMP puede facilitar la identificación de dispositivos activos y su topología por parte de atacantes. Se bloquearon específicamente los tipos 8 (echo request) y 0 (echo reply) mediante reglas en el firewall que impiden cualquier respuesta a paquetes ICMP desde la DMZ.

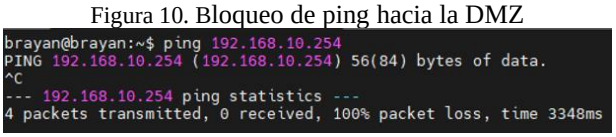
Para validar la efectividad de estas políticas, se realizaron pruebas de conectividad desde la red verde hacia la IP del servidor en la DMZ. Se comprobó exitosamente el acceso a servicios web (mediante navegador y comando curl) y a servicios FTP (mediante cliente FTP en terminal). A su vez, se verificó que el comando ping hacia la IP del servidor DMZ no obtuviera respuesta, confirmando la correcta aplicación del bloqueo ICMP.

Figura 9. Resultado de prueba de acceso FTP



Fuente: Autoría Propia

Figura 10. Bloqueo de ping hacia la DMZ



Fuente: Autoría Propia

Esta configuración demuestra una implementación efectiva del principio de "defensa en profundidad", donde cada segmento de la red tiene políticas personalizadas que limitan estrictamente los flujos de tráfico según la función que cumple cada zona. A su vez, evidencia el uso de un firewall de nueva generación como herramienta central para garantizar el aislamiento y la seguridad en infraestructuras GNU/Linux.

Se autorizó el acceso a dos servicios esenciales para la operación de redes empresariales: HTTP, mediante el puerto TCP 80, y FTP, por el puerto TCP 21. El servicio HTTP es fundamental para permitir que clientes accedan a páginas web hospedadas en servidores dentro de la DMZ, mientras que FTP resulta útil para la transferencia de archivos, especialmente en entornos donde se requiere subir o descargar contenidos desde el servidor remoto.

Las reglas en el firewall fueron implementadas de forma granular, permitiendo tráfico solo desde direcciones IP específicas de la zona verde (red interna), hacia la IP del servidor en la DMZ (Ubuntu Server). Para ello, se utilizó la interfaz web de Endian, definiendo las siguientes políticas:

Origen: Zona Verde – cualquier host o dirección IP validada.

Destino: Zona Naranja – dirección IP del servidor Ubuntu en la DMZ.

Servicio: HTTP (puerto 80 TCP) y FTP (puerto 21 TCP).

Acción: Permitir (Allow).

Registro (Logging): Activado, para auditoría de tráfico.

Esta metodología responde al principio de mínimo privilegio, donde se habilitan únicamente aquellos puertos y servicios imprescindibles, reduciendo drásticamente la superficie de ataque disponible para actores maliciosos.

Además, se activaron los registros del firewall para monitorear el tráfico permitido, lo cual no solo respalda la política de trazabilidad, sino que permite realizar auditorías posteriores para detectar posibles anomalías o accesos sospechosos.

Figura 11. Reglas creadas en Endian para habilitar HTTP

Fuente: Autoría Propia

En paralelo a la habilitación de los servicios necesarios, se implementó una política explícita para bloquear el protocolo ICMP (Internet Control Message Protocol), específicamente los tipos 8 (echo request) y 0 (echo reply), comúnmente utilizados para realizar pruebas de ping.

Aunque ICMP puede ser útil para diagnóstico de red, también representa una vía común para la recolección de información durante las fases de reconocimiento de un ataque. Permitir ICMP puede revelar la existencia de dispositivos activos, topología de red, tiempos de latencia y otros indicadores sensibles para un atacante.

Por lo tanto, se configuró en Endian una regla de denegación con las siguientes características:

Origen: Cualquier zona (específicamente zona verde).

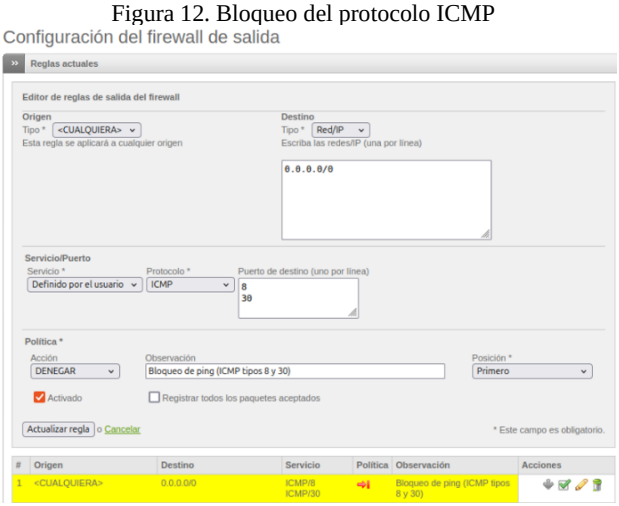
Destino: Zona naranja – IP del servidor.

Protocolo: ICMP – tipos 8 y 0.

Acción: Denegar (Deny).

Registro: Activado, para detectar intentos de escaneo.

Figura 12. Bloqueo del protocolo ICMP



Fuente: Autoría Propia

Una vez configuradas las reglas, se procedió a validar la operatividad mediante el uso de herramientas comunes desde la terminal del cliente Ubuntu Desktop. Las pruebas fueron las siguientes:

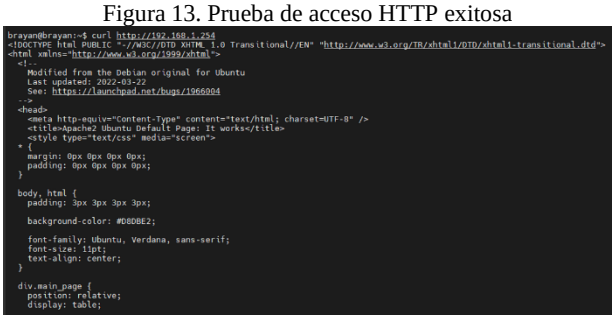
HTTP: Se utilizó curl y navegadores web para acceder al servidor en la DMZ, confirmando la respuesta correcta del servicio Apache.

FTP: Se accedió vía terminal con ftp al puerto 21 del servidor DMZ, verificando autenticación y navegación de directorios.

ICMP: Se ejecutó el comando ping desde el cliente a la IP del servidor DMZ, sin obtener respuesta, lo que confirma el bloqueo exitoso del tráfico ICMP.

Revisión de logs: Se consultaron los registros del firewall desde su consola administrativa, evidenciando intentos de ICMP rechazados y sesiones HTTP aceptadas.

Figura 13. Prueba de acceso HTTP exitosa



Fuente: Autoría Propia

La configuración aquí presentada refleja un diseño seguro basado en el principio de defensa en profundidad. Se evita cualquier acceso directo a la red interna desde la DMZ, y se habilitan únicamente servicios controlados. Esta separación funcional entre zonas y la aplicación de reglas específicas en el firewall permiten limitar las capacidades de un atacante, incluso si lograra comprometer un servicio público.

La implementación de reglas personalizadas en el firewall para permitir exclusivamente servicios HTTP y FTP desde una zona segura, junto con la denegación de ICMP, responde a una estrategia de seguridad enfocada en la limitación de exposición y la reducción de la superficie de ataque. Esta decisión técnica mitiga riesgos clave como:

Enumeración de dispositivos en red (bloqueando ICMP).

Acceso no autorizado o lateralidad entre zonas.

Explotación de puertos abiertos no controlados.

Fuga de información desde servidores DMZ comprometidos.

Además, la segmentación de servicios por zonas —y no solo por puertos— constituye un enfoque moderno de seguridad basado en zonificación funcional, común en infraestructuras críticas y entornos empresariales sensibles.

La solución desarrollada se alinea con buenas prácticas recomendadas por organizaciones como la Free Software Foundation (FSF) y el Linux Professional Institute (LPI), al combinar herramientas de código abierto robustas (Ubuntu Server, Endian Firewall) con principios fundamentales de seguridad de red:

Principio de mínimo privilegio: solo se permiten los servicios imprescindibles.

Defensa en profundidad: múltiples capas de protección entre zonas.

Seguridad por diseño: desde la configuración inicial, se considera el aislamiento.

Auditoría y trazabilidad: mediante el registro de eventos de red.

Esta implementación puede escalarse o adaptarse a entornos reales con más servicios, reglas avanzadas de NAT, VPN, o segmentación VLAN. Asimismo, sirve como modelo base para entornos académicos o empresariales donde se busque validar el concepto de una DMZ operativa y segura utilizando únicamente tecnologías Open Source.

3.3. CONFIGURACIÓN DE REGLAS DE ACCESO Y COMUNICACIÓN ENTRE ZONAS

El éxito de la implementación de Endian Firewall como dispositivo UTM en una red organizacional reside en la correcta configuración de la comunicación entre las zonas habilitadas y operativas. Es común que la zona verde, albergando los dispositivos de confianza bajo la red LAN se la zona con mayor seguridad y que la zona naranja DMZ reciba las redirecciones de solicitudes que se gestionan desde la zona roja, es decir, el acceso a la red WAN. Teniendo en cuenta las características de privacidad y seguridad que debe tener cada zona, se relacionan a continuación algunos ejemplos de configuración de reglas firewall de Endian para permitir el tráfico bajo determinados protocolos y puertos garantizando únicamente el consumo y prestación de los servicios que se encuentran autorizados por las políticas de administración de red.

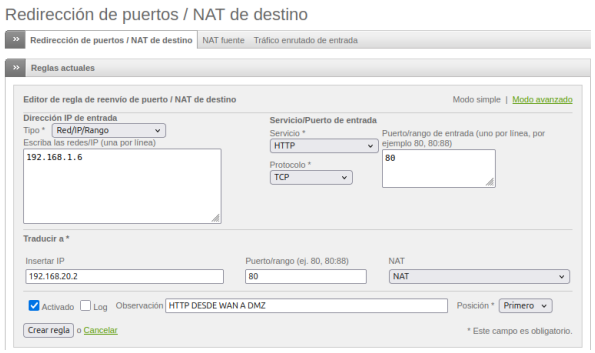
En primer lugar, es importante abordar la gestión de solicitudes entrantes desde la zona WAN hacia el servidor Endian. En este caso, la redirección se realiza directamente hacia la zona DMZ, redirigiendo el tráfico hacia los servidores y servicios que se salvaguardan en esta zona. Para definir una regla que redireccione el tráfico entrante al firewall a través de la interfaz roja se deben configurar las reglas de redirección de puertos / NAT de destino

Figura 14. Redirección de puertos / NAT Destino

Fuente: Autoría Propia

Estas reglas permiten transmitir las solicitudes de conexión bajo protocolos como HTTP, HTTPS, FTP, entre otros, desde la zona WAN hacia los equipos, servidores y/o estaciones de trabajo que se encuentran en la zona DMZ o en la zona LAN (este último no recomendado por motivos de seguridad). La traducción es equivalente, por lo tanto, si la solicitud ingresa desde por la interfaz roja hacia el protocolo web seguro, será transferida al equipo o servidor de destino bajo el mismo protocolo y puerto. A continuación, se relaciona como ejemplo la configuración de una regla de redirección de puertos desde la zona roja hacia un servidor configurado en la zona naranja, traduciendo la comunicación del protocolo HTTP bajo el puerto 80:

Figura 15. Configuración de regla de redirección de puertos

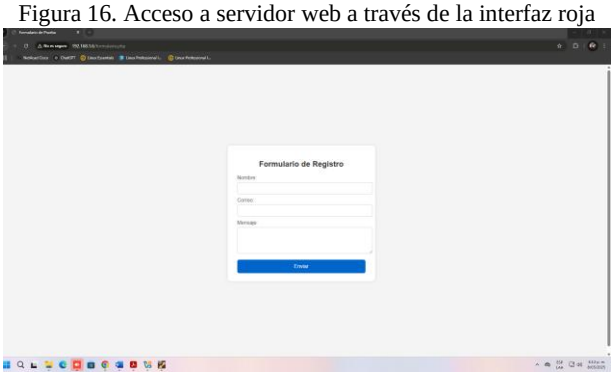


Fuente: Autoría Propia

Al aplicar y guardar la configuración en Endian Firewall, se recibirán solicitudes de conexión a través de la interfaz roja desde cualquier lugar de la red, si estas corresponden al protocolo HTTP y puerto 80 serán redireccionadas hacia la zona naranja o DMZ, permitiendo el acceso a los servicios

gestionados y suministrados por los servidores que se encuentren configurados en esta zona, sin tener acceso en ningún momento a la zona LAN ni a los equipos que se encuentran configurados en esta zona. Un ejemplo de la redirección configurada anteriormente es el ingreso a los servicios configurados en el servidor implementado en la zona DMZ desde un equipo que está fuera de red implementada, es decir, el tráfico ingresa por la interfaz roja, realiza la traducción y accede al servidor para consumir sus servicios (web en este caso).

Figura 16. Acceso a servidor web a través de la interfaz roja



Fuente: Autoría Propia

La comunicación entre zonas es un aspecto de configuración que debe ser tratado con la misma importancia que la redirección del tráfico de entrada. Bajo una configuración errada de reglas en el firewall se puede dar acceso a los atacantes a los recursos, equipos y datos de la red privada en la zona LAN desde otra zona de Endian.

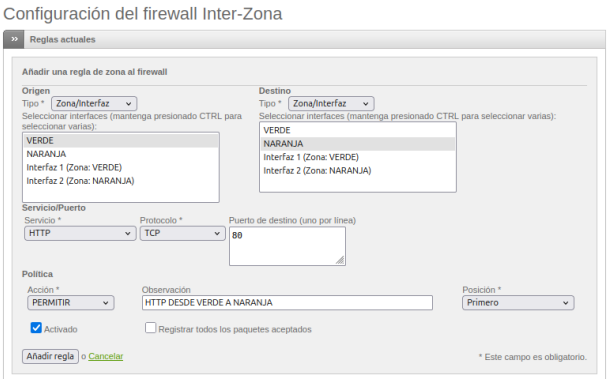
El firewall de manera predeterminada configura algunas reglas de acceso inter-zona que permiten el correcto funcionamiento de este al finalizar el despliegue inicial de la herramienta. Estas reglas se encuentran disponibles en la opción Configuración del Firewall Inter-zona

Figura 17. Reglas por defecto inter-zona

Fuente: Autoría Propia

A través de este apartado de configuración se pueden permitir y denegar el tráfico de acuerdo con las necesidades que se establezcan en la infraestructura de red. Es recomendable configurar reglas que permitan el acceso unidireccional desde la zona verde hacia la zona naranja, teniendo en cuenta, que, si en la zona DMZ se encuentran los servidores, los clientes en la red privada necesitaran consumir los recursos y servicios de estos, por lo tanto, se debe garantizar que se parametricen las reglas que permitan este requisito de comunicación. En la configuración de la regla se debe establecer las zonas de origen, destino los servicios (protocolos y puerto) que debe gestionar la regla y la política de acceso, ya que es necesario hacer la precisión que no siempre se requiere garantizar al acceso, en ocasiones se debe restringir el acceso a servicios, protocolos y puertos específicos para garantizar la integridad de todo el entorno de red. Por ejemplo:

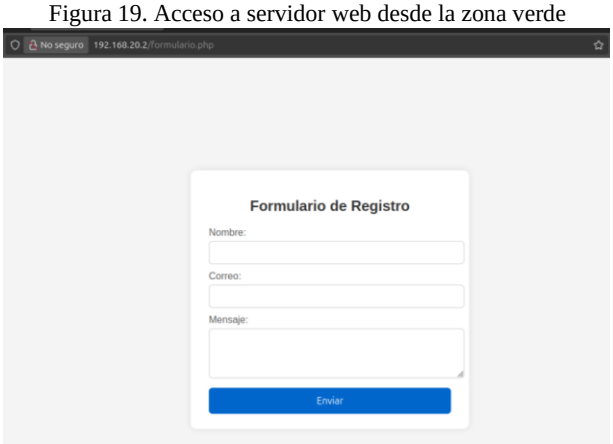
Figura 18. Regla de acceso HTTP de LAN a DMZ



Fuente: Autoría Propia

En el ejemplo anterior, se garantiza el acceso nuevamente hacia el servidor web que está configurado en la zona DMZ, pero las solicitudes son recibidas, analizadas y permitidas desde la interfaz verde, por lo tanto, se accede al mismo recurso, pero con dirección diferente, en este caso, la dirección asignada en el direccionamiento interno de la solución:

Figura 19. Acceso a servidor web desde la zona verde



Fuente: Autoría Propia

Al igual que con el tráfico entrante a Endian, así como las conexiones entre zonas, es importante realizar control del tráfico que sale de las zonas verde y naranja, así como los servicios, protocolos y puertos que se permitirán a los usuarios y equipos de estas zonas. Esta restricción del tráfico de salida permite establecer políticas de seguridad más estrictas y segmentadas reduciendo el riesgo que equipos con seguridad comprometida se comuniquen libremente hacia el exterior de la red o con el

resto de las zonas configuradas sin control o supervisión. En este panorama, es posible permitir el acceso solo a los protocolos necesarios para la operación de servicios específicos como HTTP/HTTPS, DNS, SMTP, POP/IMAP o FTP, bloqueando el resto de los servicios de manera integral. A través de esta práctica se mejora el control del tráfico saliente y es posible parametrizar medidas de detección y respuesta ante posibles escenarios de degradación de la seguridad de la red.

Desde Endian las reglas correspondientes al tráfico de salida se administran desde Configuración del firewall de salida y al igual que con las reglas inter-zona, el sistema define reglas por defecto que garantizan el funcionamiento integral básico del entorno de red:

Figura 20. Reglas por defecto de salida

Fuente: Autoría Propia

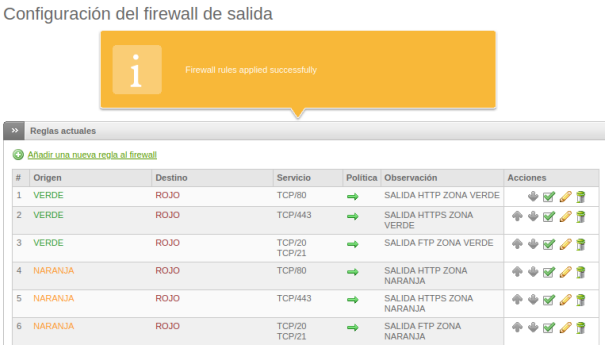
La configuración de una regla de salida no difiere de la configuración necesaria para la definición de cualquier otra regla de firewall. Se debe definir un origen (generalmente zonas internas), un destino (la zona WAN), los servicios que se configuran en la regla (protocolos y puertos) y la acción correspondiente para la regla, bien sea permitir o denegar la regla parametrizada. Por ejemplo, para permitir el acceso desde la zona verde a servicios web bajo protocolo HTTP puerto 80, la regla de salida se debe configurar de la siguiente manera:

Figura 21. Regla de salida zona verde a WAN

Fuente: Autoría Propia

De acuerdo con lo mencionado anteriormente, una gestión efectiva de reglas dentro de un entorno corporativo consiste en permitir únicamente los servicios necesarios y requeridos por la operación especifica de los usuarios, y denegar el resto de los servicios para evitar filtraciones o degradaciones de seguridad mediante la vulneración de *backdoors*. En el entorno de red implementado se permite únicamente la salida a los protocolos HTTP, HTTPS y FTP en las zonas verde y naranja, por lo tanto, las reglas de salida finales que están configuradas en el firewall de salida son las siguientes:

Figura 22. Reglas de salida zonas verde y naranja



Fuente: Autoría Propia

Para finalizar con este apartado de configuración correspondiente a las reglas de firewall en Endian, en una visión general bajo configuraciones realizadas al entorno de firewall en la infraestructura de red virtualizada e implementada desde un cliente en la zona verde es posible acceder a servicios web y FTP controlados por las zonas naranja y roja, por ejemplo:

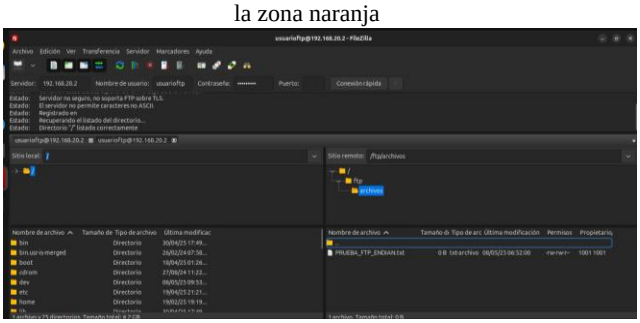
Figura 23. Acceso HTTPS desde la zona verde hacia la zona roja

Fuente: Autoría Propia

Figura 24. Acceso FTP basado en web desde la zona verde hacia la zona naranja

Fuente: Autoría Propia

Figura 25. Acceso FTP por software desde la zona verde hacia la zona naranja



Fuente: Autoría Propia

3.4 CONFIGURACIÓN DE UN PROXY NO TRANSPARENTE

Uno de los usos más populares que se ha dado en los entornos organizacionales a Endian Firewall es el de servidor proxy web. Este servidor actúa como intermediario entre el cliente y el servidor web/DNS. Cada vez que el usuario realiza una consulta web a través de un navegador, la solicitud pasa primero por el servidor proxy. Las principales características de un servidor proxy en un entorno de red son:

Filtrar el contenido mediante el bloqueo o acceso de las peticiones realizadas por el cliente al servidor.

Controlar el acceso a contenidos web mediante la autenticación de usuarios y grupos.

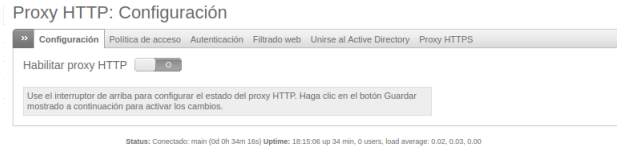
Almacenar en cache los sitios visitados, registrando una copia en el servidor para entregar tiempos de respuesta más rápidos en próximas visitas al mismo sitio.

Registro del tráfico a través del almacenamiento y seguimiento detallado de usuarios, direcciones de origen y direcciones de destino para cada consulta.

Inspección del tráfico en búsqueda de contenido prohibido, malware, spyware, virus entre otros, principalmente para sitios HTTPS.

Para habilitar las funciones de servidor proxy en Endian se deben habilitar sus servicios en Proxy HTTP: Configuración

Figura 26. Habilitar proxy HTTP



Fuente: Autoría Propia

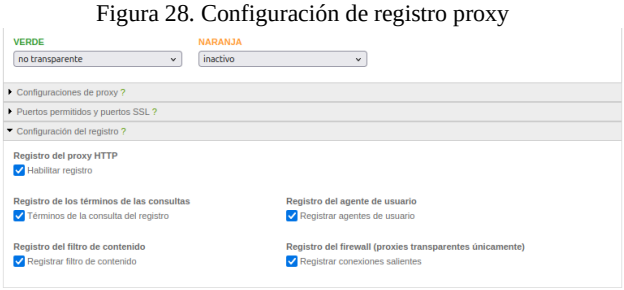
Como se pudo evidenciar anteriormente, se puede garantizar el acceso a servicios de internet para las zonas LAN y DMZ, por lo tanto, de la misma manera se pueden habilitar las funciones de proxy para las 2 zonas. En el caso del escenario simulado solo se utilizó el servidor proxy en la zona LAN, y en la zona DMZ este servicio se deja inactivo. Desde las opciones de configuración básica se confirma que el puerto de acceso predeterminado para el servidor proxy es el 8080, sin embargo, este puerto puede ser personalizado según las preferencias del administrador de red y la disponibilidad de puertos en la infraestructura interna.

Figura 27. Configuración básica proxy HTTP

Fuente: Autoría Propia

Como se mencionó anteriormente, una de las características del proxy Endian es el registro de las peticiones realizadas por los usuarios al servidor proxy. Este registro permite a los administradores de red controlar el uso de los recursos además de verificar el cumplimiento de las políticas de acceso definidas. Se debe habilitar el almacenamiento de registros desde la configuración de Endian en Configuración del registro

Figura 28. Configuración de registro proxy



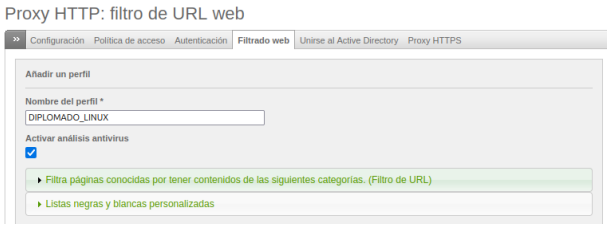
Fuente: Autoría Propia

La configuración del filtrado de contenidos para los usuarios dentro del proxy se puede abordar de manera general bajo 3 preguntas esenciales, ¿Qué?, ¿Quién? y ¿Cómo? El ¿Qué? corresponde a los filtros de contenido que se establecen, es decir, que contenido está permitido y que contenido se debe bloquear a través del proxy. ¿Quién? corresponde a los usuarios que van a acceder a los recursos web a través del servidor proxy, estos usuarios necesitan reglas de acceso establecidas por los filtros de contenido definidos. ¿Cómo? corresponde la manera en que los filtros de contenido serán aplicados a los usuarios del servidor proxy, en qué momento se aplican los filtros y si estas corresponden al bloqueo o acceso a los contenidos web.

Teniendo en cuenta el planteamiento, el primer paso para definir la configuración exitosa del servidor proxy es la

definición de los filtros de contenido. Estos filtros se definen en Endian a través de Filtrado web

Figura 29. Configuración de filtrado web



Fuente: Autoría Propia

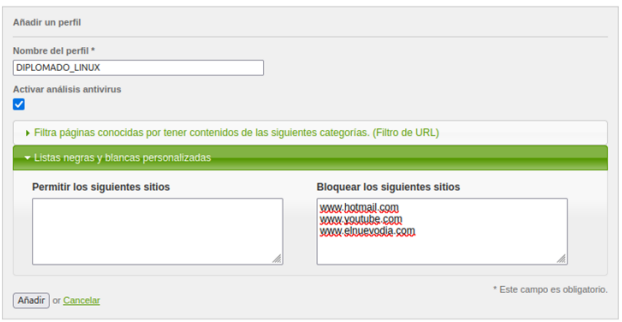
Los filtros de contenido en Endian se pueden establecer mediante 2 opciones diferentes. Por un lado, se pueden permitir o bloquear los sitios web a través de las categorías de contenido, existen 24 categorías establecidas en Endian, el servidor proxy evalúa el contenido del sitio web al que el cliente intenta acceder, si el contenido del sitio corresponde a una de las categorías se aplicara el filtro correspondiente y se garantiza o bloquea el acceso al sitio según la definición de políticas (detallada más adelante).

Figura 30. Categorías de filtros de contenido prestablecidas

Fuente: Autoría Propia

Por otro lado, es posible establecer listas personalizadas de los sitios que se requieren permitir o bloquear. Si es necesario garantizar el acceso a un sitio especifico su dirección web será incluida en el campo correspondiente a las listas blancas, si por el contrario es necesario bloqueare el acceso al sitio, su dirección se debe incluir en las listas negras. Emplear las 2 opciones de filtrado en conjunto puede permitir la construcción de un sistema robusto que gestione de manera eficiente el acceso a los recursos web, por ejemplo, en un entorno organizacional se puede realizar el bloqueo de acceso a todas las redes sociales mediante los filtros de categorías y garantizar el acceso a redes sociales corporativas como LinkedIn mediante las listas blancas personalizadas. Esta interacción conjunta es la clave para definir perfiles de filtrado web altamente eficientes. A continuación, se relaciona como ejemplo la definición de una corta lista negra personalizada.

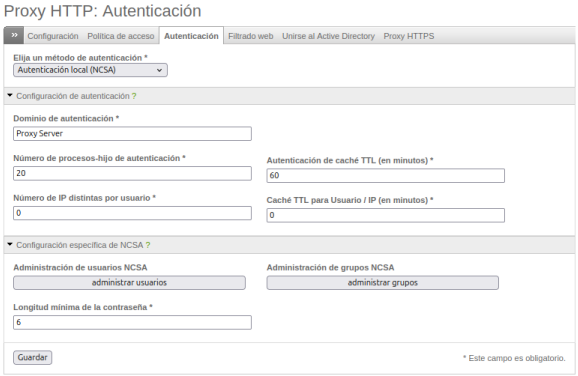
Figura 31. Lista negra personalizada



Fuente: Autoría Propia

Al terminar de definir los contenidos web permitidos y restringidos es el momento de definir los usuarios con acceso al servidor proxy. El propósito de estos usuarios va encaminado a la separación de políticas de acceso para cada usuario o grupo de usuarios y la organización de estas políticas según las similitudes existentes entre usuarios. Si un cliente no posee un usuario registrado en el proxy, no tendrá acceso a los contenidos web. La definición de usuarios se realiza en Endian desde Autenticación

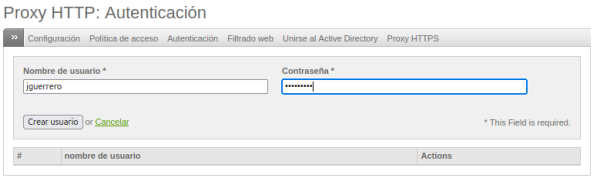
Figura 32. Configuración de autenticación proxy



Fuente: Autoría Propia

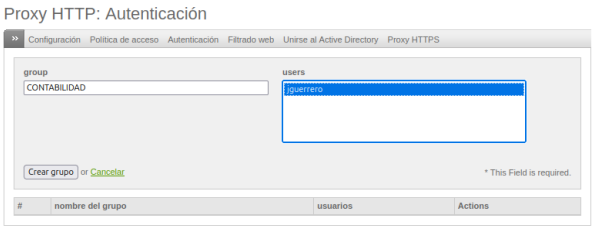
La configuración de usuarios es básica, la definición de un usuario solo contiene su nombre y una clave de autenticación. Por el lado de los grupos de usuario también se realiza una configuración básica en el proxy, se define el nombre del grupo y los usuarios registrados que pertenecen al grupo, por ejemplo:

Figura 33. Configuración de usuario proxy



Fuente: Autoría Propia

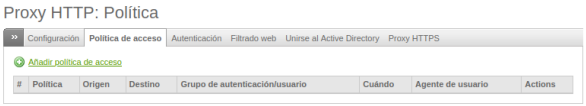
Figura 34. Configuración de grupo de usuarios proxy



Fuente: Autoría Propia

Finalmente, con los filtros de acceso definidos y los usuarios creados es momento de definir el método de asignación de los primeros a los segundos. Esta definición de políticas se realiza en Endian desde política de acceso

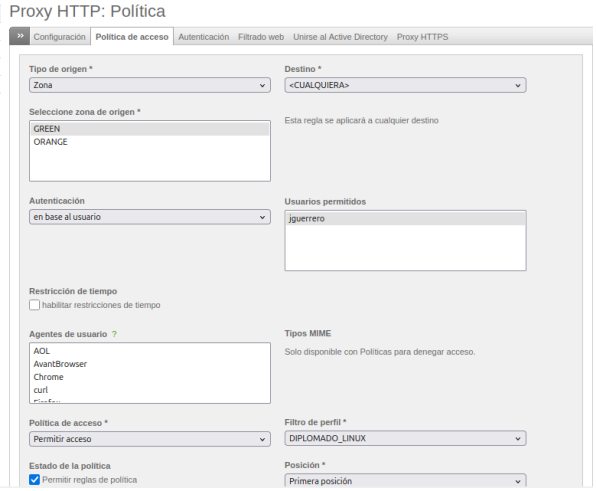
Figura 35. Políticas de acceso proxy



Fuente: Autoría Propia

En la definición de una política de acceso se debe configurar las zonas de origen y destino, la autenticación que se utilizara en la política (usuario o grupo), los agentes permitidos, es decir, en que navegadores web funcionara la política, el filtro de perfil de contenidos que se definió anteriormente y la forma específica en que se aplicara la política de acceso (permitir o denegar), por ejemplo:

Figura 36. Definición de una política de acceso proxy

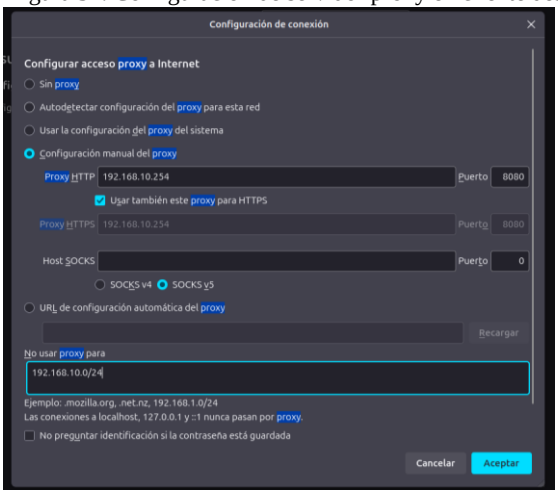


Fuente: Autoría Propia

Al finalizar esta configuración el proxy se encuentra listo para ser implementado en los equipos de la zona LAN, es necesario hacer la precisión que, al ser un proxy no transparente, la configuración debe realizarse en cada equipo cliente, una clara desventaja frente al proxy de tipo transparente que realiza el filtrado de todo el tráfico web de la infraestructura de red aplicando las políticas de acceso que se encuentren definidas.

También es importante mencionar que se debe bloquear el acceso de la configuración de proxy a los usuarios en dado caso que se opte por una implementación de proxy no transparente, teniendo en cuenta que, si se omite la configuración en un equipo cliente, este estaría fuera del control del filtrado de tráfico web y tendría un acceso ilimitado si no se establecen configuraciones adicionales desde el firewall para bloquear la salida de tráfico HTTP y HTTPS para los usuarios que no pasen primero por el servidor proxy. Desde las opciones de configuración del navegador web de un equipo cliente se define la configuración del servidor proxy, dentro de la zona LAN la dirección corresponde a la misma dirección asignada a Endian en esta zona. Se utiliza el mismo servidor proxy para el filtrado de contenidos web en protocolos HTTP y HTTPS y se excluye la red interna para continuar accediendo a la consola de configuración de Endian por fuera del servidor proxy.

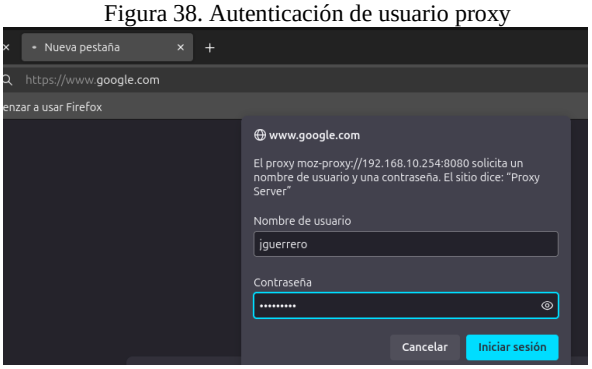
Figura 37. Configuración de servidor proxy en cliente desktop



Fuente: Autoría Propia

Después de aplicar la configuración de servidor proxy en el sistema e intentar acceder desde navegador a recursos web, se confirma que el servidor proxy se encuentra activo y funcional, este solicita la autenticación de usuario con el fin de definir las políticas de acceso que deberá aplica según la definición de reglas configuradas anteriormente.

Figura 38. Autenticación de usuario proxy



Fuente: Autoría Propia

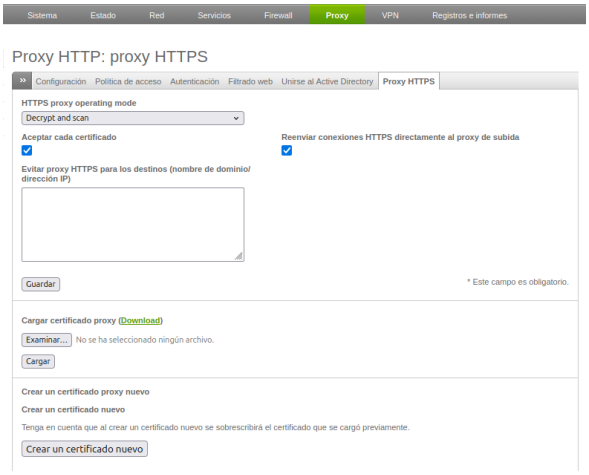
En este momento el equipo cliente está accediendo a los recursos web a través del servidor proxy, este realiza el análisis de las consultas realizadas y las permite o deniega según las reglas de acceso que tiene establecidas el usuario con el que se autentico el sistema. Si se intenta acceder a uno de los sitios definidos en la lista negra, se obtendrá un mensaje de error confirmando el bloqueo exitoso y el funcionamiento del servidor proxy:

Figura 39. Mensaje de bloqueo de contenidos

Fuente: Autoría Propia

Para que el servidor proxy de como respuesta a una solicitud de acceso el mensaje de error predeterminado en recursos disponibles para protocolo HTTPS, es necesario habilitar el servidor proxy HTTPS en la configuración de Endian y generar un certificado desde este mismo modulo que permita desencriptar y escanear los sitios web remitiendo una respuesta a los clientes sin que esta sea marcada como sospechosa o peligrosa por los navegadores web:

Figura 40. Configuración de proxy HTTPS



Fuente: Autoría Propia

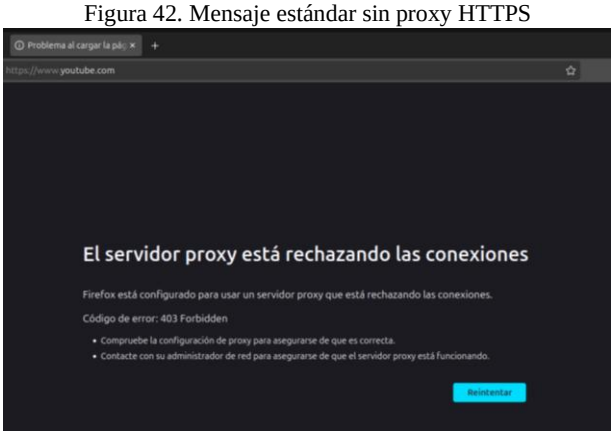
Una vez se instale el certificado generado en Endian en el equipo cliente (esta configuración debe ser realizada equipo por equipo) se puede confirmar su instalación desde la configuración del navegador web, registrando a Endian como un software seguro a través del certificado CA.

Figura 41. Administrador de certificados

Fuente: Autoría Propia

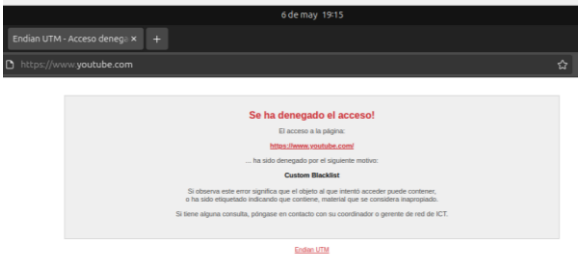
De esta manera es posible cambiar el mensaje de respuesta del error estándar establecido por el navegador al mensaje predeterminado del bloqueo del servidor proxy para las consultas de acceso realizadas a sitios bloqueados que operan bajo protocolo HTTPS, por ejemplo, YouTube.

Figura 42. Mensaje estándar sin proxy HTTPS



Fuente: Autoría Propia

Figura 43. Mensaje estándar con proxy HTTPS y certificado CA generado e instalado



Fuente: Autoría Propia

4 CONCLUSIONES

La implementación de Endian Firewall como base de arquitectura de seguridad perimetral con una DMZ demostró ser

una estrategia efectiva y confiable para la protección de servidores GNU/Linux. Realizar la segmentación de forma clara en las zonas roja, verde y naranja proporcionaron una base sólida para dicha aplicación de políticas de seguridad especificas en cada segmento. La verificación inicial de la conectividad en cada una de las zonas y su accesibilidad a la interfaz de administración del firewall son pasos necesarios e importantes para asegurar el correcto funcionamiento de una infraestructura de seguridad.

El acceso a la interfaz web de Endian Firewall, desde la red interna permitió una gestión centralizada de las reglas de firewall, verificar los servicios habilitados y la configuración de red en general. Este proceso facilita la implementación de políticas de seguridad que controlan el tráfico entre las diferentes zonas en entornos que lo ameriten y requieran, por ejemplo, permitiendo el acceso controlado desde la red externa a los servidores DMZ mientras que se restringe el acceso directo a la red interna.

El uso de tres zonas diferenciadas (roja, verde y naranja) permitió distribuir funciones de forma lógica: la zona verde como red interna confiable, la zona naranja como enclave controlado para servicios expuestos (DMZ) y la zona roja como conexión hacia la red externa (WAN). Esta topología, aplicada mediante virtualización, facilitó la simulación de un entorno real con aislamiento adecuado entre segmentos.

La correcta configuración de las reglas NAT y el tráfico enrutado en el firewall garantiza la conectividad indispensable a Internet para la red LAN, al mismo tiempo que establece una protección fundamental contra accesos no autorizados desde la WAN.

En el contexto específico del servidor DMZ, se habilitaron únicamente los servicios necesarios (HTTP y FTP) mediante reglas explícitas en el firewall, asegurando que las funcionalidades esenciales estuvieran disponibles sin abrir puertas innecesarias. La denegación del protocolo ICMP respondió a la necesidad de reducir la exposición ante técnicas de reconocimiento utilizadas comúnmente en fases iniciales de ataques. Estas decisiones, respaldadas por pruebas funcionales (consola, navegación, herramientas de red), validaron tanto el diseño como la correcta aplicación de políticas.

Las reglas de firewall permiten controlar el tráfico entrante, saliente y entre zonas gestionado por Endian, permitiendo establecer controles de seguridad integral en un entorno de red tanto físico como virtualizado. La correcta configuración e implementación de las reglas de firewall garantiza que los equipos, usuarios y servicios críticos para las organizaciones operen bajos los parámetros establecidos, fortaleciendo las segmentaciones de red definidas y de los servicios en operación, evitando al máximo posible la degradación de la seguridad, la pérdida o vulneración de la información, así como la optimización y eficiencia de los recursos disponibles.

La configuración de un servidor proxy no transparente con políticas de autenticación representa una solución altamente eficiente para garantizar el control y acceso a los servicios web dentro de una organización. Este servidor permite además la supervisión del tráfico web y la optimización de los recursos, la definición de filtros y políticas de acceso basados en la personalización a medida, mejorando la seguridad de la red interna de la organización y facilitando la navegación segura de los usuarios. Además de esto, es importante resaltar que las políticas de autenticación en conjunto con las funcionalidades del servidor proxy fortalecen el control administrativo del entorno de red, garantizan el uso de los recursos según las políticas institucionales y promueven el uso responsable de la red.

5 REFERENCIAS

[1] Linux Professional Institute. (s.f.). Linux Essentials. https://learning.lpi.org/es/learning-materials/010-160/

[2] Linux Professional Institute. (s.f.). LPIC-1: Linux Administrator Certification. https://learning.lpi.org/es/learning-materials/101-500/

[3] Free Software Foundation. (2016). Software Libre y educación. El sistema operativo GNU. http://www.gnu.org/education/education.html

[4] Endian SRL. (2016). Endian UTM 3.2 Reference Manual. Endian. https://docs.endian.com/3.2/utm/index.html

[5] Scarfone, K. & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[6] León., D. (2016). Estudio de soluciones Unified Threat Management (UTM) de libre acceso. Repositorio Institucional UNIR. https://reunir.unir.net/handle/123456789/3621.

[7] Orozco, M. (2010). Investigación y desarrollo de aplicaciones Firewall, Samba, FTP y Lamp en Ximma. Repositorio Universidad Católica de Pereira. https://repositorio.ucp.edu.co/entities/publication/5dd5cd44-d36e-414a-911b-905428ee1ba1

[8] Zapata, D., Gómez, I., Acevedo, J., Obando, C. & García, D. (2023). Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL. Revista Ingeniería: Ciencia, Tecnología E Innovación, vol. 10(1). (pp. 98 – 115). https://doi.org/10.26495/icti.v10i1.2401

[9] Caicedo, A. (2020). Herramientas firewall basadas en tecnologías Open Source. Universidad Técnica de Babahoyo. https://dspace.utb.edu.ec/handle/49000/13036

[10] Endian Knowledge Base. (2019). How to set up the HTTPS Proxy. Endian. https://help.endian.com/hc/en-us/articles/115006253507-How-to-Set-Up-The-HTTPS-Proxy

[11] Guijarro, A., Tapia, J., Viteri, X. & Zambrano, J. (2018). Guía de prácticas en Endian. Grupo Compas. http://142.93.18.15:8080/jspui/bitstream/123456789/55/1/Guia%20practicas%20endian.compressed.pdf

[12] Mancilla, G. J., et al. (2020). Implementación y administración de Infraestructura en Zentyal basada en Roles y Servicios: DHCP, Domain Services, DNS, Firewall, VPN, File Server, Print Server y Proxy. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/38562

[13] Álvarez, Z. (2019). Diseño e implementación de un sistema integrador de borde con funcionalidades de routing, firewall y central telefónica para pymes. Repositorio Digital Universidad De Las Américas. https://dspace.udla.edu.ec/handle/33000/10898