DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL INTEGRADO CON ENDIAN FIREWALL

Alvaro Dejanon Villa
advilla@unadvirtual.edu.co
Karol Andrea Bernal Reyes
kabernalr@unadvirtual.edu.co
Armando Antonio Arango Serna
aaarangos@ unadvirtual.edu.co
Luis Miguel Zarante Truaquero
lmzarantet@ unadvirtual.edu.co

RESUMEN: *En este documento se detalla el procedimiento técnico para configurar los servicios perimetrales y de conectividad de una red por medio de la herramienta open source Endian Firewall Community Edition, cubriendo la necesidad de establecer zonas de confianza, conectividad VPN y control de acceso web. Inicialmente, se establece la arquitectura base mediante la* ***definición y segmentación de las Zonas*** *(RED, GREEN, BLUE), esencial para el aislamiento del tráfico y la aplicación de políticas de seguridad. Seguidamente, se implementa la* ***conectividad remota segura*** *a través de la configuración de un túnel VPN IPSec Site-to-Site, permitiendo la comunicación cifrada entre dos redes distantes. Finalmente, se aborda la* ***gestión de acceso web*** *mediante la activación de un Proxy HTTP en modo No Transparente a través del puerto 8080, el cual exige obligatoriamente la* ***autenticación de usuarios*** *y aplica políticas de* ***filtro URL*** *para bloquear dominios específicos, resaltando la importancia de la regla crítica del Firewall de Acceso al Sistema para la correcta funcionalidad del Proxy garantizando la estabilidad de las comunicaciones perimetrales.*

PALABRAS CLAVE: Filtro URL, NAT, Proxy HTTP No Transparente, VPN, Zonas de confianza.

1 INTRODUCCIÓN

La seguridad perimetral es fundamental para proteger infraestructuras corporativas de amenazas cibernéticas. En un entorno empresarial el firewall perimetral actúa como la primera línea de defensa, filtrando el tráfico entrante y saliente según políticas de seguridad ya definidas [13]. GNU/Linux ENDIAN Firewall es una alternativa UTM con un sistema de código abierto que implementa una arquitectura en diferentes zonas de seguridad como verde (LAN), roja (WAN), naranja (DMZ). Las soluciones UTM integran múltiples funciones de seguridad en un solo dispositivo, simplificando la gestión y reduciendo costos [6]. Endian se destaca en el ecosistema open source por su interfaz unificada y su amplia documentación.

Aquí encontrará la documentación de la implementación de seguridad perimetral con ENDIAN, desde la configuración de las interfaces, pasando por la configuración de NAT, hasta la configuración de las políticas de firewall y proxy con autenticación como modelo replicable en las infraestructuras de empresas e instituciones [11]. teniendo como objetivo principal poder demostrar la viabilidad y efectividad de una UTM open source para un perímetro de red seguro, segmentado, controlado, por medio de pasos como diseñar e implementar una arquitectura de red segmentada en zonas de seguridad, configuración de reglas de NAT y firewall para el control del flujo de tráfico, Implementación de un proxy http con autenticación y filtrado de contenido y Evaluar el funcionamiento integral con pruebas de conectividad y seguridad.

.

2 METODOLOGÍA

Para esta implementación se desarrolló siguiendo una metodología de cinco fases, cada una está correlacionada con las temáticas que se realizan. La metodología adoptada es de tipo experimental aplicada, basada en el ciclo de vida de implementación de seguridad (diseño, implementación, prueba, despliegue) [3, 4], adaptada para un entorno de laboratorio controlado. Se utilizó la herramienta de virtualización VirtualBox para montar y configurar máquinas virtuales de ENDIAN Firewall, servidores Linux o zona DMZ y la red interna o zona LAN.

El direccionamiento IP que se implementó está configurado de la siguiente manera: Zona Verde LAN con dirección IP 192.168.10.1/24, Zona Roja WAN de tipo NAT se corresponde con el acceso a internet y Zona Naranja DMZ con dirección IP 192.168.20.0/24. La selección de estos rangos de direcciones privadas (RFC 1918) permite la replicación del escenario sin conflictos con redes reales. La Tabla 1 describe la arquitectura detallada.

Tabla 1. Arquitectura de Red y Configuración de Zonas

Zona / Función	Interfaz	Rango de Red	Dispositivos / Propósito	Confianza
Verde (LAN)	eth0	192.168.10./24	Hosts finales. DHCP activo.	Alto
Naranja (DMZ)	eth1	192.168.20.0/24	Server Web, FTP, Correo. Proxy.	Medio
Roja (WAN)	eth2	NAT (VM)	Conectividad saliente.	Bajo

Fuente: Autoría propia

2.1 FASES METODOLÓGICAS

Etapa 1 - El diseño y disposición: La asignación de IPs, la Generación de máquinas virtuales en VirtualBox y la definición de topología.

Etapa 2 - Instalación y configuración básica: La instalación de Endian Firewall Community Edition desde la ISO, la Generación de interfaces y su asignación a zonas.

Etapa 3 - Configuración de servicios de red: Implementación de NAT, reglas de firewall básicos y preparación de servidores en DMZ.

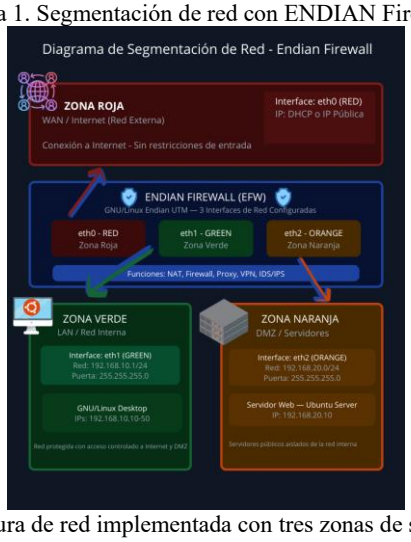
Fase 4 - Implementación de Servicios de Seguridad Avanzada: Configuración de Proxy HTTP con autenticación y filtrado URL.

Fase 5 - Pruebas y Verificación: Ejecución de pruebas de conectividad (ping, navegación), pruebas de seguridad (acceso no autenticado, filtrado) y validación de funcionalidad.

3 CONFIGURACIÓN Y SEGMENTACIÓN DE INSTANCIA ENDIAN

Se implementó la configuración de máquinas virtuales en VirtualBox, entre ellas la maquina ENDIAN la cual cuenta con tres adaptadores de red: el primero adaptador el primer adaptador en red interna "LAN" o zona verde, el segundo adaptador en red interna DMZ" o zona naranja y el tercer adaptador configurado para NAT o zona roja clave para el acceso a internet. Para poder iniciar la instalación de ENDIAN se hizo uso de la imagen ISO oficial y la documentación, del asistente de instalación tanto por vía web como por el servidor con la opción 5. En este proceso se determinaban las interfaces de red eth0 verde, eth1 naranja y eth2 roja, así como las direcciones IP que asignamos a la zona verde y naranja. La zona verde o equipos de usuarios finales la asignación de las IP se da por el servicio de DCHP mientras que la zona naranja o servidores será necesario asignarle una IP dentro de la red naranja.

Figura 1. Segmentación de red con ENDIAN Firewall.



Arquitectura de red implementada con tres zonas de seguridad.
Fuente: Autoría propia.

Los resultados mostraron que se había asignado correctamente las interfaces y que las tres zonas están totalmente operativas, también se pudo verificar la conectividad básica a través de pruebas de ping, confirmando así que existe la segmentación lógica de la red. Las pruebas de conectividad quedaron registradas en la Tabla 2. Se confirmo que no había conectividad directa no autorizada entre zonas como desde la WAN a la LAN, comprobado también el aislamiento básico. Existen latencias en las conexiones entre zona, pero son mínimas.

Tabla 2. Resultados de Pruebas de Conectividad Inicial

Prueba (Origen → Destino)	**Resultado Esperado**	**Resultado Obtenido**	**Conclusión**
LAN (Cliente) → WAN (8.8.8.8)	Sin conectividad (sin NAT)	Sin conectividad	OK. Sin NAT, no hay salida a Internet.
LAN → DMZ	Conectividad (política por defecto)	Conectividad exitosa	OK. Las zonas verdes pueden acceder a DMZ.
DMZ → LAN	Sin conectividad	Paquetes bloqueados	OK. Se aplica principio de menor privilegio.

Fuente: Autoría propia

4 INSTALACIÓN DE ENDIAN FIREWALL

La base principal para la configuración de los servicios se centra en Endian Firewall, es una distribución de seguridad de código abierto, permite transformar un sistema en un dispositivo de gestión unificada de amenazas o UTM (Unifed Threat Management).

Endian integra múltiples servicios de seguridad, tales como firewall, VPN, filtrado web, antispam y gestión de ancho de banda, todo esto permite la implementación flexible de zonas de seguridad para segmentar y administras redes corporativas

4.1 INSTALACIÓN:

Para modelar Endian en un maquina se requiere como mínimo:

- Procesador compatible x86
- 256 MB de Ram
- 2 tarjetas de Red física o virtuales
- 20 GB de disco duro o solido

Al empezar con el proceso de instalación de Endian se debe seleccionar el idioma para la instalación, cabe aclarar que antes de empezar en este proceso se debe de tener conectados los equipos o tener clara la segmentación de red.

Figura 2. Inicio del proceso de instalación de Endian

Fuente: Autoría propia

Para continuar con el proceso, El programa de instalación de Endian firewall pide confirmar la instalación.

Figura 3. Ventana de confirmación

Fuente: Autoría propia

Endian Firewall solicita usar la cantidad total del disco para continuar con la instalación.

Figura 4. Asignación de unidad de Disco

Fuente: Autoría propia

Una vez configurada la unidad de almacenamiento principal, el programa de instalación solicita asignar la dirección IP de la Zona Verde, debes colocar la dirección definida en el punto III (Configuración y Segmentación de la instancia de Endian), que para este caso es la direccion 192.168.10.1/24

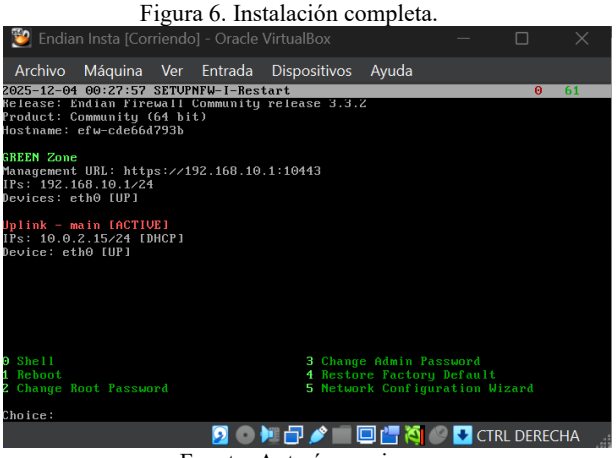
Figura 5. Configuración de la IP de la Zona Verde

Fuente: Autoría propia

Una vez que se introduce la dirección IP, el programa de instalación continua con el siguiente paso que consiste en copiar los archivos y preparar el dispositivo para utilizar el Firewall Endian.

Al finalizar el proceso de instalación observamos la interfaz del firewall como se observa en la figura 6. El firewall de Endian ahora se encuentra listo para utilizar desde la interfaz web y configurar los servicios.

Figura 6. Instalación completa.



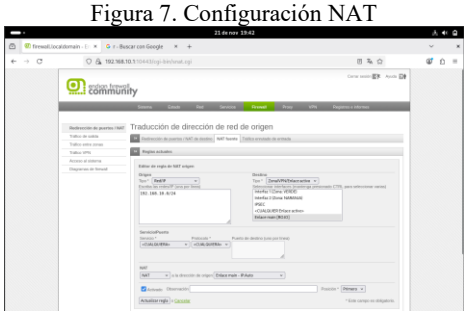
Fuente: Autoría propia

5 CONFIGURACIÓN NAT

La configuración NAT permite controlar la comunicación dentro de las redes internas y la internet, las redes verde y amarilla pueden navegar hacia el exterior, ya que el firewall direcciona a direcciones públicas, sin este redireccionamiento los equipos dentro de la red no pueden comunicarse a internet.

Para proceder con la configuración es necesario tener en cuanta cual es la red verde (192.168.10.1) y la red amarrilla (192.168.20.1), dentro del sistema de Endian hay una pestaña llamada Firewall, dentro de esa pestaña se dirige a la siguiente ruta Redirección de puertos / NAT, NAT fuente, dentro de esta opción se crea una regla, esta regla va a permitir el acceso a internet de la red verde (192.168.10.1).

Figura 7. Configuración NAT



Fuente: Autoría Propia

En origen agregamos la IP de la red ver 192.168.10.0/24, esta dirección quiere decir, que la red va abarcar el rango desde la ip 192.168.10.1 hasta la 192.168.10.255. Posteriormente en destino seleccionamos la zona roja (WAN), permitiendo que el tráfico generado desde la LAN sea traducido por el rango de las IP asignadas al firewall.

Esta regla es esencial para que las direcciones privadas de la red local puedan comunicarse con las redes externas, por otro lado, genera seguridad y un control del tráfico que abandona la infraestructura interna.

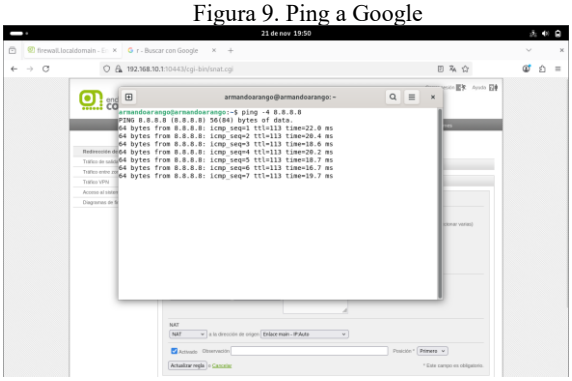
Figura 8. Aplicación de la regla

Fuente: Autoría Propia

Se verifica la creación de la regla y se aplica los cambios para que la configuración quede activa y comience a aplicar adentro del firewall.

Por último, creamos la regla, y se verifica la navegación implementada con el comando ping a 8.8.8.8 o navegando a www.google.com

Figura 9. Ping a Google

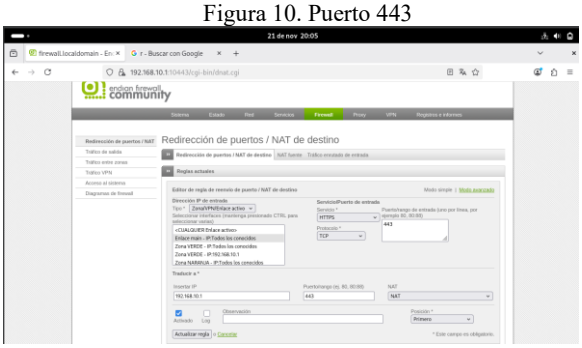


Fuente: Autoría Propia

Para la comunicación desde la zona naranja (DMZ) hacia la WAN y garantizar que lo servicios tengan acceso a internet, se crea una segunda regla de NAT. Esta regla permite mantener segmentados los dominios de la red sin exponer directamente la infraestructura interna.

Para proceder con la configuración de los puertos vamos a la opción de redirección de puertos / NAT de destino, creamos la regla para el puerto 443.

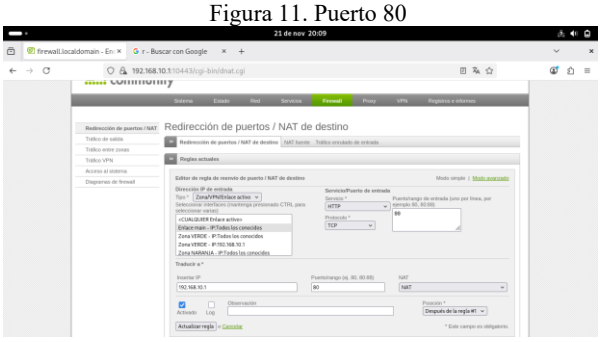
Figura 10. Puerto 443



Fuente: Autoría Propia

En dirección de IP de entrada, seleccionamos la zona roja (enlace main) en servicios escogemos el https, este servicio corresponde al puerto 443, insertamos la IP de la red verde 192.168.10.1.

Figura 11. Puerto 80



Fuente: Autoría Propia

Se implementa la misma configuración, pero en este caso se escoge el servicio http para el puerto 80 y se implementa la misma IP 192.168.10.1.

En la última configuración de los puertos permite que el firewall, las conexiones provenientes de internet se ingresen al servidor ubicado en la zona DMZ, las dos reglas activas que redirigen el tráfico hacia los puertos 80 y 443 desde la interfaz WAM hacia la dirección interna 192.168.10.1, esto garantiza que cualquier solicitud externa sea dirigida a los puertos y entregada al servidor.

Estas configuraciones tienen como finalidad controlar y asegurar los servicios internos hacia el exterior, garantizando que solo el tráfico permitido llegue al destino adecuado.

6 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

La zona DMZ se trata de un segmento de red donde se encuentra ubicado entre la red interna y la red externa (internet). Dentro de uno de sus funcionamientos estaría el adicionar una seguridad para la red interna para que estos servicios públicos como lo es el servidor web estén disponibles para todos.

6.1 ¿QUÉ SE DEBE COLOCAR EN LA ZONA DMZ?

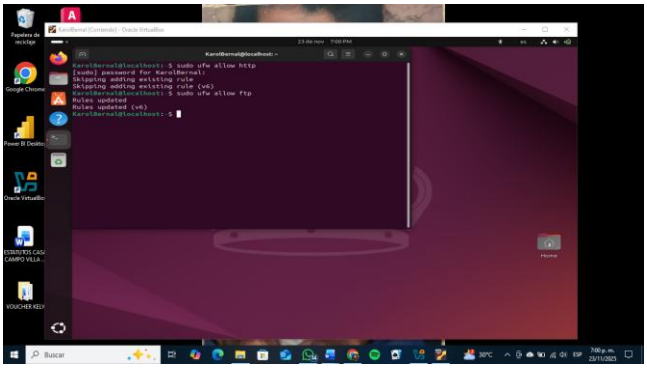
- Servidores web
- Servidores de correo electrónico
- Servidores de FTP
- Servidores públicos que requieren acceso desde la red externa.

6.2 PERMITIR SERVICIOS HTTP Y FTP

En este primer paso que es permitir los servicios de HTTP y FTP realizaremos la configuración del firewall para así poder habilitar nada más el tráfico del servidor que necesita que funcione. En este caso sería el acceso a HTTP del puerto 80 y el puerto 21.

Se ejecuta los comandos: ***sudo ufw http*** / ***sudo ufw allow ftp.*** Con este código se crea reglas donde nos pueda facilitar el servidor web y poder admitir la transferencia de archivos.

Figura 12. Permitir servicios HTTP y FTP



Fuente: Autoría propia

Con este paso logramos algo fundamental donde se delimitaría el seguimiento de los privilegios permitidos, además se aseguraría los servicios web para los usuarios y se disminuiría el ataque ya que no se dejarían abiertos los puertos que no se necesitarían.

En este paso es normal en equilibrar la accesibilidad y seguridad en servidores de producción.

6.3 DENEGAR PROTOCOLO ICMP

Para denegar el protocolo se ejecuta el comando ***sudo ufw deny icmp*** donde este protocolo es habitual para las pruebas de conectividad, pero también es utilizado bastante para atacantes y así poder descubrir existencia de un servidor por medio de escaneos de red y pueden crear mapas de topología.

Figura 13. Denegar protocolo ICMP

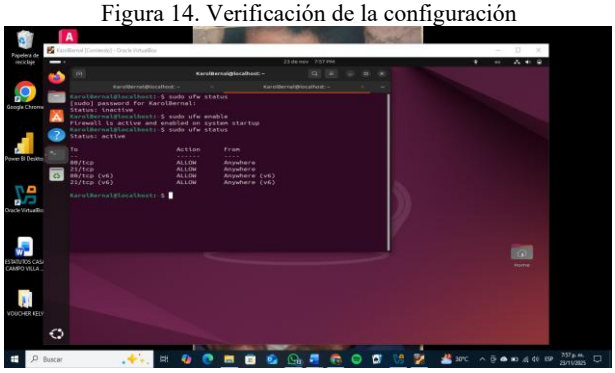
Fuente: Autoría propia

Una vez bloqueado puede aumentar la seguridad del servidor del usuario y volverlo menos visible y accesible para análisis no autorizados. También es bueno recalcar que su denegación debe de ser justificable según sean las necesidades del entorno.

6.4 VERIFICAR CONFIGURACIÓN

Después de aplicar las reglas del firewall es importante que estas se hayan realizado de manera correcta. Para esto se utiliza el comando: ***sudo ufw status***

Figura 14. Verificación de la configuración



Fuente: Autoría propia

Una vez ejecutado el comando el sistema nos permitirá visualizar todas las reglas activas y su estado actual. Este paso

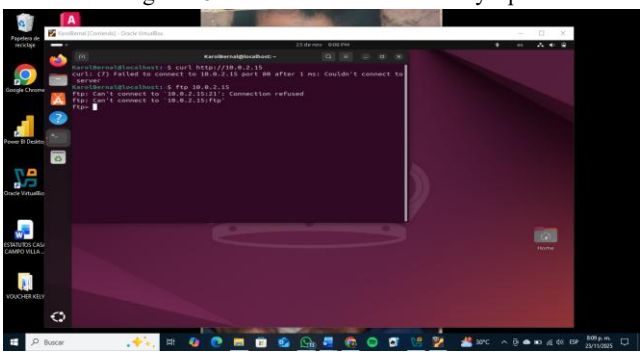
es importante ya que, valida las reglas, y garantiza la política de seguridad.

6.5 PRUEBAS DE CONEXIÓN HTTP Y FTP

Luego de configurar el firewall se procede a probar la verdadera funcionalidad del servidor. Se trabajará con dos pruebas:

1. Pruebas HTTP con curl http://10.0.2.15 donde permitirá comprobar que el sitio web responda de manera correcta desde fuera del servidor.
2. Prueba FTP con ftp 10.0.2.15 y este verificará el servicio FTP donde deberá demostrar que está accesible, autenticable y funcionando.

Figura 15. Pruebas de conexión curl y ftp



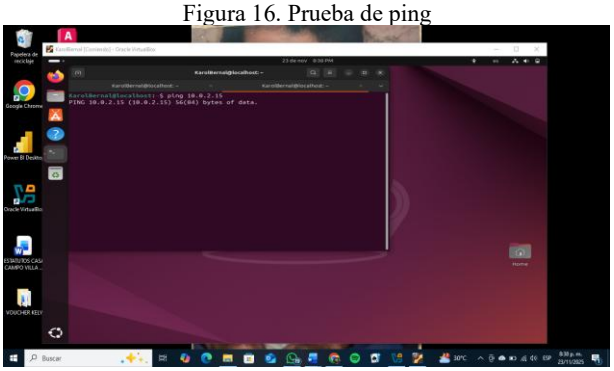
Fuente: Autoría propia

Ambas pruebas son fundamentales ya que confirman las reglas, evalúan la disponibilidad del servicio y detecta errores en la configuración o en la red.

6.6 PRUBAS DE CONEXIÓN POR MEDIO DEL COMANDO *PING*

En este paso se prueba la conexión de ping hacia el servidor web para así poder verificar que el protocolo ICMP haya sido bloqueado correctamente. A demás, al ejecutar el comando *ping 10.0.2.15* esta automáticamente manda un mensaje donde indica que el ping no ha sido exitoso. Una vez realizado este paso se estaría finalizando la prueba final de la conectividad ICMP y obtendría el ping y aseguraríamos un bloqueo por parte de ping al no ser correcto.

Figura 16. Prueba de ping



Fuente: Autoría propia

Los resultados obtenidos demuestran que el firewall está aplicado correctamente y de esta forma el servidor será invisible para otras redes, aumentando la seguridad e impidiendo la interacción externa.

7 CONFIGURACIÓN DEL SERVIDOR PROXY

La configuración de un Proxy HTTP en modo No Transparente es una práctica fundamental en la administración de redes para lograr una autenticación de usuario obligatoria y un control de tráfico granular. Este modo obliga a los clientes de la red local (Zona Verde) a especificar manualmente la dirección IP y el puerto del Proxy en su navegador, permitiendo a Endian aplicar políticas de acceso basadas en credenciales de usuario.
El objetivo principal de esta configuración consiste en:

- Implementar el Proxy HTTP en modo No Transparente (Puerto 8080).
- Exigir autenticación a usuarios asociados a un grupo.
- Bloquear el acceso a los sitios web www.youtube.com, www.hotmail.com y www.elnuevodia.com.co.

7.1 REQUISITOS PREVIOS

- Endian Firewall (UTM) instalado, configurado con la Zona Verde (GREEN 192.168.10.1), la zona naranja (ORANGE 192.168.20.1) y la Zona Roja (RED, acceso a Internet).
- Máquina cliente Ubuntu con dirección IP en el rango de la Zona Verde (192.168.10.2).

7.2 CONFIGURACIÓN DE USUARIOS Y GRUPOS PARA AUTENTICACIÓN

La autenticación se basa en usuarios y grupos internos gestionados por Endian.

A. Creación de Grupos: Navega a Sistema > Autenticación y Usuarios > Grupos. Crear un nuevo grupo con el nombre "*Contabilidad*".

B. Creación de Usuarios: Accede a la sección Usuarios. Crea un usuario con el nombre "*Contab1*" y asignar una contraseña que tenga fácil recordación, pero difícil de descifrar. Luego vincúlalo al grupo *Contabilidad*. Este grupo será el objeto de la política de acceso del Proxy.

Figura 17. Usuario vinculado en el grupo "Contabilidad"

Fuente: Autoría propia

7.3 HABILITACIÓN DEL PROXY HTTP NO TRANSPARENTE

El servicio de Proxy debe activarse en el modo que exige configuración manual por parte del cliente.

1. Entra en la sección ***Proxy HTTP***.
2. En Modo de Operación, selecciona: ***Modo no transparente*** (Non-Transparent Mode).
3. En Interfaces de Escucha, debes marcar únicamente la interfaz VERDE (GREEN).
4. Confirma que el Puerto de escucha estándar sea el 8080.
5. Marca Servidor Proxy como: ***Habilitado***.
6. Guarda y Aplica los cambios.

Figura 18. Activación de Proxy no transparente en Endian

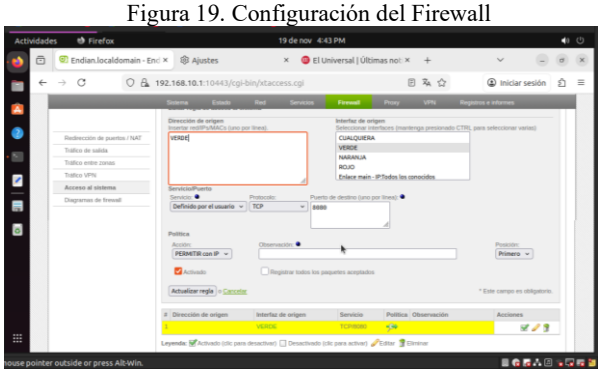
Fuente: Autoría propia

7.4 CONFIGURACIÓN DEL FIREWALL DE ACCESO AL SISTEMA (PUNTO CRÍTICO)

Para evitar el error: "*El servidor proxy está rechazando las conexiones*", es obligatorio crear una regla de firewall que permita a los clientes de la Zona Verde (GREEN) conectarse al servicio de Proxy alojado en Endian. Para hacerlo debes realizar el siguiente procedimiento:

1. Dirígete a la pestaña ***Firewall*** > ***Acceso al Sistema***
2. Crea una nueva regla (***Añadir una nueva regla de acceso al sistema***).
3. Configura los siguientes parámetros de la regla como se describe a continuación:
   • ***Dirección de Origen***: Selecciona *VERDE (GREEN)*.
   • ***Servicio/Puerto***: Definido por el usuario: ***Protocolo*** TCP, ***Puerto de destino*** 8080.
   • ***Política***: Selecciona ***PERMITIR con IP***.
4. **Guarda y Aplica** las reglas del firewall

Figura 19. Configuración del Firewall



Fuente: Autoría propia

Esta acción asegura que las peticiones que el cliente envía a 192.168.10.1:8080 sean aceptadas por el firewall de Endian antes de ser procesadas por el servicio de Proxy.

7.5 CREACIÓN DEL PERFIL DE FILTRO URL

La lista negra de sitios debe implementarse dentro de un perfil que luego será asociado a la política de acceso.

1. Entra en la sección ***Proxy HTTP***.
2. Luego dirígete a la pestaña ***Filtrado web***.
3. Crea un nuevo perfil llamado: ***lista_negra***.
4. En la sección ***Listas negras y blancas personalizadas*** ingresa los dominios a bloquear (el uso de * incluye subdominios y el protocolo HTTPS):
   *.youtube.com *.hotmail.com *.elnuevodia.com.co
5. Marca la casilla para activar el perfil.
6. Presiona Guardar y Aplicar.

Figura 20. Creación de filtro por lista negra

Fuente: Autoría propia

7.6 APLICACIÓN DE LA POLÍTICA DE ACCESO Y AUTENTICACIÓN

Se define la regla que vincula el grupo de usuarios con el perfil de bloqueo y exige la autenticación para permitir el tráfico.

1. Entra en la sección ***Proxy HTTP***.
2. Luego en la pestaña ***Política de acceso***

3. Crea una nueva regla de acceso.
4. Configura la regla:
   - ***Tipo de Origen***: Seleccionamos zona VERDE.
   - ***Destino***: definimos la zona ROJA o <ANY>.
   - ***Autenticación***: clic en en base al grupo "***Contabilidad***".
   - ***Política de acceso***: Seleccionamos: "***Permitir acceso***".
   - ***Filtro de perfil:*** Seleccionamos: ***"lista_negra"***
5. Debes asegurarte de que esta regla esté posicionada con prioridad "***1***" para que sea evaluada antes de cualquier regla general de denegación.
6. Actualiza la política y presiona Aplicar.

Esta política obliga al usuario a autenticarse con el usuario creado en el paso V-II para acceder a Internet, aplicando el filtro URL definido.

Figura 21. Política de acceso y autenticación creada

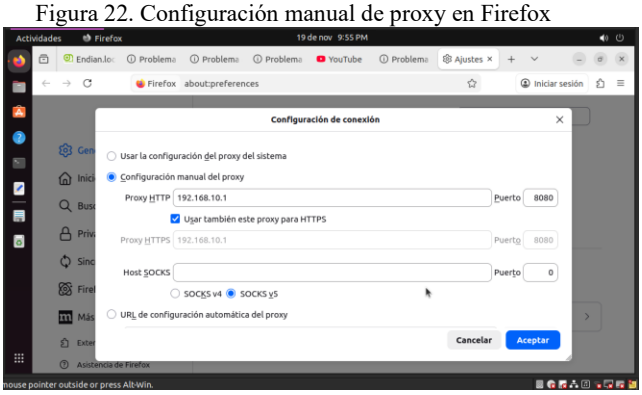
Fuente: Autoría propia

7.7 CONFIGURACIÓN Y VERIFICACIÓN FINAL DEL CLIENTE

7.7.1 CONFIGURACIÓN MANUAL DE FIREFOX

1. En la máquina cliente, abre el navegador ***Firefox***.
2. Navega a ***Configuración > General > Configuración de Red > Configuración***
3. Selecciona: ***Configuración manual del proxy***.
4. Configura: ***Proxy HTTP***: Dirección: ***192.168.10.1***, Puerto: ***8080***.
5. Marca: Usar también este proxy para ***HTTPS***.
6. Le das ***Aceptar*** para guardar la configuración.

Figura 22. Configuración manual de proxy en Firefox

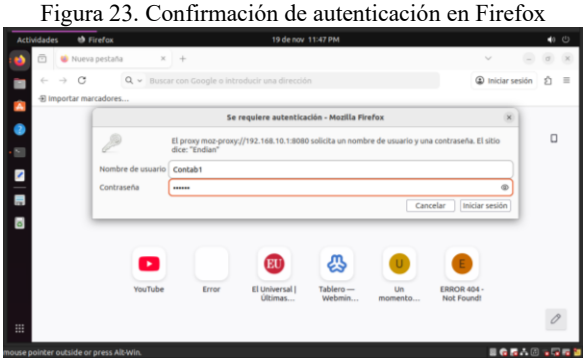


Fuente: Autoría propia

7.7.2 VERIFICACIÓN DE REQUISITOS

- ***Autenticación Requerida***: Al intentar acceder a www.google.com, el navegador muestra la ventana de autenticación.

Figura 23. Confirmación de autenticación en Firefox



Fuente: Autoría propia

- ***Navegación Funcional***: Tras ingresar las credenciales del usuario ***Contab1***, el tráfico fluye correctamente.

Figura 24. Confirmación de navegación exitosa

Fuente: Autoría propia

- ***Filtro Aplicado***: Al intentar acceder a los sitios web https://www.youtube.com, https://www.facebook.com o https://www.elnuevodia.com.co, el Proxy HTTP de Endian intercepta la solicitud y muestra la página de "*Acceso Denegado*", confirmando el funcionamiento de las políticas aplicadas.

Figura 25. Aplicación de política de lista negra

Fuente: Autoría propia

De esta manera se comprueba la efectividad del Proxy.

8 CONCLUSIONES

Endian Firewall es una de las soluciones integrales de seguridad perimetral de tipo open source, que ofrece funcionalidades completas para el manejo de seguridad en la red. Además, brinda la posibilidad de personalizar y configurar esta solución según las necesidades de cada cliente.

Implementar una solución de firewall Endian es esencial para impedir el hackeo y poder administrar la seguridad dentro de una infraestructura de red. Esta herramienta permite separar lo servicios con la posibilidad de conectarse de un equipo a otro de la misma red. Por otra parte, brinda la posibilidad de restringir sitios que no son confiables para los usuarios.

En este ejercicio, vimos como la configuración NAT permite controla los servicios que puedan ser accesibles desde la zona roja, permitiendo que los equipos conectados en la red interna (zona verde) puedan navegar sin dificultades

La puesta en marcha de un servidor Proxy HTTP en modo No Transparente permitió centralizar y controlar el tráfico web de la Zona Verde. Se pudo establecer a satisfacción un modelo de seguridad personal, forzando a la autenticación de usuarios mediante credenciales de acceso, la cual concede el acceso a Internet. Por otro lado, la implementación de un Perfil de Filtro URL con reglas de denegación basadas en dominios específicos demostró la capacidad del Endian Firewall para aplicar políticas de uso que garantizan que los sitios definidos como prohibidos fueran efectivamente bloqueados mediante la página de denegación del servidor Proxy.

9 REFERENCIAS

[1] Bueno Rosales, J. J. (2013). *Sistema de control y seguridad endian Firewall para la empresa Frada Sport (Bachelor's thesis, Quito: Universidad Israel*, 2013). [En línea]. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/493

[2] Canonical, "Security: UFW Firewall," *Ubuntu Server Documentation*. [En línea] Disponible en: https://ubuntu.com/server/docs/security-firewall

[3] Córdoba, A. (2017.) *Sistema de seguridad perimetral instalación y configuración de Endian firewall*. Silo.tips. [En línea]. Disponible en: https://silo.tips/download/sistema-de-seguridad-perimetral-instalacion-y-configuracion-de-endian-firewall

[4] D. Stenberg, "curl – *Command Line Tool and Library," cURL Project Documentation*. [En línea] Disponible en: https://curl.se/docs

[5] Endian. (n.d.). *Endian Firewall Community Docunentation: HTTP Proxy*. [En línea]. Disponible en: docs.endian.com/3.2/utm/proxy/http.html#https-proxy

[6] Endian UTM. (n.d.). *Endian UTM 3.2 Reference Manual*. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/index.html

[7] Gregg, M. (2014). *Build Your Own Security Lab: A Field Guide for Network Testing*. John Wiley & Sons.

[8] J. Postel, "RFC 792: *Internet Control Message Protocol (ICMP)," Internet Engineering Task Force (IETF)*, 1981. [En línea] Disponible en: https://datatracker.ietf.org/doc/html/rfc792

[9] J. Postel and J. Reynolds, "*RFC 959: File Transfer Protocol (FTP)," IETF, 1985*. [En línea] Disponible en: https://datatracker.ietf.org/doc/html/rfc95

[10] Lasl, F. (n.d.). *Configuración de servidor Endian Firewall*. [En línea]. Disponible en: https://www.youtube.com/watch?v=pVyJuCcm8z0

[11] Miguez Gomez, G. F. (2017). *Implementación de un sistema de gestión unificada de amenazas (UTM) para la empresa de créditos Palacio del Hogar (Master's thesis)*. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/handle/123456789/38694

[12] Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication 800-41, Rev.

[13] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

[14] Ubuntu Documentation, "*UFW – Uncomplicated Firewall*," Canonical. [En línea]. Disponible en: https://help.ubuntu.com/community/UFW

[15] Wang, S. S. (2019). *Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal, 57, 101173.* [En línea]. Disponible en: https://doi.org/10.1016/j.pacfin.2019.101173