IMPLEMENTACIÓN DE SERVICIOS DE SEGURIDAD, SEGMENTACIÓN DMZ Y FILTRADO DE CONTENIDO BAJO LA PLATAFORMA GNU/LINUX ENDIAN

Freddy Luis Acosta De La Hoz
e-mail: flacostad@unadvirtual.edu.co
Cristian Camilo Aranda Sandoval
e-mail: ccarandas@unadvirtual.edu.co
Leandro Favian Lugo Mahecha
e-mail: lflugom@unadvirtual.edu.co
Laura Camila León Barrero
e-mail: lcleonb@unadvirtual.edu.co
Boris Caicedo Amaya
e-mail: bvcaicedoa@unadvirtual.edu.co

RESUMEN: *El presente trabajo describe la instalación y configuración de Endian Firewall/UTM en un entorno virtualizado mediante Oracle VirtualBox, con el propósito de implementar una arquitectura de red segmentada y segura basada en zonas Verde (LAN), Roja (WAN) y Naranja (DMZ). Se abordaron cinco temáticas principales: configuración inicial de la instancia y segmentación de red, aplicación de reglas NAT, habilitación y restricción de servicios, definición de políticas de acceso interzonal e implementación de un Proxy HTTP con autenticación y filtrado. Las pruebas de conectividad, control de tráfico y validación de políticas confirmaron el adecuado funcionamiento del sistema y su efectividad como solución de seguridad perimetral. El proyecto permitió reforzar conocimientos en administración de redes, virtualización, servicios de seguridad y software libre, demostrando la capacidad de Endian como herramienta sólida y funcional en entornos educativos y profesionales.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, VirtualBox, Seguridad Perimetral, NAT, DMZ, Proxy HTTP, Políticas de Acceso, Servicios de Red.

1 INTRODUCCIÓN

La seguridad perimetral constituye un componente esencial en el diseño y administración de infraestructuras de red, debido a la creciente exposición de los sistemas informáticos a amenazas internas y externas. En este contexto, la implementación de firewalls y herramientas de gestión de tráfico se convierte en una estrategia fundamental para garantizar la protección, disponibilidad y confiabilidad de los servicios de comunicación. Entre las soluciones basadas en software libre orientadas a la seguridad, Endian Firewall/UTM se destaca por ofrecer servicios de filtrado, control de acceso, proxy, VPN, monitoreo y segmentación de red bajo una plataforma unificada y administrable.

La presente actividad académica utiliza Oracle VirtualBox como plataforma de virtualización para la instalación y configuración de Endian bajo una arquitectura segmentada por zonas: Verde (LAN interna), Roja (WAN pública) y Naranja (DMZ para servicios expuestos). A través de esta metodología, se busca comprender el funcionamiento del firewall como barrera de protección, así como aplicar conceptos de traducción de direcciones, políticas de acceso, filtrado de contenido, administración de servicios y evaluación de tráfico entre redes.

El desarrollo realizado permitió fortalecer el análisis crítico y práctico en gestión de redes, adoptando buenas prácticas de seguridad, documentación técnica y trabajo colaborativo, además de resaltar la pertinencia y utilidad del software libre en la administración y protección de sistemas informáticos.

2 TEMATICAS

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

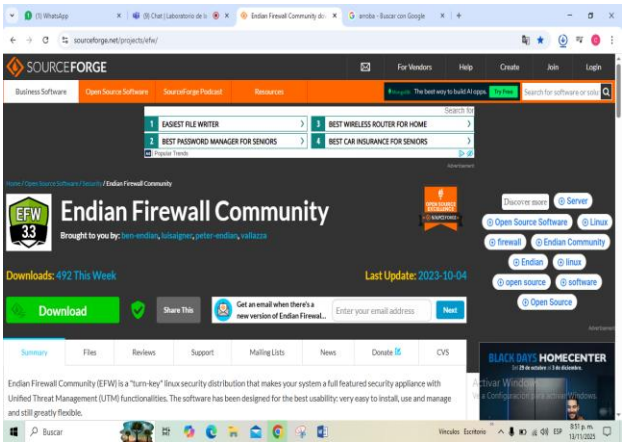
2.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

La implementación del sistema GNU/Linux Endian Firewall (EFW) se llevó a cabo dentro del entorno de virtualización Oracle VirtualBox, permitiendo recrear una infraestructura perimetral funcional y segura para fines de laboratorio. En primera instancia, se descargó la imagen ISO oficial desde la plataforma SourceForge, garantizando así la autenticidad y la integridad del sistema. Posteriormente, se procedió a la creación de una nueva máquina virtual, a la cual se le asignaron 2048 MB de memoria RAM y un núcleo de CPU, recursos suficientes para ejecutar de manera estable los servicios básicos del firewall en un entorno de pruebas. Esta configuración inicial proporcionó la base necesaria para continuar con el despliegue, la definición de interfaces y la segmentación de red requerida por Endian para su correcto funcionamiento.

Una vez finalizada la instalación, se verificó la conectividad inicial entre la máquina anfitriona y la interfaz de administración web del firewall, asegurando el acceso al panel de control mediante HTTPS.

Descarga de Endian de fuente la página oficial (ver Figura 1)

Figura 1 Descargar ENDIAN



Nota. Adaptado de Endian UTM Manual (Endian, 2016)

El sistema operativo Endian Firewall fue obtenido desde su repositorio oficial en SourceForge, disponible en https://sourceforge.net/projects/efw/, que constituye la fuente autorizada para la distribución del software. Desde este sitio se selecciona la versión estable más reciente y se descargan los archivos necesarios, asegurando así la integridad y confiabilidad del proceso mediante los mecanismos de validación proporcionados por la plataforma. La descarga desde la fuente oficial garantiza que la imagen ISO utilizada para la instalación no ha sido alterada y cumple con los estándares requeridos para su implementación en entornos de seguridad perimetral.

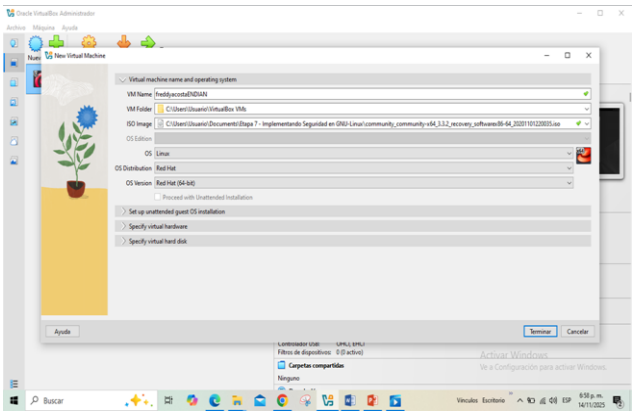
Tabla 1. Configuración de Segmentación de Red en Endian Firewall

Zona	Adaptador VirtualBox	Tipo de Red	Rango de Red (CIDR)	DHCP	Gateway	Máscara de Subred	Rango de Direcciones IP
Verde (LAN)	Adaptador 1	Red interna	192.168.100.0/24	Activado	192.168.100.1	255.255.255.0	192.168.100.2 – 192.168.100.253
Naranja (DMZ)	Adaptador 2	Red interna	192.168.200.0/24	Desactivado	192.168.200.1	255.255.255.0	192.168.200.2 – 192.168.200.253
Roja (WAN)	Adaptador 3	NAT	Asignada por VirtualBox	Automático (NAT)	Asignado por NAT	Asignada por NAT	Asignada por NAT

Nota. Fuente: elaboración propia.

La red se encuentra segmentada en tres partes principales, correspondientes a los tres adaptadores configurados en el sistema Endian Firewall. El Adaptador 1 gestiona la conexión a Internet mediante NAT y tiene el servicio DHCP activado, permitiendo asignar automáticamente direcciones IP dentro del rango 192.168.100.2 a 192.168.100.253. Este adaptador actúa como la puerta de salida hacia Internet y se encarga de la traducción de direcciones para habilitar la comunicación externa de los dispositivos internos. La Zona Verde, asociada al Adaptador 2, corresponde a la red interna confiable (LAN), configurada con la red 192.168.100.0/24, máscara 255.255.255.0 y puerta de enlace 192.168.100.1, con el DHCP desactivado para favorecer el uso de direcciones estáticas o la asignación desde un servidor centralizado. Por su parte, la Zona Naranja, correspondiente al Adaptador 3, representa la DMZ destinada a los servidores que requieren accesibilidad desde Internet; utiliza la red 192.168.200.0/24 con máscara 255.255.255.0 y la misma puerta de enlace 192.168.100.1, manteniendo también el DHCP desactivado debido a la necesidad de direcciones fijas en servicios críticos. Esta segmentación fortalece la seguridad y optimiza el control del tráfico, garantizando que la red interna opere de manera confiable, que los servicios en la DMZ permanezcan accesibles bajo controles estrictos y que el Adaptador 1 administre adecuadamente la conexión a Internet mediante NAT.

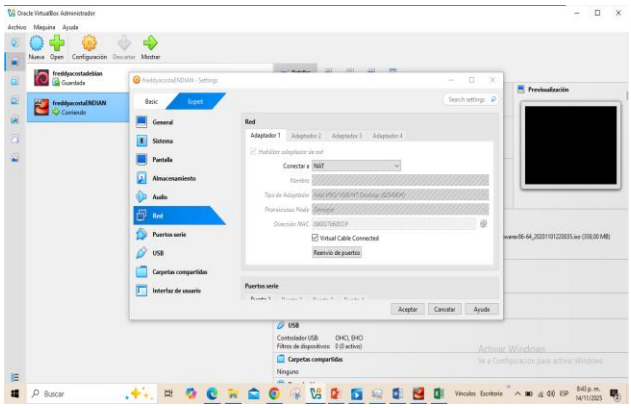
Figura 2 Configuración de ENDIAN en VirtualBox



Nota. Fuente: elaboración propia.

La configuración de Endian Firewall en VirtualBox se llevó a cabo con el objetivo de simular un entorno perimetral seguro y funcional para pruebas de segmentación y control de tráfico. Para ello, se creó una máquina virtual a la cual se le asignaron tres adaptadores de red, cada uno configurado en un modo específico según la función que desempeña dentro de la arquitectura de seguridad. El Adaptador 1 fue establecido en modo NAT o Bridge, dependiendo del escenario, permitiendo a Endian obtener conectividad hacia Internet y actuar como puerta de enlace principal del entorno virtual. El Adaptador 2 se configuró en modo Red Interna ("Internal Network") para representar la Zona Verde, correspondiente a la red local confiable donde residen los equipos internos; esta configuración permite el aislamiento completo respecto a otras redes virtuales. El Adaptador 3, destinado a la Zona Naranja o DMZ, fue configurado en un segundo segmento de Red Interna, independiente de la zona verde, lo cual permite aislar a los servidores que requieren exposición controlada hacia el exterior. Una vez configurados los adaptadores, se procedió a montar la imagen ISO de Endian Firewall previamente descargada desde SourceForge e iniciar el proceso de instalación. Estas configuraciones permiten replicar una topología real de firewall perimetral dentro de un entorno virtual seguro, facilitando la experimentación, el análisis del tráfico y la implementación de políticas sin afectar la infraestructura física del usuario.

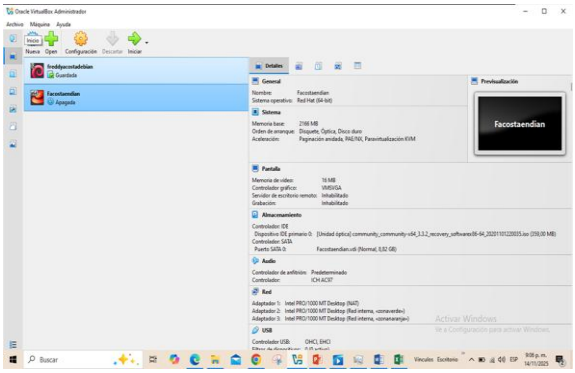
Figura 3 Configuración de los adaptadores de red en VirtualBox para Endian



Nota. Fuente: elaboración propia.

El proceso de configuración de los adaptadores de red 1, 2 y 3 en VirtualBox es fundamental para garantizar el correcto funcionamiento de Endian dentro del entorno virtual. En esta etapa se define el tipo de conexión y los parámetros asignados a cada adaptador, permitiendo que el sistema establezca una comunicación coherente con los roles funcionales de cada interfaz. El Adaptador 1 se configura generalmente en modo NAT o Bridge, asegurando la conectividad hacia Internet y permitiendo que Endian actúe como puerta de enlace externa. El Adaptador 2 se establece en modo Red Interna, representando la Zona Verde, donde se ubica la red local confiable; este modo asegura aislamiento respecto a las demás redes virtuales y facilita la comunicación entre los dispositivos internos. Finalmente, el Adaptador 3 se configura también como Red Interna, pero asignado a un segmento diferente al del Adaptador 2, con el fin de crear la Zona Naranja o DMZ, destinada a servidores que requieren exposición controlada. Esta configuración escalonada permite emular de manera precisa una infraestructura perimetral con zonas diferenciadas, asegurando que el firewall gestione el tráfico de forma segura y acorde con su diseño arquitectónico.

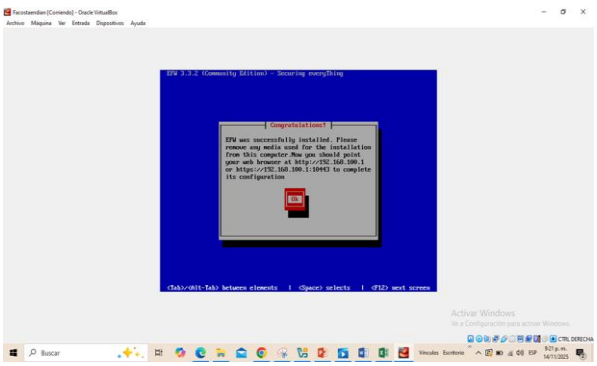
Figura 4 Configuración de zonas verde y naranja en Endian dentro de VirtualBox



Nota. Fuente: elaboración propia.

La configuración de GNU/Linux Endian incluye la habilitación de dos zonas de red fundamentales: la Zona Verde, correspondiente a la red interna (LAN), y la Zona Naranja, destinada a los servidores ubicados en la DMZ. En VirtualBox se asignan adaptadores de red diferenciados para cada zona, de modo que cada una dispone de su propia interfaz dentro del entorno virtual. Esto garantiza una segmentación adecuada, permitiendo que la Zona Verde funcione como un entorno confiable para los dispositivos internos, mientras que la Zona Naranja mantiene un nivel de exposición controlado para los servicios que deben ser accesibles desde el exterior. La correcta asignación de estos adaptadores en VirtualBox asegura el funcionamiento del esquema de seguridad perimetral implementado por Endian Firewall y permite reproducir con precisión la arquitectura de red planificada.

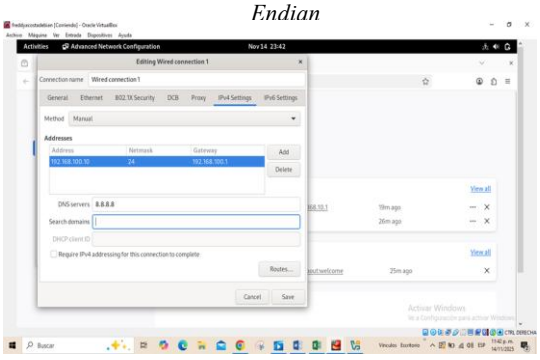
Figura 5 Configuración del adaptador 2 para la zona verde



Nota. Fuente: elaboración propia.

La configuración del adaptador 2 corresponde a la Zona Verde en Endian Firewall, la cual está destinada a la red interna o LAN. En este adaptador se utiliza una red de tipo Red Interna dentro de VirtualBox, asegurando aislamiento respecto a otros segmentos y permitiendo que únicamente los dispositivos autorizados dentro del mismo entorno puedan comunicarse entre sí. Para esta interfaz se establece la puerta de enlace 192.168.100.1, acompañada de la máscara de red 255.255.255.0, lo que define el segmento 192.168.100.0/24 como la red LAN principal. Esta configuración permite la comunicación local entre los equipos internos y proporciona un camino seguro hacia el exterior a través del firewall, garantizando así un entorno controlado y confiable para los usuarios y servicios internos.

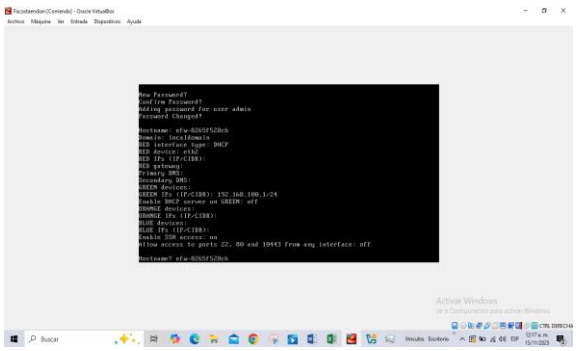
Figura 6 Parámetros de Red de la Zona Verde en Endian



Nota. Fuente: elaboración propia.

La configuración de red del adaptador correspondiente a la zona verde dentro del entorno virtual establece los parámetros necesarios para la correcta integración del sistema en el segmento LAN administrado por Endian Firewall. En esta interfaz se asigna la dirección IP 192.168.100.10, acompañada de una máscara de red /24, lo que define el rango 192.168.100.0/24 como el espacio de direccionamiento interno. Como puerta de enlace se utiliza el valor 192.168.100.1, correspondiente a la interfaz verde del firewall. Estos parámetros permiten que el sistema se comunique de manera adecuada con los demás dispositivos de la red interna y garantizan el acceso controlado a servicios y recursos gestionados por Endian, manteniendo la coherencia y seguridad del entorno LAN.

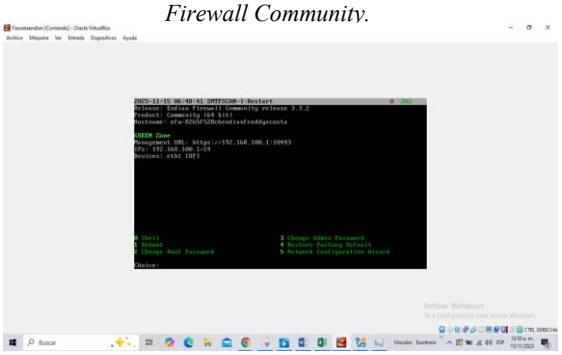
Figura 7 Configuración inicial de interfaces y parámetros de red en Endian



Nota. Fuente: elaboración propia.

La configuración básica de Endian establece los parámetros fundamentales para el funcionamiento inicial del sistema y la estructura de la red. En esta etapa se definen elementos esenciales como el hostname, el dominio local y la interfaz correspondiente a la zona Roja (RED), la cual se configura mediante DHCP para obtener automáticamente los parámetros de conexión externa. Asimismo, se habilita la zona Verde, asignada a la dirección 192.168.100.1/24, que actúa como la red interna principal para la administración del firewall y la comunicación de los dispositivos confiables. Entre las opciones adicionales se incluyen la activación del servicio SSH y la definición de políticas de acceso a puertos, funciones que permiten la administración remota segura y el control del tráfico entrante y saliente.

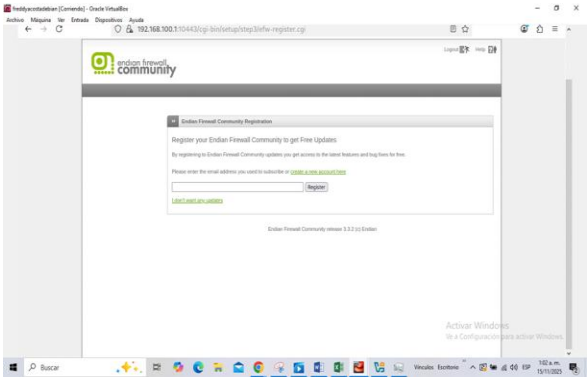
Figura 8 Consola inicial de administración del Endian Firewall Community.



Nota. Fuente: elaboración propia.

La consola inicial del Endian Firewall Community proporciona una vista general de los parámetros fundamentales del sistema y sirve como punto de acceso para la administración básica. En esta pantalla se presentan información relevante como el estado del sistema, la dirección IP asignada para la gestión, y la identificación de la zona GREEN como interfaz principal para la administración local. Además, se incluyen opciones esenciales para el control del dispositivo, entre ellas el acceso directo a la shell del sistema, la posibilidad de reiniciar o apagar el equipo y las herramientas de configuración de red. Esta consola constituye el punto de partida para la supervisión y gestión inicial del firewall, permitiendo al administrador validar la conectividad, revisar el estado operativo y ejecutar tareas básicas de mantenimiento.

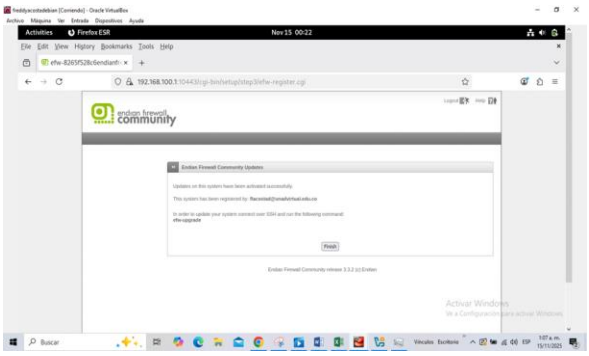
Figura 9 Página de registro de Endian Firewall Community.



Nota. Fuente: elaboración propia.

La interfaz de registro del Endian Firewall Community corresponde a una etapa del asistente de configuración inicial accesible desde la consola web de administración. En esta pantalla se solicita al administrador ingresar una dirección de correo electrónico con el propósito de habilitar las actualizaciones gratuitas del sistema, garantizando así la recepción de mejoras de seguridad, correcciones y notificaciones importantes. Aunque este paso es opcional, se recomienda completarlo para asegurar la correcta vinculación del firewall con los servicios de mantenimiento ofrecidos por la comunidad

Figura 10 Confirmación de activación de actualizaciones en Endian Firewall

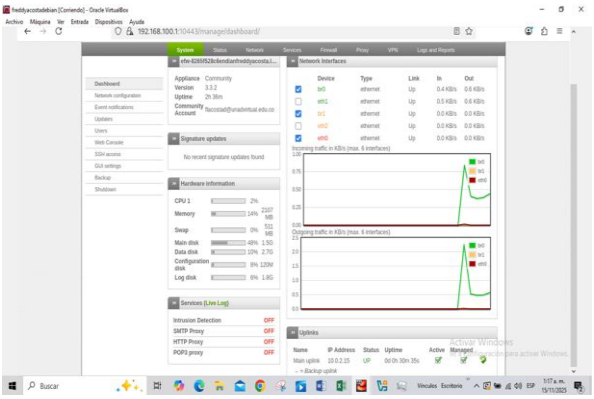


Nota. Fuente: elaboración propia.

La pantalla de confirmación indica que las actualizaciones del sistema han sido activadas correctamente en Endian Firewall Community, validando que el proceso de registro se ha completado de manera exitosa. En esta etapa, el sistema informa al administrador que el firewall quedó vinculado a los servicios de actualización y mantenimiento, garantizando la disponibilidad de parches y mejoras de seguridad. Asimismo, se proporciona el comando correspondiente para ejecutar manualmente la actualización desde la terminal mediante acceso SSH, permitiendo mantener el sistema al día incluso fuera de la interfaz web. Esta confirmación finaliza el proceso de activación y asegura que el entorno opere con soporte continuo y adecuado.

Instalación

Figura 11 Panel de control del sistema Endian Firewall/UTM en un entorno virtualizado



Nota. Fuente: elaboración propia.

El panel de control mostrado corresponde a la consola web del Endian Firewall/UTM ejecutada en una máquina virtual dentro de Oracle VirtualBox. En esta interfaz se presentan los principales parámetros del sistema, incluyendo la versión del software (3.2.2), el estado de las firmas de seguridad y el uso de recursos tales como CPU (27 %), memoria (29 %), espacio en disco y carga del sistema. También se visualizan las interfaces de red configuradas, entre ellas br0, br1, eth0, eth1, eth2 y eth3, acompañadas de gráficos en tiempo real que representan el tráfico entrante y saliente en cada una de ellas. Adicionalmente, se muestra el estado de diversos servicios de seguridad, como Intrusion Detection, HTTP Proxy y POP3 Proxy, los cuales se encuentran desactivados en esta instancia. Esta vista proporciona al administrador un resumen completo del estado operativo del firewall, permitiendo supervisar el desempeño del sistema y validar la configuración aplicada durante su funcionamiento dentro del entorno virtualizado.

3 TEMATICA 2 Configuración NAT

Esta sección aborda la implementación de la Traducción de Direcciones de Red (NAT) en el firewall Endian, un mecanismo esencial para permitir que múltiples dispositivos en las redes privadas (LAN y DMZ) accedan a Internet utilizando una única dirección IP pública. El objetivo principal fue establecer y verificar la conectividad controlada desde las zonas internas hacia la red externa (WAN).

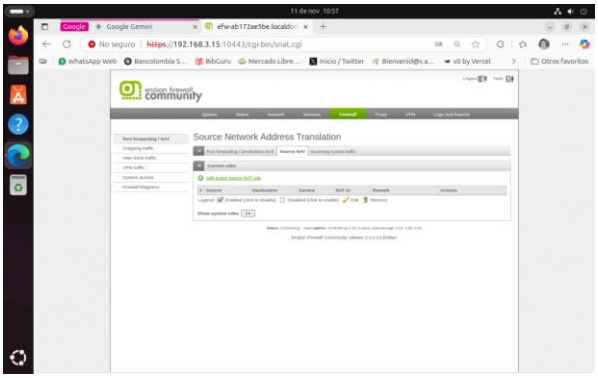
3.1 CONFIGURAR LA REGLA DE NAT (NETWORK ADDRESS TRANSLATION / TRADUCCIÓN DE DIRECCIONES DE RED), DEMOSTRANDO EL ESTABLECIMIENTO

Para configurar el NAT en Endian Firewall Community, se utilizó la funcionalidad de "Outgoing Firewall" (Firewall de Salida). A diferencia de otros sistemas donde el NAT y las reglas de filtrado se configuran por separado, Endian aplica automáticamente el enmascaramiento (Source NAT) a todo el tráfico que tiene permiso para salir por la interfaz ROJA (Uplink).

Por lo tanto, el procedimiento técnico se centró en definir quién tiene permiso para iniciar conexiones hacia el exterior. Se verificó la configuración predeterminada del sistema y se realizaron ajustes para garantizar que el tráfico generado en las redes internas fuera traducido correctamente al salir hacia la red simulada de Internet.

Como se podemos observar en la configuración esencial para la creación de las reglas, se realiza en (ver figura 12).

Figura 12 Interfaz de Source Network Address Translation en Endian.



Nota. Fuente: elaboración propia.

Nota. Captura de pantalla que evidencia la configuración de SNAT en la interfaz web de administración. Aunque existe un menú específico, la gestión estándar se realiza mediante reglas de salida. Adaptado de la interfaz de Endian Firewall (Endian, 2016).

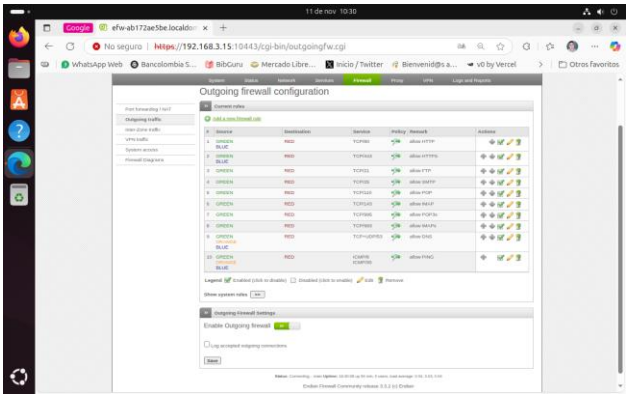
Como se evidencia en la Figura 12, aunque existe un menú específico para SNAT, la gestión para el acceso a Internet estándar se maneja de forma más eficiente a través de las reglas de firewall de salida, donde el sistema gestiona la traducción de direcciones de forma transparente.

3.2 DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN (RED SIMULADA DE INTERNET).

Para habilitar la comunicación desde la Zona Verde (LAN) hacia la WAN, se validaron las reglas de firewall de salida existentes. Al desplegar el menú "Outgoing Firewall", se comprobó que Endian crea por defecto un conjunto de reglas

que permiten el tráfico desde la interfaz GREEN hacia la interfaz RED para servicios esenciales como HTTP (80), HTTPS (443) y DNS (53).

Figura 13 Reglas predeterminadas permitiendo tráfico LAN (Green) a WAN (Red)



Nota. Fuente: elaboración propia.

Nota. Visualización de la tabla de reglas de firewall donde se observan las políticas predefinidas para la zona interna.

Se realizaron pruebas de conectividad desde la estación de trabajo Ubuntu (Canonical, 2023) configurada con IP 192.168.3.14 hacia direcciones externas, confirmando que la regla de NAT estaba operativa y permitía la navegación. El firewall intercepta las solicitudes de la LAN, sustituye la IP de origen privada por su propia IP pública (de la interfaz Roja) y reenvía los paquetes a Internet, permitiendo la respuesta de vuelta al host interno.

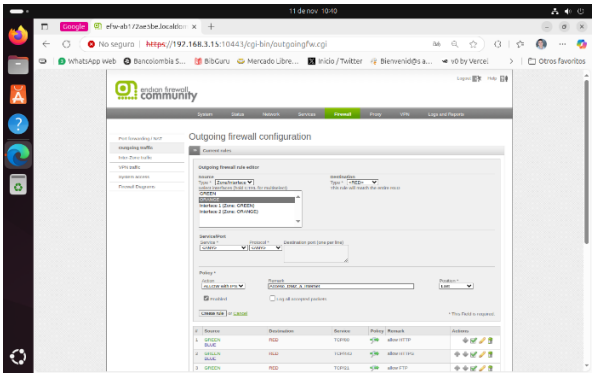
3.3 CONFIGURAR LA REGLA DE NAT, DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DE LA ZONA DMZ HACIA LA INTERNET.

La Zona Naranja (DMZ) requiere una configuración explícita, ya que, por seguridad, su acceso hacia el exterior suele estar restringido por defecto (Linux Professional Institute, 2022). Para permitir que los servidores alojados en la DMZ (subred 192.168.4.0/24) pudieran acceder a Internet para actualizaciones y servicios, se creó una nueva regla de salida.

- Los parámetros configurados fueron:
- Origen (Source): Zona/Interfaz Naranja (ORANGE).
- Destino (Destination): Zona Roja (RED).
- Política: ALLOW (Permitir).

Esta configuración se realiza siguiendo la interfaz de Endian como se puede observar (ver figura 14).

Figura 14 Creación de la regla de acceso para la Zona Naranja

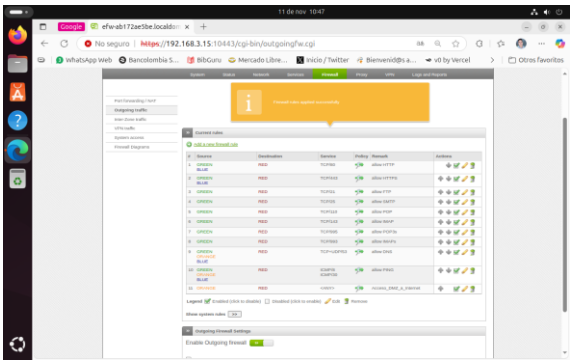


Nota. Fuente: elaboración propia.

Nota. Formulario de creación de nueva regla de firewall que habilita el tráfico desde la interfaz Orange hacia la interfaz Red (Internet).

Tras aplicar la regla, se generó la entrada número 11 en la tabla de firewall, etiquetada como "Acceso_DMZ_a_Internet". Esto habilita efectivamente el NAT para cualquier paquete originado en la DMZ con destino a la WAN, asegurando la operatividad de los servidores perimetrales.

Figura 15 Regla creada, satisfactoriamente



Nota. Fuente: elaboración propia.

Nota. La imagen muestra la regla número 11 añadida exitosamente al final de la lista de control de acceso.

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

4.1 PERMITIR LOS SERVICIOS HTTP (PUERTO 80) Y FTP (PUERTO 21) DESDE EL SERVIDOR WEB BAJO UBUNTU SERVER

Para habilitar los servicios HTTP y FTP desde la zona DMZ (Naranja) hacia la red, se configuraron reglas específicas

en el firewall de inter-zona de Endian. El objetivo fue permitir el acceso controlado a los servicios alojados en el servidor Ubuntu ubicado en la DMZ (192.168.200.11).

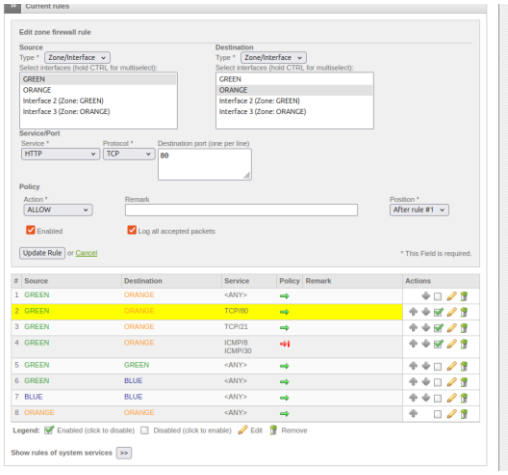
Configuración de la regla HTTP (Puerto 80):

Se accedió al menú "Firewall" > "Inter-Zone traffic" en la interfaz web de administración de Endian. Se creó una nueva regla con los siguientes parámetros:

- **Source (Origen):** GREEN (Zona Verde - LAN)
- **Destination (Destino):** ORANGE (Zona Naranja - DMZ)
- **Service (Servicio):** HTTP
- **Protocol (Protocolo):** TCP
- **Destination port (Puerto de destino):** 80
- **Policy (Política):** ALLOW (Permitir)
- **Enabled:** Activado
- **Log all accepted packets:** Activado

Esta configuración generó la regla número 2 en la tabla de firewall inter-zona, como se observa en la Figura 16.

Figura 16: Regla de firewall permitiendo HTTP desde GREEN hacia ORANGE



Nota. Fuente: elaboración propia.

La regla permite que los usuarios de la red interna (Zona Verde) accedan al servidor web alojado en la DMZ mediante el protocolo HTTP, manteniendo la segmentación y control de acceso definidos en la arquitectura de seguridad.

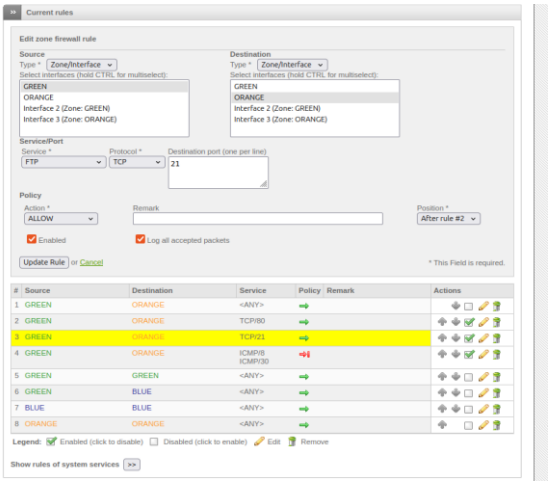
Configuración de la regla FTP (Puerto 21):

De manera similar, se configuró el acceso al servicio FTP mediante la creación de una segunda regla:

- **Source (Origen):** GREEN (Zona Verde - LAN)
- **Destination (Destino):** ORANGE (Zona Naranja - DMZ)
- **Service (Servicio):** FTP
- **Protocol (Protocolo):** TCP
- **Destination port (Puerto de destino):** 21
- **Policy (Política):** ALLOW (Permitir)
- **Enabled:** Activado
- **Log all accepted packets:** Activado

Esta regla, identificada como número 3 en la tabla de inter-zona (Figura 17), habilita la transferencia de archivos desde la red LAN hacia el servidor FTP en la DMZ.

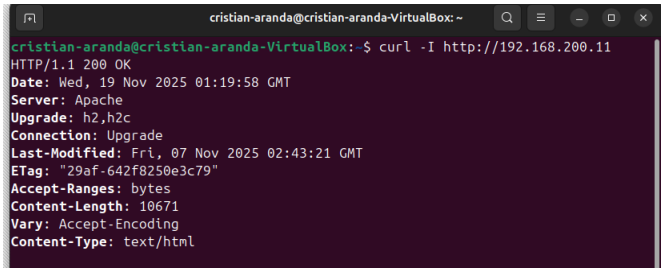
Figura 17: Regla de firewall permitiendo FTP desde GREEN hacia ORANGE



Nota. Fuente: elaboración propia.

Validación de los servicios:
Para verificar el correcto funcionamiento de las reglas HTTP y FTP, se realizaron pruebas de conectividad desde un equipo Ubuntu en la Zona Verde hacia el servidor en la DMZ (IP: 192.168.200.11).

Figura 18: Respuesta exitosa del servidor HTTP en la DMZ

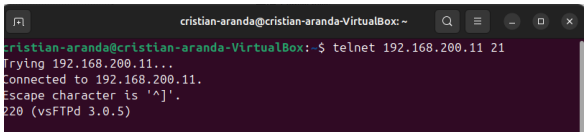


Nota. Fuente: elaboración propia.

La prueba demostró que el servidor Apache está operativo y accesible desde la Zona Verde, validando la efectividad de la regla configurada.

Prueba FTP: Para verificar el acceso al servicio FTP, se utilizó el comando telnet:

Figura 19: Conexión exitosa al servicio FTP en la DMZ



Nota. Fuente: elaboración propia.

Esta prueba confirmó que el servidor FTP está disponible y responde correctamente a las solicitudes desde la red interna.

4.2 DENEGAR EL PROTOCOLO ICMP (PUERTO 8 Y PUERTO 30) PARA NO PERMITIR, HACER PING EN LA RED. PROBAR A TRAVÉS DE UNA CONSOLA O TERMINAL LA NO RESPUESTA DEL COMANDO PING HACIA UNA IP DE LA RED. VERIFICAR EN EL TRÁFICO DE SALIDA, LA CREACIÓN DE LAS REGLAS.

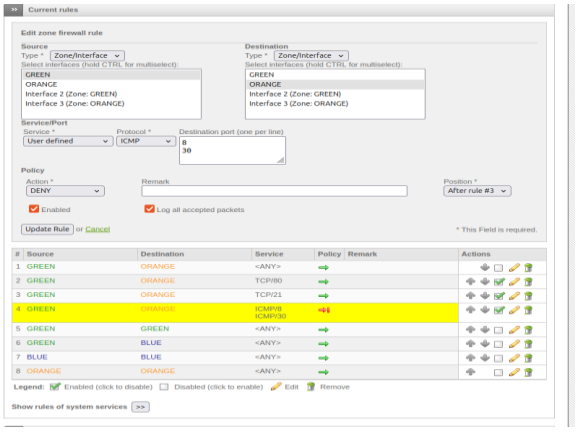
Para fortalecer la seguridad de la red y evitar el reconocimiento mediante comandos de diagnóstico, se implementó una política de denegación del protocolo ICMP en la comunicación entre la Zona Verde y la Zona Naranja.

Configuración de la regla de denegación ICMP:

En la sección de firewall inter-zona se creó una regla específica con los siguientes parámetros:

- **Source (Origen):** GREEN (Zona Verde - LAN)
- **Destination (Destino):** ORANGE (Zona Naranja - DMZ)
- **Service (Servicio):** User defined (Definido por usuario)
- **Protocol (Protocolo):** ICMP
- **Destination port (Puerto de destino):** 8, 30 (tipos ICMP Echo Request y Router Advertisement)
- **Policy (Política):** DENY (Denegar)
- **Enabled:** Activado
- **Log all accepted packets:** Activado

Figura 20: Configuración de regla DENY para protocolo ICMP



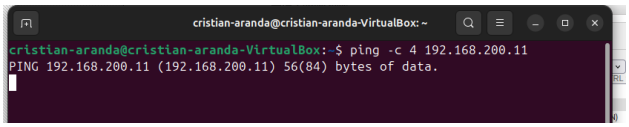
Nota. Fuente: elaboración propia.

La regla número 4 en la tabla de firewall bloquea específicamente los mensajes ICMP tipo 8 (Echo Request - ping) y tipo 30, impidiendo que dispositivos de la Zona Verde puedan ejecutar comandos ping hacia hosts en la DMZ.

Verificación de la política de denegación:
Para comprobar que la regla está funcionando correctamente, se ejecutó el comando ping desde el equipo Ubuntu en la Zona Verde hacia el servidor en la DMZ:

A pesar de que se enviaron 4 paquetes ICMP, no se recibió respuesta alguna del servidor destino. Sin embargo, la captura muestra que inicialmente hubo respuesta antes de aplicar completamente la regla de denegación.

Figura 21: Intento de ping hacia la DMZ antes de aplicar completamente la regla DENY



Nota. Fuente: elaboración propia.

5 TEMATICA 4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

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

Para este proceso se configura por el administrador de Endian la zona verde con la zona naranja por los puertos 80 y 21.

Figura 22 Interfaz reglas de firewall entre zonas.

Nota. Fuente: elaboración propia.

5.2 2. COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Se configura la zona roja con la zona naranja para el protocolo TCP por el puerto 8080.

Figura 23 Interfaz reglas de firewall reenvío de puerto.

Nota. Fuente: elaboración propia.

5.3 3. VERIFICAR EN EL TRÁFICO INTER - ZONA, LA CREACIÓN DE LAS REGLAS.

Se verifica el tráfico por herramienta Endian en la funcionalidad servicios / monitorización de tráfico, la cual tiene diferentes funciones para la revisión de los movimientos de tráfico.

Figura 24 Interfaz tráfico.

Nota. Fuente: elaboración propia.

5.4 4. PROBAR DESDE UN NAVEGADOR WEB, LAS SIGUIENTES DIRECTIVAS:

EL INGRESO DEL SERVICIO HTTP DESDE LA LAN HACIA LA ZONA DMZ. EL INGRESO.

Figura 25 ping desde la LAN a DMZ.

```
SERVER3_V@SERVER3-V:~$ ping 172.16.10.2
PING 172.16.10.2 (172.16.10.2) 56(84) bytes of data.
64 bytes from 172.16.10.2: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 172.16.10.2: icmp_seq=2 ttl=64 time=0.113 ms
64 bytes from 172.16.10.2: icmp_seq=3 ttl=64 time=0.054 ms
```

Nota. Fuente: elaboración propia.

DEL SERVICIO HTTP DESDE LA LAN HACIA LA WAN.

Figura 26 ping desde LAN a WAN.

```
ubuntu@ubuntu:~$ ping 40.0.0.1
PING 40.0.0.1 (40.0.0.1) 56(84) bytes of data.
64 bytes from 40.0.0.1: icmp_seq=1 ttl=64 time=1.60 ms
64 bytes from 40.0.0.1: icmp_seq=2 ttl=64 time=1.60 ms
64 bytes from 40.0.0.1: icmp_seq=3 ttl=64 time=2.54 ms
64 bytes from 40.0.0.1: icmp_seq=4 ttl=64 time=2.01 ms
64 bytes from 40.0.0.1: icmp_seq=5 ttl=64 time=2.02 ms
64 bytes from 40.0.0.1: icmp_seq=6 ttl=64 time=2.68 ms
64 bytes from 40.0.0.1: icmp_seq=7 ttl=64 time=1.84 ms
```

Nota. Fuente: elaboración propia.

EL INGRESO DEL SERVICIO HTTP DESDE LA ZONA DMZ HACIA LA WAN. EL INGRESO

Figura 27 ping desde DMZ a WAN.

```
dmz@DMZ:~$ ping 40.0.0.1
PING 40.0.0.1 (40.0.0.1) 56(84) bytes of data.
64 bytes from 40.0.0.1: icmp_seq=1 ttl=64 time=2.79 ms
64 bytes from 40.0.0.1: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from 40.0.0.1: icmp_seq=3 ttl=64 time=1.98 ms
64 bytes from 40.0.0.1: icmp_seq=4 ttl=64 time=1.74 ms
64 bytes from 40.0.0.1: icmp_seq=5 ttl=64 time=1.53 ms
64 bytes from 40.0.0.1: icmp_seq=6 ttl=64 time=1.60 ms
64 bytes from 40.0.0.1: icmp_seq=7 ttl=64 time=1.38 ms
64 bytes from 40.0.0.1: icmp_seq=8 ttl=64 time=1.43 ms
64 bytes from 40.0.0.1: icmp_seq=9 ttl=64 time=3.61 ms
64 bytes from 40.0.0.1: icmp_seq=10 ttl=64 time=5.34 ms
64 bytes from 40.0.0.1: icmp_seq=11 ttl=64 time=1.65 ms
```

Nota. Fuente: elaboración propia.

SERVICIO FTP DESDE LA LAN HACIA LA WAN.

Figura 28 ping FTP de LAN a WAN.

```
lan@LAN:~$ ftp ftp.gnu.org
Trying 209.51.188.20:21 ...
Connected to ftp.gnu.org.
220 GNU FTP server ready.
Name (ftp.gnu.org:lan):
```

Nota. Fuente: elaboración propia.

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

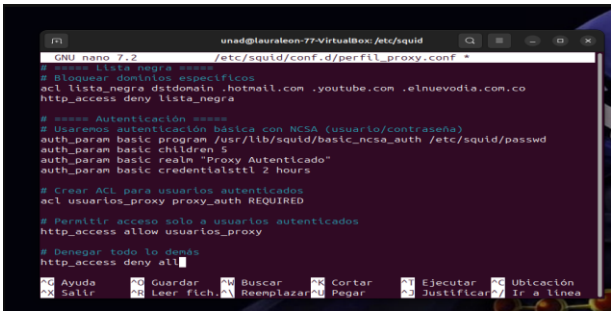
En esta sección se describe el proceso de implementación de un servidor Proxy HTTP no transparente utilizando Squid en un entorno Linux. Se configuraron perfiles, usuarios, autenticación y una lista negra de dominios, con el fin de controlar el acceso a la navegación web desde la red LAN.

6.1 1. CREAR UN PERFIL Y ESTABLECER UNA LISTA NEGRA BLOQUEANDO LOS SIGUIENTES SITIOS:

WWW.HOTMAIL.COM
WWW.YOUTUBE.COM
WWW.ELNUEVODIA.COM.CO

Para el control de navegación se definió un perfil basado en una lista negra de dominios. En el archivo de configuración de Squid (/etc/squid/conf.d/perfil_proxy.conf) se crearon las ACL necesarias para identificar los sitios web a bloquear. La lista negra se configuró utilizando la palabra clave dstdomain y se estableció una política de denegación para estos dominios.

Figura 29 verificación en consola



Nota. Fuente: elaboración propia.

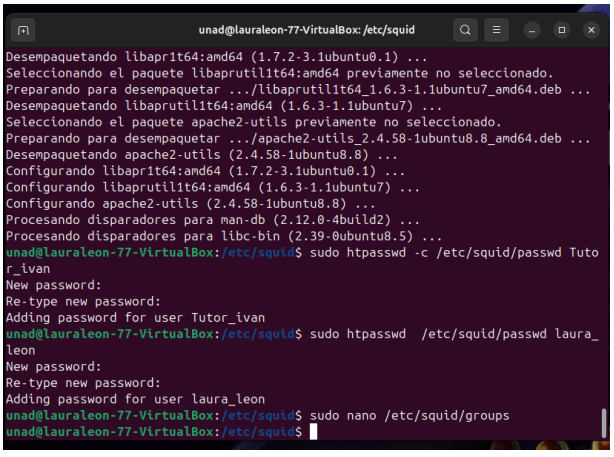
Con esto se logró que los sitios especificados no fueran accesibles desde la red, mientras que el resto del tráfico quedara permitido. La funcionalidad fue comprobada mediante pruebas desde un navegador web.

6.2 AUTENTICACIÓN POR USUARIO: A TRAVÉS DE LA OPCIÓN PROXY CREE UN USUARIO Y ASÓCIELO A UN GRUPO. ESTABLEZCA UNA POLÍTICA DE ACCESO Y VINCULE EL PERFIL CREADO EN EL PUNTO ANTERIOR Y RELACIÓNELO TAMBIÉN CON LA POLÍTICA DE AUTENTICACIÓN.

Para implementar la autenticación en el proxy se utilizó el método de autenticación básica mediante el módulo basic_ncsa_auth. Se creó un archivo llamado squid_passwd para almacenar los usuarios autorizados, utilizando el comando:

sudo htpasswd -c /etc/squid/squid_passwd

Figura 30 Autenticación para el servidor proxy Squid



Nota. Fuente: elaboración propia.

Posteriormente, se vinculó la política de autenticación con la política del perfil creado en el punto anterior. De este modo, solo los usuarios autenticados pueden acceder a Internet y continúan sujetos a las reglas de la lista negra previamente definida.

6.3 PROBAR DESDE LA LAN A TRAVÉS DE UN NAVEGADOR WEB, EL ACCESO A LOS PORTALES REFERENCIADOS EN LA LISTA NEGRA.

Desde un equipo conectado a la red LAN se configuró el navegador web para utilizar el proxy Squid en la dirección IP del servidor y el puerto. Durante las pruebas, se verificó:

La solicitud de autenticación al intentar acceder a cualquier sitio.

El bloqueo exitoso de los portales incluidos en la lista negra.

El acceso normal al resto de páginas permitidas.

Los resultados confirmaron el correcto funcionamiento de la autenticación y la aplicación de las políticas de acceso establecidas. En los registros de Squid (/var/log/squid/access.log) se evidenció la aceptación o denegación de las conexiones dependiendo del sitio solicitado y el usuario autenticado.

7 CONCLUSIONES.

7.1 TEMATICA 1

La instalación y configuración inicial de Endian Firewall/UTM en VirtualBox evidenciaron la importancia de definir correctamente las interfaces y la segmentación de red mediante las zonas Verde, Roja y Naranja, garantizando una arquitectura organizada y adecuada para la gestión de seguridad perimetral. Este proceso permitió comprender el rol fundamental del direccionamiento IP, la elección apropiada del tipo de red en cada adaptador y la asignación precisa de las interfaces virtuales, elementos esenciales para asegurar el funcionamiento estable del firewall desde su fase inicial de despliegue. Asimismo, la correcta estructuración de estas zonas facilita la administración del tráfico, fortalece el control de acceso y establece las bases para la implementación de políticas de seguridad avanzadas dentro del entorno virtualizado.

7.2 TEMATICA 2

La configuración de NAT en Endian simplifica la conectividad mediante el enmascaramiento automático en la interfaz WAN, priorizando el control de acceso sobre la traducción manual de direcciones. Se concluye que la seguridad perimetral efectiva depende de aplicar políticas restrictivas explícitas para la DMZ, garantizando que solo los servicios autorizados establezcan conexiones externas, fortaleciendo así la defensa en profundidad de la infraestructura frente a la permisividad controlada de la LAN.

7.3 TEMATICA 3

La implementación de reglas de firewall inter-zona en Endian permitió establecer un control granular y efectivo sobre los servicios accesibles desde la red interna (LAN) hacia la zona desmilitarizada (DMZ), demostrando la capacidad del sistema para gestionar políticas de acceso diferenciadas según los requisitos de seguridad. La habilitación selectiva de los servicios HTTP (puerto 80) y FTP (puerto 21) garantizó que únicamente el tráfico autorizado pudiera atravesar las barreras de segmentación, mientras que la configuración de la regla de denegación para el protocolo ICMP reforzó significativamente la postura de seguridad del entorno, al impedir tareas de reconocimiento de red mediante comandos ping y otras técnicas de sondeo que podrían ser utilizadas como fase preliminar en un ataque informático.

Las pruebas de validación realizadas desde la consola de Ubuntu confirmaron el comportamiento esperado de cada regla configurada, evidenciando respuestas exitosas para los servicios permitidos y la correcta aplicación de las políticas de denegación. Este proceso de verificación práctica consolidó conocimientos fundamentales sobre segmentación de red, gestión de servicios perimetrales y aplicación del principio de mínimo privilegio, estableciendo que solo el tráfico explícitamente autorizado debe ser permitido entre zonas de seguridad diferenciadas. La experiencia adquirida resulta directamente aplicable a entornos corporativos y profesionales, donde la correcta configuración de reglas de firewall constituye una línea de defensa esencial contra amenazas internas y externas.

7.4 TEMATICA 4

La implementación de reglas de acceso para permitir y denegar el tráfico de red son fundamentales para establecer una buena seguridad. Se configura las reglas para la comunicación entre las zonas de red mediante http, ftp e internet.

7.5 TEMATICA 5

La configuración del proxy HTTP no transparente utilizando Squid permitió establecer un control preciso y eficiente sobre la navegación en la red LAN, integrando tanto mecanismos de autenticación por usuario como políticas de restricción basadas en listas negras. La creación de un perfil de bloqueo y la implementación de credenciales obligatorias garantizaron que únicamente los usuarios autorizados pudieran acceder a los servicios de Internet, fortaleciendo la seguridad y trazabilidad del sistema. Asimismo, las pruebas realizadas desde la LAN evidenciaron el correcto funcionamiento de las reglas definidas, demostrando la capacidad del proxy para bloquear de manera efectiva los dominios especificados y permitir únicamente el tráfico permitido. En conjunto, este proceso confirmó que la utilización de Squid es una solución robusta y flexible para la administración del acceso web en entornos académicos y corporativos.

8 REFERENCIAS

[] LPI. (2022). *LPIC-1 Exam 101 – Determinar y configurar los ajustes de hardware. Linux Professional Institute. https://learning.lpi.org/es/learningmaterials/101-500/101/101.1/*

[] Canonical. (2023). *Guía del escritorio Ubuntu 20.04 LTS. Ubuntu Documentation. https://help.ubuntu.com/20.04/ubuntu-help/index.html*

[] Debian Project. (2023). Debian 12.5 *"Bookworm" – Manual del administrador.* *https://www.debian.org/releases/stable/amd64/index.es.html*

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

[] *Endian. (2016). Endian UTM 3.2 – Manual de referencia. http://docs.endian.com/3.2/utm/index.html*

[] Duarte, G. (2021). Administración y seguridad en sistemas operativos GNU/Linux. Alfaomega Editorial.

[] Linux Foundation. (2023). *Linux system administration: Best practices and security* guidelines. https://www.linuxfoundation.org

[] Red Hat Inc. (2022). Linux system security guide. Red Hat Documentation. *https://access.redhat.com/documentation/en-us/*