IMPLEMENTANDO SEGURIDAD EN LINUX: PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Julián Humberto Méndez Brand
email: jhmendezb@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de un proxy HTTP no transparente utilizando Endian Firewall Community como parte de la práctica de seguridad en redes Linux. Se explica la preparación del entorno virtual, la configuración de las interfaces de red, la activación del servicio de proxy y la creación de políticas de acceso basadas en usuarios. Además, se describen las pruebas de conectividad realizadas desde un cliente Ubuntu Desktop y la validación del funcionamiento del filtrado web, evidenciando el fortalecimiento del control perimetral en el entorno académico propuesto.*

PALABRAS CLAVE: Endian, interfaz, red, configuración, HTTP, Linux.

1. INTRODUCCIÓN

La seguridad perimetral es uno de los pilares fundamentales en la protección de infraestructuras tecnológicas dentro de organizaciones empresariales. En entornos donde múltiples dispositivos acceden a Internet, es indispensable controlar, registrar y filtrar el tráfico para prevenir amenazas, mejorar el rendimiento de la red y garantizar el cumplimiento de políticas institucionales. En este contexto, los firewalls basados en Linux —especialmente soluciones robustas como Endian Firewall Community— representan herramientas confiables, flexibles y de acceso libre que permiten implementar mecanismos avanzados de gestión del tráfico. Entre ellos destaca el uso de proxies HTTP como elemento central para la supervisión, autenticación y regulación del acceso web.

La temática desarrollada en este trabajo se enfoca en la implementación de un proxy HTTP no transparente, configurado a través de Endian Firewall Community sobre una máquina virtual, igual que en los trabajos anteriores. Dicho proxy permite intervenir el tráfico web antes de que salga hacia Internet, exigiendo autenticación y aplicando reglas de filtrado basadas en políticas diseñadas por el administrador. Esta aproximación permite tener un mayor control sobre el comportamiento de los usuarios, ofreciendo trazabilidad, bloqueo selectivo de contenidos y reducción de riesgos asociados a malware y conexiones no deseadas. Además, la modalidad no transparente obliga al cliente a declarar explícitamente el uso del proxy, lo cual refuerza la supervisión del tráfico y evita el acceso no autorizado.

Para llevar a cabo la práctica, se configuró un laboratorio conformado por dos máquinas virtuales: un servidor con Ubuntu Server y otra máquina con Ubuntu Desktop, complementadas por la instalación y despliegue de Endian Firewall Community 3.3.2 como dispositivo de seguridad intermedio. Se abordaron procedimientos como la asignación de direcciones IP, la activación del servicio de proxy, la habilitación de mecanismos de autenticación local (NCSA) y la creación de políticas específicas para la gestión del acceso HTTP. Finalmente, se realizaron pruebas de conectividad y navegación desde el cliente para validar el correcto funcionamiento del sistema.

A través de esta implementación, el estudiante adquiere una comprensión profunda del funcionamiento del proxy, los servicios implicados, la importancia del filtrado web y la administración de políticas perimetrales. Este ejercicio práctico no solo fortalece las competencias técnicas en Linux y herramientas de firewall, sino que también prepara al estudiante para enfrentar escenarios reales de ciberseguridad en instituciones educativas y corporativas.

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

Para el desarrollo de esta temática, implementar un proxy HTTP (no transparente) con políticas de autenticación para navegación en Internet, se debe contar con tres máquinas: una con Ubuntu Desktop, otra con Ubuntu Server y la otra con Endian Community Firewall. El proceso de instalación de esta última se describe a continuación.

2.1. Descarga del ISO de Endian Community Firewall desde la web oficial

Ilustración 1. Descarga de Endian

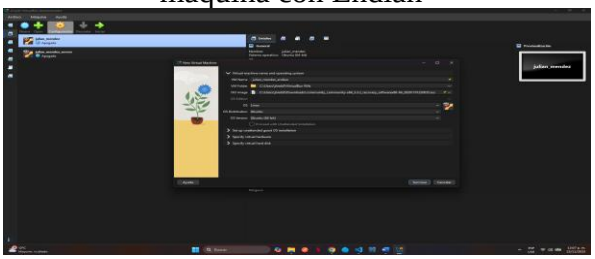
Fuente: Autoría Propia

2.2. Instalación de la máquina virtual

Aquí se deben seguir las instrucciones para la descarga sin mayor complicación, obtener el archivo .iso, y proceder a crear una nueva máquina virtual. Recordar que Endian funciona como un sistema operativo Linux propio.

El proceso de montaje debe realizarse de manera cuidadosa, vigilando que las cuotas para los recursos sean suficientes como para permitir su operación de manera fluida y natural. El programa de instalación de Endian es notablemente más ligero que el de Ubuntu, tanto en Desktop como en Server.

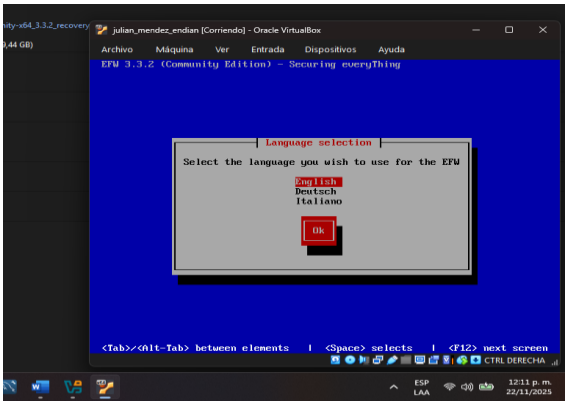
Ilustración 2. Configuración de nueva máquina con Endian



Fuente: Autoría Propia

Seleccionar el idioma de preferencia entre los tres de la lista.

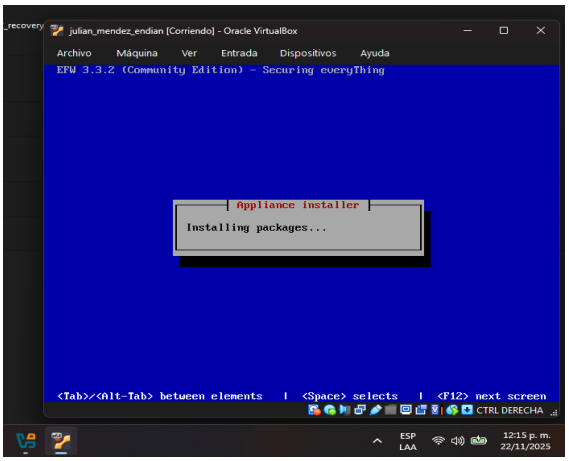
Ilustración 3. Selección de idioma de instalación



Fuente: Autoría Propia

El sistema informa de la instalación en curso.

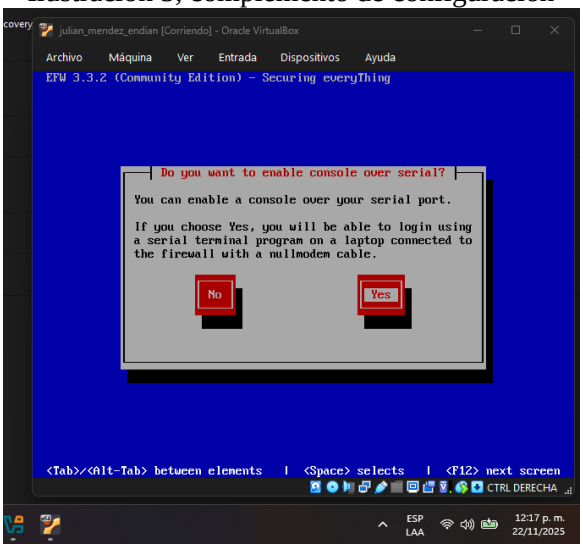
Ilustración 4. Instalando



Fuente: Autoría Propia

Seleccionar Sí en el paso siguiente. Esto facilita la configuración inicial.

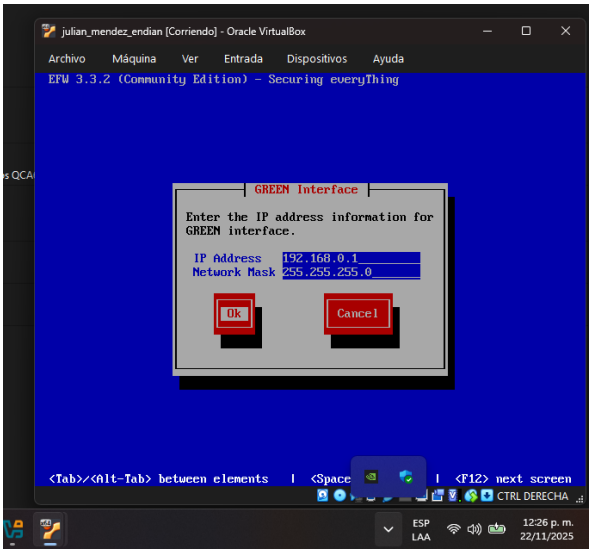
Ilustración 5, complemento de configuración



Fuente: Autoría Propia

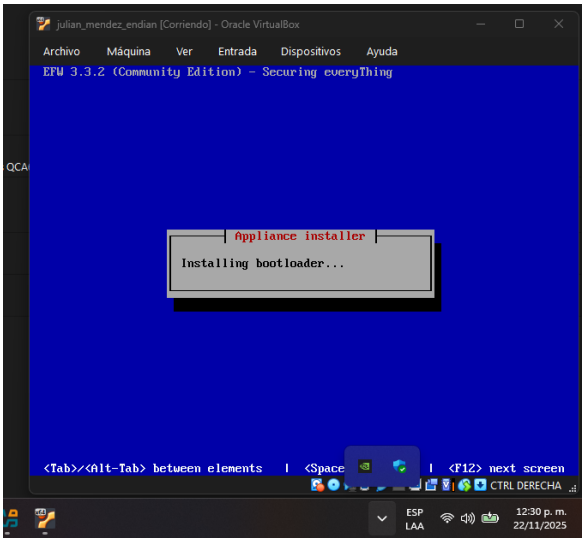
Aquí definimos la IP *192.168.0.1* para la interfaz verde

Ilustración 6. Asignación de IP para Green Interface



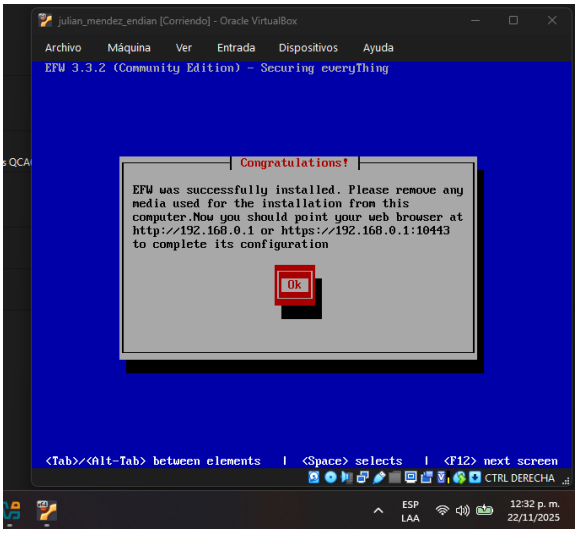
Fuente: Autoría Propia

Ilustración 7. Continuación de instalación



Fuente: Autoría Propia

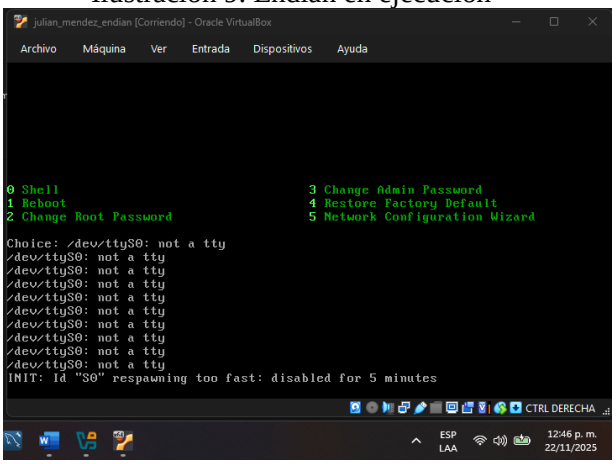
Ilustración 8. Instalación terminada



Fuente: Autoría Propia

Retirar la unidad óptica virtual (el .iso), y reiniciar la máquina para arrancar Endian. Si el programa de instalación es correcto, se verá una terminal como esta:

Ilustración 9. Endian en ejecución

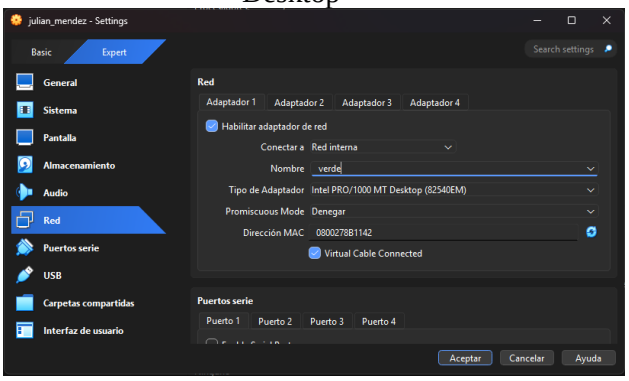


Fuente: Autoría Propia

2.3. Desarrollo de la Temática:

2.3.1. Verificar la configuración de red interna en las máquinas: en la máquina Desktop, debe verse algo como esto en su configuración de red:

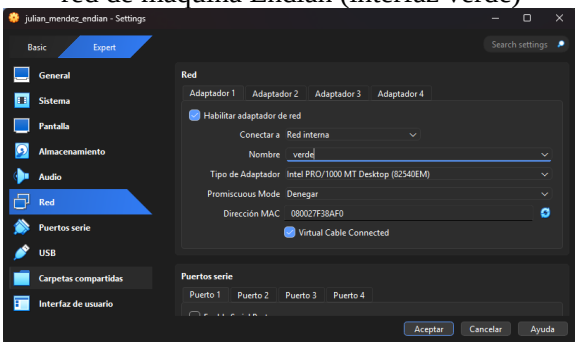
Ilustración 10. Parámetros de red de máquina Desktop



Fuente: Autoría Propia

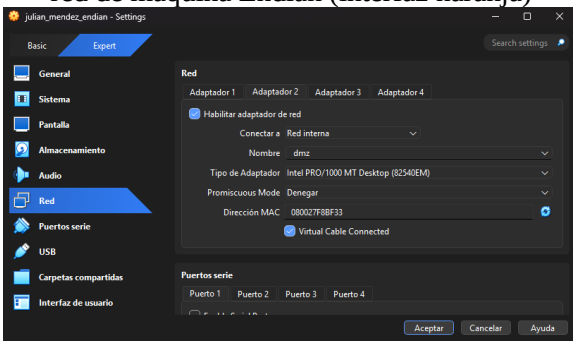
Tipo Red interna, llamada ‘verde’. Esa configuración funciona de manera global en la LAN que intenta montarse.

Ilustración 11. Parámetros de Adaptador 1 de red de máquina Endian (interfaz verde)



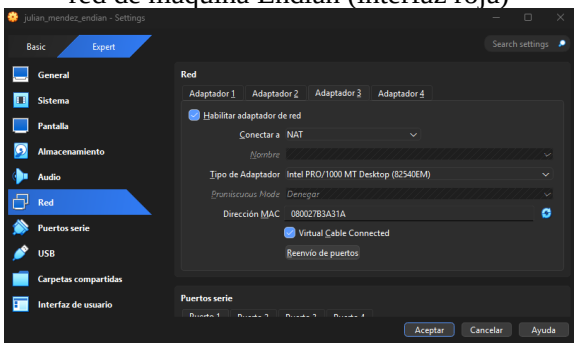
Fuente: Autoría Propia

Ilustración 12. Parámetros de Adaptador 2 de red de máquina Endian (interfaz naranja)



Fuente: Autoría Propia

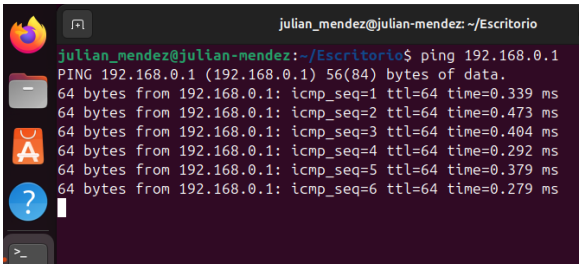
Ilustración 13. Parámetros de Adaptador 3 de red de máquina Endian (interfaz roja)



Fuente: Autoría Propia

Luego, verificar que Desktop se conecte con Endian. Puede usarse ping para esto.

Ilustración 14. Ping exitoso desde Desktop hacia Endian

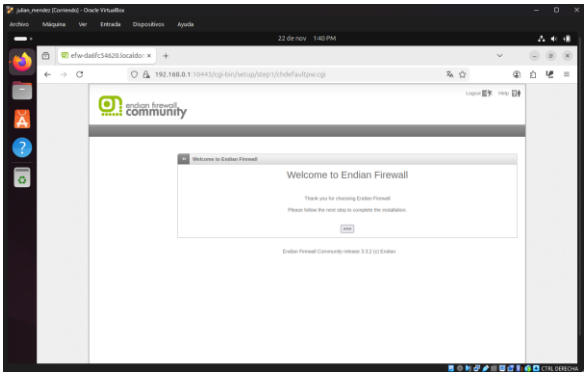


Fuente: Autoría Propia

2.3.2. Configuración de la red desde el panel web de Endian (en Desktop):

Abrir Firefox, o el navegador que tenga la máquina y acceder a la siguiente dirección: *https://192.168.0.1:10443*.

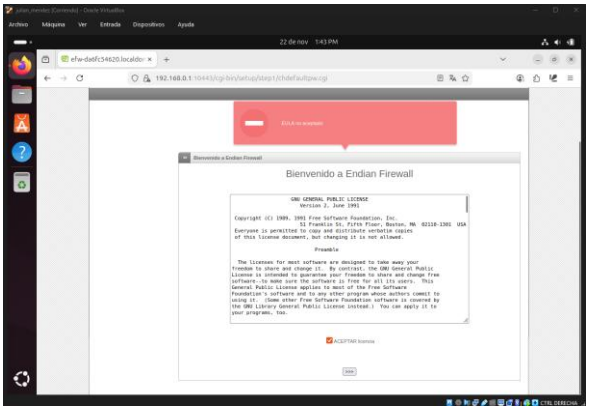
Ilustración 15. Vista general del panel web de Endian



Fuente: Autoría Propia

Seleccionar las opciones siguientes según las preferencias, y aceptar el acuerdo (en inglés).

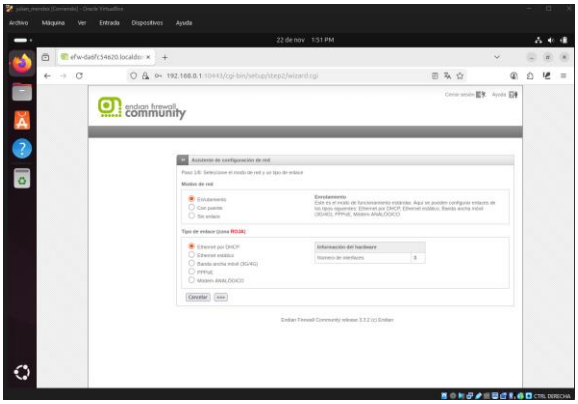
Ilustración 16. Acuerdo de uso de Endian



Fuente: Autoría Propia

Aparece el paso 1/8. Dejar como se ve en la imagen y pulsar sobre >>>

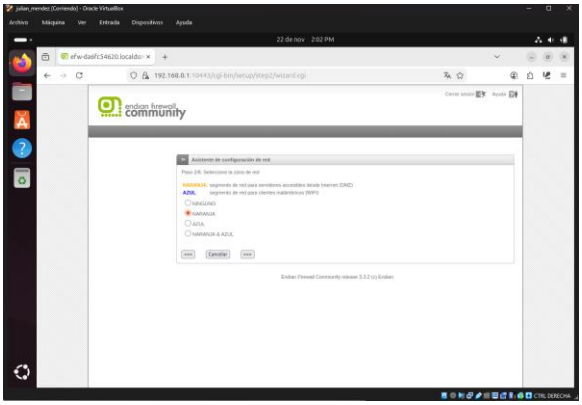
Ilustración 17. Paso 1/8



Fuente: Autoría Propia

Paso 2/8. Seleccionar NARANJA y continuar.

Ilustración 18. Paso 2/8



Fuente: Autoría Propia

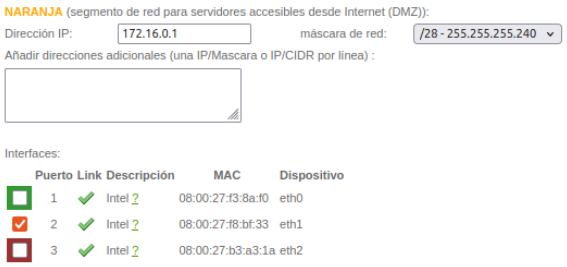
Paso 3/8. Preferencias de red. Configurar como se ve en las dos imágenes siguientes, y pulsar en >>> para continuar con el proceso.

Ilustración 19. Paso 3/8. Configuración para la red verde

Fuente: Autoría Propia

La red naranja necesita la siguiente configuración: máscara de red de rango más pequeño, porque así lo exige la Guía de Actividades. Asignar la IP de la imagen y esa máscara. Seleccionar la interfaz *eth1*.

Ilustración 20. Paso 3/8. Configuración para la red naranja

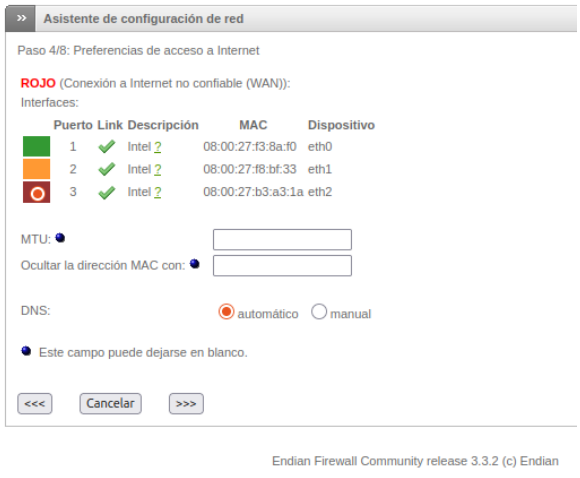


Fuente: Autoría Propia

Luego de esto, todo lo demás se deja igual, y continuar.

Paso 4/8. Preferencias de acceso a Internet. Si las configuraciones de red iniciales desde VirtualBox son correctas, sobre todo las del adaptador 3 de la máquina Endian, este paso se verá así. Solo hay que pulsar sobre >>> para continuar, sin tocar nada más:

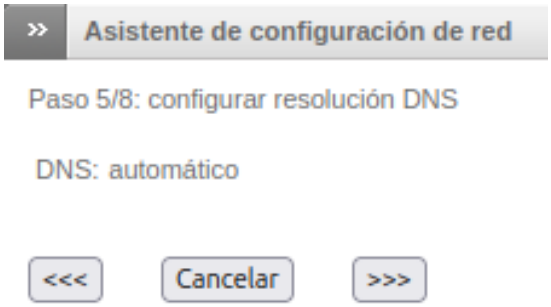
Ilustración 21. Paso 4/8



Fuente: Autoría Propia

Paso 5/8. Configurar resolución DNS. Este paso, si todo está bien configurado, aparece así:

Ilustración 22. Paso 5/8

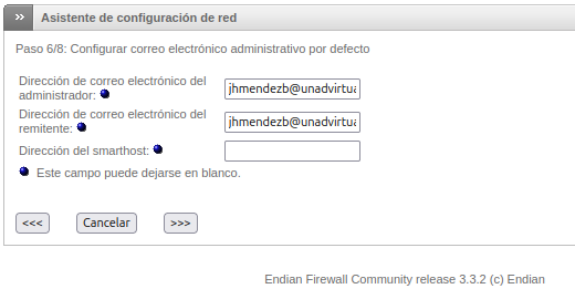


Fuente: Autoría Propia

Esto es así porque 1) la interfaz roja (*eth2*) está conectada a NAT desde VirtualBox; 2) VirtualBox asigna DNS al firewall de forma automática; y 3) Endian asume esos DNS de manera fluida. Solo queda continuar.

Paso 6/8. Configurar correo electrónico administrativo por defecto. Para efectos prácticos del desarrollo de la temática, esto se puede dejar vacío. Sin embargo, en el ejemplo se usa un correo institucional como prueba. Pulsar sobre >>> y continuar.

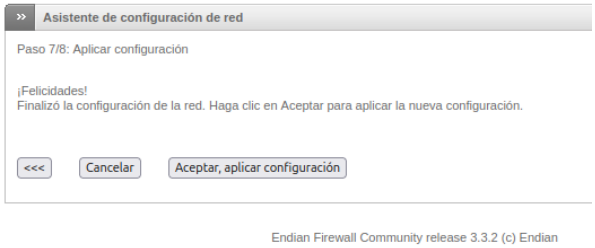
Ilustración 23. Paso 6/8



Fuente: Autoría Propia

Paso 7/8. Aplicar configuración. Para confirmar los parámetros definidos en el asistente, solo hay que pulsar sobre *Aceptar*, *aplicar configuración*.

Ilustración 24. Paso 7/8

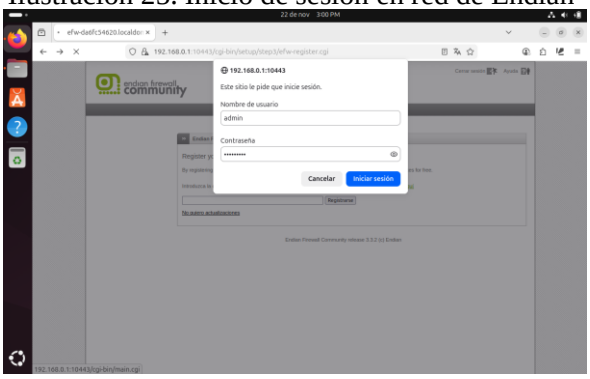


Fuente: Autoría Propia

Para acceder a la zona de administración de la nueva red de Endian, hay que volver a entrar por la URL *https://192.168.0.1:10443*. Lo más probable es que aparezca la pantalla de registro de Endian Firewall Community. Por ahora se puede saltar pulsando sobre *No recibir actualizaciones*.

A continuación, aparecerá un cuadro de diálogo del navegador para hacer login. Se ve así:

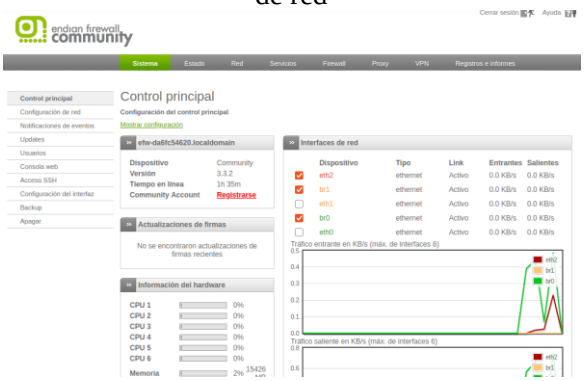
Ilustración 25. Inicio de sesión en red de Endian



Fuente: Autoría Propia

La contraseña es la creada durante el asistente de creación de la red, y el usuario es *admin*. La vista inicial del asistente se ve de manera similar a esta:

Ilustración 26. Vista principal de administración de red



Fuente: Autoría Propia

2.3.3. Activar el Proxy HTTP en modo No transparente. En el menú superior (fondo gris), hacer clic sobre Proxy. Luego, activar la opción Habilitar Proxy HTTP y 1) asegurar que la configuración para verde y naranja sea *no transparente*, 2) que el puerto que será usado sea el 8080. Lo demás se puede dejar como está, y la vista de estas opciones sería similar a esta:

Ilustración 27. Activación del Proxy no transparente

Fuente: Autoría Propia

Hacer clic en *Guardar*, y luego en *Aplicar*.

2.3.4. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:

- www.hotmail.com
- www.youtube.com
- www.elnuevodia.com.co

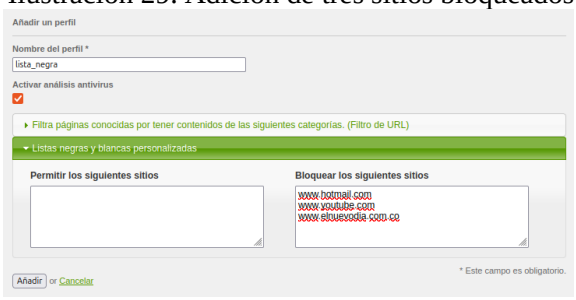
1) Ir a Proxy, 2) luego a HTTP, 3) luego a Filtrado web, y 4) hacer clic en *Añadir nuevo perfil*, así:

Ilustración 28. Secuencia de pasos para crear lista negra

Fuente: Autoría Propia

Ahora: asignar nombre al perfil, hacer clic sobre *Listas negra y blancas personalizadas* y, en los sitios a bloquear, completar el trabajo. Así debe verse:

Ilustración 29. Adición de tres sitios bloqueados



Fuente: Autoría Propia

Hacer clic en *Guardar* y luego en *Aplicar*.

5.3.5. 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.

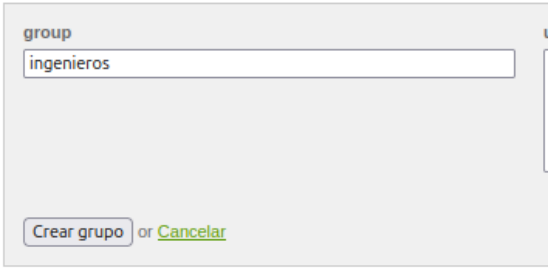
1) Ir a Proxy, 2) luego a HTTP, 3) luego a Autenticación, y 4) hacer clic en *administrar grupos*, así:

Ilustración 30. Secuencia de pasos para crear grupo

Fuente: Autoría Propia

Al pulsar sobre *Crear nuevo grupo*, asignarle nombre y pulsar sobre *Crear grupo*, y luego sobre *Aplicar*.

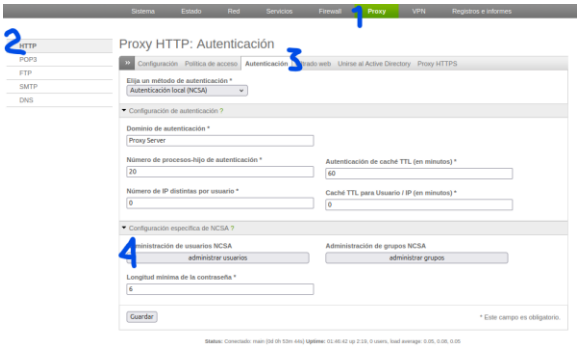
Ilustración 31. Muestra de grupo a punto de ser creado



Fuente: Autoría Propia

Luego, crear al usuario: 1) Proxy, 2) HTTP, 3) Autenticación, y 4) hacer clic en *administrar usuarios*, así:

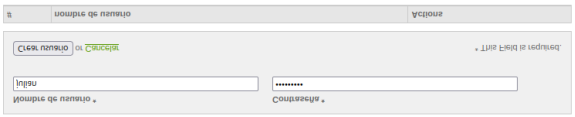
Ilustración 32. Secuencia de pasos para crear usuario



Fuente: Autoría Propia

Crear al usuario y asignarle contraseña:

Ilustración 33. Creación de nuevo usuario



Fuente: Autoría Propia

Al volver atrás/administrar grupos, y entrar al grupo *ingenieros*, se evidenciará que el usuario recién creado fue asignado automáticamente a ese grupo. Así se ve:

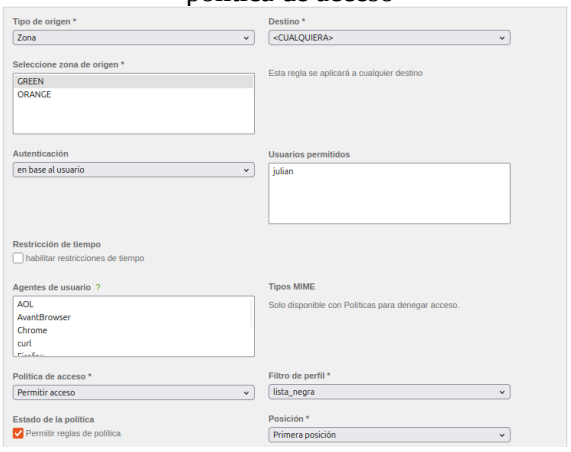
Ilustración 34. Usuario asignado automáticamente a grupo

Fuente: Autoría Propia

Ahora, sigue el establecimiento de la política de acceso: 1) Proxy, 2) HTTP, 3) luego a Política de acceso y 4) hacer clic en *Añadir política de acceso*.

Configurar de acuerdo con la siguiente imagen:

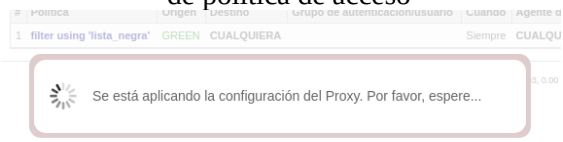
Ilustración 35. Parámetros de configuración de política de acceso



Fuente: Autoría Propia

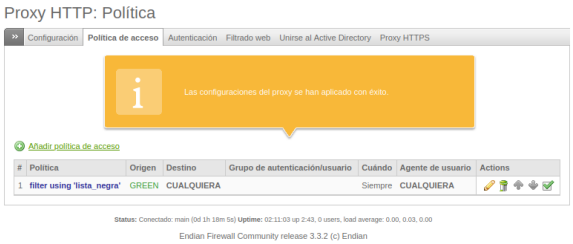
Guardar y Aplicar, como siempre. Aparecerá este mensaje:

Ilustración 36. Endian aplicando configuración de política de acceso



Fuente: Autoría Propia

Ilustración 37. Política de acceso creada exitosamente



Fuente: Autoría Propia

5.3.6. Configurar la máquina Desktop para funcionar bajo el proxy HTTP.

En la máquina Desktop, abrir el menú de configuración, luego ir a Red, luego a Proxy.

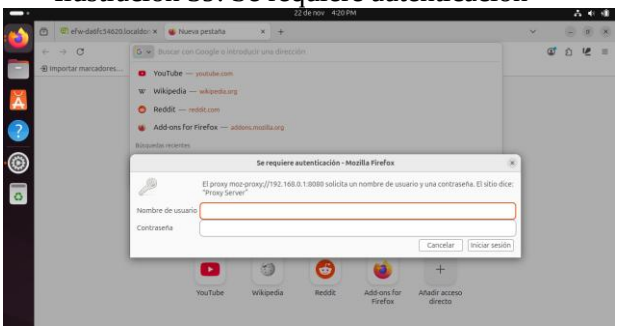
Luego activar la opción Proxy de la red, seleccionar *Manual* en Configuración, y colocar los valores definidos previamente en el desarrollo de la actividad. Así debe verse:

Ilustración 38. Asignando proxy a Ubuntu Desktop

Fuente: Autoría Propia

Al abrir una nueva pestaña, el navegador informa que se requiere autenticación, así:

Ilustración 39. Se requiere autenticación



Fuente: Autoría Propia

Finalmente, al intentar entrar a YouTube, se evidencia que el proxy deniega su acceso, devolviendo un error de tipo *timeout*, así:

Ilustración 40. Acceso denegado por lista negra en el proxy HTTP

Fuente: Autoría Propia

Link del video: https://youtu.be/gxAdllKOH7g

3. CONCLUSIONES

La configuración del proxy HTTP no transparente en Endian Firewall permitió comprobar cómo una herramienta de seguridad perimetral puede gestionar de manera centralizada el tráfico de una red, aplicando autenticación, filtrado y supervisión directa sobre las solicitudes web. El proceso de instalación, ajuste de interfaces, activación de servicios y creación de políticas confirmó la importancia de comprender la arquitectura interna de un firewall y su interacción con los equipos presentes en la red. Asimismo, las pruebas realizadas desde Ubuntu Desktop validaron la capacidad del sistema para controlar el acceso mediante reglas específicas, demostrando su relevancia para entornos corporativos.

Además, este ejercicio ha fortalecido competencias esenciales en administración de redes y diagnóstico de problemas relacionados. La experiencia permitió enfrentar escenarios reales donde es necesario gestionar permisos, reiniciar procesos y demás, interviniendo directamente desde una consola para mantener la operatividad del sistema. Se reafirma la utilidad del proxy como un recurso fundamental para garantizar seguridad, trazabilidad y cumplimiento de políticas dentro de una infraestructura tecnológica.

4. REFERENCIAS BIBLIOGRÁFICAS

- *LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware.* https://learning.lpi.org/es/learning-materials/101-500/101/101.1/
- *Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html*
- *Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html*
- Oracle (2020), Manual de usuario VirtualBox. VirtualBox. *https://www.virtualbox.org/manual/*
- Endian (2016), Endian UTM 3.2 Manual referencia. Endian. *http://docs.endian.com/3.2/utm/index.html*