DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL SEGMENTADA (LAN/DMZ/WAN) BASADA EN ENDIAN FIREWALL: VALIDACIÓN DE POLÍTICAS DE ACCESO Y CONTROL DE CONTENIDO EN ENTORNOS GNU/LINUX.

EDINSON FERNEY SOSCUE MUÑOZ
e-mail: efsoscuem@unadvirtual.edu.co

RESUMEN: *Este estudio presenta la construcción y evaluación de una arquitectura de seguridad perimetral segmentada (WAN, LAN y DMZ) mediante el uso de Endian Firewall (EFW), una herramienta de código abierto basada en GNU/Linux. El objetivo fue determinar la efectividad de EFW en la aplicación de políticas de seguridad. Para ello, se configuró NAT para el acceso externo, se establecieron reglas de filtrado entre zonas para reducir riesgos y se incorporó un Proxy HTTP para gestionar el contenido web. Los resultados evidencian que el modelo proporciona un control sólido de protocolos (como bloquear ICMP o permitir HTTP/FTP) y restringe adecuadamente sitios web a partir de perfiles definidos. Esto confirma que las soluciones libres pueden utilizarse exitosamente para el fortalecimiento de la seguridad perimetral.*

PALABRAS CLAVE: Endian, firewall Open Source, seguridad perimetral, DMZ, políticas NAT, filtrado de tráfico, proxy en GNU/Linux..

1 INTRODUCCIÓN

En el contexto tecnológico actual, marcado por una creciente interconexión digital y un volumen cada vez mayor de intercambio de datos, la seguridad perimetral se ha convertido en un componente esencial para garantizar la continuidad operativa de cualquier organización. La evolución constante de las amenazas cibernéticas demanda soluciones capaces no solo de bloquear accesos no autorizados, sino también de gestionar y segmentar eficientemente los flujos de información dentro de la infraestructura de red. En este sentido, mantener una arquitectura de red plana y sin segmentación incrementa significativamente la superficie de ataque, ya que una vulneración en un único punto puede comprometer la totalidad del entorno corporativo.

Ante esta realidad, el uso de sistemas operativos basados en GNU/Linux como plataforma para la infraestructura de seguridad ha adquirido un papel destacado, dada su estabilidad, flexibilidad y naturaleza de código abierto. En este escenario, Endian Firewall (EFW) se consolida como una solución Unified Threat Management (UTM) que permite definir políticas avanzadas de control de acceso y establecer segmentación mediante zonas lógicas como WAN, LAN y DMZ. Este trabajo se enmarca en los principios de la seguridad en entornos Open Source, aplicando técnicas de hardening mediante la configuración detallada de reglas de firewall y servicios complementarios.

En consecuencia, el propósito central de este artículo es diseñar, implementar y validar una arquitectura de seguridad perimetral segmentada utilizando Endian Firewall en un entorno virtualizado. En particular, se busca evaluar su efectividad en tres componentes fundamentales: (1) la correcta aplicación de la Traducción de Direcciones de Red (NAT), (2) la creación de reglas de filtrado capaces de permitir o restringir protocolos específicos según la zona, y (3) la implementación de un Proxy HTTP con control de contenido y autenticación de usuarios. Los resultados obtenidos demuestran no solo la funcionalidad de la solución propuesta, sino también la pertinencia de emplear herramientas de software libre para fortalecer la seguridad de redes corporativas, contribuyendo así al conocimiento práctico en administración de redes y mitigación de riesgos.

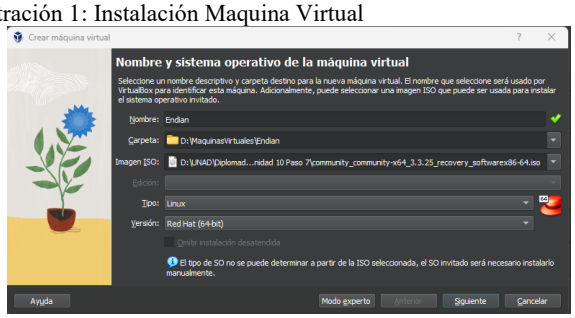
Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Producto esperado:
1. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:
www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

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.
3. Probar desde la LAN a través de un navegador Web, el acceso a los
portales referenciados en la lista negra.

Desarrollo actividad
Para realizar la actividad es necesario instalar la distribución de Linux llamada Endian, la cual maneja diversas herramientas para la ciberseguridad, enrutamiento, cortafuegos, servidor proxy entre otros.
Inicialmente creamos los parámetros que va a llevar la máquina virtual, que es el nombre la carpeta, ubicación de la ISO, que tipo de sistema operativo vamos a usar y la versión en la cual se basa, para nuestro caso es Red Hat(64-bit).

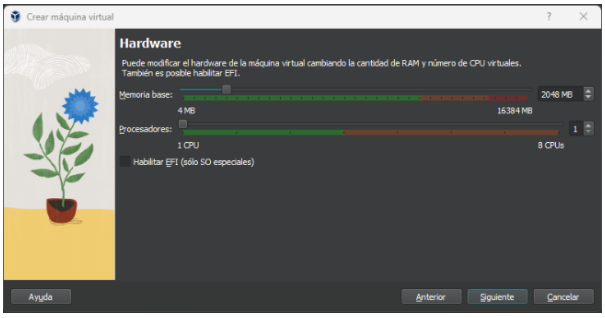
Ilustración 1: Instalación Maquina Virtual



Fuente: Autoría Propia

Seguimos con los parámetros de memoria y procesadores

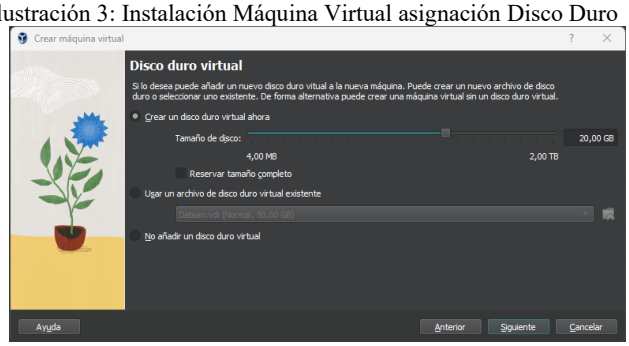
Ilustración 2: Instalación Máquina Virtual asignación Memoria RAM



Fuente: Autoría Propia

Le asignamos una parte del disco duro.

Ilustración 3: Instalación Máquina Virtual asignación Disco Duro



Fuente: Autoría Propia

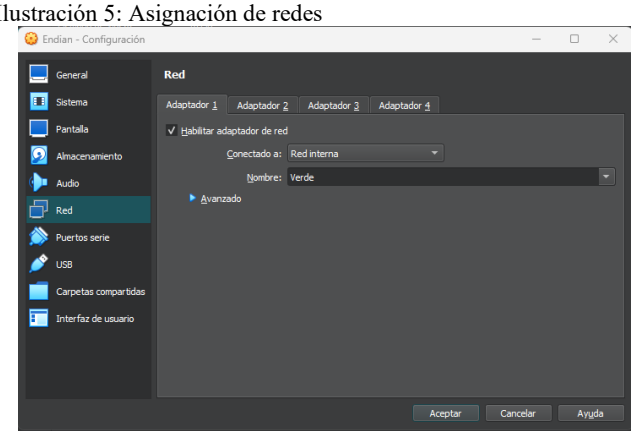
El VirtuaBox nos presenta un resumen de los parámetros seleccionados.

Ilustración 4: Finalización Maquina virtual

Fuente: Autoría Propia

Tenemos que tener muy claro que se van a establecer 3 conexiones de red para el Endian, las cuales de deben habilitar y discriminar con los nombres verde y naranja.
El primer adaptador se parametriza tipo red interna y se le asigna el nombre de verde, este será el encargado de administrar la red interna de los hosts tipo cliente.

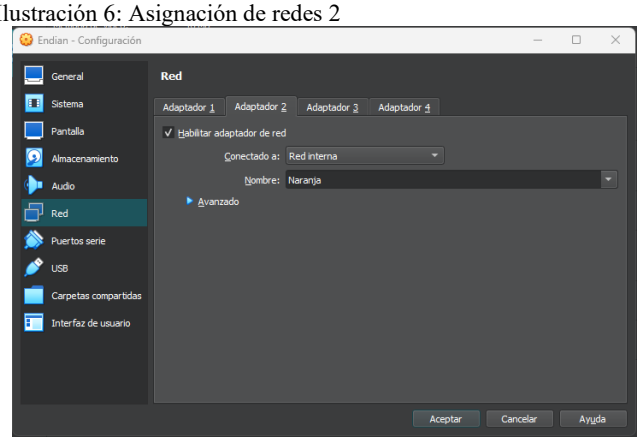
Ilustración 5: Asignación de redes



Fuente: Autoría Propia

El segundo adaptador se parametriza tipo red interna y se le asigna el nombre de naranja, este será el encargado de administrar la red interna de los hosts tipo servidor. (para esta actividad no se utilizará)

Ilustración 6: Asignación de redes 2



Fuente: Autoría Propia

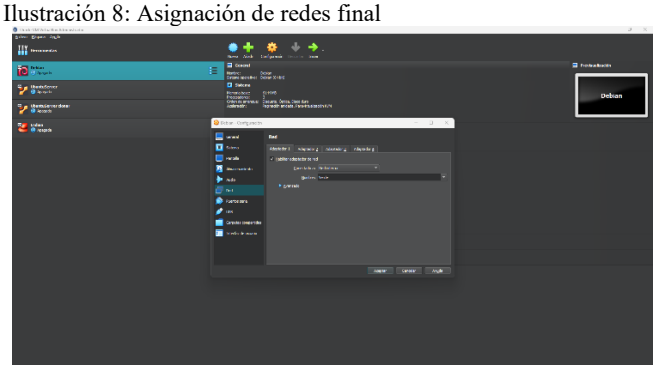
El tercer adaptador se parametriza tipo NAT y por default no se le asigna nombre, este será el encargado de administrar el internet.

Ilustración 7: Asignación de redes 3

Fuente: Autoría Propia

Luego de configurar los parámetros del Endian, nos dirigimos a una de las máquinas virtuales que se utilizaron en otras actividades y ajustamos el parámetro del adaptador para sea red interna y seleccionamos verde (el que se creó previamente)

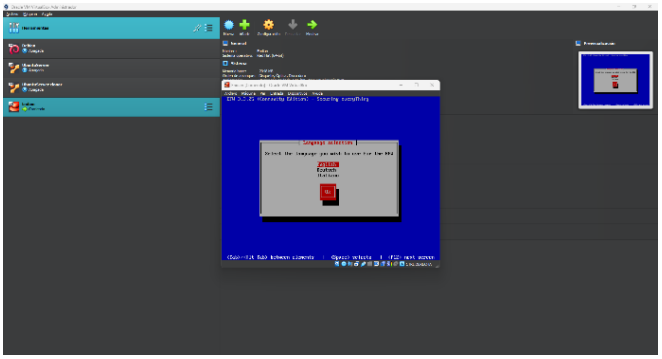
Ilustración 8: Asignación de redes final



Fuente: Autoría Propia

En este momento iniciamos la instalación del Endian, se empieza eligiendo el idioma.

Ilustración 9: Instalación ENDIAN



Fuente: Autoría Propia

El sistema da la bienvenida, con las flechas de dirección nos posicionamos en ok y presionamos enter.

Ilustración 10: Instalación ENDIAN parte 2

Fuente: Autoría Propia.

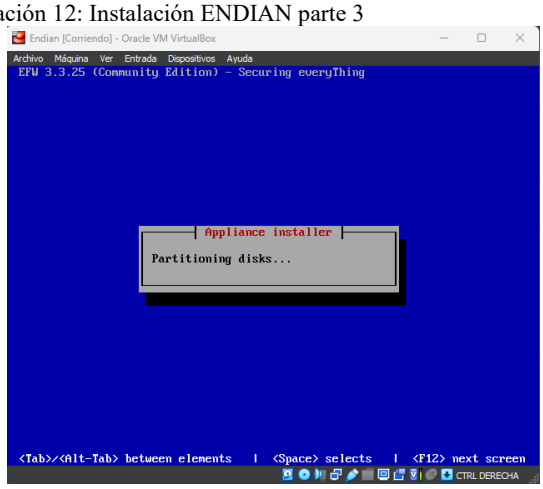
En el siguiente menú, el sistema nos indica que si deseamos continuar todos los datos en el disco se perderán. Seleccionamos YES

Ilustración 11: Instalación ENDIAN parte 3

Fuente: Autoría Propia

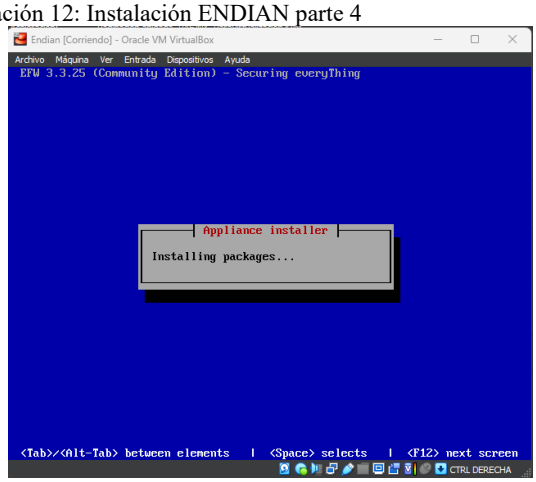
El sistema inmediatamente empieza a particionar el disco e instalaciones de paquetes.

Ilustración 12: Instalación ENDIAN parte 3



Fuente: Autoría Propia

Ilustración 12: Instalación ENDIAN parte 4



Fuente: Autoría Propia.

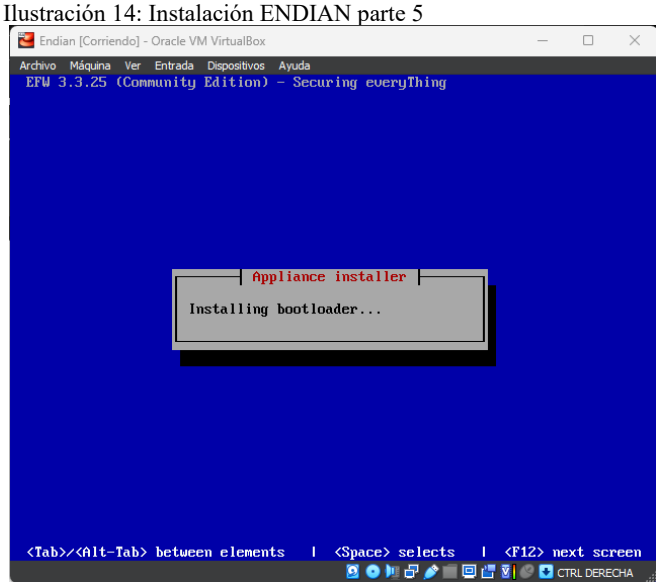
El paso siguiente es ingresar la dirección ip a la GREEN interface , para este caso se utiliza la dirección ip 192.168.2.15 /24

Ilustración 13: Instalación ENDIAN parte 5 Asignación de IP

Fuente: Autoría Propia

Luego continua con la instalación del bootloader

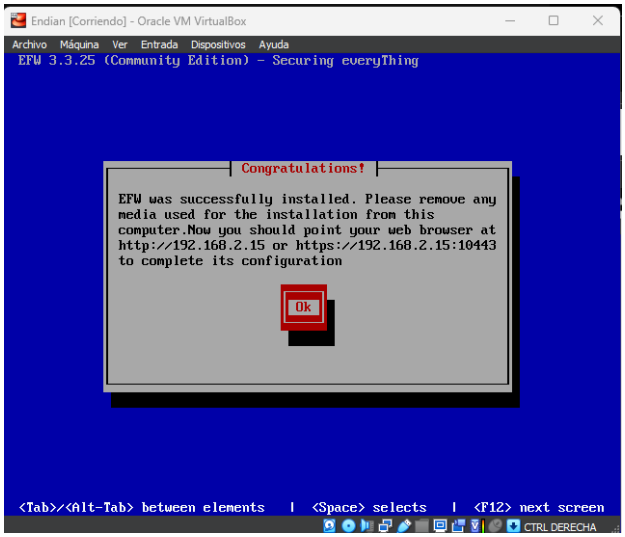
Ilustración 14: Instalación ENDIAN parte 5



Fuente: Autoría Propia

Cuando se termine la instalación nos saldrá el siguiente mensaje, el cual nos dará los datos de acceso al Endian via web.

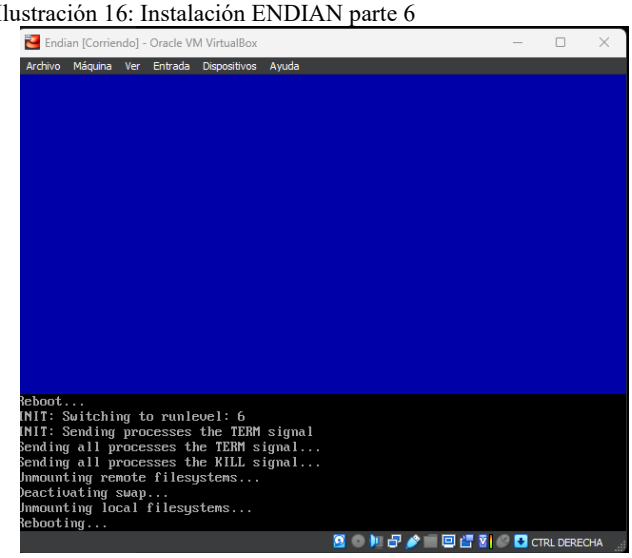
Ilustración 15: Instalación ENDIAN parte 6 afirmación de asignación de IP



Fuente: Autoría Propia.

Después de presionar OK, el sistema se reiniciara para iniciar con todos los servicios correspondientes

Ilustración 16: Instalación ENDIAN parte 6



Fuente: Autoría Propia

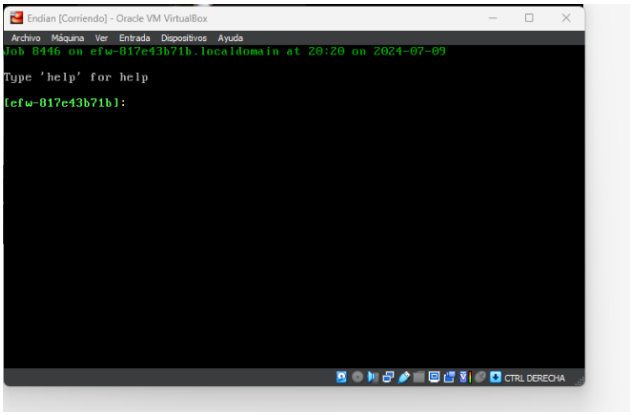
Cuando inicia la maquina nos muestra los datos que podemos apreciar en la siguiente imagen , con un menú que va del 0 al 5 . en estos casos el servicio ya esta corriendo y es necesario su configuración. La clave del root por default es Endian.

Ilustración 17: Configuración ENDIAN 1

Fuente: Autoría Propia.

Seleccionamos 0 y en este momento ingresamos a una terminal igual a cualquier distribución de Linux y el nombre por defecto del firewall es **efw-817e43b71b** aca en este paso ya se pueden utilizar los comandos normalmente.

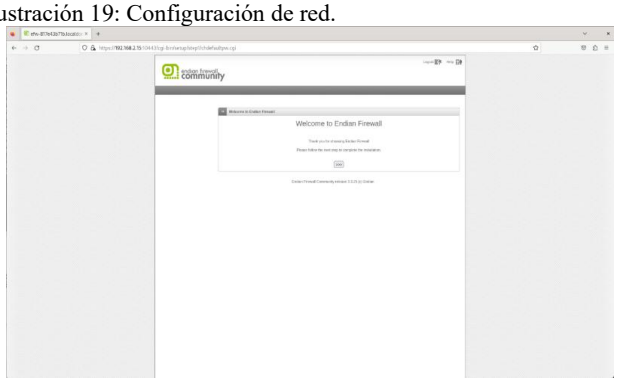
Ilustración 18: cambio de contraseña 1



Fuente: Autoría Propia.

Luego de dejar funcionando el Endian , el paso que sigue es ingresar a la maquina que se tiene con debían , en la cual se hace un testeo para validar si esta en el mismo segmento de red que el interfaz verde. Posterior a validar la conectividad entre debian y Endian nos dirigimos al navegador web de debian e iniciamos la configuración.

Ilustración 19: Configuración de red.



Fuente: Autoría Propia.

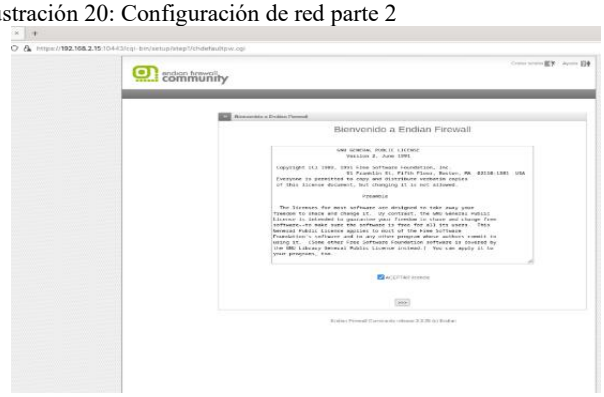
Lo primero es elegir el idioma y la zona horaria.

Ilustración 19: Configuración de red.

Fuente: Autoría Propia

Luego se aceptan los acuerdos de la licencia.

Ilustración 20: Configuración de red parte 2



Fuente: Autoría Propia.

En caso de contar con un respaldo de la configuración, en este momento se podría cargar. Como nuestro firewall es nuevo seleccionamos NO.

Ilustración 21: Configuración de red parte 3

Fuente: Autoría Propia.

En la siguiente parte se establecen las contraseñas para el acceso web y ssh.

Ilustración 22: Configuración de red parte 3

Fuente: Autoría Propia

En el paso 1 de la configuración nos permite cambiar el tipo de enlace y el modo de red , para efectos del ejercicio lo dejamos con los datos por default.

Ilustración 23: Configuración de red parte 4

Fuente: Autoría Propia.

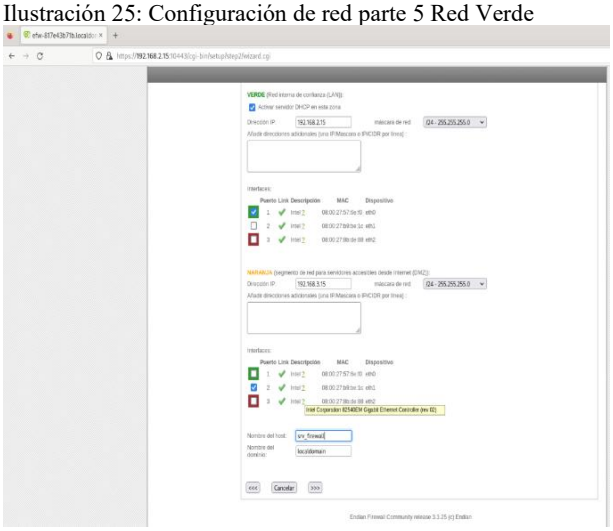
El paso 2 nos permite configurar las zonas de red, vamos a seleccionar NARANJA, aunque para este ejercicio no utilizaremos esta zona.

Ilustración 24: Configuración de red parte 5 Red Naranja

Fuente: Autoría Propia

Creamos el segmento de red naranja y le asignamos la dirección ip 192.168.3.15 /24 . este se usará en caso tal de ingresar servidores.
También asignamos a que interfaz pertenece el segmento recién creado, en este caso a la interface 2.
Y por último le cambiamos el nombre del equipo en nuestro caso le ponemos el nombre srv_firewall

Ilustración 25: Configuración de red parte 5 Red Verde



Fuente: Autoría Propia

El paso siguiente nos enseña el interfaz que proporciona acceso a internet, en este caso es el tercer interfaz el que se estableció como NAT

Ilustración 26: Configuración de red parte 5 Azul

Fuente: Autoría Propia

El paso 5 consiste en la configuración de los DNS, para este ejercicio se deja con la configuración por default.

Ilustración 27: Configuración de red parte 5 Finalización

Fuente: Autoría Propia.

El paso 6 consiste en configurar un correo electrónico para la administración de la plataforma, el cual tampoco es necesario para este ejercicio.

Ilustración 28: Configuración de red parte 6

Fuente: Autoría Propia.

El paso 7 es la aceptación de todos los ajustes realizados, en este caso presionamos Aceptar, aplicar configuración.

Ilustración 29: Configuración de red en seguridad.

Fuente: Autoría Propia

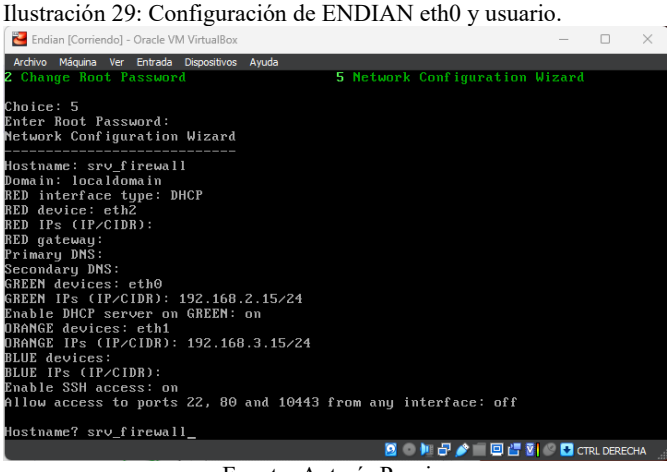
El paso 8 es el mensaje de final informando que se realizaron todos los ajustes.

Ilustración 29: Configuración de red en seguridad parte 2.

Fuente: Autoría Propia

Podriamos validar todos los ajustes desde la consola del endian , escogiendo la opcion 5.

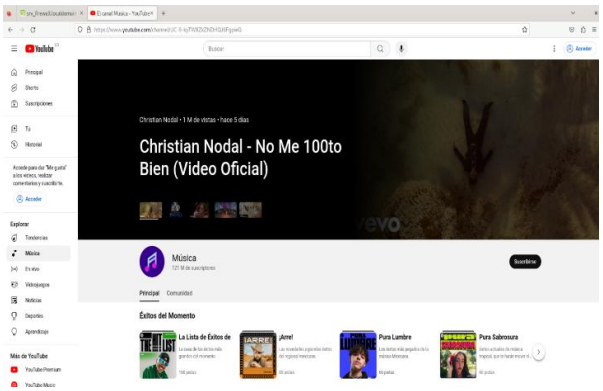
Ilustración 29: Configuración de ENDIAN eth0 y usuario.



Fuente: Autoría Propia

Validamos que el host Debian conectado a la red verde , tenga navegación antes de hacer los ajustes.

Ilustración 30: Prueba de configuración.



Fuente: Autoría Propia.

Luego ingresamos de nuevo a la administración web del Endian y el primer paso es habilitar la opción de Proxy , tal como se ve en la imagen.

Ilustración 31: Prueba de configuración y servicio

Fuente: Autoría Propia

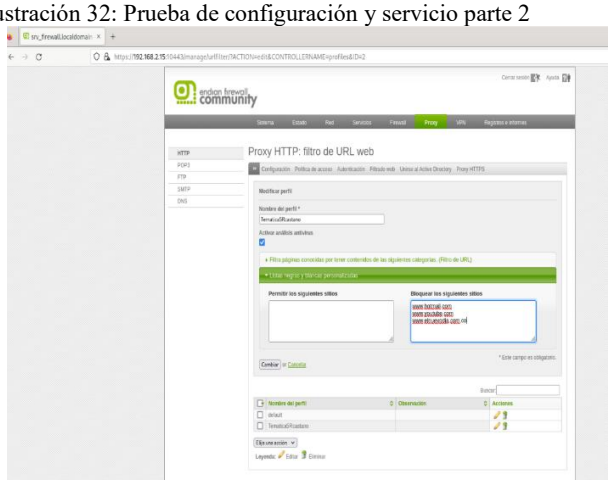
El paso siguiente es crear un perfil, para eso nos vamos al apartado Proxy y seleccionamos Añadir nuevo perfil.

Ilustración 31: Prueba de configuración y servicio

Fuente: Autoría Propia

Luego en esta parte le creamos un nombre, para este caso se digito tematica5rcastano y adicional a eso se le agregaron 3 páginas web a las listas negras (Hotmail, YouTube, elnuevodia) por último guardamos el perfil.

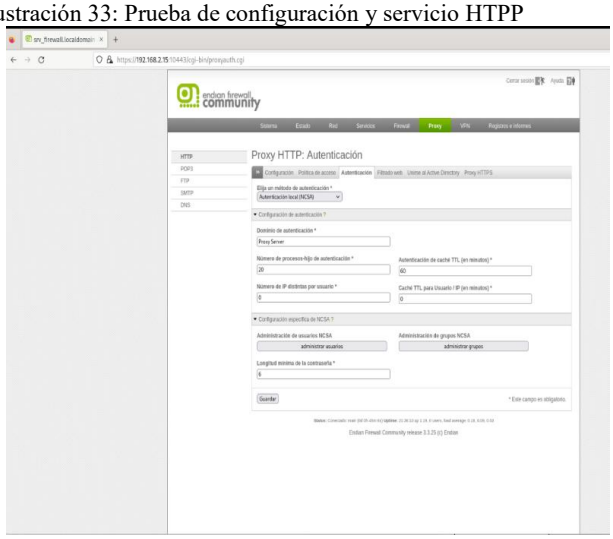
Ilustración 32: Prueba de configuración y servicio parte 2



Fuente: Autoría Propia.

El siguiente paso consiste en crear el usuario, para eso nos dirigimos a la opción de autenticación y elegimos como método la **Autenticación local (NCSA)** y seleccionamos administrar usuarios.

Ilustración 33: Prueba de configuración y servicio HTPP



Fuente: Autoría Propia.

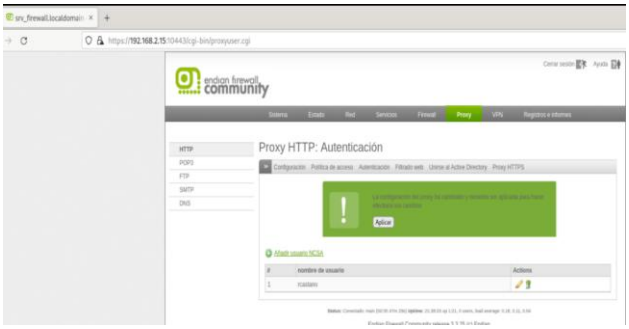
En el siguiente formulario, seleccionamos Añadir Usuario NCSA y creamos un usuario y contraseña, finalmente presionamos crear usuario.

Ilustración 33: Prueba de configuración y servicio HTPP

Fuente: Autoría Propia

Aplicamos los cambios y el usuario se crearía sin problemas.

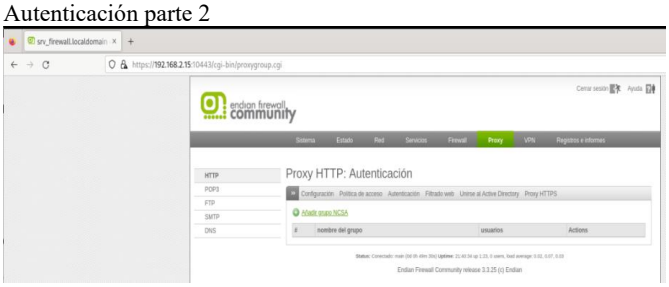
Ilustración 34: Prueba de configuración y servicio HTPP Autenticación



Fuente: Autoría Propia

Por este mismo lado de autenticación se pueden crear los grupos , y el proceso es prácticamente el mismo pero en vez de seleccionar administrar usuarios , seleccionamos administrar equipos y en los menús que presenta elegimos añadir grupo NCSA

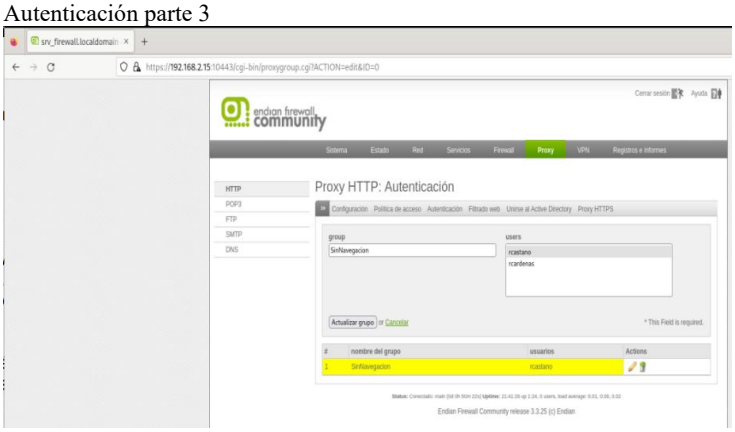
Ilustración 35: Prueba de configuración y servicio HTPP Autenticación parte 2



Fuente: Autoría Propia

Creamos un grupo, para efectos de esta practica creamos uno con el nombre SinNavegacion y agregamos al usuario previamente creado rcastano.

Ilustración 36: Prueba de configuración y servicio HTPP Autenticación parte 3



Fuente: Autoría Propia.

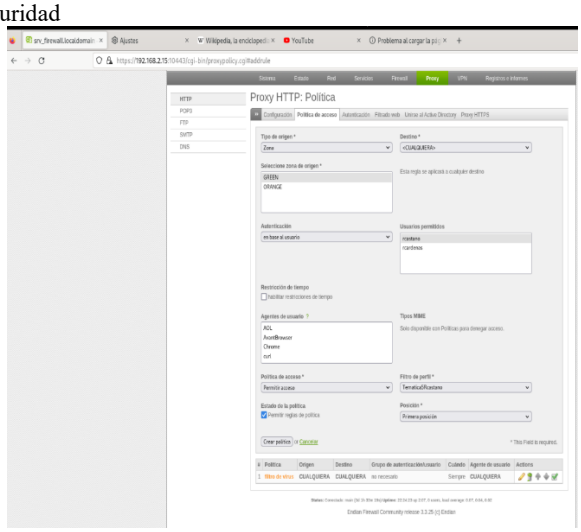
Aplicamos los cambios y continuamos.

Ilustración 36: Prueba de configuración y servicio HTPP Autenticación parte 4

Fuente: Autoría Propia

Ahora lo que corresponde es crear una política de navegación, para ello elegimos la zona, esto corresponde a cuáles de las zonas aplica la política, en nuestro caso aplicara a la zona **GREEN** en la cual están todos los hosts tipo cliente.
Luego elegimos el destino, para este ejemplo elegimos **cualquiera**, esto con el fin que aplique también para la zona roja a la cual corresponde el internet.
En autenticación seleccionamos en base a usuario y seleccionamos un usuario de la lista de la derecha, para este caso elegimos **rcastano**, el que se creó para el ejercicio.
La política de acceso se elige **permitir acceso**,
Filtro de perfil elegimos el filtro creado **Tematica5Rcastano**
Estado de la política, seleccionamos **Permitir reglas de políticas**
Posición, seleccionamos **primera posición** (esto asigna prioridad sobre otras reglas)
El ultimo paso es seleccionar **crear política** , con esto la política esta creada.

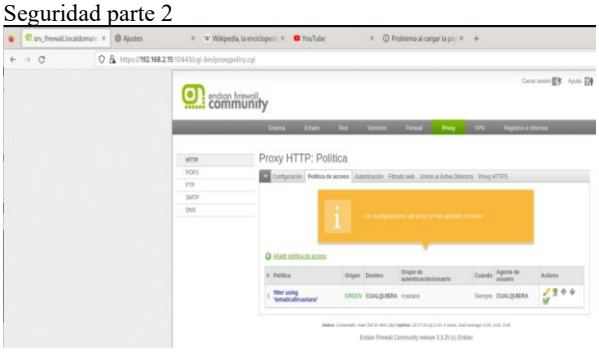
Ilustración 37: Prueba de configuración y servicio HTPP Política de Seguridad



Fuente: Autoría Propia.

Luego de aplicar los cambios, podemos ver la política debidamente creada.

Ilustración 38: Prueba de configuración y servicio HTPP Política de Seguridad parte 2



Fuente: Autoría propia

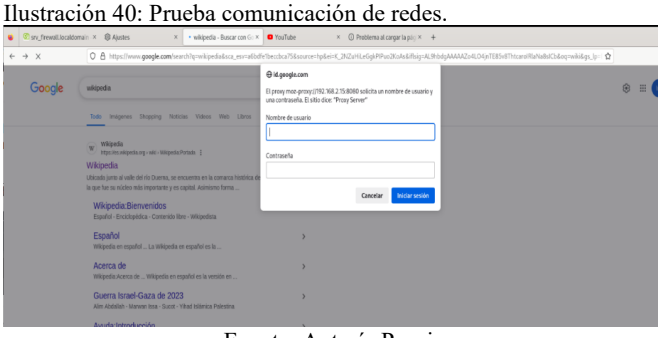
El paso a seguir es configurar nuestro host cliente para que se entienda con el proxy, para ello en los ajustes del navegador nos vamos y establecemos los datos de nuestro proxy.

Ilustración 39: Prueba de configuración de comunicación

Fuente: Autoría Propia

Inmediatamente se guardan los cambios, al tratar de navegar en cualquier página nuestro navegador nos pedirá un usuario y una contraseña para validar el perfil

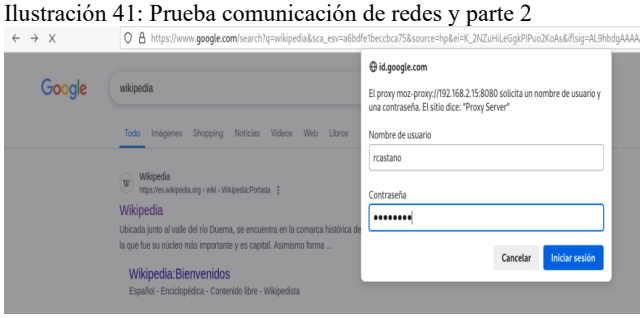
Ilustración 40: Prueba comunicación de redes.



Fuente: Autoría Propia

Ingresamos el usuario creado para el ejercicio e inmediatamente carga la búsqueda en Google.

Ilustración 41: Prueba comunicación de redes y parte 2



Fuente: Autoría Propia

También se carga la página de Netflix sin ningún problema

Ilustración 42: Prueba comunicación de redes y parte 3

Fuente: Autoría Propia

Pero si tratamos de acceder a las paginas registradas en la lista negra , la navegación no es posible , ejemplo youtube.com

Ilustración 43: Prueba comunicación de redes y parte 3 youtube

Fuente: Autoría Propia

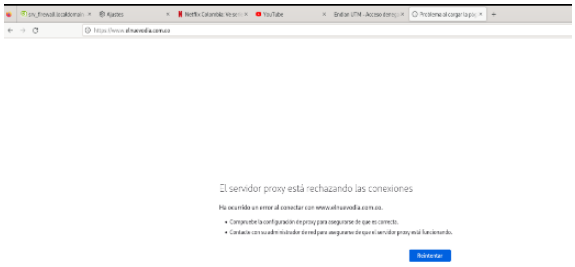
Ejemplo Hotmail.com

Ilustración 43: Prueba comunicación de redes y parte 4 El Nuevodia

Fuente: Autoría Propia

Ejemplo elnuevodia.com.co

Ilustración 44: Prueba Final



Fuente: Autoría Propia

4 CONCLUSIONES

Durante el desarrollo de la práctica se fortalecieron de manera significativa las competencias en seguridad perimetral mediante la implementación del firewall Endian y la configuración de servicios fundamentales dentro de una arquitectura de red segmentada. La actividad permitió consolidar habilidades en diseño, administración y protección de infraestructuras corporativas en entornos virtualizados, favoreciendo una comprensión integral del funcionamiento de un perímetro seguro.

Se logró comprender y aplicar correctamente el esquema de zonas de seguridad (LAN, WAN y DMZ), verificando la adecuada configuración de interfaces, direccionamiento IP y servicios esenciales. Esto permitió afianzar los fundamentos operativos del firewall y su rol como elemento central en la defensa de la red.

Asimismo, se configuraron reglas de NAT para habilitar el tráfico de entrada y salida entre las distintas zonas, comprobando el funcionamiento adecuado de la traducción de direcciones y la creación automática de reglas asociadas. Este proceso hizo posible entender de forma práctica cómo se gestionan flujos externos e internos dentro de un perímetro corporativo.

De igual manera, se implementaron políticas de acceso específicas que permitieron habilitar servicios como HTTP y FTP desde la DMZ, además de la restricción del protocolo ICMP. Estas configuraciones evidenciaron la importancia del control granular del tráfico para preservar la integridad, disponibilidad y confidencialidad de los recursos.

Finalmente, se evaluó la comunicación controlada entre zonas internas y externas, analizando el comportamiento del tráfico permitido y bloqueado. Esto permitió reafirmar la relevancia de diseñar políticas de seguridad coherentes con las necesidades de la organización, garantizando un flujo seguro de información y reduciendo la superficie de exposición ante posibles amenazas.

5 REFERENCIAS

[1] Endian Team. (s.f.). Endian Firewall Community (Versión 3.3.2) [Software de código abierto]. SourceForge. https://sourceforge.net/projects/efw/

[2] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Upper Saddle River, NJ, USA: Pearson, 2020.

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

hardware. Linux Professional Institute. Recuperado de https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

Oracle. (2020). Manual de usuario VirtualBox. VirtualBox. Recuperado de https://www.virtualbox.org/manual