IMPLEMENTACIÓN DE UN PROXY HTTP NO TRANSPARENTE CON POLÍTICAS DE AUTENTICACIÓN DENTRO DE GNU/LINUX ENDIAN

Juan Camilo Carvajal Gallego
e-mail: juancamilocarvajalgallego6@gmail.com

RESUMEN: *La seguridad perimetral en las organizaciones es fundamental para proteger la información y la infraestructura tecnológica. En este trabajo se implementó un Proxy HTTP no transparente con políticas de autenticación utilizando GNU/Linux Endian Firewall Community como plataforma principal de seguridad. La solución permitió controlar la navegación de los usuarios desde la red LAN hacia Internet mediante autenticación, creación de perfiles y aplicación de listas negras para restringir el acceso a sitios web no autorizados. La infraestructura fue diseñada en VirtualBox utilizando máquinas virtuales Ubuntu Desktop, Ubuntu Server y Endian Firewall, distribuidas en las zonas GREEN, RED y ORANGE. Los resultados obtenidos permitieron fortalecer la seguridad perimetral y mejorar el control de acceso a Internet mediante políticas de filtrado y administración del tráfico de red.*

PALABRAS CLAVE: Proxy HTTP, Endian, Firewall, GNU/Linux.

1 INTRODUCCIÓN

La seguridad perimetral constituye uno de los elementos más importantes dentro de la administración de redes empresariales, debido a que permite controlar el acceso entre redes internas y externas, reduciendo riesgos relacionados con accesos no autorizados y amenazas informáticas. La implementación de firewalls con servicios proxy permite establecer políticas de navegación, autenticación de usuarios y filtrado web, fortaleciendo la protección de la información y mejorando la gestión del tráfico de red.

GNU/Linux Endian Firewall Community es una distribución orientada a la seguridad perimetral que incorpora herramientas como firewall, proxy HTTP y filtrado web. Además, permite segmentar la red en diferentes zonas, tales como GREEN (LAN), RED (Internet) y ORANGE (DMZ), facilitando la administración y el aislamiento de servicios. En este trabajo se implementó un Proxy HTTP no transparente con autenticación de usuarios, listas negras y políticas de acceso, con el objetivo de restringir la navegación hacia determinados sitios web y fortalecer la seguridad de la red local.

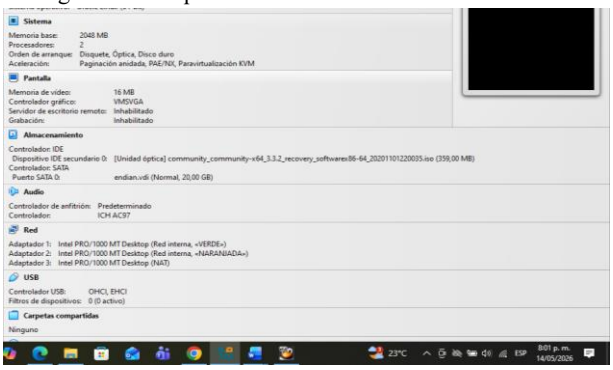
2 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Para el desarrollo de esta actividad se utilizó la máquina Virtual Box, en donde se usó 3 máquinas virtuales, las cuales son Ubuntu Desktop, Ubuntu Server y GNU/Linux Endian Firewall Community que es la herramienta principal para la seguridad perimetral. La red fue segmentada en tres zonas, la primera fue zona verde que corresponde a la red interna LAN, posterior fue la zona roja a través de la configuración DHCP y por último la zona naranja correspondiente a la DMZ.

2.1 CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES

Se sigue minuciosamente las instrucciones para instalar cada una de las máquinas virtuales y realizar sus respectivas configuraciones y particiones, al obtener el archivo iso, procedemos a crear una nueva máquina virtual, la cual es Endian. Se debe tener mucho cuidado cuando se configura el disco duro y la RAM, ya que de esto va a depender mucho el rendimiento de nuestras máquinas.

Figura 1.
Configuración máquina virtual de Endian



Fuente: Autoría propia

Se puede observar la ventana principal de Virtual Box, en donde se evidencia las tres máquinas virtuales y la segmentación de red. Para garantizar el funcionamiento adecuado del sistema, se asigna los recursos de los hardware pertinentes, en donde se adecúa la memoria RAM, el procesador y la capacidad de almacenamiento; de igual forma se configuró los diferentes adaptadores para poder segmentar

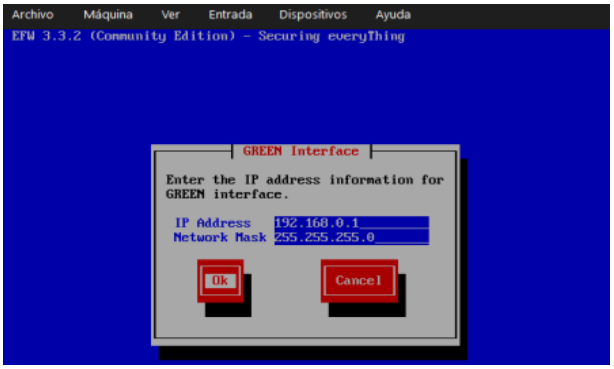
correctamente las zonas, GREEN, RED, y ORANGE en la infraestructura de red.

Figura 2.
Instalación del programa Endian

Fuente: autoría propia

Al abrir la máquina, se selecciona el idioma y posterior a esto empieza la instalación, con el asistente de instalación se pudo preparar el entorno necesario en donde se va a implementar los servicios de seguridad perimetral, Proxy HTTP y el firewall. También se comprobó el correcto funcionamiento de los recursos de hardware asignados anteriormente y de esta manera se garantiza la estabilidad del SO.

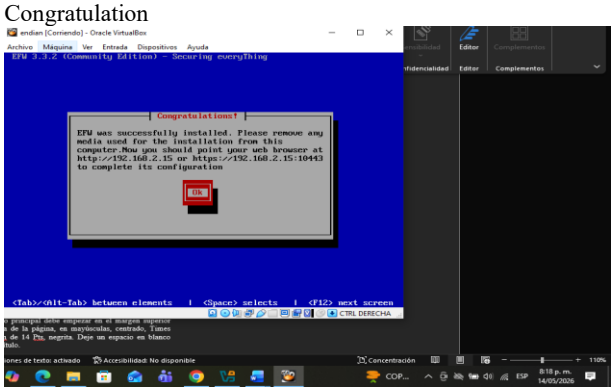
Figura 3.
Green interface



Fuente: Autoría propia

Se presenta la configuración de la interfaz GREEN en GNU/Linux, esta interfaz pertenece a la red interna LAN, la cual va a permitir la comunicación entre los equipos que estén dentro de la infraestructura local. Se asignó la dirección IP 192.168.0.1 con su máscara de red correspondiente. Esta configuración resulta ser fundamental ya que administra los servicios internos y los accesos a internet.

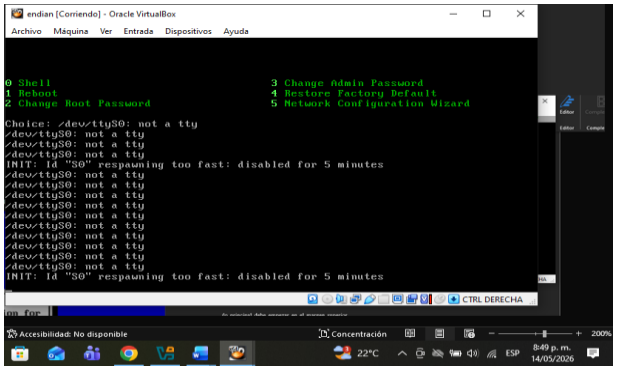
Figura 4.
Congratulation



Fuente: Autoría propia

La instalación terminó satisfactoriamente, y de inmediato empieza la máquina a efectuar todos los cambios, se confirma que todos los servicios fueron instalados satisfactoriamente, y se realiza todo sin errores. Después de esto se procede a aplicar los cambios de manera automática, preparando así los servicios internos para el correcto funcionamiento.

Figura 5.
Endian funcionando



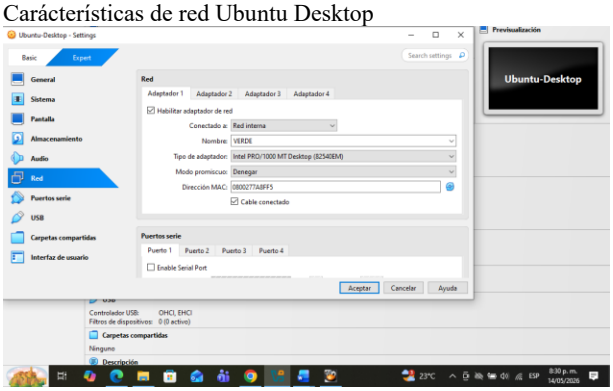
Fuente: Autoría propia

Se evidencia el correcto funcionamiento cuando finaliza la instalación, se puede observar que el SO está iniciando correctamente y que todos los funcionamientos se encuentran activos. También se verifica que las redes configuradas anteriormente hayan sido reconocidas adecuadamente, pemitiendo la comunicación entre ellas. Esto es muy importante antes de implementar el Proxy HTTP, las políticas y las restricciones.

3 DESARROLLO DE LA ACTIVIDAD

3.1 VERIFICACIÓN DE LAS MÁQUINAS VIRTUALES

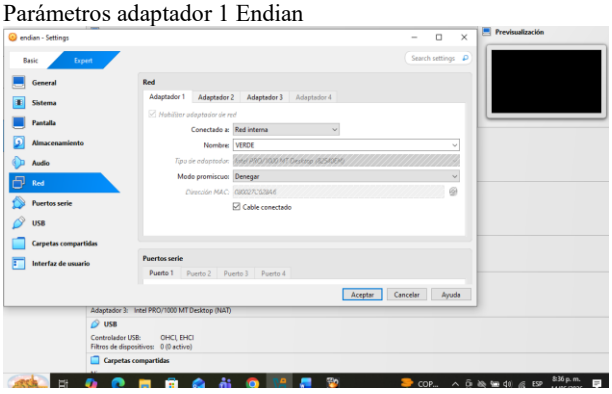
Figura 6.
Carácterísticas de red Ubuntu Desktop



Fuente: Autoría propia

Se puede evidenciar que el adaptador de red fue establecido en red interna, para permitir de esta forma la comunicación con la zona GREEN. Resulta fundamental esta configuración ya que permite la conexión entre el Ubuntu Desktop y el firewall, para que después permita un acceso controlado a internet a través del Proxy HTTP.

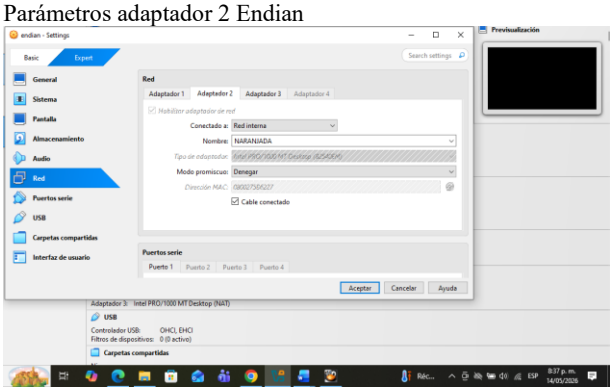
Figura 7.
Parámetros adaptador 1 Endian



Fuente: Autoría propia

Este adapatador se configuró para la interfaz GREEN, en donde representa la red interna que es LAN, la cual se utiliza para los equipos autorizados en la insfraestructura virtualizada. Con esta configuración se pudo lograr la conexión Desktop y el firewall y de esta manera adminstrar el tráfico de red y las políticas de autenticación.

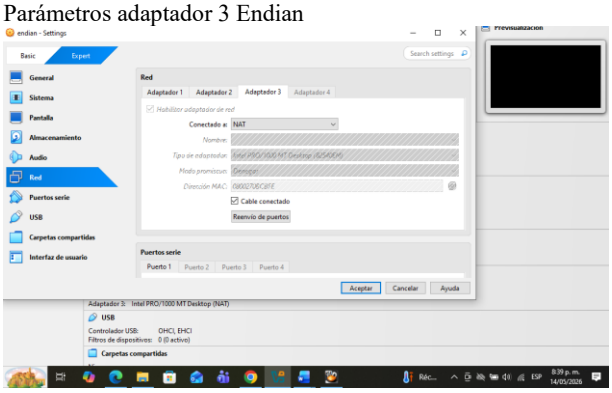
Figura 8.
Parámetros adaptador 2 Endian



Fuente: Autoría propia

Representa la zona desmilitarizada, que se utiliza para alojar todos los servicios que necesiten un acceso intermedio entre la red interna y externa. Con esta configuración se está aumentando la seguridad de la infraestructura y se reducen los riesgos de accesos no autorizados. Además con la interfaz ORANGE se está protegiendo la red interna con las políticas impementadas con el firewall.

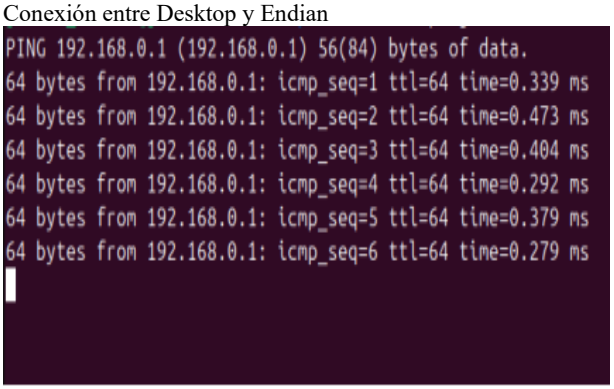
Figura 9.
Parámetros adaptador 3 Endian



Fuente: Autoría propia

Corresponde a la interfaz RED, es la que se encarga de proporcionar una conexión hacia internet y que se puedan comunicar la infraestructura virtualizada y la red externa. Con esta configuración se habilita el acceso controlado en donde el firewall supervise y filtre las entradas y salidas en la red. Se está garantizando la conectividad a internet, la aplicación de las políticas de seguridad y el filtrado web.

Figura 10.
Conexión entre Desktop y Endian

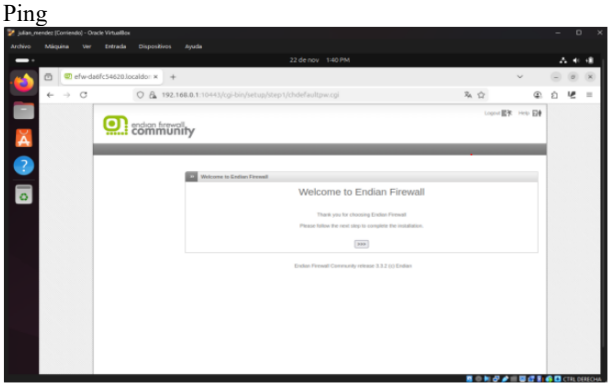


Fuente: Autoría propia

Se evidencia, a través del comando ping la prueba de conectividad hacia la dirección ip 192.168.0.1, que corresponde a la interfaz Green. Esta conexión resulta fundamental entre ambas máquinas para poder garantizar los funcionamientos de autenticación , filtrado web y navegación controlada en donde se implementó anteriormente en el Proxy HTTP.

3.1.1 ACCESO AL PANEL DE ENDIAN

Figura 11.
Ping



Fuente: Autoría propia

Se puede observar el panel inicial de Endian, a la cual se accede a través de la dirección IP de la zona Green mediante el navegador Firefox. Desde acá se va a poder realizar el Proxy HTTP, la configuración del firewall y la gestión de la seguridad perimetral. Desde este panel es posible administrar los servicios de seguridad y las políticas de autenticación.

Figura 12.
Configuración de la zona Green en Endian

Fuente: Autoría propia

Corresponde a la red interna es decir LAN, en donde se encuentran todos los equipos que han sido autorizados de la infraestructura virtualizada. En esta configuración se asignó la dirección IP y los parámetros para garantizar la comunicación en la red interna. En la interfaz GREEN se administra los usuarios internos y se restringe el acceso a algunos servicios mediante el Proxy HTTP.

Figura 13.
Configuración de la zona naranja

Fuente: Autoría Propia

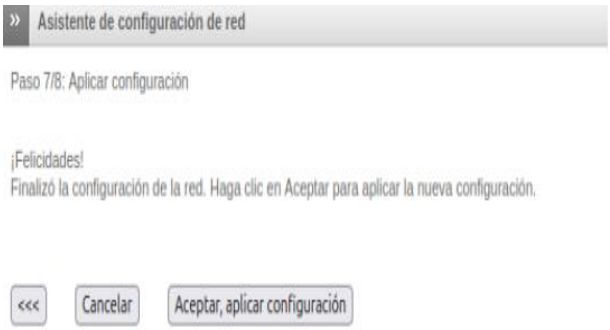
Zona naranja que corresponde a la DMZ es decir la zona desmilitarizada, que son los servidores accesibles desde internet. La ip que se asigna es 172.16.0.1 con una máscara de red de /28, así de esta manera se aislan los servicios públicos de la red interna y se mejora la seguridad perimetral.

Figura 14.
Configuración de la zona RED (WAN)

Fuente: Autoría propia

Se puede observar la configuración de la zona red, en donde se permite la salida y la entrada del tráfico y de esta manera se está facilitando que se pueda acceder a la red pública y que haya una comunicación entre la red interna y los servicios externos.

Figura 15.
Finalización del asistente de red



Fuente: Autoría propia

Se confirma la configuración de las interfaces, que fue realizada correctamente, también se evidencia el registro del correo electrónico y los cambios efectuados durante la instalación. Con este mensaje de culminación satisfactoria, quiere decir que el Firewall quedó preparado para gestionar el tráfico de red, además de la implementación de las políticas de autenticación y el filtrado web.

4 CONFIGURACIÓN DEL SERVICIO PROXY HTTP

Figura 16.
Activación del Proxy HTTP

Fuente: Autoría propia

Se habilita el servicio Proxy en modo no transparente en el panel administrativo de Endian. Con esta configuración se está indicando que los usuarios de la red LAN deben autenticarse para acceder y así de esta forma se lleva un mejor control de la navegación y el filtrado web. Resulta muy importante esta configuración para controlar la navegación de los usuarios, el tráfico de red y las políticas de filtrado.

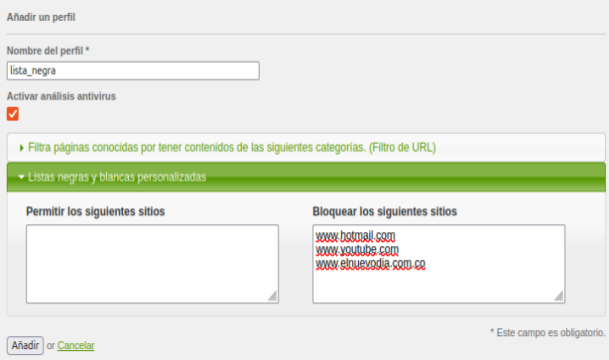
4.1 CREACIÓN DE LA LISTA NEGRA PARA LA RESTRICCIÓN

Figura 17.
Paso a paso para crear una lista negra

Fuente: Autoría propia

A través de esta configuración se accede a las opciones de filtrado web, se permite agregar dominios y páginas web restringidas por los usuarios. Las listas negras son muy esenciales dentro de la seguridad perimetral ya que controla los accesos a contenidos no autorizados y gestionar de una manera más eficiente la navegación de los usuarios.

Figura 18.
Adición de sitios web bloqueados

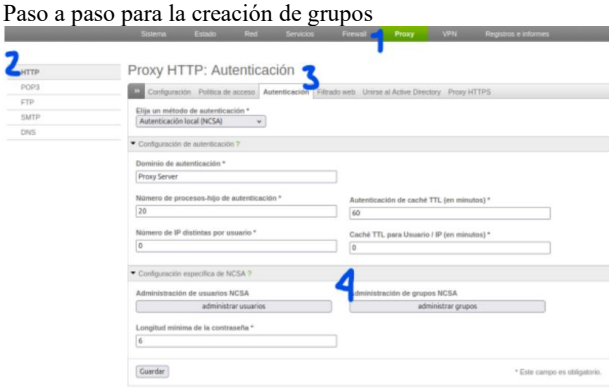


Fuente: Autoría propia

Se pudo agregar los sitios web de hotmail, youtube, elnuevodia, a la lista negra, quedando así como páginas redtringidas, con esta función no se permite el ingreso a páginas no autorizadas.

5 CREACIÓN DE USUARIOS Y POLÍTICA DE AUTENTICACIÓN

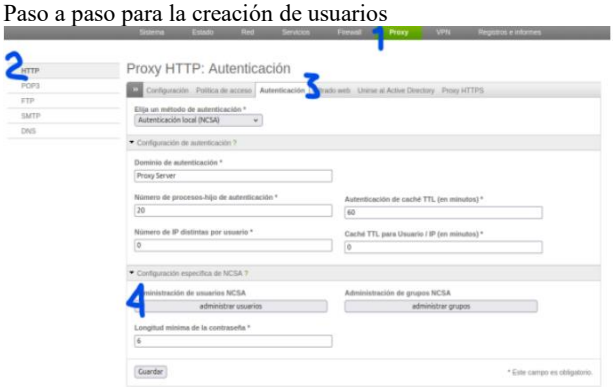
Figura 19.
Paso a paso para la creación de grupos



Fuente: Autoría propia

Se evidencia la ruta dentro del panel administrativo para poder gestionar grupos de autenticación de usuarios. De esta manera se crean grupos que permite organizar a los usuarios y crear políticas restrictivas. Se aplican políticas de navegación controlada y seguridad perimetral a través del filtrado de contenido no autorizados. Con esto se gestiona el acceso de internet dentro de la organización.

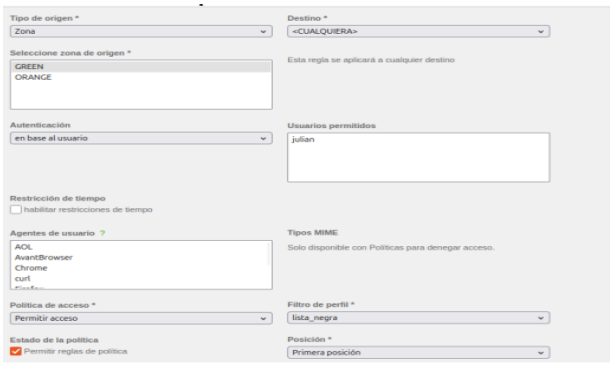
Figura 20.
Paso a paso para la creación de usuarios



Fuente: Autoría propia

Mediante esta configuración se definen las credenciales de acceso, los nombres de usuario y los parámetros que sean necesarios para la autenticación dentro del Proxy HTTP. Resulta fundamental la creación de los usuarios ya que se puede administrar de manera individual y aplicar las políticas en la organización, se permite el control de acceso, supervisión y mejoramiento de la seguridad a través de la autenticación y el filtrado web.

Figura 21.
Política de acceso



Fuente: Autoría propia

Se estableció las reglas de autenticación que deben de cumplir los usuarios de la red interna para poder acceder a internet. Con las políticas se definen permisos, restricciones y control según los grupos de usuarios creados anteriorme, además de facilitar el tráfico de red y fortalecer la seguridad perimetral.

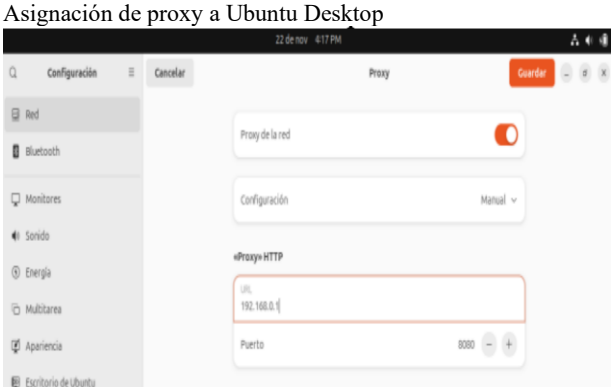
Figura 22.
Política de acceso creada satisfactoriamente

Fuente: Autoria propia

Al aplicar la configuración correspondiente, el sistema confirma que fueron implementados correctamente en el servicio Proxy HTTP, permitiendo el acceso controlado de los usuarios a internet a través de restricciones. También con esta configuración se garantiza el funcionamientos adecuado de la seguridad perimetral, autenticación de usuarios y la navegación dentro de la infraestructura virtualizada.

6 CONFIGURACIÓN DEL UBUNTU DESKTOP EN EL PROXY HTTP

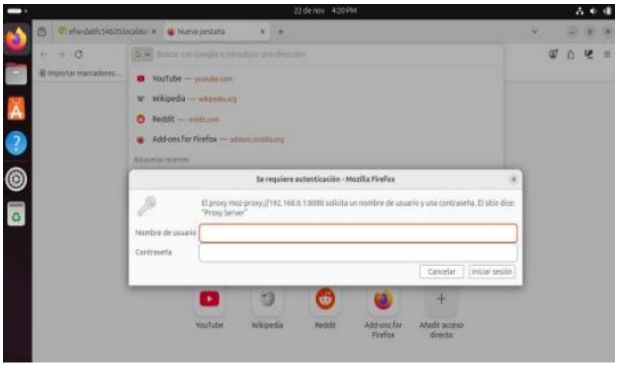
Figurra 23.
Asignación de proxy a Ubuntu Desktop



Fuente: Autoría propia

En este proceso se configuró manualmente la dirección IP y el puerto del proxy que corresponde a GNU/Linux firewall Community, permitiendo que todo lo generado desde Desktop sea administrado por firewall. Esta configuración es muy importante para habilitar los mecanismos de autenticación, filtrado web y los controles de acceso.

Figura 24.
Autenticación



Fuente: Autoría propia

El sistema solicita las credenciales, permitiendo de esta forma verificar la identidad del usuario antes de autorizar la navegación por internet. Con esta configuración se Fortalece la seguridad perimetral ya que controla el acceso a los recursos de red y políticas de navegación según los perfiles configurados.

Figura 25.
Acceso denegado

Fuente: Autoría propia

Se evidencia el correcto funcionamiento de las listas negras que se implementaron anteriormente, en donde se impide el acceso a los usuarios a sitios web no autorizados, además se demuestra la efectividad de las políticas de seguridad perimetral aplicadas en el firewall, permitiendo controlar el tráfico de navegación.

7 CONCLUSIONES

La implementación de un Proxy HTTP, permitió comprender lo importante que es la seguridad perimetral, controlando el acceso de los usuarios a internet a través de políticas de autenticación, también se pudo adquirir conocimientos de gestión de redes, aplicación de políticas de seguridad en sistemas GNU/Linux y la configuración de servicios proxy.

8 REFERENCIAS

[1] Canonical, Guía de Ubuntu Desktop 20.04 LTS, Help Ubuntu, 2023. Disponible en: https://help.ubuntu.com/

[2] Debian Project, Manual del Administrador de Debian 12.5.0, 2023. https://www.debian.org/releases/stable/amd64/index.es.html

[3] Ángel José Cervelión, "*Instalación de Nagios Core 4.4 en Ubuntu 22.04*", Repositorio Institucional UNAD, 2023. Disponible en: https://repository.unad.edu.co/handle/10596/54230

[4] Endian, Endian UTM 3.2 Manual Reference, 2016. Disponible en: http://docs.endian.com/3.2/utm/index.html

[5] Linux Professional Institute, LPI LPIC-1 Exam 101 – Tema 102: Comandos GNU y Unix, 2022. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/