Implementando Seguridad en GNU/Linux

Otilia Quiñones Ochavano

e-mail:oquinoneso@unadvirtual.edu.co

RESUMEN: *En el este artículo se plasmo la implementación y Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo. En la primera temática la implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ) Configuración NAT.*

En la seguda tematica Configuración NAT. 1. Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet). 2. Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el re-envió de puertos / NAT, la creación de las reglas.

En la tercera temática, Permitir servicios de la Zona DMZ para la red1. Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. 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.

En la cuarta temática se aplica las reglas de acceso para permitir o denegar el tráfico. 1. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos. 2. Comunicar la zona Internet con la zona DMZ. 3. Verificar en el tráfico Inter - Zona, la creación de las reglas. 4. Probar desde un navegador Web, las siguientes directivas: El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso del servicio HTTP desde la LAN hacia la WAN. El ingreso del servicio HTTP desde la zona DMZ hacia la WAN. El ingreso del servicio HTTP desde la WAN hacia la zona DMZ. El ingreso del servicio FTP desde la LAN hacia la WAN. El ingreso del servicio FTP desde la WAN hacia la zona DMZ.

La quinta temática, Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet. 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

***PALABRAS CLAVE**: Endian, LAN, WAN, NAT, VirtualBox, HTTP, ICMP, FTP, Zona DMZ..*

1. INTRODUCCIÓN

Esta guía proporciona un paso a paso para la Configurar Interfaces de usuario y escritorio a través de tareas administrativas con los servicios esenciales dándole un óptimo nivel de seguridad al sistema operativo GNU Linux. Para gestionar y controlar el acceso a internet de los equipos conectados a una red, mejorando la administra

2. IMPLEMENTACIÓN

2.1 CARACTERÍSTICAS GENERALES

*Uso de sistemas operativos de código abierto para optimizar recursos al utilizar estaciones de trabajo con GNU/Linux **por su** estabilidad, seguridad y bajo consumo de recursos, lo que permite un entorno de red eficiente.*

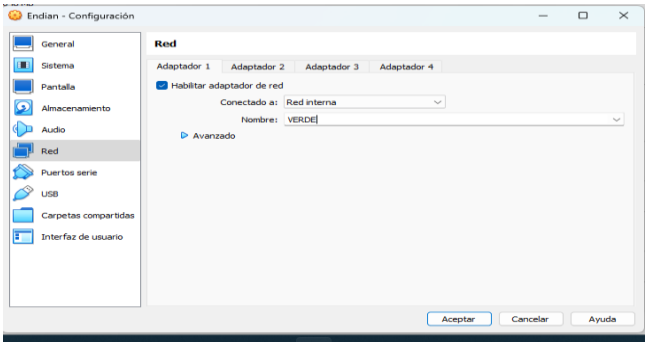
La Implementación de seguridad mediante un Firewall Endian ya que actúa como cortafuegos y puerta de enlace entre la red LAN (interna) y la red WAN (externa, como Internet) y controla el tráfico de datos, aplicando políticas de seguridad, NAT, VPN y filtros para proteger la red interna contra accesos no autorizados o amenazas externas.

Se utiliza un servidor GNU/Linux en la DMZ (zona desmilitarizada) como servidor web y bases de datos accesibles desde Internet) sin comprometer la seguridad de la LAN.

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

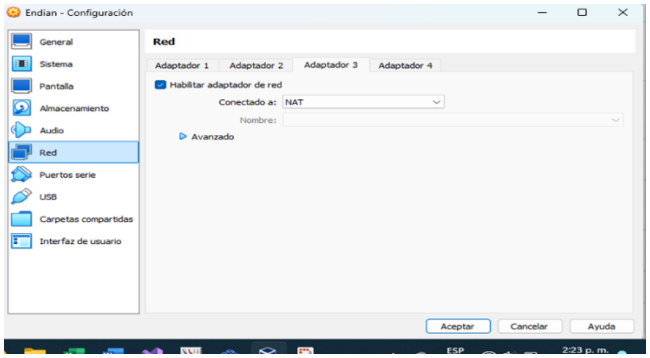
Para la instalación se requiere tener instalada una máquina virtual en el computador de escritorio o portátil.

Figura 1. Configurar Endian- Adaptador 1-Red interna-verdad



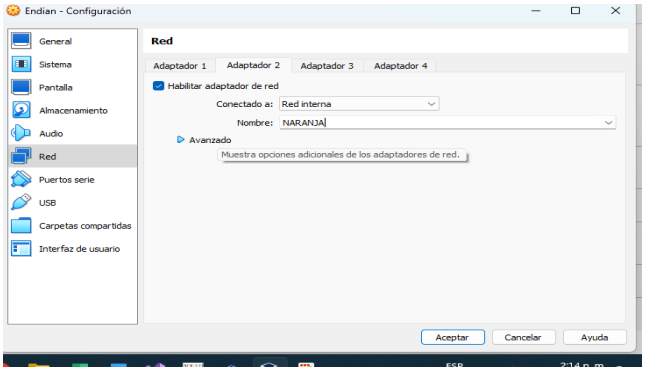
Fuente: Autoría propia

Figura 2. Configurar Endian- Adaptador 2-Red interna-Naranja



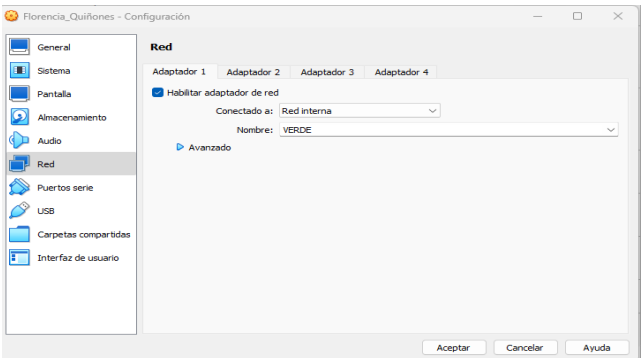
Fuente: Autoría propia

Figura 3. Configurar red Endian NAT



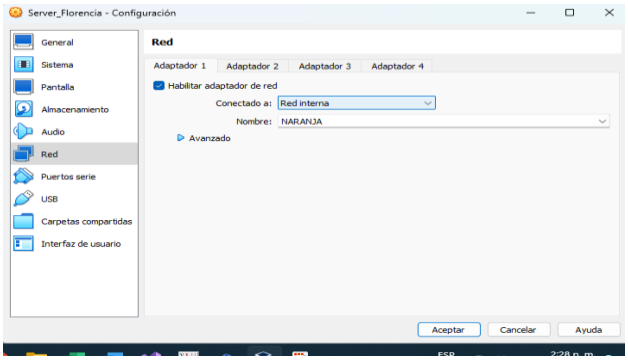
Fuente: Autoría propia

Figura 4. Configuración de tarjeta de red de Ubuntu



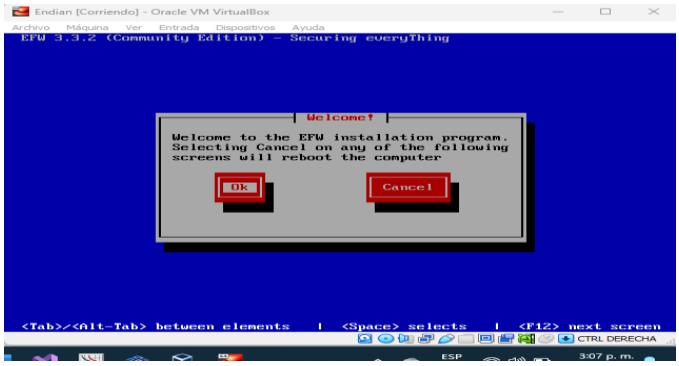
Fuente: Autoría propia

Figura 5. Configuración adaptadores de red



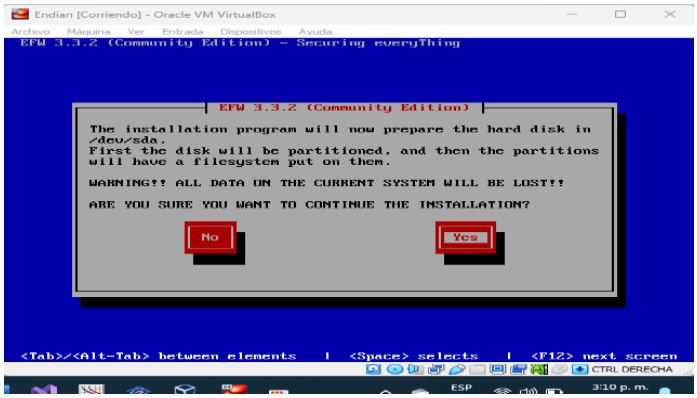
Fuente: Autoría propia

Figura 6. seleccionar el idioma en el que se va a trabajar



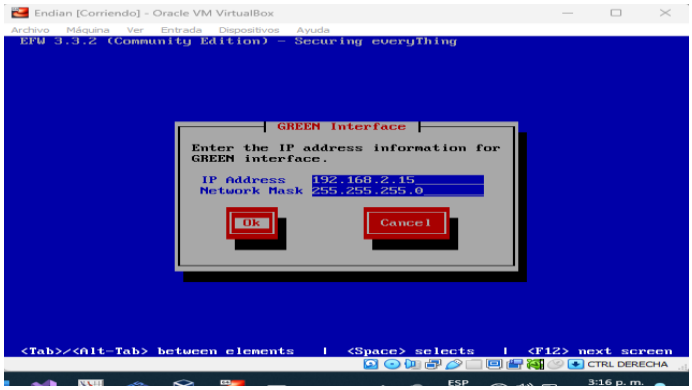
Fuente: Autoría propia

Figura 7. Da la bienvenida y se le da ok



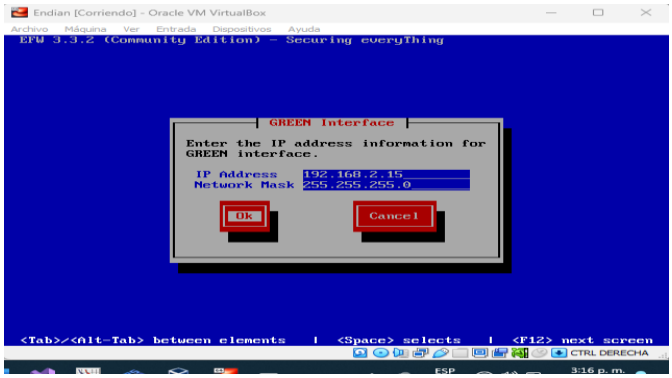
Fuente: Autoría propia

Figura 8. Seleccionamos la casilla NO



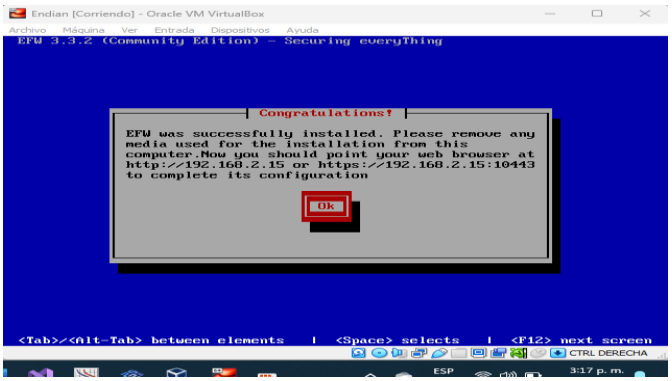
Fuente: Autoría propia

Figura 8. Ponemos la dirección IP d la tarjeta verde. 192.168.2.15



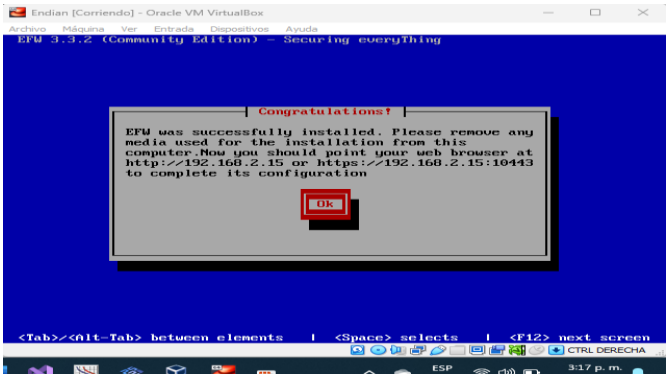
Fuente: Autoría propia

Figura 9. Nos indica que todo salió correcto



Fuente: Autoría propia

Figura 10: Nos indica que todo salió correcto



Fuente: Autoría propia

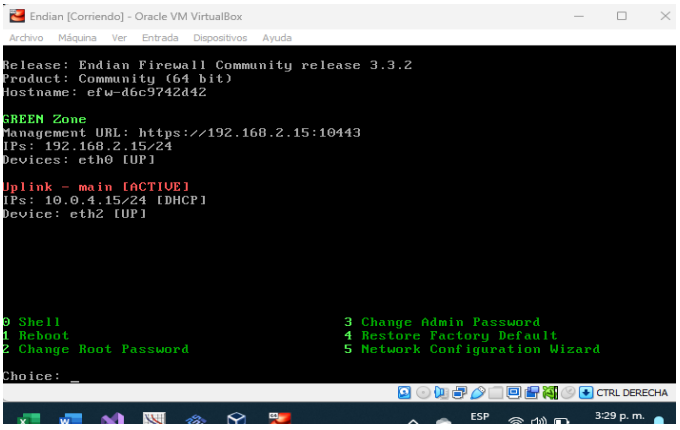
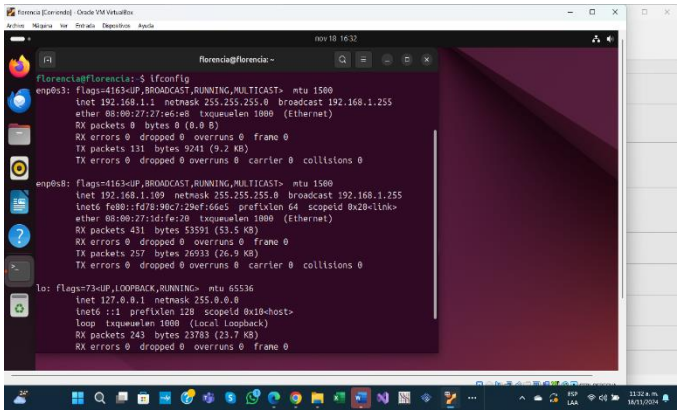


Figura 11: Configuración en Endian

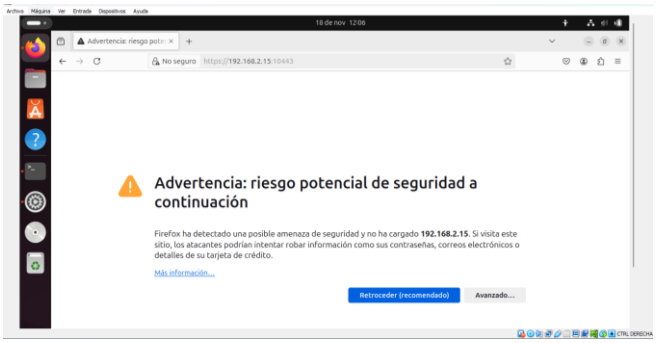
Fuente: Autoría propia

Figura 12: Verificamos la Ip de ubuntu server



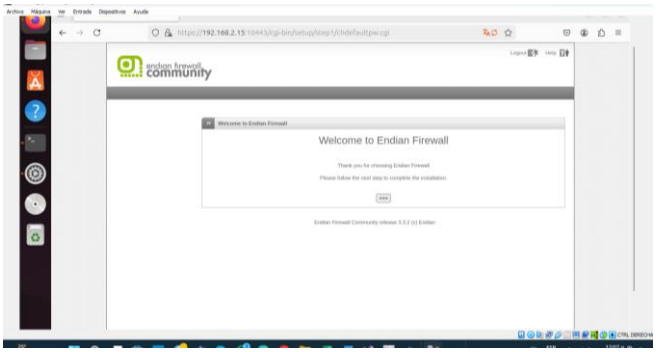
Fuente: Autoría propia

Figura 13: Ingresamos al navegador con la Ip: 192.168.2.15



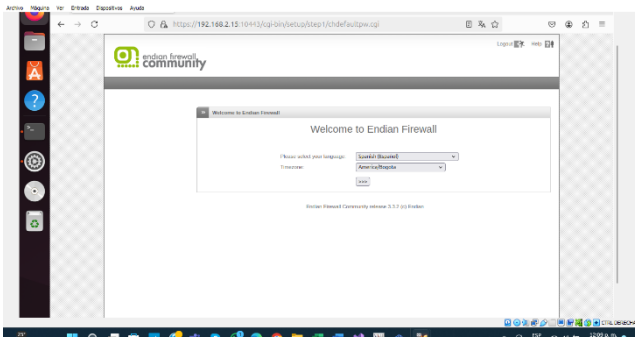
Fuente: Autoría propia

Figura14: Endian da la Bienvenida



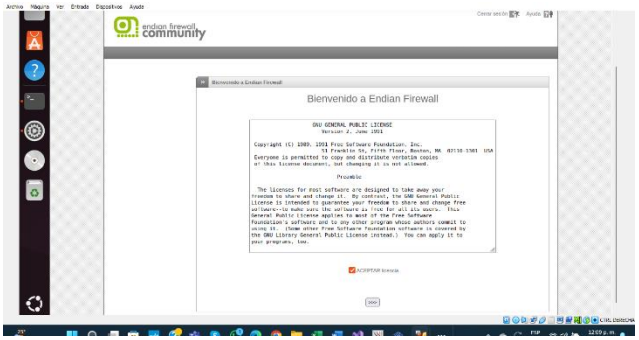
Fuente: Autoría propia

Figura 15: Le damos siguiente



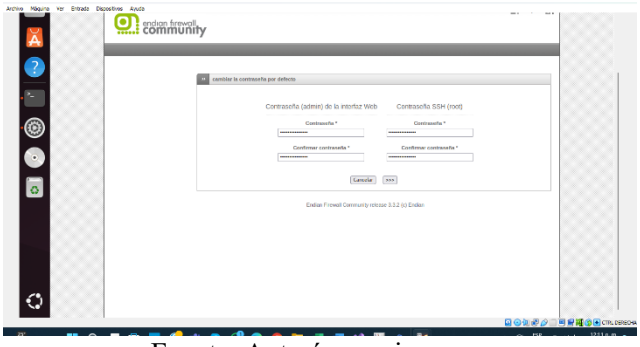
Fuente: Autoría propia

Figura 16: Aceptamos la licencia



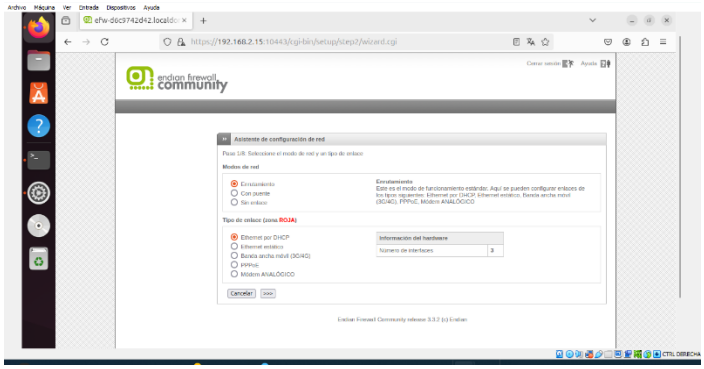
Fuente: Autoría propia

Figura 17: ponemos contraseñas y las confirmamos



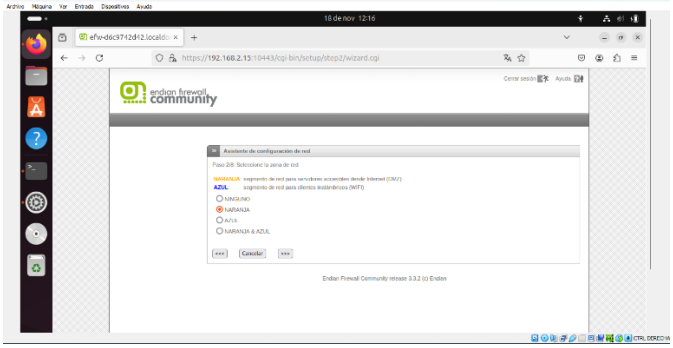
Fuente: Autoría propia

Figura 18: Ingresamos a Endian



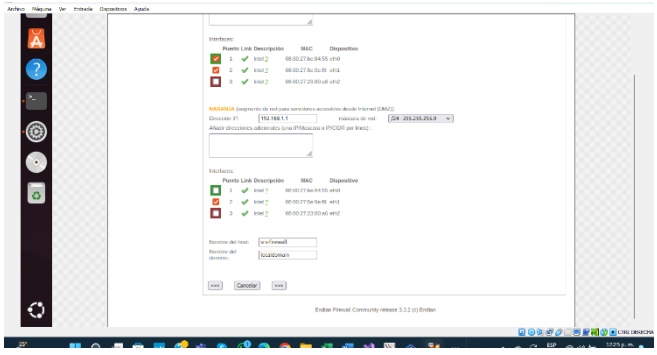
Fuente: Autoría propia

Figura 19: Configuramos la red Naranja



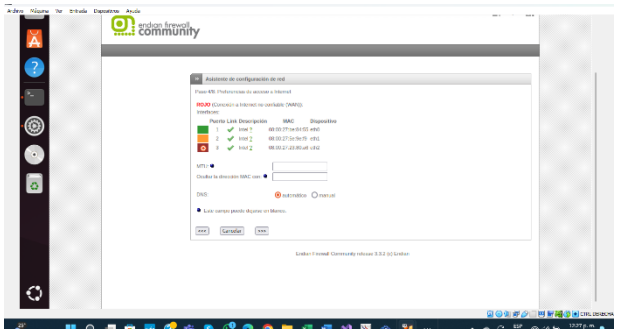
Fuente: Autoría propia

Figura 20: Ponemos la Ip de y seleccionamos



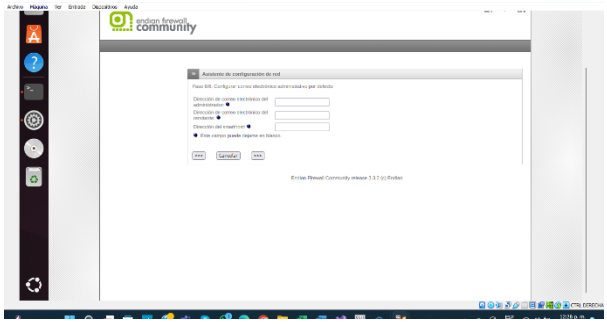
Fuente: Autoría propia

Figura 21: Ingresamos y aparecen los 3 colores activos



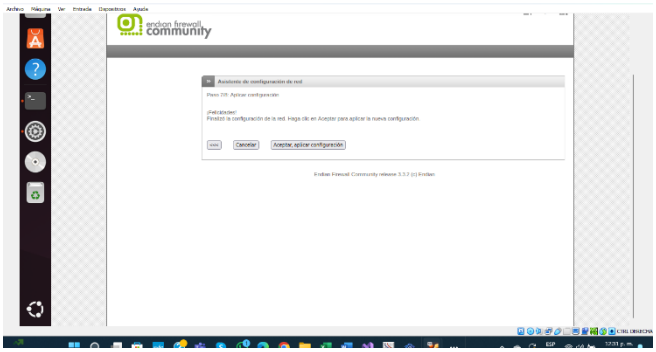
Fuente: Autoría propia

Figura 22: Le damos seguir



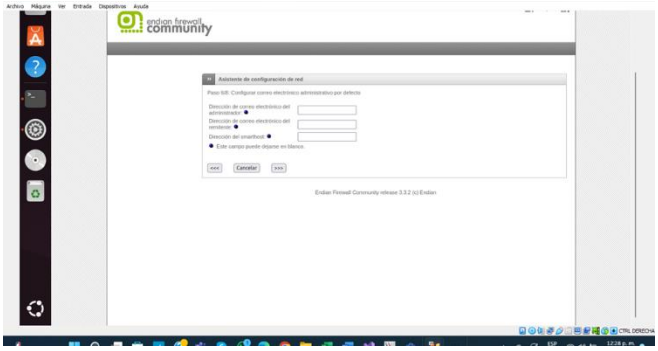
Fuente: Autoría propia

Figura 23: Seguimos



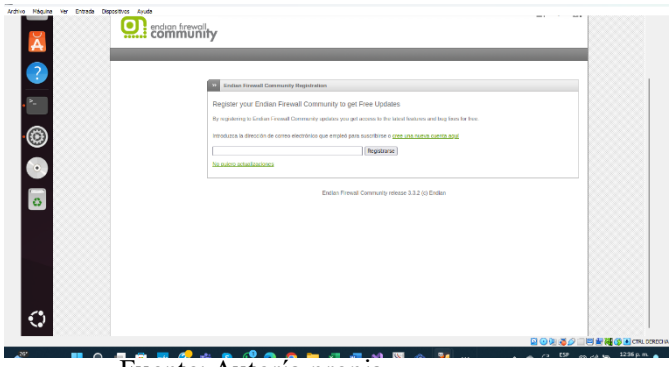
Fuente: Autoría propia

Figura 24 :le damos aceptar



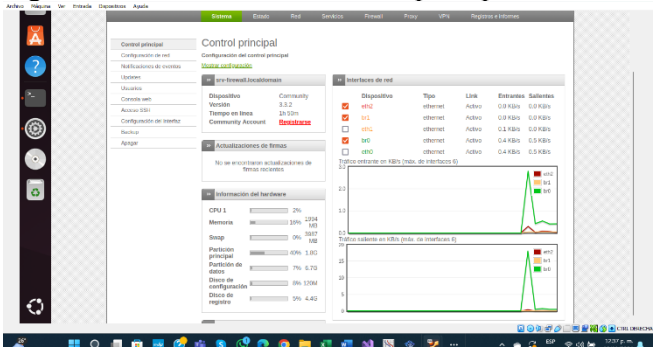
Fuente: Autoría propia

Figura 25 :Terminamos



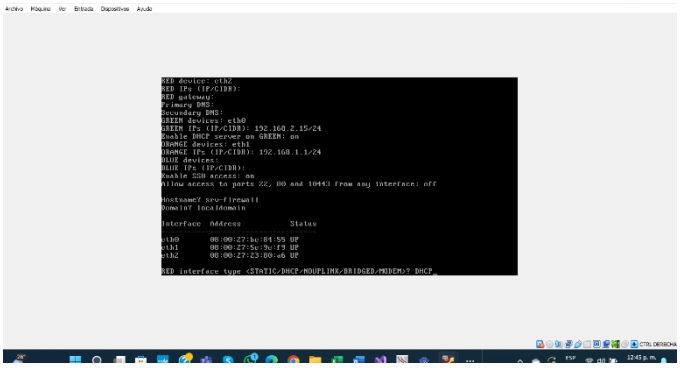
Fuente: Autoría propia

Figura 26: Se muestra el control principal de Endian



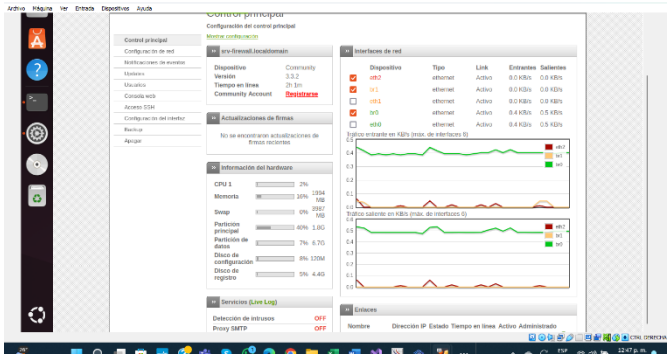
Fuente: Autoría propia

Figura 27: Ingresamos a la terminal de Endian y verificamos los tarjetas y conexiones



Fuente: Autoría propia

Figura 28: Entramos de nuevo Endian y observamos el flujo de las tarjetas

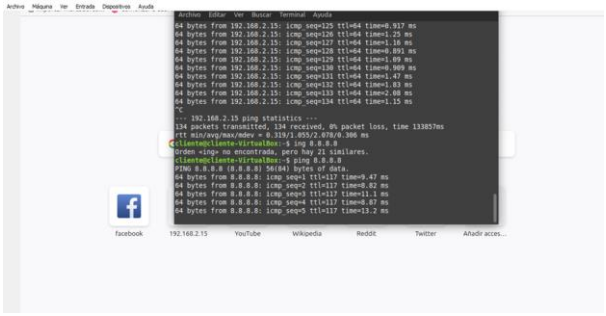


Fuente: Autoría propia

3. :TEMÁTICA CONFIGURACIÓN NAT. PRODUCTO ESPERADO

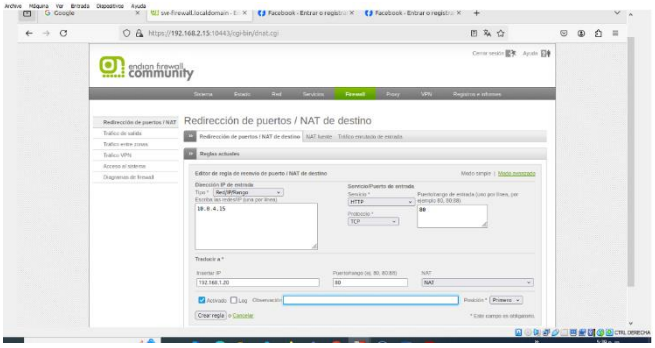
Figura 29: Configurar la regla de NAT

(Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet). Comprobando la conexión de internet desde el cliente



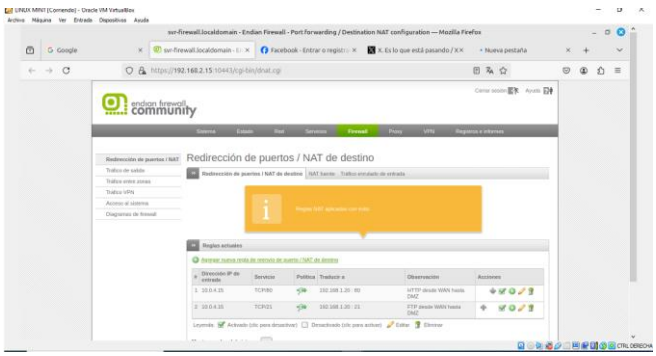
Fuente: Autoría propia

Figura 30: Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el re-envió de puertos / NAT, la creación de las reglas.



Fuente: Autoría propia

Figura 31: Configuración de la regla

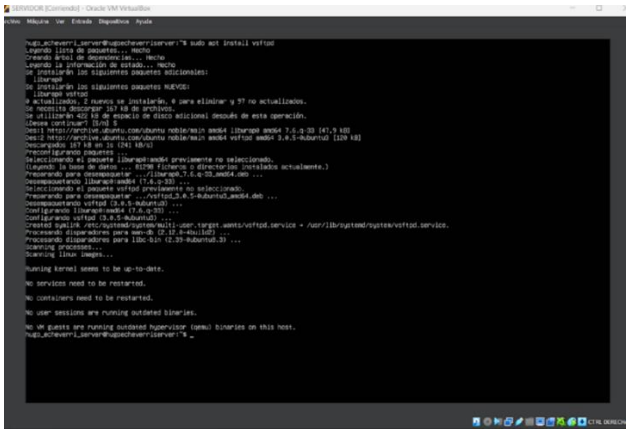


Fuente: Autoría propia

4. PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

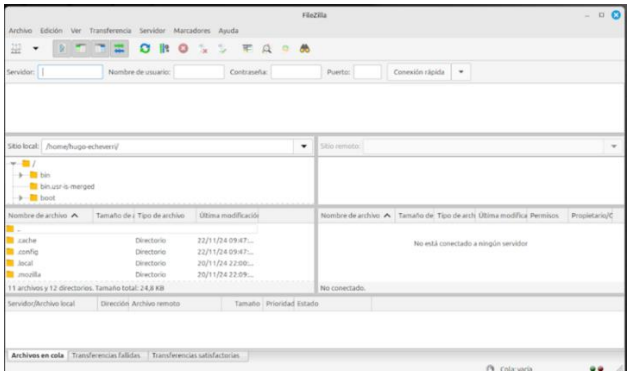
1. Figura 32: Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

Realizamos la instalación de “vsftpd” para habilitar el servicio en el servidor.



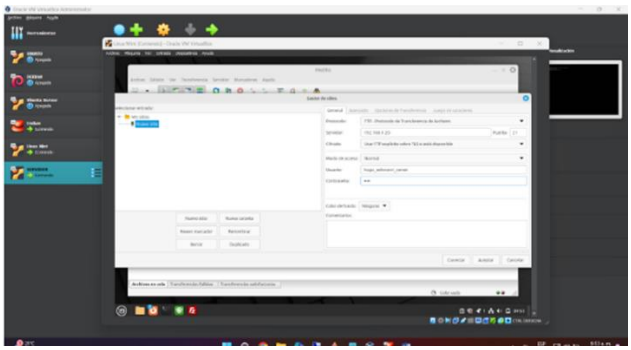
Fuente: Autoría propia

Figura 33: Instalamos y ejecutamos FileZilla para poder validar la conexión FTP.



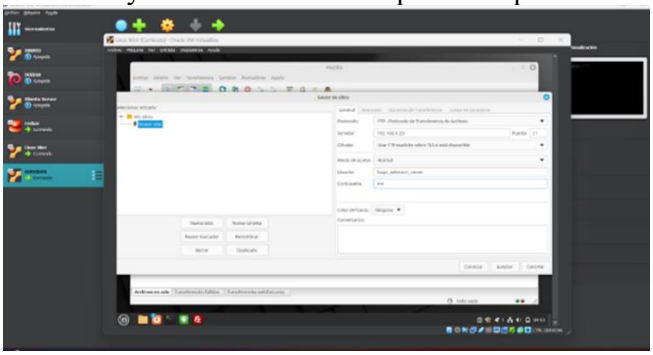
Fuente: Autoría propia

Figura 34: Ingresamos un nuevo sitio con la dirección del servidor y nuestro usuario por el puerto 21.



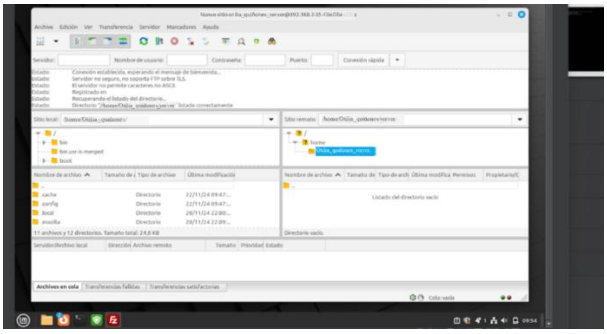
Fuente: Autoría propia

Figura 35: Ingresamos un nuevo sitio con la dirección del servidor y nuestro usuario por el puerto 21.



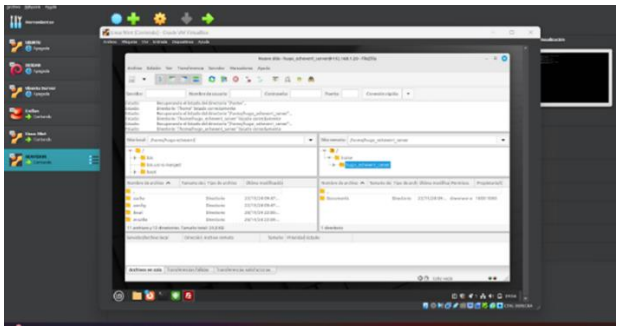
Fuente: Autoría propia

Figura 36: Validamos que se conecta correctamente a las carpetas del servidor.



Fuente: Autoría propia

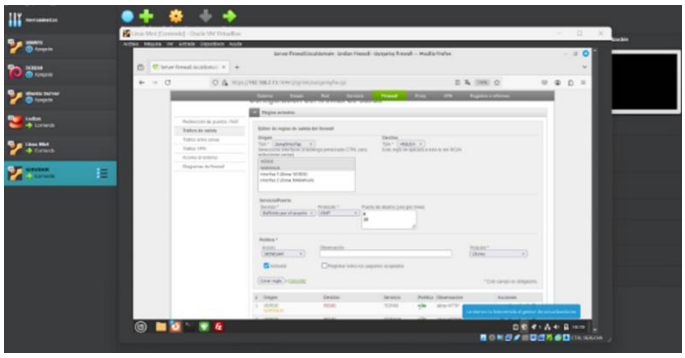
Figura 37: Podemos crear una nueva carpeta llamada “Documents” para validar la conexión.



Fuente: Autoría propia

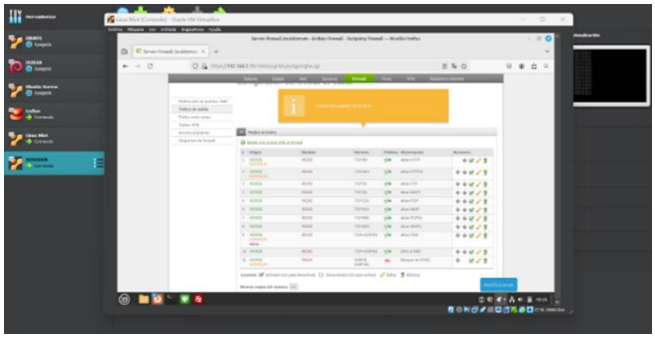
4.1. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Figura 38:



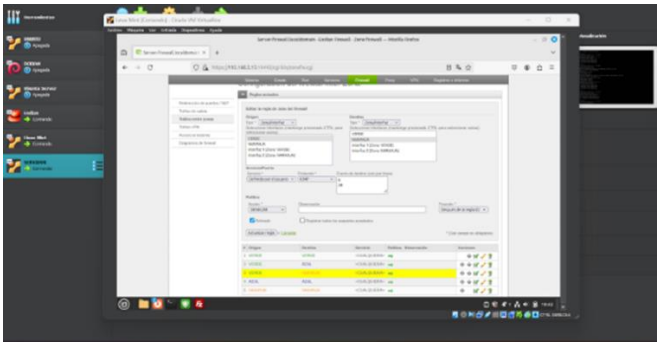
Fuente: Autoría propia

Figura 39: Activamos la nueva regla y eliminamos cualquier otra regla creada que permitía la conexión ICPM para los puertos 8 y 30.



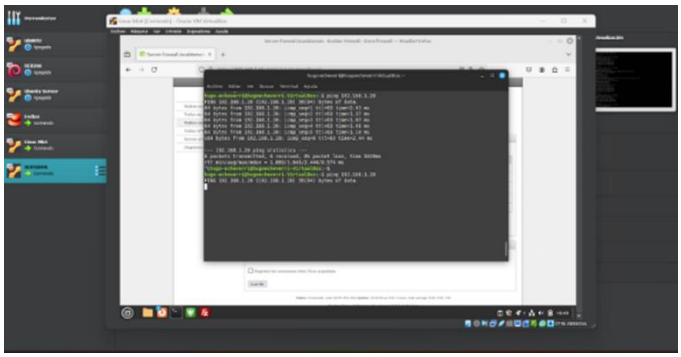
Fuente: Autoría propia

Figura 40: También ingresamos al “Trafico entre zonas” para realizar la misma denegación.



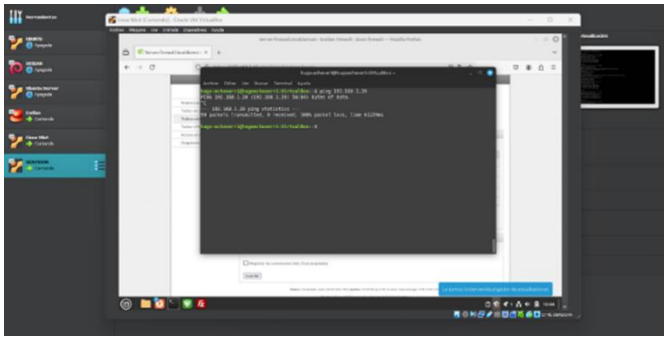
Fuente: Autoría propia

Figura 41: Ahora podemos validar nuevamente realizando un ping a nuestro servidor que se encuentra en la zona NARANJA DMZ.



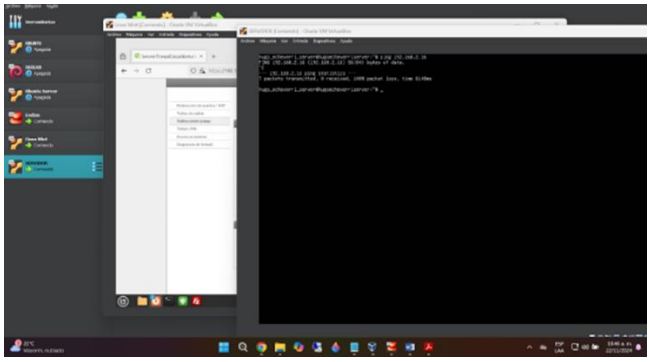
Fuente: Autoría propia

Figura 42: Validamos que ya no permite realizar PING.



Fuente: Autoría propia

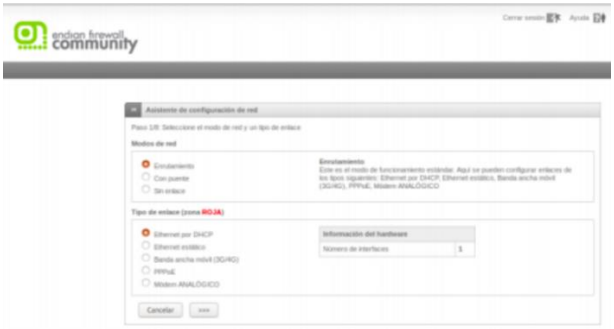
Figura 43: También podemos validar que no permite realizar el PING desde el servidor a la zona GREEN con la IP del Linux Mint



Fuente: Autoría propia

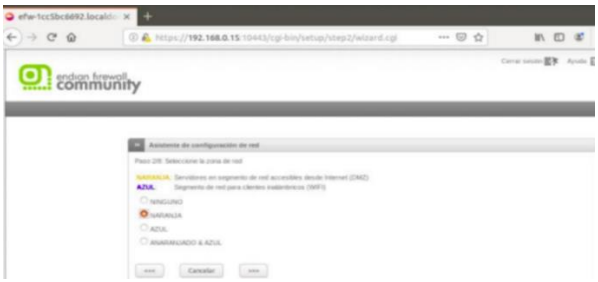
5. REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Figura 44: Seleccionamos el modo red enrutamiento y tipo de enlace DHCP



Fuente: Autoría propia

Figura 45: Seleccionamos la zona de red NARANJA para las dmz

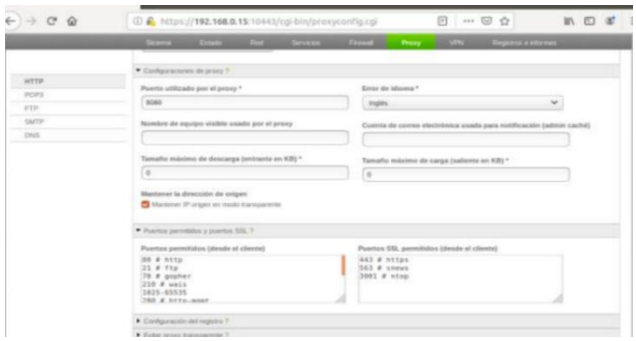


Fuente: Autoría propia

Figura 46: ingresamos al panel

Fuente: Autoría propia

Figura 47: para permitir los servicios HTTP realizamos la configuración HTTP y permitimos los puertos 80 y 21 para la zona NARANJAFuente:

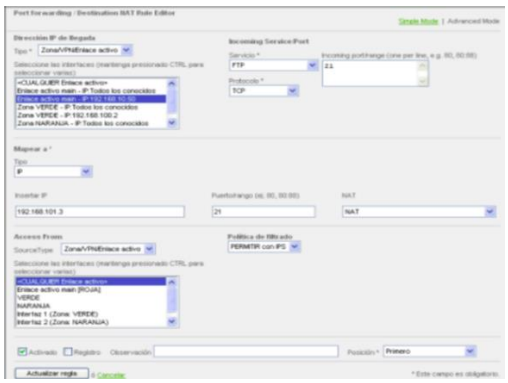


Autoría propia

Figura 48: Para denegar el protocolo ICMP (Puerto 80) creamos una nueva regla en firewall de protocolo ICM donde deniegue los accesos a los puertos 8 y 30 y damos aplicar

Fuente: Autoría propia

Figura 49: Configuración de las reglas de reenvíos y nos dirigimos a NAT Rule Editor



Fuente: Autoría propia

Figura 50: Buscamos zona VPN Enlace activo

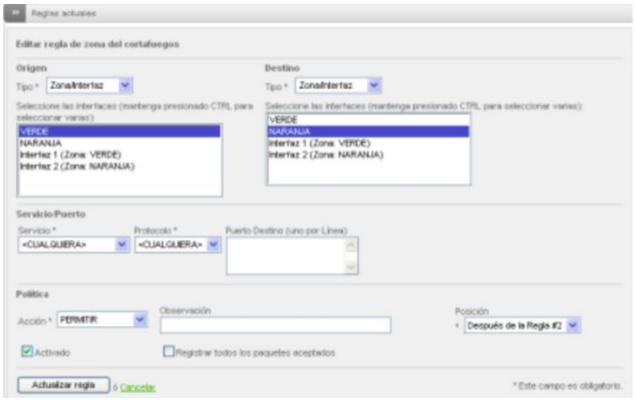
y ahí nos muestra WAN y le diremos que es servicio FTP y también seleccionamos que sea tipo IP y

ponemos la dirección de DMZ donde está el servicio

FTP y su puerto

Fuente: Autoría propia

Figura 51: Configuramos y añadimos una nuevo tráfico entre zonas



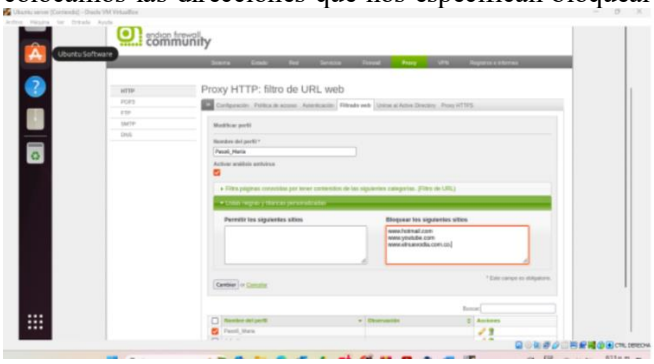
Fuente: Autoría propia

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

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

Figura 52: Luego de crear el nuevo perfil, ingresamos en la sección de listas negras

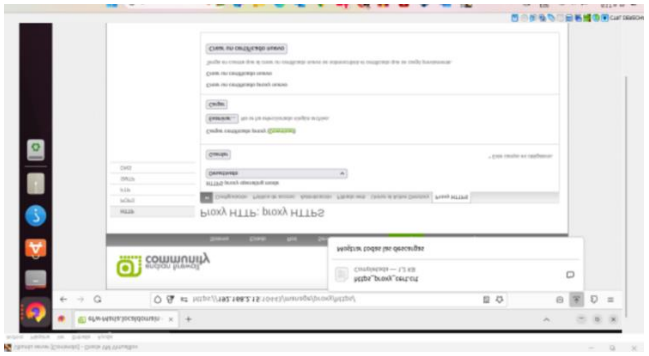
colocamos las direcciones que nos especifican bloquear



Fuente: Autoría propia

Figura 53: Posteriormente ingresamos a proxy HTTPS para el caso de las listas negra

procedan a conectarse mediante el protocolo https, se debe crear un certificado e instalarlo.



Fuente: Autoría propia

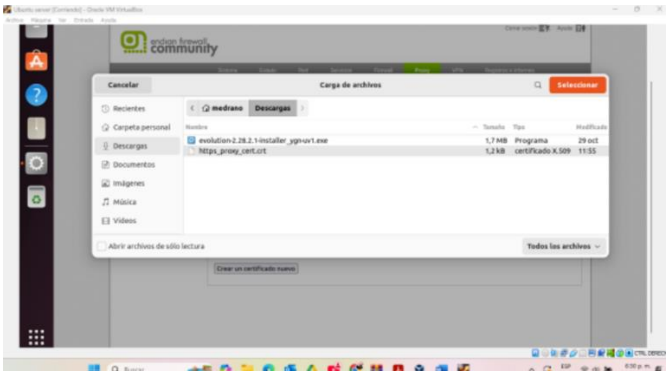
Figura 54: Luego se instala en el navegador de internet en este caso Mozilla Firefox (Ajustes,

Privacidad y seguridad, ver certificados, importar certificado).

Fuente: Autoría propia

Figura 55: Siguiendo con los pasos ingresamos a la opción descarga en donde quedo el

certificado y lo importamos.

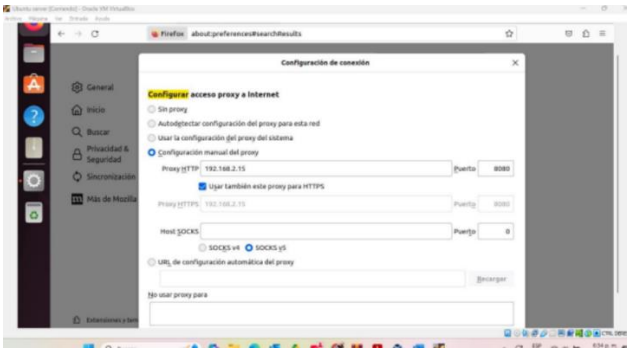


Fuente: Autoría propia

Figura 56: Luego de a ver configurado el Proxy como no es transparente, manualmente se

configura el servidor proxy en el navegador con los datos del servidor que se

configuro al comienzo de la instalación de EFW (dirección IP y mascara de red).

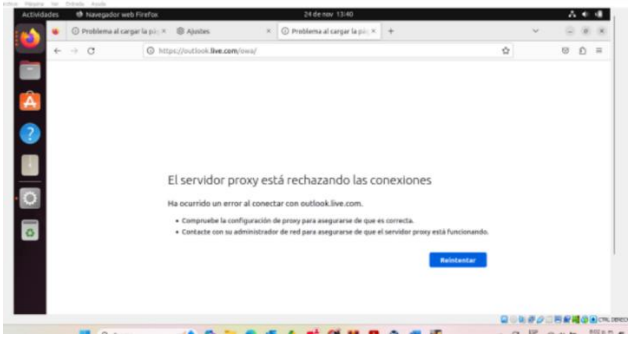


Fuente: Autoría propia

Figura 57: Luego al intentar acceder al sitio web que fueron añadidos en las listas negras se

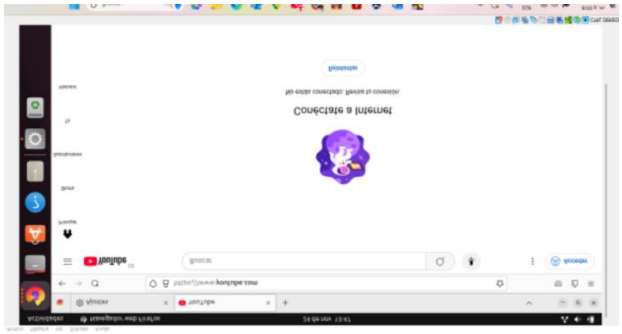
obtiene el siguiente resultado.

hotmail.com



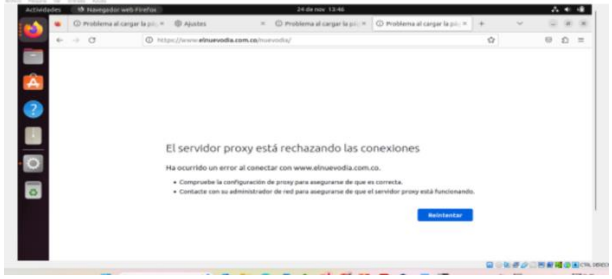
Fuente: Autoría propia

Figura 58: Youtube.com



Fuente: Autoría propia

Figura 59: El nuevodia



Fuente: Autoría propia

7.1. 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.

Figura 60: Siguiendo con lo mencionado al segundo punto se define el dominio de

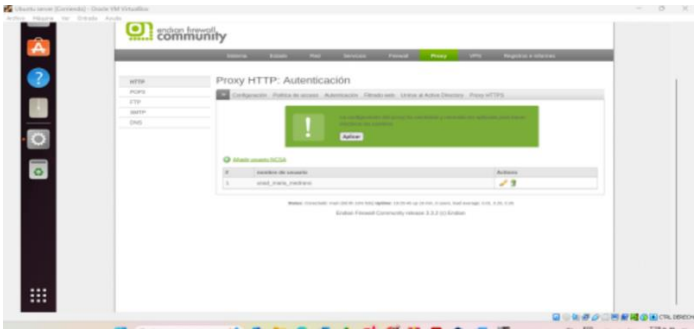
autenticación (Unad_endian), en la cual se define los grupos y usuarios para

autorizar la navegación en nuestro servidor proxy.

Fuente: Autoría propia

Figura 61: Luego se crea un usuario al que se llamara unad_Otilia_Quiñones como se logra

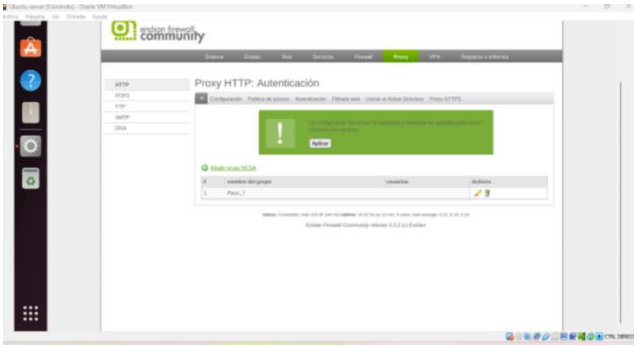
evidenciar.



Fuente: Autoría propia

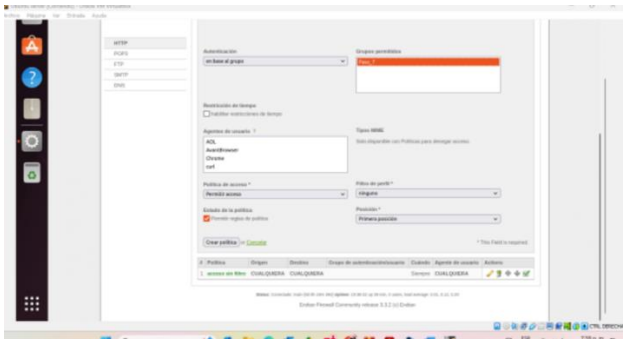
Figura 62: Se sigue creando un grupo llamado Paso_7 y se le asigna el usuario creado en el

paso anterior.



Fuente: Autoría propia

Figura 63: Luego se asigna el grupo de autorización.



Fuente: Autoría propia

Figura 64: Se procede a verificar que coincidan todo con la asignación del grupo de

autorización en la política de acceso del proxy.

Fuente: Autoría propia

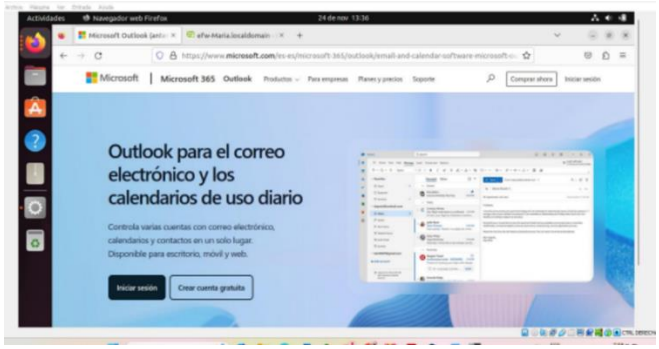
Figura 65: Probar desde la LAN a través de un navegador Web, el acceso a los portales

referenciados en la lista negra.

Por último, se inicia sesión cuando lo solicita y se puede acceder a los sitios web

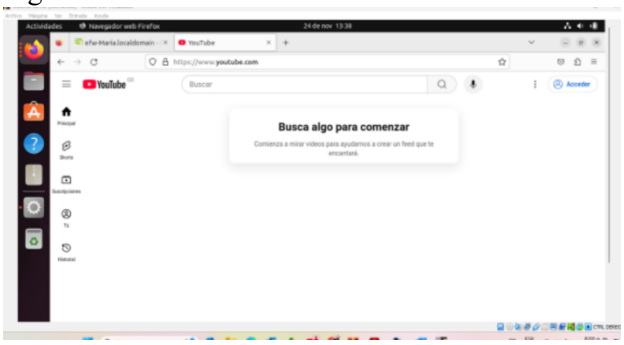
anteriormente bloqueados

hotmail.com



Fuente: Autoría propia

Figura 66: Youtube.com



Fuente: Autoría propia

Figura 67: Elnuevodia.com.co

Fuente: Autoría propia

7. CONCLUSIÓN

Con el desarrollo de este diplomado de profundización en administración de sistemas operativos Open Source con certificación en Linux el estudiante adquirió conocimiento sobre las diferentes distribuciones de GNU/Linux. El uso de estaciones de trabajo y servidores con GNU/Linux lo cual permite optimizar los recursos disponibles, aprovechar software libre de alta calidad y mantener un entorno de red estable y seguro y La implementación de Endian como firewall se entendió la fortaleza en la seguridad y el control del tráfico
Y al colocar a Endian entre la LAN y la WAN proporciona una barrera efectiva contra amenazas externas, permitiendo filtrar y monitorear el tráfico de forma centralizada, y facilitar configuraciones de VPN y reglas de acceso. Y con el uso de una red DMZ con un servidor GNU/Linux mejora la disponibilidad y seguridad de los servicios web y al alojar aplicaciones web y bases de datos en una DMZ separada, se protege la red interna de accesos directos desde Internet, permitiendo a la vez una alta disponibilidad de los servicios públicos sin comprometer la integridad de la LAN

8. BIBLIOGRAFIAS

[1] ***LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix. https://learning.lpi.org/es/learning-materials/101-500/102/***

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

[3] ***Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html***

[4] ***Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/***

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

[6] ***Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/***

[7] ***linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952***