IMPLEMENTANDO SEGURIDAD EN GNU-LINUX USANDO EFW

Santiago Posada Espinosa
e-mail: sposadae@unadvirtual.edu.co
Diego Armando Useche Oyuela
e-mail: dausecheo@unadvirtual.edu.co
Sergio Daniel Polanco Mahecha
e-mail: sdpolancom@unadvirtual.edu.co
Luisa Fernanda Castillo Pacheco
e-mail: lfcastillop@unadvirtual.edu.co
Jorge Itsván Flórez Herrera
e-mail: jiflorez@unadvirtual.edu.co

RESUMEN. En este artículo se describe el desarrollo de una actividad orientada a la implementación de medidas de seguridad mediante el uso de la distribución GNU/Linux Endian Firewall (EFW), donde, se fortalece el conocimiento del sistema operativo GNU/Linux realizando estudios en el módulo 101-500 del material educativo Linux Essentials del Linux Professional Institute (LPI), el objetivo central de la actividad es configurar redes LAN, WAN y DMZ para garantizar la protección de datos y servicios, así como en establecer reglas de control de tráfico, servicios y autenticación mediante proxy, donde se debe documentar paso a paso el proceso de descarga, instalación, configuración y ajuste clave de cada una de las temáticas desarrolladas.

PALABRAS CLAVE: GNU/Linux, seguridad, Endian Firewall, NAT, DMZ, firewall, redes, proxy, HTTP, autenticación, VirtualBox.

ABSTRACT. This article describes the development of a practical activity focused on implementing security measures using the GNU/Linux Endian Firewall (EFW) distribution. Simultaneously, it strengthens knowledge of the GNU/Linux operating system through the study of module 101-500 of the Linux Essentials educational material provided by the Linux Professional Institute (LPI). The main objective of the activity is to configure LAN, WAN, and DMZ networks to ensure data and service protection, as well as to establish traffic control rules, service permissions, and proxy-based authentication. The process involves step-by-step documentation of the download, installation, configuration, and key adjustments associated with each topic addressed.

1 INTRODUCCIÓN

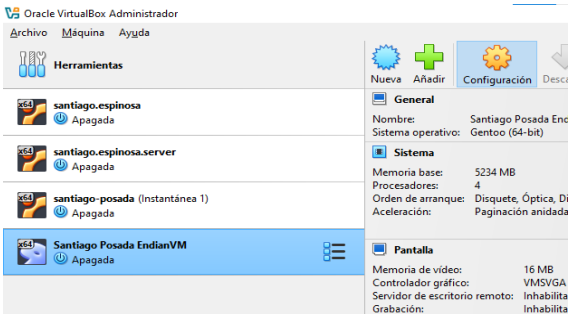
En el desarrollo de esta actividad, se centra en abordar el construir una infraestructura tecnológica para prevenir accesos no autorizados y vulnerabilidades a través de herramientas de control de tráfico y segmentación lógica como las zonas LAN, WAN y DMZ. Para lograrlo, se utilizan soluciones de software libre como Endian Firewall sobre plataformas GNU/Linux, que permiten establecer políticas de seguridad efectivas y flexibles, donde utilizando conocimientos adquiridos en el desarrollo de las temáticas ofrecidas por el Linux Professional Institute, podemos abordar con certeza y eficacia ya que nos plasman circunstancias y de uso diario en el manejo del ecosistema Linux, donde su core se centra por lo general en el área de IT, en alojar servicios de seguridad, gestión y despliegue de software.

2 CONTENIDOS

3 TEMÁTICA 1 - CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX E INSTALACIÓN EFECTIVA DEL MISMO.

Descargar Endian desde su link oficial https://sourceforge.net/projects/efw/ y crear máquina virtual para Endian, después configurar Tarjetas de red -> configuración. Y en la parte superior seleccionamos Expert

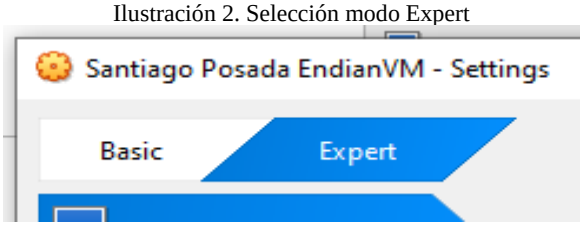
Ilustración 1. Configuración Virtuabox



Fuente: Autoría propia (Santiago Posada Espinosa)

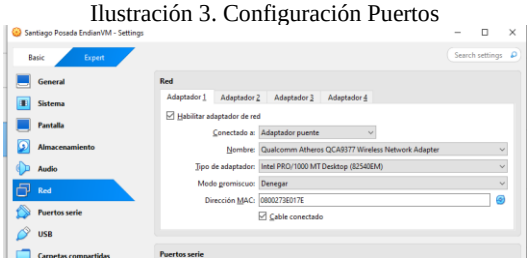
Ahora buscamos el apartado de RED

Ilustración 2. Selección modo Expert



Fuente: Autoría propia (Santiago Posada Espinosa)

Ilustración 3. Configuración Puertos



Fuente: Autoría propia (Santiago Posada Espinosa)

Ahora vemos los 4 puertos, los habilitamos y hacemos la siguiente configuración.

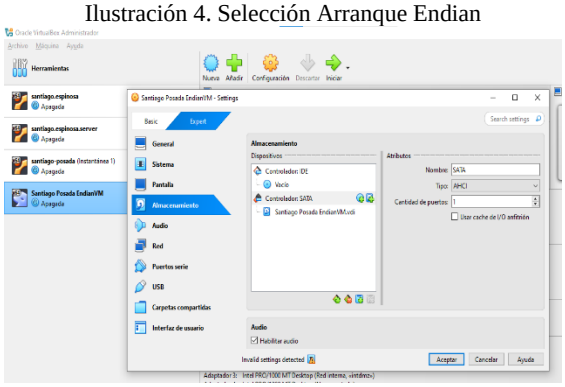
Tabla 1. Configuración de redes

Zona Verde - LAN	Zona Naranja – DMZ	Zona Roja – WAN
Adaptador 1	Adaptador 2	Adaptador 3
Nombre red intlan	Nombre red intdmz	Adaptador Puente
192.168.10.15	192.168.20.1	DHCP

Fuente: Autoría Propia (Santiago Posada Espinosa)

Ahora procedemos a cargar la ISO de Endian como disco de arranque, vamos a configuración -> expert -> almacenamiento

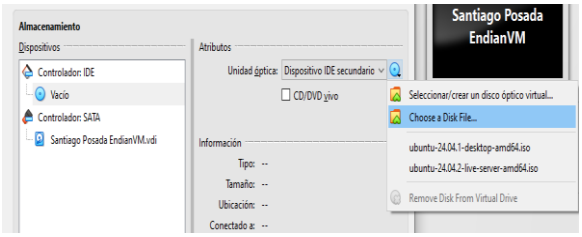
Ilustración 4. Selección Arranque Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

Damos clic en Controlador IDE -> Vacío ahí veremos en la parte derecha el apartado de atributos, ahí damos clic en el icono azul del CD y seleccionamos la opción Choose a Disk File…

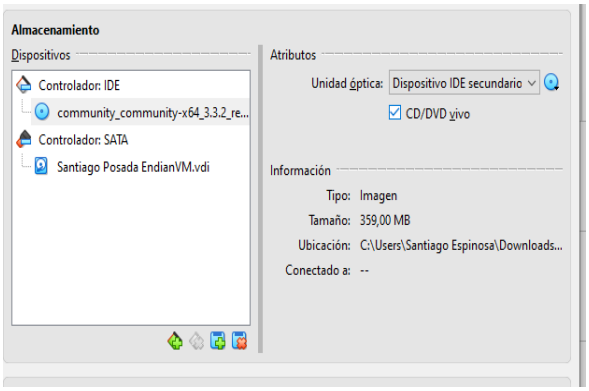
Ilustración 5. Selección Disco



Fuente: Autoría propia (Santiago Posada Espinosa)

Seleccionamos la .iso de Endian y marcamos la opción CD/DVD vivo, o Live CD/DVD, para que el sistema arranque desde la .iso como si fuese un DVD

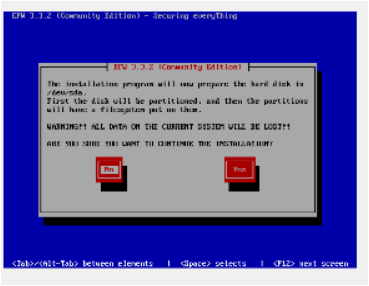
Ilustración 6. Montar Disco Instalación Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

Iniciamos la maquina e iniciamos con instalación de Endian

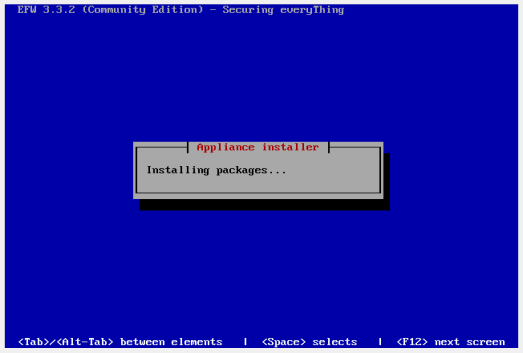
Ilustración 7. Inicio instalación Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

Particionará el disco, y la instalación de Ubuntu original se perderá, pero como arrancamos desde CD no habría lio, seleccionamos YES, esto iniciará a instalar paquetería

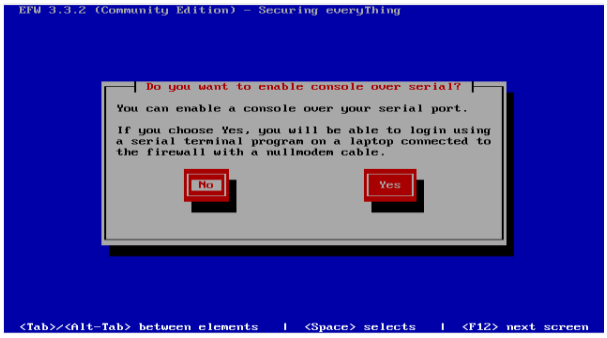
Ilustración 8. Descomprimiendo paquetes Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

En este caso, seleccionamos NO, ya que en VirtualBox no usamos consola serial, ya que el acceso se hará por la consola directa de la VM o por navegador web después de la instalación via IP, además evitamos configurar algo innecesario que puede generar confusión más adelante.

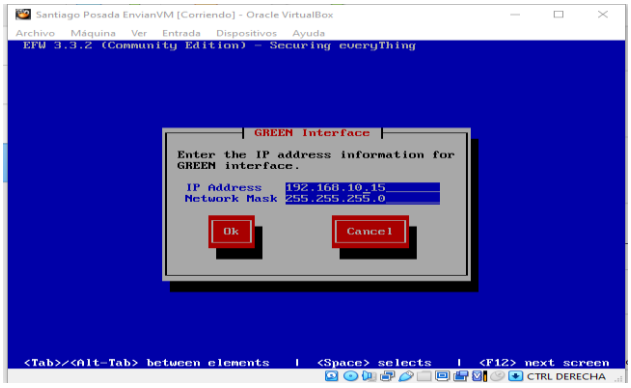
Ilustración 9. Advertencia Consola sobre Serial



Fuente: Autoría propia (Santiago Posada Espinosa)

Procedemos a configurar la IP de la red verde. en este caso usaremos la red que también use el usuario de Ubuntu desktop, dejaré la IP por defecto que pone, la cual la obtiene del adaptador puente, esto para no enredarnos después con permisos o fallos en firewall y no poder acceder al puerto de endian donde permite realizar su administración

Ilustración 10. IP red verde



Fuente: Autoría propia (Santiago Posada Espinosa)

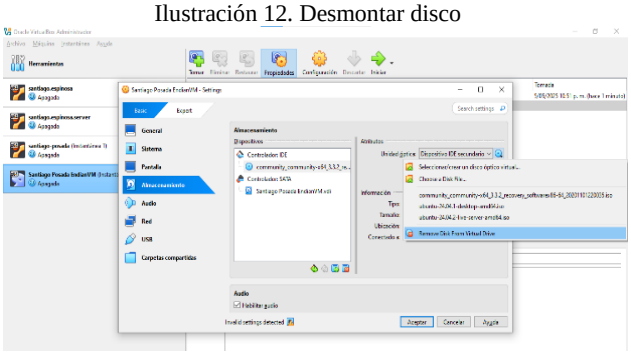
Se aplicarán los cambios y nos enviara un mensaje satisfactorio

Ilustración 11. Instalacion Exitosa de Endian

Fuente: Autoría propia (Santiago Posada Espinosa)

Ahora esperamos, el Endian hará reboot solo, podríamos apagar la máquina virtual y tomar una instantánea por seguridad., después, vamos a la configuración de VirtualBox, Configuración -> Almacenamiento -> seleccionamos “Quitar disco del dispositivo”.

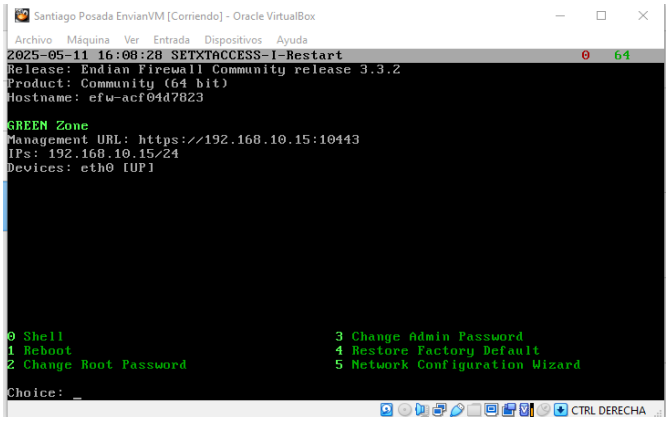
Ilustración 12. Desmontar disco



Fuente: Autoría propia (Santiago Posada Espinosa)

Guardamos y volvemos a iniciar la máquina.

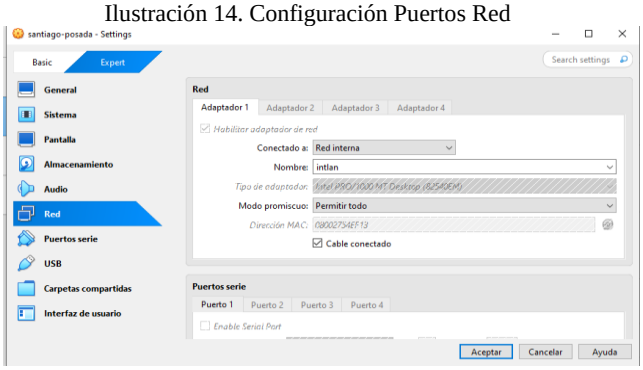
Ilustración 13. Interfaz Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

Ahora intentaremos acceder al panel de configuración del endian desde la maquina Ubuntu desktop, esta también debe de estar configurada para enlazarnos con nuestro adaptador puente de esta manera

Ilustración 14. Configuración Puertos Red



Fuente: Autoría propia (Santiago Posada Espinosa)

Modo promiscuo en permitir todo y que el adaptador 1 esté usando una IP del mismo segmento de red que el endian y conectado a la red intlan.

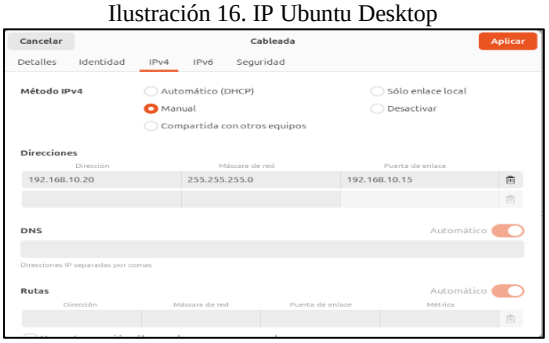
En la maquina desktop, tendremos que configurar la red IPv4 en el mismo segmento de la red de Endian, iremos a configuración de red

Ilustración 15. Configurar Red Ubuntu Desktop

Fuente: Autoría propia (Santiago Posada Espinosa)

Opciones de red cableada y le daremos una IP en el segmento del Endian

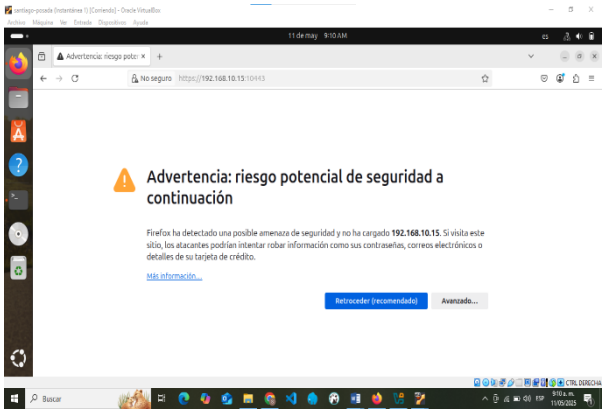
Ilustración 16. IP Ubuntu Desktop



Fuente: Autoría propia (Santiago Posada Espinosa)

Una vez hecho esto, iremos al navegador y pondremos la IP configurada en el Endian y su puerto de acceso, el cual es 10443, en este caso https://192.168.10.15:10443, donde si todo es exitoso, veremos un mensaje de advertencia del navegador.

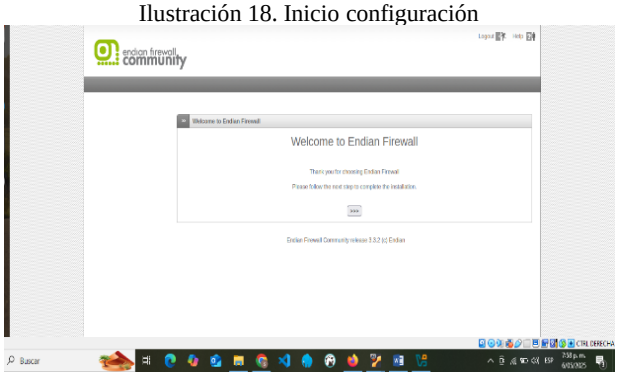
Ilustración 17. Acceso a Interfaz Administración Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

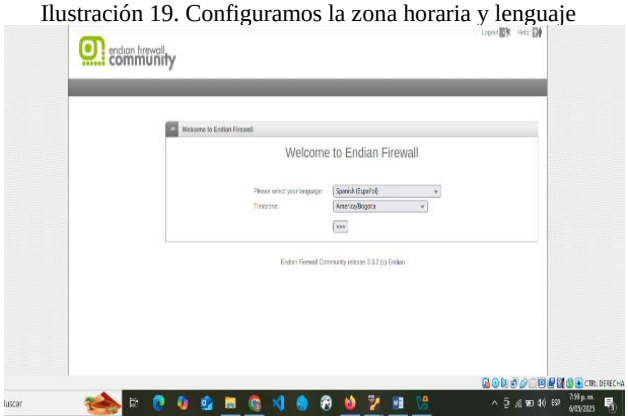
Daremos donde dice Avanzado… y después en aceptar y continuar, esto nos dará acceso al panel de endian

Ilustración 18. Inicio configuración



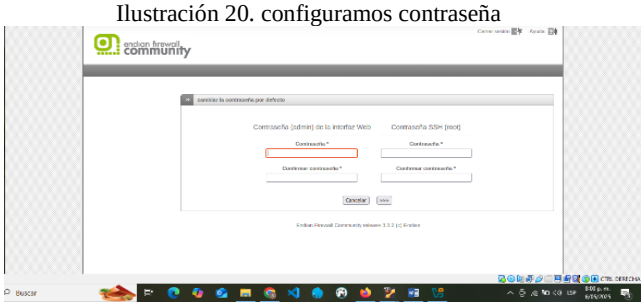
Fuente: Autoría propia (Santiago Posada Espinosa)

Ilustración 19. Configuramos la zona horaria y lenguaje



Fuente: Autoría propia (Santiago Posada Espinosa)

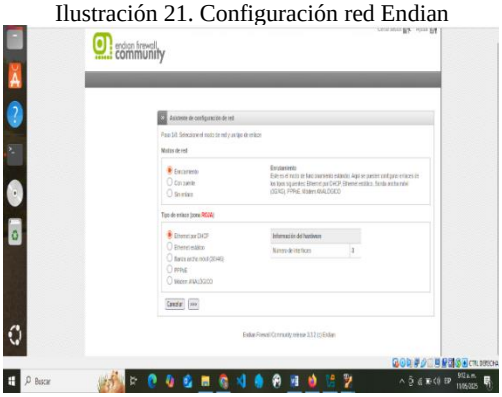
Ilustración 20. configuramos contraseña



Fuente: Autoría propia (Santiago Posada Espinosa)

Ingresamos nueva contraseña tanto para el servicio de interfaz web como de SSH, en mi caso, tienen que tener mínimo 6 caracteres, una vez ya ingresada la contraseña, nos pedirá confirmar la configuración de la red Roja, por defecto dejamos así.

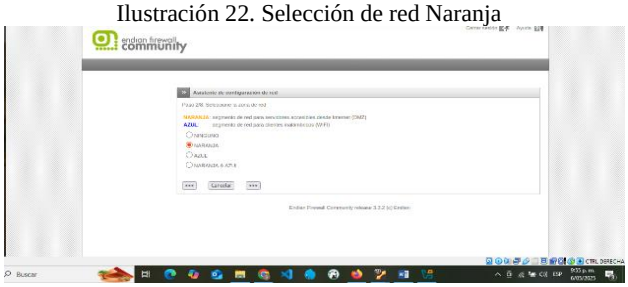
Ilustración 21. Configuración red Endian



Fuente: Autoría propia (Santiago Posada Espinosa)

En el paso 2, nos pedirá seleccionar que configuración de red adicional añadiremos al Endian

Ilustración 22. Selección de red Naranja

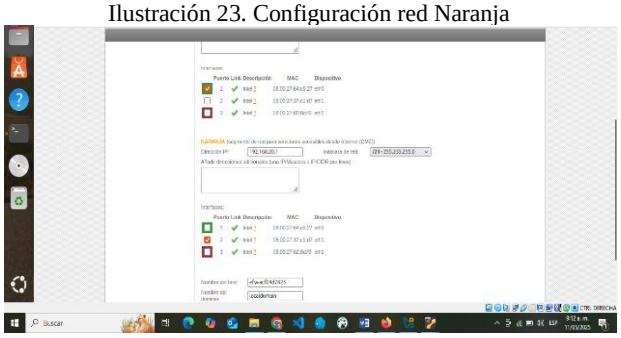


Fuente: Autoría propia (Santiago Posada Espinosa)

Seleccionaremos el check de la casilla NARANJA ya que esta corresponde al servidor DMZ

En el siguiente paso desplegará un menú donde configuraremos las IP de las redes NARANJA y podemos también editar la configuración de la red VERDE si fuese necesario

Ilustración 23. Configuración red Naranja



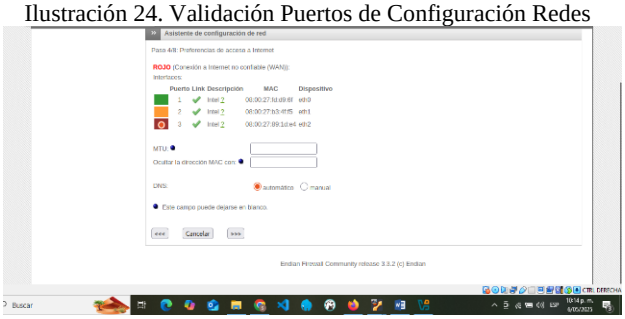
Fuente: Autoría propia (Santiago Posada Espinosa)

Para la IP NARANJA usé la IP: 192.168.20.1 y máscara: 255.255.255.0

Por defecto endian nos configurará las redes ya ocupadas y asignadas, dejándonos el puerto libre sin un color en su borde, dichos colores indican que puerto está ocupado por qué zona, seleccionaremos en mi caso el puerto eht1, y ajustaremos la configuración posteriormente en el virtualbox de nuevo

Nos llevara a la confirmación y de las zonas seleccionadas, y veremos unos campos como MTU, Dirección MAC y DNS, los cuales dejaremos en blanco a no ser que requiramos una configuración manual de alguno de estos.

Ilustración 24. Validación Puertos de Configuración Redes



Fuente: Autoría propia (Santiago Posada Espinosa)

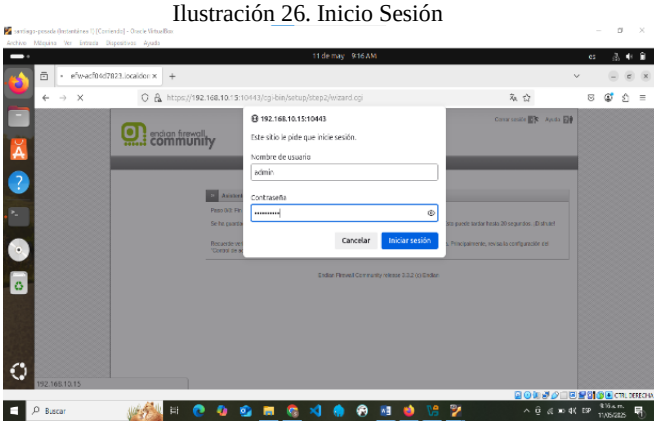
Continuamos con la configuración de servicios de correo, los cuales dejaremos en blanco porque no son necesarios

Ilustración 25. Configuración DNS

Fuente: Autoría propia (Santiago Posada Espinosa)

Ahora nos pedirá iniciar sesión

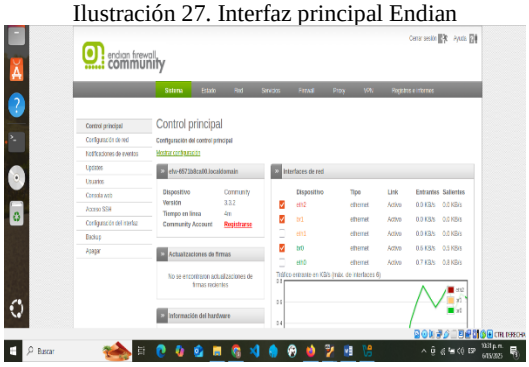
Ilustración 26. Inicio Sesión



Fuente: Autoría propia (Santiago Posada Espinosa)

Iniciaremos con admin y la contraseña que hayamos ingresado en los pasos anteriores.

Ilustración 27. Interfaz principal Endian

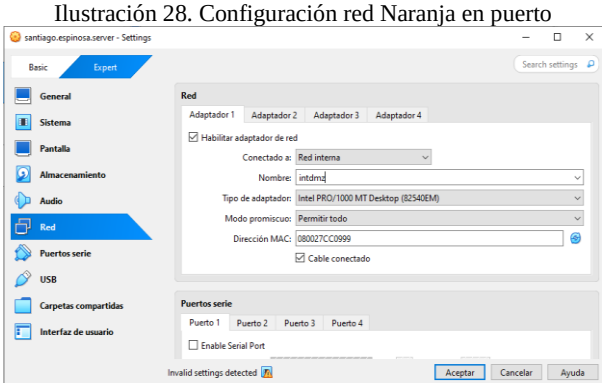


Fuente: Autoría propia (Santiago Posada Espinosa)

Nos desplegará un dashboard con la información, desde donde podremos modificar las redes y demás facultades de administración del endian.

Ahora configuramos nuestra maquina Ubuntu server con la Ip asignada a la red naranja

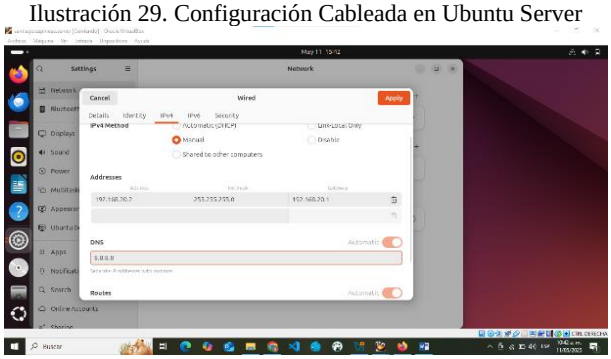
Ilustración 28. Configuración red Naranja en puerto



Fuente: Autoría propia (Santiago Posada Espinosa)

En el adaptador 1 seleccionamos la red interna y guardamos la configuración e iniciamos la máquina, donde posteriormente, configuraremos su segmento de red de acuerdo al configurado en Endian, es decir podríamos usar cualquiera dentro del segmento 192.168.20.x, y una máscara de subred de 255.255.255.0 con el gateway la cual sería la ip dmz 192.168.20.1

Ilustración 29. Configuración Cableada en Ubuntu Server



Fuente: Autoría propia (Santiago Posada Espinosa)

Ilustración 30. Ping a Gateway Ubuntu Server

Fuente: Autoría propia (Santiago Posada Espinosa)

Con esto tendríamos la segmentación realizada y preparada para la implementación de las demás temáticas.

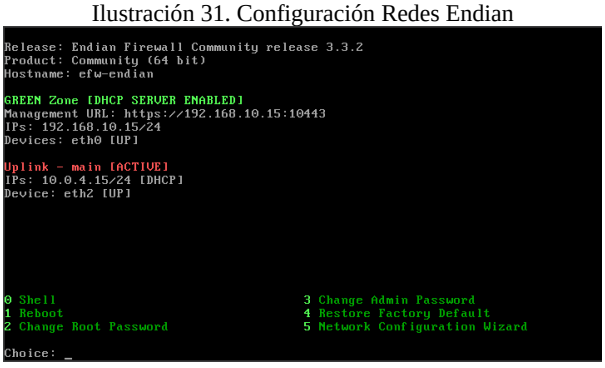
4 TEMÁTICA 2: CONFIGURACIÓN NAT.

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).

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.

Ya teniendo la previa configuración de las direcciones de red en el Endian Firewall

Ilustración 31. Configuración Redes Endian



Fuente: Autoría propia (Jorge Flórez)

En el servidor Ubuntu Server

Ilustración 32. Configuración Red Ubuntu Server

Fuente: Autoría propia (Jorge Flórez)

Y en el Cliente Ubuntu Desktop

Ilustración 33. Configuración Red Ubuntu Desktop

Fuente: Autoría propia (Jorge Flórez)

Procedemos a la configuración del firewall de Endian y creamos la regla NAT para la comunicación de la LAN (zona verde) hacia la WAN (zona roja) y la creación de la regla NAT para la comunicación de la zona DMZ (zona naranja o desmilitarizada) hacia la WAN (zona roja).

Ilustración 34. Configuración Firewall Endian

Fuente: Autoría propia (Jorge Flórez)

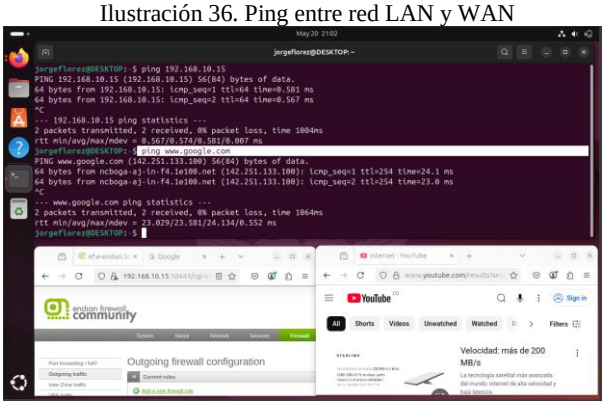
Evidenciamos reenvío de puertos DMZ – WAN

Ilustración 35. Ping entre red DMZ y red WAN

Fuente: Autoría propia (Jorge Flórez)

Y evidenciamos reenvío de puertos LAN – WAN

Ilustración 36. Ping entre red LAN y WAN



Fuente: Autoría propia (Jorge Flórez)

5 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

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

Ilustración 37. Configuración Puertos HTTP y FTP (1)

Fuente: Autoría propia (Sergio Daniel Polanco Mahecha)

Ilustración 37. Configuración Puertos HTTP y FTP (2)

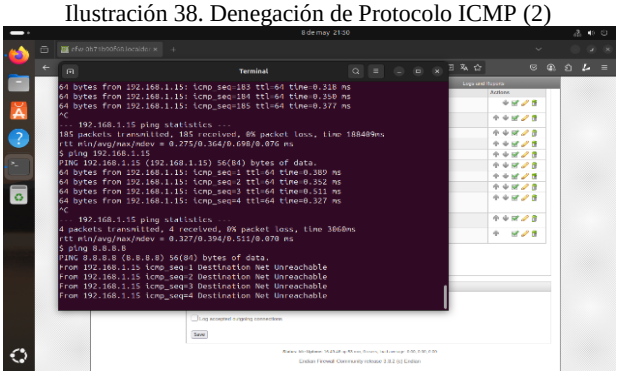
Fuente: Autoría propia (Sergio Daniel Polanco Mahecha)

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

Ilustración 38. Denegación de Protocolo ICMP (1)

Fuente: Autoría propia (Sergio Daniel Polanco Mahecha)

Ilustración 38. Denegación de Protocolo ICMP (2)



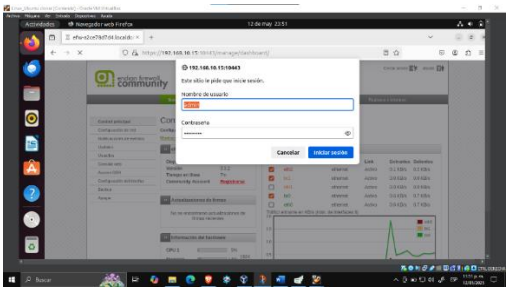
Fuente: Autoría propia (Sergio Daniel Polanco Mahecha)

6 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO. PRODUCTO ESPERADO:

Comunicar la zona Verde con la zona Naranja (HTTP y FTP) permitir el tráfico desde LAN (verde) hacia DMZ (naranja) usando HTTP (puerto 80) y FTP (puerto 21).

Pasos, ingresa a la interfaz web de Endian, luego navega a https://192.168.10.15:10443, inicia sesión como administrador.

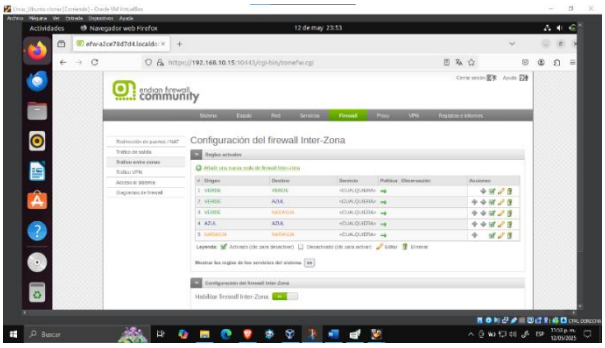
Ilustración 39. Inicio Sesión en Endian



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Vamos al menú: Menú → Firewall → Reglas entre zonas Haz clic en “Agregar nueva regla” (Add a new rule)

Ilustración 40. Panel Administración Firewall



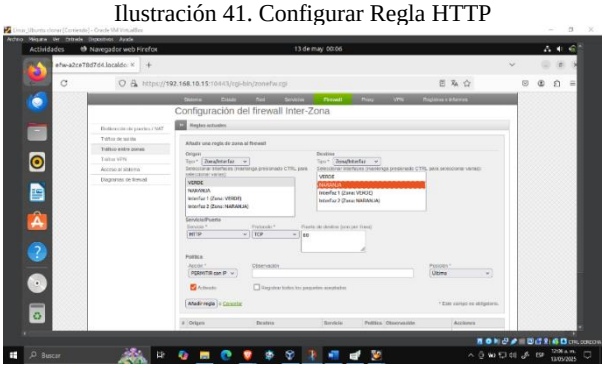
Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Tabla 2. Configuración Zonas

Origen	Zona Verde (LAN)
Destino	Zona Naranja (DMZ)
Servicio	HTTP (80)
Acción	Permitir con IP
Protocolo	TCP

Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 41. Configurar Regla HTTP



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 42. Confirmación Regla HTTP

Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

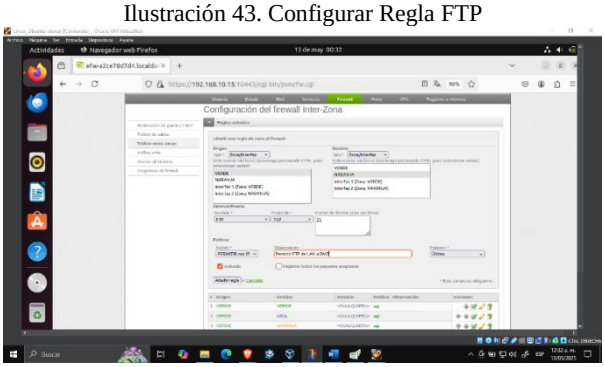
Repite el proceso para FTP:

Tabla 3. Configuración Zona FTP

Origen	Zona Verde (LAN)
Destino	Zona Naranja (DMZ)
Servicio	FTP (21)
Acción	Permitir con IP
Protocolo	TCP

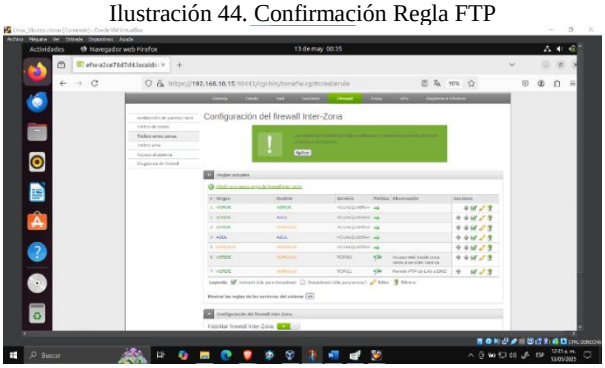
Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 43. Configurar Regla FTP



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 44. Confirmación Regla FTP



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Comunicar la zona Internet (Roja) con la zona DMZ (Naranja)

Tabla 4. Configuración Zonas - WAN

Origen	Zona Roja (WAN)
Destino	Zona Naranja (DMZ)
Servicio	HTTP (80)
Acción	Permitir con IP
Protocolo	TCP

Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 44. Configuración Comunicación Zona ROJA con DMZ

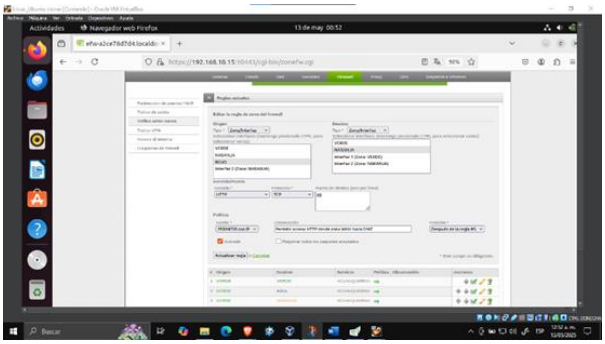
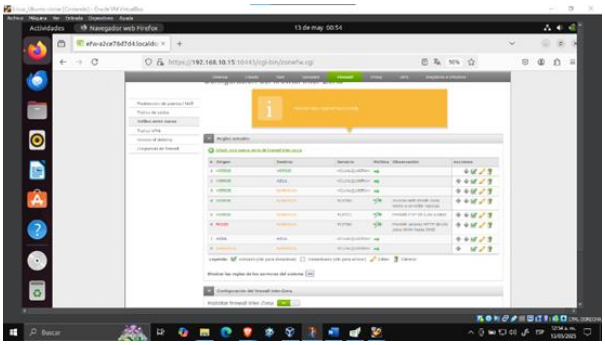


Ilustración 38. Comunicar Zona Roja

Ilustración 45. Validación Comunicación Zona ROJA con DMZ



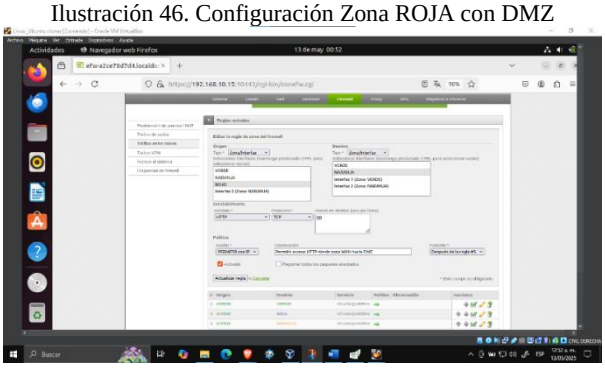
Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Tabla 5. Configuración Zonas WAN - DMZ

Origen	Zona Roja (WAN)
Destino	Zona Naranja (DMZ)
Servicio	FTP (21)
Acción	Permitir con IP
Protocolo	TCP

Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

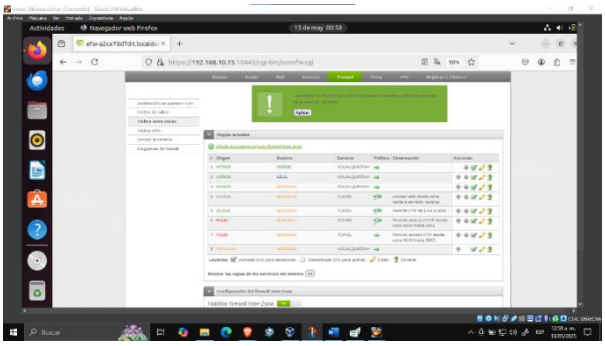
Ilustración 46. Configuración Zona ROJA con DMZ



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Verificar en el tráfico Inter-Zona la creación de reglas, me dirijo a firewall – Reglas entre zonas y observó el listado completo de reglas agregadas.

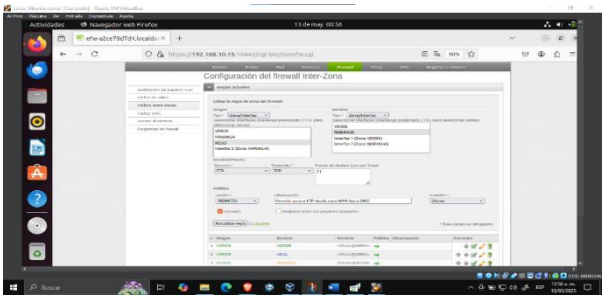
Ilustración 47. Trafico entre zonas



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

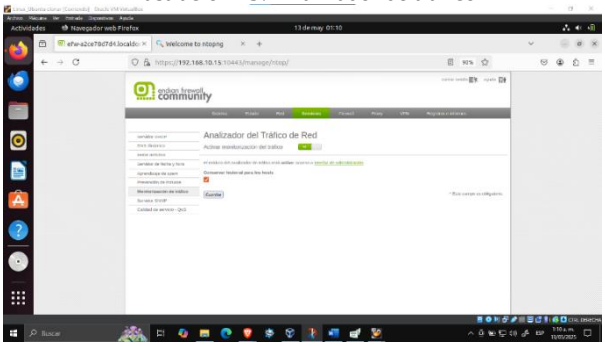
Verificamos la monitorización de tráficos, nos dirigimos a la ventana servicios y dentro de servicios activamos monetización de tráfico en la interfaz administración.

Ilustración 48. Monetización de trafico



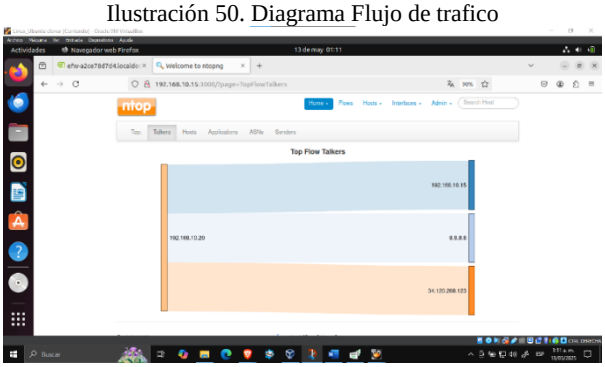
Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 49. Analizador de trafico



Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

Ilustración 50. Diagrama Flujo de trafico

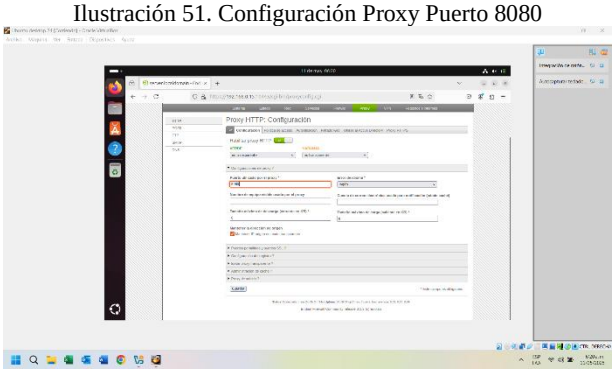


Fuente: Autoría propia (Luisa Fernanda Castillo Pacheco)

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

En este paso procedemos a la configuración del proxy HTTP. Se deja solo establecido el puerto 8080.

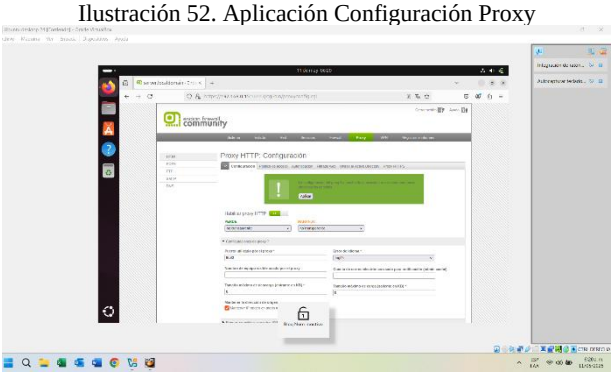
Ilustración 51. Configuración Proxy Puerto 8080



Fuente: Autoría propia (Diego Armando Useche Oyuela)

Una vez configurado el puerto y las dos opciones de la red Naranja y Verde “No transparente”. Aplicamos configuración.

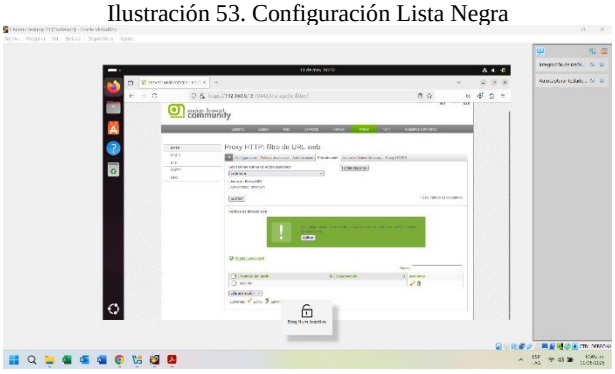
Ilustración 52. Aplicación Configuración Proxy



Fuente: Autoría propia (Diego Armando Useche Oyuela)

Luego pasamos a la pestaña de "filtrado web", donde seleccionamos a cada hora, en la opción de rutina de actualizaciones. Seguidamente creamos un perfil adicionando en la lista negra las paginas a restringir www.hotmail.com, www.youtube.com, www.elnuevodia.com.co, el perfil fue nombrado "security".

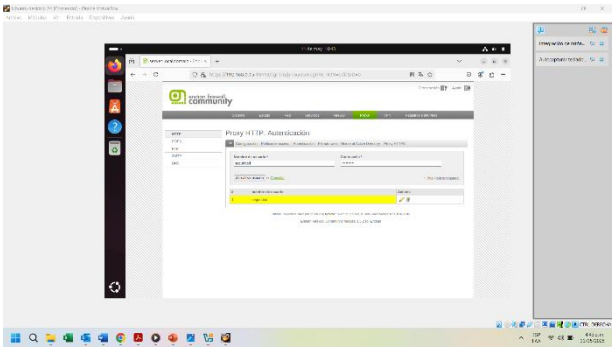
Ilustración 53. Configuración Lista Negra



Fuente: Autoría propia (Diego Armando Useche Oyuela)

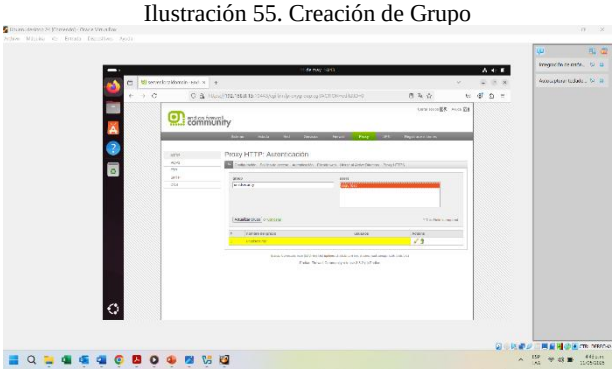
En esta pestaña de "Autenticación", creamos un usuario y un grupo que a continuación se relaciona en las imágenes.

Ilustración 54. Creación de Usuario



Fuente: Autoría propia (Diego Armando Useche Oyuela)

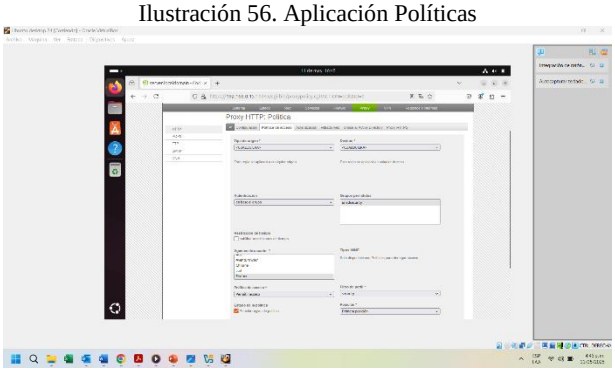
Ilustración 55. Creación de Grupo



Fuente: Autoría propia (Diego Armando Useche Oyuela)

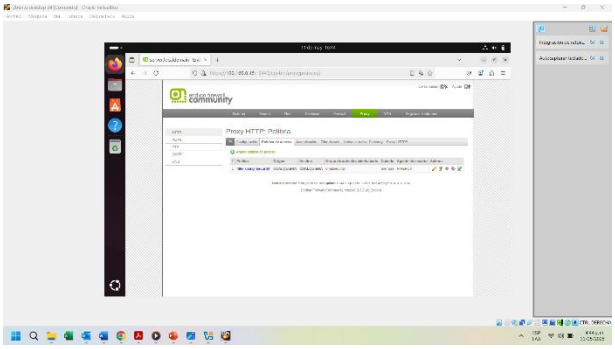
Por último, pasamos a la pestaña "Política de acceso", aquí seleccionamos las dos opciones iniciales <CUALQUIERA>, en la opción de autenticación, seleccionamos el grupo que creamos "unadsecurity". En la opción agente de usuario, seleccionamos el navegador Firefox, posteriormente seleccionamos en filtro de perfil, "security". Y guardamos cambios.

Ilustración 56. Aplicación Políticas



Fuente: Autoría propia (Diego Armando Useche Oyuela)

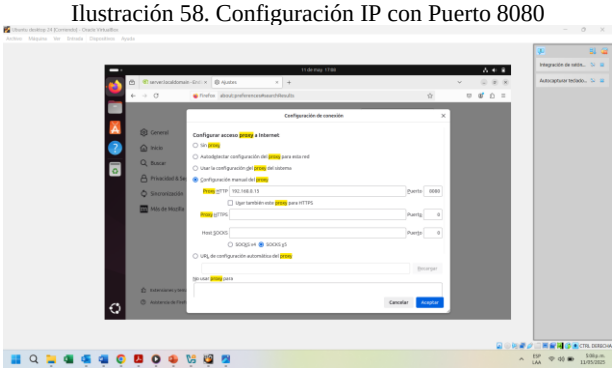
Ilustración 57. Visualización Política Creada



Fuente: Autoría propia (Diego Armando Useche Oyuela)

Por último, configuramos la dirección IP 192.168.0.15, con el puerto 8080, en el navegador Firefox del Ubuntu desktop.

Ilustración 58. Configuración IP con Puerto 8080

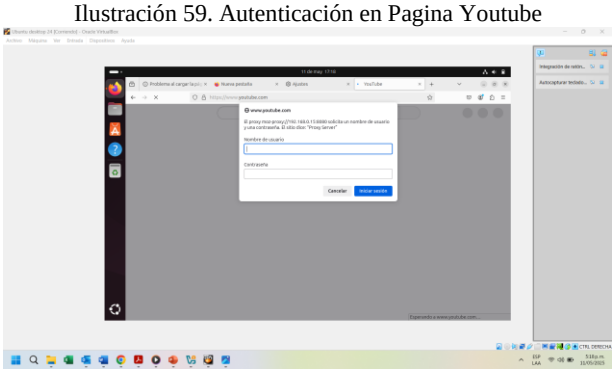


Fuente: Autoría propia (Diego Armando Useche Oyuela)

Procedemos hacer las pruebas, cargando las páginas www.hotmail.com, www.youtube.com, www.elnuevodia.com.co.

Evidencia de la solicitud de autenticación en la página de www.youtube.com.

Ilustración 59. Autenticación en Pagina Youtube



Fuente: Autoría propia (Diego Armando Useche Oyuela)

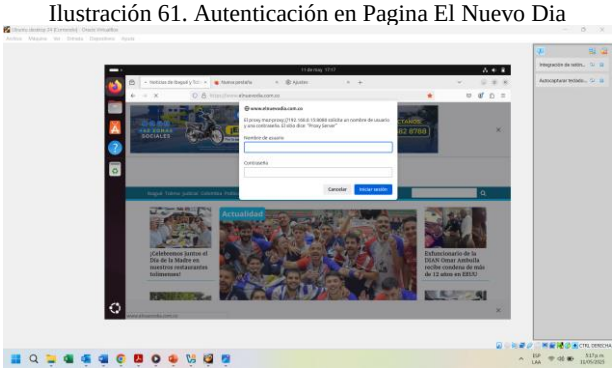
Si no registra el usuario la contraseña asignada, no permite la navegación.

Ilustración 60. Demostración de Ingreso Youtube

Fuente: Autoría propia (Diego Armando Useche Oyuela)

Evidencia de la solicitud de autenticación en la pagina www.elnuevodia.com.co.

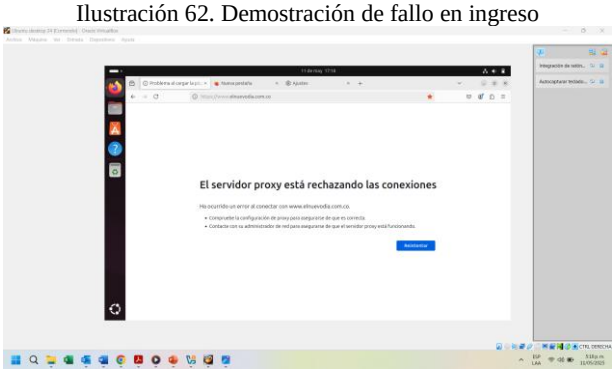
Ilustración 61. Autenticación en Pagina El Nuevo Dia



Fuente: Autoría propia (Diego Armando Useche Oyuela)

Si, no registra el usuario la contraseña asignada, no permite la navegación.

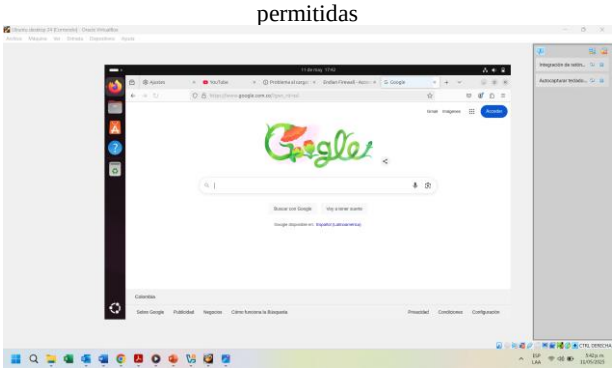
Ilustración 62. Demostración de fallo en ingreso



Fuente: Autoría propia (Diego Armando Useche Oyuela)

Navegación por el buscador Google.com.

Ilustración 63. Validación de navegación en páginas permitidas



Fuente: Autoría propia (Diego Armando Useche Oyuela)

8 CONCLUSIONES

La distribución Endian Firewall demostró ser una solución eficiente para la implementación de seguridad y segmentación de redes, ya que permitió establecer una separación clara entre las zonas LAN, DMZ y, potencialmente, WAN.

La implementación de reglas de acceso en Endian permitió comprender de forma práctica la gestión del tráfico entre zonas de red diferenciadas por niveles de seguridad y

funcionalidad. Aunque no se contó con una zona Roja (WAN) activa, fue posible configurar y simular reglas entre la zona Verde (LAN) y la zona Naranja (DMZ), permitiendo así servicios como HTTP y FTP de manera controlada.

Las temáticas abordadas durante la práctica evidenciaron la importancia de definir políticas de acceso, monitorear servicios y emplear herramientas de control de tráfico, para garantizar la integridad, disponibilidad y seguridad de los recursos dentro de un entorno de red administrado.

El uso del material de Linux Essentials fortaleció significativamente los conocimientos sobre el entorno de línea de comandos en GNU/Linux, una competencia clave para la administración de servidores y redes.

Esta experiencia permitió integrar conocimientos teóricos y prácticos en un entorno real de red, lo que favoreció el desarrollo de habilidades técnicas aplicables en el campo de la ciberseguridad y la gestión de infraestructuras IT.

El trabajo colaborativo y el análisis reflexivo durante las configuraciones promovieron una mayor comprensión del rol de los firewalls dentro de una arquitectura de red, además de fomentar la toma de decisiones fundamentadas en criterios de seguridad y eficiencia.

9 REFERENCIAS

[1] LPI, "LPIC-1 Exam 101: Tema 101 - Arquitectura del Sistema," 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/101/

[2] LPI, "LPIC-1 Exam 101: Tema 102 - Instalación de Linux y gestión de paquetes," 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/102/

[3] Canonical, "Guía del Ubuntu Desktop 20.04 LTS," Help Ubuntu, 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[4] Debian, "El manual del administrador de Debian 12.5.0," 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html

[5] Oracle, "Manual de usuario VirtualBox," 2020. [Online]. Available: https://www.virtualbox.org/manual/

[6] J. LaCroix, *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*, Packt Publishing, 2020. [Online]. Available: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[7] IBM, "Introducción a Linux," IBM SkillsBuild, 2021. [Online]. Available: https://skillsbuild.org/learning-paths/linux

[8] Endian Firewall Community, "Endian Firewall Documentation," 2021. [Online]. Available: https://wiki.endian.com/Community/

[9] C. Negus, *Linux Bible*, 10th ed., Wiley, 2020. [Online]. Available: https://www.wiley.com/en-us/Linux+Bible%2C+10th+Edition-p-9781119578888

[10] Cisco Systems, "Conceptos básicos de redes: Guía del estudiante," Cisco Networking Academy, 2022. [Online]. Available: https://www.netacad.com/courses/packet-tracer

[11] W. E. Shotts, *The Linux Command Line: A Complete Introduction*, 2nd ed., No Starch Press, 2019. [Online]. Available: https://nostarch.com/tlcl2