IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Narly Julieth Parra Diaz
njparrad@unadvirtual.edu.co
Diego Andres Arias Sanabria
daariassana@unadvirtual.edu.co
Jesus Esteban Riascos Urbano
jeriascosu@unadvirtual.edu.co
Yennifer Alexandra Melo Castiblanco
yameloc@unadvirtual.edu.co
Fanny Julieth Uribe Gil
fjuribeg@unadvirtual.edu.co

RESUMEN: *El presente trabajo académico describe la infraestructura de la seguridad perimetral utilizando el firewall GNU/Linux Endian con zonas RED, GREEN y ORANGE, con el fin de proteger los servidores internos y permitir servicios controlados desde la WAN y la DMZ. Cada instancia fue configurada en VirtualBox, definiendo direccionamientos IP coherentes para la LAN, WAN y DMZ. Se implementaron reglas de NAT para permitir la comunicación desde la LAN hacia la WAN y desde la DMZ hacia Internet, verificando su funcionamiento mediante pruebas de conectividad. Además, se configuraron servicios web y FTP en la DMZ, así como reglas de acceso que permiten o restringen protocolos entre zonas. Los resultados evidencian el correcto funcionamiento del firewall y la efectividad de la segmentación de zonas para garantizar seguridad y control del tráfico.*

PALABRAS CLAVE: DMZ, Endian Firewall, LAN, NAT, Seguridad Perimetral, Servidor Ubuntu, VirtualBox, WAN.

1 INTRODUCCIÓN

La seguridad perimetral es la primera línea de defensa en cualquier infraestructura de red. En un mundo donde las amenazas avanzan más rápido que las excusas, proteger los sistemas no es un lujo: es una obligación. Por eso, el uso de firewalls y gestores de tráfico se convierte en un pilar estratégico para mantener la integridad, disponibilidad y confiabilidad de los servicios digitales. Dentro del ecosistema de soluciones libres, Endian Firewall/UTM sobresale al unificar filtrado, control de acceso, proxy, VPN, monitoreo y segmentación en una sola plataforma robusta y administrable.

Esta actividad académica emplea Oracle VirtualBox como entorno de virtualización para instalar y configurar Endian en una arquitectura dividida por zonas: Verde (LAN interna), Roja (acceso WAN) y Naranja (DMZ para servicios expuestos). Esta estructura permite entender con claridad cómo opera un firewall como escudo perimetral y cómo se aplican, en la práctica, conceptos clave como NAT, políticas de acceso, filtrado de contenido, gestión de servicios y análisis del tráfico entre redes.

El trabajo desarrollado fortaleció la mirada crítica y operativa sobre la administración de redes, impulsando la adopción de buenas prácticas, documentación técnica y gestión colaborativa. Además, evidenció el valor real del software libre como herramienta eficaz para proteger, organizar y optimizar los sistemas informáticos en entornos académicos y profesionales.

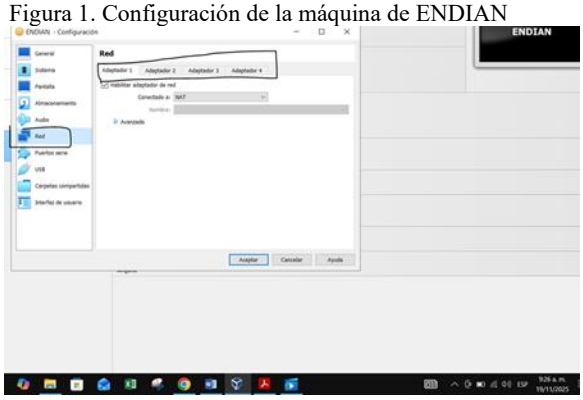
2 INSTALACIÓN ENDIAN

Configuración de la instancia para GNU/Linux Endian
en Virtualbox (tarjetas de red) e instalación efectiva del mismo.
Lo primero que se debe hacer es descargar el ISO de endian desde su página principal https://www.endian.com/en/community/ y luego se debe configurar en la máquina virtualbox las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

3 TEMÁTICA 1

Producto esperado:
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).

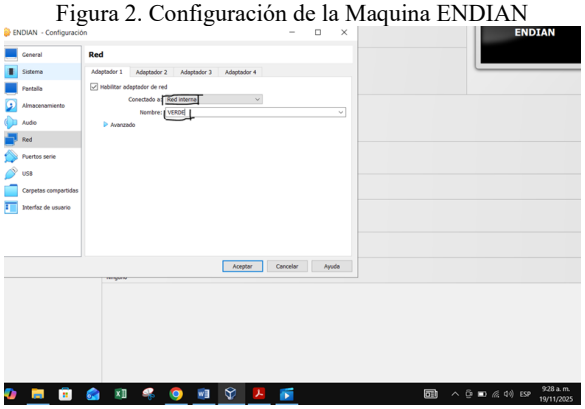
Figura 1. Configuración de la máquina de ENDIAN



Fuente Autoría Propia

Creamos una nueva máquina llamada ENDIAN y comenzamos en el apartado de configuraciones, en la opción de red y es ahí donde vamos a designar los adaptadores que va a conectar.

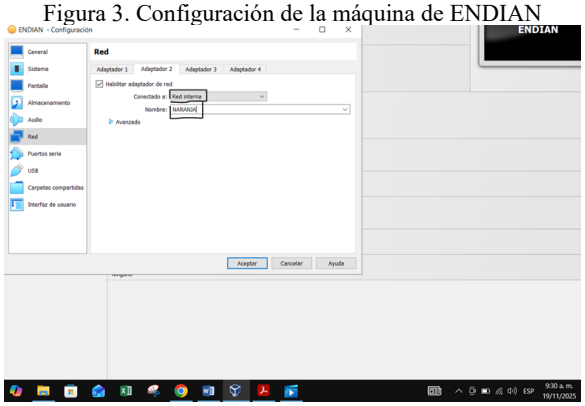
Figura 2. Configuración de la Maquina ENDIAN



Fuente: Autoría Propia

Seleccionamos el adaptador 1 que va a ser la zona verde: Red Interna (LAN) y se cambia el nombre a VERDE.

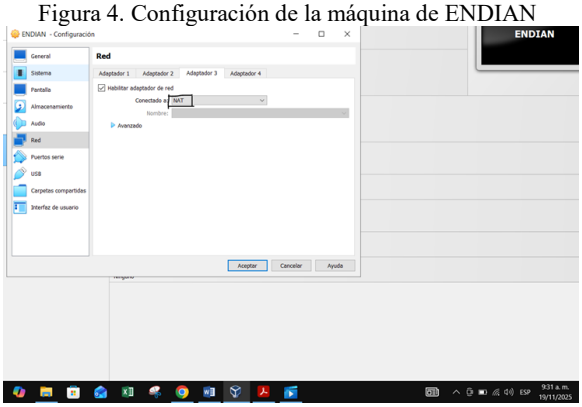
Figura 3. Configuración de la máquina de ENDIAN



Fuente: Autoría propia

Seleccionamos el adaptador 2 que va ser la zona Naranja: Servidores (DMZ) y se da el nombre de Naranja.

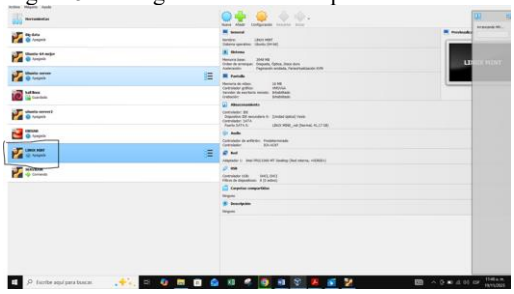
Figura 4. Configuración de la máquina de ENDIAN



Fuente: Autoría propia

Seleccionamos el adaptador 3 el cual va a ser la Zona roja: Acceso a internet

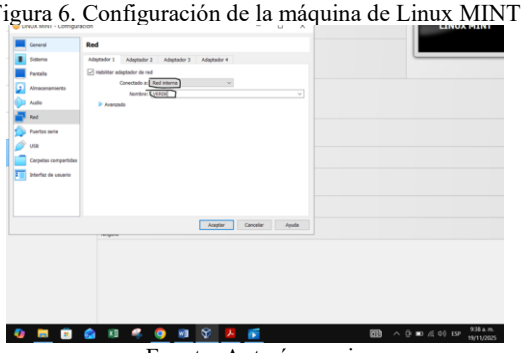
Figura 5. Configuración de la máquina Linux MINT



Fuente: Autoría propia

Creamos una máquina nueva la cual va a contener el Linux MINT

Figura 6. Configuración de la máquina de Linux MINT



Fuente: Autoría propia

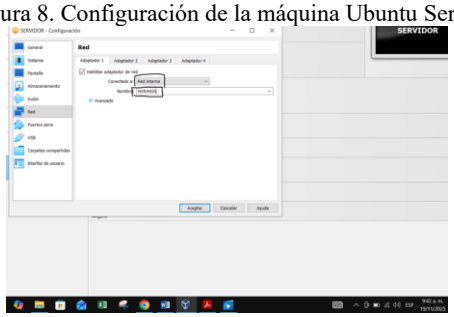
En el adaptador seleccionamos la red interna verde previamente configurada en el ENDIAN que es con la cual va a trabajar el Linux MINT

Figura 7. Configuración de la máquina Ubuntu Server

Fuente: Autoría propia

En el adaptador se selecciona la red interna verde previamente configurada en la maquina virtual ENDIAN que es con la cual se trabaja el Linux MINT.

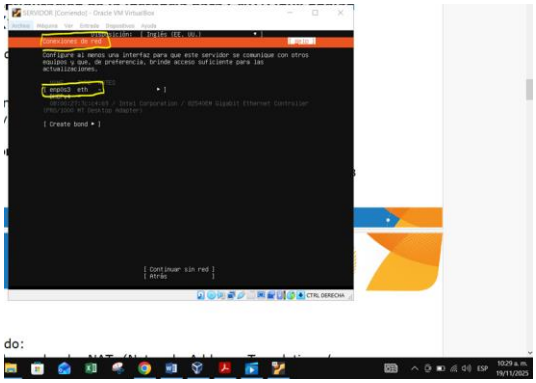
Figura 8. Configuración de la máquina Ubuntu Server



Fuente: Autoría propia

En el apartado de adaptador selecciono la red interna naranja

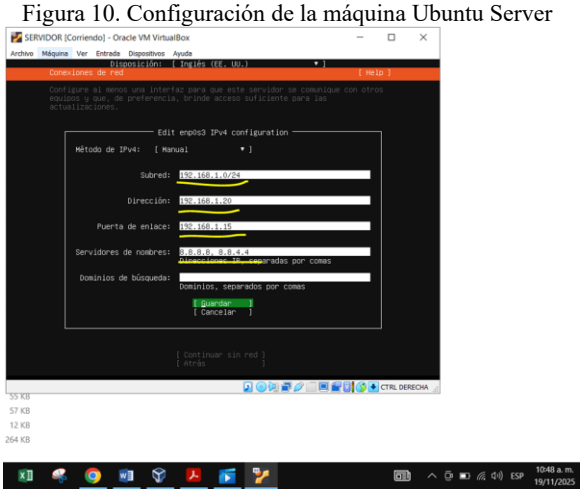
Figura 9. Configuración de la máquina Ubuntu Server



Fuente: Autoría propia

En la instalación del ubuntu server en el apartado de conexiones de red y vamos a configurar el eth de forma manual

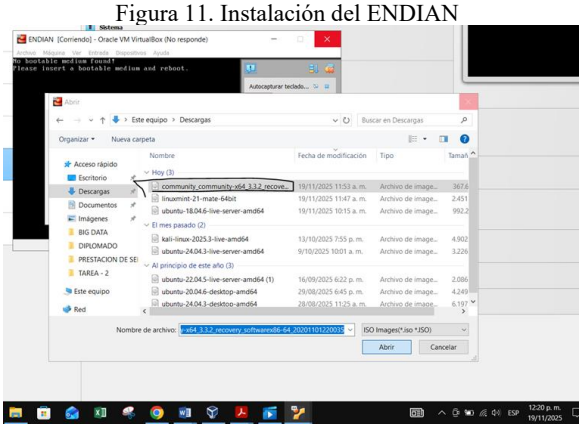
Figura 10. Configuración de la máquina Ubuntu Server



Fuente: Autoría propia

Llenamos los campos de subred, escogemos una dirección, y una puerta de enlace. En los servidores escogemos el de Google que es 8.8.8.8, 8.8.4.4

Figura 11. Instalación del ENDIAN



Fuente: Autoría propia

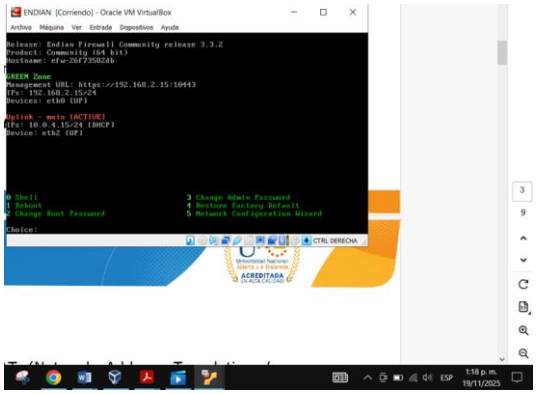
Después de configurar la máquina de ENDIAN procedemos con su instalación

Figura 12. Instalación del ENDIAN

Fuente: Autoría propia

En el aparto de la IP colocamos 192.168.2.15 que es la ip seleccionada para trabajar con las demas maquinas

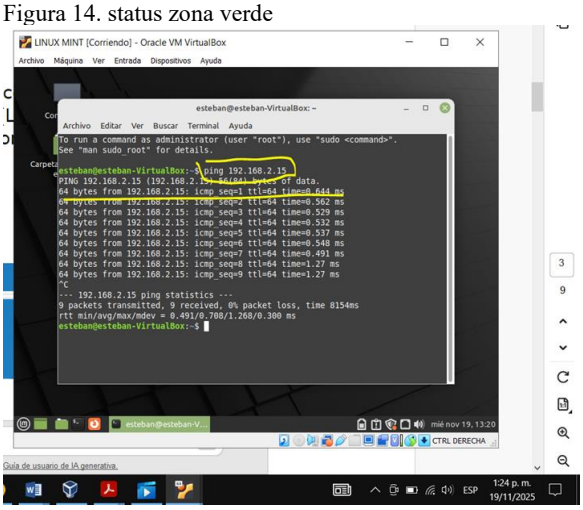
Figura 13. Instalación del ENDIAN



Fuente: Autoría propia

Proceso terminado con éxito

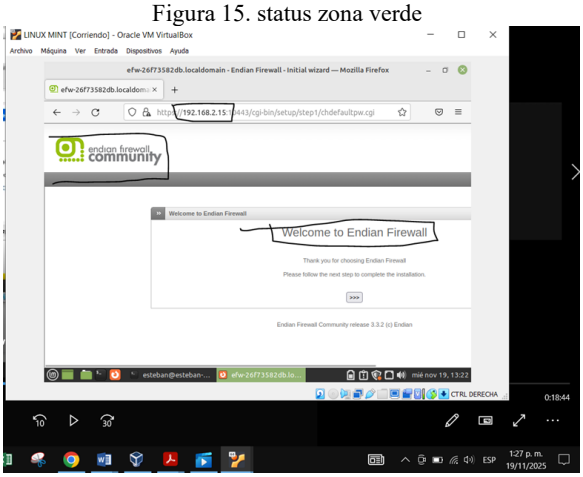
Figura 14. status zona verde



Fuente: Autoría propia

Comprobamos el correcto funcionamiento y conexión exitosa en la red interna verde que está conectada al linux MINT abriendo la consola y con ayuda del comando ping seguido de la red ip del ENDIAN

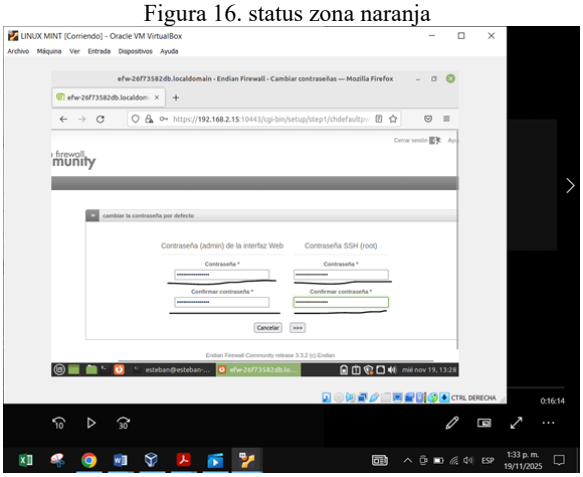
Figura 15. status zona verde



Fuente: Autoría propia

Procedemos con la configuración de la zona naranja el primer paso es entrar al navegador del Linux MINT y colocamos la red IP y seguido realizamos todos los pasos que nos vaya pidiendo

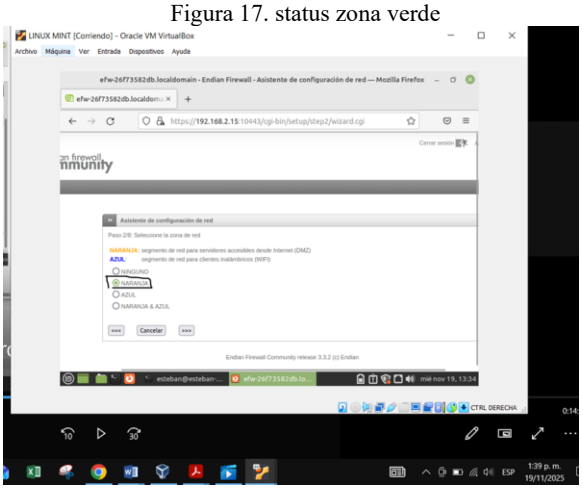
Figura 16. status zona naranja



Fuente: Autoría propia

Colocamos una contraseña para el usuario admin y el usuario root

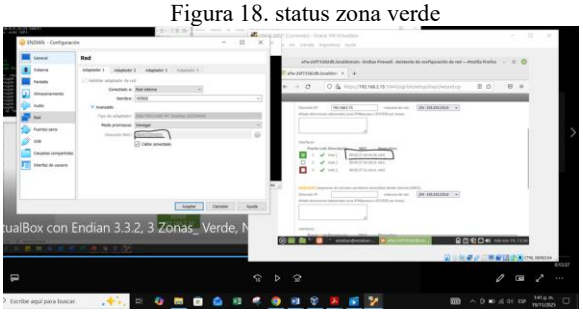
Figura 17. status zona verde



Fuente: Autoría propia

Seleccionamos la zona de red naranja que es la que queremos configurar

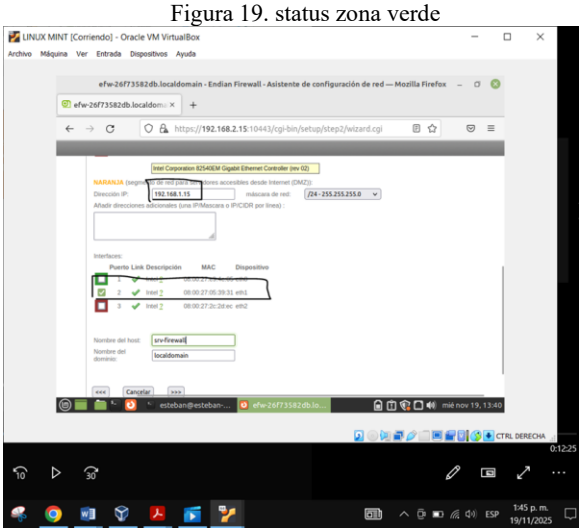
Figura 18. status zona verde



Fuente: Autoría propia

Observamos cómo cada una de las direcciones MAC concuerdan con los datos que configuramos en cada uno de los adaptadores de red

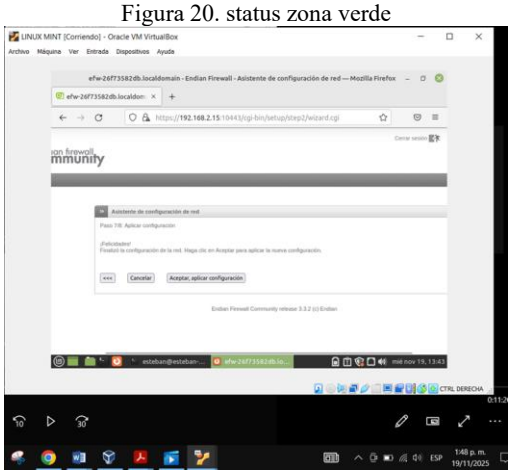
Figura 19. status zona verde



Fuente: Autoría propia

Colocamos la dirección IP que designamos para la zona naranja que está ubicada en el Ubuntu Server de nombre servidor. Además, seleccionamos la MAC dos la cual estamos tratando de activar y por último le damos un nombre al host.

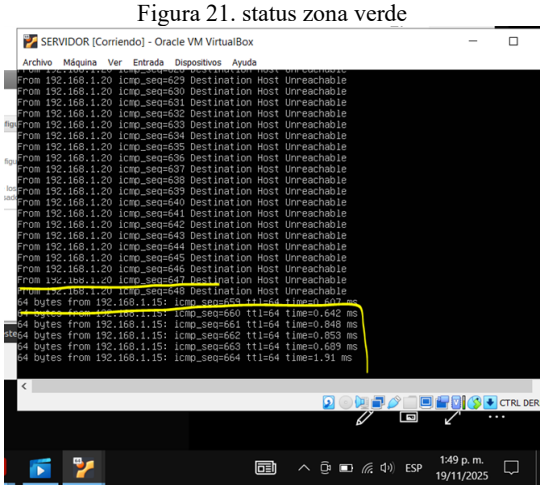
Figura 20. status zona verde



Fuente: Autoría propia

Terminamos la configuración y la damos aceptar

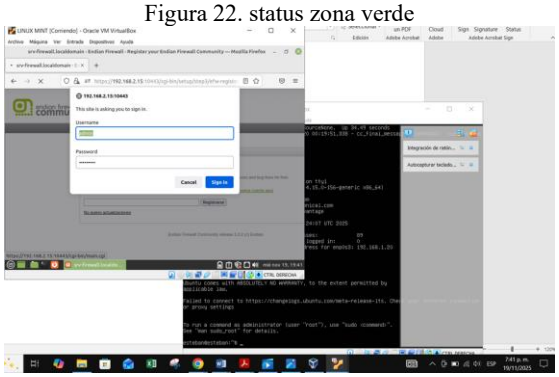
Figura 21. status zona verde



Fuente: Autoría propia

Gracias al comando ping dentro de la máquina servidor observamos cómo se activa y cambia su estado en el cual estaba apagado.

Figura 22. status zona verde



Fuente: Autoría propia

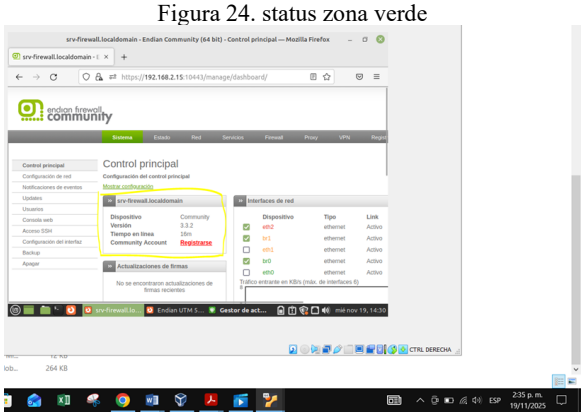
Cuando volvemos a ingresar con la IP nos pide el usuario y la contraseña que creamos anteriormente.

Figura 23. status zona verde

Fuente: Autoría propia

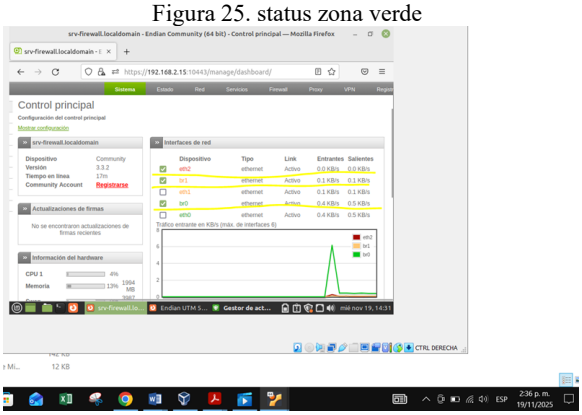
Para probar que el proceso se realizó con efectividad lo podemos hacer de dos formas la primera es dentro del ENDIAN donde nos da información como el hostname, el dominio etc.

Figura 24. status zona verde



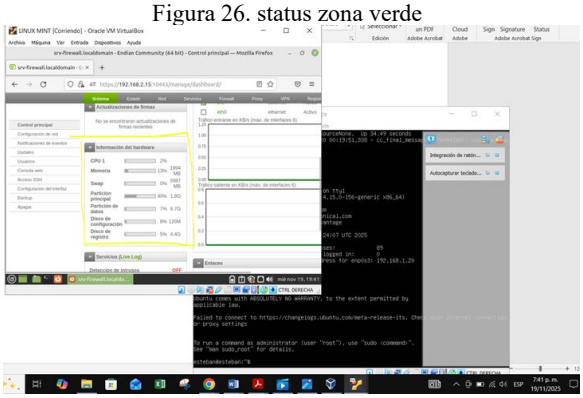
Fuente: Autoría propia

Figura 25. status zona verde



Fuente: Autoría propia

Figura 26. status zona verde



Fuente: Autoría propia

La otra forma es entrando por medio de la IP al ingresar el usuario y contraseña correctas nos da la siguiente interfaz gráfica indicando aspectos importantes como las interfaces de red disponibles, la información del hardware y un menú donde hay herramientas las cuales podemos utilizar.

4 TEMÁTICA 2 Configuración NAT.

Producto esperado:

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 reenvío de puertos / NAT, la creación de las reglas.

La configuración de NAT (Network Address Translation) es un elemento clave en la seguridad perimetral ya que permite el manejo del tráfico entre redes internas y externas sin revelar directamente la infraestructura privada. En un entorno que utiliza un firewall Endian, la NAT facilita que los dispositivos en la LAN y los servidores en la DMZ puedan comunicarse con la red WAN de forma controlada. Este proceso de traducción de direcciones protege las redes internas y asegura que el tráfico se maneje según reglas estrictas establecidas por el

administrador. A continuación, se ofrece una explicación sobre la arquitectura utilizada y los tipos de NAT configurados para permitir una conectividad segura entre diferentes zonas

4.1 TOPOLOGÍA Y SEGMENTACIÓN DE RED VIRTUAL

Tabla 1 Segmentaciòn de red

Zona/Interfaz	Tipo de red	Red/Rango IP
Verde (LAN)	Red interna	192.168.2.0
Naranja (DMZ)	Red interna	192.168.3.0
Roja (WAN)	Nat / Puente	10.0.2.0

Fuente: Autoría Propia

4.2 PRINCIPIOS BÁSICOS DE NAT Y CONFIGURACIÓN DE REDIRECCIÓN DE PUERTOS

NAT permite que múltiples equipos ubicados en redes privadas puedan acceder a redes públicas utilizando una o pocas direcciones IP visibles externamente y esta tecnología cumple una función de seguridad y de optimización del direccionamiento ya que entre sus variantes principales se encuentran SNAT y DNAT, cada una enfocada en direcciones de origen y destino respectivamente.

4.2.1 FUNCIONAMIENTO DEL SOURCE NAT (SNAT)

El Source NAT es un mecanismo mediante el cual las direcciones IP privadas de los equipos internos se sustituyen por la dirección IP pública del firewall al enviar tráfico hacia la WAN. Este proceso permite que distintos dispositivos de la LAN o la DMZ compartan una misma dirección pública sin ser identificados individualmente. Además de ofrecer conectividad, SNAT evita que las direcciones internas queden expuestas, ya que todo el tráfico parece originarse directamente desde la interfaz WAN del firewall.

4.2.1.1 OPERACIÓN DEL DESTINATION NAT (DNAT)

El port forwarding es una aplicación de DNAT que habilita que ciertas solicitudes externas lleguen a servicios concretos dentro de la red interna. Mediante reglas específicas, el firewall redirige tráfico recibido en un puerto público hacia una dirección IP privada y un puerto interno. Esta técnica permite que servidores web, FTP u otros servicios accesibles en la DMZ puedan ser consultados desde la WAN sin comprometer el resto de la infraestructura.

4.1.2.2 PORT FORWARDING COMO APLICACIÓN DE DNAT

Para permitir que los equipos de la red verde se comuniquen con Internet, Endian aplica reglas de SNAT. Debido a que las direcciones de la LAN no son válidas en la red pública, el firewall sustituye la IP privada del dispositivo por su propia IP pública antes de enviar el tráfico hacia la WAN. De este modo, todo el flujo parece provenir del firewall, garantizando anonimato y seguridad.

4.3 REGLAS NAT PARA HABILITAR ACCESO DE LA LAN A LA WAN

Para permitir que los equipos de la red verde se comuniquen con Internet, Endian aplica reglas de SNAT. Debido a que las direcciones de la LAN no son válidas en la red pública, el firewall sustituye la IP privada del dispositivo por su propia IP pública antes de enviar el tráfico hacia la WAN. De este modo, todo el flujo parece provenir del firewall, garantizando anonimato y seguridad.

4.3.1 CREACIÓN DE UNA REGLA SNAT EN ENDIAN PASO A PASO

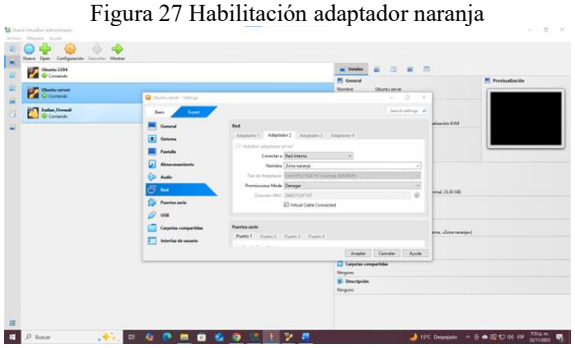
- Acceder a la consola web de Endian.
- Abrir el menú Firewall.
- Seleccionar Port Forwarding / NAT.
- Ingresar a la pestaña Source NAT.
- Crear una nueva regla con Add new source NAT rule.
- Definir:
- Source: zona VERDE (LAN).
- Destination: zona ROJA (WAN).
- Servicio / Puerto / Protocolo: según tipo de tráfico o regla general.
- Policy: Allow.
- Habilitar regla.
- Comentario: por ejemplo, "SNAT salida LAN".

Figura 26 Visualización del Panel Endian Firewall

Fuente: Autoría Propia

Se observa el panel principal (dashboard) de la interfaz web de Endian Firewall, accedido desde el navegador mediante la dirección IP *192.168.2.15*. Este panel muestra un resumen del estado del sistema, incluyendo información del dispositivo, versión instalada, tiempo de actividad y cuenta de administración. Asimismo, se presentan las interfaces de red configuradas (como *br0*, *eth1*, *br1*, *eth2* y *eth0*), indicando su tipo, estado de enlace y tráfico entrante y saliente en tiempo real. También se visualizan indicadores del hardware, tales como uso de CPU, memoria, almacenamiento y discos. Por último, se listan los servicios activados o desactivados, lo que permite una supervisión rápida del funcionamiento general del firewall.

Figura 27 Habilitación adaptador naranja

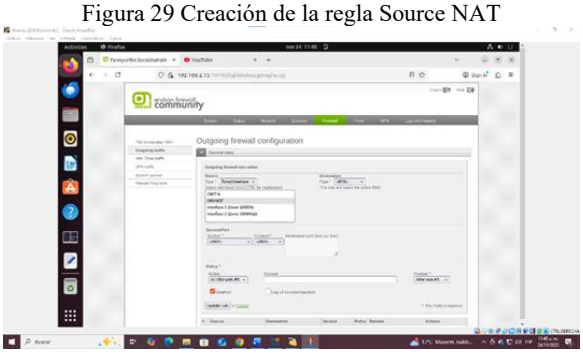


Fuente: Autoría Propia

Figura 28 Menú firewall - Source NAT

Fuente: Autoría Propia

Figura 29 Creación de la regla Source NAT

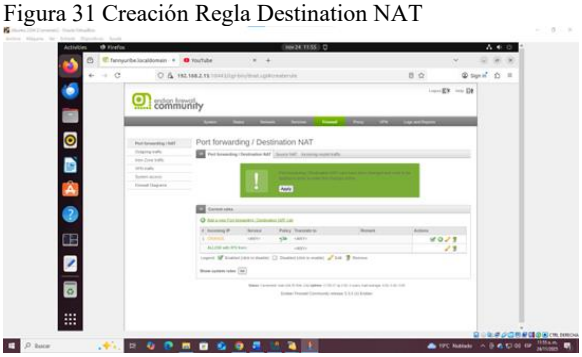


Fuente: Autoría Propia

Figura 30 Navegación web

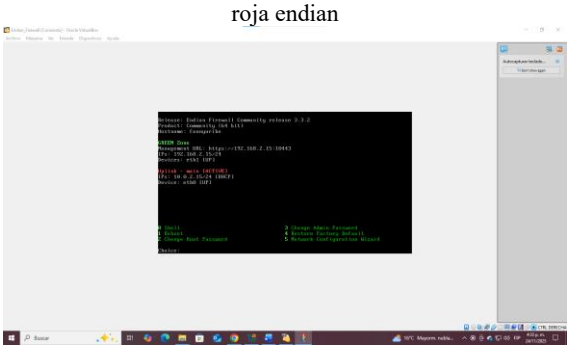
Fuente: Autoría Propia

Figura 31 Creación Regla Destination NAT



Fuente: Autoría Propia

Figura 32 Verificación De direcciones IP redes verde y roja endian

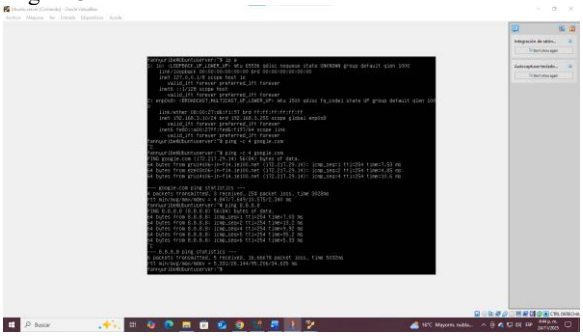


Fuente: Autoría Propia

Figura 33 IP server

Fuente: Autoría Propia

Figura 34 Conexión del servidor a la zona DMZ a internet



Fuente: Autoría Propia

Para una correcta configuración, se debe acceder a la interfaz web de Endian y definir las reglas DNAT que permitan el reenvío de puertos desde la red externa (WAN) hacia la IP interna específica del servidor o equipo que provee el servicio, escogiendo el protocolo y los puertos necesarios. Igualmente, las reglas SNAT se utilizan para modificar la IP de origen del tráfico que sale de la red interna, lo cual es útil si se manejan múltiples IPs públicas o para balancear el tráfico saliente. Finalmente, establecer reglas específicas para el tráfico saliente permite limitar los servicios permitidos y controlar la comunicación basada en protocolos y destinos.
Conocer cómo se relacionan estas configuraciones con la estructura de zonas (Verde para red interna, Naranja para DMZ, Roja para Internet, etc.) es esencial para definir políticas de seguridad adecuadas, asegurando que los accesos se mantengan estrictamente bajo control para cada segmento de la red y minimizando posibles vulnerabilidades. Por tanto, un manejo detallado y ordenado de las reglas NAT, junto con un monitoreo constante, facilita la protección y estabilidad de la red en un entorno Endian Firewall.
Esta combinación de configuración técnica detallada y la comprensión arquitectónica da como resultado una gestión eficaz y segura de los accesos externos e internos, garantizando que solo el tráfico autorizado pueda transitar entre las zonas de la red y hacia Internet, reforzando la seguridad global del sistema.

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

Producto esperado:

1. 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.

5.1 ACCESO AL DASHBOARD

Se ingresa desde la máquina virtual de Ubuntu Escritorio al navegador con la IP del servidor a Endian Firewall Community, se observa las interfaces Networks, el dominio, información de hardware y demás información.

Figura 35 Acceso a dashboard.

Fuente: Autoría Propia

5.2 CONFIGURACIÓN MANUAL UBUNTU ESCRITORIO Y UBUNTU SERVER

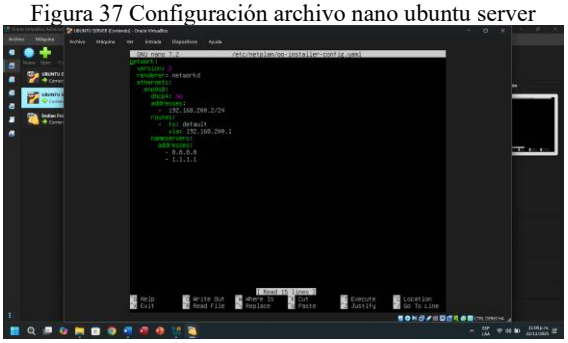
Se configura la dirección IP 192.168.100.2 con una máscara de red 255.255.255.0 y puerta de enlace 192.168.100.1 se ingresa desde la configuración de red de la máquina para el método IPv4 en Ubuntu Escritorio (zona verde), se guarda la configuración a aplicar.

Para el servidor (zona naranja) se ingresa a la ruta del archivo nano que es /etc/netplan/oo-installer-config.yaml se ingresa la configuración network de la figura 36 se agrega las direcciones IPs y los puertos de enlace 8.8.8.8 y 1.1.1.1 se guarda la configuración nano con ctrl + o y Enter.

Figura 36 Configuración red cableada IPv4

Fuente: Autoría Propia

Figura 37 Configuración archivo nano ubuntu server



Fuente: Autoría Propia

5.3 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS PERMITIDOS Y DENEGADOS

5.3.1 Regla de permiso servicio HTTP

Se crea la regla que permite el servicio HTTP en el puerto 80 desde la pestaña firewall se ingresa a tráfico interzona, se crea la regla en fuente se selecciona zona NARANJA y en destino zona VERDE, en servicio se seleccionó HTTP, en protocolo se seleccionó TCP y el puerto destino 80.
En política en acción se seleccionó ALLOW with IPS, en observación se ingresa una observación que describe permitir HTTP desde el servidor web, se selecciona la casilla habilitado y se agrega la regla, luego se da en aplicar.

Figura 38 Creación regla servicio HTTP en puerto 80

Fuente: Autoría Propia

5.3.2 Regla de permiso servicio FTP

Se crea la regla que permite el servicio FTP en el puerto 21 desde la pestaña firewall se ingresa a tráfico interzona, se crea la regla en fuente se selecciona zona NARANJA y en destino zona VERDE, en servicio se seleccionó FTP en protocolo se seleccionó TCP y el puerto destino 21.
En política en acción se seleccionó ALLOW with IPS, en observación se ingresa una observación que describe permitir FTP desde el servidor web, se selecciona la casilla habilitado y se agrega la regla, luego se da en aplicar.

Figura 39 Creación regla servicio FTP en puerto 21

Fuente: Autoría Propia

5.3.3 Regla denegación del protocolo ICMP (Puerto 8 y puerto 30)

Se crea la regla que deniega el protocolo ICMP en el puerto y 30 desde la pestaña firewall se ingresa a tráfico interzona, se crea la regla en fuente se selecciona todas las zona VERDE, NARANJA, Interfaz 2 (Zona:VERDE), Interfaz 3 (Zona:NARANJA) y en destino se selecciona todas las zona VERDE, NARANJA, Interfaz 2 (Zona:VERDE), Interfaz 3 (Zona:NARANJA), en servicio se seleccionó User defined y en protocolo se seleccionó ICMP, se ingresó en el puerto destino 8 y 30. En política en acción se seleccionó REJECT para que rechace a la hora de hacer ping en la red, en observación se ingresa una observación que describe que deniega ICMP y bloquea ping, se selecciona la casilla habilitado, en posición se selecciona First para que se posicione en primera posición y se agrega la regla, luego se da en aplicar.

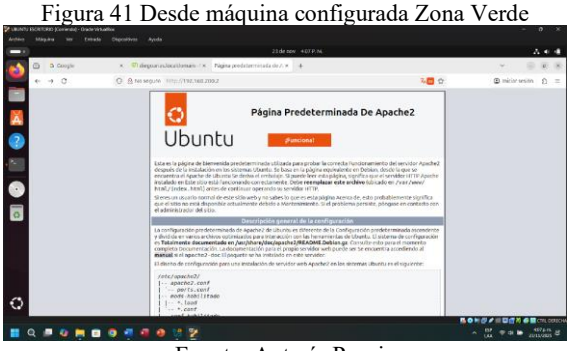
Figura 40 Creación regla que deniega protocolo ICMP

Fuente: Autoría Propia

5.4 PRUEBAS REALIZADAS PARA CADA REGLA

1. Desde Ubuntu Escritorio con el usuario diego_arias:
Regla 1: HTTP

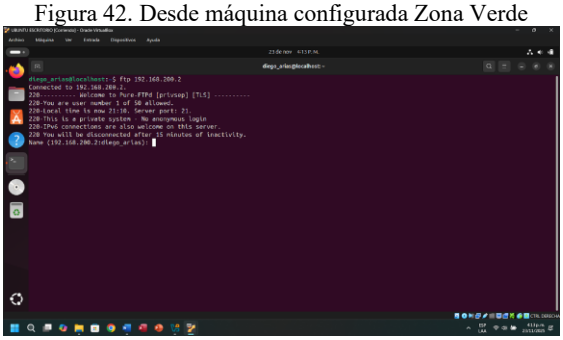
Figura 41 Desde máquina configurada Zona Verde



Fuente: Autoría Propia

2. Desde Ubuntu Escritorio con el usuario diego_arias:
Regla 2: FTP

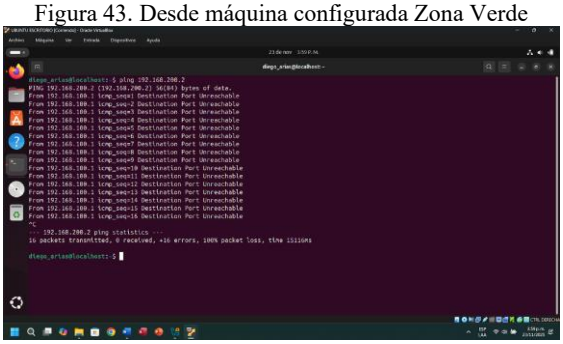
Figura 42. Desde máquina configurada Zona Verde



Fuente: Autoría Propia

3. Desde Ubuntu Escritorio con el usuario diego_arias:
Regla 3: Bloqueo ICMP

Figura 43. Desde máquina configurada Zona Verde



Fuente: Autoría Propia

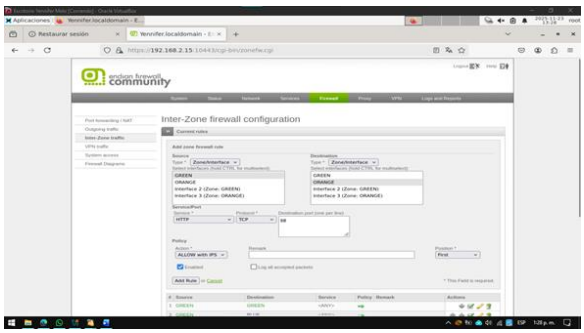
5.5 RESULTADOS TEMÁTICA 3

La implementación permitió validar el aislamiento de zonas de red mediante el firewall. El acceso al dashboard solo fue posible desde Ubuntu Escritorio zona verde, y se pudo controlar qué servicios se permiten o se deniega entre zonas, simulando un entorno real con zona desmilitarizada con redes seguras internas

6 TEMÁTICA 4 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.
En el apartado de inter-zonas configuramos las reglas para que las zonas se puedan comunicar, para este caso tenemos que realizar la configuración de los protocolos HTTP y FTP.
Creamos la primera regla que tiene como objetivo establecer una comunicación entre la zona verde y la zona naranja para el servicio HTTP, la posicionamos de primera porque el orden tiene una importancia.

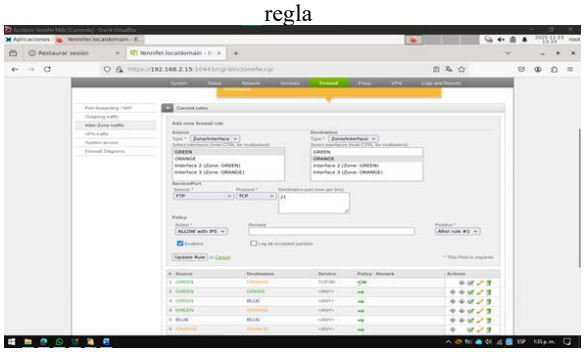
Figura 44. Comunicación zona verde con zona naranja



Fuente: Autoría Propia

Creamos la segunda regla que es prácticamente la misma que la anterior pero con la diferencia que esta cambia el servicio y se utiliza FTP.

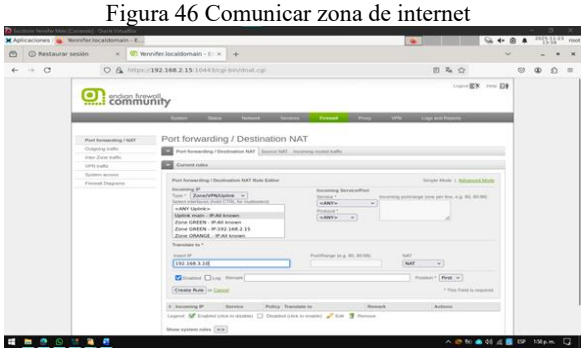
Figura 45 Creamos segunda regla



Fuente: Autoría Propia

2. Comunicar la zona Internet con la zona DMZ.
Para poder establecer una comunicación entre internet y la zona dmz, lo que tenemos que configurar es el direccionamiento de puertos.
Como se observa, creamos una regla, entonces cuando una IP de un cliente se quiere comunicar con nuestro servidor Endia se encarga de redirigir el tráfico hacia nuestro servidor y este se encarga de dar una respuesta al servicio solicitado.

Figura 46 Comunicar zona de internet



Fuente: Autoría Propia

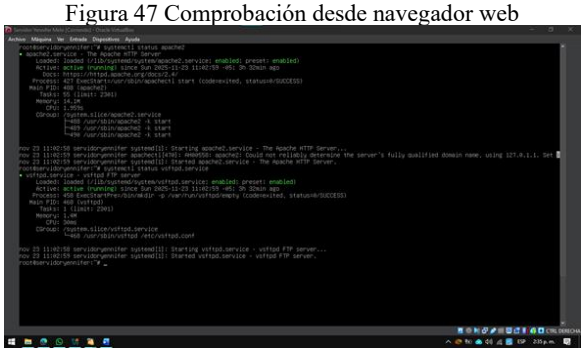
3. Verificar en el tráfico Inter - Zona, la creación de las reglas. En la parte de Inter-zonas tenemos creadas nuestras reglas de primera y las demás reglas son creadas por el sistema para que la comunicación funcione correctamente esto lo hace Endian automáticamente.

Figura 47 Verificar tráfico de la Interzona

Fuente: Autoría Propia

4. Probar desde un navegador Web, las siguientes directivas: Antes de iniciar las pruebas comprobamos que los servicios estén funcionando correctamente, para ello ejecutamos un comando que verifica que los servicios están corriendo.

Figura 47 Comprobación desde navegador web



Fuente: Autoría Propia

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. A través de la IP de nuestro servidor ingresamos a la página web desde un navegador y cómo podemos ver está funcionando correctamente

Figura 48 Ingreso al servicio HTTP desde LAN.

Fuente: Autoría Propia

El ingreso del servicio HTTP desde la LAN hacia la WAN.
Ingresamos a una página HTTP que está ojeada en internet desde nuestro cliente.

Figura 49 Ingreso al servicio HTTP desde LAN a WAN.

Fuente: Autoría Propia

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN. Con el comando curl realizamos la verificación de que servidor tenga acceso al servicio HTTP alojado en la red.

Figura 50 Ingreso al servicio HTTP desde DMZ a WAN

Fuente: Autoría Propia

El ingreso del servicio HTTP desde la WAN hacia la zona DMZ. Con la IP pública de endian podemos acceder al servidor web de nuestro servidor

Figura 51 Ingreso del HTTP desde la zona DMZ

Fuente: Autoría Propia

El ingreso del servicio FTP desde la LAN hacia la WAN.

Utilizamos un servicio FTP que este alojado en internet y tenemos varias opciones, para este caso voy a utilizar el de test.rebex.net

Figura 51 Ingreso del servicio FTP desde LAN a WAN

Fuente: Autoría Propia

El ingreso del servicio FTP desde la WAN hacia la zona DMZ.
Para ingresar al servicio FTP desde internet utilizamos la IP pública de Endian.

Figura 52 Ingreso del servicio FTP desde LAN a DMZ

Fuente: Autoría Propia

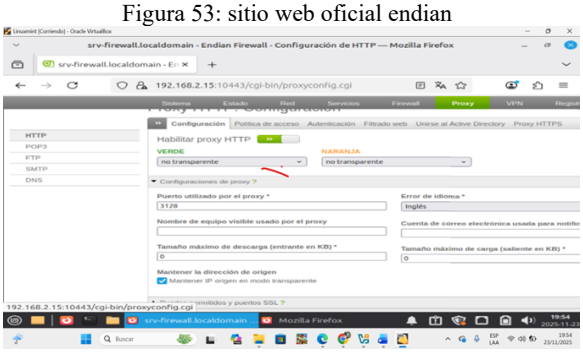
7 TEMÁTICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

Producto esperado:

1. creación del perfil y lista negra que bloquea los sitios:

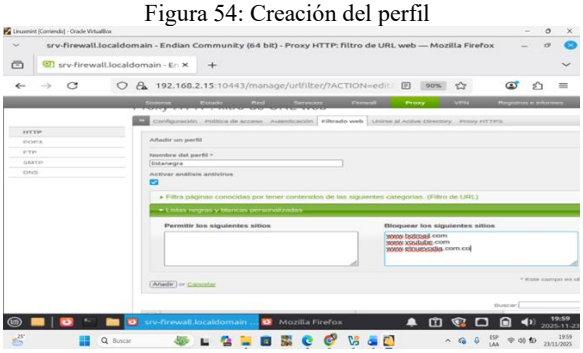
www.youtube.com
www.hotmail.com
www.elnuevodia.com.co

Figura 53: sitio web oficial endian



Fuente: autoría propia

Figura 54: Creación del perfil



Fuente: autoría propia

2. **Autenticación por usuario:** a través del proxy creamos un nuevo usuario y lo asociamos a un grupo. Establecemos la política de acceso y vinculamos el perfil creado anteriormente y también lo relacionamos con la política de autenticación.

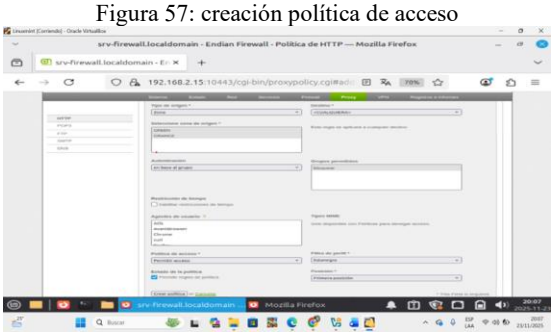
Figura 55: Creación del usuario

Fuente: autoría propia

Figura 56: Creación del grupo

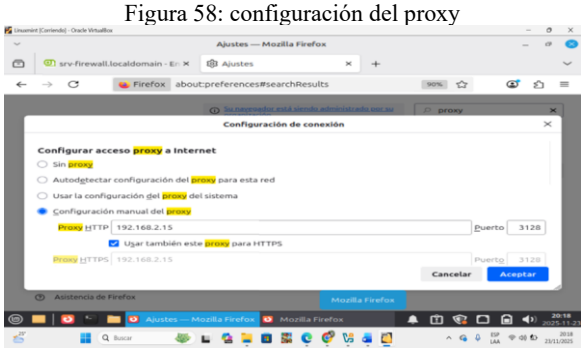
Fuente: autoría propia

Figura 57: creación política de acceso



Fuente: autoría propia

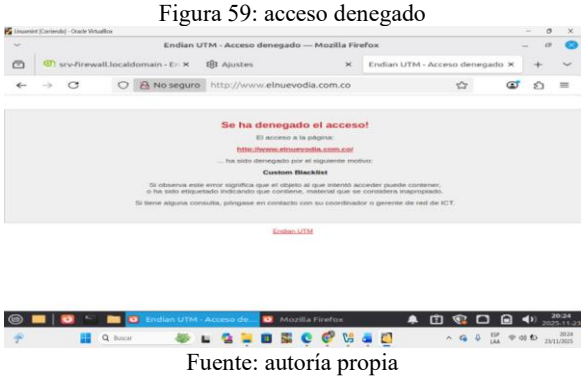
Figura 58: configuración del proxy



Fuente: autoría propia

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

Figura 59: acceso denegado



Fuente: autoría propia

CONCLUSIONES

La implementación de ENDIAN Firewall bajo una arquitectura segmentada en zonas Verde, Roja y Naranja, permitió comprender de manera práctica el rol del Firewall como el núcleo de la seguridad perimetral, reforzando los conceptos esenciales del filtrado, control de acceso y separación lógica de redes. El uso de capturas y material audiovisual (imágenes y vídeos) facilitó la claridad de los procesos realizados.

La virtualización con Oracle VirtualBox demostró ser un entorno adecuado para experimentar sin riesgo, permitiendo probar configuraciones reales, el de aplicar las reglas especificas y analizar los comportamientos del tráfico. Esto fortaleció las competencias en administración de redes y preparación para el estudio de fundamentos de Linux y certificaciones como LPI.

El uso del proxy HTTP no transparente evidenció el poder de las políticas de acceso aplicadas de manera correcta, ya que, mediante listas negras, autenticación y reglas de restricción se logró controlar con precisión el uso de Internet. Este resultado confirmó la importancia del firewall como herramienta para gestionar y asegurar servicios críticos.

El proyecto resaltó el valor del software libre en infraestructuras de seguridad, demostrando que soluciones como Endian pueden alcanzar niveles profesionales de rendimiento, protección y administración. Su implementación fomenta independencia tecnológica, eficiencia y una visión estratégica orientada a infraestructuras más seguras.

El desarrollo de esta actividad fortaleció la capacidad analítica, operativa y documentativa del estudiante, integrando buenas prácticas de seguridad, segmentación, monitoreo y gestión de tráfico. Además, reafirmó la necesidad de adoptar modelos perimetrales bien diseñados como base para redes confiables, escalables y alineadas con las demandas de la cuarta revolución industrial.

2. REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

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

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

[5] Jhonatan Sanchez Giraldo (2025) VirtualBox con endian 3.3.2, 3 zonas, Verde, Anaranjada y Roja https://drive.google.com/drive/folders/1jHtVKKv41sj1hhaO4tg9krt0DhgOcYCC

[6] Andrews, J., & Dark, J. (2024). *Network Security, Firewalls, and VPNs* (3rd ed.). Jones & Bartlett Learning.
[7] Stewart, J. M., Chapple, M., & Gibson, D. (2022). *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (9th ed.). Wiley.
[8] Rountree, D., & Castrillo, I. (2014). *The Basics of Cloud Computing and Network Defense*. Syngress.