Implementación Operativa de un Firewall Perimetral: Endian en Entornos GNU/Linux Virtualizados

Jhon Jairo Vargas Manrique e-mail:
jjvargasma@unadvirtual.edu.co
Ronal Jaison Márquez Mora e-mail:
rjmarquezm@unadvirtual.edu.co
Nicolas Payan Tascón e-mail:
npayant@unadvirtual.edu.co
Ingrid Paola Escobar Bonilla e-mail:
ipescobarb@unadvirtual.edu.co
Roberth Andrey Daza Loaiza e-mail:
Radazalo@unadvitual.edu.co

RESUMEN: *Este artículo proporciona un análisis detallado sobre la instalación y configuración del firewall Endian en una máquina virtual utilizando VirtualBox, organizado en cinco áreas clave. En primer lugar, se crea una arquitectura de red segmentada que incluye zonas verdes (LAN), roja (WAN) y naranja (DMZ), con el objetivo de mejorar la seguridad en los puntos de acceso y facilitar la comunicación entre zonas. En segundo lugar, se establecen reglas de SNAT y DNAT que permiten la difusión controlada de servicios internos, como los servidores web, sin poner en riesgo la integridad de la red LAN. La tercera sección se centra en la activación de servicios HTTP y FTP desde la DMZ hacia las otras zonas, así como en la restricción del protocolo ICMP como una medida de prevención. A continuación, se establecen reglas de acceso que regulan el tráfico según parámetros tales como la dirección IP, el puerto, la interfaz y el estado de conexión. Por último, se introduce un proxy HTTP no transparente con autenticación, lo que posibilita un control más riguroso sobre el tráfico web.*

PALABRAS CLAVE: Configuración de firewall, Zonas de red, Segmentación de red, Virtualización, Redes LAN y WAN.

ABSTRACT: *This article provides a detailed análisis of the installation and configuration of the Endian firewall on a virtual machine using VirtualBox, organized into five key areas. First, a segmented network architecture is created, including green (LAN) red (WAN), and Orange (DMZ) zones, with the goal of improving security at access points and facilitating communication between zones. Second, SNAT and DNAT rules are established to allow the controlled exposure of internal services-such as web servers-without compromising the integrity of the LAN. The third section focuses on enabling HTTP and FTP services from the DMZ to the other zones, as well as restricting the ICMP protocol as a preventive measure. Next access rules are configured to regulate traffic based on parameters such as IP address, port, interface, and connection state. Finally, a non-transparent HTTP proxy with authentication is introduced, enabling tighter control over web traffic.*

KEY WORDS: Firewall configuration, Network zones, Network segmentation, Virtualization, LAN and WAN networks.

1 INTRODUCCIÓN

En la actualidad, las redes informáticas y su seguridad han pasado de ser un valor añadido a convertirse en una necesidad crítica. Implementar un firewall es equivalente a colocar un guardia en la entrada de una red: controla, supervisa y filtra el tráfico que circula entre el entorno interno y el exterior. En este contexto, Endian Firewall (EFW) se posiciona como una solución robusta y de código abierto, basada en GNU/Linux, orientada a quienes buscan proteger su infraestructura sin recurrir a grandes inversiones ni hardware especializado. Su enfoque accesible lo convierte en una herramienta ideal tanto para entornos de formación como para pequeñas implementaciones reales.

2 TEMATICAS

2.1 TEMATICA 1: CONFIGURACION DE LA INSTANCIA PARA GNU/LUNUX ENDIAN EN VIRTUALBOX (TARGGETAS DE RED) E INSTALACION EFECTIVA DEL MISMO.

En el contexto actual, donde la seguridad de red y la segmentación del tráfico son prioridades fundamentales, la implementación de firewalls de nivel empresarial se convierte en un componente indispensable para la protección de servicios y sistemas críticos.

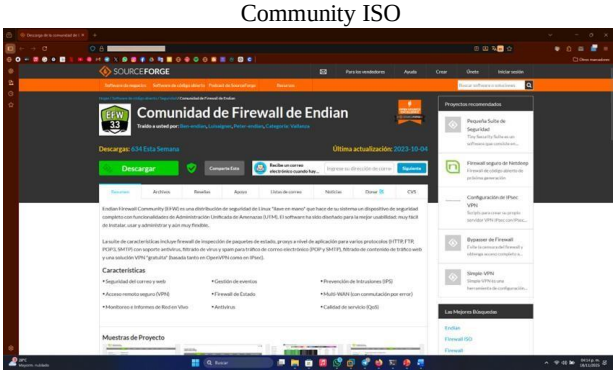
Dentro de este ámbito, GNU/Linux Endian destaca como una solución de código abierto orientada a la seguridad perimetral, permitiendo estructurar entornos controlados mediante zonas de red como LAN (verde), WAN (roja) y DMZ (naranja).

La presente temática se centra en el despliegue inicial de una instancia de Endian en VirtualBox, haciendo énfasis en la correcta configuración de las interfaces de red virtuales

y en el proceso de instalación del sistema operativo. Estas acciones constituyen la base para garantizar una gestión eficiente del tráfico, así como para establecer políticas de seguridad coherentes y bien estructuradas.

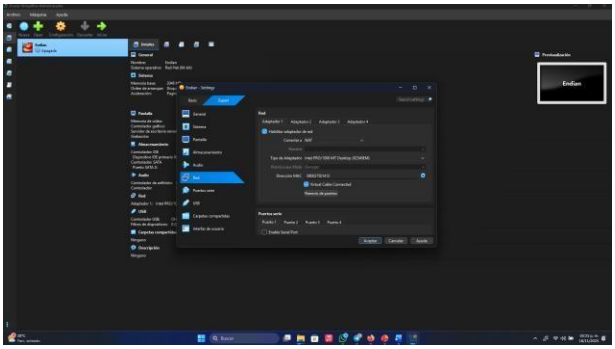
A continuación, se describen de manera detallada los pasos necesarios para el desarrollo de la Temática 1:

Ilustración 1. Página para descargar Endian Firewall Community ISO



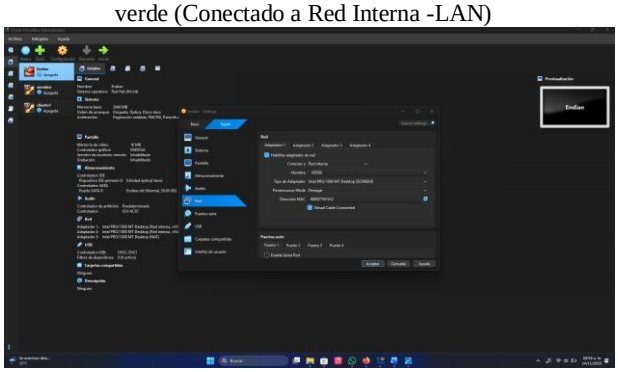
Fuente: Autoría Propia

Ilustración 2. Creando máquina virtual de Endian en Virtual Box



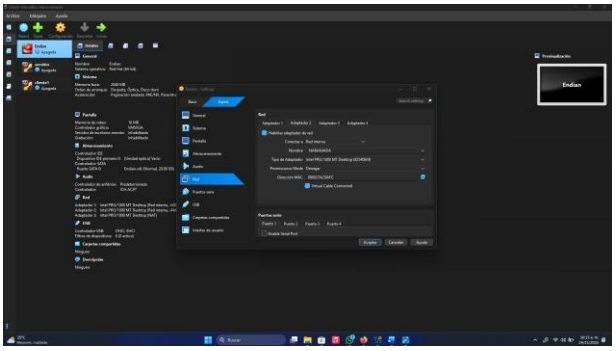
Fuente: Autoría Propia

Ilustración 3. Configuración de adaptador de red en la zona verde (Conectado a Red Interna -LAN)



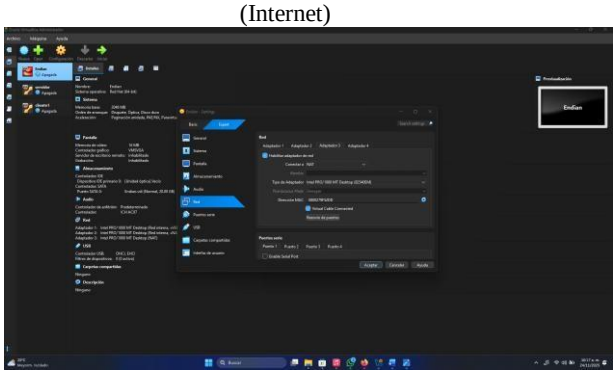
Fuente: Autoría Propia

Ilustración 4. Configuración de adaptador de red en la zona naranja (Conectado servidores DMZ



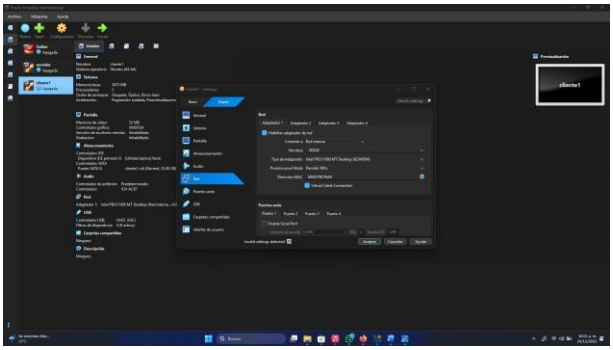
Fuente: Autoría Propia

Ilustración 5. Configuración de adaptador de red en la zona roja (Internet)



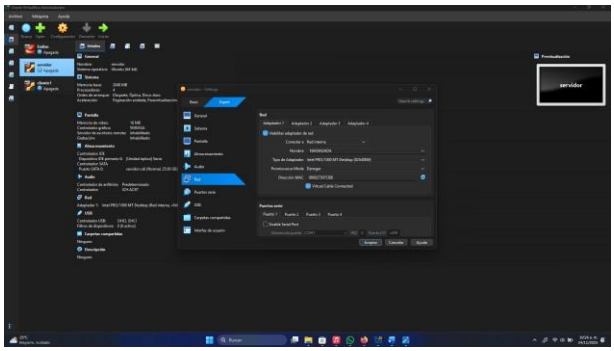
Fuente: Autoría Propia

Ilustración 6. Configuración de adaptador de red en la zona roja Ubuntu escritorio – Cliente



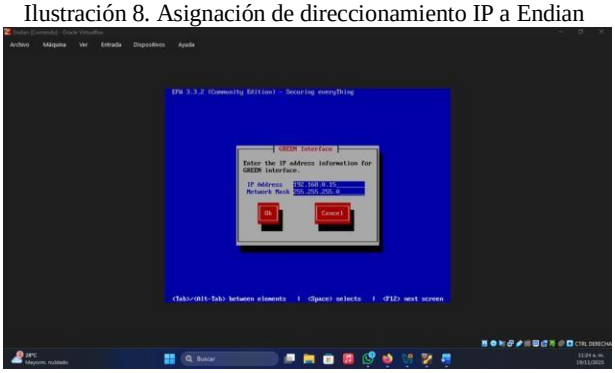
Fuente: Autoría Propia

Ilustración 7. Configuración de adaptador de red en la zona verde Ubuntu server – Servidor



Fuente: Autoría Propia

Ilustración 8. Asignación de direccionamiento IP a Endian



Fuente: Autoría Propia

Ilustración 9. Interfaz de Endian, donde se visualiza la zona verde y la zona roja activa

Fuente: Autoría Propia

3 TEMATICA 2: CONFIGURACION NAT

Realizaremos la configuración NAT en Endian, con esto buscamos poder permitir la comunicación segura entre la red verde (LAN), la zona naranja (DMZ) y la red roja (WAN). Con esta configuración se permite el enmascaramiento de las direcciones internas y el control del tráfico entre zonas de seguridad, con esto garantizamos la salida a internet desde la zona verde (LAN) y la zona naranja (DMZ) mediante reglas SNAT y así se verifica su funcionamiento a través de pruebas reales de conectividad.

3.1 FUNDAMENTOS NAT

Esta es un mecanismo utilizado en redes para poder modificar las direcciones IP en los encabezados de paquetes mientras que estos atraviesan un router o firewall. El propósito de esto es poder permitir que múltiples dispositivos de una red privada accedan a una red pública mediante una única dirección pública o un conjunto reducido de direcciones.

3.1.1 TIPOS DE NAT

SNAT (Source NAT)

Se utiliza para cambiar la dirección IP de origen de los paquetes de red salientes, reemplazando la IP privada de un dispositivo interno por una IP pública (generalmente la del router o firewall), para que el dispositivo pueda acceder a internet. Esta tecnología permite que varios dispositivos en una red privada compartan una única dirección IP pública y mejora la seguridad al ocultar las direcciones IP internas.

DNAT (Destination NAT)

Mecanismo de traducción de direcciones que modifica la dirección IP de destino de los paquetes entrantes cuando se dirigen desde una red externa hacia una red privada. DNAT permite redirigir conexiones provenientes de Internet hacia hosts internos mediante reglas basadas en IP y puertos, facilitando el acceso remoto a servicios internos, la publicación de servidores alojados en redes privadas y la implementación de reenvío de puertos. Este proceso permite mantener la seguridad del direccionamiento privado mientras se garantiza la accesibilidad de servicios esenciales desde redes externas.

PAT (port address trannslation)

direcciones de red (NAT) que asigna las direcciones IPv4 internas privadas de una red a una única dirección IP pública mediante puertos de red. NAT es un proceso que utilizan los enrutadores para traducir direcciones IP internas no registradas a direcciones IP externas registradas. PAT se diferencia de otras formas de NAT porque utiliza números de puerto al asignar direcciones IP privadas a una dirección IP pública, que es la dirección que ven los sistemas externos.

La traducción de direcciones de puerto también se denomina portabilidad, sobrecarga de puertos, NAT multiplexada a nivel de puerto y NAT de dirección única. PAT es la forma más común de NAT utilizada en la mayoría de los hogares y pequeñas y medianas empresas.

PAT se introdujo para conservar las direcciones IPv4 hasta que se implementara una solución más permanente. Esta solución finalmente se materializó en IPv6. Sin embargo, IPv4 aún se utiliza ampliamente en las comunicaciones de red, por lo que PAT sigue siendo relevante. PAT también contribuye a mejorar la seguridad en la red local al ocultar las direcciones IP internas del público.

3.1.2 PORQUE ES FUNDAMENTAL NAT

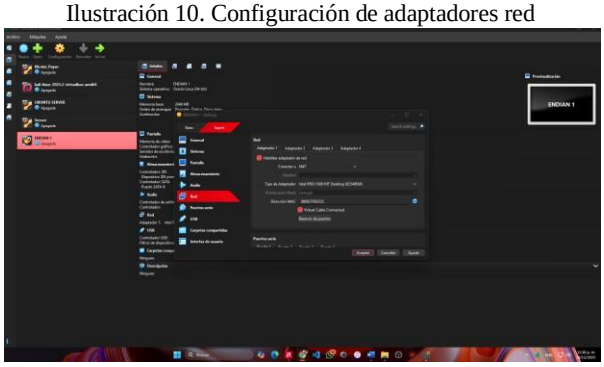
- Podemos proteger la red interna ocultando las direcciones privadas.
- Permite conectividad de redes aisladas
- Controla de forma gradual el tráfico entrante y saliente
- Facilitar el acceso a Internet desde zonas internas sin comprometer la seguridad.

3.2 TOPOLOGIA Y ENTORNO DE TRABAJO

Para esta actividad se implementó un entorno virtualizado compuesto por Endian, un servidor Ubuntu en la DMZ y un equipo Ubuntu en la LAN. Las redes configuradas fueron:

- Zona verde (LAN): 10.0.0.0/24
- Zona naranja (DMZ): 172.16.0.0/28
- Zona roja (WAN): esta ya la designa automáticamente Endian

Ilustración 10. Configuración de adaptadores red



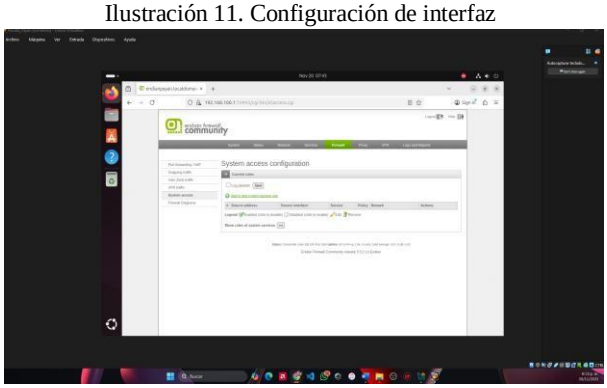
Fuente: Autoría Propia

3.3 CONFIGURACION DE RED EN ENDIAN.

Esta configuración es importante en esta temática, ya que esta define como se comunicarán las distintas zonas que se van a manejar y sobre que interfaces se aplicarían las reglas. en este apartado este proceso se inició cuando se realizó la temática 1, a medida que se va realizando el proceso de esta temática al final se configuraba automáticamente el acceso a internet.

Es importante realizar todos estos procesos antes de aplicar alguna regla de NAT a que una configuración incorrecta en las interfaces podría impedir la salida a internet, bloquear el tráfico interno o generar conflictos entre zonas. tras confirmar que cada interfaz estaba correctamente asignada y operativa, Endian quedó listo para aplicar políticas SNAT y realizar las pruebas de conectividad**.**

Ilustración 11. Configuración de interfaz



Fuente: Autoría Propia

3.4 CONFIGURACION DE SOURCE NAT.

Con la configuración de SNAT permite que los equipos de la red Verde (LAN) salgan a Internet utilizando la dirección IP de la interfaz Roja (WAN).

Para nosotros verificar esto, ingresaremos al panel de Firewall - NAT / Port Forwarding - Source NAT**,** donde se confirmaron las reglas activas. Estas reglas enmascaran las IP privadas de la LAN y permiten la comunicación hacia Internet de forma segura.

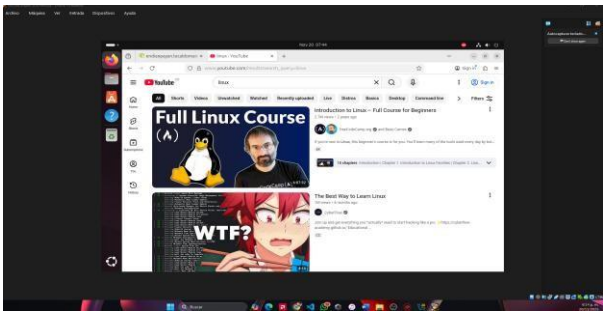
Ilustración 12. Reglas SNAT

Fuente: Autoría Propia

3.5 PRUEBA DE CONECTIVIDAD.

Con esto validamos la conexión desde la LAN hacia la WAN mediante pruebas de navegación y comandos de verificación con ping, se comprueba de manera más efectiva con el acceso exitoso a sitios web como YouTube, demostrando el funcionamiento del NAT.

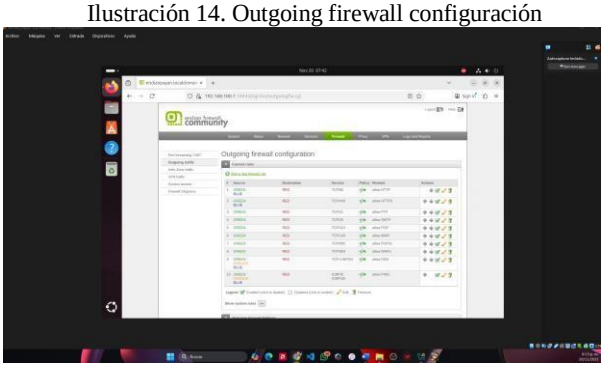
Ilustración 13. Validación de conectividad desde LAN



Fuente: Autoría Propia

3.6 REVISION Y CONFIGURACION DE REGLAS NAT Y TRAFICO SALIENTE PARA DMZ.

Ilustración 14. Outgoing firewall configuración

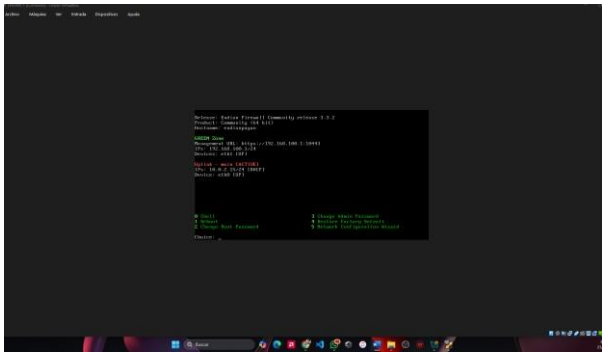


Fuente: Autoría Propia

3.7 VERIFICANDO LA ZONA ROJA DESDE LA MAQUINA NARANJA.

En este apartado verificamos las direcciones IP asignadas en las zonas trabajadas, con esto podemos confirmar que la máquina reconoce correctamente las tres interfaces de red y que la configuración inicial se realizó de manera adecuada.

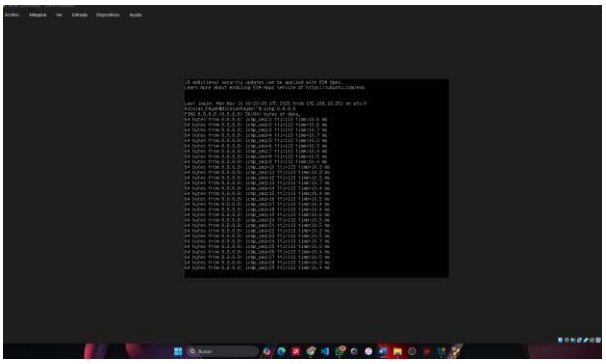
Ilustración 15. Verificación de las IP



Fuente: Autoría Propia

Esta prueba de conectividad que hemos realizado desde la maquina mediante el comando ping 8.8.8.8. nos da como respuesta exitosa indica que el servidor en la DMZ cuenta con acceso a Internet, confirmando que las reglas de NAT y las políticas del firewall permiten la salida de tráfico desde esta zona hacia la red externa.

Ilustración 16. Conexión a internet exitosa



Fuente: Autoría Propia

4 TEMATICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

La instalación pide en este momento los parámetros de red para la interfaz GREEN (la red local). La dirección IP estática necesaria se introduce y servirá como puerta de enlace interna para todos los dispositivos conectados a tu red laboral. A continuación, se determina su máscara de subred. La Zona GREEN es considerada la de mayor confianza, por lo que su configuración adecuada es esencial para que Endian tenga la capacidad de filtrar y enrutar el tráfico desde esta zona hacia la DMZ (Naranja) y hacia el exterior (RED), asegurando así la conectividad interna.

Ilustración 17: Configuración de Endian

Fuente: Autoría Propia

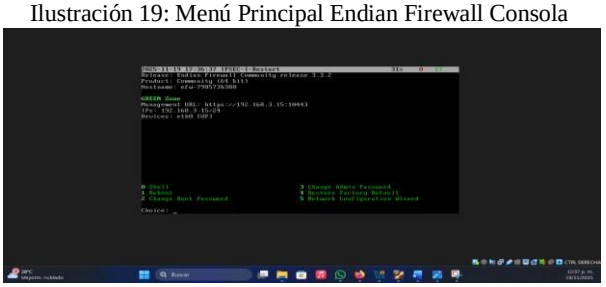
Afirma que la instalación del software EFW (probablemente Endian Firewall) se ha completado con éxito. El sistema te señala que, como primer paso, debes desconectar cualquier medio de instalación (como el USB, el CD o el archivo ISO) de la computadora antes de seguir. Luego de realizar esto, para terminar de configurar el cortafuegos en sus primeros pasos, tienes que acceder a la interfaz web (WebGUI). Para ello, abre un navegador en otro equipo conectado a la misma red y dirígete a la URL http://192.168.3.15 o a la dirección segura https://192.168.3.15:10443.N

Ilustración 18. Instalación EFW Completada Acceso Web

Fuente: Autoría Propia

Para este paso, después de la instalación, la pantalla de Endian Firewall Community te muestra el menú principal de configuración basado en consola (CLI), indicando que el sistema está corriendo. Aquí, se muestra la dirección IP y el puerto para acceder a la interfaz web (WebGUI): https://192.168.3.15:10443. Además, te presenta las opciones para apagar, reiniciar, cambiar contraseñas o iniciar el asistente de configuración de red.

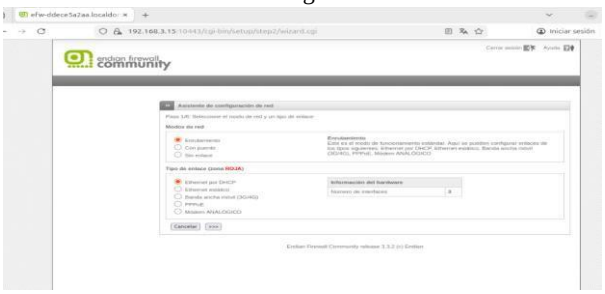
Ilustración 19: Menú Principal Endian Firewall Consola



Fuente: Autoría Propia

Después de ingresar a la interfaz web de Endian Firewall por medio de la dirección lógica https://192.168.3.15:10443, el Asistente de Configuración de Red se muestra en esta etapa. El proceso se inicia estableciendo la topología del cortafuegos, eligiendo el Modo de red (por defecto "Enrutamiento") y el Tipo de enlace que empleará la interfaz para la zona ROJA (Internet), ya sea IP estática o DHCP

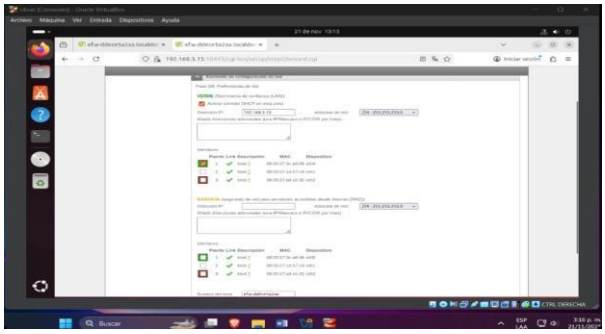
Ilustración 20. configuración de Endian



Fuente: Autoría Propia

la sección de Preferencias de red del asistente muestra la configuración inicial de las interfaces, donde la zona VERDE (LAN) está definida como 192.168.3.15 y la zona NARANJA (DMZ) como 192.168.1.15. Se procede a la asignación de las interfaces físicas de hardware a estas zonas y a la zona ROJA (Internet). Este paso también requiere configurar los parámetros de red esenciales, como la dirección IP del gateway y los servidores DNS.

Ilustración 21. Configuración Interfaces Endian Firewall Zonas



Fuente. Autoría Propia

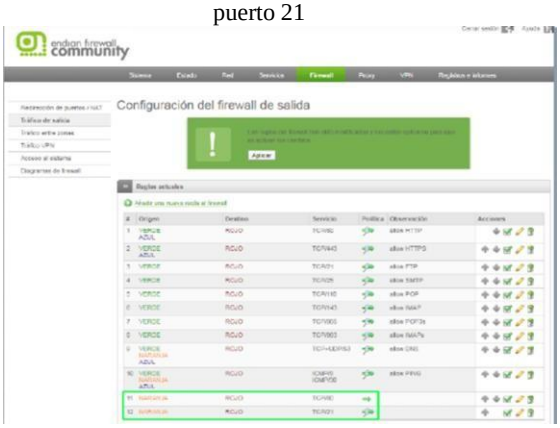
El asistente se enfoca en la configuración de la zona NARANJA (DMZ), donde se establece la dirección IP 192.168.1.15 con una máscara de red /24, distinta a la IP VERDE (192.168.3.15). Adicionalmente, se selecciona y asigna la interfaz física correspondiente (parece ser eth0) que operará como esta zona de servidores. Finalmente, se definen el nombre de host y el nombre del dominio del sistema.

Ilustración 22: Configuración Zona NARANJA (DMZ)

Fuente: Autoría Propia

En este paso, se definió la política de seguridad para el tráfico de salida (Outbound) hacia Internet (Zona ROJA). Esto se logró creando y revisando reglas que otorgan permisos específicos para que la Zona VERDE y la Zona NARANJA (192.168.1.15) puedan utilizar servicios esenciales como HTTP (puerto 80) y FTP (puerto 21), asegurando así la comunicación externa controlada.

Ilustración 23. Permisos de http con puerto 80 y FTP con puerto 21



Fuente: Autoría Propia

En este paso, se ha implementado una regla de bloqueo en el firewall inter-zona para restringir la comunicación entre las redes internas. Específicamente, se bloquea el tráfico del protocolo ICMP (que incluye PING - Tipo 8, y Traceroute - Tipo 30) desde la Zona VERDE (192.168.3.15) hacia la Zona NARANJA (192.168.1.15), mejorando así la segmentación de la red.

Ilustración 24. bloqueo de protocolo ICMP para tipo 8 y 30

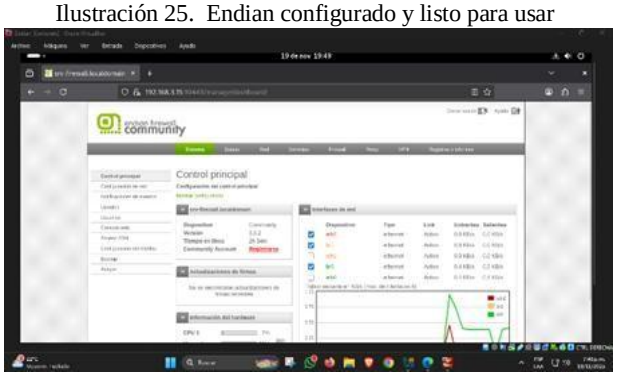
Fuente: Autoria Propia

5 TEMATICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

Sabemos que la seguridad perimetral es muy importante para proteger los servidores y servicios que trabajan dentro de una red empresarial. Por eso para conocer más a fondo, en esta actividad se utiliza la distribución Endian Firewall como plataforma de seguridad, con el fin de controlar el tráfico entre la LAN, la DMZ y la WAN. Se debe instalar, configurar y administrar Endian, donde verificamos el funcionamiento de los servicios y las conexiones entre zonas mediante comandos y pruebas de acceso.

Esta Temática se basa en la implementación y configuración de un entorno de seguridad perimetral usando Endian, donde se definen las zonas LAN, DMZ y WAN, aplicando reglas de acceso para permitir o bloquear el tráfico entre ellas. Donde una vez instalada la distribución, se procede con la temática propuesta.

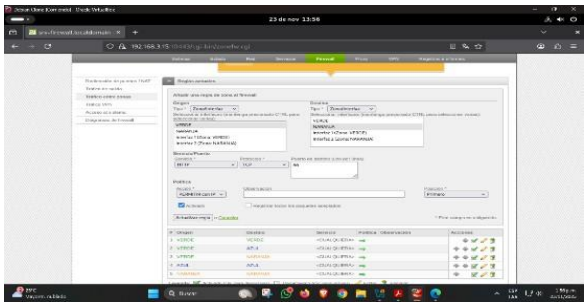
Ilustración 25. Endian configurado y listo para usar



Fuente: Autoría Propia

Aquí se realiza la conexión Inter zona, donde lo realizo añadiendo una nueva regla, donde comuniquemos la zona verde con la zona naranja con el protocolo HTTP como se puede evidenciar. Ibagué.

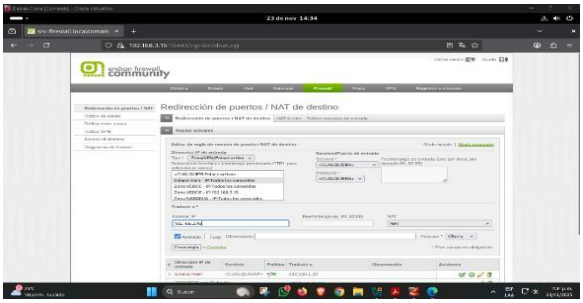
Ilustración 26. Conexión entre zonas



Fuente: Autoría Propia

Creamos una regla de reenvío de puerto, NAT de destino. Donde escogemos el enlace main, IP todos los conocidos, luego insertamos la dirección IP de la zona naranja servidor.

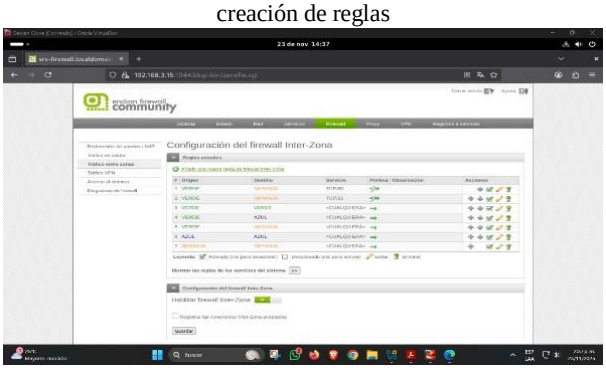
Ilustración 26. Comunicar la zona internet con la zona DMZ



Fuente: Autoría Propia

En este tercer punto de la temática 4, procedemos a verificar el tráfico inter – zonas

Ilustración 27. Verificar el tráfico inter – zona, la creación de reglas



Fuente: Autoría Propia

Probamos el ingreso del servicio ftp desde la LAN hacia la WAN.

Ilustración 28. Probando el ingreso del servicio FTP

Fuente: Autoría Propia

Aquí podemos apreciar el ingreso del servicio ftp desde la WAN hacia la zona DMZ.

Ilustración 29. Probando el ingreso del servicio FTP

Fuente: Autoría Propia

Probando acceso HTTP desde la LAN hacia la WAN, donde se comprobó que la pagina cargo correctamente, lo cual confirma que el firewall permite el tráfico HTTP desde la LAN hacia la WAN.

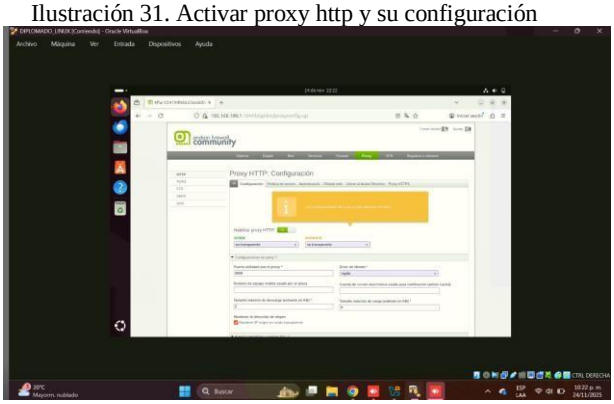
Ilustración 30. Probando el ingreso del servicio FTP

Fuente: Autoría Propia

6 TEMATICA 5 IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET

En esta temática se configura en Endian Firewall un Proxy HTTP no transparente para controlar la navegación de la red interna. Se habilita la autenticación por usuario, se crea una **lista negra** de sitios restringidos y se aplican políticas de acceso que determinan qué usuarios pueden navegar y qué contenidos se bloquean. Finalmente, se realizan pruebas desde la LAN para verificar que el proxy solicita credenciales y bloquea los sitios definidos, fortaleciendo así la seguridad y el control del tráfico web en la organización. 4,52 cm 8,04 cm

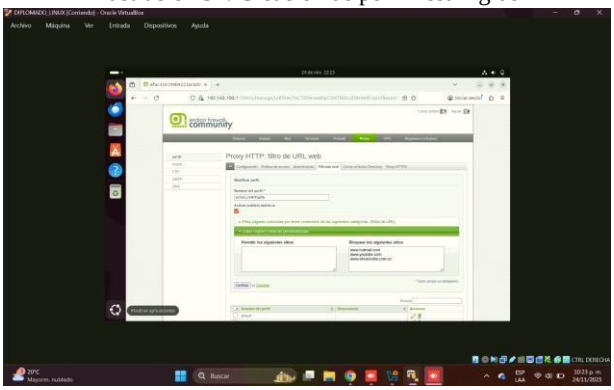
Ilustración 31. Activar proxy http y su configuración



Fuente: Autoría Propia

Se activa la configuración del proxy y se realiza la configuración en el puerto 8080

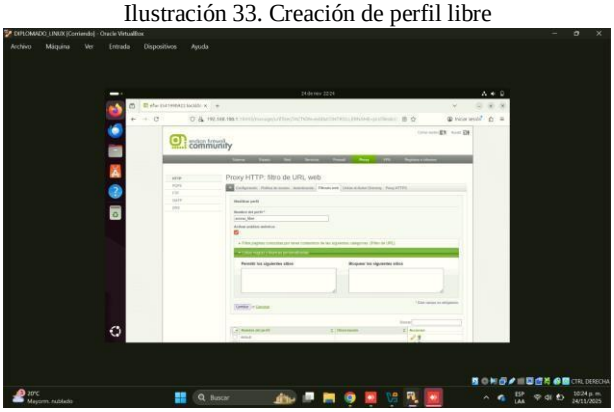
Ilustración 32. Creación de perfil restringido



Fuente: Autoría Propia

Se crea el perfil restringido donde se agregan las 3 url que se van a impedirle el ingreso

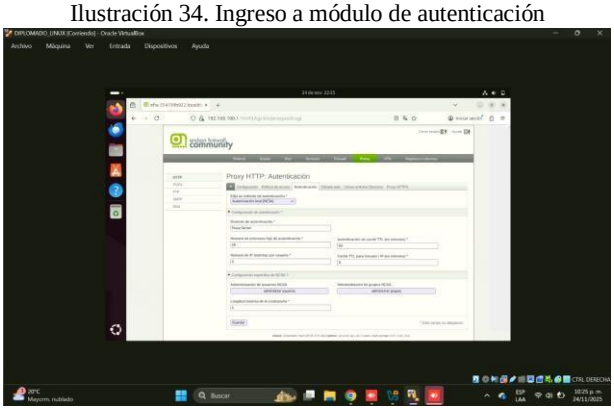
Ilustración 33. Creación de perfil libre



Fuente: Autoría Propia

Se crea el perfil libre donde este no va a tener limitaciones

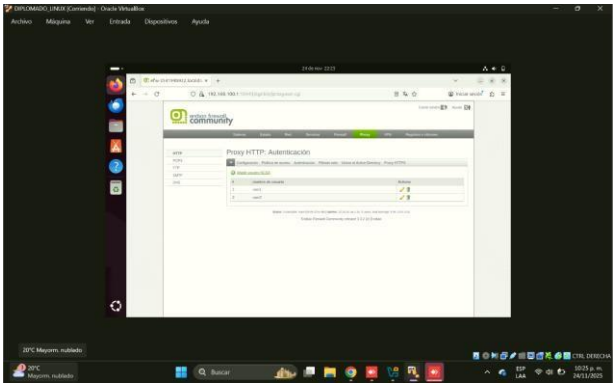
Ilustración 34. Ingreso a módulo de autenticación



Fuente: Autoría Propia

Se ingresa al módulo de autenticación donde se van a administrar usuarios y administrar grupos

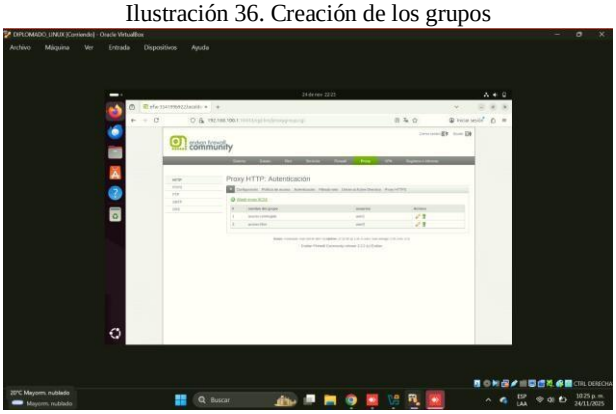
Ilustración 35. Creación de usuarios



Fuente: Autoría Propia

Se crean los diferentes usuarios que se van a utilizar para el proxy por autenticación.

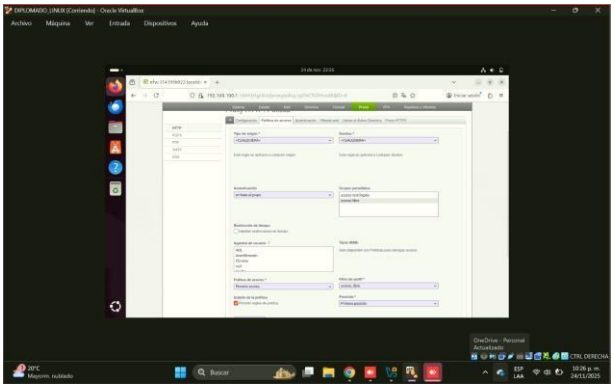
Ilustración 36. Creación de los grupos



Fuente: Autoría Propia

Se crean los 2 grupos que se van a utilizar para el acceso restringido y el acceso libre.

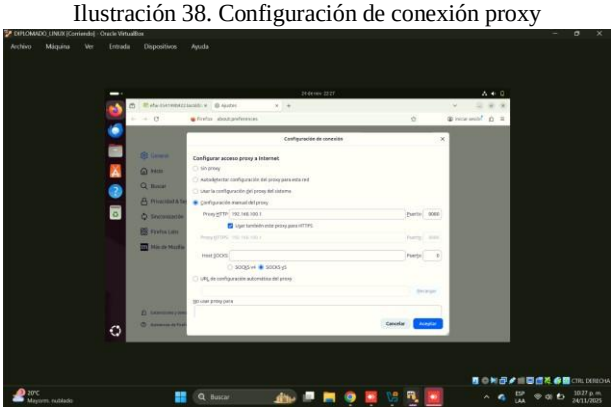
Ilustración 37. Políticas de acceso



Fuente: Autoría Propia

Se crean las 2 políticas de acceso para cada uno de los grupos que se crearon anteriormente.

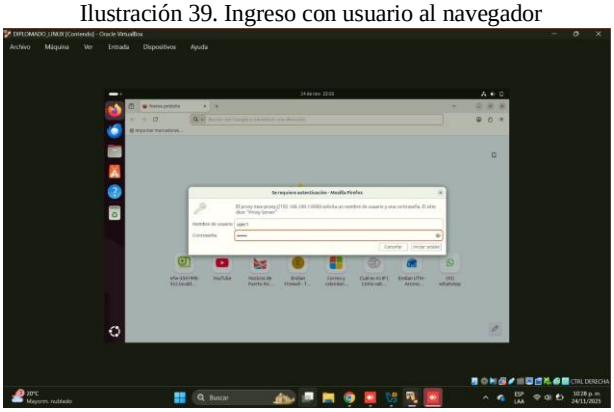
Ilustración 38. Configuración de conexión proxy



Fuente: Autoría Propia

Se realiza la configuración del proxy en el navegador donde se va a utilizar el proxy y en este se asigna la IP de Endian.

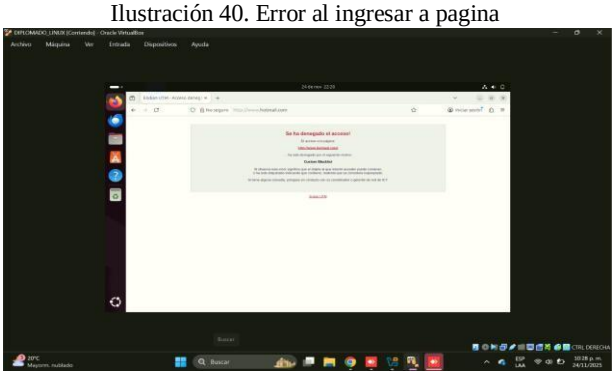
Ilustración 39. Ingreso con usuario al navegador



Fuente: Autoría Propia

Se inicia sesión al navegador con el usuario limitado para validar las url bloqueadas.

Ilustración 40. Error al ingresar a pagina



Fuente: Autoría Propia

Se ingresa a la página que debe estar bloqueada y se valida que el ingreso no lo permitan.

7 CONCLUSIONES

La implementación del esquema de red con Endian Firewall permitió comprender cómo la segmentación por zonas (Roja, Verde y Naranja) facilita el control del tráfico y la protección de los recursos internos. A través de la asignación correcta de direcciones, la activación de servicios y la verificación mediante pruebas de conectividad entre las máquinas, se evidenció la importancia de un firewall perimetral para garantizar aislamiento, filtrado y estabilidad en la comunicación. En conjunto, este ejercicio demuestra que una configuración adecuada de red y seguridad es esencial para mantener un entorno funcional y protegido.

La configuración de NAT en Endian permitió comprobar cómo el firewall gestiona la salida de las redes internas mediante reglas automáticas de enmascaramiento. La correcta asignación de las zonas Verde, Naranja y Roja fue fundamental para asegurar que cada segmento funcionara según su propósito. Con esto podemos decir que LAN y DMZ lograron comunicarse con la red externa sin comprometer la estructura interna, donde se demuestra la importancia de la segmentación y el manejo adecuado de las direcciones en entornos de seguridad

La definición de una sólida arquitectura de seguridad marcó la conclusión del proceso de implementación del Endian Firewall. Se definieron las áreas NARANJA (192.168.1.15) y VERDE (192.168.3.15). La administración de seguridad se centró en establecer políticas de tráfico saliente que habilitan el acceso a servicios fundamentales como FTP (puerto 21) y HTTP (puerto 80) hacia la red de Internet. Al mismo tiempo, para asegurar la segmentación, se estableció una rigurosa norma de bloqueo de ICMP entre NARANJA y VERDE. Esta regla limitaba específicamente el ping y otras herramientas de diagnóstico entre las subredes.

Con el desarrollo de esta actividad, he logrado adquirir nuevos conocimientos, fortalecer los que ya poseo y saber que este mundo de Linux es muy grande, entonces es algo bueno porque podré seguir aprendiendo y mejorando cada más, pero con dedicación y esfuerzo ya que eso es la clave. Como mencioné, he fortalecido conocimientos como el uso de VirtualBox, donde cada vez voy mejorando en la creación de una nueva máquina virtual, voy mejorando en cuanto el uso de comandos, y voy mejorando en cuanto a la analítica e investigación de información cuando se me presenta algún error al usar un comando o al intentar gestionar alguna función o actualización.

No conocía sobre seguridad perimetral, y gracias a esta actividad me he dado cuenta que existe la distribución Endian, la cual me ayuda con la protección de los servidores que conforman la Intranet, donde se pueden hacer limitaciones a través de una zona DMZ para garantizar la integridad de las bases de datos y aplicaciones de Linux, entonces pienso que saber esto, y bueno no solo saber, sino conocer y saber usar esta distribución es algo sumamente importante y ayuda mucho en la vida del profesional que quiera trabajar administrando servicios esenciales.

La implementación del Proxy HTTP no transparente en Endian permite controlar y supervisar de forma efectiva la navegación desde la red interna, aplicando autenticación de usuarios y filtrado de contenidos. Esta configuración fortalece la seguridad perimetral, garantiza el cumplimiento de las políticas de acceso y asegura un uso adecuado de los recursos de Internet dentro de la organización.

8 REFERENCIAS

[1] UNAD. (2025, mayo). Diseño de una arquitectura de red segura segmentada usando Endian Firewall Community. Universidad Nacional Abierta y a Distancia.

[2] Ubuntu Documentation. (s. f.). Cómo instalar y configurar isc-dhcp-server. Recuperado de https://ubuntu.com/server/docs/how-to-install-andconfigure-isc-dhcp-server

[3] AprendoLinux. (s. f.). Qué es DHCP y cómo instalar un servidor en Ubuntu. Recuperado de https://aprendolinux.com/que-es-dhcp-y-como-instalar-unservidor-en-ubuntu/

[4] Ubuntu Documentation. (s. f.). Cómo instalar y configurar isc-dhcp-server. Recuperado de https://ubuntu.com/server/docs/how-to-install-andconfigure-isc-dhcp-server

[5] Endian Technologies. (2016). Endian Firewall Community Documentation. Recuperado de https://community.endian.com/

[6] Jones, J. (2007, febrero 6). Networks (2.ª ed.). http://www.atm.com

[7] WordPress. (s. f.). WordPress.com: Todo lo que necesitas para crear tu web. Recuperado de https://wordpress.com/es/

[8] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server. Packt Publishing.https://research-ebscocom.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[9] Linux Professional Institute. (2023). Linux Essentials Study Guide (versión en español). Recuperado de https://www.lpi.org/es/study-resources

[10] Debian Handbook. (2022). Administración de redes en GNU/Linux. Recuperado de https://debian-handbook.info