GNU/LINUX ENDIAN COMO SOLUCIÓN DE SEGURIDAD PARA REDES SEGMENTADAS

Juan David Hurtado Giraldo
e-mail: jdhurtadog@unadvirtual.edu.co
Kennedy Absalom Zuñiga Ceron
e-mail: kazunigac@unadvirtual.edu.co
Jhon Jairo Rodriguez Arcos
e-mail: jjrodriguezarc@unadvirtual.edu.co
Walter Pajon Giraldo
e-mail: Wpajong@unadvirtual.edu.co
Jeison Andrés Tabares Duque
e-mail: jatabaresd@unadvirtual.edu.co

RESUMEN: En e*ste documento se presenta la implementación de un entorno virtual de red segmentado utilizando VirtualBox y GNU/Linux Endian. El escenario se organiza en tres zonas: verde, naranja y roja, cada una conectada a diferentes interfaces del sistema operativo Endian. Se implementaron diversos mecanismos de seguridad, incluyendo reglas de NAT, control de tráfico mediante firewall, autenticación de usuarios a través de un proxy y la utilización de una lista negra de navegación. El objetivo principal de este trabajo es demostrar el potencial de Endian como una solución libre y eficaz para el aseguramiento de redes. La segmentación de la red permite gestionar el tráfico de manera más eficiente y aplicar políticas de seguridad específicas para cada zona, minimizando los riesgos y mejorando la protección general del entorno. Además, se destaca la facilidad de configuración y administración que ofrece Endian, lo que lo convierte en una opción atractiva para organizaciones que buscan robustecer su infraestructura de seguridad sin incurrir en altos costos. En conclusión, la implementación de este entorno virtual no solo resalta la funcionalidad de Endian, sino que también proporciona un marco práctico para la gestión segura de redes en entornos diversos.*

PALABRAS CLAVE: Endian firewall, DMZ, NAT, seguridad perimetral.

1 INTRODUCCIÓN

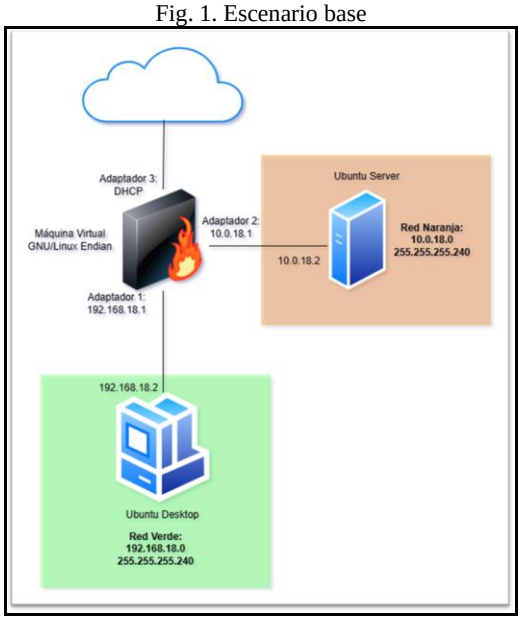
Dada la creciente velocidad con la que evolucionan y se propagan las amenazas informáticas en la actualidad, contar con soluciones de seguridad robustas y confiables se ha convertido en una necesidad crítica para organizaciones y entornos educativos por igual. En este contexto, la distribución GNU/Linux Endian destaca como una opción especialmente diseñada para la protección perimetral, ofreciendo de manera integrada una serie de herramientas esenciales como firewall, traducción de direcciones de red (NAT), servidor proxy, y otros servicios relacionados con la seguridad de redes.

Este documento tiene como propósito mostrar la implementación práctica de un entorno virtualizado en el cual se despliega GNU/Linux Endian como una solución de seguridad dentro de una red segmentada. Esta red está compuesta por distintas zonas: una red local (LAN), una zona desmilitarizada (DMZ), y una simulación de acceso a Internet, lo que permite evaluar su rendimiento en escenarios diversos y controlados.

2 METODOLOGÍA

El escenario base consiste en una máquina virtual con GNU/Linux Endian que cuenta con 3 interfaces de red, la red verde (LAN) utilizará el direccionamiento 192.168.18.0/28 en donde se tendrá una máquina virtual con Ubuntu desktop, la red naranja (DMZ) que contará con una máquina virtual con Ubuntu Server y la red roja (WAN) en donde se encuentra el equipo host que ejecuta los diferentes equipos virtualizados. A continuación, se muestra una ilustración del escenario.

Fig. 1. Escenario base



Fuente: Autoría propia

Una vez definido el escenario base, se crea la máquina virtual que se utilizará para el sistema GNU/Linux Endian y se configuran los adaptadores de red tal como se muestra en la siguiente imagen.

Fig. 2. Adaptadores de red

Fuente: Autoría propia

3 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN

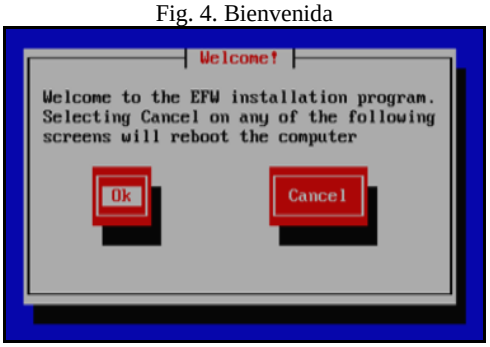
Teniendo la configuración de las tarjetas de red en cada una de las zonas en la máquina virtual de Endian, se procede a iniciar el equipo, configurado para que inicie desde la unidad óptica virtual que apunta a la imagen iso del sistema operativo y, a continuación, se comienza en el primer paso con la selección del idioma de instalación [1], como se observa en la siguiente figura.

Fig. 3. Selección de idioma

Fuente: Autoría propia

Para este caso se selecciona el idioma inglés y se continúa con la instalación, la cual brinda la bienvenida e indica que al presionar "Cancel" en cualquiera de las pantallas de instalación se reiniciará el sistema, tal como se muestra en la siguiente ilustración.

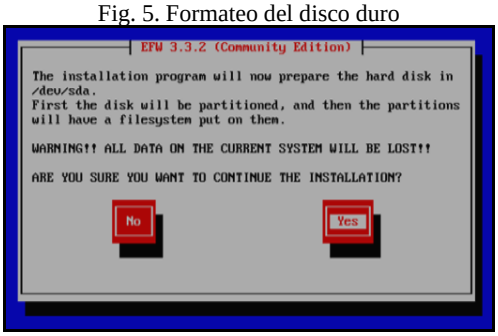
Fig. 4. Bienvenida



Fuente: Autoría propia

En la siguiente pantalla se indica que toda la información del disco duro va a ser eliminada ya que se va a particionar y formatear, se debe aceptar esta condición para poder continuar con la instalación, como se observa a continuación.

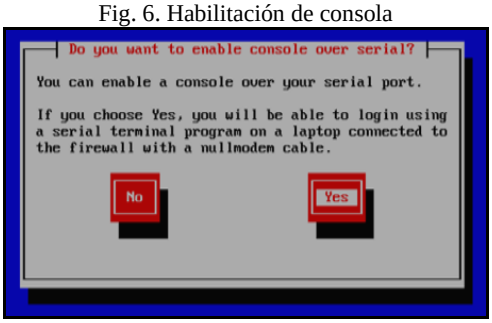
Fig. 5. Formateo del disco duro



Fuente: Autoría propia

Posteriormente se consulta si se desea habilitar la consola a través de un puerto serial, aunque este es un escenario virtual controlado, se selecciona que si ya que es ideal contar con dicho acceso desde otro equipo en escenarios reales en los que se requiera.

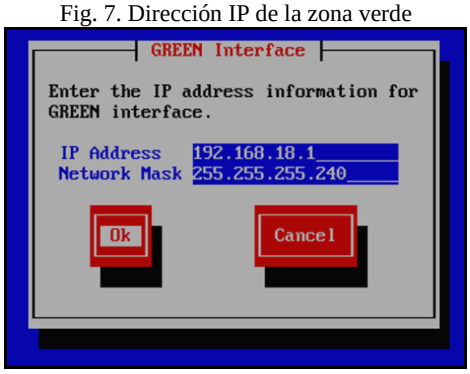
Fig. 6. Habilitación de consola



Fuente: Autoría propia

Como último paso de la instalación, se solicita configurar la dirección ip al adaptador de red conectado a la zona verde. En ese caso, se configura la dirección 192.168.18.1 de acuerdo con lo establecido en el escenario base de la figura 1.

Fig. 7. Dirección IP de la zona verde



Fuente: Autoría propia

Finalmente, se muestra la pantalla de felicitación, en donde se confirma la instalación exitosa de EFW en el computador y se informa que para finalizar la configuración del sistema se puede acceder desde un navegador web de un equipo en la zona verde a la dirección ip que se configuró al

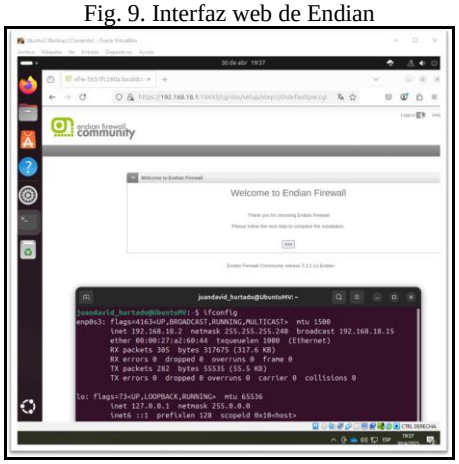
servidor, en este caso 192.168.18.1, tal como se observa en la siguiente imagen.

Fig. 8. Finalización de instalación

Fuente: Autoría propia

Al finalizar la instalación el sistema se reinicia, ahora se puede realizar la conexión a su interfaz de configuración web desde el navegador de un equipo que se encuentre en la red verde, para este caso se utiliza otra máquina virtual con Ubuntu Desktop, la cual tiene configurada una dirección ip 192.168.18.2 y se muestra por medio de la siguiente imagen el acceso desde el navegador Firefox a la interfaz de configuración web de Endian.

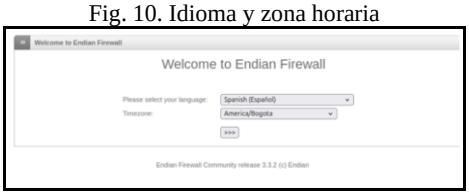
Fig. 9. Interfaz web de Endian



Fuente: Autoría propia

Al presionar siguiente, en la primera pantalla de configuración se solicita elegir el idioma de la interfaz y la zona horaria, para este caso se selecciona “Español” y la zona “America/Bogota” como se observa en la siguiente imagen

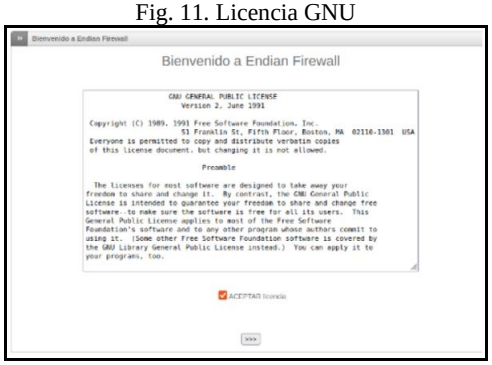
Fig. 10. Idioma y zona horaria



Fuente: Autoría propia

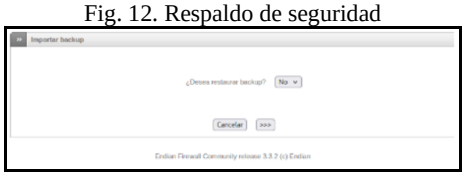
Posteriormente, se deben aceptar los términos de licencia, elegir si se va a restaurar alguna copia de seguridad (en este caso se selecciona “No” ya que es un escenario nuevo) y se configuran las contraseñas del usuario “admin” (acceso a la interfaz web) y del usuario “root” (acceso por consola o conexión presencial) como se observa en las siguientes figuras.

Fig. 11. Licencia GNU



Fuente: Autoría propia

Fig. 12. Respaldo de seguridad



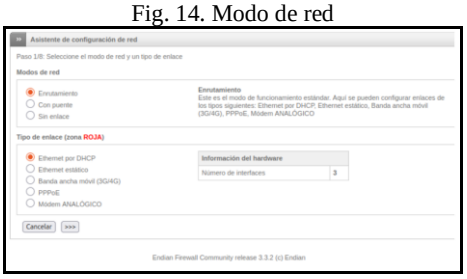
Fuente: Autoría propia

Fig. 13. Configuración de contraseñas

Fuente: Autoría propia

Una vez configuradas las contraseñas, se inicia el asistente de configuración de la red, en donde se selecciona el modo de red de enrutamiento (para este escenario de implementación de firewall y segmentación) y se habilita el direccionamiento DHCP en la interfaz roja (WAN) para que la máquina virtual tenga acceso a internet por medio del proveedor de servicios de la red física en el escenario de pruebas virtualizado.

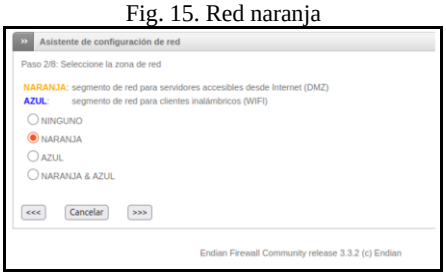
Fig. 14. Modo de red



Fuente: Autoría propia

Después, se procede a iniciar la configuración de la interfaz de red que apunta hacia la DMZ, es decir, la zona naranja en la que se ubicará otra máquina virtual con Ubuntu Server como sistema operativo y desde la cual se ofrecerán algunos servicios con protocolos como HTTP y FTP.

Fig. 15. Red naranja



Fuente: Autoría propia

A continuación, se configura la ip 10.0.18.1 con su respectiva máscara de 28 para la red naranja de acuerdo con lo establecido en el diagrama de la red, se selecciona el segundo adaptador de red y se configura el nombre de host como se observa en la siguiente imagen

Fig. 16. Direccionamiento en red naranja

Fuente: Autoría propia

Al continuar, se procede a finalizar la configuración de la zona roja, se confirma la configuración de servidores DNS automática para el presente escenario, a manera opcional se configuran direcciones de correo electrónico para el administrador y se acepta para finalizar la configuración, lo que reiniciará la conexión a la interfaz web del servidor como se muestra en las siguientes imágenes.

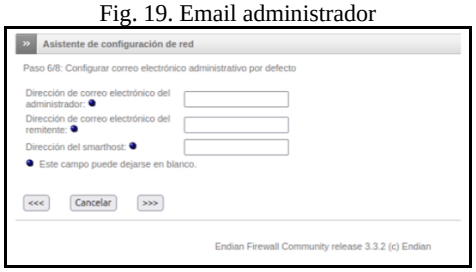
Fig. 17. Zona roja

Fuente: Autoría propia

Fig. 18. DNS: automático

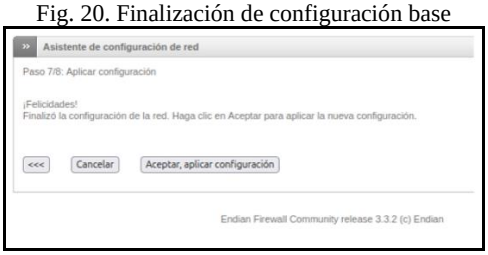
Fuente: Autoría propia

Fig. 19. Email administrador



Fuente: Autoría propia

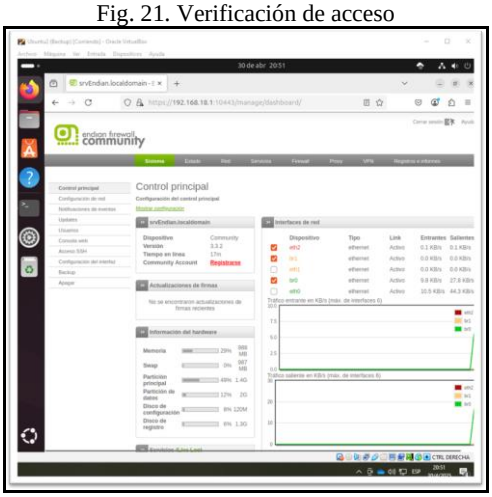
Fig. 20. Finalización de configuración base



Fuente: Autoría propia

Una vez se finaliza la configuración base, los servicios de Endian se reinician y la interfaz web se recarga solicitando las credenciales del usuario “admin” que se configuró. Al ingresar nuevamente se puede observar el panel de administración principal del sistema Endian como se muestra en la siguiente imagen

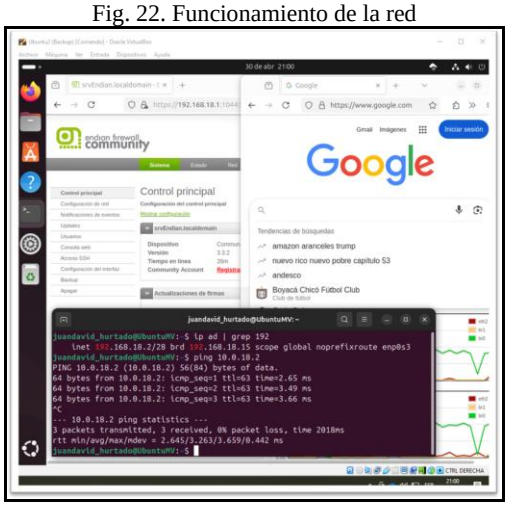
Fig. 21. Verificación de acceso



Fuente: Autoría propia

En este punto ya se finalizó la configuración del escenario base y se pueden iniciar las pruebas de conectividad. Para este escenario, se procede a confirmar la comunicación utilizando el navegador web Firefox y la terminal del sistema Ubuntu Desktop que se encuentra en la red LAN (zona verde). Desde el navegador se evidencia comunicación al servidor Endian ya que se tiene cargada su interfaz web de configuración. Además, en otra ventana del navegador se confirma el acceso a internet por medio del cargue del portal de Google y, finalmente, por medio de la terminal se realiza un ping a la dirección ip del servidor que se encuentra en la DMZ (zona naranja) con dirección ip 10.0.18.2. Estas pruebas se evidencian en la imagen a continuación.

Fig. 22. Funcionamiento de la red

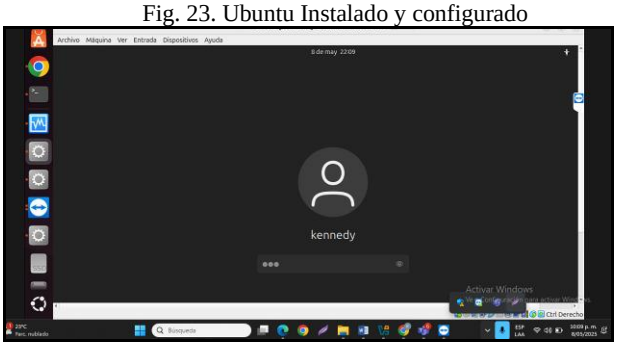


Fuente: Autoría propia

4 CONFIGURACIÓN NAT

Se inicia con la configuración de Ubuntu, verificando que el adaptador de red se encuentre en la misma red del servidor DCHP, en este caso red NAT. Se verifica si la maquina Ubuntu accede a internet. Finalmente, se verificó la dirección IP obtenida mediante DCHP (evidenciando que este en el rango de direcciones IP previamente configurados en nuestro DCHP Server).

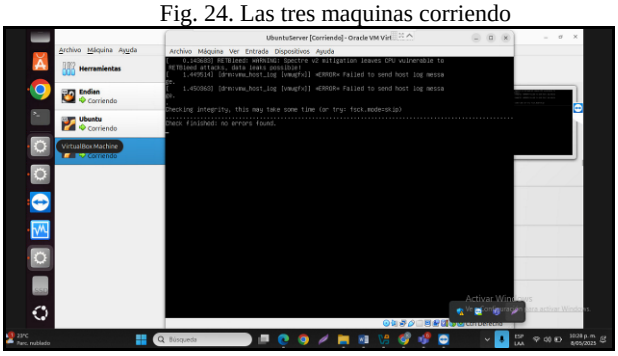
Fig. 23. Ubuntu Instalado y configurado



Fuente: Autoría propia

En este punto las 3 máquinas, se inicia exitosa las 3 corren con normalidad y de acuerdo con el requerimiento de la actividad.

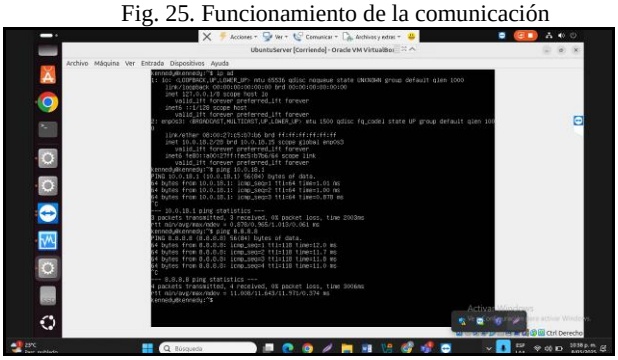
Fig. 24. Las tres maquinas corriendo



Fuente: Autoría propia

En este punto se configura la IP mediante el comando “ip ad”, y se ejecuta el, ping 10.0.18.1 se verifica que los servicios (como servidores web, FTP, etc.) estén corriendo en las interfaces.

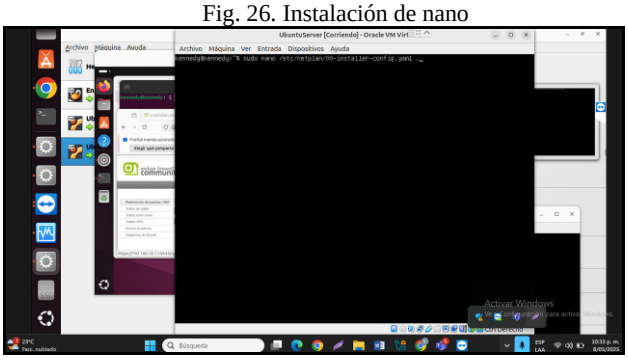
Fig. 25. Funcionamiento de la comunicación



Fuente: Autoría propia

Se procede a instalar nano mediante el comando sudo nano /etc/netplan/00-installer-config.yami

Fig. 26. Instalación de nano

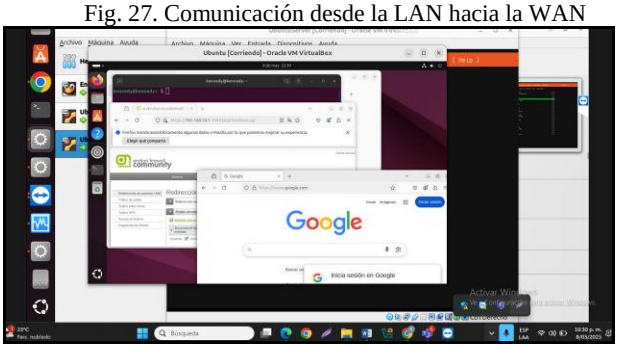


Fuente: Autoría propia

Se procede a Configurar la regla de NAT (Network Address Translación / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la

LAN hacia la WAN (Red simulada de Internet), el proceso genero un resultado exitoso, como se puede observar en la siguiente imagen que se anexa como evidencia, dando respuesta con ello al punto 1 de la tematica 2. Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el re-envió de puertos / NAT, la creación de las reglas.

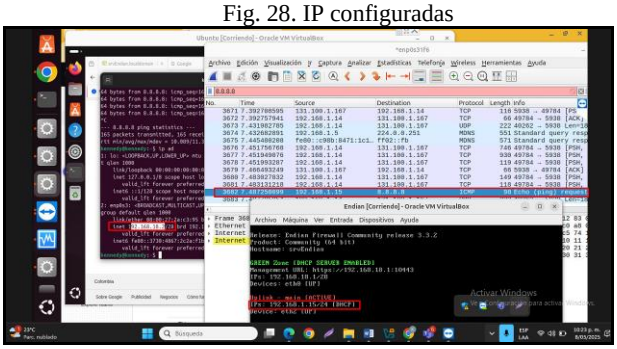
Fig. 27. Comunicación desde la LAN hacia la WAN



Fuente: Autoría propia

Se configura y ejecuta la respectiva instalacion mediante comandos, donde se obtiene la comunicación de las diferentes ip requeridas, inet 192.168.18.2/24, ping 192.168.1.15, endian 192.168.1.15/24 DCHP, como se evidencia en la siguiente imagen.

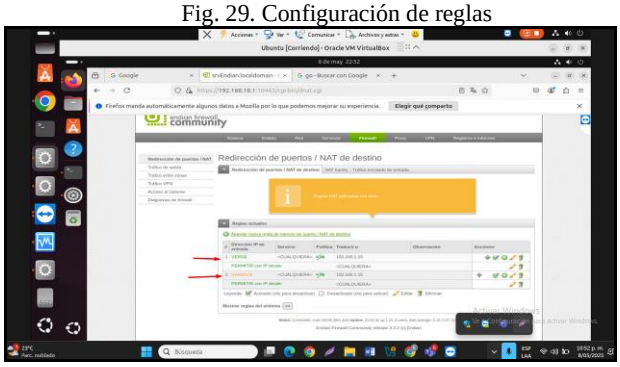
Fig. 28. IP configuradas



Fuente: Autoría propia

Ejecutado lo anterior se procede a realizar el punto 2, donde se configura la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Donde se verifico re-envió de puertos / NAT y se creo reglas, se anexa imagen como soporte de evidencia.

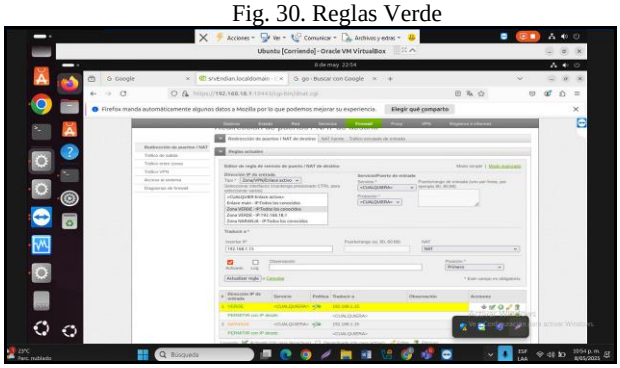
Fig. 29. Configuración de reglas



Fuente: Autoría propia

Realizado este punto se crean dos reglas en este caso, la siguientes, primera que desde la direccion ip de entrada Verde, genere un servicio cualquiera traducido a la ip 192.168.1.15 de Endian.

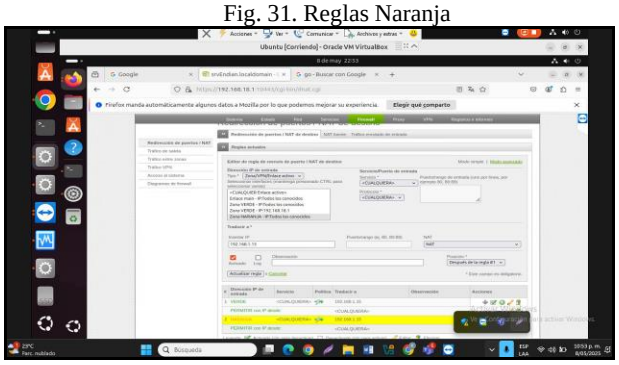
Fig. 30. Reglas Verde



Fuente: Autoría propia

Segunda regla, que desde la direccion ip de entrada Naranja, genere un servicio cualquiera traducido a la ip 192.168.1.15 de Endian.

Fig. 31. Reglas Naranja



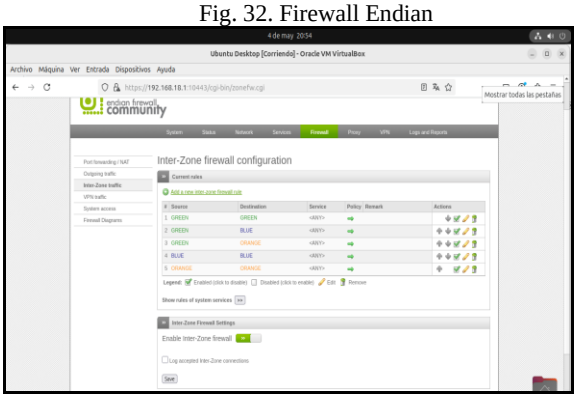
Fuente: Autoría propia

5 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

A continuación, se realiza la primera actividad, Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.

Se ingresa por el navegador a la interfaz del Servidor Endian por medio de la ip https://192.168.18.1:10443, y luego a la opción de firewall

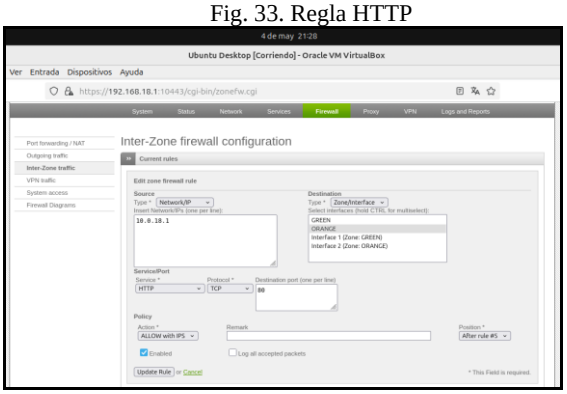
Fig. 32. Firewall Endian



Fuente: Autoría propia

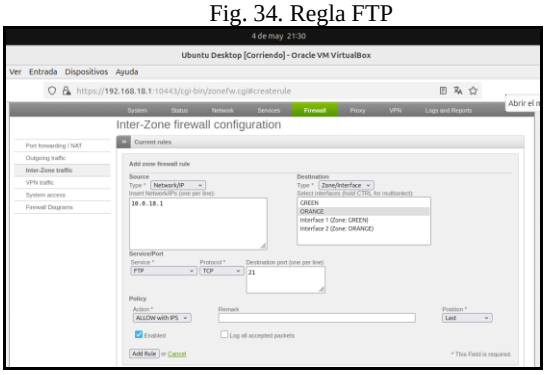
En la opción inter-Zone Traffic, se crea la regla para permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21)

Fig. 33. Regla HTTP



Fuente: Autoría propia

Fig. 34. Regla FTP



Fuente: Autoría propia

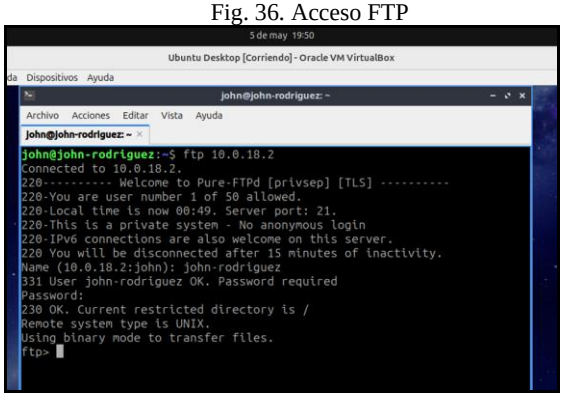
Se valida el acceso por el puerto 80 http desde el navegador y se indica la página del servicio Apache, ya que no hay configuradas páginas en el server por el momento

Fig. 35. Acceso HTTP

Fuente: Autoría propia

Se realiza la validación de la conexión ftp por el puerto 21, desde una terminal del Ubuntu de escritorio

Fig. 36. Acceso FTP

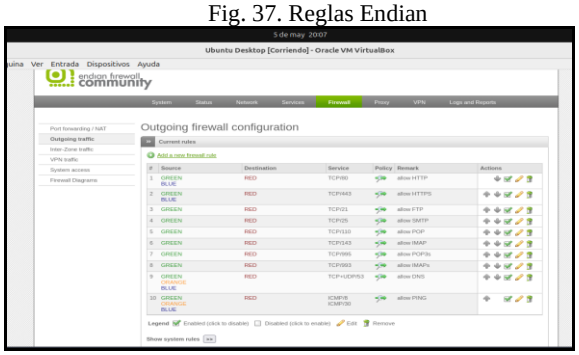


Fuente: Autoría propia

A continuación, se realiza la segunda actividad, 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.

Se ingresa a la interfaz del servidor Endian y luego a Firewall y Trafico de Salida y se cren las reglas

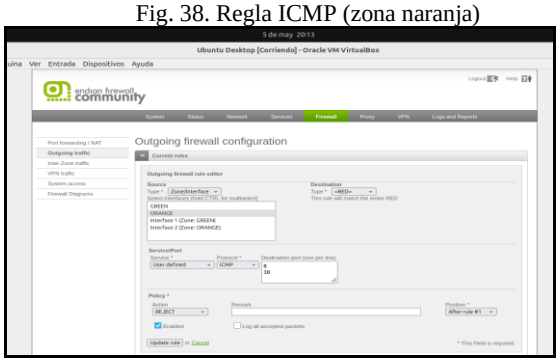
Fig. 37. Reglas Endian



Fuente: Autoría propia

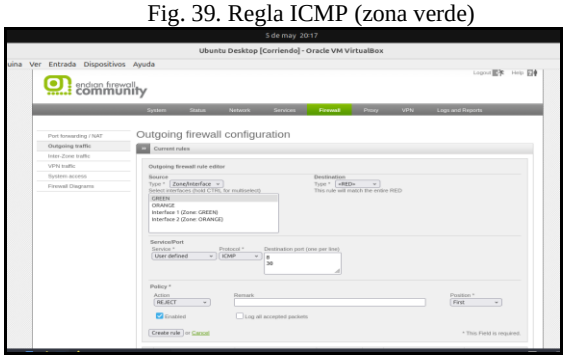
Se realiza la configuración ICMP (Puerto 8 y puerto 30)

Fig. 38. Regla ICMP (zona naranja)



Fuente: Autoría propia

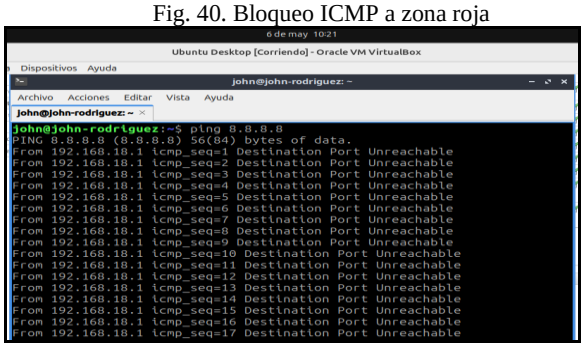
Fig. 39. Regla ICMP (zona verde)



Fuente: Autoría propia

Se realizan las comprobaciones de las reglas, por medio de validación con el ping a internet a los dns 8.8.8.8

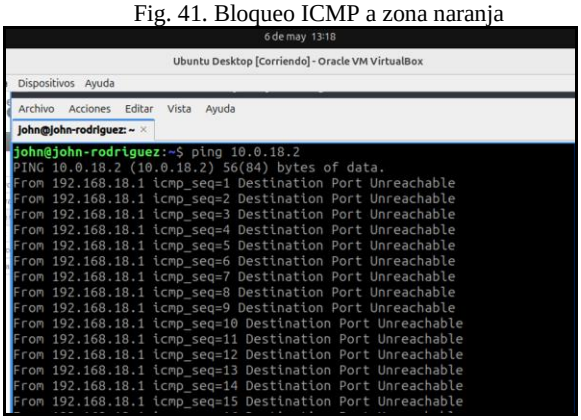
Fig. 40. Bloqueo ICMP a zona roja



Fuente: Autoría propia

Se realiza la validación ejecutando el ping al Server Ubuntu 10.0.18.2

Fig. 41. Bloqueo ICMP a zona naranja



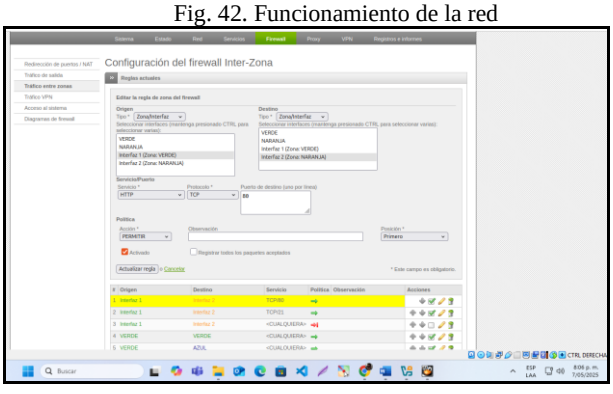
Fuente: Autoría propia

6 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En todo sistema de seguridad de red, la correcta configuración de las reglas de acceso es fundamental para controlar el flujo de datos entre diferentes zonas o segmentos de red. Estas reglas permiten definir qué tipo de tráfico está autorizado o restringido, según su origen, destino, protocolo o puerto utilizado. A través del firewall, es posible establecer políticas que protejan los recursos internos, permitan servicios específicos como HTTP o FTP, y bloqueen intentos no autorizados, reduciendo así riesgos de intrusión o fuga de información. En esta sección se documenta la creación, aplicación y verificación de reglas de acceso utilizando Endian Firewall, como herramienta clave para garantizar una comunicación segura y segmentada entre zonas como LAN, DMZ y WAN.

Se configura la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos, se crea regla en nuestro firewall para permitir la comunicación y el tráfico desde la zona verde a la naranja como se muestra en la siguiente imagen.

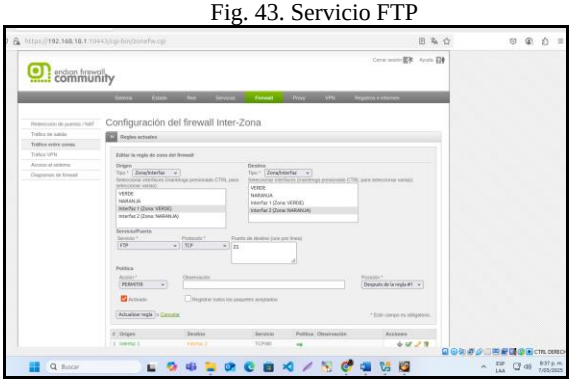
Fig. 42. Funcionamiento de la red



Fuente: Autoría propia

Creación regla ftp puerto 20 para comunicar nuestro desktop con la zona naranja.

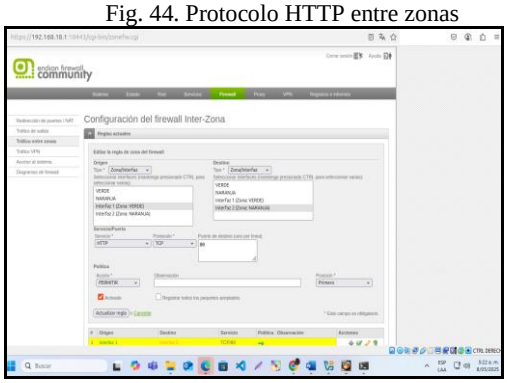
Fig. 43. Servicio FTP



Fuente: Autoría propia

Esta imagen muestra la configuración de una regla en el firewall de Endian para permitir el tráfico HTTP desde la zona verde (LAN) hacia la zona naranja (DMZ). Esta regla utiliza el protocolo TCP en el puerto 80, lo que permite que el tráfico web fluya correctamente entre estas zonas de la red como se muestra en la siguiente imagen.

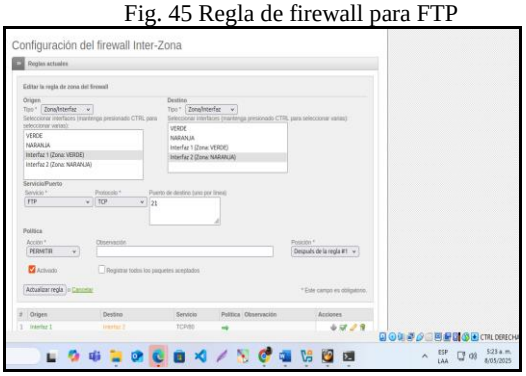
Fig. 44. Protocolo HTTP entre zonas



Fuente: Autoría propia

Se realiza la configuración de una regla en Endian Firewall para permitir el tráfico FTP desde la zona verde (LAN) hacia la zona naranja (DMZ). La regla se configura para permitir el tráfico en el puerto 21, el puerto por defecto para FTP, garantizando la transferencia de archivos entre estas zonas. como se muestra en la siguiente imagen.

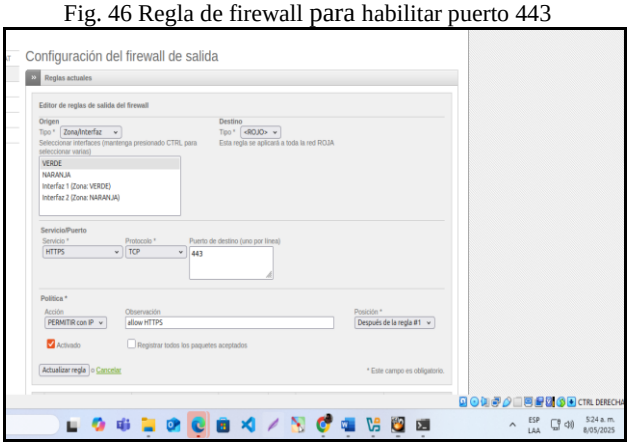
Fig. 45 Regla de firewall para FTP



Fuente: Autoría propia

En esta imagen se configura una regla en el firewall de Endian para permitir el tráfico de salida en el puerto 443, que corresponde a HTTPS. Esta regla permite que los dispositivos de la LAN puedan acceder a sitios web seguros en Internet, garantizando una navegación segura como se muestra en la siguiente imagen.

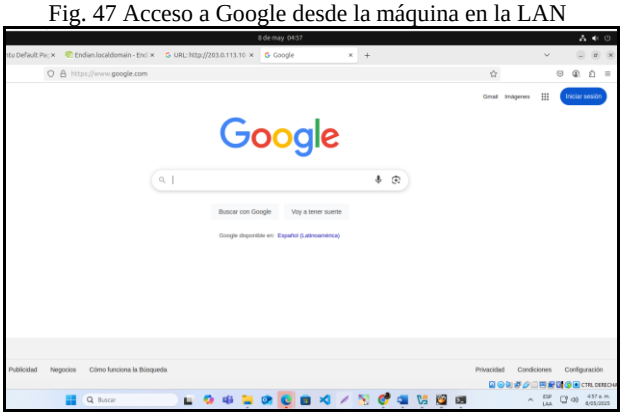
Fig. 46 Regla de firewall para habilitar puerto 443



Fuente: Autoría propia

Pruebas: la LAN tiene acceso a Internet, ya que se ha abierto la página de Google a través de un navegador web de Ubuntu Desktop. Esto indica que el tráfico de salida hacia la WAN está correctamente configurado y que la máquina puede acceder a sitios web externos sin problemas

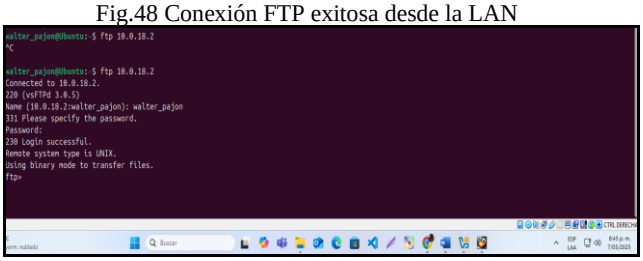
Fig. 47 Acceso a Google desde la máquina en la LAN



Fuente: Autoría propia

Una conexión FTP exitosa desde una máquina en la LAN hacia un servidor FTP ubicado en la DMZ. La conexión se estableció correctamente utilizando las credenciales configuradas, lo que confirma que el servicio FTP está funcionando correctamente entre estas zonas como se muestra en la siguiente imagen.

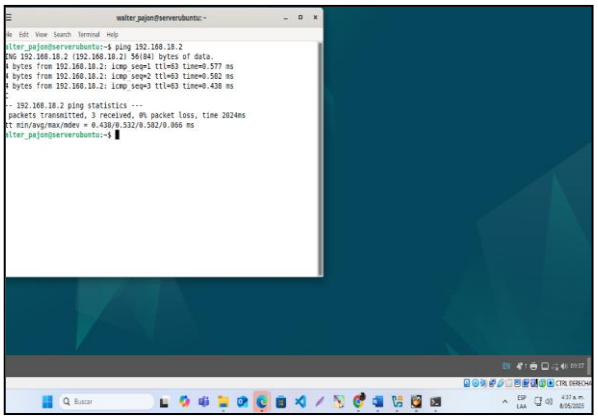
Fig.48 Conexión FTP exitosa desde la LAN



Fuente: Autoría propia

Se realiza prueba de ping desde una máquina en la LAN hacia un servidor en la DMZ (10.0.18.2). La prueba fue exitosa, ya que se recibieron respuestas con un tiempo de 204 ms y sin pérdida de paquetes, lo que indica que la conectividad entre la LAN y la DMZ está funcionando correctamente como se muestra en la siguiente imagen.

Fig.49 Prueba de ping en la máquina en la LAN hacia la DMZ



Fuente: Autoría propia

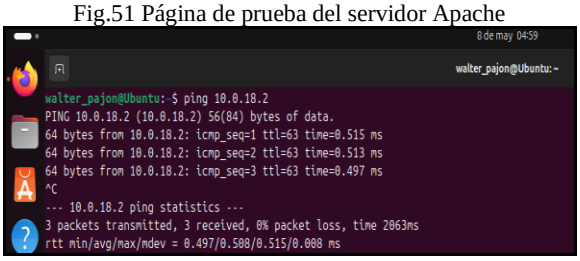
Página de bienvenida predeterminada de Apache en el servidor ubicado en la zona DMZ. Esta página aparece al acceder al servidor web a través del protocolo HTTP y confirma que el servidor Apache está instalado correctamente y funcionando

Fig.50 Página de prueba del servidor Apache

Fuente: Autoría propia

Prueba de ping desde la LAN hacia la DMZ con la IP 10.0.18.2, que muestra que los paquetes se enviaron y recibieron correctamente con 0% de pérdida. Esto confirma que la conexión entre estas dos zonas es estable y funcional como se muestra en la siguiente imagen.

Fig.51 Página de prueba del servidor Apache

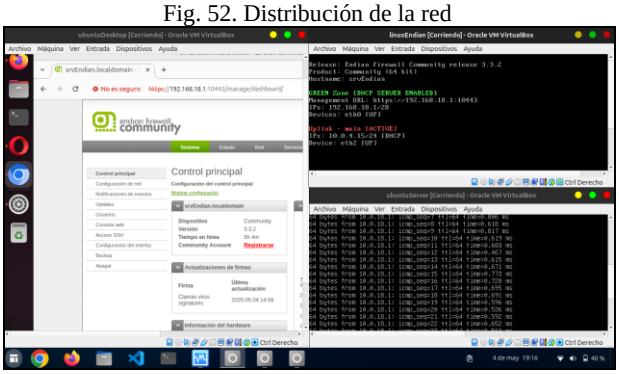


Fuente: Autoría propia

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

Para restringir el acceso a sitios web, es necesario configurar el proxy HTTP no transparente con políticas de autenticación en Endian Firewall para la distribución de red establecida. Los sitios a bloquear son www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.

Fig. 52. Distribución de la red



Fuente: Autoría propia

Para configurar el filtrado de contenido en Endian Firewall, se accede al panel de administración y se selecciona la opción **Proxy** en el menú superior. Dentro de las configuraciones disponibles, se procede a activar y ajustar los parámetros correspondientes al módulo de **Filtrado Web**, el cual permite gestionar políticas de acceso a sitios según los criterios predefinidos.

Fig. 53. Filtrado web

Fuente: Autoría propia

Dentro del módulo de **Filtrado Web**, se genera un **nuevo perfil** donde se definen los parámetros de bloqueo.

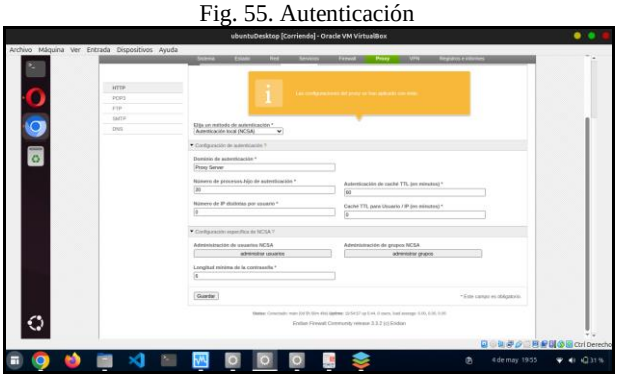
En la configuración del perfil creado, se registran los dominios o URLs a restringir mediante su inclusión en **la lista negra**. Este mecanismo permite un control sobre el acceso a contenidos no permitidos según las políticas de seguridad establecidas.

Fig. 54. Perfil de filtrado

Fuente: Autoría propia

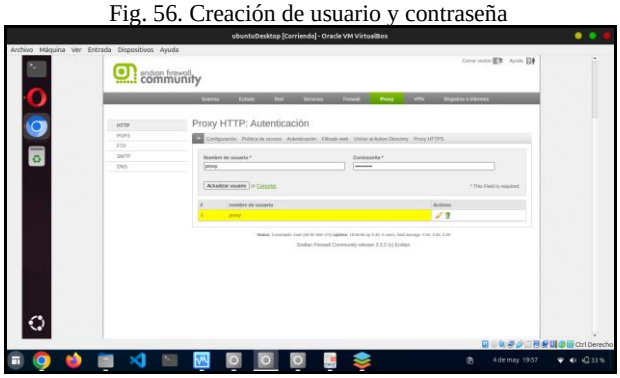
Para verificar la identidad de los usuarios antes de permitirles conectarse a la web, en el módulo de **autenticación** del proxy, se registran los **usuarios y grupos autorizados**, definiendo credenciales únicas para cada uno.

Fig. 55. Autenticación



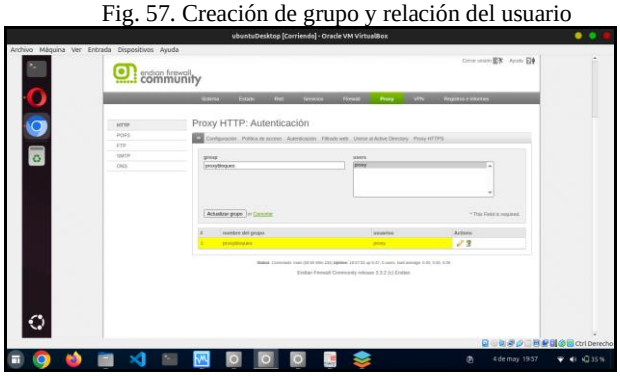
Fuente: Autoría propia

Fig. 56. Creación de usuario y contraseña



Fuente: Autoría propia

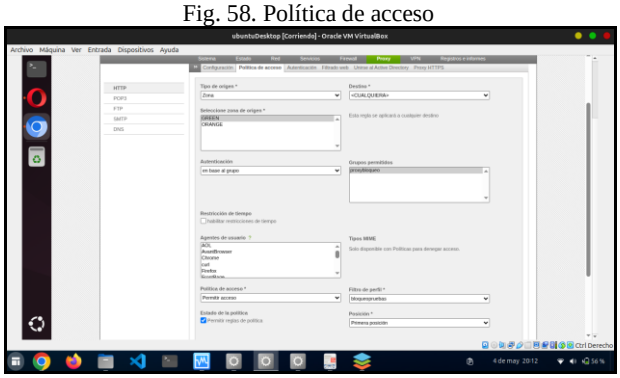
Fig. 57. Creación de grupo y relación del usuario



Fuente: Autoría propia

En el apartado de **política de acceso**, se define una **nueva política** donde se especifican los permisos de navegación para el **grupo de usuarios** previamente establecido.

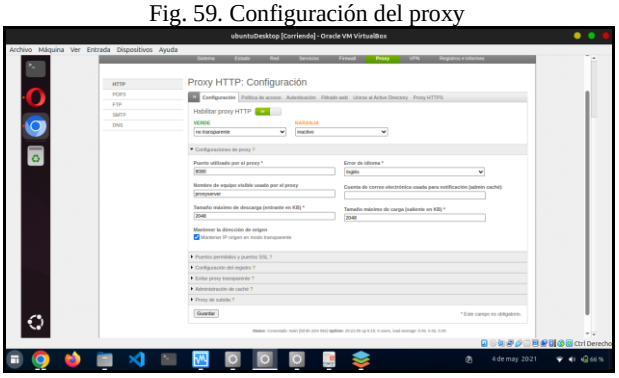
Fig. 58. Política de acceso



Fuente: Autoría propia

Por último, se enciende el proxy estableciéndolo como no transparente. Este ajuste requiere que las aplicaciones cliente, como navegadores web, sean configuradas para saber que el proxy está en uso.

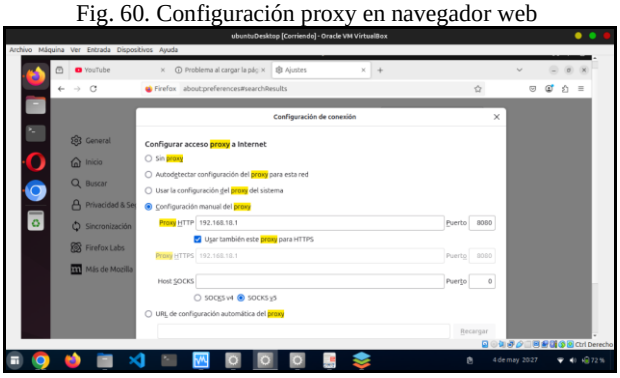
Fig. 59. Configuración del proxy



Fuente: Autoría propia

Tras guardar los ajustes en el servidor proxy, es necesario configurar manualmente los navegadores web para redirigir el tráfico HTTP/HTTPS a través del servicio proxy implementado.

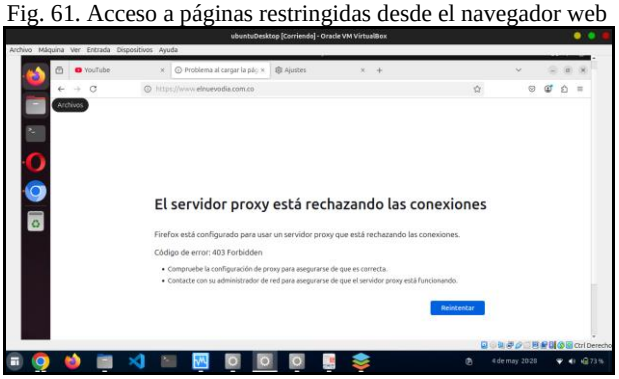
Fig. 60. Configuración proxy en navegador web



Fuente: Autoría propia

Al intentar acceder a páginas web, los usuarios deben autenticarse mediante las credenciales previamente registradas en el proxy de Endian.

Fig. 61. Acceso a páginas restringidas desde el navegador web



Fuente: Autoría propia

8 CONCLUSIONES

La configuración inicial de GNU/Linux Endian en el entorno virtualizado permitió montar una red segmentada implementando seguridad perimetral ya que, la distribución de las interfaces de red y configuración del enrutamiento, permitieron la conexión entre las zonas verde, naranja y roja. Este escenario otorga un ejemplo de como proteger una red local incluso al estar ofreciendo servicios alojados en su interior por medio de la traducción NAT.

La habilitación de los servicios HTTP (puerto 80) y FTP (puerto 21) en un servidor web bajo Ubuntu Server es un proceso fundamental para garantizar la accesibilidad y gestión remota de los contenidos web y archivos. A través de la correcta configuración del firewall (UFW), se logró permitir el tráfico entrante a estos servicios, asegurando que el servidor esté disponible para clientes web y aplicaciones FTP.

La denegación del protocolo ICMP, específicamente los tipos de mensaje Echo Request (tipo 8) y Timestamp Request, es una medida efectiva para limitar la capacidad de diagnóstico y exploración de red por parte de usuarios externos o no autorizados.

En el contexto de Endian Firewall, las reglas de acceso juegan un papel fundamental para garantizar la seguridad y el control del tráfico entre diferentes zonas de red, como la zona de Internet, la zona DMZ y la red interna (zona verde).

Por último, la implementación de un proxy HTTP con autenticación explicita puede ser una solución efectiva para el control de acceso a páginas web en entornos corporativos y ofrece ventajas significativas en términos de seguridad y gestión debido a la autenticación obligatoria para asociar el tráfico web, facilitando la auditoría, el cumplimiento de políticas y la detección de patrones de uso inapropiado

9 REFERENCIAS

[1] Caratar, D., Tovar, B. Endian firewall. instalación y configuración. Servicio Nacional de Aprendizaje SENA. 2012

[2] Molina, K. J. M., Meneses, J. P., & SILGADO, I. Z. (2009). Firewall–linux: Una solución de seguridad informática para pymes (pequeñas Y medianas empresas). Revista UIS Ingenierías, 8(2), 155-165.

[3] Sotelo Salamanca, E. D. Configuración de NAT, DHCP y protocolos de enrutamiento.

[4] Fernández Rojas, Á. (2013). Diseño y desarrollo de un sistema de detección de NATS para un monitor de tráfico residencial.

[5] Escobar, D. E. Z., Tangarife, I. L. G., Munera, J. D. A., Ibarra, C. H. O., & Arango, D. A. G. (2023). Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL. INGENIERÍA: Ciencia, Tecnología e Innovación, 10(1), 98-115.

[6] Corpeño, I. A. C. (2020). Zona Desmilitarizada (DMZ).

[7] Caicedo Veintimilla, A. T. (2022). Herramientas firewall basadas en tecnologías OpenSource (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

[8] Sánchez Cristancho, S. C., Bautista Cuevas, W., Cuero Tovar, A. M., Cruz Franco, J. C., & Rojas Peña, C. O. (2018). Diplomado de profundización en Linux.

[9] Iñaguazo Velepucha, J. S. (2022). Estudio de Alternativas para la implementación de un Sistema Unificado de Seguridad Informática utilizando hardware de bajo costo y software libre (Bachelor's thesis, Quito: EPN, 2022.).

[10] Vargas Rodríguez, S. F., Méndez Madrigal, D. E., Moreno, M. S., & Torres Gasca, I. S. Proxy no transparente.