IMPLEMENTACIÓN DE ENDIAN FIREWALL PARA LA PROTECCIÓN DE REDES INFORMÁTICAS

Manuel Andrés De Avila Cantillo
e-mail: madeavilac@unadvirtual.edu.co
Joan Manuel Ocampo Herrera
e-mail: jmocampoh@unadvirtual.edu.co
Kevin Yesid Rodríguez Obediente
e-mail: kjrodriguezob@unadvirtual.edu.co
Yecid Pimentel Chávez
e-mail: yapimentelc@unadvirtual.edu.co

RESUMEN: *Garantizar la seguridad perimetral en las redes informáticas se ha convertido en una necesidad para los administradores de red en las distintas empresas a nivel internacional, debido a las constantes amenazas a las que se pueden ver expuestos los servidores y bases de datos que poseen información sensible de alta relevancia. En este artículo se expone la instalación, configuración y puesta en marcha de la distribución de GNU/Linux Endian (EFW). Esta distribución será el cortafuegos que se encargará de administrar el tráfico de la red en general, firewall de administración para la aplicación de las reglas NAT, el habilitador de servicios en puertos específicos y el regulador que permitirá o denegará el tráfico sobre ciertos protocolos de red.*

PALABRAS CLAVE: Cortafuegos, protección de servidores, protocolos, tráfico entre zonas.

1 INTRODUCCIÓN

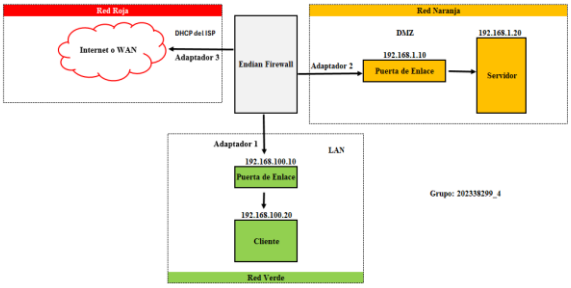
La implementación de las reglas de acceso mediante cortafuegos es una parte importante para la protección de ordenadores, servidores y bases de datos, ya que a través de estas se puede permitir o denegar el tráfico en la red, mitigando ataques cibernéticos y la propagación de virus mal intencionados a través de las redes informáticas.

En este contexto el poder identificar las necesidades a nivel de seguridad que requiere una red corporativa es indispensable para mantener un apropiado uso de cada uno de los servicios, protocolos y los equipos presentes en la red. Con base a estas necesidades se implementó la distribución GNU/Linux Endian (EFW) la cual actúa como un cortafuegos, dando paso a reglas de seguridad que brindan conectividad entre las zonas verde, naranja y roja, a su vez delimita servicios en la zona DMZ y realiza la apertura de puertos específicos. Como primer paso se creó el direccionamiento de red en cada una de las zonas para posteriormente parametrizar el tráfico entre ellas, los accesos permitidos y los servicios disponibles.

2 DIRECCIONAMIENTO DE LA RED

Una buena estructuración de la red permitirá parametrizar de una forma adecuada cada proceso y cada servicio, por lo cual es importante segmentar de manera correcta. A continuación, se expone el esquema que define el direccionamiento a trabajar.

Figura 1. Direccionamiento de la red



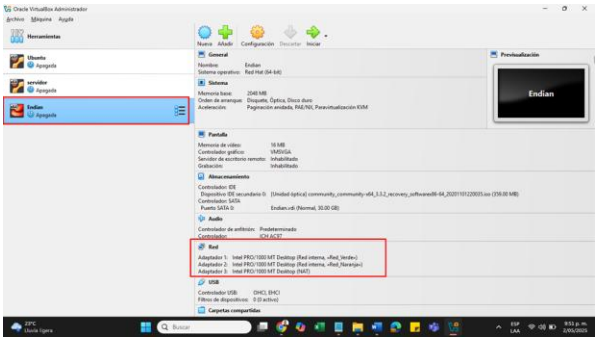
Fuente: Autoría Propia

3 IMPLEMENTACION DE SEGURIDAD PERIMETRAL PARA LA PROTECCION INTRANET Y EXTRANET

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

Se inició creando la máquina virtual para la instalación de GNU/Linux Endian en la herramienta VirtualBox, habilitando 3 adaptadores de red dispuestos para las zonas verde, naranja y roja. El adaptador 1 corresponde a la zona verde (LAN), el adaptador 2 a la zona naranja (DMZ) y el adaptador 3 a la zona roja (WAN), los adaptadores 1 y 2 quedaran segmentados en red interna, mientras que el 3 queda como NAT.

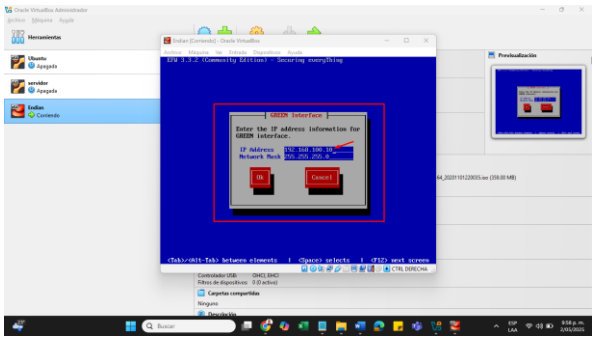
Figura 2. Configuración de adaptadores de red en VirtualBox



Fuente: Autoría Propia

Después de configurar los adaptadores de red en VirtualBox se procede con la instalación de los paquetes y las configuraciones iniciales. Se configura el direccionamiento de la zona verde, para este caso se asigna la dirección IP de la puerta de enlace 192.168.100.10 con prefijo /24

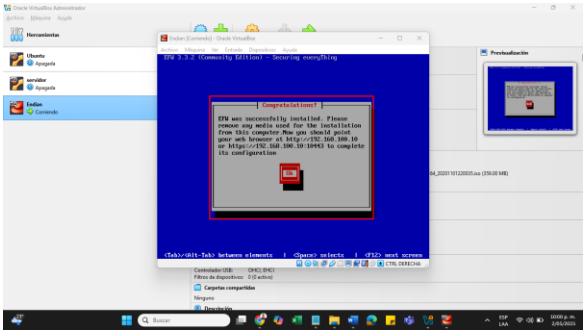
Figura 3. Asignación de la zona verde



Fuente: Autoría Propia

Cuando el asistente de instalación culmine el proceso, arroja el pantallazo que muestra la Fig. 4 indicando el enlace destinado para ingresar desde el navegador web de la máquina del cliente y poder acceder al panel de configuraciones del Endian Firewall.

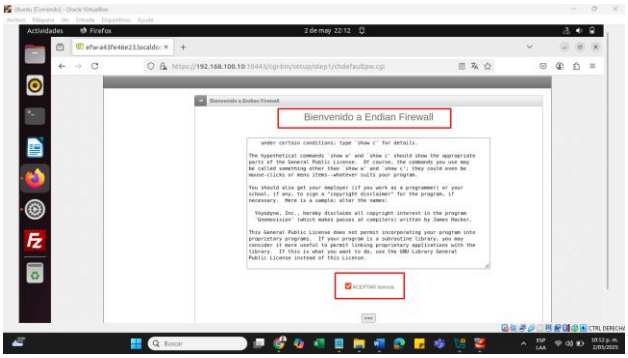
Figura 4. Ingreso al panel de configuraciones del Endian



Fuente: Autoría Propia

Ingresar al panel de configuraciones implica que se debe elegir el idioma con el que se desea trabajar, la zona horaria y aceptar la licencia.

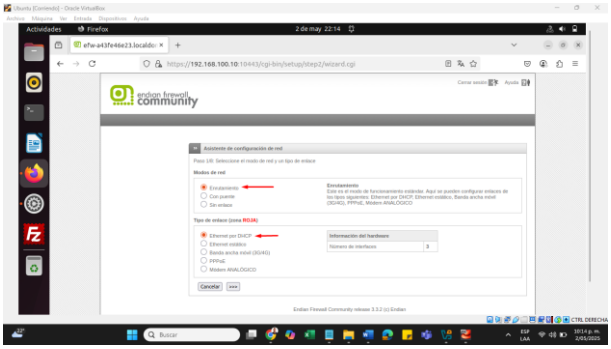
Figura 5. Aceptación de la licencia de Endian Firewall



Fuente: Autoría Propia

En el asistente de configuración se valida que el modo de red sea enrutamiento y el tipo de enlace en la zona roja sea por DHCP, para adquirir el direccionamiento desde el proveedor de servicio de internet (ISP) en esta zona.

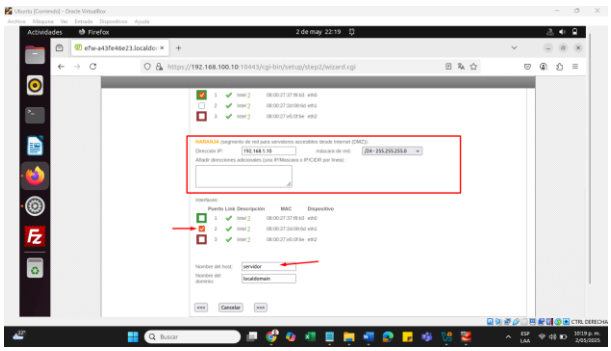
Figura 6. Verificación de modos de red



Fuente: Autoría Propia

Configurar la zona naranja es fundamental en este proceso de seguridad perimetral, porque es la encargada de administrar la zona DMZ en donde se encuentra alojado el servidor, para ello se aplica el segmento de red a trabajar y se selecciona la interfaz. La dirección IP que se debe asignar es la 192.168.1.10 la cual corresponde a la puerta de enlace de la zona DMZ, se habilita el puerto y se modifica el nombre del host.

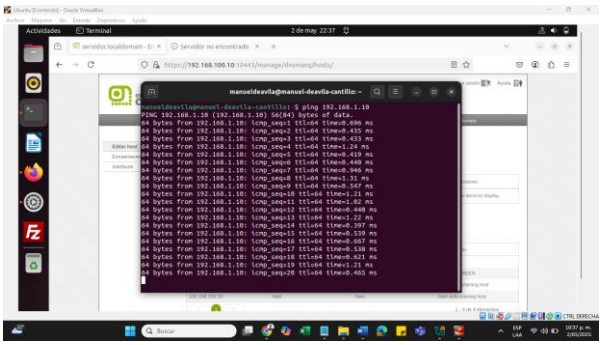
Figura 7. Segmentación de zona naranja



Fuente: Autoría Propia

Se realiza un ping a la puerta de enlace de la zona naranja previamente configurada para comprobar respuesta y la conexión exitosa.

Figura 8. Ping hacia la zona naranja



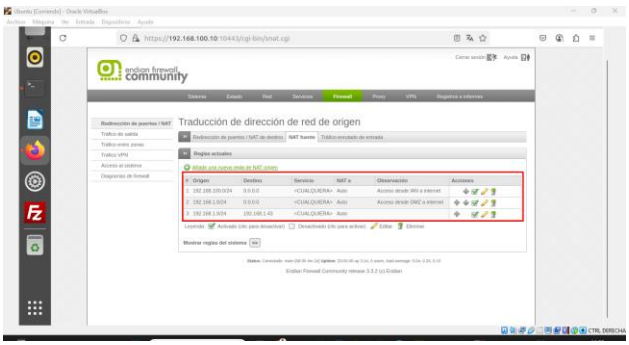
Fuente: Autoría Propia

3.2 CONFIGURACIÓN NAT

Se busca configurar reglas NAT para la traducción de direcciones de red, demostrar conexión desde la LAN hacia la WAN y desde la zona DMZ hacia internet, se debe verificar el reenvió de puertos y comprobar los resultados.

La solución inicia ingresando al apartado Firewall > NAT Fuente del panel de configuraciones de Endian Firewall. Se establece la regla para que la LAN identificada con dirección de red 192.168.100.0/24 pueda tener acceso a internet, luego se crea la regla que permita a la zona DMZ identificada con la red 192.168.1.0/24 acceder a internet o a la red WAN.

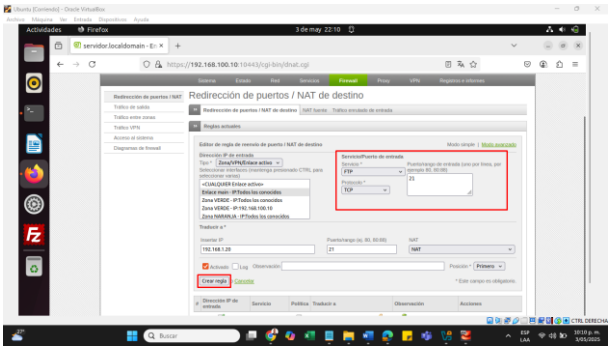
Figura 9. Lista de reglas NAT



Fuente: Autoría Propia

Se define la redirección de puertos mediante una regla NAT para que se pueda acceder a ciertos servicios en el servidor como el servicio ftp en el puerto 21, capaz de permitir la transferencia de archivos o el servicio http con el puerto 80.

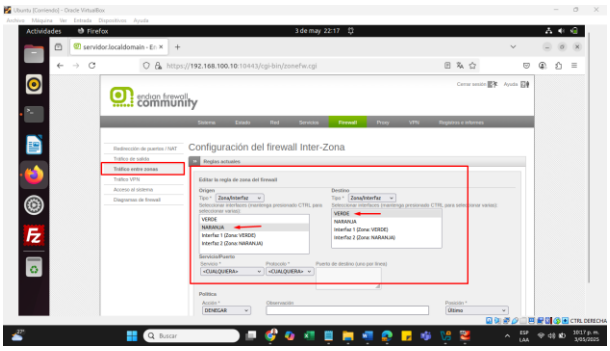
Figura 10. Apertura de puertos



Fuente: Autoría Propia

Cuando las reglas estén creadas, se debe habilitar el tráfico entre zonas para que se dé la comunicación entre ellas como muestra la Fig. 11, así mismo se aplican las reglas necesarias para comunicar las distintas zonas de la red.

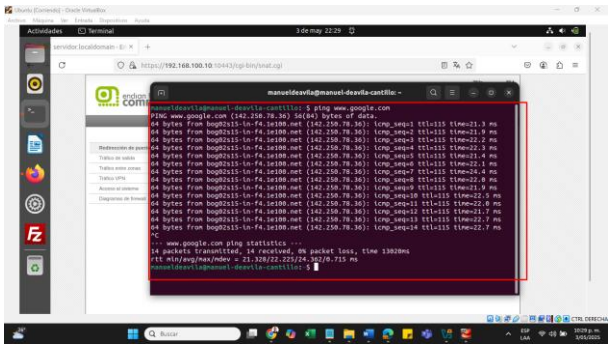
Figura 11. Tráfico entre zonas



Fuente: Autoría Propia

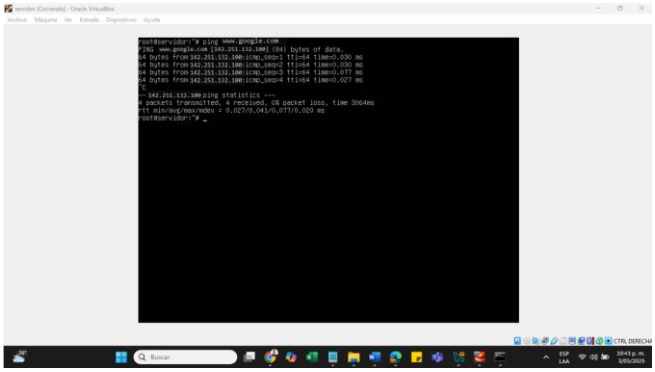
Se necesita verificar la funcionalidad de las reglas creadas anteriormente, demostrando la conexión desde la LAN hacia la WAN y la conectividad desde la zona DMZ a internet, en las Fig. 12 y Fig. 13 se realiza ping hacia www.google.com y se observa la conexión exitosa.

Figura 12. Ping desde la LAN a la WAN



Fuente: Autoría Propia

Figura 13. Ping desde la zona DMZ hacia internet



Fuente: Autoría Propia

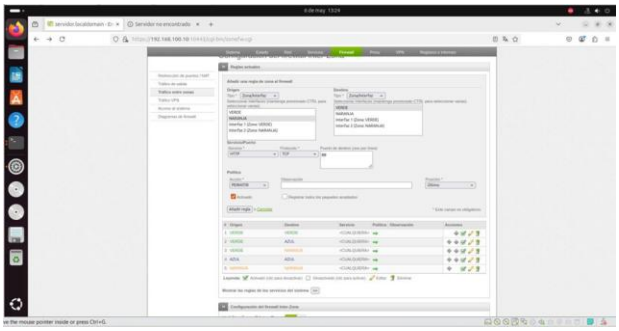
Con el uso del comando netstat -tuln se listan los puertos disponibles en el servidor de la zona DMZ, brindando una visión de su disponibilidad. De esta manera se comprueba el correcto funcionamiento de las reglas NAT creadas, la conectividad entre las zonas y el reenvió de los puertos habilitados.

3.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

En este punto de la implementación de la seguridad perimetral se desea permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor web bajo Ubuntu Server. Al mismo tiempo denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red por medio de ellos.

La habilitación de los servicios inicia dirigiéndose al apartado Firewall > Trafico de Salida, se crea la regla que permita el servicio HTTP.

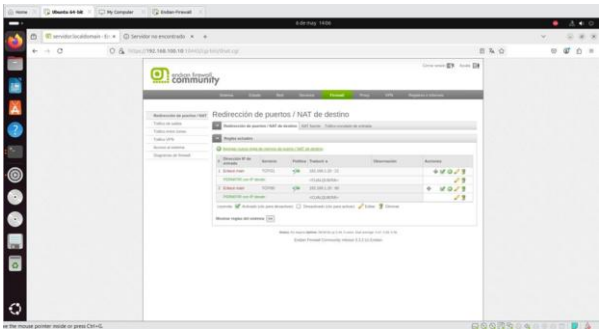
Figura 14. Habilitación del servicio HTTP en el puerto 80.



Fuente: Autoría Propia

Como muestra la Fig. 15 las reglas para permitir los servicios HTTP y FTP en los puertos 80 y 21 fueron creadas exitosamente.

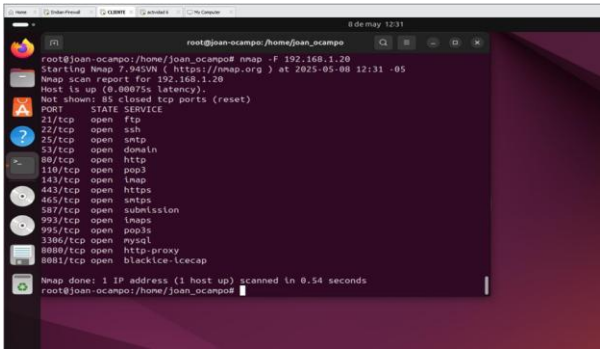
Figura 15. Listado de reglas



Fuente: Autoría Propia

Para la validación de la apertura de puertos en el servidor, se ejecuta en la terminal el comando nmap -F 192.168.1.20 el cual lista el estado de los puertos del servidor de la zona DMZ, allí se aprecia los puertos 21 y 80 abiertos en los servicios ftp y http respectivamente.

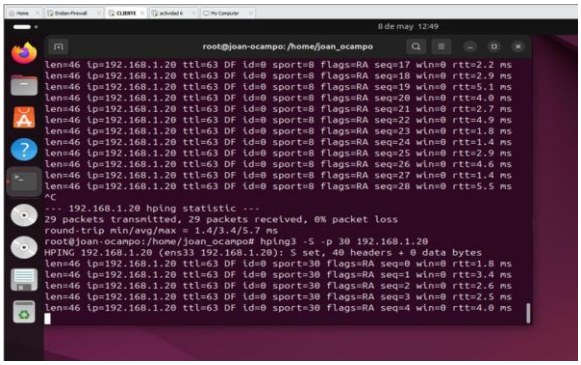
Figura 16. Verificación de la apertura de puertos



Fuente: Autoría Propia

Dentro de la temática que se viene trabajando se ha solicitado denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red, antes de aplicar las reglas de denegación se debe comprobar que si se tiene acceso al destino por medio de dichos puertos, hecho esto aplicar las reglas y demostrar la denegación del protocolo ICMP.

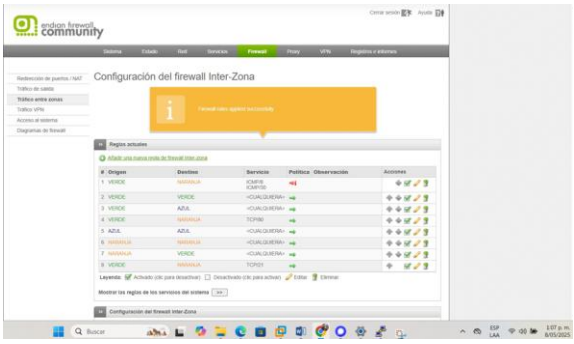
Figura 17. Ping por los puertos 8 y 30 con el protocolo ICMP



Fuente: Autoría Propia

Creación de la regla de denegación del protocolo ICMP en los puertos 8 y 30, impidiendo el ping por medio de estos, de acuerdo con la Fig. 18 en el ítem #1 la regla se encuentra aplicada.

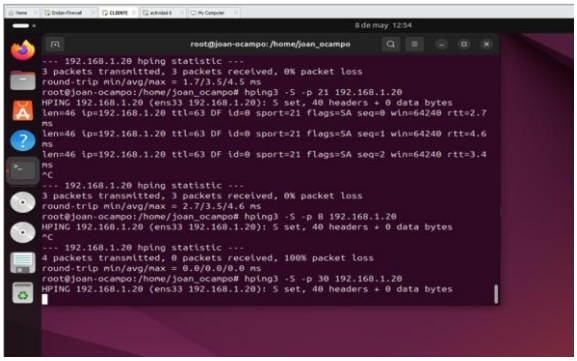
Figura 18. Creación de la regla de denegación



Fuente: Autoría Propia

Se realiza ping hacia el servidor con dirección IP 192.168.1.20 apuntando a los puertos 8 y 30 para comprobar que la aplicación de la regla de denegación fue exitosa.

Figura 19. Ping a los puertos denegados



Fuente: Autoría Propia

3.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

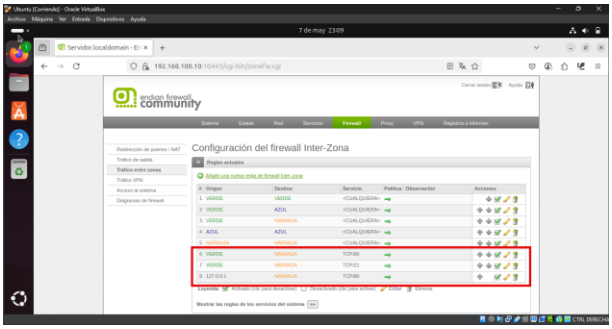
Para este apartado se tiene como fin crear reglas de acceso que permitan o denieguen el tráfico de servicios en las zonas verde, naranja y roja, se busca:

- Comunicar la zona verde con la zona naranja mediante los protocolos HTTP y FTP en sus respectivos puertos.
- Comunicar la zona Internet con la zona DMZ.

Se utilizo el firewall Endian, como sistema perimetral, realizando la configuración de reglas inter-zona para establecer la comunicación entre las zonas verde (LAN) y la naranja (DMZ), utilizando los servicios HTTP en el puerto 80 y FTP en el puerto 21, tomando como origen la zona verde y como destino la naranja, en la sección de política, no se limita el acceso a solo una IP, por lo que se selecciona la opción permitir para evitar inconvenientes con las pruebas a realizar más adelante.

De acuerdo con lo anterior y una vez guardados los cambios se puede observar en la sección de tráfico entre zonas las reglas añadidas como lo muestra la Fig. 20.

Figura 20. Trafico entre zonas reglas añadidas.



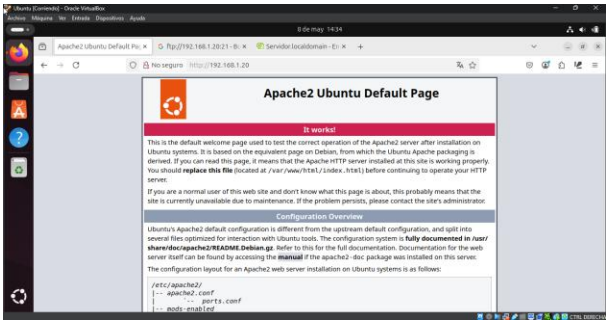
Fuente: Autoría Propia

Del mismo modo se crean reglas de trafico de salida entre las zonas roja (WAN) y la zona naranja (DMZ), designando como origen la zona roja para permitir la comunicación entre estas redes a través de los servicios HTTP

y FTP con sus respectivos puertos, para el caso de las políticas se decide no limitar el acceso a solo una dirección IP.

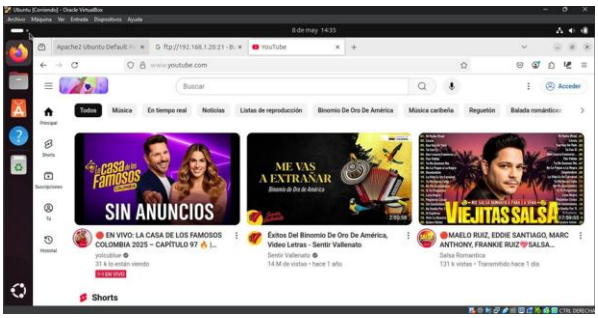
La creación de las reglas surte efecto, permitiendo la comunicación entre las zonas verde (LAN), naranja (DMZ) y roja (WAN), lo cual es demostrado al realizar las pruebas de ingreso entre redes, comprobando la funcionalidad de los servicios HTTP y FTP utilizando los puertos respectivos (80 y 21), como se evidencia a continuación.

Figura 21. Uso del servicio HTTP desde la LAN hacia la zona DMZ.



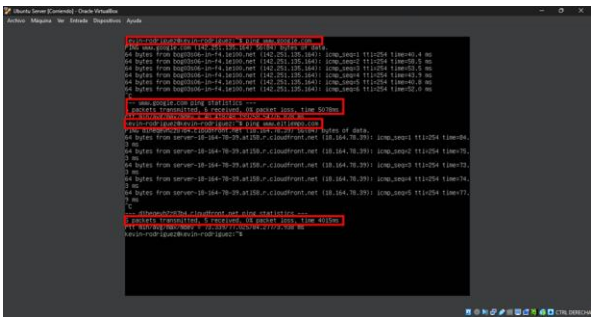
Fuente: Autoría Propia

Figura 22. Ingreso al servicio HTTP desde la LAN hacia la WAN.



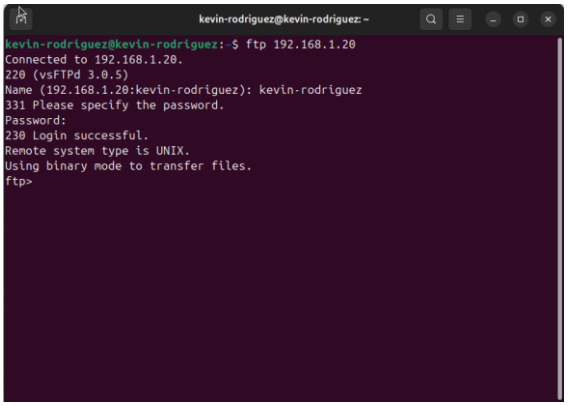
Fuente: Autoría Propia

Figura 23. Uso del servicio HTTP desde la zona DMZ hacia la WAN.



Fuente: Autoría Propia

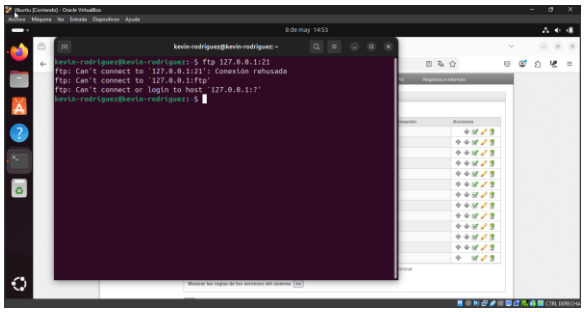
Figura 24. Ingreso mediante FTP desde la LAN hacia la zona DMZ.



Fuente: Autoría Propia

Se puede observar cómo en algunos casos al no estar establecidas las reglas de tráfico inter-zona que permitan la comunicación, el acceso de una zona hacia la otra es denegado, tal y como se muestra en la Fig. 25.

Figura 25. Ingreso mediante FTP desde la LAN hacia la WAN.



4 CONCLUSIONES

Endian es una excelente distribución de open source, la cual permite implementar políticas de seguridad de acuerdo con las necesidades de una red corporativa que requiere procesos de calidad y confiables.

Las reglas NAT permiten la traducción de direcciones de red, admitiendo la comunicación entre las zonas a las cuales los administradores de red le otorguen accesos.

La implementación de una zona DMZ utilizando Endian Firewall (EFW) permite establecer un entorno segmentado y seguro, donde los servicios públicos pueden ser accedidos sin exponer directamente la red interna, los servidores y bases de datos.

Endian Firewall facilita la configuración de distintos tipos de redes, capaces de realizar la interpolación en un sistema, abarcando zonas militarizadas, desmilitarizadas y redes de área

local (LAN), mediante el establecimiento de reglas de tráfico, gestión de accesos y control a los servicios de cada entorno.

5 REFERENCIAS

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

[2] Slashdot Media. (2025), Source Forge. Comunidad de firewalls de Endian https://sourceforge.net/projects/efw/

[3] Guía Completa del SO: Endian Firewall Cómo Funciona, Orientación y Curiosidades – LINUXMIND.DEV. (2024, Mayo 15). https://linuxmind.dev/2024/05/15/guia-completa-del-so-endian-firewall-como-funciona-orientacion-y-curiosidades/.

[4] C0bi. (2024, Enero 29). Cómo configurar endian firewall en una red existente. Mundowin. https://mundowin.com/como-configurar-endian-firewall-en-una-red-existente/?expand_article=1