SOLUCIONES DE SEGURIDAD PERIMETRAL EN LAN/WAN/DMZ CON ENDIAN FIREWALL

Ana Cristina Quiñonez Caicedo
e-mail: acquinonezc@unadvirtual.edu.co
Duvan Alejandro Vega Leon
e-mail: davegale@unadvirtual.edu.co
Gustavo Adolfo Quintero Vergara
e-mail: gaquinterover@unadvirtual.edu.co
Maria Alejandra Montoya Yepes
e-mail: mamontoyaye@unadvirtual.edu.co
Steven Lozano Astudillo
e-mail: slozanoa@unadvirtual.edu.co

RESUMEN**:** *En el presente artículo se expone la implementación de controles de seguridad robustos, que buscan minimizar el impacto que pueda llegar a tener una vulnerabilidad dentro de un sistema de información moderno. Para brindar una solución que sea lo suficientemente robusta, se decide usar Endian Firewall como punto central de la infraestructura de un sistema de información. La arquitectura se divide en 3 zonas clave que van de mayor a menor protección: la zona verde, cuyo contenido son redes LAN que requieren una alta protección contra el mundo exterior, la zona naranja o también llamada la zona desmilitarizada, cuyo contenido son servidores que están hasta cierto punto expuestos al mundo exterior y la zona roja, es donde se maneja el Internet y es la zona más expuesta a vulnerabilidades. Esta implementación brinda una guía para diseñar arquitecturas seguras con redes, servidores Linux y equipos de escritorio con el Endian Firewall.*

PALABRAS CLAVE: DMZ, Endian, FIREWALL, Seguridad

1 INTRODUCCIÓN

La creciente dependencia de las organizaciones en infraestructuras digitales ha incrementado la necesidad de implementar mecanismos de seguridad robustos que garanticen la integridad, disponibilidad y confidencialidad de la información. En este contexto, los sistemas GNU/Linux ofrecen una plataforma flexible y confiable para la administración de servicios críticos, pero requieren configuraciones avanzadas que permitan mitigar vulnerabilidades y ataques externos.

El presente trabajo aborda la implementación de una arquitectura de seguridad perimetral mediante el uso de Endian Firewall como núcleo de protección, dividiendo la red en tres zonas estratégicas: verde (LAN interna), naranja (DMZ con servidores expuestos) y roja (WAN). Esta segmentación permite aplicar políticas diferenciadas de acceso y control, reduciendo la superficie de ataque y fortaleciendo la defensa de los servicios.

A través de la configuración de reglas de traducción de direcciones (NAT), control de tráfico inter-zona y un proxy HTTP con autenticación, se busca establecer un entorno seguro y replicable que sirva como guía práctica para estudiantes y profesionales en la administración de sistemas operativos de código abierto. El artículo presenta los resultados obtenidos en cada temática, discute su impacto en la seguridad perimetral y propone buenas prácticas aplicables a escenarios reales.

2 TEMÁTICA 1: CONFIGURACIÓN E INSTALACIÓN DE ENDIAN FIREWALL

En este tipo de entornos basados en GNU/Linux, la segmentación e implementación de políticas de seguridad son esenciales para garantizar una red que sea confiable para sus usuarios. Los componentes principales de la arquitectura son: las zonas verde, naranja, roja y también el uso del Endian Firewall, que permite configurarlas de manera relativamente sencilla y robusta.

2.1 DIAGRAMA DE ZONAS

Antes de entrar en detalle sobre la instalación, es necesario tener definida la arquitectura de manera gráfica, con el objetivo de tener claro qué zonas se implementarán y qué configuraciones tendrá cada una. A continuación se describe cada elemento dentro de la arquitectura y su función dentro de esta. El punto de partida o central de la arquitectura es el Endian Firewall, donde se configuran cada una de las zonas y los adaptadores de red junto con los gateways o puertas de enlace para la comunicación entre zonas o Internet basado en reglas predefinidas.

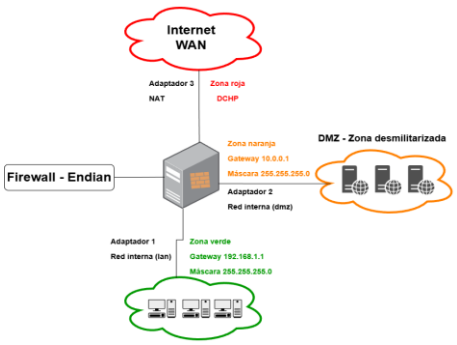
La zona más segura de la arquitectura es la zona verde. Esta zona va conectada al adaptador 1 del firewall que hace las veces de red interna (LAN) y que usará como puerta de enlace la IP 192.168.1.1 y la máscara 255.255.255.0. Aquí se tendrán equipos de escritorio y servidores que requieren un mayor nivel de seguridad, por ejemplo, con información sensible de la organización que no debe ser accedida de forma externa mediante Internet sino solamente para consumo interno de la red.

La zona desmilitarizada o zona naranja es una zona que no tiene la misma protección de la verde pero aun así no significa

que esté completamente desprotegida. Esta zona va conectada al adaptador 2 del firewall que hace las veces de red interna. Aquí la puerta de enlace será la 10.0.0.1 y la máscara será 255.255.255.0. Aquí se tendrán servidores que presten servicios que pueden ser expuestos a Internet bajo un puerto en específico, por ejemplo un servicio de correos, web o proxy. Al tener una cierta exposición al mundo exterior es importante configurar el firewall de tal manera que se exponga únicamente el puerto al que pertenezca el servicio y que se definan reglas claras para evitar brindar un control total sobre la red a cualquiera que pueda acceder a la red.

Finalmente la zona más desprotegida es la zona roja. Aquí el adaptador 3 brinda conexión a Internet facilitando a la zona verde y naranja conectarse usando el NAT, dado que estas zonas tienen equipos con IPs privadas. Y por otro lado se usa DHCP para obtener la IP desde el ISP de manera automática sin necesidad de configurar IPs de manera manual. La explicación anterior puede representarse gráficamente en el diagrama siguiente:

Figura 1. Diagrama de zonas Endian Firewall

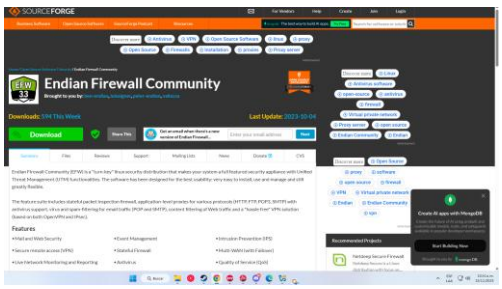


Fuente: Autoría Propia

2.2 DESCARGA DE LA ISO Y CREACIÓN DE LA MÁQUINA VIRTUAL

Como se mencionó anteriormente se usará el Endian Firewall, por lo que el paso inicial para esto es acceder a la página https://sourceforge.net/projects/efw/ para descargar el ISO oficial de este firewall.

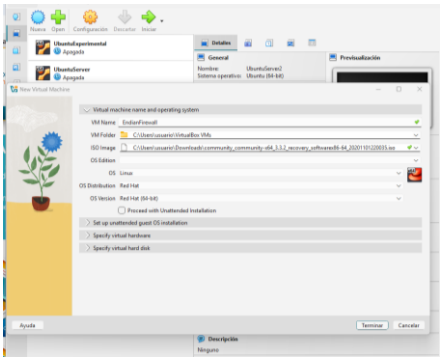
Figura 2. Sitio oficial descarga Endian Firewall



Fuente: https://sourceforge.net/projects/efw

Después se procede a configurar la máquina virtual que nos servirá como firewall para nuestra red. Para esto, asignamos el ISO del Endian Firewall, se le da el nombre de "EndianFirewall" a la máquina virtual, se establece "Linux" como el OS y "Red Hat" como la OS distribution.

Figura 3. Creación de la máquina virtual



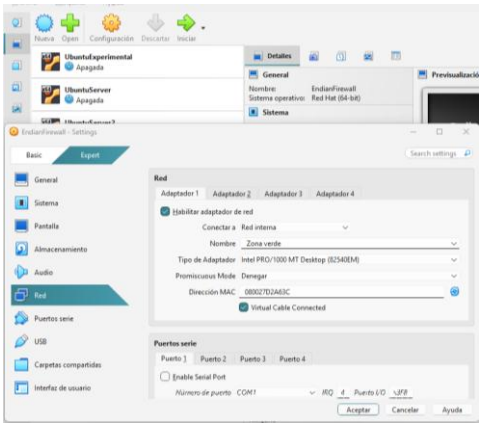
Fuente: Autoría Propia

La asignación de recursos queda a criterio propio, en nuestro caso se establecieron recursos mínimos de 2GB de RAM, 2 CPU y 50GB de almacenamiento ya que no es necesario tener unos recursos elevados para este caso.

2.3 CONFIGURACIÓN DE ADAPTADORES DE RED

Ya con la máquina virtual configurada, se pueden agregar los adaptadores de red definidos en el diagrama explicado al inicio del desarrollo de la temática. Para la zona verde, se asigna el "adaptador 1". En este adaptador se selecciona "Red interna" y el nombre "Zona verde".

Figura 4. Creación de adaptador 1, zona verde



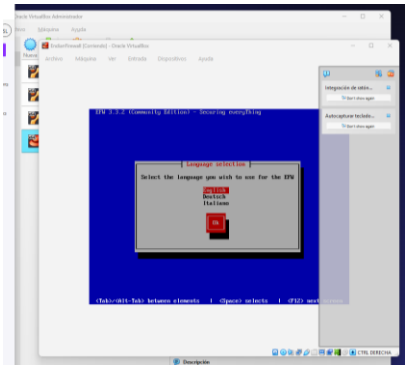
Fuente: Autoría Propia

De igual manera para el adaptador 2 se asigna la zona naranja y esta será una "Red interna" de igual manera que con el adaptador 1. Para el adaptador 3 se establece la zona roja que se conectará mediante NAT. Al crear estas zonas, cada equipo y servidor correspondiente se debe conectar a su zona correspondiente, por ejemplo los servidores a la naranja y los equipos de escritorio a la verde.

2.4 INSTALACIÓN Y CONFIGURACIÓN

Al abrir por primera vez la máquina virtual creada, el sistema arrancará y lo primero que se solicitará es el lenguaje, en este caso se escoge “English” dentro de las opciones disponibles.

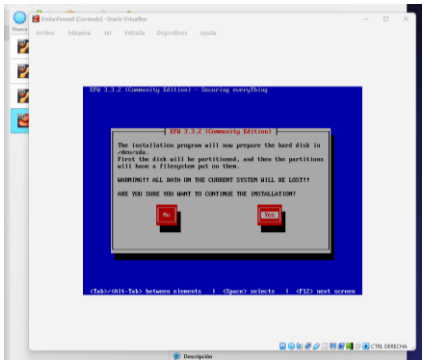
Figura 5. Lenguaje de instalación Endian Firewall



Fuente: Autoría Propia

Luego de esto, pregunta sobre el reinicio del computador durante la instalación a lo cual se responde “Ok”. Posterior a esto se pide confirmación para particionar el disco y continuar con la instalación. para continuar se selecciona la opción “Yes”.

Figura 6. Confirmación de particionado

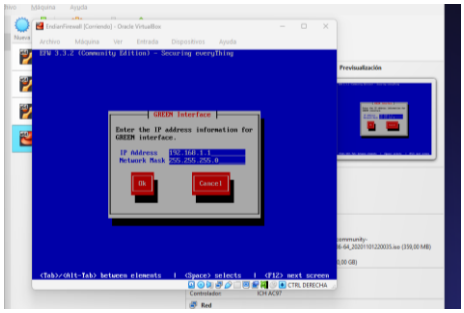


Fuente: Autoría Propia

A la siguiente pregunta que realiza el instalador de que si se quiere habilitar una consulta sobre el serial port, se selecciona “Yes” para continuar con la instalación.

Una vez pasada esta pregunta, se muestra una nueva ventana de configuración para la “GREEN interface” a la cual se asigna la IP definida en el diagrama para la puerta de enlace en la zona verde, la cual es 192.168.1.1 y luego se presiona “Ok” para continuar.

Figura 7. Asignación IP zona verde



Fuente: Autoría Propia

Luego de esto, se realizan instalaciones y configuraciones automáticamente. Una vez completado esto, se nos mostrará un mensaje de configuración exitosa y que se puede acceder a la url http://192.168.1.1 o https://192.168.1.1:10443 para completar la configuración desde una interfaz gráfica desde el navegador, tal como lo explica Endian en su manual UTM (2016) [5]. En esta ventana final se presiona “Ok” para continuar. Posteriormente, el sistema se reinicia automáticamente para continuar con la instalación y finalmente se mostrará en la terminal que ya se tiene la zona verde y se pueden usar los diferentes comandos o herramientas proveídas para su configuración.

2.5 CONFIGURACIÓN DE INTERFAZ GRÁFICA DEL ENDIAN FIREWALL DESDE EL NAVEGADOR

Desde un equipo de escritorio se puede acceder a la IP que mostró Endian al configurar la máquina, para el manejo del firewall mediante una interfaz gráfica en el navegador. La IP de acceso es http://192.168.1.1:10443. Al acceder a esta IP nos muestra una ventana de bienvenida a la cual le daremos “Siguiente” o en el caso de esta interfaz se identifica con el símbolo “>>>”.

Los pasos iniciales son sencillos, a continuación, se describen brevemente:

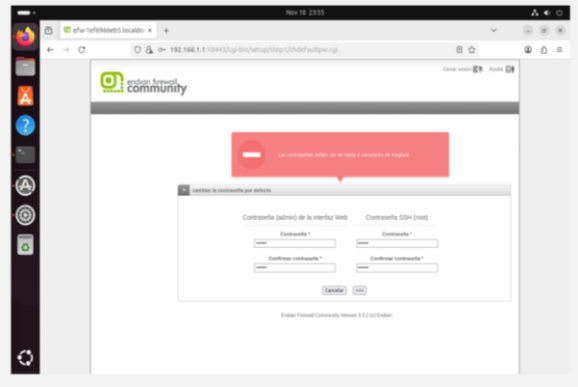
1. Se configura el idioma y zona horaria de preferencia. Posteriormente se presiona “>>>” para pasar al siguiente paso.

2. En el siguiente paso, se mostrará la licencia de Endian Firewall y una opción para aceptarla. En este caso, se acepta para continuar con el proceso. Luego de seleccionar la opción, se presiona el botón “>>>”

3. El nuevo paso se pide si se restaura un backup pero como es primera instalación se marca la opción “No” y luego se presiona el botón “>>>”.

En los pasos siguientes se pide inicialmente configurar dos contraseñas: una para la interfaz web y otra para SSH. En este paso se configuran las contraseñas a preferencia personal, teniendo en cuenta que deben ser contraseñas robustas y seguras.

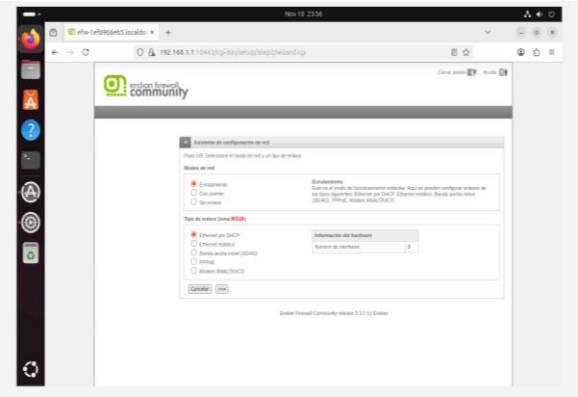
Figura 8. Contraseñas interfaz gráfica y SSH



Fuente: Autoría Propia

Finalmente, se muestra una ventana donde nos muestra una configuración por defecto donde “Modos de red” debe tener seleccionada la opción “Enrutamiento” y Tipos de enlace (zona ROJA) debe tener seleccionada la opción Ethernet por DHCP tal como se tiene definido en el diagrama de zonas.

Figura 9. Configuración de red

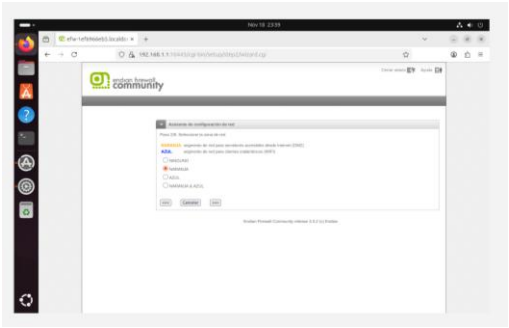


Fuente: Autoría Propia

2.6 CONFIGURACIÓN DE ZONA NARANJA

Hasta este punto se ha configurado la zona verde y roja junto a una serie de parámetros pero no se ha tocado en ningún momento la zona naranja. Después del paso anterior donde se selecciona los modos de red y tipo de enlace para la zona roja, el asistente sugiere configurar la zona naranja, la azul, ambas o ninguna. El diagrama visto anteriormente sugiere que se debe tener una zona naranja por lo que se debe seleccionar la opción “NARANJA” y presionar el botón “>>>” para continuar.

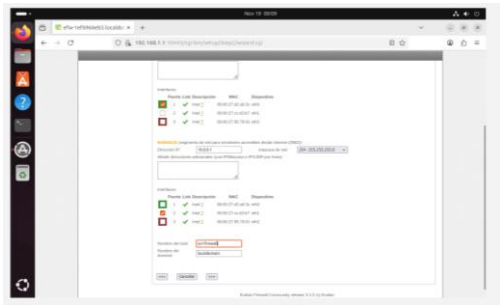
Figura 10. Selección para la creación de zona naranja



Fuente: Autoría Propia

Posteriormente se mostrará la configuración actual de las zonas roja, verde y adicionalmente se permitirá la configuración de la zona naranja. En esta configuración se pone la IP de la puerta de enlace de la zona naranja definida en el diagrama, que es 10.0.0.1, se marcará la interfaz eth1 definida en esta zona. Para identificar la interfaz se sugiere revisar las direcciones mac de los adaptadores y seleccionar la correcta. Adicionalmente se le dará el nombre de “svr-firewall” al host. Al hacer esto se selecciona “>>>” para continuar.

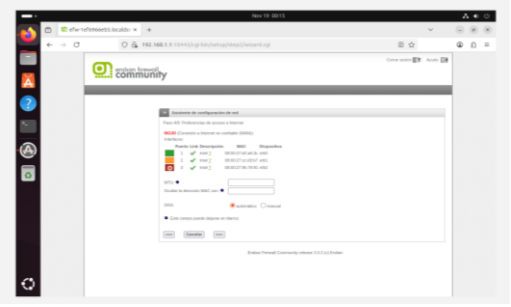
Figura 11. Configuración zona naranja



Fuente: Autoría Propia

Lo siguiente que se muestra es la confirmación de cómo quedan configuradas las zonas y dónde se puede revisar si todo quedó bien de acuerdo al diagrama de zonas definido.

Figura 12. Confirmación de la configuración de zonas



Fuente: Autoría Propia

En esta ventana se presiona la opción ">>>" y el resto de pasos son simplemente darle siguiente sin cambiar nada:

1. Luego de confirmar las zonas se muestra la configuración del DNS en la cual no se debe cambiar nada, solo es informativo. Se presiona la opción ">>>"

2. Se sigue presionando ">>>" hasta que aparezca la opción de aplicar la configuración realizada.

Una vez se aplique la configuración la interfaz nos indica que se aplicó correctamente y que en segundos veremos estos cambios efectuados.

Figura 13. Confirmación de cambios aplicados

Fuente: Autoría Propia

2.7 PRUEBAS DE FUNCIONAMIENTO

Los pasos anteriores permiten crear de forma exitosa cada una de las zonas junto con el firewall que cumplirá con lo establecido en el diagrama. A continuación se establecen ciertas pruebas base para confirmar el funcionamiento.

1. Los servidores deben estar conectados en el adaptador 2, que identifica a la zona naranja.

2. Los servidores pueden tener una IP fija o se puede obtener mediante DHCP.

3. Para probar que los servidores estén conectados a la zona naranja, se puede hacer un ping a la puerta de enlace cuya IP es 10.0.0.1.

4. Los equipos de escritorio u otros dispositivos que se quieran proteger en la zona verde deben estar conectados al adaptador 1.

5. Para probar que los equipos estén conectados a la zona verde, se puede hacer ping a la puerta de enlace cuya IP es 192.168.1.1.

3 TEMÁTICA 2: CONFIGURACIÓN NAT

En el entorno de seguridad de redes, la configuración adecuada de NAT (Network Address Translation) representa un componente crítico para establecer y gestionar la comunicación controlada entre diferentes zonas de red.

Dentro de la infraestructura implementada con el Firewall Endian (EFW), esta temática se centró en explorar la aplicación práctica de las reglas NAT. El objetivo principal fue permitir que tanto los dispositivos en la Red Interna (LAN/Zona Verde) como los servidores alojados en la Zona Desmilitarizada (DMZ/Zona Naranja) obtuvieran acceso controlado a la Internet (Red WAN/Zona Roja) de una forma segura y la creación de las reglas.

3.1 ARQUITECTURA DE RED

Tabla 1. Configuración zonas

Zona	Interfaz VirtualBox	Tipo de red VirtualBox	Rango IP
Verde (LAN)	Adaptador 1	Red interna	192.168.1.1/24
Naranjada (DMZ)	Adaptador 2	Red interna	10.0.0.1/24
Roja (WAN)	Adaptador 3	Red NAT	DHCP

Fuente: Autoría Propia

3.2 IMPLEMENTACIÓN Y MECANISMO DEL NAT DE ORIGEN (SNAT)

La Traducción de Direcciones de Red de Origen (SNAT) es esencial para que múltiples dispositivos con IP privadas (Zona Verde y Zona Naranja) puedan acceder a Internet a través de una única dirección IP pública del firewall (la IP de la Zona Roja), tal como explica Cisco (s.f.) [8].

Este mecanismo garantiza la seguridad al ocultar las direcciones internas del exterior. La forma más común de SNAT, conocida como Mascarada (Masquerading), se utiliza cuando la dirección WAN del firewall (10.0.4.15 en este caso) es dinámica, lo cual aplica a la configuración de la Zona Roja de Endian. El firewall traduce la IP de origen saliente de los clientes (ej., 192.168.1.x o 10.0.0.x) a su propia IP WAN, y mantiene una tabla de estado para revertir la traducción de los paquetes de respuesta.

3.2.1 CONFIGURACIÓN DE LA MASCARADA (MASQUERADING)

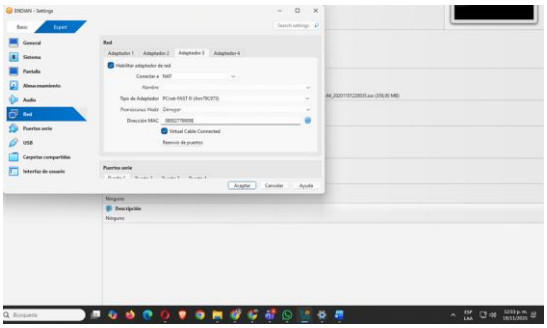
La configuración del NAT de Origen (SNAT) constituye el mecanismo primordial para permitir la salida del tráfico desde las subredes privadas (Zona Verde y Zona Naranja) hacia la red

pública (Zona Roja/WAN). Esta funcionalidad es conocida en Endian como Mascarada. En el entorno de virtualización, la regla SNAT se activó implícitamente al configurar el Adaptador 3 del Firewall Endian en modo NAT dentro de VirtualBox, y al designar la interfaz internamente con DHCP. Como resultado, Endian adquirió la dirección 10.0.4.15/24 para su Uplink. El Masquerading traduce de forma dinámica las direcciones IP de origen de los clientes (ej., 192.168.1.x o 10.0.0.x) a esta única dirección WAN (10.0.4.15) al salir de la red, logrando así el objetivo de la comunicación LAN -> WAN y DMZ -> WAN.

3.2.2 VISUALIZACIÓN DE LA CONFIGURACIÓN Y DIRECCIÓN WAN

El Adaptador 3 del Endian fue configurado en VirtualBox en modo NAT, lo cual se muestra en la Figura 14. Esta configuración activa el DHCP, permitiendo que la interfaz WAN del Endian obtenga su dirección.

Figura 14. Configuración Endian VirtualBox



Fuente: Autoría Propia

3.2.3 DESTINATION NAT (DNAT)

Se aplica al tráfico que se origina en una red externa (como Internet) y se dirige a una dirección IP dentro de la red privada. DNAT se utiliza normalmente para reenviar tráfico a servidores específicos alojados en la red interna. Cuando una solicitud externa llega al firewall Endian en una dirección IP pública y un puerto específico, una regla de DNAT puede traducir la dirección IP y el puerto de destino a la dirección IP privada y el puerto de un servidor específico dentro de la red interna.

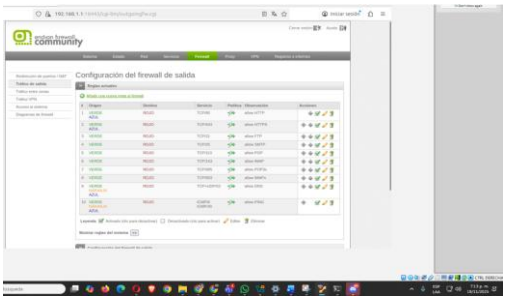
3.2.4 PRUEBAS DE CONECTIVIDAD Y DEMOSTRACIÓN DEL NAT DE SALIDA

La correcta implementación del NAT de Origen (SNAT/Mascarada) se verificó mediante la demostración del establecimiento de comunicación bidireccional desde las subredes privadas hacia la WAN, lo cual constituye los dos primeros productos esperados de la temática. Inicialmente, la conectividad fue probada desde un cliente GNU/Linux en la Zona Verde (192.168.1.29), confirmándose que el tráfico de ping fue traducido exitosamente por la IP WAN del Endian (10.0.4.15). Posteriormente, esta misma validación se extendió a la Zona Naranja (DMZ), garantizando que el tráfico de los servidores (10.0.0.x) también es traducido y retransmitido correctamente a Internet, completando así la prueba funcional del SNAT para ambas redes internas.

3.2.5 VERIFICACIÓN DE REGLAS DE SALIDA DEL FIREWALL (SNAT)

Una vez confirmada la operatividad del NAT de Origen (SNAT) mediante las pruebas de conectividad, se procedió a la verificación de las reglas en la interfaz web de Endian, específicamente en la sección Firewall ->Tráfico de salida. Aunque la función de Mascarada se activó automáticamente con la configuración de la Zona Roja, el firewall utiliza reglas de filtro de paquetes para controlar qué tráfico de la Zona Verde y Zona Naranja tiene permiso para acceder a la Zona Roja. La inspección de estas reglas actuales confirma que el sistema permite el tráfico esencial para la comunicación WAN, incluyendo servicios como HTTP, HTTPS, y los protocolos requeridos para la demostración: DNS (TCP+UDP/53) y PING (ICMP/8) para las zonas VERDE y NARANJA. Estas reglas de salida son el complemento necesario para que la traducción de direcciones (SNAT) pueda completarse exitosamente.

Figura 15. Configuración del firewall de salida Endian



Fuente: Autoría Propia

3.2.6 CREACIÓN DE REGLAS EN EL FILTRO DE PAQUETES DE SALIDA

Para añadir una regla de acceso total de la Zona Naranja (NARANJA) a la WAN (ROJO) se siguen los siguientes pasos en el Editor de reglas de salida del firewall:

1. Origen: Se selecciona NARANJA en la lista de interfaces, indicando que la regla aplica a todo el tráfico saliente desde esta zona.

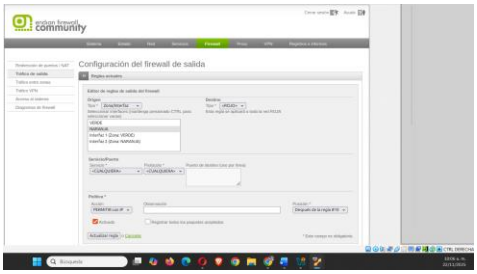
2. Destino: Se selecciona ROJO, lo que significa que la regla se aplicará a toda la red WAN.

3. Servicio/Puerto: Se puede seleccionar CUALQUIERA para un acceso irrestricto, o especificar un servicio y protocolo particular (ej., TCP/22 para SSH).

4. Política: Se establece la acción como PERMITIR con IP, que permite el flujo del tráfico saliente.

5. Activado: La opción se marca como Activado para aplicar la regla.

Figura 16. Configuración del firewall de salida Endian



Fuente: Autoría Propia

3.2.7 VERIFICACIÓN DE REGLAS DNAT Y REENVÍO DE PUERTOS

La verificación del requisito de Reenvío de Puertos (DNAT) se realiza documentando el proceso para configurar el tráfico entrante. Esta funcionalidad es opuesta al filtro de paquetes de salida, ya que su objetivo es traducir una dirección pública a una privada para acceder a un servicio interno en la DMZ.

Para añadir una regla de reenvío para el tráfico entrante, se siguen los siguientes pasos en el editor de regla de reenvío de puerto / NAT de destino:

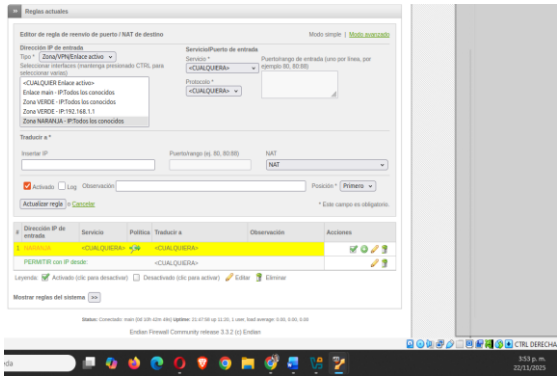
1. Dirección de IP de entrada: Se selecciona el tipo de Zona/VPN/Enlace activo y se especifica la interfaz que recibirá la solicitud externa. Se ha seleccionado Zona Naranja - IP: Todos los conocidos, lo que significa que esta regla está diseñada para traducir el tráfico que se origina o llega a través de la zona.

2. Servicio/Puerto de entrada: Se ha elegido la opción CUALQUIERA para el Servicio y CUALQUIERA para el Protocolo.

3. Traducir a: El campo NAT está seleccionado.

4. Activado y Posición: La regla está marcada como Activado y su Posición está establecida como Primero.

Figura 17. Regla para redirección de puertos



Fuente: Autoría Propia

3.2.8 PRUEBA DE CONEXIÓN SALIENTE (ZONA VERDE HACIA WAN)

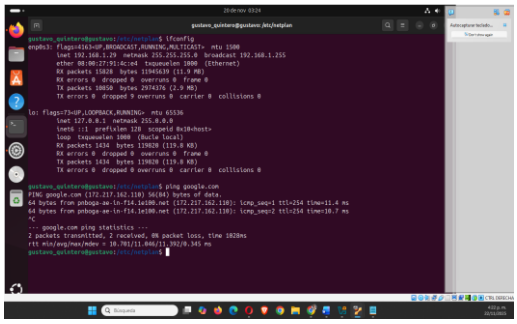
Para demostrar el establecimiento de comunicación de la LAN hacia la WAN (Producto Esperado 1), se realiza una prueba simple de conectividad desde el cliente Ubuntu en la Zona Verde (192.168.1.29).

La verificación se realiza en dos partes:

1. Comando PING: Desde la consola, se consulta el estado de la conexión mediante PING a un destino externo. La Figura 18 muestra que el tráfico ICMP y la resolución de DNS son exitosos.

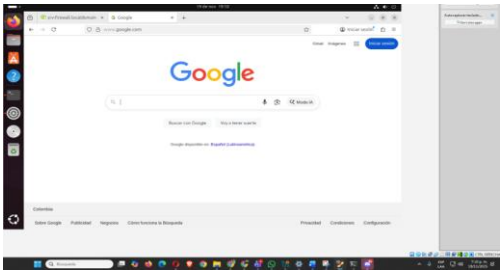
2. Navegación: Al intentar navegar en Internet, se confirma que los servicios HTTP/HTTPS también son permitidos y traducidos, completando la demostración del flujo LAN a WAN, como se visualiza en la figura 19.

Figura 18. Prueba de PING



Fuente: Autoría Propia

Figura 19. Prueba de conexión a internet



Fuente: Autoría Propia

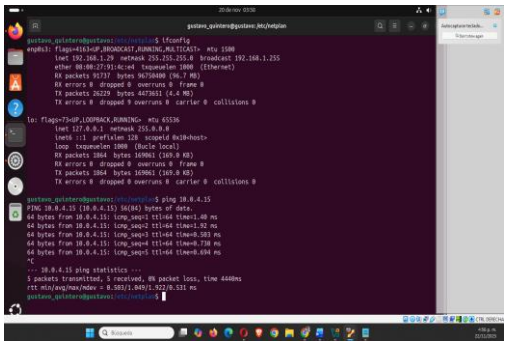
3.2.9 PRUEBA DE CONEXIÓN SALIENTE (ZONA NARANJA HACIA WAN)

Para concluir la demostración del NAT de Origen (SNAT) y validar la primera parte del Producto Esperado 2 (comunicación DMZ a Internet), se realiza una prueba de conectividad desde el servidor dentro de la Zona Naranja (10.0.0.x).

La verificación se realiza mediante PING hacia la interfaz WAN del firewall (IP: 10.0.4.15) y a un destino externo:

Comando PING a la WAN: La Figura 20 muestra un PING exitoso a la IP 10.0.4.15 del Endian, verificando que la máquina DMZ puede alcanzar su Gateway y que la regla de filtro de paquetes de salida lo permite.

Figura 20. Prueba de Conexión a internet



Fuente: Autoría Propia

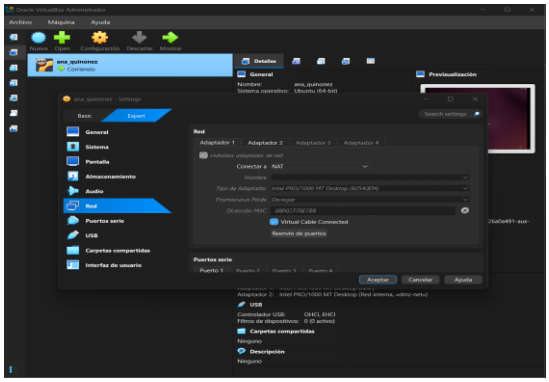
4 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

En el panorama empresarial actual, proteger los límites de la red es fundamental para garantizar la integridad de los sistemas, aplicaciones y bases de datos esenciales de una organización. Implementar una DMZ (Zona Desmilitarizada) ayuda a aislar los servidores expuestos a Internet de la red interna, generando así una barrera extra que reduce los riesgos de intrusión. En esta configuración, se implementó un Firewall Endian junto con un servidor Ubuntu Server en la DMZ, con el objetivo de habilitar servicios cruciales como HTTP y FTP, e integrar medidas de seguridad como el bloqueo del protocolo ICMP. Estos ajustes sirven para demostrar el funcionamiento de una arquitectura segura y la gestión apropiada del tráfico mediante reglas de firewall personalizadas.

4.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN FIREWALL

Para iniciar la práctica, se creó la máquina virtual para instalar Endian Firewall en VirtualBox. Se configuró como sistema “Linux – Other Linux 64-bit”, se asigna memoria RAM y se creó un disco dinámico.

Figura 21. Máquina Virtual Endian – VB

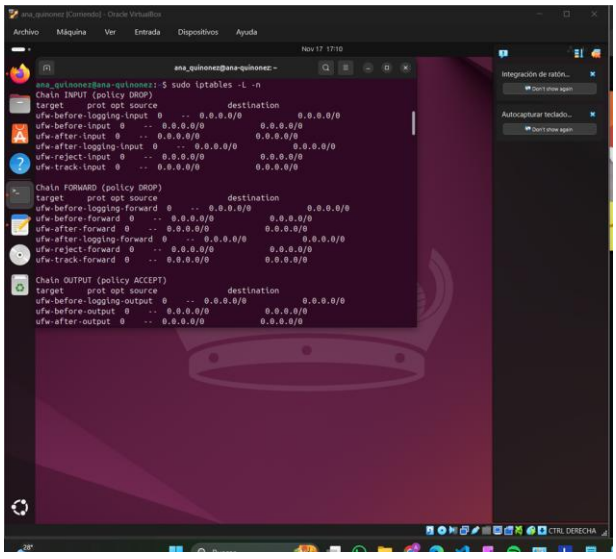


Fuente: Autoría Propia

4.2 ASISTENTE DE INSTALACIÓN DE ENDIAN FIREWALL

El instalador guía al usuario a través de la selección de disco, creación de particiones, asignación de interfaces y configuración inicial del sistema. Este proceso prepara el firewall para gestionar el flujo de datos entre la LAN y la WAN. El asistente de instalación guía al usuario en la configuración inicial, pero es en la posterior administración donde se aprecia la potencia del sistema. Endian incorpora funcionalidades adicionales como IDS/IPS, proxy, VPN y antivirus perimetral, características que son comunes en firewalls profesionales. Su uso en esta actividad permite al estudiante familiarizarse con escenarios reales del mundo laboral.

Figura 22. Asistente de instalación de Endian Firewall.



Fuente: Autoría Propia

4.3 CONFIGURACIÓN DEL SERVIDOR UBUNTU

El servidor Ubuntu fue configurado con dos interfaces:

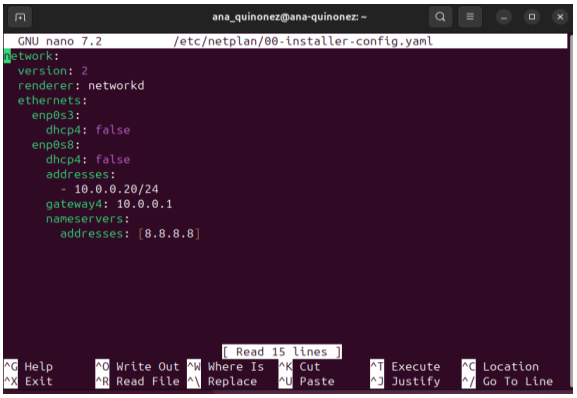
enp0s3 → DHCP
enp0s8 → 10.0.0.20/24

Dentro del archivo Netplan se utilizó:

sudo nano /etc/netplan/00-installer-config.yaml

El uso de Netplan en Ubuntu Server facilita la administración de la red mediante archivos YAML, que permiten definir de manera estructurada y clara cada interfaz. Este mecanismo reemplaza herramientas más antiguas y se integra completamente con el administrador systemd-networkd, ofreciendo mayor estabilidad y consistencia en la gestión del entorno.

Figura 23. IP estática enp0s8



Fuente: Autoría Propia

4.4 INSTALACIÓN DE APACHE

Se instaló Apache con:

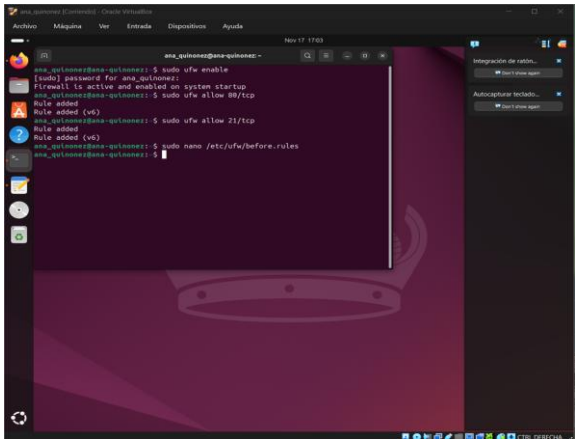
sudo apt update
sudo apt install apache2 -y

Luego se verificó que Apache estuviera escuchando en el puerto 80:

sudo ss -tulnp | grep 80

La verificación mediante el comando curl permitió comprobar que el servicio estaba correctamente levantado y escuchando en el puerto 80, requisito indispensable antes de proceder a la creación de reglas de firewall. Este tipo de pruebas son esenciales dentro del proceso de diagnóstico que un administrador de sistemas debe realizar para garantizar la continuidad de los servicios.

Figura 24. Instalación de apache y actualización del servicio.



Fuente: Autoría Propia

4.5 CREACIÓN DE REGLAS DE FIREWALL EN ENDIAN PARA PERMITIR HTTP Y FTP

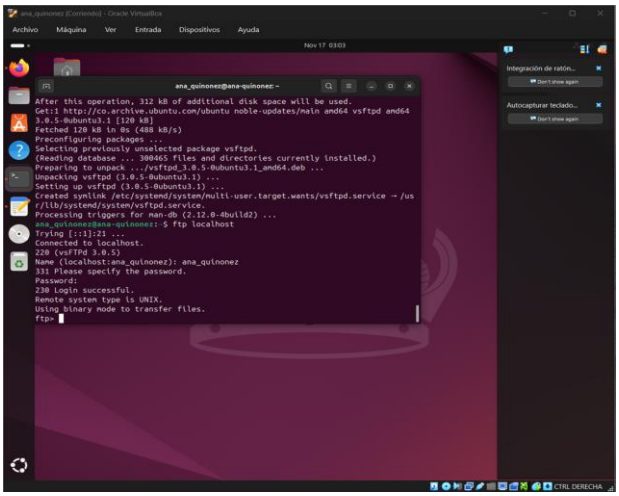
Se configuraron dos reglas:

HTTP – Puerto 80
FTP – Puerto 21

Ambas reglas apuntando al servidor 10.0.0.20 (DMZ).

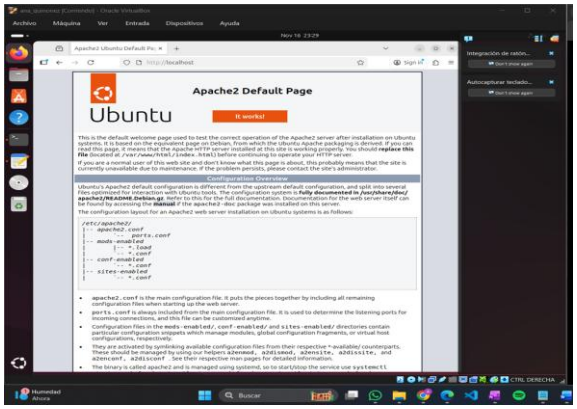
Endian Firewall permite gestionar las reglas de manera intuitiva mediante su interfaz gráfica, pero cada regla aplicada se traduce internamente en configuraciones equivalentes a iptables. De esta forma, el estudiante se familiariza indirectamente con la estructura de un firewall basado en Linux, comprendiendo cómo el tráfico se acepta, redirige o bloquea dependiendo de la política configurada.

Figura 25. Reglas Firewall Endian: HTTP y FTP



Fuente: Autoría Propia

Figura 26. Interfaces de red mostrando en localhost.



Fuente: Autoría Propia

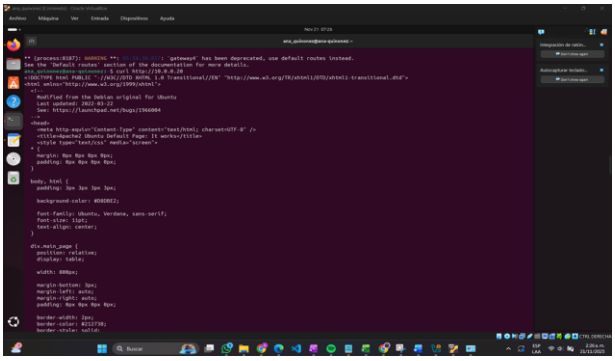
4.6 PRUEBA DEL SERVICIO HTTP

Su instalación dentro de la DMZ resulta apropiada, ya que permite simular un entorno real donde se alojan aplicaciones o páginas web corporativas. La verificación mediante el comando curl permitió comprobar que el servicio estaba correctamente levantado y escuchando en el puerto 80, requisito indispensable antes de proceder a la creación de reglas de firewall. Este tipo de pruebas son esenciales dentro del proceso de diagnóstico que un administrador de sistemas debe realizar para garantizar la continuidad de los servicios.

Se probó desde el firewall:

curl http://10.0.0.20

Figura 27. Comprobación del servicio HTTP mediante curl



Fuente: Autoría Propia

[7] Endian. (s.f.). *Endian Firewall Community*. https://www.endian.com/community

4.7 COMPROBACIÓN EN EL NAVEGADOR SU CONEXIÓN

Una vez configurado el servidor web Apache en la zona DMZ y aplicada la regla correspondiente en el firewall Endian, se procedió a verificar su correcto funcionamiento accediendo desde un navegador web. Esta comprobación es fundamental, ya que permite validar no solo que el servicio se encuentra activo y escuchando en el puerto 80, sino también que el firewall está permitiendo el tráfico entrante hacia el servidor según las políticas definidas.

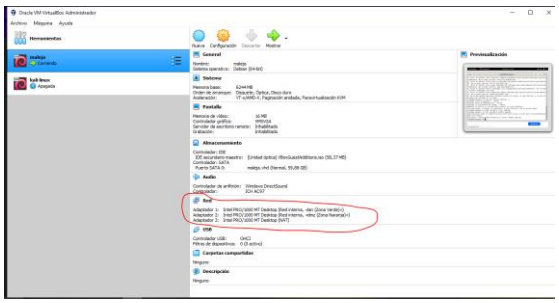
Figura 28. Comprobación de conexión en el navegador

Fuente: Autoría Propia

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

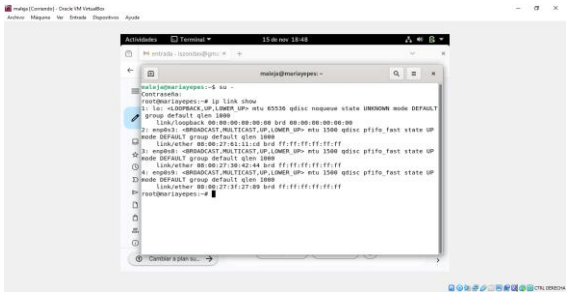
En esta sección se presentan las reglas de acceso diseñadas para controlar el flujo de tráfico entre las distintas zonas de la red en un entorno Linux. El objetivo es establecer políticas claras que permitan únicamente las comunicaciones autorizadas y bloqueen cualquier intento no previsto, garantizando así la seguridad y segmentación de los servicios. Para ello, se parte de la configuración estática de las interfaces de red y posteriormente se aplican directivas de firewall mediante iptables, con el fin de validar la conectividad y comprobar que los protocolos HTTP y FTP funcionan de acuerdo con las restricciones definidas. Esta temática constituye un paso fundamental en la simulación de arquitecturas seguras, ya que permite evaluar cómo las reglas de acceso influyen en la interacción entre LAN, DMZ e Internet. La correcta configuración de interfaces en sistemas GN/Linux es un requisito previo para aplicar reglas de firewall efectivas, tal como lo documenta la guía oficial de Ubuntu Desktop (Canonical, 2023).

Figura 29. Configuración de Red en VirtualBox



Fuente: Autoría Propia

Figura 30. Verificación de Interfaces de Red en Linux

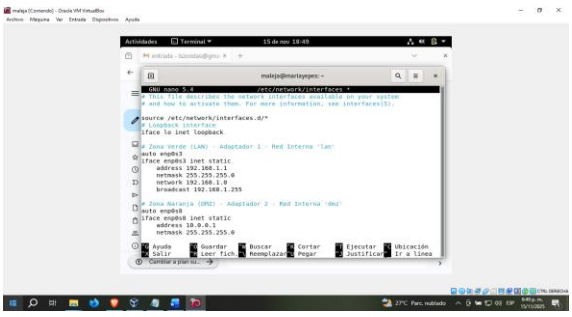


Fuente: Autoría Propia

5.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

Se edita el archivo /etc/network/interfaces, para asignar direcciones IP estáticas a cada una de las interfaces de red de la máquina virtual Linux, que corresponden a las zonas previamente definidas, es decir: LAN (eth0), DMZ (eth1) y WAN (eth2). Cada interfaz de red fue configurada con IPs, máscara de red y broadcast concretos, para que la máquina pueda comunicarse con los nodos que se encuentran en su correspondiente zona, tal cual se quería. Esta configuración manual es un paso importante para entornos de prueba donde se quiere tener un control absoluto sobre la topología de red. Entonces, al guardar los cambios y reiniciar el servicio de red, se asegura que las interfaces obtendrán las correspondientes IPs en el arranque. Esta base de la configuración es necesaria antes de crear reglas de firewall dado que se apoya en direcciones fijas para definir las políticas de acceso entre zonas.

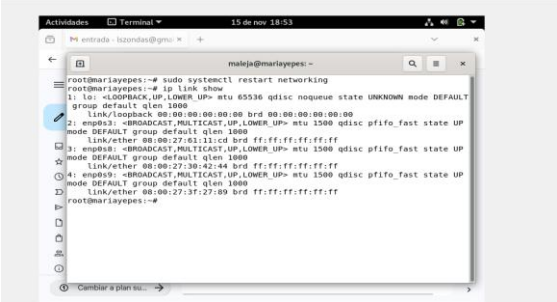
Figura 31. Configuración estática de interfaces en Linux



Fuente: Autoría Propia

Una vez completada la modificación del fichero de red /etc/network/interfaces, se procede a ejecutar el comando sudo systemctl restart networking de forma que de esta manera se aplique la nueva configuración de la red. Este reinicio provoca que el sistema operativo vuelva a leer las IP's estáticas que tiene asignadas cada una de las interfaces de forma que éstas se activen de acuerdo a lo que se ha establecido en las respectivas zonas LAN, DMZ y WAN. A continuación de la modificación del fichero de configuración de red y del reinicio de este servicio, se comprobó el estado de las interfaces de red mediante la ejecución de ip link show y se certificó de que todas las interfaces de las máquinas virtuales están en modo "UP" y son capaces de operar. Este paso es fundamental a la hora de garantizar que la máquina virtual tiene conectividad a través de cada una de las zonas establecidas antes de aplicar las correspondientes reglas de firewall. Si la red no está correctamente configurada cualquier directiva de acceso fallaría. La correcta aplicación de estas configuraciones permite estar preparado para llevar a cabo las pruebas de tráfico entre zonas para validar la seguridad y el control de acceso en un entorno Linux.

Figura 32. Reinicio del servicio de red en Linux

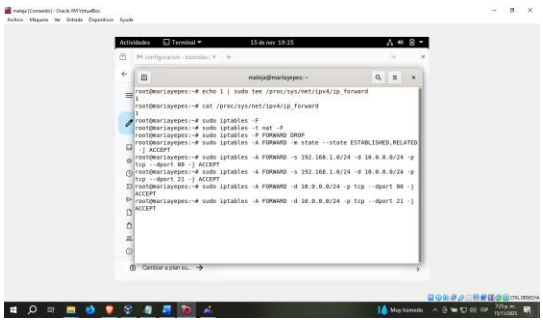


Fuente: Autoría Propia

5.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ.

Se establecieron reglas de firewall utilizando iptables para regular el tráfico entre las zonas LAN, DMZ y WAN. Se activó el enrutamiento IPv4 mediante el archivo /proc/sys/net/ipv4/ip_forward. Se configuraron, en primer lugar, las políticas por defecto (-P FORWARD DROP) y se establecieron las correspondientes reglas para permitir el tráfico de HTTP (puerto 80) y de FTP (puerto 21) entre cada zona. Por ejemplo, se consideró para el tráfico HTTP el ingreso desde LAN a DMZ y desde WAN a DMZ y para el tráfico FTP desde LAN a WAN. Se realizó una verificación de todas las reglas mediante iptables -L -n -v, para validar el estado de las reglas y el número de contadores de paquetes. Esta configuración es clave para simular un entorno seguro donde únicamente se permite el tráfico autorizado, mejorando la defensa perimetral en los sistemas Linux.

Figura 33. Reglas de firewall con iptables

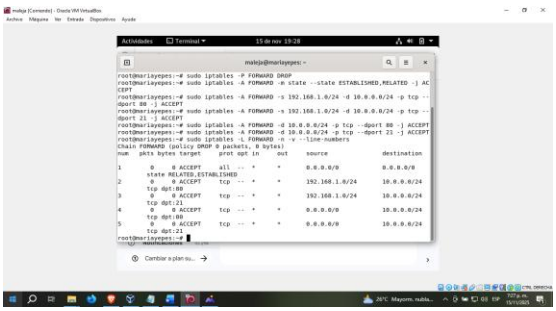


Fuente: Autoría Propia

5.3 VERIFICACIÓN DE TRÁFICO INTER - ZONA Y REGLAS HTTP

Este último paso consiste en comprobar que las reglas del firewall en el router están activas y funcionan adecuadamente. Para ello, se ha ejecutado el comando sudo iptables -L -v -n --line-numbers que, entre otras cosas, muestra una lista pormenorizada de las reglas de las tablas en la cadena FORWARD con el número de paquetes y bytes procesados; con ello se confirma si el tráfico se permite o se bloquea, tal como se ha planteado para desgranar en el procedimiento correspondiente de este laboratorio, todo el tráfico HTTP (puerto 80) y FTP (puerto 21) está activo y se aplican adecuadamente a las direcciones IP del LAN, DMZ y WAN, la política por defecto de la cadena FORWARD es DROP, es decir, el tráfico que no es explícitamente permitido por una regla entre zonas no fluirá entre zonas. Para validar la seguridad del entorno y confirmar que las políticas de acceso se apliquen como han sido diseñadas, es importante realizar esta verificación. La aplicación de reglas firewall en servidores Linux constituye una práctica esencial para la administración segura de entornos productivos, como lo enfatiza LaCroix en Masterting Ubuntu Server (2020).

Figura 34. Verificación de reglas de firewall



Fuente: Autoría Propia

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

La gestión del tráfico web dentro de una red local es un aspecto fundamental para garantizar seguridad, trazabilidad y buen uso de los recursos. En este trabajo se configuró un Proxy HTTP en modo no transparente utilizando Endian Firewall Community, con el propósito de controlar y monitorear la navegación desde la red interna.

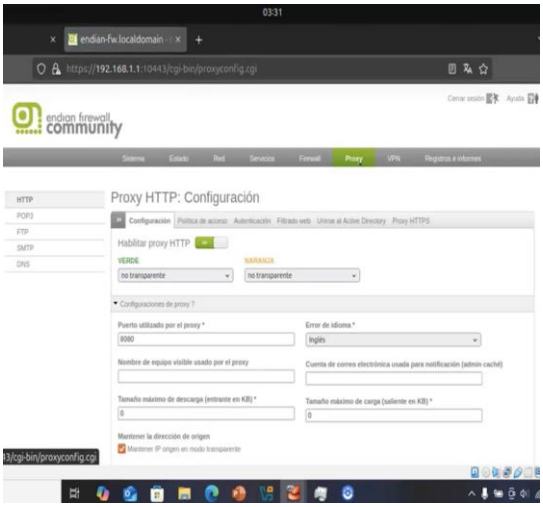
La modalidad no transparente obliga a que cada estación de trabajo configure manualmente el uso del proxy en su navegador, lo cual permite aplicar medidas adicionales como autenticación individual por usuario y perfiles de filtrado personalizados. Para este caso, se creó un perfil de bloqueo que contiene una lista negra con tres sitios específicos: Hotmail, YouTube y El Nuevo Día, los cuales se incluyeron siguiendo los lineamientos de la actividad.

Además del perfil de filtrado, se habilitó el sistema de autenticación NCSA, que permite registrar usuarios y agruparlos para asociarlos directamente a las políticas del proxy. Esto garantiza que solamente quienes posean credenciales válidas puedan navegar en Internet y que las restricciones de contenido se apliquen estrictamente a los usuarios autorizados.

Durante las pruebas en la red LAN, se configuró un cliente Ubuntu para utilizar el proxy de Endian en el puerto 8080. Al intentar ingresar a los sitios incluidos en la lista negra, el sistema mostró mensajes de denegación generados por el filtro de contenido, mientras que el acceso a páginas no restringidas se mantuvo disponible. Esto permitió comprobar que tanto la autenticación como las reglas de bloqueo estaban funcionando correctamente. La implementación confirmó que el uso de un proxy no transparente es una herramienta eficaz para administrar el uso de Internet, establecer controles claros y mantener una navegación más segura dentro de la organización o entorno académico.

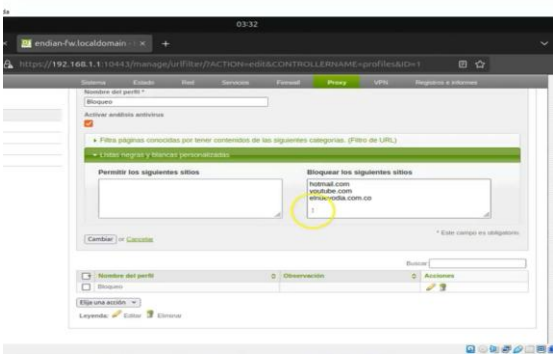
Referencia: Endian Firewall Community. (2023). *Endian* Firewall Documentation. https://www.endian.com/community/

Figura 35. Activación del proxy y puerto 8080



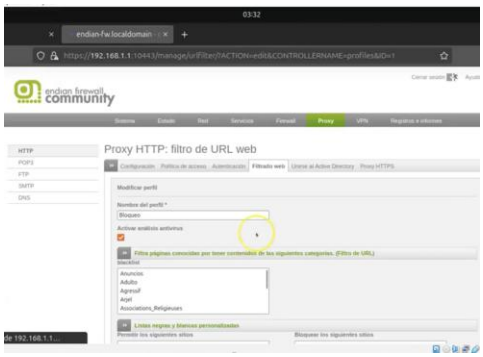
Fuente: Autoría Propia

Figura 36. Creación del perfil de filtrado



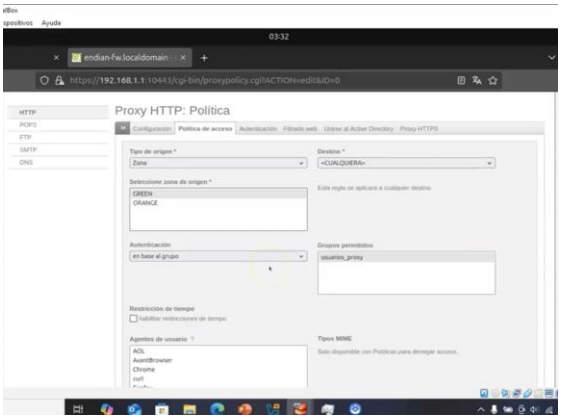
Fuente: Autoría Propia

Figura 37. Asociación del perfil a zona GREEN



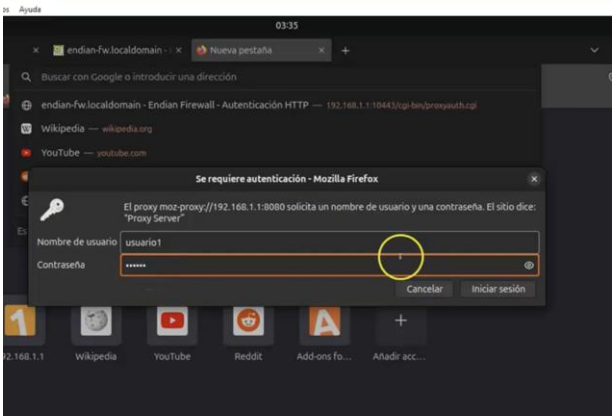
Fuente: Autoría Propia

Figura 38. Configuración de autenticación NCSA



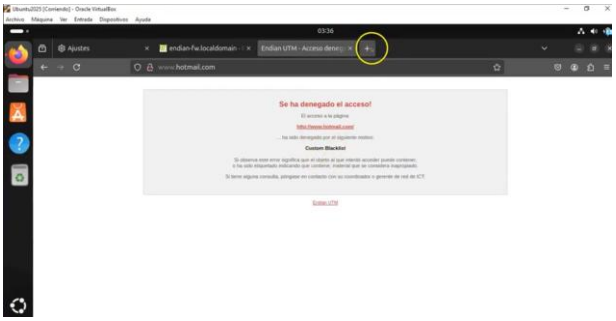
Fuente: Autoría Propia

Figura 39. Solicitud de inicio de sesión



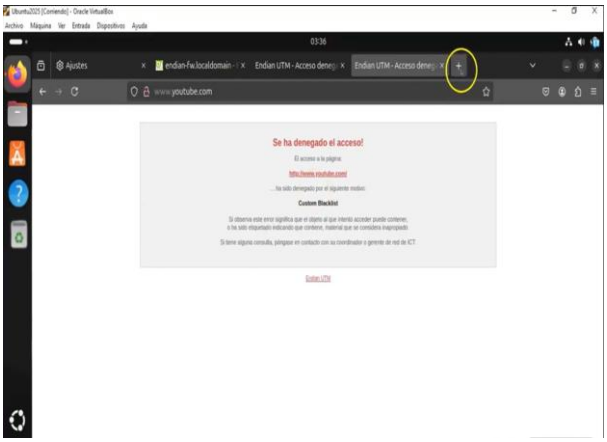
Fuente: Autoría Propia

Figura 40. Bloqueo de Hotmail



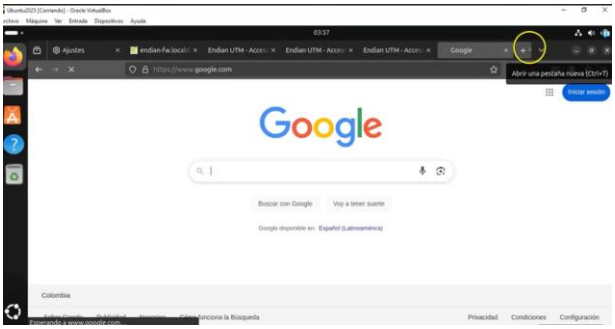
Fuente: Autoría Propia

Figura 41. Bloqueo de YouTube



Fuente: Autoría Propia

Figura 42. Acceso permitido a Google
Confirma que el proxy solo bloquea los sitios definidos



Fuente: Autoría Propia

6. CONCLUSIONES

Conclusión temática 1: La implementación del Endian Firewall en una infraestructura virtualizada permitió configurar y asegurar efectivamente las zonas de red verde (LAN interna), naranja (DMZ de servidores) y roja (acceso a Internet). Se logró establecer una segmentación comprensible y segura que aísla los activos críticos, controla el tráfico de red entre las zonas y se protege contra vulnerabilidades y amenazas externas a las que pueden estar expuestos los sistemas de información modernos. La verificación mediante pings y acceso a la interfaz gráfica de Endian en el navegador, permitió confirmar el correcto funcionamiento de la solución de la temática, cumpliendo con los objetivos de seguridad y administración definidos en la temática. Esta configuración y diseño demuestra la eficacia al utilizar soluciones open source para tener una seguridad robusta en redes corporativas.

Conclusión temática 2: La configuración de NAT en el entorno del Firewall Endian se establece como un mecanismo de seguridad imprescindible que permite gestionar de forma eficiente y controlada la comunicación entre las zonas aisladas (LAN, DMZ y WAN). A través de la implementación validada de SNAT (enmascaramiento) para el acceso a Internet y DNAT para el redireccionamiento de puertos, junto con la aplicación de reglas de filtrado de paquetes, se logró demostrar que es posible garantizar la conectividad necesaria para los usuarios y servidores internos sin comprometer la seguridad de la red, protegiendo la identidad de la infraestructura privada al ocultar su direccionamiento detrás de la interfaz pública.

Conclusión temática 3: En pocas palabras, trabajar con este tema hizo más sencillo comprender cómo opera una DMZ y cómo se manejan las reglas de seguridad usando un cortafuegos en la entrada de la red. La experiencia adquirida proporciona saberes cruciales para diseñar y poner en marcha infraestructuras protegidas en entornos de trabajo. La correcta división, control y monitoreo del flujo de datos que cruza el cortafuegos es vital para una arquitectura de red robusta frente a peligros tanto del exterior como del interior.

Conclusión temática 4: La Temática 4 permitió implementar y validar reglas de acceso en Linux mediante el uso de iptables, garantizando la segmentación y el control del tráfico entre las zonas LAN, DMZ y WAN. La configuración de interfaces, la definición de políticas de seguridad y la verificación de flujos de comunicación evidenciaron la importancia de aplicar principios de seguridad perimetral en sistemas operativos open source. Los resultados obtenidos demuestran que, al establecer políticas restrictivas y habilitar únicamente los servicios necesarios, se logra un entorno más seguro y confiable para la administración de redes. Este ejercicio constituye una base práctica para el fortalecimiento de competencias en gestión de seguridad informática y administración de sistemas operativos bajo estándares abiertos.

Conclusión temática 5: La configuración del Proxy HTTP no transparente en Endian permitió establecer un control real sobre la navegación desde la red interna. Con la creación del perfil de filtrado y la lista negra, fue posible restringir el acceso a los sitios definidos en la actividad, mientras que la autenticación por usuario garantizó que solo quienes tenían permisos pudieran conectarse a Internet. Las pruebas realizadas desde la LAN confirmaron que el sistema responde como se espera: bloquea los portales restringidos y permite la navegación general cuando el usuario se autentica correctamente. Esta práctica demuestra la utilidad del proxy como herramienta para administrar el uso de la red y fortalecer la seguridad en entornos donde es necesario regular el acceso a Internet.

7. REFERENCIAS

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

[2] Canonical (2023). *Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu*. https://help.ubuntu.com/20.04/ubuntu-help/index.html

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

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

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

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

[7] Endian. (s.f.). *Endian Firewall Community*. https://www.endian.com/community

[8] Cisco. (s.f.). Implementing Network Address Translation (NAT) for IPv4. Cisco Systems. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13605-23.html