IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Hossman Leonardo Egea Sossa
hlegeas@unadvirtual.edu.co
Maritza Castellanos Melo
mcastellanosme@unadvirtual.edu.co
Mayra Marcela González Rojas
mmgonzalezroj@unadvirtual.edu.co
Odair Alonso Jimenez Santos
oajimenezsa@unadvirtual.edu.co
Ferney Duvan Moncada Duran
fdmoncadad@unadvirtual.edu.co

RESUMEN: *En este trabajo se construyó un entorno de administración y control de tráfico utilizando Endian Firewall como sistema encargado de organizar y vigilar las comunicaciones entre las distintas áreas de una red simulada. Se configuraron las zonas interna, de servidores y de salida a Internet dentro de VirtualBox, asignando direcciones IP y validando la conexión entre ellas. Se aplicaron reglas de traducción de direcciones para permitir el acceso hacia el exterior y se habilitaron servicios como HTTP y FTP desde la zona de servidores. También se bloquearon solicitudes ICMP y se verificó el comportamiento desde las estaciones de trabajo. Adicionalmente, se configuraron reglas de acceso entre zonas y se comprobó su efecto desde navegadores y herramientas de consola. Finalmente, se implementó un proxy no transparente con autenticación y restricción de sitios. Los resultados confirmaron una correcta segmentación, control del flujo de datos y funcionamiento estable del entorno configurado.*

PALABRAS CLAVE: Autenticación, DMZ, Firewall, NAT.

1 INTRODUCCIÓN

La protección de la infraestructura digital se ha convertido en un elemento esencial dentro de cualquier organización que gestione información sensible o servicios expuestos a la red. En este trabajo se presenta el desarrollo completo de un entorno de práctica orientado a comprender, implementar y evaluar mecanismos de seguridad utilizando la distribución GNU/Linux Endian como plataforma principal de control y filtrado. A partir del despliegue de una arquitectura con zonas diferenciadas —LAN, DMZ y WAN— cada integrante del grupo abordó una temática específica que permitió analizar funciones reales de un firewall, tales como la gestión de reglas, la traducción de direcciones, el control de servicios y la aplicación de políticas de acceso.

El documento reúne los resultados individuales, describe la metodología aplicada y muestra la forma en que se verificó el funcionamiento de cada configuración. De esta manera, se ofrece una visión general del proceso de aseguramiento básico de una red corporativa y del papel que cumplen las herramientas de código abierto en este tipo de implementaciones.

2 TEMÁTICAS

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

RESUMEN: *En esta temática se llevó a cabo la implementación de un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall en VirtualBox. El proceso incluyó la creación de la máquina virtual, la configuración de tres adaptadores de red correspondientes a las zonas Green (LAN), Orange (DMZ) y Red (WAN), y la instalación efectiva del sistema Endian 3.3.2. Se asignaron direcciones IP a cada zona y se validó la conectividad interna mediante pruebas de ping entre equipos del segmento LAN y DMZ. Además, se verificó el acceso al panel web de administración y la conexión a Internet desde la zona Roja. Los resultados obtenidos confirmaron el funcionamiento correcto de la segmentación, las reglas de seguridad predeterminadas y la salida WAN, demostrando un entorno seguro y funcional para la gestión del tráfico en una red corporativa.*

PALABRAS CLAVE: DMZ, Endian Firewall, Segmentación de red, VirtualBox.

2.1.1 INTRODUCCIÓN

La presente sección introduce el desarrollo de la Temática 1, cuyo propósito fue implementar un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall dentro de la plataforma VirtualBox. Esta temática permitió configurar la instancia del firewall, definir las tarjetas de red necesarias y establecer la segmentación por zonas Green (LAN), Orange (DMZ) y Red (WAN), conforme a los lineamientos planteados en la guía de aprendizaje de la Etapa 7. La instalación del sistema Endian 3.3.2, la asignación de direccionamientos IP, la validación de conectividad y la verificación de políticas predeterminadas permitieron demostrar el funcionamiento adecuado del modelo perimetral. Este artículo describe los procedimientos realizados, la estructura configurada y los resultados obtenidos, presentando

la información en un formato alineado con las especificaciones IEEE para la elaboración de reportes técnicos.

2.1.2 PROCEDIMIENTO Y RESULTADO

El desarrollo de la Temática 1 consistió en la instalación y configuración inicial de GNU/Linux Endian Firewall dentro del entorno virtual VirtualBox, con el objetivo de implementar una arquitectura de seguridad perimetral basada en las zonas Green (LAN), Orange (DMZ) y Red (WAN). Este proceso permitió establecer una estructura ordenada y segmentada para el control del tráfico interno y externo de la red.

El procedimiento inició con la creación de la máquina virtual destinada para Endian Firewall, a la cual se le asignaron 2048 MB de memoria RAM y un procesador, recursos suficientes para garantizar un funcionamiento estable durante las pruebas de seguridad. Posteriormente, se configuraron los tres adaptadores de red necesarios para la segmentación perimetral: el primer adaptador se definió como red interna Green-Net para la LAN, el segundo como red interna Orange-DMZ para la zona de servidores, y el tercero en modo NAT con el fin de permitir el acceso a la red WAN simulada.

Tras configurar el entorno virtual, se procedió con la instalación del sistema Endian Firewall 3.3.2. Una vez finalizada la instalación, se validó que la interfaz Green estuviera activa y que el firewall estuviera disponible para su administración mediante la interfaz web. Esta verificación inicial permitió confirmar que el sistema estaba correctamente instalado y funcional.

Para garantizar que la zona LAN tuviera comunicación con el firewall, se realizó una prueba de conectividad desde un equipo Ubuntu configurado en la red Green. La respuesta correcta a la solicitud ICMP validó que el direccionamiento, la red interna y la interfaz Green estaban operativas. De manera similar, se configuró un servidor Ubuntu en la DMZ, desde el cual se verificó la conectividad hacia la interfaz Orange, confirmando la correcta asignación del direccionamiento correspondiente.

Uno de los puntos clave de la temática fue comprobar el comportamiento por defecto del firewall entre zonas. Se evidenció que, inicialmente, la comunicación entre la LAN y la DMZ se encontraba bloqueada. Esto demostró la eficacia de las políticas de seguridad predeterminadas, diseñadas para impedir el tráfico entre segmentos sin autorización. Para permitir el intercambio controlado, se creó una regla específica que habilitó el protocolo ICMP desde la zona Green hacia la Orange. Una vez aplicada, se verificó que el tráfico entre ambas zonas se restableció correctamente, asegurando al mismo tiempo la trazabilidad mediante el registro de conexiones.

La zona Red también fue validada como parte del proceso. El firewall obtuvo una dirección IP de manera automática mediante DHCP, lo que permitió confirmar la correcta salida hacia Internet. La conectividad hacia direcciones externas reflejó que la interfaz WAN funcionaba adecuadamente y que el tráfico saliente se gestionaba correctamente mediante NAT.

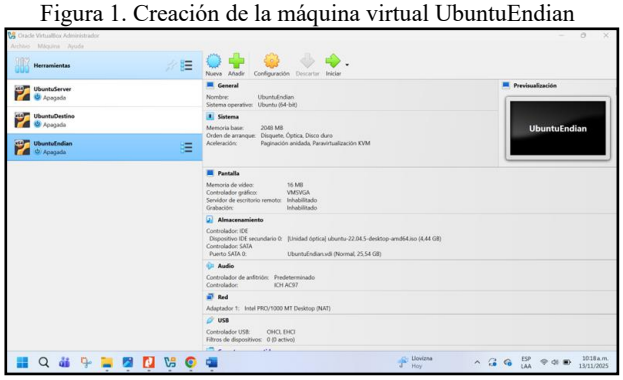
Finalmente, se consolidó la estructura completa de segmentación de la red: la zona Green configurada con el direccionamiento 192.168.1.1/24, la zona Orange con 10.0.0.1/24 y la zona Red funcionando bajo asignación dinámica de direcciones. Esta segmentación permitió diferenciar claramente los niveles de acceso, el flujo de paquetes y los roles de cada segmento dentro del entorno de pruebas.

Con ello, se cumplió satisfactoriamente el objetivo principal de la temática: implementar y validar una instancia funcional de Endian Firewall con las tres zonas perimetrales requeridas, garantizando su conectividad interna, la administración por interfaz web y la salida exitosa hacia Internet.

2.1.3 IMÁGENES RELACIONADAS A LA TEMÁTICA 1 CON SU PROCESO DE DESARROLLO

El proceso inicia con la preparación del entorno virtual en el que se implementaría el firewall. Para ello se creó la máquina virtual destinada a alojar Endian Firewall 3.3, definiendo los recursos necesarios para garantizar un funcionamiento estable dentro del laboratorio. Se asignaron 2048 MB de memoria RAM y 1 CPU, parámetros adecuados para ejecutar los servicios de filtrado, monitoreo y administración del sistema sin afectar su desempeño. Luego, se cargó la imagen ISO correspondiente para proceder con la instalación del sistema.

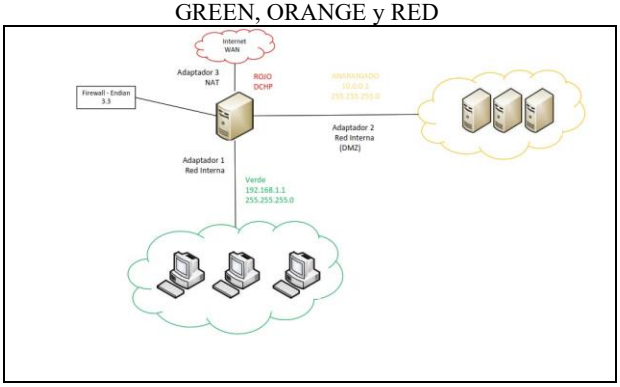
Figura 1. Creación de la máquina virtual UbuntuEndian



Fuente. Autoría propia

Tras la creación de la máquina virtual, fue necesario configurar los adaptadores de red, elemento fundamental para que Endian pudiera cumplir su función como firewall de múltiples zonas.

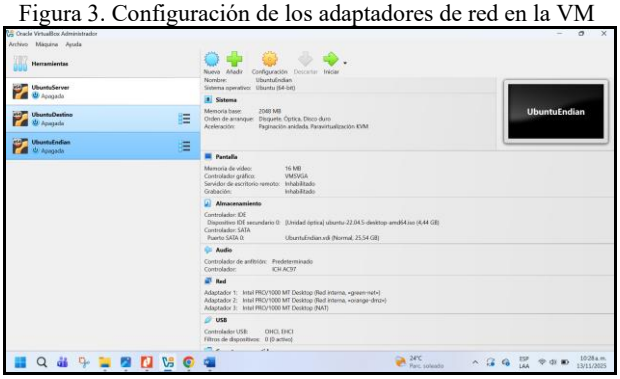
Figura 2. Segmentación de red en Endian Firewall 3.3: Zonas GREEN, ORANGE y RED



Fuente. Autoría propia

En esta configuración se establecieron tres adaptadores, cada uno asignado a una zona específica: el adaptador 1 para la zona GREEN (LAN interna), el adaptador 2 para la zona ORANGE (DMZ) y el adaptador 3 para la zona RED (WAN). Las zonas GREEN y ORANGE se configuraron como redes internas independientes (green-net y orange-dmz), permitiendo simular adecuadamente la separación de redes propuesta por la segmentación. Por su parte, la zona RED se configuró en modo NAT para proporcionar salida a Internet al firewall.

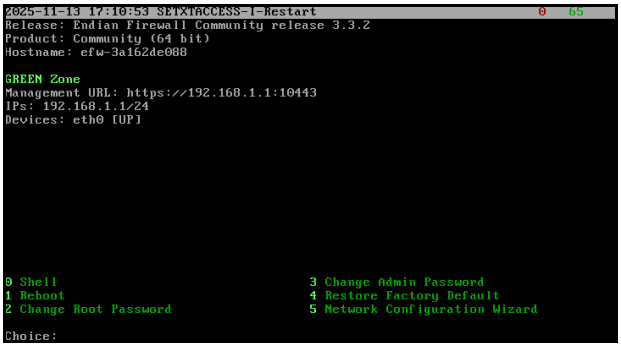
Figura 3. Configuración de los adaptadores de red en la VM



Fuente. Autoría propia

Una vez completada la instalación del sistema, se accedió a la consola principal de Endian, donde fue posible validar que la interfaz GREEN se encontraba operativa y que se había asignado correctamente la dirección IP para el acceso al panel web de administración. Este punto fue esencial, ya que confirmaba que el firewall estaba inicializado y listo para ser gestionado desde su interfaz gráfica.

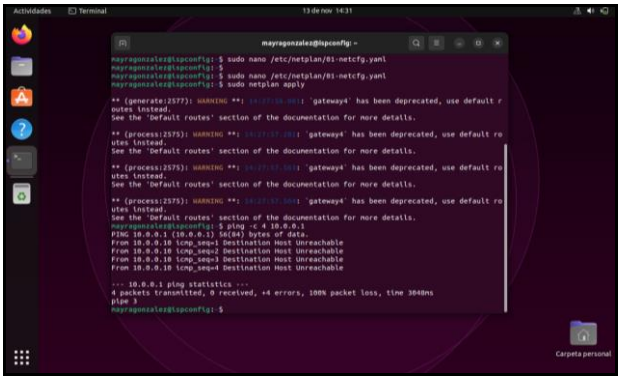
Figura 4. Pantalla principal de Endian Firewall con zona GREEN activa tras la instalación



Fuente. Autoría propia

Posteriormente, se realizó una verificación de conectividad desde la máquina UbuntuDestino ubicada en la zona GREEN. Mediante el comando ping hacia la dirección IP del firewall (192.168.1.1), se confirmó que ambas máquinas se encontraban correctamente comunicadas dentro de la misma red interna.

Figura 5. Prueba de conectividad entre UbuntuServer y la zona ORANGE en Endian Firewall



Fuente. Autoría propia

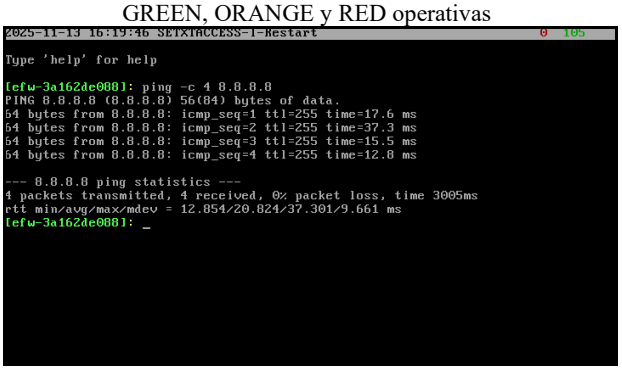
Con la conectividad de la zona GREEN verificada, se procedió a acceder al panel web de administración de Endian Firewall, donde se visualizó el tablero principal. Desde este panel se gestionan las zonas de red, las políticas de seguridad, los servicios del sistema y los registros de actividad, permitiendo administrar por completo el comportamiento del firewall.

Figura 6. Panel web principal de administración de Endian Firewall Community

Fuente. Autoría propia

Finalmente, se validaron las configuraciones de las zonas ORANGE y RED, así como la conexión entre ellas. Se comprobó que la segmentación de red funcionaba correctamente, que las reglas aplicadas eran efectivas y que el firewall obtenía dirección IP en la interfaz WAN para permitir salida a Internet. Con ello se completó la implementación del modelo de seguridad propuesto, basado en la segmentación en zonas y control de tráfico.

Figura 7. Configuración final de Endian Firewall con zonas GREEN, ORANGE y RED operativas



Fuente. Autoría propia

2.2 CONFIGURACIÓN NAT

RESUMEN: *En esta sección se presenta el proceso de la configuración y validación de las reglas NAT en la plataforma Endian Firewall como parte de un ejercicio práctico, el cual fue enfocado en la seguridad de Red. Ya que se trabajó directamente en la creación de reglas para permitir así la comunicación controlada desde la red interna "Verde" y la red intermedia "Naranja - DMZ", hacia la red externa "Roja", de esta manera se aplican conceptos fundamentales tales como la traducción de direcciones y el filtrado de tráfico. De este modo los resultados nos permiten demostrar el funcionamiento correcto de las reglas que se han implementado y la efectividad del firewall para gestionar así las políticas de acceso.*

PALABRAS CLAVE: Endian, DMZ, Seguridad de red.

2.2.1 INTRODUCCIÓN

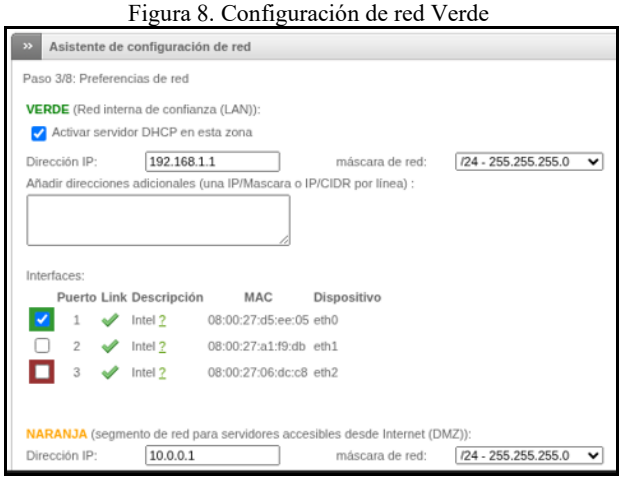
El control del tráfico entre las redes internas y externas son un aspecto de suma importancia, ya que estas son esenciales en la administración de sistemas orientados a la seguridad. Por lo tanto, los Firewalls permitirán definir políticas claras que determinarán que servicios pueden comunicarse hacia el exterior sin comprometer así la integridad del sistema. Es por esto que Endian Firewall es una solución que integra funcionalidades de Firewall, Proxy, Filtrado y Monitoreo. Debido a esto en el presente desarrollo se trabajó única y exclusivamente en la creación, validación y análisis de las reglas NAT con la finalidad de permitir la comunicación segura entre diferentes zonas de red. Ya que la práctica se enfocó únicamente en los procesos internos del firewall y su comportamiento frente a las reglas ya previamente configuradas y establecidas por el administrador.

2.2.2 PROCEDIMIENTO

- Configuración de regla NAT para la red verde:

El primero ejercicio consistió en realizar la creación de una regla NAT que permitiera a los equipos de la red "Verde" acceder a servicios externos por medio de la Red. Por lo tanto, la regla fue configurada desde el módulo NAT del Firewall

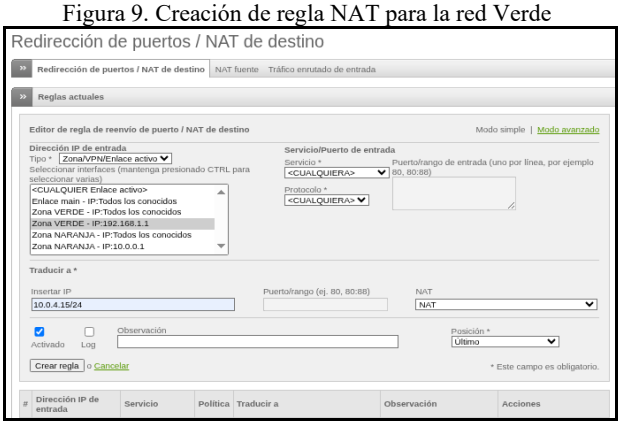
Figura 8. Configuración de red Verde



Fuente. Autoría propia

Especificando así la red de origen "Verde" y definiendo de esta forma la traducción hacia la red externa.

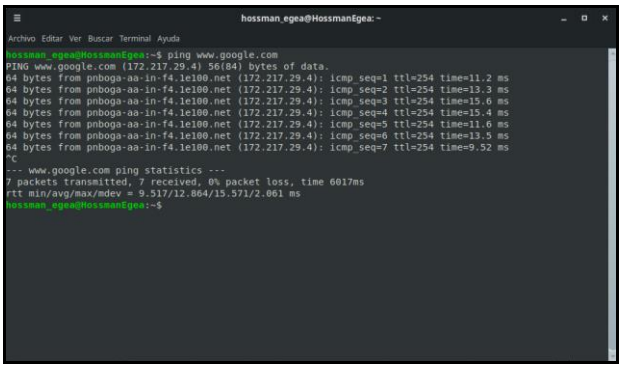
Figura 9. Creación de regla NAT para la red Verde



Fuente. Autoría propia

Luego de esto se realizaron pruebas de conectividad desde el cliente asociado a esta red, por lo cual se verifico la salida a internet mediante comandos como “ping” y la comprobación de resoluciones “DNS”.

Figura 10. Comprobación de conexión a Internet desde la red Verde



Fuente. Autoría propia

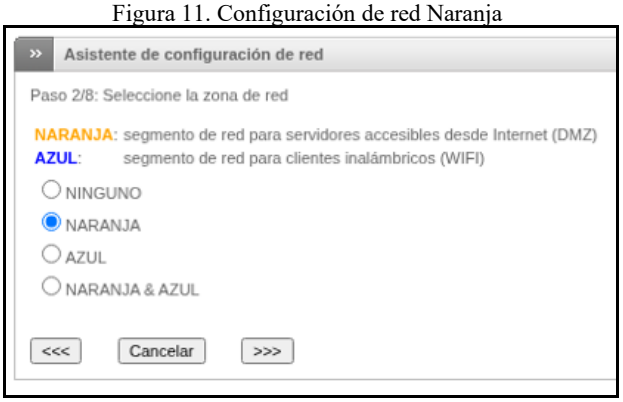
De este modo la respuesta correcta confirmo que la traducción de direcciones funcionaba correctamente.

- Configuración de regla NAT para la DMZ “Naranja”:

La segundad actividad se centró en realizar la habilitación de una regla NAT para permitir de este modo que la red DMZ estableciera una comunicación hacia el Exterior. Ya que esta zona intermedia requiere un control especial, debido a su papel como punto de conexión entre los servicios internos y externos.

La prense regla fue creada igualmente desde el módulo NAT

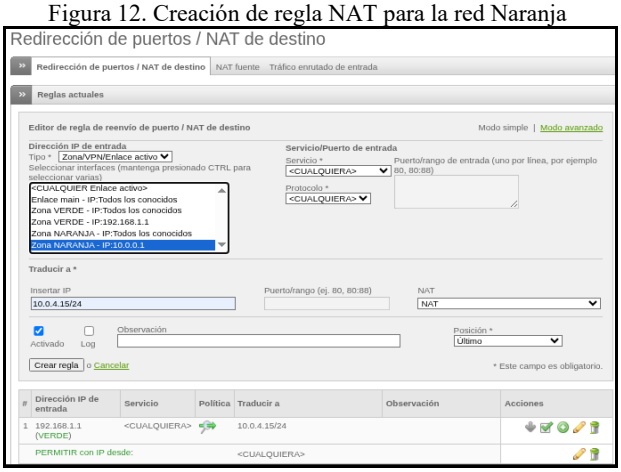
Figura 11. Configuración de red Naranja



Fuente. Autoría propia

Asignando como origen la red Naranja. Luego de realizar la aplicación de esta regla

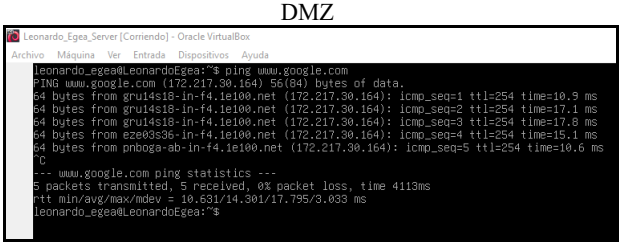
Figura 12. Creación de regla NAT para la red Naranja



Fuente. Autoría propia

Se realizaron pruebas de conectividad desde la estación ubicada en la DMZ, comprobando de esta forma el acceso hacia la red Verde y de igual forma hacia la red Roja.

Figura 13. Comprobación de conexión a Internet desde la DMZ



Fuente. Autoría propia

2.2.3 RESULTADOS

Con los resultados obtenidos demostramos lo siguiente:

- Las reglas NAT fueron aplicadas correctamente y se reflejaron de forma inmediata en el módulo de gestión de Endian.

- La Red “Verde” obtuvo acceso estable a los servicios externos según lo anteriormente previsto.
- La “DMZ” logro establecer comunicación hacia internet respetando así las políticas ya definidas.
- Las pruebas realizadas confirmaron flujo de paquetes, traducción de las direcciones y el funcionamiento total del firewall.
- Endian cumplió su función como una herramienta de seguridad red, aplicado control y segmentación del tráfico.

2.3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

RESUMEN: *En esta temática se habilitaron y controlaron servicios esenciales dentro de una red segmentada mediante Endian Firewall, empleando una máquina Ubuntu Server como servidor ubicado en la zona DMZ. Se verificó inicialmente la disponibilidad de los servicios HTTP y FTP mediante comandos de inspección de puertos en el servidor. Posteriormente, desde el panel web de Endian se configuraron reglas específicas en el tráfico entre zonas para permitir el acceso desde la zona Verde hacia la DMZ, garantizando la comunicación segura con el servidor. También se implementó una regla personalizada para bloquear el protocolo ICMP, impidiendo respuestas de ping desde la LAN hacia la zona Naranja. Las pruebas realizadas desde el cliente confirmaron el acceso correcto a los servicios permitidos y la efectiva denegación de ICMP. Los resultados demostraron el funcionamiento esperado de las políticas aplicadas y la correcta gestión del tráfico entre las zonas.*

PALABRAS CLAVE: Endian Firewall, ICMP, Servicios HTTP y FTP.

2.3.1 INTRODUCCIÓN

La correcta administración del tráfico entre redes internas y segmentos expuestos es un componente esencial en cualquier esquema de seguridad basado en zonas. En este contexto, la Temática 3 se centra en el control selectivo de los servicios que pueden atravesar la DMZ, asegurando que únicamente el tráfico necesario llegue al servidor y evitando solicitudes no autorizadas. Para ello, se utilizó Endian Firewall como plataforma de gestión perimetral y un servidor GNU/Linux Ubuntu Server ubicado dentro de la zona naranja.

En este apartado se describe el proceso de habilitar servicios específicos para garantizar el acceso controlado desde la red interna, así como el procedimiento para bloquear el protocolo ICMP con el fin de evitar diagnósticos remotos mediante ping. A lo largo del desarrollo se detallan las configuraciones realizadas, la verificación funcional de cada regla y el impacto de estas medidas en la seguridad del entorno. Esta sección proporciona una visión clara del objetivo, el alcance y la lógica aplicada para asegurar adecuadamente la comunicación entre zonas.

2.3.2 PROCEDIMIENTO

Para el desarrollo de la temática 3 se siguió un proceso progresivo que inició con la verificación del correcto funcionamiento de los servicios instalados en el servidor ubicado en la zona Naranja. Antes de realizar cualquier modificación al firewall de Endian, se comprobó que tanto el servicio web (Apache) como el servicio FTP (ProFTPD) estuvieran activos, escuchando en sus respectivos puertos y respondiendo adecuadamente dentro del propio servidor. Esto aseguró que cualquier falla posterior pudiera atribuirse a la configuración del firewall y no a los servicios en sí.

Figura 14. Verificación del estado de Apache y ProFTPD en el servidor de la zona Naranja

Fuente. Autoría propia

Posteriormente, se realizaron pruebas desde el cliente ubicado en la zona Verde para confirmar la conectividad inicial entre ambas zonas. Desde este cliente se verificó que el servidor respondiera al ping y que los servicios HTTP y FTP fueran accesibles sin restricciones. Esta serie de pruebas iniciales permitió establecer un punto de comparación entre el comportamiento antes y después de aplicar las reglas del firewall.

Después de documentar el estado inicial del firewall, se comenzó a implementar las reglas específicas solicitadas para este ejercicio. En primer lugar, se creó una regla que permitiera únicamente el tráfico HTTP desde la zona Verde hacia la zona Naranja. Esta regla se ubicó en una posición superior dentro de la lista para asegurar que fuera evaluada antes que la regla general. Se realizó un proceso equivalente para el tráfico FTP, creando una segunda regla que autorizara únicamente el acceso al puerto correspondiente.

Figura 15. Reglas de firewall configuradas para permitir HTTP y FTP desde la zona Verde hacia la zona Naranja

Fuente. Autoría propia

Con estas dos reglas instaladas, se procedió a realizar pruebas nuevamente desde el cliente para verificar que el acceso al servidor web y al servidor FTP se mantuviera en funcionamiento. La disponibilidad de ambos servicios confirmó que las reglas específicas habían sido aplicadas correctamente y que el tráfico permitido continuaba fluyendo sin interrupciones.

Una vez comprobado el funcionamiento adecuado, se eliminó la regla general que permitía todo el tráfico entre ambas zonas. Al retirar esta regla, únicamente quedarían activas las reglas específicas que autorizaban HTTP y FTP, alineándose con el objetivo del ejercicio: restringir el acceso solo a los servicios requeridos y evitar que la zona Verde pudiera acceder a cualquier otro puerto o protocolo del servidor.

El siguiente paso consistió en aplicar la política de bloqueo del tráfico ICMP desde la zona Verde hacia la zona Naranja, específicamente los tipos de mensajes utilizados para solicitudes de eco y trazas. Para ello, se creó una regla personalizada dentro de Endian que deniega expresamente este tipo de tráfico.

Figura 16. Regla de bloqueo de tráfico ICMP entre la zona Verde y la zona Naranja

Fuente. Autoría propia

Tras aplicar esta política de bloqueo, se realizaron nuevas pruebas desde el cliente. Se observó que el servidor dejó de responder a las solicitudes de ping, lo cual demostró que el firewall estaba bloqueando correctamente dichos paquetes. Al mismo tiempo, se verificó que tanto el servicio web como el servicio FTP permanecieran accesibles, lo que confirmó que el bloqueo selectivo del ICMP no afectó los protocolos permitidos.

Finalmente, se revisó la tabla actualizada de reglas en el firewall para corroborar que solo permanecieran activas las reglas específicas creadas durante el ejercicio: la regla de permiso HTTP, la regla de permiso FTP y la regla de bloqueo ICMP. Con esto se confirmó que la configuración del firewall quedó ajustada de acuerdo con los requisitos propuestos, permitiendo únicamente el tráfico necesario entre ambas zonas y bloqueando todo tipo de tráfico no autorizado.

2.3.3 RESULTADOS

Los resultados obtenidos confirmaron que cada una de las configuraciones aplicadas produjo los efectos esperados en el tráfico entre la zona Verde y la zona Naranja. Para iniciar, se verificó que los servicios instalados en el servidor Apache para HTTP y ProFTPD para FTP estuvieran activos antes de modificar el firewall. Para ello se utilizaron los comandos systemctl status apache2 y systemctl status proftpd, con los cuales se evidenció que ambos servicios estaban en ejecución y escuchando correctamente en los puertos 80 y 21. Esta comprobación inicial permitió asegurar que cualquier cambio en el comportamiento posterior sería atribuible a las reglas de Endian y no al servidor.

En las primeras pruebas desde el cliente ubicado en la zona Verde se confirmó que existía comunicación total hacia el servidor en la zona Naranja. Se utilizó el comando ping para validar la conectividad general, observándose respuestas sin pérdida de paquetes. De igual forma, se probó el acceso HTTP mediante curl http://10.0.0.X, y el acceso FTP a través de ftp 10.0.0.X, lo que demostró que el servidor respondía adecuadamente antes de aplicar reglas restrictivas.

Una vez creadas las reglas específicas en Endian para permitir únicamente HTTP y FTP, se repitieron las pruebas. El uso de curl permitió comprobar que el portal web del servidor continuaba siendo accesible desde la zona Verde, demostrando que la regla de permiso para el puerto 80 funcionaba correctamente. De la misma manera, el cliente FTP pudo establecer conexión empleando ftp 10.0.0.X, lo que confirmó que el puerto 21 permanecía autorizado y operativo.

Finalmente, al aplicar la regla de bloqueo de ICMP, se realizaron pruebas nuevamente con el comando ping. Como resultado, el servidor dejó de responder mostrando ausencia total de respuesta.

Figura 17. Intento de ping desde la zona Verde tras aplicar la regla de bloqueo ICMP

Fuente. Autoría propia

Este comportamiento demostró que Endian estaba filtrando correctamente los paquetes ICMP, sin interferir con los protocolos previamente autorizados.

En conjunto, las pruebas realizadas confirmaron que las reglas creadas en el firewall funcionaron según lo esperado: HTTP y FTP continuaron accesibles tras la configuración; ICMP fue bloqueado de forma efectiva. El comportamiento observado validó que la segmentación entre zonas operó de manera precisa, garantizando un control adecuado del tráfico entre la LAN y la DMZ.

2.4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

RESUMEN: *En esta temática se implementó un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall en VirtualBox. El proceso contempló la creación de la máquina virtual, la configuración de tres adaptadores de red correspondientes a zonas Green (LAN), Orange (DMZ) y Red (WAN), y la instalación del sistema Endian 3.3.2. Se asignaron direcciones IP a cada zona y se validó la conectividad interna mediante pruebas de ping entre los equipos del segmento LAN y DMZ. También se verificó el acceso al panel web de administración y la conexión a Internet desde la zona Roja. Posteriormente, se configuraron reglas específicas para permitir el tráfico HTTP y FTP entre LAN y DMZ, junto con reglas de salida hacia WAN y NAT para habilitar el acceso controlado desde Internet hacia la DMZ. Los resultados confirmaron el funcionamiento correcto de la segmentación, las políticas aplicadas y la salida WAN, demostrando un entorno seguro y operativo.*

PALABRAS CLAVE: NAT, DMZ, LAN, WAN.

2.4.1 INTRODUCCIÓN

La segmentación de redes y el control del tráfico son pilares fundamentales en la seguridad perimetral. Este trabajo documenta la implementación de reglas en Endian Firewall para permitir o denegar tráfico entre zonas, aplicando protocolos HTTP y FTP, y configurando NAT para acceso seguro desde Internet hacia la DMZ. Se empleó VirtualBox como plataforma de virtualización, lo que permitió simular un entorno corporativo con tres zonas diferenciadas.

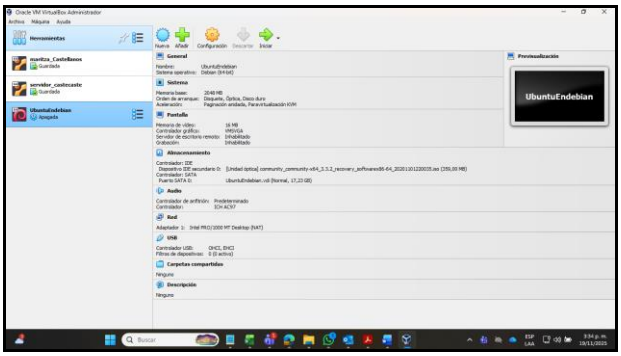
2.4.2 PROCEDIMIENTO

- Preparación del entorno

Se creó la máquina virtual Endian Firewall en VirtualBox, asignando 2048 MB de RAM y 1 CPU. Se configuraron tres adaptadores: GREEN (LAN interna), ORANGE (DMZ) y RED (WAN con NAT).

En la fig. 18 se evidencia la vista general de la máquina virtual en Oracle VM VirtualBox. La imagen muestra la interfaz del administrador de VirtualBox con la máquina virtual seleccionada. Se observan los parámetros asignados: sistema operativo Debian (64-bit), memoria RAM, CPU, almacenamiento con disco virtual y adaptadores 3.

Figura 18. Vista general de la máquina virtual en Oracle VM VirtualBox



Fuente. Autoría propia

- Configuración de zonas

Se asignaron direcciones IP: GREEN (192.168.1.1), ORANGE (10.0.0.1) y RED (DHCP). Se validó conectividad mediante pruebas de ping entre LAN y DMZ.

- Creación de reglas

Se configuraron reglas para permitir HTTP (puerto 80) y FTP (puerto 21) entre LAN y DMZ, reglas de salida hacia WAN y NAT para acceso desde WAN hacia DMZ.

Tabla 1.

Origen	Destino	Servicio	Acción
LAN	DMZ	HTTP (80)	Permitir
LAN	DMZ	FTP (21)	Permitir
LAN	WAN	HTTP/FTP	Permitir
DMZ	WAN	HTTP/FTP	Permitir
WAN	DMZ	HTTP/FTP	NAT

Fuente. Autoría propia

La tabla muestra las reglas configuradas en el firewall para controlar el tráfico entre las zonas LAN, DMZ y WAN. Cada regla define el origen, destino, servicio y acción:

- Se permite tráfico HTTP (80) y FTP (21) entre LAN y DMZ.

- Se habilita la salida de LAN y DMZ hacia WAN para HTTP/FTP.

- Se aplica NAT para permitir acceso desde WAN hacia DMZ, garantizando la publicación segura de servicios internos.

Estas reglas aseguran comunicación controlada y segmentación segura entre las zonas.

2.4.3 RESULTADOS

Las pruebas confirmaron acceso HTTP y FTP entre LAN y DMZ, salida a Internet y acceso controlado desde WAN hacia DMZ mediante NAT. Los registros del firewall evidenciaron la aplicación correcta de las políticas y la segmentación segura entre zonas.

Figura 19. Configuración de reglas HTTP y FTP

Fuente. Autoría propia

La imagen muestra el panel de administración de Endian Firewall con las reglas creadas para permitir tráfico HTTP y FTP entre las zonas LAN, DMZ y WAN. Se observan las políticas aplicadas, los puertos habilitados y las acciones configuradas (permitir o NAT), confirmando la correcta implementación de las directivas.

- Diagrama de segmentación de red

El diagrama ilustra la arquitectura configurada en Endian Firewall:

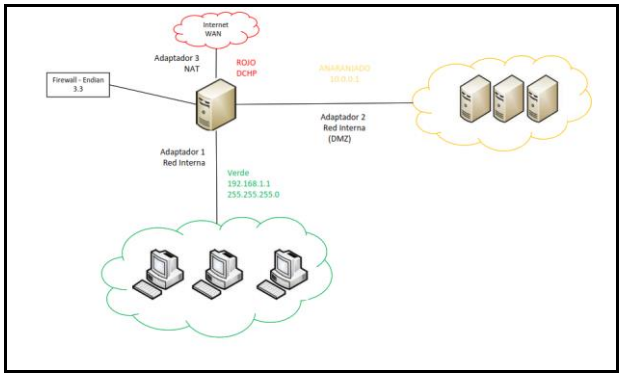
- Zona Verde (LAN interna): 192.168.1.1.

- Zona Naranja (DMZ): 10.0.0.1.

- Zona Roja (WAN): salida a Internet mediante NAT.

Cada adaptador cumple una función específica, garantizando comunicación controlada y segura entre las zonas.

Figura 20. Arquitectura de red configurada en Endian Firewall 3.3



Fuente. Autoría propia

El diagrama ilustra la arquitectura de red configurada en Endian Firewall 3.3, donde cada adaptador cumple una función específica dentro del esquema de seguridad:

- Adaptador 1 enlaza la Zona Verde (LAN interna – 192.168.1.1/24), destinada a los equipos de usuario.

- Adaptador 2 conecta la Zona Naranja (DMZ – 10.0.0.1), reservada para servidores y servicios expuestos.

- Adaptador 3 gestiona la Zona Roja (WAN), que proporciona salida a Internet mediante NAT y asignación dinámica de IP por DHCP.

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

RESUMEN: *Este artículo describe el diseño e implementación de una arquitectura de seguridad perimetral basada en la distribución de código abierto Endian Firewall 3.3. La topología propuesta separa el tráfico en tres zonas de seguridad (WAN, LAN y DMZ) e implementa un proxy HTTP no transparente con autenticación de usuarios y políticas de listas negras. El trabajo se desarrolló empleando infraestructura virtualizada en Oracle VirtualBox y clientes GNU/Linux, donde se requiere comprender conceptos de seguridad perimetral y la configuración práctica de gateways de seguridad.*

PALABRAS CLAVE: Seguridad perimetral, Endian Firewall, DMZ, Proxy HTTP.

2.5.1 INTRODUCCIÓN

Las redes informáticas que exponen o publican servicios a Internet requieren mecanismos de protección para reducir la superficie de ataque y controlar el acceso a los recursos internos. Los firewalls, servidores proxy y la segmentación de red son técnicas que nos permiten implementar un perímetro seguro.

En este trabajo se documenta el despliegue práctico de Endian Firewall Community 3.3 como dispositivo central en

una topología de laboratorio. El objetivo principal es proteger servicios internos y externos mediante la separación de la red en tres zonas: LAN (GREEN), DMZ (ORANGE) y WAN (RED). Además, se implementa un proxy HTTP no transparente con autenticación y listas negras, cumpliendo con los requisitos del escenario educativo.

2.5.2 PROCEDIMIENTO

- Marco teórico

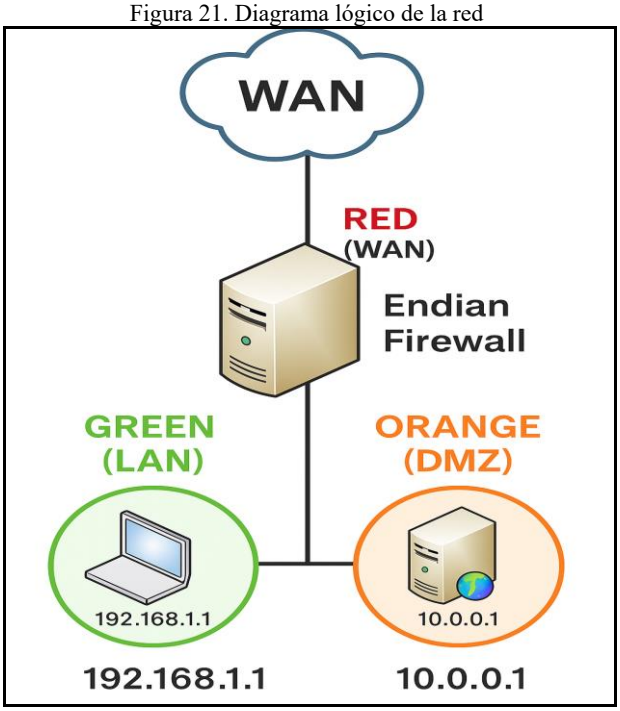
El concepto de seguridad perimetral se basa en separar redes internas confiables de redes externas no confiables. Los firewalls operan usualmente en las capas 3 y 4 del modelo OSI, aplicando políticas basadas en direcciones IP, puertos y protocolos. Los proxys complementan esta función inspeccionando protocolos específicos como HTTP, SMTP, etc.

Endian Firewall es una distribución GNU/Linux que integra el motor de firewall Netfilter/iptables con una interfaz web de administración. Define cuatro zonas codificadas por colores: RED (WAN), GREEN (LAN), ORANGE (DMZ) y BLUE (red inalámbrica o especial) para esta actividad trabajaremos solo las tres primeras. Cada zona tiene políticas predeterminadas que controlan el flujo del tráfico.

- Entorno de Laboratorio y Diseño de Red

El proyecto se implementó utilizando Oracle VirtualBox como plataforma de virtualización. Se configuraron tres adaptadores de red virtuales en la máquina donde se instaló Endian Firewall, asignando cada uno a una zona específica:

Figura 21. Diagrama lógico de la red



Fuente. Autoría propia

- Adaptador 1 – RED (WAN): modo NAT, obteniendo IP por DHCP.
- Adaptador 2 – GREEN (LAN): red interna Zona_GREEN con IP 192.168.1.1 / 24.
- Adaptador 3 – ORANGE (DMZ): red interna Zona_ORANGE con IP 10.0.0.1 / 24.

El cliente LAN se configuró en la red Zona_GREEN con IP estática 192.168.1.10 / 24, puerta de enlace 192.168.1.1 y DNS 8.8.8.8. Un servidor en la DMZ puede configurarse en la red 10.0.0.1 / 24 para alojar servicios web o de base de datos.

- Configuración de Endian Firewall

Después de finalizar la instalación, la configuración inicial se realizó mediante el asistente de consola. Se asignó cada interfaz a su zona correspondiente, manteniendo RED en DHCP y definiendo manualmente las direcciones GREEN y ORANGE. Posteriormente, la administración se llevó a cabo ingresando a https://192.168.1.1:10443/ desde el cliente LAN.

- Proxy HTTP No Transparente con Autenticación

El proxy HTTP se habilitó para la zona GREEN en modo no transparente, usando el puerto 8080. La autenticación se configuró mediante el backend local (NCSA), creando un grupo llamado grupoProxy y añadiendo los usuarios correspondientes.

Se añadió una política de acceso asociada al grupo autenticado. En el navegador del cliente se configuró el proxy manual apuntando a 192.168.1.1:8080 para HTTP y HTTPS.

- Lista Negra de URLS

Se creó un perfil de filtrado Web donde se añadieron a la lista negra los sitios: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Este perfil se enlazó a la política del proxy, bloqueando el acceso a dichos dominios.

2.5.3 RESULTADOS

Las pruebas demostraron conectividad correcta hacia Internet mediante NAT a través de la interfaz RED. Sin la configuración del proxy en el navegador, el tráfico fue bloqueado, mientras que con autenticación válida el acceso se permitió excepto para los dominios en lista negra.

3 CONCLUSIONES

La implementación de la Temática 1 permitió consolidar correctamente la configuración inicial del entorno de seguridad perimetral mediante la instalación y puesta en marcha de GNU/Linux Endian Firewall en VirtualBox. A través de la creación de la máquina virtual, la asignación de 2048 MB de RAM y 1 CPU, y la configuración precisa de los tres adaptadores de red, se logró establecer la segmentación requerida en las zonas Green (LAN), Orange (DMZ) y Red (WAN). Las pruebas de conectividad realizadas entre las máquinas evidenciaron el funcionamiento adecuado del enrutamiento interno, así como la aplicación de las políticas predeterminadas que inicialmente bloqueaban el tráfico entre

zonas. La activación de la regla ICMP demostró la capacidad del firewall para gestionar y controlar el flujo de paquetes de manera granular. Adicionalmente, el acceso exitoso al panel web y la obtención de conectividad WAN confirmaron que Endian opera correctamente como punto central de administración y salida a Internet. En conjunto, la configuración realizada cumple totalmente con los objetivos planteados y establece una base funcional, estable y segura para el desarrollo de temáticas posteriores relacionadas con NAT, reglas avanzadas y servicios perimetrales.

La configuración de reglas NAT en Endian permitió comprender de forma práctica como se controla y gestiona el tráfico desde zonas internas, hacia la red externa por medio de políticas de traducción de direcciones. Tanto en la red "Verde", como en la DMZ se lograron conexiones seguras y supervisadas, cumpliendo de este modo los objetivos del ejercicio. Ya que, gracias a las actividades desarrolladas, nos permitieron reforzar el entendimiento del Rol del firewall dentro de una infraestructura real, destacando así la importación de aplicar configuraciones adecuadas para poder garantizar la protección de la red y el flujo regulado de la información.

La Temática 3 permitió evidenciar el valor de establecer controles estrictos sobre los servicios expuestos en una zona DMZ, asegurando que solo el tráfico necesario sea autorizado. El uso de reglas específicas en el firewall mostró cómo una adecuada administración puede equilibrar accesibilidad y seguridad sin comprometer la integridad del entorno.

Las pruebas realizadas confirmaron la importancia de validar las configuraciones mediante herramientas de diagnóstico, ya que permiten observar de forma directa el comportamiento del tráfico entre zonas. También quedó demostrado que la restricción de protocolos como ICMP contribuye a reducir la superficie de exposición, fortaleciendo la protección del servidor sin afectar la operación de los servicios legítimos.

Las reglas HTTP y FTP son esenciales para controlar tráfico en entornos segmentados.

NAT permite publicar servicios internos de forma segura.

Endian Firewall es eficaz para seguridad perimetral en entornos virtualizados.

El uso de Endian Firewall 3.3 permitió comprender de manera práctica conceptos de seguridad perimetral, zonas de red, ruteo, proxy y filtrado de contenido. La virtualización con VirtualBox facilitó replicar escenarios reales sin costos adicionales.

4 REFERENCIAS

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

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

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

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

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

[6] CCNA. (2023). Configuración de la NAT [En línea]. CCNA. https://ccnadesdecero.es/configuracion-nat-estatica-dinamica-pat/

[7] Fortinet. (2020). Redes DMZ [En línea]. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz