Endian Firewall: NAT, DMZ y Filtrado de Tráfico ICMP en GNU/Linux

Pierre Elías Álvarez Gutiérrez
e-mail: pealvarezg@unadvirtual.edu.co
Oscar Euclidez Rocha Gómez
e-mail: oerochag@unadvirtual.edu.co
Jaime Alejandro Becerra Salazar
e-mail: jabecerrasa@unadvirtual.edu.co

RESUMEN: *El presente trabajo describe la implementación de un firewall basado en GNU/Linux Endian Community sobre VirtualBox, configurando tres zonas de seguridad: LAN (verde), WAN (roja) y DMZ (naranja). Se establecen reglas de NAT para permitir la comunicación desde la LAN hacia la WAN y desde la DMZ hacia Internet, verificando el reenvío de puertos. Además, se permiten los servicios HTTP (puerto 80) y FTP (puerto 21) desde un servidor Ubuntu Server en la DMZ, mientras se deniega explícitamente el protocolo ICMP (tipos 8 y 30) para bloquear el comando ping en toda la red. Finalmente, se verifica desde la terminal la ausencia de respuesta al comando ping y se documenta la creación de reglas en el tráfico de salida.*

PALABRAS CLAVE: Endian Firewall, NAT, DMZ, zonas de seguridad, ICMP, VirtualBox

ABSTRACT: *This paper describes the implementation of a firewall based on GNU/Linux Endian Community running on VirtualBox, configuring three security zones: LAN (green), WAN (red) and DMZ (orange). NAT rules are established to allow communication from the LAN to the WAN and from the DMZ to the Internet, with port forwarding verified. Furthermore, HTTP (port 80) and FTP (port 21) services are permitted from an Ubuntu Server in the DMZ, whilst the ICMP protocol (ports 8 and 30) is explicitly denied to block the ping command across the entire network. Finally, the lack of response to ping is verified via the terminal and the creation of rules for outbound traffic is documented.*

KEYWORDS: Endian Firewall, NAT, DMZ, security zones, ICMP, VirtualBox

1 INTRODUCCIÓN

La seguridad perimetral en redes de computadoras es un componente fundamental para proteger los activos de información de una organización [1]. Los firewalls de código abierto, como GNU/Linux Endian Community, ofrecen una solución accesible y robusta para implementar políticas de control de tráfico.

El objetivo de este trabajo consiste en instalar y configurar un firewall Endian en VirtualBox con tres zonas de seguridad: verde (LAN), roja (WAN) y naranja (DMZ). Posteriormente, se establecen reglas NAT para permitir comunicación hacia Internet y reglas de filtrado para habilitar servicios específicos (HTTP y FTP) mientras se bloquea el protocolo ICMP.

El presente informe documenta el desarrollo de la Temática 1 correspondiente a la Etapa 7 del Diplomado de Profundización en Administración de Sistemas Operativos Open Source. La actividad consistió en la configuración e instalación de la distribución GNU/Linux Endian Firewall Community (EFW) versión 3.3.2 dentro de un entorno virtualizado con Oracle VirtualBox, estableciendo una infraestructura de red con tres zonas de seguridad claramente diferenciadas: Zona Verde (LAN), Zona Naranja (DMZ) y Zona Roja (WAN).

Para el desarrollo de esta práctica se emplearon tres máquinas virtuales: Pierre Alvarez (estación de trabajo cliente en la Zona Verde), Ubuntu Server (servidor web Apache en la Zona Naranja/DMZ) y Endian (firewall perimetral). La conectividad entre estas máquinas se gestionó a través de redes internas configuradas en VirtualBox, permitiendo simular una arquitectura de forma realista de red empresarial segura.

Se documentan de forma detallada cada uno de los pasos ejecutados, desde la creación de la máquina virtual para Endian, la configuración de sus adaptadores de red, el proceso de instalación del sistema operativo, la asignación de direccionamiento IP por zonas, hasta la verificación de conectividad entre las máquinas del entorno.

Este documento se estructura de la siguiente manera: la Sección II detalla las características generales del formato IEEE aplicadas; la Sección III describe la implementación de las zonas en VirtualBox; la Sección IV presenta la configuración NAT; la Sección V muestra el filtrado de servicios y bloqueo ICMP; finalmente, la Sección VI expone las conclusiones.

2. CARACTERÍSTICAS GENERALES

El presente trabajo sigue los lineamientos de formato establecidos por el Institute of Electrical and Electronics Engineers (IEEE) para conferencias y revistas técnicas [2]. En la Tabla I se resumen los parámetros aplicados.

3. TEMÁTICA 1 – CONFIGURACIÓN DE INSTANCIA ENDIAN EN VIRTUALBOX

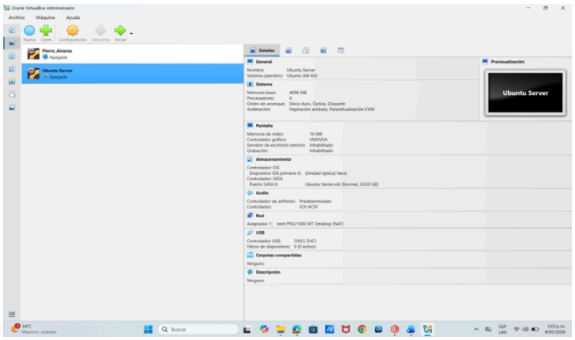
Se crea una máquina virtual en VirtualBox 7.0 con las siguientes especificaciones:

Nombre: Endian Firewall
Sistema operativo: Linux / Red Hat (64 bits)
RAM: 2048 MB
Disco duro: 20 GB VDI
Red: 3 adaptadores configurados como se indica en la Tabla II.

3.1 ENTORNO INICIAL DE VIRTUALBOX

Instalación de Endian a través de la máquina virtual, se realizan los pasos de acuerdo con la guía de actividad, desde la ilustración 1 hasta la 26 se documenta la instalación de Endian

Figura 1.
Pantalla de inicio de Virtual Box con el PC.



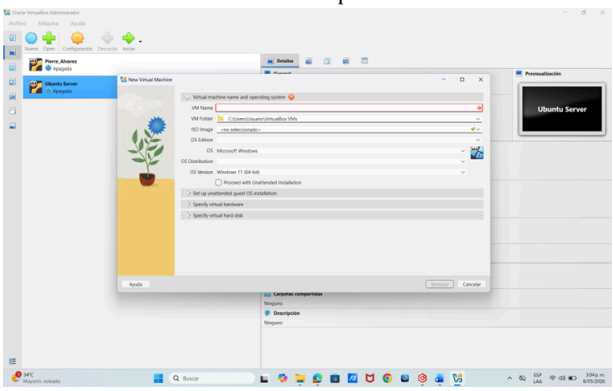
Fuente: Autoría Propia

Antes de iniciar la instalación de Endian, se verificó el estado del entorno de virtualización. Se contaba con dos máquinas virtuales preexistentes: Pierre Alvarez, correspondiente a la estación de trabajo cliente con sistema Ubuntu Desktop, y Ubuntu Server, el servidor que alojaría los servicios web en la zona DMZ. Ambas máquinas se encontraban apagadas, listas para integrar la nueva infraestructura de red una vez configurado el firewall.

3.2. CREACIÓN DE LA MÁQUINA VIRTUAL EN ENDIAN

Se procedió a crear una nueva máquina virtual desde el asistente de VirtualBox. Se accedió a la opción "Nueva" y se completó el formulario indicando el nombre de la VM, la carpeta de destino (C:\Users\Usuario\VirtualBox VMs) y el tipo de sistema operativo. El asistente presenta campos para el nombre de la VM, la imagen ISO fuente, la edición del sistema operativo y la versión. En este punto se configuró el sistema para instalar Endian, que corre sobre un kernel Linux de 64 bits.

Figura 2.
Asistente de creación de nueva máquina virtual en VirtualBox.



Fuente: Autoría Propia

En el paso de configuración del disco duro virtual se seleccionó la opción de crear un nuevo disco duro VDI (VirtualBox Disk Image) con un tamaño de 10 GB, suficiente para el sistema operativo Endian y sus logs de seguridad. Se dejó desmarcada la opción de reserva completa para optimizar el espacio en disco del anfitrión. La ruta del archivo quedó configurada como C:\Users\Usuario\VirtualBox VMs\Endian\Endian.vdi.

3.3. CONFIGURACIÓN DE LOS ADAPTADORES DE RED EN ENDIAN

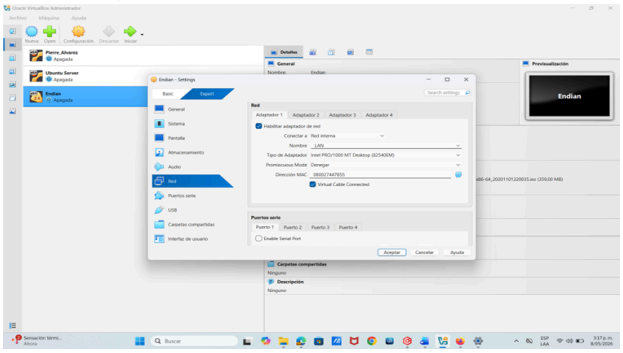
Una vez creada la máquina virtual, se procedió a configurar sus adaptadores de red desde la sección "Configuración > Red" de VirtualBox. La correcta asignación de las interfaces es crítica para que Endian pueda segmentar el tráfico entre las tres zonas de seguridad. Se configuraron tres adaptadores independientes, cada uno asociado a una red interna diferente o a NAT según corresponda.

El Adaptador 1 se configuró como Red Interna con el nombre "LAN". Esta interfaz corresponde a la Zona Verde de Endian, que es la red local interna donde se conectan las estaciones de trabajo de los usuarios. La opción "Virtual Cable Connected" se dejó habilitada para asegurar la conectividad virtual.

El Adaptador 2 se configuró como Red Interna con el nombre "DMZ". Esta interfaz representa la Zona Naranja de Endian, destinada a alojar los servidores que deben ser

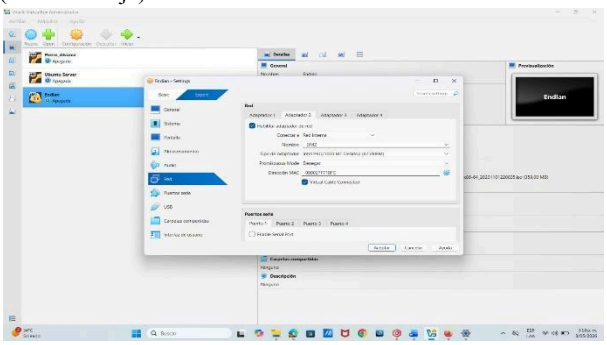
accesibles tanto desde la LAN como potencialmente desde Internet, pero bajo control estricto del firewall.

Figura 3.
Adaptador 1 de Endian Configurado como Red Interna LAN (Zona Verde).



Fuente: Autoría propia

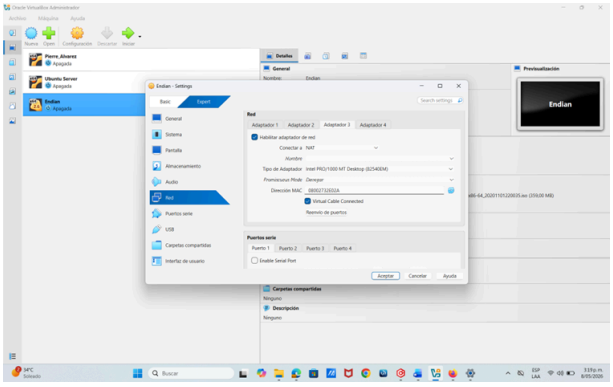
Figura 4.
Adaptador 2 de Endian Configurado como Red Interna DMZ (Zona Naranja).



Fuente: Autoría propia

El Adaptador 3 se configuró en modo NAT, lo que permite que Endian simule una conexión a Internet a través del adaptador de red del equipo anfitrión. Esta interfaz corresponde a la Zona Roja o WAN de Endian. VirtualBox actúa como el router NAT, proporcionando conectividad hacia el exterior simulada.

Figura 5.
Adaptador 3 de Endian Configurado como NAT para la Zona Roja (WAN).



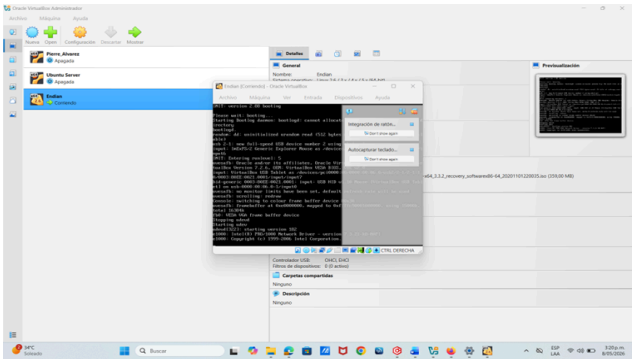
Fuente: Autoría propia

Con los tres adaptadores configurados, la vista de detalles de la máquina virtual Endian muestra el resumen completo de la configuración de red: Adaptador 1 conectado a Red Interna "LAN", Adaptador 2 a Red Interna "DMZ" y Adaptador 3 en modo NAT. El sistema operativo reconocido es Linux 2.6/3.x/4.x/5.x de 64 bits, con 4096 MB de RAM, 4 procesadores y disco de 10GB.

3.4. PROCESO DE INSTALACIÓN DE ENDIAN FIREWALL

Se inició la máquina virtual Endian con la imagen ISO community_community-x64_3.3.2_recovery_softwarex86-64_20201101220035.iso montada en la unidad óptica. Al arrancar, el sistema mostró los mensajes de inicialización del kernel Linux, incluyendo la detección del hardware del sistema: procesador AMD Ryzen 7 7730U, inicialización de los controladores de red Intel PRO/1000 para las tres interfaces y carga de módulos del sistema. Se presentaron también los cuadros de diálogo de integración de ratón y captura de teclado de VirtualBox.

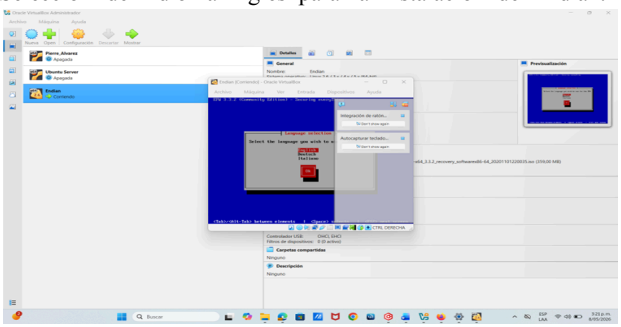
Figura 6.
Arranque inicial de Endian con mensajes de iniciación del Kernel de Linux.



Fuente: Autoría propia

Una vez completada la carga inicial, el instalador presentó la pantalla de selección de idioma. Se seleccionó el idioma English para el proceso de instalación, que es el idioma usado. Se confirmó la selección con el botón Ok para continuar con el proceso de instalación.

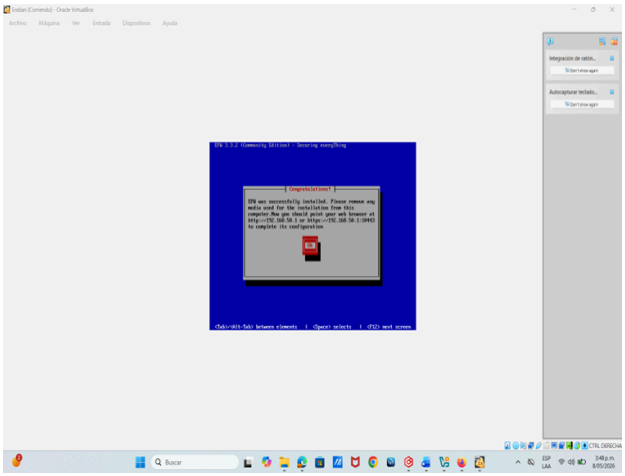
Figura 7.
Selección del Idioma inglés para la instalación de Endian.



Fuente: Autoría propia

El instalador presentó la pantalla de bienvenida (¡Welcome!) informando que el programa de instalación de EFW comenzaría el proceso. Se advierte que seleccionar Cancel en cualquier pantalla posterior reiniciará el equipo. Se confirmó con Ok para proceder con la instalación del firewall.

Figura 8.
Confirmación de Instalación Exitosa de Endian

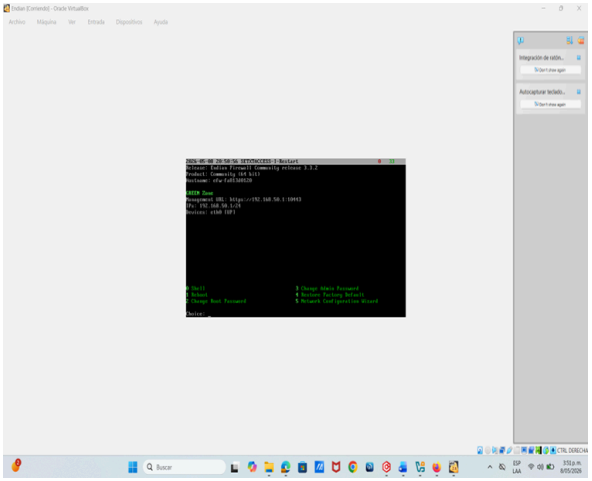


Fuente: Autoría propia

Tras retirar la imagen ISO y reiniciar la máquina virtual, Endian arrancó desde el disco duro por primera vez. La pantalla mostró los mensajes de inicialización del kernel Linux con la detección del hardware: procesador AMD Ryzen 7 7730U con 4 núcleos físicos activados (15930.80 BogoMIPS), inicialización de los buses PCI, tabla de hash futex, y los controladores de red Intel PRO/1000 para las tres interfaces eth0, eth1 y eth2.

Una vez completado el arranque, Endian presentó su menú de administración por consola. Se mostró el resumen de la configuración de la Zona Verde: IP de gestión 192.168.50.1/24 asignada a la interfaz eth0, la URL de administración web y el estado de la interfaz.

Figura 9.
Menú de administración de Endian Firewall.



Fuente: Autoría propia

Se accedió al Network Configuration Wizard (opción 5 del menú) para configurar todas las interfaces de red. La pantalla mostró el resumen actual de la configuración: Zona GREEN con IP 192.168.50.1/24, interfaz RED sin IP asignada aún, y las tres interfaces de red disponibles: eth0, eth1 y eth2. Se configuró el tipo de interfaz RED como DHCP para que tome IP automática del NAT de VirtualBox.

Durante la configuración del Network Configuration Wizard se establecieron los parámetros de la Zona Roja (RED/WAN). Se seleccionó eth2 como dispositivo RED, se ingresó la IP estática 176.32.56.241/30 con gateway 176.32.56.240, DNS primario 8.8.8.8 y secundario 8.8.4.4. La Zona Verde quedó con eth0 en 192.168.50.1/24 con DHCP habilitado. A continuación, se configuró la Zona Naranja (ORANGE) con eth1 y se solicitó la IP para esa interfaz.

Al finalizar la configuración de todas las zonas, el asistente mostró un resumen completo de los parámetros que se aplicarían: hostname Endian, dominio localdomain, RED en eth2 con IP estática 176.32.56.241/30 y gateway 176.32.56.240, DNS 8.8.8.8/8.8.4.4, GREEN en eth0 con 192.168.50.1/24 y DHCP habilitado, ORANGE en eth1 con 10.21.10.1/29. Se solicita confirmación antes de escribir la configuración.

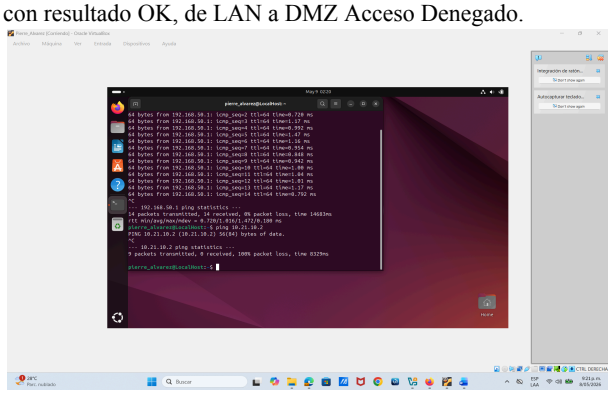
3.5. VERIFICACIÓN DE CONECTIVIDAD ENTRE ZONAS

Una vez configurado el firewall Endian, se procedió a verificar la conectividad entre las máquinas del entorno. Desde Ubuntu Server (en la Zona DMZ con IP 10.21.10.2/29) se ejecutó el comando ping hacia la IP 10.21.10.1, que corresponde a la interfaz ORANGE de Endian. Los resultados mostraron 12 paquetes transmitidos y 12 recibidos con 0% de pérdida, tiempos de respuesta de entre 0.944 ms y 2.190 ms, confirmando la comunicación exitosa entre el servidor y el gateway de la DMZ.

Adicionalmente se intentó hacer ping desde Ubuntu Server hacia la IP 192.168.50.2 (Zona Verde), obteniendo el mensaje "ping: connect: Network is unreachable". Este comportamiento es el esperado y correcto, ya que el firewall Endian controla el tráfico inter-zona y no permite por defecto que la DMZ acceda directamente a la LAN sin reglas explícitas de firewall. Esto confirma que la segmentación de red está funcionando correctamente.

Desde la estación de trabajo Pierre Alvarez (Ubuntu Desktop en la Zona Verde) se verificó la conectividad hacia la interfaz GREEN de Endian (192.168.50.1). El ping mostró 14 paquetes transmitidos y 14 recibidos con 0% de pérdida y tiempos de respuesta entre 0.720 ms y 1.472 ms. Posteriormente se intentó ping hacia 10.21.10.2 (Ubuntu Server en DMZ), obteniendo 100% de pérdida de paquetes, lo cual confirma que las políticas de seguridad inter-zona de Endian están activas y requieren configuración explícita para permitir ese tráfico.

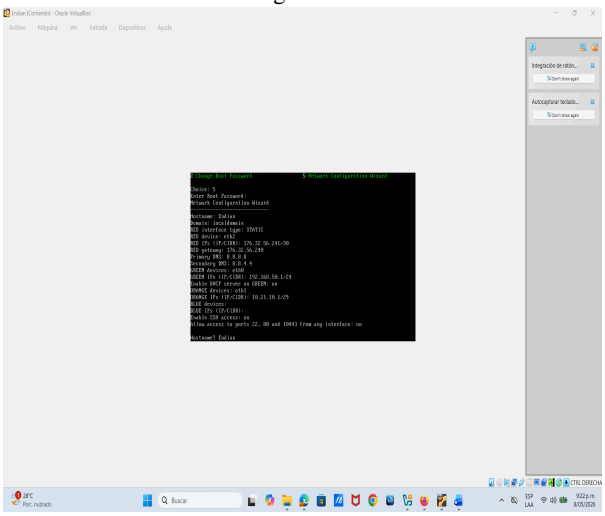
Figura 10.
Prueba de conectividad de Ubuntu Desktop con LAN a Endian con resultado OK, de LAN a DMZ Acceso Denegado.



Fuente: Autoría propia

Finalmente, al acceder nuevamente al Network Configuration Wizard de Endian (opción 5 del menú de consola), se verificó la configuración definitiva aplicada al sistema. El resumen confirmó: RED en eth2 con IP 176.32.56.241/30, gateway 176.32.56.240, DNS 8.8.8.8/8.8.4.4, GREEN en eth0 con 192.168.50.1/24, ORANGE en eth1 con 10.21.10.1/29, SSHhabilitado y puertos 22, 80 y 10443 accesibles desde cualquier interfaz.

Figura 11.
Verificación final de la configuración de red de Endian.



Fuente: Autoría propia

4. TEMÁTICA 2: CONFIGURACIÓN NAT.

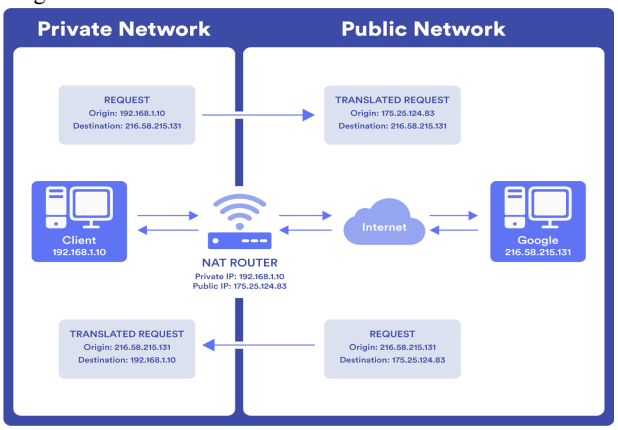
Para el desarrollo de esta actividad primero conozcamos un poco acerca de que es NAT.

Para acceder a Internet, se necesita una dirección IP pública, aunque también podemos usar una dirección IP privada en nuestra propia red privada. Esto se logra a través la traducción de una dirección IP privada a una dirección IP pública, apoyándonos en un traductor de direcciones de IP o Network Address Translator (NAT).

4.1. FUNCIONAMIENTO DE NAT

Su función es la de permitir que múltiples dispositivos (PC, tablet, laptop, celulares, servidores, etc.) accedan a Internet a través de una misma dirección pública mediante la traducción de un conjunto de direcciones IP, por lo general internas, para que sean comprendidos por otro conjunto de direcciones, por lo general externas (Internet) y viceversa.

Figura 12.
Diagrama de funcionamiento de NAT



Fuente: Tomado de https:/pandorafms.com/es/it-topics/que-es-nat

Con esto, vemos que NAT realiza dos funciones básicas: la asignación de una o múltiples direcciones IP públicas para la red local y la simplificación del direccionamiento mediante el enmascaramiento de direcciones IP privadas.

4.2. TIPOS DE NAT

Por su configuración, existen tres diferentes tipos de NAT con distintas funciones:

4.2.1. NAT ESTÁTICA

Donde se establece una asociación fija y permanente entre una dirección IP privada en la red local y una dirección IP pública específica. Generalmente se usa para hosting de web, no para organizaciones donde hay múltiples dispositivos porque cada dispositivo demandaría una dirección pública, lo que resultaría muy costoso y difícil de gestionar.

4.2.2. NAT DINÁMICA

Donde se establece un conjunto de direcciones IP públicas disponibles para que un dispositivo de la red local solicite acceso a Internet y esta le asigne temporalmente una dirección IP pública disponible. En caso de que la dirección IP del grupo no esté libre, el paquete se descarta, ya que solo un número fijo de direcciones IP privadas se pueden traducir a direcciones públicas. Entendiendo esto, este tipo de NAT puede ser también muy costoso ya que la organización tiene que comprar muchas direcciones IP globales para crear un grupo.

4.2.3. NAT PAT

Port (Address Translation) donde se establece una asociación entre los dispositivos de red local y una única IP pública, diferenciando en cada dispositivo un puerto que se le asigna para recibir el tráfico de red correspondiente para cada dispositivo. PAT busca conservar el puerto de origen inicial.

En caso de que el puerto de origen inicial ya esté en uso, se asigna el siguiente puerto disponible, en un proceso continuo, hasta que no haya más direcciones IP externas o puertos disponibles.

4.3. SEGURIDAD NAT

Actualmente, muchos ingenieros de redes recurren al uso de NAT para proteger a sus dispositivos en la red de los ataques cibernéticos, ya que actúa como una capa adicional de seguridad entre los dispositivos de una red privada e Internet.

Esto es porque el enrutador NAT o firewall NAT pueden ordenar y verificar los datos a medida que se envían a un dispositivo, ocultando direcciones IP internas, dejándolas inaccesibles desde Internet. Esto puede ayudar a evitar ataques como escaneos de puertos, que permiten identificar vulnerabilidades en los dispositivos de la red.

También NAT permite la integración con firewalls de los routers y de los propios dispositivos de la red, mejorando la implementación de políticas de seguridad.

Otro aspecto importante de la seguridad es que NAT contribuye a prevenir el agotamiento de las direcciones IP públicas, ya que el uso de una única dirección IP pública para varios dispositivos en una red también ayuda a garantizar que la asignación de IP públicas sea lo más eficiente posible.

Cabe mencionar que las direcciones privadas no pueden garantizar una seguridad total. Sin duda, también deberías utilizar cifrado y otras herramientas de seguridad. También se debe mantener los dispositivos en una dirección IP local como una buena medida de seguridad adicional.

4.4. VENTAJAS Y DESVENTAJAS DE LAS NAT

Entre las ventajas de las NAT tenemos lo siguiente:

- NAT proporciona una capa de seguridad en la red, ya que las redes privadas no anuncian sus direcciones ni su topología interna, de manera que son seguras al tener controlado el acceso externo, aunque no reemplaza a los firewalls.

- Aumenta la flexibilidad de las conexiones a la red pública, además de compatibilidad con Protocolos de Internet Versión 4 (IPv4). Se pueden implementar conjuntos y conjuntos de respaldo/ equilibrio de carga para asegurar conexiones de red pública confiables.

- En caso de sobrecarga, los hosts internos pueden compartir una única dirección IPv4 pública para todas las comunicaciones externas. Se requieren muy pocas direcciones externas para admitir varios hosts internos, lo que también implica menos gestión y costos.

- Coherencia con los esquemas de direccionamiento de red interna. Si se quiere cambiar el esquema de direcciones IPv4 públicas en una red sin direcciones IPv4 privadas ni NAT, se deben redireccionar todos los hosts en la red existente. NAT permite conservar las direcciones IPv4 privadas, a la vez que agiliza el cambio a un nuevo esquema de direccionamiento público.

La otra cara de la moneda, son las desventajas partiendo de que los hosts en Internet se comunican con el dispositivo con NAT y no con el host real, lo que implica:

- Aumento de retraso o latencia en la comunicación de red, ya que la traducción de cada dirección IPv4 en los encabezados del paquete de datos toma su tiempo.

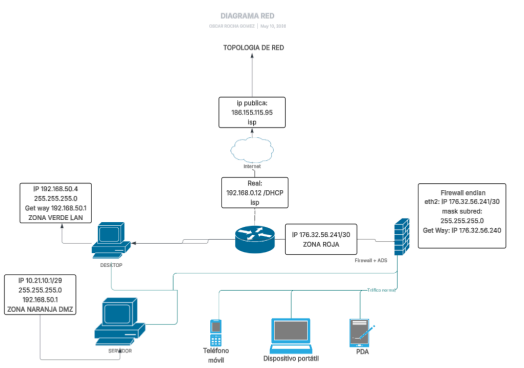
- Posible deterioro en la funcionalidad de punta a punta. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento, desde el origen hasta el destino. Por ejemplo, algunas aplicaciones de seguridad (firma digital) fallan porque la dirección IPv4 de origen ha cambiado antes de alcanzar su destino.

- Pérdida de trazabilidad IPv4 a la hora de rastrear paquetes en la red. Esto es porque los paquetes pasan por varios cambios de dirección en varios saltos de NAT, dificultando su seguimiento. Esto impacta en la resolución de problemas.

- Mayor complejidad en configuración y mantenimiento, principalmente a la hora de establecer reglas de traducción de direcciones IP y puertos para aplicaciones específicas. Por ejemplo, NAT modifica los valores en los encabezados que interfieren en las verificaciones de integridad realizadas por IPsec y otros protocolos de tunneling.

- Posibles interrupciones en conexiones de Protocolo de Control de Transmisión (Transmission Control Protocol, TCP). Los servicios que requieren una conexión TCP desde una red externa o “protocolos” sin estado pueden interrumpirse. A menos que el router NAT esté configurado para admitir estos protocolos, los paquetes entrantes podrían no llegar a su destino.

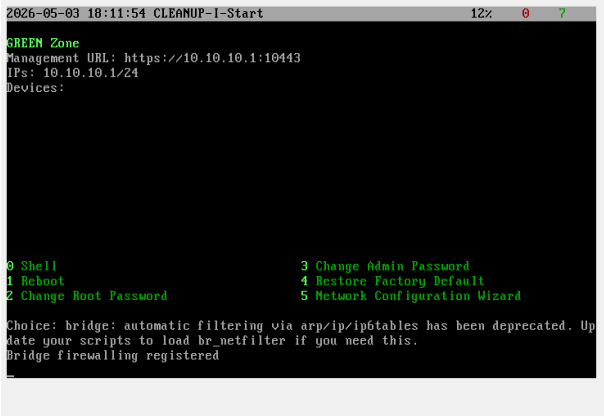
Figura 13.
Topología de la red.



Fuente: Autoría propia

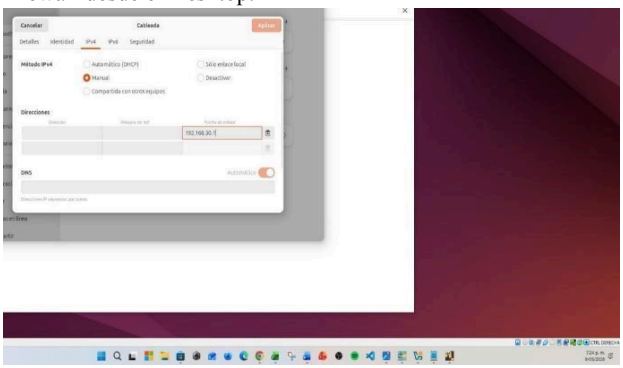
Establecemos la comunicación entre las diferentes Mv de VirtualBox tales como: Desktop Mv Oracle VirtualBox.

Figura 14.
Pantalla de inicio de Endian Firewall con opciones de configuración.



Fuente: Autoría propia

Figura 15.
Acceso a la interfaz gráfica de administración de Endian Firewall desde el Desktop.



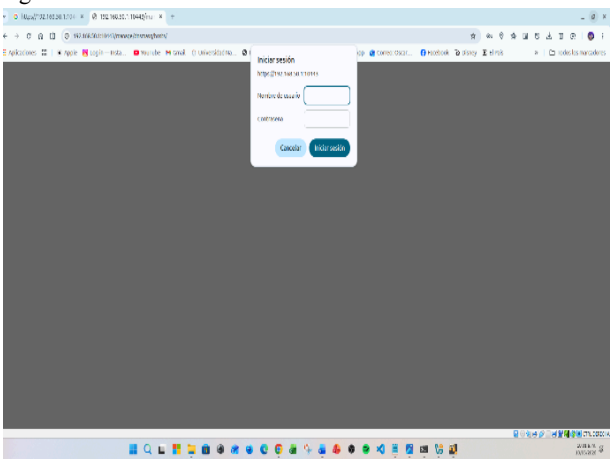
Fuente: Autoría propia

Realizamos la Configuración de los diferentes adaptadores para poder permitir la conectividad con el firewall y realizar el tráfico de datos de nuestra red virtual.

En la imagen podemos observar la configuración de los diferentes adaptadores desde el firewall de endian. Para que exista comunicación entre las 2 máquinas virtuales y el firewall.

A través de firewall de endian accedemos a la consola grafica para realizar e implementar las diferentes reglas para la temática de NAT. Implementamos las reglas desde entorno grafico accediendo desde El Desktop con la ip 192.168.50.1:10443

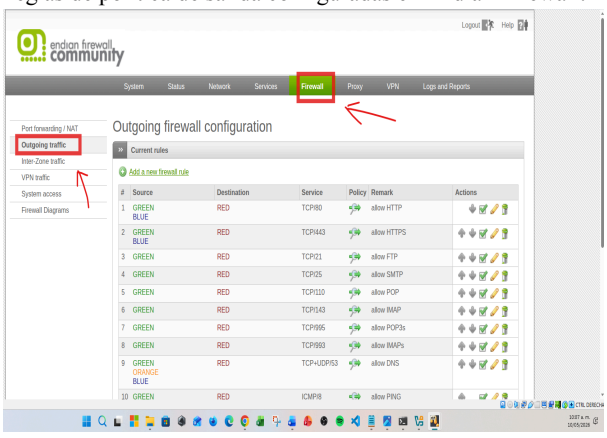
Figura 16.
Ingreso de credenciales de administrador en Endian Firewall.



Fuente: Autoría propia

4.5. PRIMERA REGLA

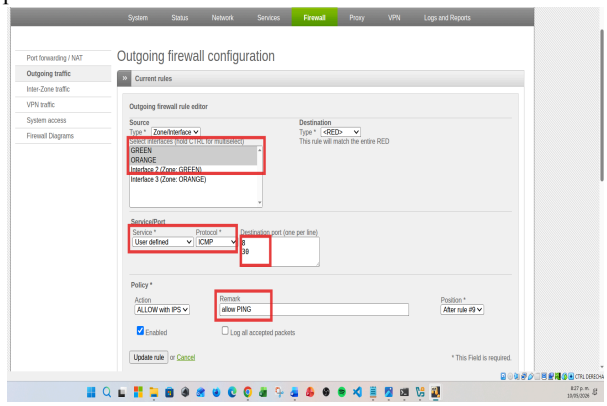
Figura 17.
Reglas de política de salida configuradas en Endian Firewall.



Fuente: Autoría propia

Hacia el icmp LAN y el DMZ para permitirles tener salida hacia internet la creamos el tráfico de datos hacia estas redes y le hacemos ping.

Figura 18.
Regla Outgoing traffic en Endian Firewall para permitir protocolo ICMP.



Fuente: Autoría propia

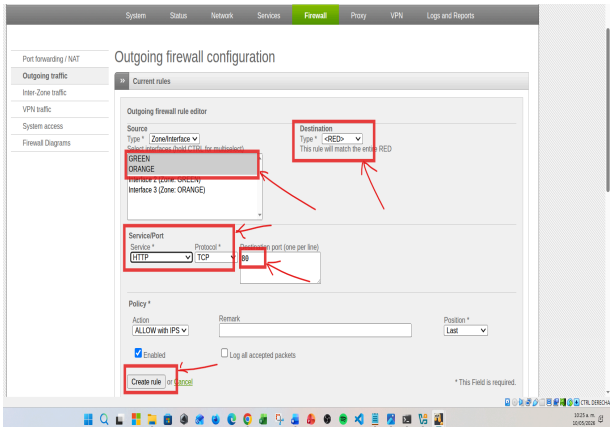
4.5.1. SEGUNDA REGLA

La segunda regla es darle permisos al ICMP para que tenga salida a internet y poder hacerle ping y que responda a esa dirección ip o las direcciones que nosotros configuremos en el firewall. Seleccionamos Green y Orange. De igual forma en el destino la salida que es red servicie puerto cualquier y lo mismo con el protocolo y damos en crear.

4.5.2. TERCERA REGLA

Se otorgaron permisos a la red para que puedan tener salida por HTTP por el puerto 80

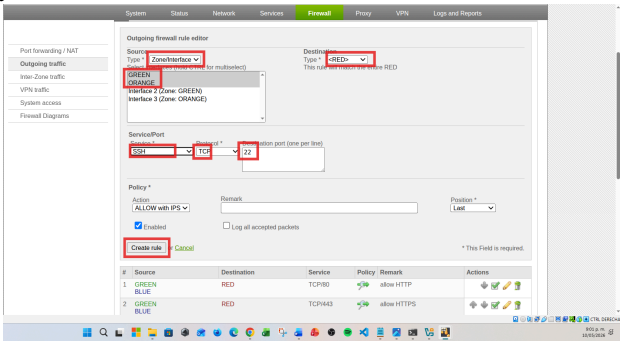
Figura 19.
Regla de firewall en Endian para tráfico TCP con política ALLOW.



Fuente: Autoría propia

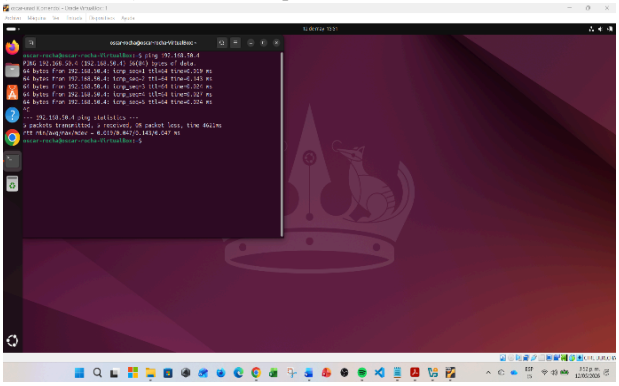
Activamos los diferentes servicios que tenemos para otorgar los servicios de red diferentes puertos para que algunos servicios como por ejemplo ISP que utiliza el Puerto 8080. De igual forma activamos o aprobamos los servicios SSh para poder utilizar este servicio a través del puerto 22.

Figura 20.
Reglas Outgoing traffic en Endian Firewall para servicios SSH y HTTP.



Fuente: Autoría propia

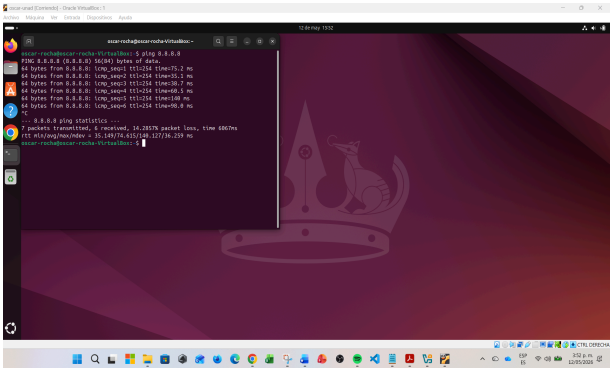
Figura 21.
Prueba de conectividad mediante ping desde el Desktop (192.168.50.4) hacia otra máquina en la red.



Fuente: Autoría propia

Validamos la conexión a través del ping y realizamos si existe la comunicación entre las máquinas virtuales con el ping: 192.168.50.4 que es nuestro desktop.

Figura 22.
Prueba de conectividad a internet mediante ping a 8.8.8.8 (Google DNS) confirmando salida a la WAN.



Fuente: Autoría propia

Validamos que exista salida de internet y realizamos un ping a los DNS de google.com 8.8.8.8, como podemos observar en la imagen tenemos respuesta hacia la dirección y al DNS.

4.5.3. CONCLUSIÓN DE NAT

En conclusión, NAT desempeña un papel importante en la conectividad actual de las redes informáticas, especialmente en entornos IPv4, donde las direcciones IP públicas son limitadas.

Es importante que los estrategas de seguridad deben también tomar en cuenta sus consideraciones y posibles desventajas en cuanto a latencia y trazabilidad.

En ese sentido, se requiere la correcta configuración y mantenimiento de protocolos y puerto para lograr que las IP públicas estén disponibles para su uso y entrega de servicios, al mismo tiempo que se ahorra dinero y se agrega una capa adicional de seguridad, que además refuerza las políticas de seguridad integrando firewalls de routers y dispositivos.

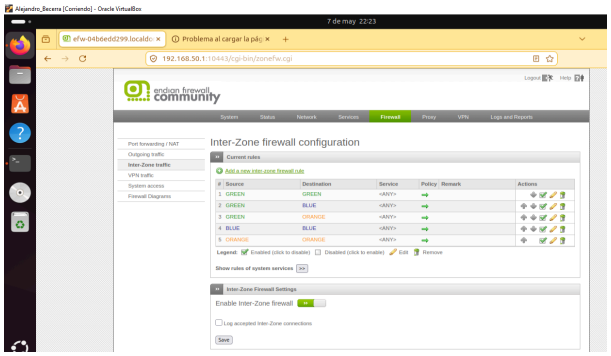
5. TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ

Para dar cumplimiento a los productos esperados de la Temática 3, se configuraron reglas de filtrado en Endian Firewall con el objetivo de permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde la zona DMZ hacia la zona LAN, y denegar el protocolo ICMP (ping) entre dichas zonas.

5.1 CONFIGURACIÓN DE REGLAS EN INTER-ZONE TRAFFIC

Las reglas de filtrado se crearon en la sección "Inter-Zone traffic" del panel de administración web de Endian. Se estableció una regla de **ACCEPT** para el tráfico TCP/80 desde la zona ORANGE (DMZ) hacia la zona GREEN (LAN), permitiendo el acceso al servidor web. Adicionalmente, se configuró una regla independiente de **DENY** para el protocolo ICMP, con el fin de bloquear cualquier intento de comunicación mediante el comando ping entre la DMZ y la LAN. La correcta activación de estas reglas se verificó en la interfaz gráfica, donde quedaron listadas con sus políticas asignadas *(Figura 23)*.

Figura 23.
Configuración de reglas entre zonas.

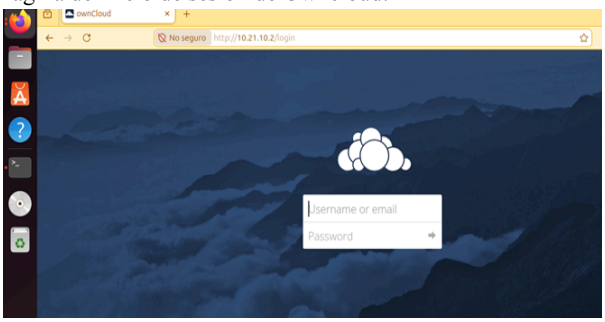


Fuente: Autoría propia

5.2. VERIFICACIÓN DEL SERVICIO HTTP

Para verificar la correcta habilitación del servicio HTTP, desde un equipo Ubuntu Desktop ubicado en la LAN (con IP 192.168.50.10) se accedió mediante un navegador web a la dirección http://10.21.10.2, correspondiente al servidor Owncloud-Final situado en la DMZ. Como resultado, la pantalla de login de Owncloud se cargó de manera exitosa (*Figura* 24), confirmando así que el tráfico HTTP en el puerto 80 está siendo permitido por la regla configurada en Endian. Este resultado valida el enrutamiento y filtrado correcto del protocolo de aplicación entre las zonas.

Figura 24.
Página de inicio de sesión de Owncloud.

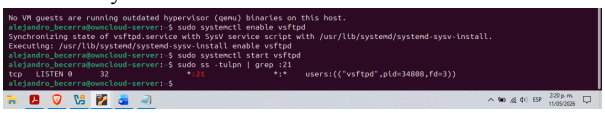


Fuente: Autoría propia

5.3. VERIFICACIÓN DEL SERVICIO FTP

Para el servicio FTP, se instaló y configuró el servidor vsftpd en la máquina Owncloud-Final. Posteriormente, desde la terminal del equipo Desktop se ejecutó el comando ftp 10.21.10.2. Tras ingresar las credenciales de usuario, la conexión fue exitosa, permitiendo listar los archivos del directorio remoto (*Figura* 25). Esta prueba demuestra que el puerto 21 está correctamente permitido para la comunicación desde la LAN hacia la DMZ, cumpliendo con el segundo objetivo de la temática.

Figura 25.
Instalación y verificación del servicio FTP.



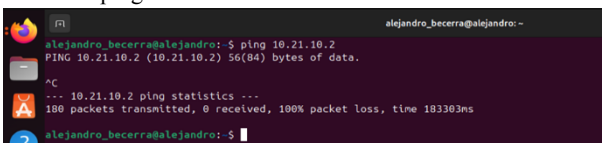
Fuente: Autoría propia

5.4. VERIFICACIÓN DEL BLOQUEO DE ICMP (PING)

Para comprobar el bloqueo de ICMP, se ejecutó el comando ping 10.21.10.2 desde la terminal del equipo Desktop. Como resultado, no se obtuvo respuesta alguna; tras la interrupción manual, el resumen mostró 0 packets received, 100% packet loss (*Figura* 26). Este resultado evidencia que el tráfico ICMP es efectivamente denegado por la regla DENY configurada en Endian. La efectividad del bloqueo se corroboró adicionalmente desde la consola del firewall mediante el comando iptables -L FORWARD -n -v, donde se observó una regla DROP para ICMP con contadores

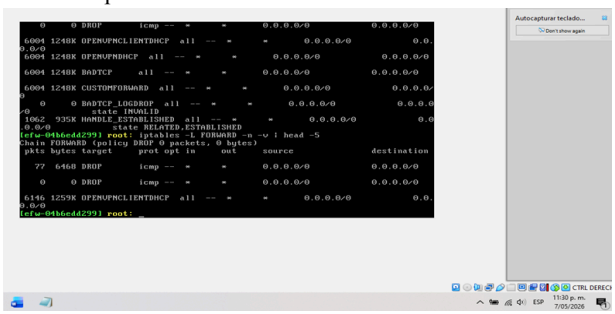
de paquetes (*Figura* 27), confirmando el procesamiento y descarte activo de los paquetes.

Figura 26.
Prueba de ping.



Fuente: Autoría propia

Figura 27.
Comando iptables.



Fuente: Autoría propia

5.5 ANÁLISIS DE RESULTADOS

Los resultados obtenidos validan plenamente la implementación de las políticas de seguridad. La correcta habilitación de servicios críticos (HTTP y FTP) asegura la funcionalidad requerida para el servidor en la DMZ, mientras que el bloqueo efectivo de ICMP refuerza la seguridad perimetral al impedir la exploración de red mediante ping. No se presentaron desviaciones significativas entre los resultados esperados y los obtenidos, demostrando la eficacia de Endian Firewall para gestionar el tráfico inter-zona basado en reglas específicas.

6. CONCLUSIONES

El desarrollo de la Etapa 7 permitió implementar y validar el funcionamiento de Endian Firewall Community como solución de seguridad perimetral en entorno virtualizado con VirtualBox. Se logró configurar las tres zonas de seguridad (LAN verde, WAN roja y DMZ naranja) con las direcciones IP 192.168.50.1/24 para GREEN, 10.21.10.1/29 para ORANGE y NAT para RED, estableciendo las bases para la comunicación entre las máquinas virtuales y la implementación de reglas de firewall.

En cuanto a la conectividad externa, se implementaron reglas NAT que permitieron la comunicación desde la LAN y desde la DMZ hacia Internet, verificada mediante pruebas de ping exitosas a 8.8.8.8, confirmando el correcto reenvío de puertos y la traducción de direcciones. Adicionalmente, se configuraron reglas de filtrado en la sección Inter-Zone traffic para permitir los servicios HTTP (puerto 80) y FTP (puerto 21) desde la DMZ hacia la LAN, y para denegar el protocolo ICMP (ping) entre estas zonas. Las pruebas realizadas desde el equipo Desktop (IP 192.168.50.10) confirmaron el acceso exitoso al servidor web Owncloud y al servicio FTP, mientras que el comando ping no obtuvo respuesta, demostrando la efectividad del bloqueo.

En síntesis, la combinación de zonas de seguridad, reglas NAT y filtrado de servicios en Endian Firewall Community permite diseñar arquitecturas de red seguras, controlar el acceso a Internet y proteger los servidores en la DMZ, demostrando que esta solución es robusta y accesible para implementar seguridad perimetral en entornos virtualizados, cumpliendo así con los objetivos planteados en la Etapa 7 del diplomado.

7. REFERENCIAS

[1] LPI LPIC-1 Exam 101. *Tema 102: Comandos GNU y Unix*. v. 101-500. s.l.: Linux Professional Institute, 2022. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Canonical. *Help Ubuntu*. v. 22.04. Londres, UK: Canonical Group, 2023. Disponible en: https://help.ubuntu.com/

[3] Debian. *El manual del administrador de Debian 12.5.0*. v. 12.5.0. s.l.: Debian, 2023. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle Corporation. *Oracle VM VirtualBox*, v. 7.0. Palo Alto, CA, USA: Oracle Corp., 2020. Disponible en: https://www.virtualbox.org/manual/

[5] Endian. *Endian UTM 3.2 Manual de referencia*. v. 3.2. Bolzano, Italia: Endian, 2016. Disponible en: http://docs.endian.com/3.2/utm/index.html

[6] LaCroix, J. *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*. 4th ed. Birmingham, UK: Packt Publishing, 2020. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952