ETAPA 7 IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Adrián Guevara Rodríguez
agurvarar@unadvirtual.edu.co
Lewis Flores Flaker
lflorezfla@unadvirtual.edu.co
Anderson Cristian Tulcan Bocanegra
actulcanb@unadvirtual.edu.co
Julian David Gamboa Roa
jdgamboaro@unadvirtual.edu.co

RESUMEN: *El presente artículo describe la implementación y configuración del firewall Endian sobre una máquina virtual en VirtualBox, estructurada en cinco ejes temáticos. En primer lugar, se define una arquitectura de red segmentada mediante las zonas verde (LAN), roja (WAN) y naranja (DMZ) , con el fin de reforzar la seguridad perimetral y optimizar la comunicación entre zonas.*

También en segundo lugar, se realiza la configuración de las reglas de SNAT y DNAT para permitir la publicación controlada de servicios internos, como servidores web alojados en la DMZ, sin comprometer la integridad de la red LAN. La tercera temática aborda la activación de servicios HTTP y FTP desde la DMZ hacia el resto de las zonas, junto con el bloqueo del protocolo ICMP como medida preventiva de seguridad.

A continuación, se definen reglas de acceso que filtran el tráfico en función de parámetros como dirección IP, puerto, interfaz y estado de la conexión, permitiendo un control granular del flujo de datos. Finalmente, se implementa un proxy HTTP no transparente con autenticación, que permite auditar y gestionar el acceso a internet mediante credenciales, reforzando así el control y la trazabilidad del tráfico web en la organización.

PALABRAS CLAVE: ICMP (Internet Control Message Protocol), SNAT (Source NAT), DNAT (Destination NAT), DMZ (Zona Desmilitarizada), NAT (Network Address Translation).

1 INTRODUCCIÓN

Desde finales de los años setenta, con el auge de Internet y el crecimiento continuo del desarrollo tecnológico, ha surgido la necesidad de proteger las comunicaciones y la información. En un entorno digital cada vez más expuesto a amenazas, son indispensables soluciones eficientes de seguridad para redes y dispositivos conectados.

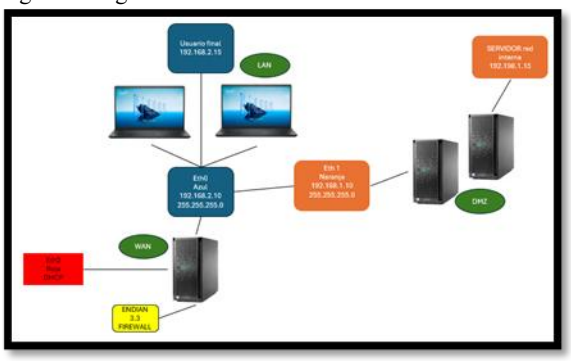
Endian Firewall, una distribución libre basada en Linux, ofrece una solución de seguridad unificada (UTM) para proteger, controlar y gestionar el tráfico en redes corporativas o domésticas. En este trabajo se presentan pautas para instalar y configurar Endian sobre una máquina virtual en VirtualBox, describiendo desde la creación de la máquina virtual hasta la configuración de interfaces de red, reglas de firewall, filtros de tráfico y herramientas de monitoreo. El objetivo es brindar los conocimientos necesarios para implementar una solución de seguridad, mejorar la visibilidad del tráfico y proteger la integridad de los sistemas y los datos asociados a la comunicación y los dispositivos conectados.

2 DESARROLLO DE ACTIVIDAD COLABORATIVA

2.1 INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ENDIAN (EFW)

Se realiza primero propuesta del diseño del diagrama de red que será utilizado para la configuración en zonas Naranja, Azul y roja en Endian 3.3.

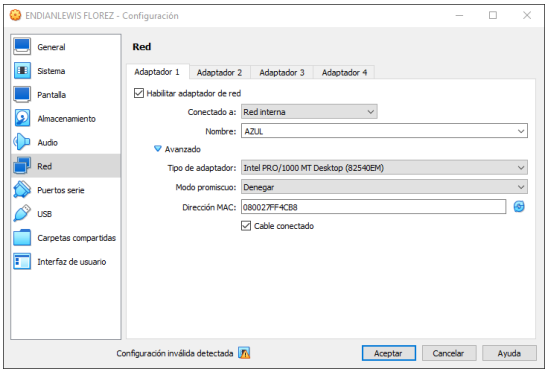
Figura 0 diagrama de red Endian



Fuente: autoría propia

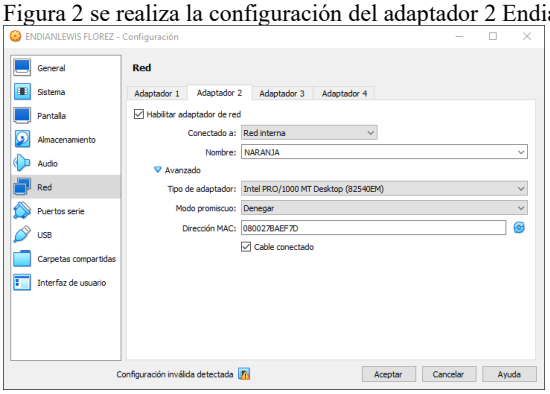
Se realizala descarga del Edian 3.3 desde la página oficial https://sourceforge.net/projects/efw/, a continuación, realizamos la instalación correspondiente en los sistemas operativos (Ubuntu Desktop Cliente, Ubuntu Server Servidor), utilizar para el desarrollo de la actividad. Iniciamos configurando las tarjetas de red. Adaptador 1, red interna y la llamo la red VERDE. Adaptador 2, red interna y la llamo la red NARANJADA. Adaptador 3, es el internet, lo dejo en NAT, vendría siendo la red ROJA.

Figura1 se realiza la configuración del adaptador Endia 3.3



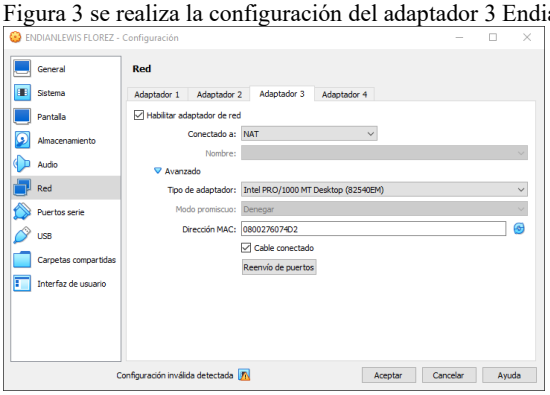
Fuente: autoría propia

Figura 2 se realiza la configuración del adaptador 2 Endia 3.3



Fuente: autoría propia

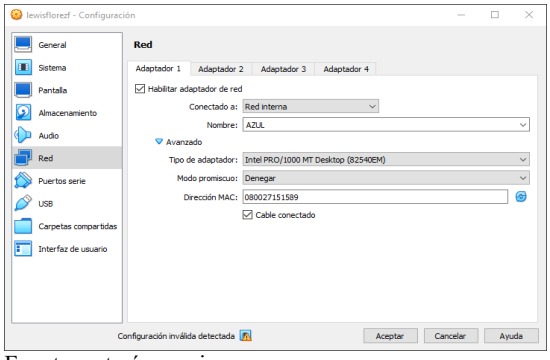
Figura 3 se realiza la configuración del adaptador 3 Endia 3.3



Fuente: autoría propia

Se realiza la configuración de la tarjeta de red en el cliente lewisflorez como adaptador 1, como red interna perteneciente a la red azul.

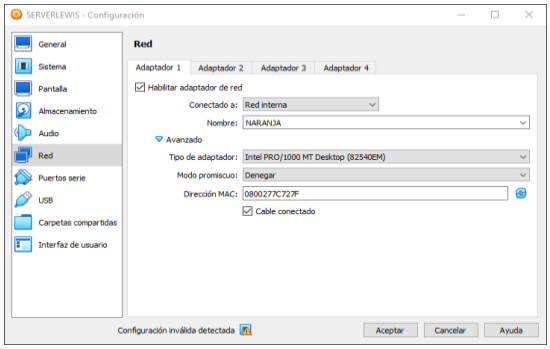
Figura 3 se realiza la configuración de adaptador 1 lewisflorezf



Fuente: autoría propia

Si realiza la configuración de la tarjeta del servidor SERVERLEWIS, donde utiliza la red Naranja

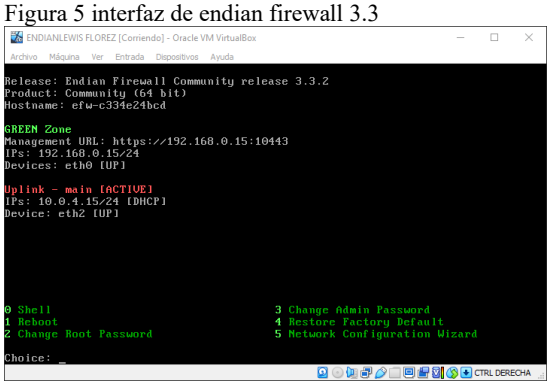
Figura 4 se realiza la configuración del adaptador 1 del SERVERLEWIS



Fuente: autoría propia

Instalacion de máquina virtual ENDIAN firewll network

Figura 5 interfaz de endian firewall 3.3



Fuente: autoría propia

Se tienen la culminación y configuración de Endia 3.3, ingresamos a la máquina virtual se abre el navegador del cliente lewisflorez, y escribimos la dirección ip como URL https:192.168.2.15 o la dirección IP, donde vemos reflejado un mensaje de alerta se deben aceptar los riesgo y continuamos.

2.2 TEMÁTICA 1: INSTALACIÓN Y CONFIGURACIÓN DE LA DISTRIBUCIÓN GNU/LINUX ENDIAN (EFW).

En esta práctica se realizó la implementación de un sistema de seguridad perimetral utilizando Endian Firewall Community sobre una máquina virtual en Oracle VM VirtualBox, con el objetivo de segmentar la red en tres zonas principales:

Zona verde (GREEN): Red interna o LAN
Zona roja (RED): Conexión a Internet (WAN)
Zona naranja (ORANGE): Zona desmilitarizada (DMZ)

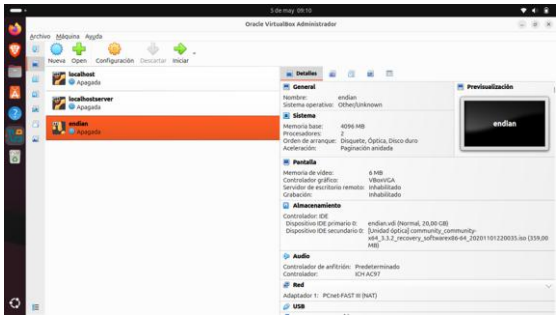
Esta arquitectura permite mejorar la seguridad, controlando el tráfico entre redes y protegiendo los recursos internos.

Creación de la máquina virtual

Se inició creando una nueva máquina virtual en VirtualBox con las siguientes características:

Nombre: Endian
Tipo: Linux
Versión: Other Linux (64-bit)
Memoria RAM: 4GB (mínimo recomendado)
Disco duro: 20 GB (dinámico)
Posteriormente, se cargó la imagen ISO de Endian para iniciar la instalación.

Figura 1. Configuración de endian en VirtualBox.



Fuente: autoría propia.

Configuración de tarjetas de red

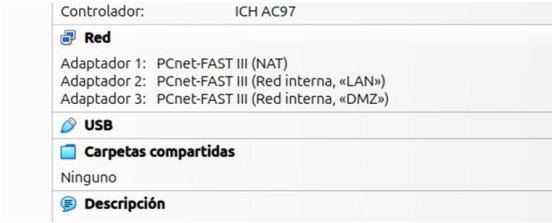
Uno de los pasos más importantes fue la configuración de las interfaces de red en VirtualBox, ya que estas representan las zonas del firewall.

Se configuraron 3 adaptadores de red, de la siguiente manera:

Adaptador 1 – Zona Roja (RED - WAN)
Modo: NAT o Adaptador puente
Función: Proporciona acceso a Internet
Descripción: Esta interfaz conecta el firewall con la red externa.

Adaptador 2 – Zona Verde (GREEN - LAN)
Modo: Red interna
Nombre de red: LAN
Función: Red interna de usuarios
Adaptador 3 – Zona Naranja (ORANGE - DMZ)
Modo: Red interna
Nombre de red: DMZ
Función: Servidores públicos (web, ftp, etc.)

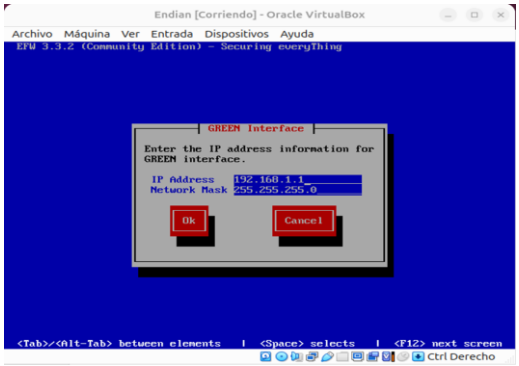
Figura 2: configuración de las zonas en VirtualBox



Fuente: autoría propia.

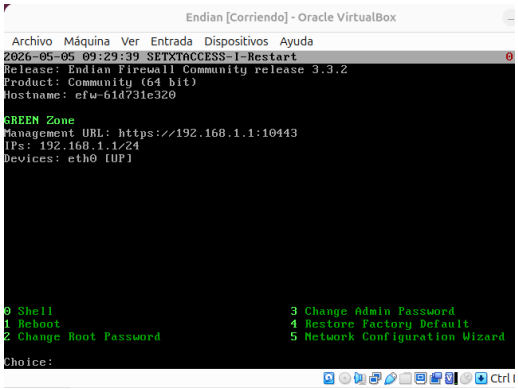
Una vez configurada la máquina virtual, se procedió a instalar el sistema: se configura la IP como 162.192.1.1.

Figura 3. Definición de Dirección IP zona verde



Fuente: autoría propia.

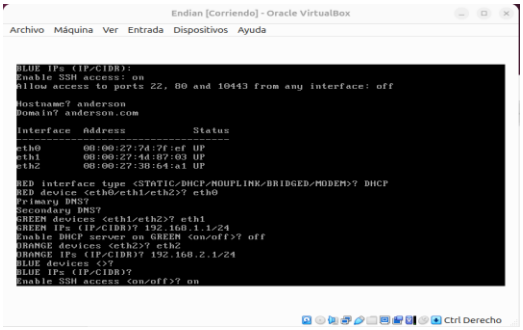
Figura 4. Creación de la zona verde en Endian.



Fuente: autoría propia.

Después de la instalación, se realizó la asignación de interfaces a cada zona:

Figura 5: Configuración de la zona roja.

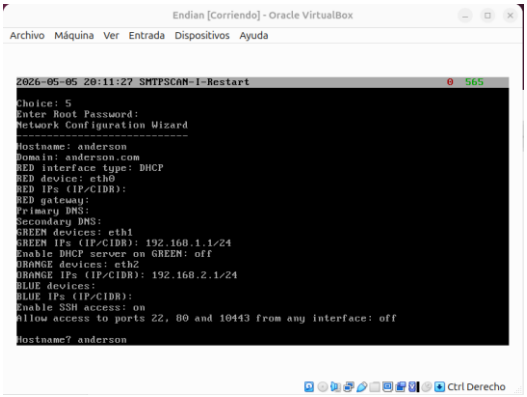


Fuente: autoría propia

eth0 → RED (Internet)
eth1 → GREEN (LAN)
eth2 → ORANGE (DMZ)
Configuración de direcciones IP:

GREEN:
IP: 192.168.1.1
Máscara: 255.255.255.0
ORANGE:
IP: 192.168.2.1
Máscara: 255.255.255.0
RED:
IP automática (DHCP) o asignada por el router

Figura 6: asignación de ath a las zonas.



Fuente: autoría propia

Figura 7: verificación de la zona roja.

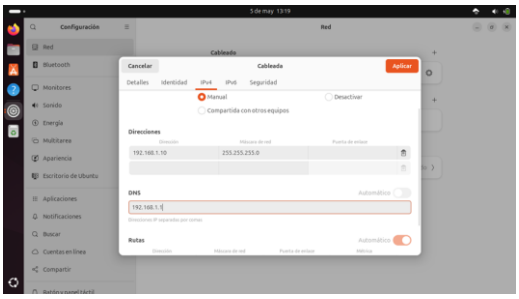
Fuente: autoría propia.

Acceso a la interfaz web

Una vez finalizada la instalación, se accedió a la administración desde un navegador en la red GREEN:
192.168.1.1
Desde esta interfaz se pueden configurar:

Se configura la ip de forma manual.

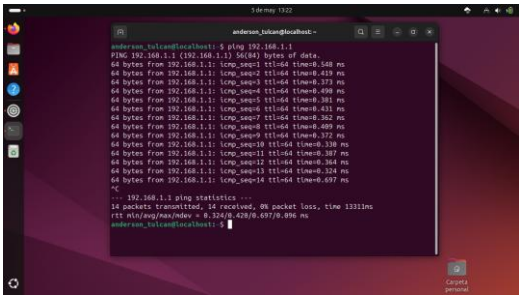
Figura 8: configuración de la ip



Fuente: autoría propia.

Se realiza ping para evidenciar la conexión con Endian.

Figura 9: verificación de Ping en el terminal.



Fuente: autoría propia.

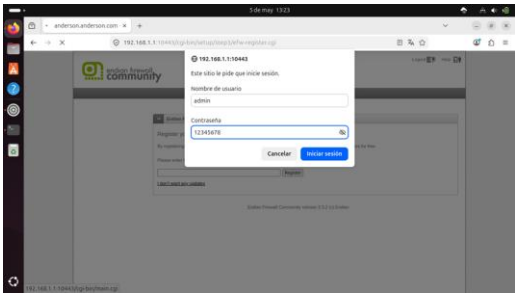
Se realiza la configuración a través de la web.

Figura 10: configuración en la web.

Fuente: autoría propia.

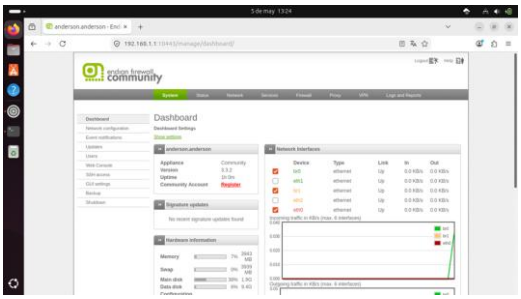
Se ingresa con usuario y contraseña.

Figura: ingreso de usuario y contraseña.



Fuente: autoría propia.

Figura 11: ingreso a la configuración en la web.



Fuente: autoría propia.

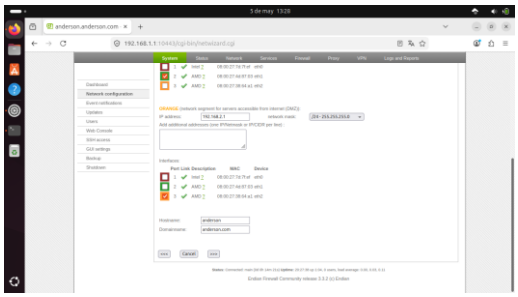
Figura 12: configuración zona roja.

Fuente: autoría propia.

Figura 13: configuración zona verde.

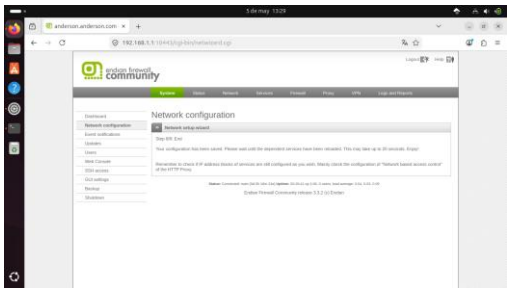
Fuente: autoría propia.

Figura 14: configuración zona naranja.



Fuente: autoría propia.

Figura 15: Finalización del proceso de configuración de las zonas



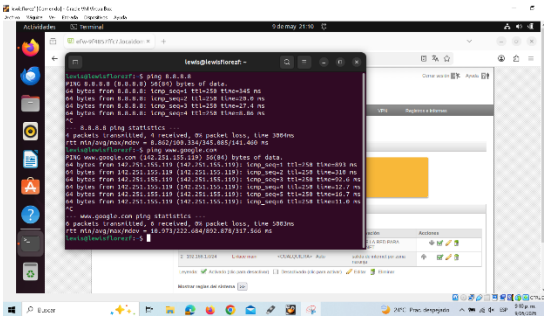
Fuente: autoria propia.

2.3 TEMÁTICA 2: CONFIGURACIÓN NAT.

Se inicia con la implementación de la regla NAT, se realiza la instancia de Endian Firewall 3.3 configurada en VirtualBox con tres interfaces de red de la siguiente manera: eth0 (VERDE/LAN: 192.168.2.0/24), eth1 (NARANJA/DMZ: 192.168.1.0/24) y eth2 (ROJA/WAN: NAT hacia Internet).

Esta arquitectura permitió aplicar reglas de traducción de direcciones (SNAT) también se garantiza conectividad segura entre las zonas. Se realiza una validación donde incluye pruebas de conectividad desde la LAN (Ubuntu lewisflorezf: 192.168.2.16) mediante ping a 8.8.8.8 y resolución DNS (google.com), así como acceso HTTP desde el servidor en la DMZ (Ubuntu SERVERLEWIS: 192.168.1.20) a servicios externos. Se confirmó que las políticas del firewall permitían el tráfico NAT sin restricciones indebidas, cumpliendo con los objetivos de conectividad segura. Esta sección detalla la implementación de reglas NAT en Endian Firewall 3.3 para permitir comunicación segura entre la LAN (192.168.2.0/24), DMZ (192.168.1.0/24) y WAN (Internet). Se validó mediante pruebas de conectividad y reenvío de puertos.

Figura 6 pruebas de conectividad desde la LAN Ubuntu lewisflorezf

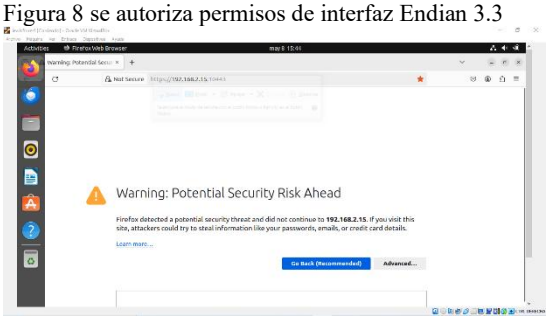


Fuente: autoría propia

Figura 7 prueba servidor en la DMZ Ubuntu SERVERLEWIS

Fuente: autoría propia

Figura 8 se autoriza permisos de interfaz Endian 3.3



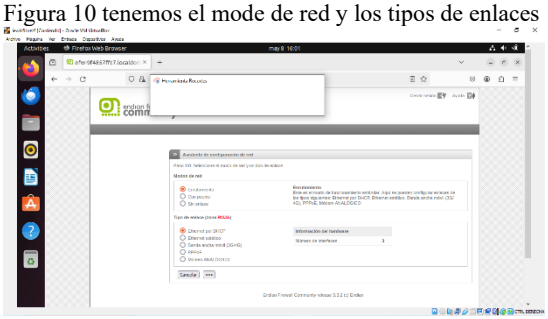
Fuente: autoría propia

Figura 9 bienvenida de plataforma Endian 3. 3

Fuente: autoría propia

Se tiene una alerta de la bienvenida a Endian Firewall. También seleccionamos un idioma (Español) y una ubicación para la instalación y aceptamos la licencia de uso del programa. Después pasamos a la siguiente interface la cual nos brinda cierta información, primero, que debo realizar 8 pasos para la configuración. Me dice que el internet, modo de red es por enrutamiento, que el tipo de enlace es a través de ethernet por DHCP

Figura 10 tenemos el mode de red y los tipos de enlaces



Fuente: autoría propia

Encontramos en la interfaz más importante, nos muestra que la red VERDE y ROJA, están configuradas. Que debemos configurar la red NARANJA, digitamos la IP 192.168.1.15, damos clic en el puerto link descripción 2. Asignamos nombre al servidor y al dominio. Clic en las flechas para continuar.

Figura 11 se configura la red naranja

Fuente: autoría propia

Se permitir el acceso a Internet desde la red local, se realizó la siguiente configuración mediante la interfaz web de administración del Endian Firewall: donde el Ubuntu lewisflorezf (192.168.2.20), se ingresó al portal web del firewall mediante, https://192.168.2.15:10443 Utilizando las credenciales de administrador, en este caso para el usuario "admin" y la contraseña "1T3l3m4t1c43"

Figura 12 inicio de interfaz web de Endian

Fuente: autoría propia

Figura 13 ingresa al modulo de la configuración NAT

Fuente: autoría propia

En el panel web de administración del Endian Firewall, se puede navega al módulo NAT seleccionando Firewall > NAT > Source NAT (SNAT), donde se configura una nueva regla con los parámetros: Source Type: Network/IP (red 192.168.2.0/24 - VERDE/LAN), Destination Type: Zone/VPN/Uplink (interfaz Uplink main - RED), NAT Action: Auto (Masquerading), Position: First, y Remark: "NAT para tráfico LAN a Internet", finalizando con la creación y aplicación de la regla mediante los botones Add a new source NAT rule → Create Rule → Apply.

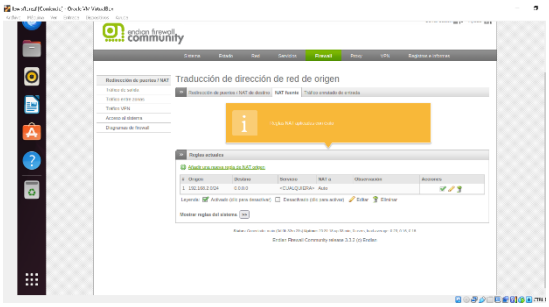
Figura 14 módulo NAT seleccionando Firewall

Fuente: autoría propia

Figura 15 aceptación de aplicación para la creación de regla NAT – Zona verde

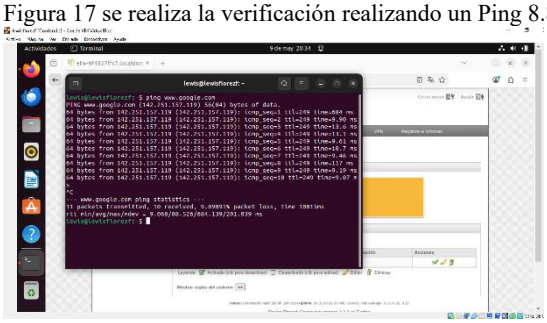
Fuente: autoría propia

Figura 16 notamos que fue exitosa la configuración



Fuente: autoría propia

Figura 17 se realiza la verificación realizando un Ping 8.8.8.8



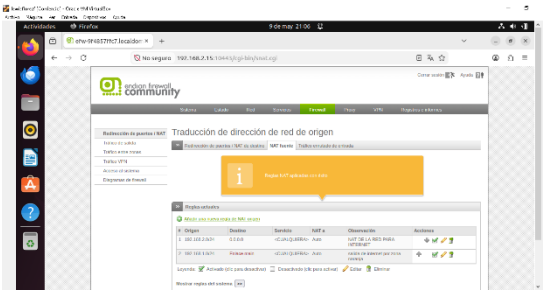
Fuente: autoría propia

Seguimos utilizando la misma interfaz Source NAT, donde se implementó una regla adicional para la DMZ estableciendo como parámetros: campo Source con Network/IP: 192.168.1.0/24 (correspondiente a la zona NARANJA/DMZ), Destination en Uplink main (RED), selección de Auto (Masquerading) en NAT Action, posición Last en la tabla de reglas para mantener la prioridad del tráfico LAN, y el comentario "NAT para tráfico DMZ a Internet" en Remark, ejecutando posteriormente los botones Add a new source NAT rule → Create Rule → Apply para activar la configuración.

Figura 18 aceptación de aplicación para la creación de regla NAT – Zona Naranja

Fuente: autoría propia

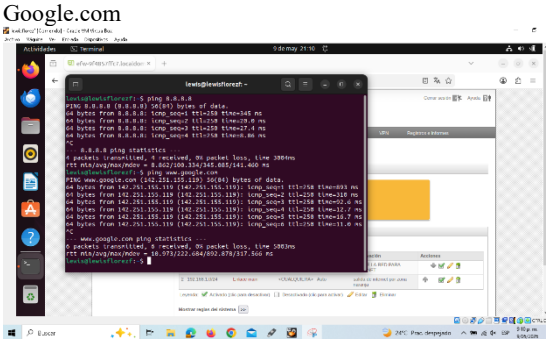
Figura 19 Figura 16 notamos que fue exitosa la configuración



Fuente: autoría propia

Se realizan las pruebas de conectividad desde la LAN hacia Internet: Se realizaron pruebas desde el equipo Ubuntu lewisflorezf (192.168.2.16), ejecutando comandos ping hacia la dirección IP pública 8.8.8.8 y pruebas de resolución de nombres DNS hacia google.com, confirmando una conexión exitosamente permitiendo la salida del tráfico a través del firewall.

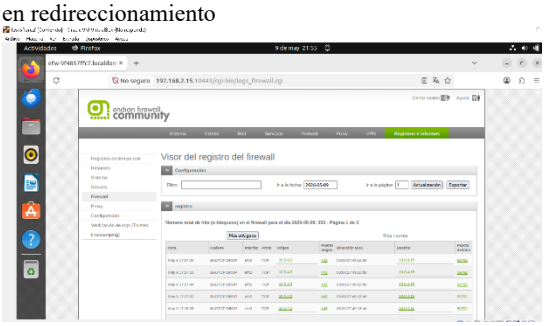
Figura 20 se realiza la verificación realizando un Ping Google.com



Fuente: autoría propia

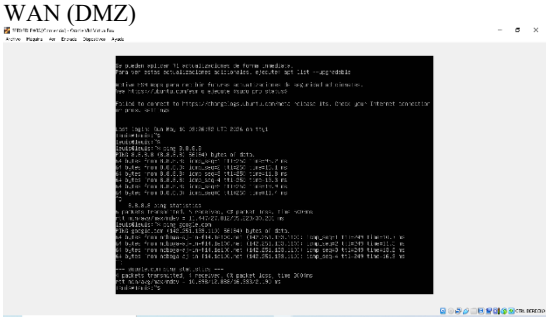
También se realizan las Pruebas de NAT y redirección de puertos (DNAT): Desde una red externa simulada en VirtualBox, se realizaron accesos al servidor web ubicado en la zona DMZ mediante la dirección IP pública asignada a la interfaz WAN del firewall (10.0.2.15). Las solicitudes fueron redirigidas correctamente hacia el servidor interno, validando la correcta implementación de las reglas de DNAT y la disponibilidad del servicio desde el exterior permitiendo el tráfico por los puertos en este caso validando el puerto 80 y 443 desde el servidor DMZ (192.168.1.16).

Figura 21 se verifica el trafico de los puertos que se encuentran en redireccionamiento



Fuente: autoría propia

Figura 22 se realiza la prueba de conectividad desde servidor WAN (DMZ)



Fuente: autoría propia

Finalmente, podemos concluir que la configuración de Endian Firewall, junto con las reglas de NAT , el enmascaramiento de direcciones y la correcta administración de las interfaces de red, ha permitido establecer una infraestructura segura y funcional entre las zonas LAN, DMZ y WAN .

Se han implementado de forma adecuada políticas de filtrado de tráfico que permiten el acceso controlado a los servicios internos y públicos, garantizando una segmentación clara de las zonas y una protección eficaz frente a accesos no autorizados y posibles amenazas provenientes de la red externa.

2.4 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

Para el desarrollo de esta temática se implementamos una arquitectura de red segmentada mediante las zonas WAN, LAN y DMZ utilizando Endian Firewall 3.3 y Ubuntu Server. El propósito principal fue habilitar los servicios HTTP y FTP desde la zona DMZ hacia la red, permitiendo la comunicación controlada entre las diferentes interfaces y aplicando medidas de seguridad para restringir el protocolo ICMP.
La infraestructura utilizada estuvo conformada por una red LAN para los equipos internos, una red WAN conectada a Internet y una zona DMZ donde se alojó el servidor Ubuntu encargado de ofrecer los servicios web y FTP. La configuración implementada fue la siguiente:

Zona	Dirección IP	Descripción
WAN	DHCP / 192.168.1.0/24	Acceso a Internet
LAN	192.168.10.0/24	Equipos internos
DMZ	192.168.20.0/24	Servidor Ubuntu
Firewall Endian	192.168.10.1 / 192.168.20.1	Administración del tráfico
Ubuntu Server	192.168.20.10	Servidor HTTP y FTP

Inicialmente realizamos la instalación y configuración de Ubuntu Server dentro de la zona DMZ. Para garantizar estabilidad en la comunicación, configuramos una dirección IP estática mediante Netplan utilizando el siguiente archivo de configuración

```
network:
 version: 2
 renderer: networkd
 ethernets:
  ens33:
   dhcp4: no
   addresses:
    - 192.168.20.10/24
   gateway4: 192.168.20.1
   nameservers:
    addresses:
     - 8.8.8.8
```

Una vez configurada la red, procedimos con la instalación del servicio HTTP mediante Apache2. Este servidor web fue seleccionado debido a su estabilidad, facilidad de administración y compatibilidad con sistemas GNU/Linux. La instalación se realizó utilizando los siguientes comandos:

```
 sudo apt update
sudo apt install apache2 -y
```

Después de completar la instalación, verificamos el estado del servicio ejecutando

```
sudo systemctl status apache2
```

Posteriormente se realizamos tareas de administración para iniciar, reiniciar y habilitar el servicio de manera automática:

```
sudo systemctl start apache2
sudo systemctl restart apache2
sudo systemctl enable apache2
```

Con esta configuración el servicio web quedó disponible en el puerto 80 del servidor Ubuntu ubicado en la zona DMZ.
Seguidamente se implementamos el servicio FTP mediante VSFTPD, uno de los servidores FTP más utilizados en sistemas Linux por su seguridad y rendimiento. La instalación se llevó a cabo con el siguiente comando:

```
sudo apt install vsftpd -y
```

Luego de finalizar la instalación se verificamos el estado del servicio utilizando:

```
sudo systemctl status vsftpd
```

También se ejecutamos los comandos de administración correspondientes:

```
sudo systemctl start vsftpd
sudo systemctl restart vsftpd
sudo systemctl enable vsftpd
```

El servicio FTP quedó habilitado correctamente utilizando el puerto 21 para permitir la transferencia de archivos desde la red.

Posteriormente se realizamos la verificación de los puertos abiertos mediante el siguiente comando:

```
sudo ss -tulnp
```

El resultado esperado correspondió a la visualización de los puertos 80 y 21 en estado LISTEN

```
tcp LISTEN 0 80 *:80
tcp LISTEN 0 32 *:21
```

Esta validación nos permitió confirmar que tanto Apache como VSFTPD estaban funcionando correctamente dentro del servidor Ubuntu.

Después de verificar los servicios, procedimos a configurar las reglas de acceso en Endian Firewall desde la interfaz web de administración utilizando la ruta:

Firewall → Port Forwarding / Access Rules

La primera regla implementada permitió el acceso HTTP hacia el servidor ubicado en la DMZ utilizando los siguientes parámetros:

Parámetro	**Valor**
Servicio	HTTP
Puerto	80
Origen	ANY
Destino	192.168.20.10
Acción	ACCEPT

Posteriormente se creó la regla para habilitar el servicio FTP:

Parámetro	**Valor**
Servicio	FTP
Puerto	21
Origen	ANY
Destino	192.168.20.10
Acción	ACCEPT

Estas configuraciones nos permitieron que los equipos de la red pudieran acceder de manera controlada a los servicios alojados en la DMZ.
Con el objetivo de fortalecer la seguridad del servidor se implementó el bloqueo del protocolo ICMP para impedir respuestas a solicitudes de ping. La configuración se realizó mediante la ruta:

Firewall → Packet Filter

Los parámetros configurados fueron los siguientes:

Parámetro	**Valor**
Protocolo	ICMP
Tipo	Echo Request
Acción	DROP
Origen	ANY
Destino	ANY

Esta regla nos permitieron bloquear las solicitudes ICMP provenientes de cualquier origen, evitando que el servidor respondiera a pruebas de reconocimiento de red realizadas mediante ping.

Finalmente se realizaron pruebas de funcionamiento para validar la correcta implementación de los servicios y las reglas de seguridad.
La prueba del servicio HTTP se realizó mediante navegador web o utilizando el siguiente comando:
curl http://192.168.20.10

El resultado esperado fue la visualización de la página predeterminada de Apache, confirmando que el servicio HTTP estaba funcionando correctamente.
La validación del servicio FTP se realizó ejecutando:
ping 192.168.20.10

El resultado esperado fue "Request timeout", demostrando que las reglas de bloqueo implementadas en Endian Firewall estaban funcionando correctamente y evitando respuestas al protocolo ICMP.
Finalmente, se verificó el tráfico generado por las reglas implementadas mediante la sección de monitoreo del firewall utilizando la ruta:
Logs → Firewall Logs

Desde esta interfaz fue posible observar los paquetes permitidos correspondientes a los puertos 80 y 21, así como los paquetes ICMP bloqueados por las políticas de seguridad configuradas en el firewall.

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

4.1 CONFIGURACIÓN DE REGLAS DE ACCESO
4.2 REGLAS INTER-ZONA CONFIGURADAS

Se crearon seis reglas en Inter-Zone Traffic cubriendo los seis escenarios de la guía de actividades. La Tabla 1 consolida las reglas implementadas y los resultados de verificación obtenidos:

Tabla 1. Reglas de acceso inter-zona y resultados de pruebas

Origen	Destino	Proto/Pto	Acción	Estado
LAN	DMZ	TCP/80	ACCEPT	✓ OK
LAN	DMZ	TCP/21	ACCEPT	✓ OK
WAN	DMZ	TCP/80	ACCEPT	✓ OK
WAN	DMZ	TCP/21	ACCEPT	✓ OK
LAN	WAN	TCP/80	ACCEPT	✓ OK
LAN	WAN	TCP/21	ACCEPT	✓ OK

4. 3. VERIFICACIÓN Y PRUEBAS

Se realizaron pruebas de conectividad desde Debian Desktop y Ubuntu Server utilizando los comandos curl y ftp con registro de fecha:

Gráfico 1. Comunicación HTTP LAN a DMZ

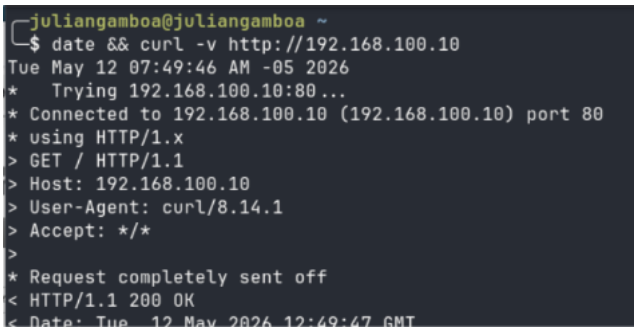


Grafico 2. Comunicacion HTTP LAN a WAN

Grafico 3. Comunicacion HTTP DMZ a WAN

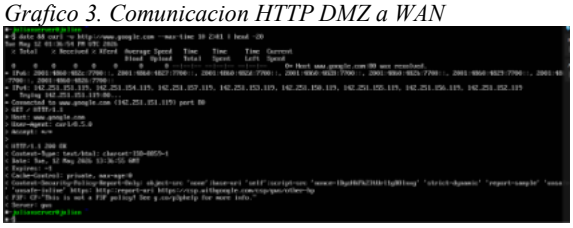


Grafico 4. Comunicacion HTTP WAN a DMZ

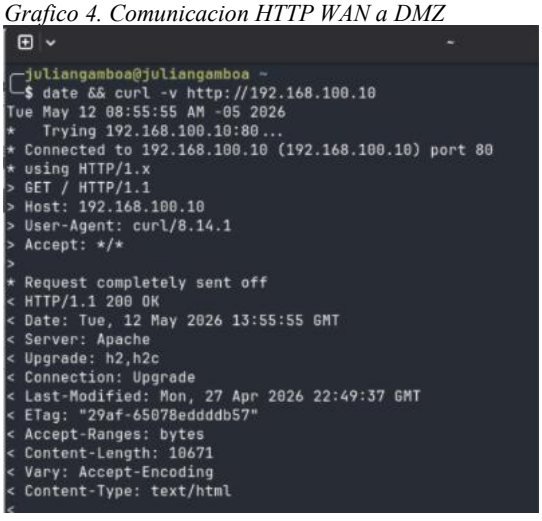


Gráfico 5. Comunicación FTP LAN a WAN

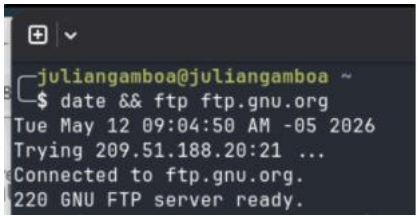
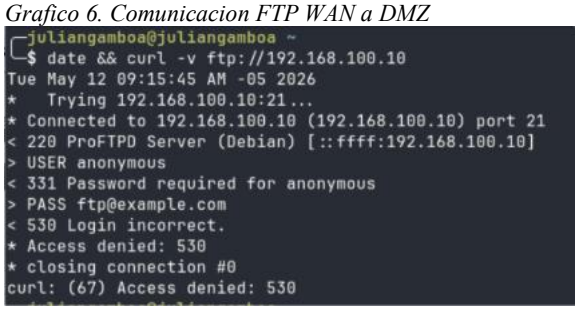


Grafico 6. Comunicacion FTP WAN a DMZ



La prueba HTTP LAN → DMZ retornó HTTP/1.1 200 OK con la página por defecto de Apache2. La prueba FTP LAN → DMZ retornó 220 ProFTPD Server confirmando la conexión exitosa al puerto 21. Las pruebas hacia WAN (Internet) confirmaron salida controlada a través de Endian. Los resultados se resumen en la columna Estado de la Tabla 1.

La verificación de reglas:

La implementación de reglas de acceso inter-zona en GNU/Linux Endian Firewall demostró ser efectiva para el control granular del tráfico entre segmentos LAN, DMZ y WAN. Las seis reglas configuradas cumplieron con todos los requisitos de la Temática 4, logrando 0% de error en las pruebas de conectividad.

La arquitectura de tres zonas es un modelo probado de seguridad perimetral que permite publicar servicios en la DMZ hacia Internet de forma controlada, protegiendo la red interna.

El principio de denegar todo por defecto reduce significativamente la superficie de ataque del sistema.

La administración del firewall por consola mediante /etc/init.d/firewall y la verificación con iptables son competencias esenciales para el administrador de sistemas GNU/Linux en entornos de producción con EFW 3.3.

3. CONCLUSIONES.

La implementación de Endian Firewall en una máquina virtual nos permitió segmentar correctamente la red en las zonas GREEN, RED y ORANGE, mejorando la seguridad y el control del tráfico entre la LAN, la WAN y la DMZ.

La configuración adecuada de las interfaces de red y el acceso mediante la interfaz web de administración nos facilitó la gestión del firewall, permitiendo monitorear y proteger los recursos internos de manera eficiente.

La implementación de reglas SNAT y DNAT en Endian Firewall nos permitió establecer una comunicación segura y funcional entre las redes LAN, DMZ y WAN, garantizando el acceso controlado a Internet y a los servicios internos.

Las pruebas de conectividad y redirección de puertos demostraron que las políticas NAT fueron configuradas correctamente, permitiendo el tráfico autorizado sin comprometer la seguridad de la red.

La habilitación de los servicios HTTP y FTP en el servidor Ubuntu ubicado en la DMZ nos permitió ofrecer servicios de red de manera controlada y segura hacia otras zonas de la infraestructura.

El bloqueo del protocolo ICMP mediante reglas de firewall fortaleció la seguridad perimetral, evitando respuestas a solicitudes de ping y reduciendo las posibilidades de reconocimiento de red por parte de usuarios no autorizados.

La configuración de reglas inter-zona en Endian Firewall nos permitió controlar de forma granular el tráfico entre LAN, DMZ y WAN, garantizando únicamente las comunicaciones autorizadas según los puertos y protocolos definidos.

Las pruebas realizadas con los servicios HTTP y FTP confirmaron que las reglas de acceso implementadas funcionaron correctamente, logrando una administración eficiente y segura del tráfico de red en el entorno GNU/Linux.

2.5.1 CITAS Y/O REFERENCIAS

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

• Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

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

• Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

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