IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Evelyn Gisel Herrera Puentes
e-mail: egherrerap@unadvirtual.edu.co

RESUMEN: *El propósito de esta actividad fue implementar un esquema de seguridad perimetral en un entorno GNU/Linux mediante el uso de Endian Firewall, apoyado en un modelo de segmentación de red conformado por las zonas Green (LAN), Orange (DMZ) y Red (WAN). El desarrollo del ejercicio siguió los lineamientos establecidos en la Guía de Aprendizaje correspondiente a la Etapa 7 e incluyó la configuración de servicios, reglas de control de acceso, traducción de direcciones (NAT), protocolos orientados a una navegación segura y el despliegue de servidores dentro de la DMZ.*

El proceso contempló la instalación de la plataforma, así como pruebas de validación y comprobaciones a través de consola para asegurar el correcto funcionamiento de las comunicaciones entre los distintos segmentos de red. Como resultado, se verificó la correcta aplicación de políticas de seguridad, fortaleciendo la protección, disponibilidad e integridad de los recursos de la infraestructura de red.

PALABRAS CLAVE: Seguridad perimetral, Endian Firewall, GNU/Linux, DMZ, segmentación de red, NAT (Network Address Translation), control de acceso, firewall, LAN, WAN, políticas de seguridad.

1 INTRODUCCIÓN

La implementación de mecanismos de seguridad perimetral es un componente esencial en la gestión de infraestructuras basadas en GNU/Linux, debido a su función en la protección de los recursos tecnológicos frente a amenazas externas e internas. En entornos organizacionales, la correcta segmentación de la red y la definición de políticas de filtrado permiten preservar la confidencialidad, integridad y disponibilidad de la información.

En el desarrollo de la Etapa 7 del Diplomado de Profundización en Administración de Sistemas Operativos Open Source, se realizó la configuración de una solución de seguridad mediante Endian Firewall, estructurando la red en diferentes zonas lógicas: LAN (Green), WAN (Red) y DMZ (Orange). Esta arquitectura facilitó la aplicación práctica de controles de tráfico, reglas de acceso, traducción de direcciones (NAT), habilitación de servicios específicos y la implementación de mecanismos de navegación segura, incluyendo proxy con autenticación.

El trabajo integró tanto la configuración a nivel de interfaz como la verificación y validación desde la línea de comandos, fortaleciendo las competencias técnicas en administración de sistemas GNU/Linux. En este documento se describen los procedimientos ejecutados, las configuraciones realizadas y los resultados obtenidos, siguiendo los lineamientos de presentación establecidos bajo el formato académico IEEE.

2. PROCEDIMIENTO TEMÁTICA 1

2.1. Configuración de la instancia GNU/Linux Endian en VirtualBox (interfaces de red) e instalación

Para la implementación del entorno de seguridad, se creó una máquina virtual en VirtualBox destinada a alojar la distribución GNU/Linux Endian. Durante la configuración de la instancia, se asignaron múltiples adaptadores de red con el fin de simular una arquitectura perimetral segmentada.

Se establecieron tres zonas principales:

- **Zona Green (LAN):** configurada como red interna para los equipos locales.
- **Zona Red (WAN):** destinada a la conexión externa o acceso a Internet.
- **Zona Orange (DMZ):** utilizada para el alojamiento de servidores accesibles desde el exterior bajo políticas controladas.

La correcta asignación de las interfaces permitió diferenciar el tráfico entre segmentos y aplicar posteriormente las reglas de filtrado y control correspondientes.

2.2. Instalación de GNU/Linux Endian

La imagen ISO de la distribución Endian fue obtenida desde el sitio oficial del proveedor. Posteriormente, se procedió con el montaje del archivo en la máquina virtual y se ejecutó el proceso de instalación, configurando los parámetros básicos del sistema, tales como idioma, zona horaria, credenciales administrativas y asignación inicial de interfaces de red.

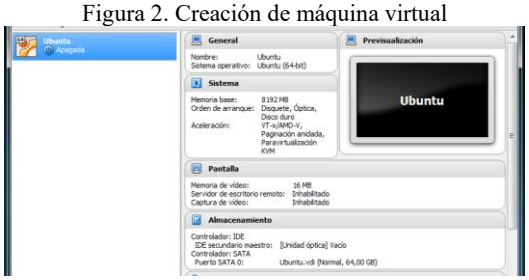
Una vez completada la instalación, se verificó el acceso a la consola y a la interfaz de administración web, confirmando el correcto despliegue del sistema.

Figura 1. Página de descarga de Endian

Fuente: Autoría propia

Muestra el sitio oficial desde donde se obtiene la distribución Endian Firewall

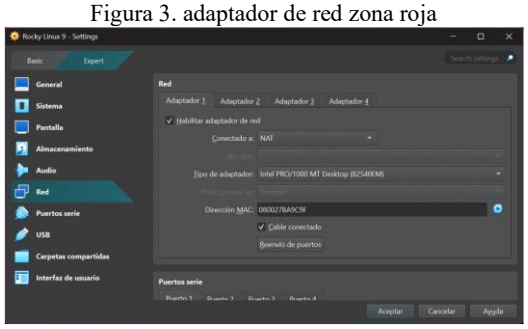
Figura 2. Creación de máquina virtual



Fuente: Autoría propia

Se observa el proceso de creación de la máquina virtual en VirtualBox para alojar Endian.

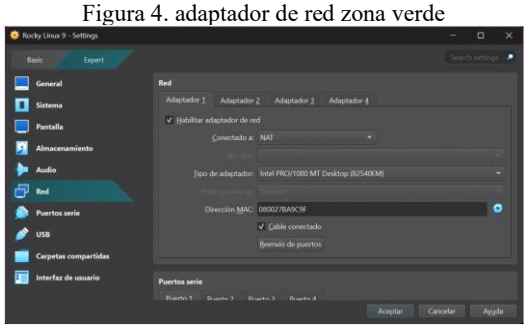
Figura 3. adaptador de red zona roja



Fuente: Autoría propia

Configuración del adaptador de red en modo NAT para la zona WAN

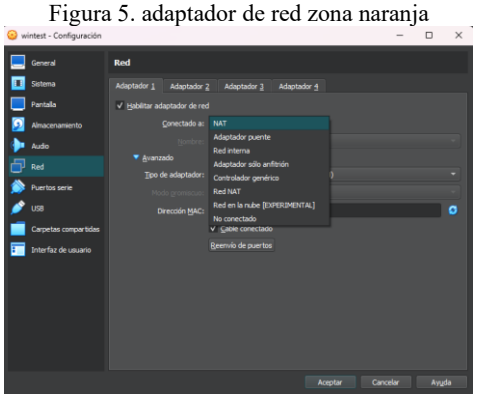
Figura 4. adaptador de red zona verde



Fuente: Autoría propia

Configuración del adaptador de red en modo red interna para la zona LAN

Figura 5. adaptador de red zona naranja



Fuente: Autoría propia

Configuración del adaptador de red en modo red interna para la zona DMZ
Adaptador ethernet 1 IP: 192.168.20.1 Máscara de subred: 255.255.255.0

Figura 6. Asignación IP zona verde

Fuente: Autoría propia

Pantalla de configuración de la dirección IP para la interfaz GREEN.

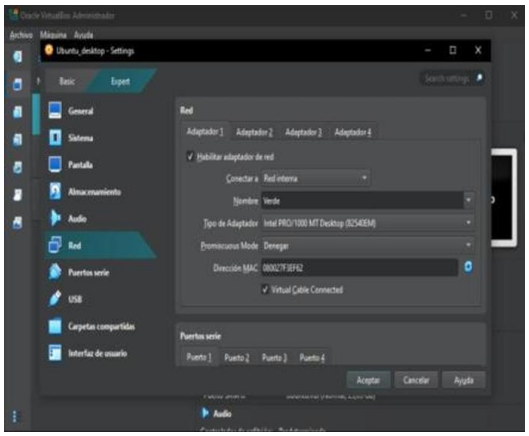
Figura 7. Entorno de Endian con las IP de las zonas

Fuente: Autoría propia

2.3. ACCESO A INTERFAZ WEB DESDE EQUIPO CLIENTE

Se realizó la reconfiguración del adaptador de red en la máquina cliente con Ubuntu Desktop dentro de VirtualBox, asignándolo a la Zona Green (LAN) con el fin de integrarlo correctamente al segmento de red interno definido en la arquitectura perimetral.

Figura 8. Asignación de adaptador de red equipo cliente



Fuente: Autoría propia

Se realizó la verificación de conectividad desde el equipo cliente ubicado en la Zona Green (LAN) hacia el servidor Endian, utilizando la herramienta de línea de comandos. Para ello, se ejecutó el comando ping 192.168.20.1, con el fin de comprobar la disponibilidad del gateway y validar la correcta comunicación dentro del segmento de red interno.

Figura 7. Verificación de conexión desde la zona verde

Fuente: Autoría propia

Se Ingresó desde el equipo cliente a la URL de Administración en la web, correspondiente a la IP de la Zona Verde 192.168.20.1

Figura 8. Acceso al entorno web de Endian

Fuente: Autoría propia

2.4 CONFIGURACION DE ZONA NARANJA DESDE EL ENTORNO WEB

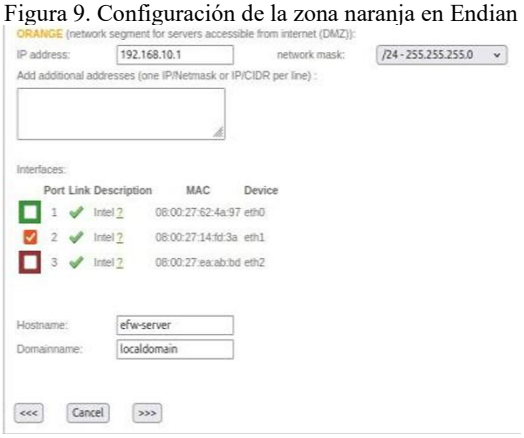
Posteriormente, a través de la interfaz web de administración, se realizó la configuración inicial del sistema, definiendo los parámetros fundamentales para su correcto funcionamiento. En esta etapa se establecieron los siguientes aspectos:

- Selección de idioma y configuración de la zona horaria del sistema.
- Restauración de una copia de seguridad, en caso de requerirse una configuración previa.
- Definición de credenciales para el usuario administrador, tanto para el acceso a la interfaz web como para la conexión remota mediante SSH.
- Configuración del modo de operación de red en enrutamiento (routing).
- Asignación del tipo de conexión de la Zona Red (WAN) mediante DHCP, permitiendo la obtención automática de la dirección IP externa.

Finalmente, se procedió con la parametrización de la Zona Orange (DMZ), estableciendo la dirección IP correspondiente, asociando la interfaz física Ethernet 2 y definiendo el nombre del servidor dentro de la arquitectura de red.

Adaptador ethernet 2
IP: 192.168.10.1
Máscara de subred: 255.255.255.0

Figura 9. Configuración de la zona naranja en Endian



Fuente: Autoría propia

Una vez definidos los parámetros iniciales, se procedió al acceso del panel principal de administración a través de la interfaz web de Endian, utilizando las credenciales previamente configuradas. Desde este entorno se gestionaron y supervisaron los distintos servicios del sistema, así como las políticas de red y seguridad asociadas.

Figura 10. Dashboard entorno web Endian

Fuente: Autoría propia

Se efectuó la validación de conectividad a Internet desde el equipo Ubuntu Desktop ubicado en la Zona Green (LAN), con el propósito de comprobar el correcto enrutamiento del tráfico hacia la Zona Red

(WAN) a través del firewall y verificar la adecuada aplicación de las reglas de salida configuradas.

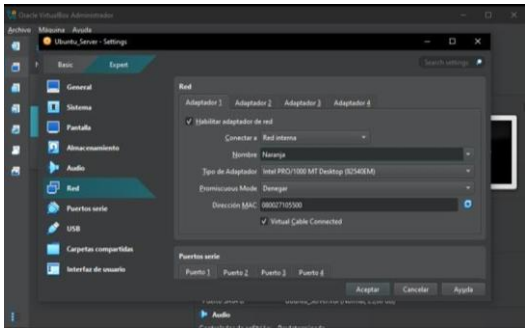
Figura 11. Acceso a internet desde equipo Ubuntu Desktop

Fuente: Autoría propia

2.5 CONFIGURACION DE IP EQUIPO SERVER PARA ZONA NARANJA

Se realizó la configuración del adaptador de red en la máquina servidor con Ubuntu Server dentro de VirtualBox, asignándolo a la Zona Orange (DMZ) con el fin de ubicarlo en el segmento destinado a la publicación de servicios y aislarlo del entorno interno (LAN).

Figura 12. Asignación de adaptador de red equipo servidor



Fuente: Autoría propia

Para la configuración de red en el servidor Ubuntu Server, se editó el archivo de Netplan mediante el comando:

sudo nano 50-cloud-init.yaml

Dentro del archivo se realizaron los siguientes ajustes:

- Desactivación del direccionamiento dinámico (DHCP): **dhcp4: false**
- Asignación de dirección IP estática: **addresses: - 192.168.10.2/24**
- Configuración de la puerta de enlace predeterminada: **routes: - to: default via: 192.168.10.1**
- Definición de servidores DNS (nameservers): **nameservers: addresses: - 8.8.8.8 / - 8.8.4.4**

Esta configuración permitió establecer una dirección IP fija en la Zona Orange (DMZ), asegurando la estabilidad del servicio y la correcta resolución de nombres de dominio.

Figura 13. Asignación de la dirección IP en equipo servidor

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.10.2/24
      routes:
        - to: default
          via: 192.168.10.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
```

Fuente: Autoría propia

Posteriormente, se aplicaron los cambios realizados en la configuración de red mediante el comando sudo netplan apply, con el fin de activar la nueva asignación de dirección IP estática.

Una vez implementada la configuración, se verificó la conectividad con el firewall Endian ejecutando un ping a la dirección IP 192.168.10.1, correspondiente a la interfaz de la Zona Orange (DMZ). Esta prueba permitió confirmar la correcta comunicación entre el servidor y el gateway definido para dicho segmento de red.

Figura 14. Verificación de conexión desde la zona naranja

```
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.431 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.40 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.40 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.25 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=1.04 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=1.06 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=1.39 ms
64 bytes from 192.168.10.1: icmp_seq=8 ttl=64 time=1.27 ms
64 bytes from 192.168.10.1: icmp_seq=9 ttl=64 time=0.535 ms
64 bytes from 192.168.10.1: icmp_seq=10 ttl=64 time=1.21 ms
64 bytes from 192.168.10.1: icmp_seq=11 ttl=64 time=1.33 ms
^C
--- 192.168.10.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10168ms
rtt min/avg/max/mdev = 0.431/1.120/1.403/0.323 ms
freddygarnica@unadserver:~$ _
```

Fuente: Autoría propia

Se verificó ingreso a internet con un ping a la URL de Google

Figura 15. Acceso a internet desde equipo Ubuntu Server

```
freddygarnica@unadserver:~$ ping google.com
PING google.com (172.217.162.142) 56(84) bytes of data.
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=1 ttl=254 time=18.6 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=2 ttl=254 time=16.8 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=3 ttl=254 time=19.1 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=4 ttl=254 time=18.1 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=5 ttl=254 time=16.3 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=6 ttl=254 time=10.6 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=7 ttl=254 time=13.1 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=8 ttl=254 time=22.4 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=9 ttl=254 time=21.5 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=10 ttl=254 time=15.6 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=11 ttl=254 time=32.2 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=12 ttl=254 time=152 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=13 ttl=254 time=33.8 ms
64 bytes from pnboga-ad-in-f14.1e100.net (172.217.162.142): icmp_seq=14 ttl=254 time=34.0 ms
^C
--- google.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13196ms
```

Fuente: Autoría propia

3 PROCEDIMIENTO TEMATICA 2

3.1 IMPLEMENTACIÓN Y CONFIGURACIÓN DE NAT EN ENDIAN PARA COMUNICACIÓN LAN-WAN Y DMZ-INTERNET

Se describe el proceso de creación de reglas de traducción de direcciones de red (NAT) y la configuración de reenvío de puertos (port forwarding), con el objetivo de permitir el acceso controlado a determinados servicios alojados en la red, garantizando al mismo tiempo el cumplimiento de las políticas de seguridad establecidas entre las distintas zonas (LAN, WAN y DMZ).

3.2 CONFIGURACIÓN DE LA INFRAESTRUCTURA

La implementación de Endian en VirtualBox se estructuró mediante una arquitectura segmentada en tres zonas principales:

- **Zona Green (LAN):** destinada a la red interna, donde se ubican las estaciones de trabajo y equipos cliente.
- **Zona Orange (DMZ):** segmento reservado para servidores que ofrecen servicios como aplicaciones web y bases de datos, expuestos de manera controlada.
- **Zona Red (WAN):** interfaz orientada a la conexión externa o acceso a Internet.

Cada una de estas zonas fue asociada a interfaces de red independientes y a rangos de direcciones IP específicos, permitiendo la separación lógica del tráfico y facilitando la aplicación de políticas de filtrado y control entre segmentos.

3.2 CONFIGURACIÓN NAT EN ENDIAN

Se configuró una regla de traducción de direcciones de red (NAT) con el propósito de permitir que el tráfico generado en la Zona Green (LAN) pudiera acceder a la Zona Red (WAN). Esta configuración realiza la conversión de direcciones IP privadas a la dirección IP asignada a la interfaz externa del firewall, posibilitando la salida a Internet.
Como ejemplo simplificado, la regla en iptables se define de la siguiente manera:

iptables -t nat -A POSTROUTING -o eth_red -s 192.168.20.0/24 -j MASQUERADE

En esta instrucción:

- -t nat indica que la regla pertenece a la tabla de traducción de direcciones. POSTROUTING especifica que la modificación se realiza antes de que el paquete abandone el firewall.
- -o eth_red hace referencia a la interfaz de salida correspondiente a la Zona Red (WAN).
- -s 192.168.20.0/24 define la red de origen, en este caso la LAN.
- MASQUERADE habilita la traducción dinámica de direcciones, utilizando la IP de la interfaz externa.

Esta configuración garantiza que los equipos internos puedan establecer comunicación hacia redes externas sin exponer directamente sus direcciones IP privadas.

NAT para la Zona Orange (DMZ) hacia la Zona Red (WAN)

Se configuró una regla de NAT similar a la aplicada en la LAN, permitiendo que los servidores ubicados en la Zona Orange (DMZ) pudieran establecer conexiones hacia Internet a través de la Zona Red (WAN). Esta configuración resulta necesaria para la descarga de actualizaciones, sincronización de repositorios o consumo de servicios externos.

Mediante esta traducción de direcciones, las IP privadas de la DMZ son enmascaradas utilizando la dirección asignada a la interfaz externa del firewall.

Reenvío de puertos (Port Forwarding)

Con el fin de habilitar el acceso desde Internet a servicios específicos alojados en la DMZ — por ejemplo, un servidor web HTTP que opera en el puerto 80— se implementaron reglas de redirección de puertos (DNAT).

Ejemplo de configuración en iptables:
iptables -t nat -A PREROUTING -i eth_red -p tcp --dport 80 -j DNAT --to-destination 192.168.10.10:80
iptables -A FORWARD -p tcp -d 192.168.10.10 --dport 80 -j ACCEPT

En este caso: la primera regla, ubicada en la cadena PREROUTING de la tabla nat, redirige el tráfico entrante por la interfaz eth_red (WAN) en el puerto 80 hacia el servidor interno ubicado en la IP 192.168.10.10.

La segunda regla, en la cadena FORWARD, permite explícitamente el paso del tráfico hacia el destino configurado.

Esta implementación posibilita la publicación controlada de servicios en la DMZ, manteniendo el aislamiento entre los diferentes segmentos de red y aplicando principios de mínima exposición.

3.3 VERIFICACIÓN Y PRUEBAS

Se llevaron a cabo pruebas de validación de conectividad con el fin de comprobar el correcto funcionamiento de las configuraciones implementadas:

- Desde una estación ubicada en la Zona Green (LAN) se confirmó el acceso a Internet, verificando la correcta aplicación

de las reglas de enrutamiento y NAT de salida.

- Desde la red externa (WAN) se logró acceder al servidor web alojado en la Zona Orange (DMZ) a través del puerto 80, validando la correcta configuración del reenvío de puertos (DNAT).
- Se comprobó que únicamente los puertos explícitamente habilitados se encontraran accesibles desde el exterior, asegurando el cumplimiento de las políticas de filtrado y manteniendo el aislamiento entre segmentos de red.

Estas pruebas permitieron evidenciar la efectividad de la arquitectura perimetral implementada y la adecuada aplicación de los controles de seguridad definidos.

4 PROCEDIMIENTO TEMATICA 3

4.1 DESCRIPCIÓN GENERAL DE LA TEMÁTICA

La Temática 3 se orientó a la habilitación controlada de servicios específicos entre segmentos de red, permitiendo el acceso a los servicios FTP (puerto 21/TCP) y HTTP (puerto 80/TCP) desde la Zona Green (LAN) hacia la Zona Orange (DMZ). En esta última se desplegó una máquina virtual con Ubuntu Server, configurada para operar como servidor web y servidor FTP.

De manera complementaria, se estableció el bloqueo del protocolo ICMP en ambos sentidos (LAN–DMZ y DMZ–LAN), con el propósito de impedir respuestas a solicitudes de eco (ping). Esta medida contribuye a reducir la exposición del entorno ante posibles tareas de reconocimiento de red, fortaleciendo así la postura de seguridad perimetral.

4.2 CONFIGURACIÓN DEL SERVIDOR EN LA DMZ

El servidor Ubuntu ubicado en la Zona Orange (DMZ) fue configurado con direccionamiento IP estático, definiendo los siguientes parámetros de red:

- Dirección IP: 192.168.10.10
- Máscara de subred: 255.255.255.0 (/24)
- Puerta de enlace predeterminada: 192.168.10.1

La configuración se realizó mediante la edición del archivo de Netplan con el siguiente comando:

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

Una vez guardados los cambios, se aplicó la nueva configuración ejecutando: sudo netplan apply

Este procedimiento permitió integrar correctamente el servidor dentro del segmento DMZ y garantizar su comunicación con el firewall configurado como gateway.

4.3 INSTALACIÓN DE SERVICIOS REQUERIDOS EN EL UBUNTU SERVER (SERVIDOR)

Posteriormente, se realizó la actualización del sistema operativo con el fin de garantizar la instalación de paquetes en su versión más reciente y corregir posibles vulnerabilidades:

sudo apt update && sudo apt upgrade -y

Una vez actualizado el servidor, se procedió a la instalación de los servicios web y FTP mediante el siguiente comando:

sudo apt install apache2 vsftpd -y

Tras la instalación, se verificó el estado de los servicios utilizando systemctl, confirmando que se encontraran activos y en ejecución:

systemctl status apache2
systemctl status vsftpd

Esta validación permitió asegurar que tanto el servidor web (Apache2) como el servicio FTP (vsftpd) estuvieran correctamente habilitados dentro de la Zona Orange (DMZ) antes de aplicar las reglas de acceso correspondientes en el firewall.

4.4 CONFIGURACIÓN DE LAS REGLAS EN ENDIAN FIREWALL

4.4.1 PERMITIR TRÁFICO HTTP Y FTP DESDE GREEN → ORANGE

En el módulo Firewall → Trafico de Salida, se crearon las siguientes reglas:

Tabla 1.

Origen	Destino	Servicio	Puerto	Acción
Green	Orange	Http	TCP/ :80	Permitir
Green	Orange	Ftp	TCP/: 21	Permitir

Fuente: autoría propia

Estas reglas fueron aplicadas y definidas en la tabla de tráfico de salida.

4.4.2 BLOQUEO DEL PROTOCOLO ICMP

El requerimiento indica denegar ping (tipo 8) y tipo (30) En el Firewall ENDIAN se configuro de la siguiente manera:

Tabla 2.

Origen	Destino	Servicio	Puerto	Acción
Cualquiera	Cualquiera	ICMP	ICMP/ :8 / :30	Denegar

Fuente: Autoría propia

Esta regla impide realizar ping a cualquier dirección de la red y desde cualquier zona.

4.5 VERIFICACIÓN DE ACCESO A SERVICIOS PERMITIDOS

4.5.1 VALIDACIÓN DEL SERVICIO HTTP DESDE LA LAN

Desde un equipo Ubuntu Desktop en GREEN se ingresó mediante el navegador web a:

http://192.168.10.10/

Figura 1. Validación acceso WEB

Fuente: Autoría propia

Respuesta obtenida: página por defecto de Apache, demostrando acceso correcto.

4.5.2 VALIDACIÓN DEL SERVICIO FTP

Desde la Terminal del equipo desktop (Green) se digitó: ftp 192.168.10.10

Figura 2. Validación conexión FTP

Fuente: Autoría propia

El servicio vsftpd respondio satisfactoriamente a la solicitud de conexión, confirmando la disponibilidad del servicio FTP y validando la correcta conectividad entre los segmentos de red configurados.

4.5.3 VALIDACIÓN DEL BLOQUEO DE ICMP

Desde la Terminal del equipo desktop (Green) se digitó: ping 192.168.10.10

Figura 3. Validación conexión FTP

Fuente: Autoría propia

Se obtuvo como resultado: Destination Host Unreachable

Lo cual confirma que la regla de negación de ICMP funciona correctamente.

5 RESULTADOS

Los resultados obtenidos evidencian que los servicios habilitados operan conforme a lo esperado y que las restricciones implementadas cumplen su función de control y protección. En detalle:

1. El servidor Ubuntu desplegado en la Zona Orange (DMZ), con los servicios Apache2 y vsftpd en ejecución, demostró un funcionamiento adecuado, lo cual fue verificado mediante los comandos systemctl status, confirmando su estado activo.

2. Se validó exitosamente la comunicación de los servicios FTP (21/TCP) y HTTP (80/TCP) desde la Zona Green (LAN) hacia la Zona Orange (DMZ), lo que confirma la correcta creación y aplicación de las reglas de filtrado en el firewall Endian.

3. El bloqueo del protocolo ICMP fue efectivo, ya que no se obtuvieron respuestas a las solicitudes de eco (ping) realizadas desde la LAN hacia la DMZ, reduciendo la posibilidad de reconocimiento de red.

4. La ejecución del procedimiento se ajustó estrictamente a la metodología establecida en la guía de trabajo, priorizando la administración mediante consola, la configuración directa de servicios y la validación funcional sobre la infraestructura implementada en la DMZ.

En conjunto, estos hallazgos confirman la adecuada implementación de los controles de seguridad y la coherencia entre la configuración técnica y los objetivos planteados.

6 CONCLUSIONES

La implementación de una arquitectura de seguridad perimetral mediante Endian Firewall en un entorno virtualizado permitió validar, en un escenario controlado, la efectividad de los mecanismos de segmentación y filtrado en infraestructuras basadas en GNU/Linux. La división de la red en zonas

diferenciadas (LAN, DMZ y WAN) facilitó la aplicación de políticas específicas para cada segmento, asegurando un control detallado del tráfico y una exposición controlada de los servicios publicados.

La configuración de reglas de traducción de direcciones (NAT) y reenvío de puertos demostró la relevancia de establecer criterios de acceso precisos, garantizando la conectividad necesaria sin comprometer la postura de seguridad. Asimismo, la habilitación selectiva de servicios como HTTP y FTP, junto con el bloqueo estratégico del protocolo ICMP, evidenció la importancia de aplicar el principio de mínimo privilegio en la definición de políticas de firewall.

El uso de VirtualBox como plataforma de virtualización resultó fundamental para realizar pruebas, validaciones y ajustes antes de un posible despliegue en producción, reduciendo riesgos operativos y permitiendo la experimentación en un entorno aislado.

En síntesis, la práctica confirma que la planificación estructurada de la red, la segmentación lógica adecuada y la correcta implementación de controles de seguridad constituyen elementos esenciales en la administración de sistemas operativos Open Source, tanto en contextos académicos como en entornos organizacionales.

7 REFERENCIAS

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

[2] Endian Firewall Community. (2023). Manual de usuario y documentación oficial. https://www.endian.com/community

[3] Linux Professional Institute. (2022). Linux Essentials – Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

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

[5] Ubuntu Documentation. (2024). Official Ubuntu Server Guide. https://ubuntu.com/server/docs

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

[7] Install and Configure Endian Firewall on VirtualBox - kifarunix.com. (2019, May 21). Kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/