FORTALECIMIENTO DE LA SEGURIDAD PERIMETRAL: IMPLEMENTACIÓN DE ENDIAN FIREWALL EN UN ENTORNO VIRTUALIZADO CON SEGMENTACIÓN, NAT, REGLAS DE ACCESO Y PROXY HTTP

Jonny Wilmer Lasso Rios
e-mail: jwlassor@unadvirtual.edu.co
Juan Carlos Galindez Torres
e-mail: jcgalindezt@unadvirtual.edu.co
Byron José García Loaiza
e-mail: bjgarcialoaiza@unadvirtual.edu.co
Juan Esteban León Urán
e-mail: jeleonu@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la instalación práctica de Endian Firewall (EFW) en VirtualBox, detallando la configuración de las interfaces correspondientes a las zonas Verde (LAN), Roja (WAN) y Naranja (DMZ), junto con el proceso de instalación del sistema. Se implementó la traducción de direcciones de red (NAT) para proporcionar acceso a Internet tanto a la LAN como a la DMZ, y se definieron reglas de firewall que permiten el tráfico HTTP/FTP desde la DMZ, mientras se bloquea el tráfico ICMP con el fin de reducir la exposición de la red. Asimismo, se configuraron y validaron reglas específicas para el control de tráfico entre las distintas zonas mediante pruebas funcionales. Como resultado, se obtuvo un entorno de red virtual segmentado, funcional y seguro, ideal para fines educativos y de experimentación.*

PALABRAS CLAVE: DMZ, Endian, Firewall, LAN, NAT, Red, Segmentación, Seguridad, WAN, Zonas.

1 INTRODUCCIÓN

En la actualidad, las redes informáticas y su seguridad han pasado de ser un valor añadido a convertirse en una necesidad crítica. Implementar un firewall es equivalente a colocar un guardia en la entrada de una red: controla, supervisa y filtra el tráfico que circula entre el entorno interno y el exterior. En este contexto, Endian Firewall (EFW) se posiciona como una solución robusta y de código abierto, basada en GNU/Linux, orientada a quienes buscan proteger su infraestructura sin recurrir a grandes inversiones ni hardware especializado. Su enfoque accesible lo convierte en una herramienta ideal tanto para entornos de formación como para pequeñas implementaciones reales.

Este artículo ofrece una guía práctica centrada en la instalación y configuración de EFW utilizando VirtualBox como entorno de laboratorio. Esta plataforma de virtualización permite simular escenarios de red reales sin intervenir en infraestructuras físicas, facilitando un entorno controlado para pruebas. La configuración incluye la asignación de adaptadores de red virtuales que representan distintas zonas de seguridad: la zona Verde (LAN), destinada a la red interna; la zona Roja (WAN), que conecta con Internet; y la zona Naranja (DMZ), donde se alojan servicios públicos como servidores web o FTP. Cada zona cumple una función estratégica en el diseño de seguridad perimetral.

Posteriormente, se procede con la instalación de EFW y la activación de funciones clave como el NAT, que permite que tanto los dispositivos de la red interna como los de la DMZ accedan a Internet utilizando la dirección IP pública del firewall. Se definen también políticas precisas de filtrado: se habilitan únicamente los servicios necesarios, como HTTP y FTP, y se bloquean protocolos como ICMP, reduciendo así la exposición a escaneos externos.

Finalmente, se implementan reglas específicas para controlar la comunicación entre las zonas, estableciendo qué tipos de tráfico están permitidos y cuáles deben ser restringidos. De este modo, se construye una red segmentada, segura y funcional, que responde a los principios fundamentales de una arquitectura defensiva moderna.

En el presente artículo se detalla la configuración de un entorno de red segmentado utilizando Endian Firewall como sistema de seguridad perimetral. como temática 3. Se implementaron redes LAN, DMZ y WAN mediante máquinas virtuales, siguiendo las buenas prácticas de seguridad para filtrar servicios entre zonas.

2 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO

2.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX

La implementación del sistema GNU/Linux Endian Firewall (EFW) se realizó dentro del entorno de virtualización Oracle VirtualBox. Inicialmente, se descargó la imagen ISO oficial desde SourceForge [1], y se creó una nueva máquina virtual con 2048 MB de RAM y 1 núcleo de CPU, suficiente para pruebas de laboratorio.

Ilustración 1 Descarga Endian

Fuente: Autoría Propia

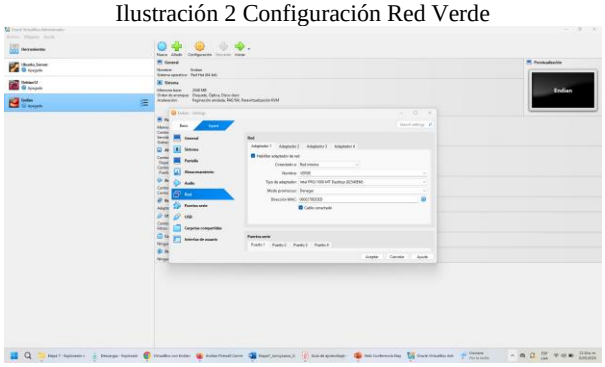
La correcta segmentación de red es fundamental para un entorno seguro. En este caso, se configuraron tres interfaces de red virtuales en la máquina EFW, cada una representando una zona distinta de seguridad. La siguiente tabla resume la configuración realizada:

Tabla 1.

Zona	**Interfaz VirtualBox**	**Tipo de red VirtualBox**	**Rango IP**
Verde (LAN)	Adaptador 1	Red interna	10.0.0.0/24
Naranja (DMZ)	Adaptador 2	Red interna	172.16.0.0/28
Roja (WAN)	Adaptador 3	NAT	Asignada por VirtualBox

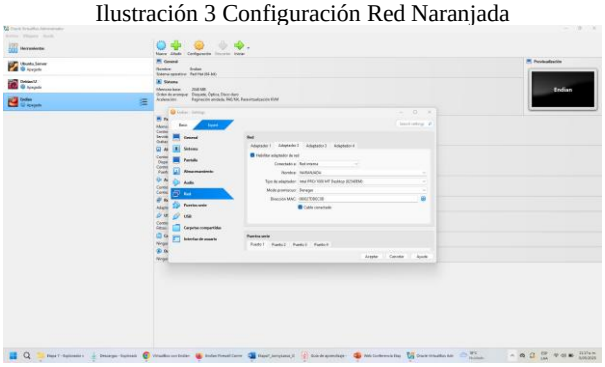
Fuente: Autoría Propia

Ilustración 2 Configuración Red Verde



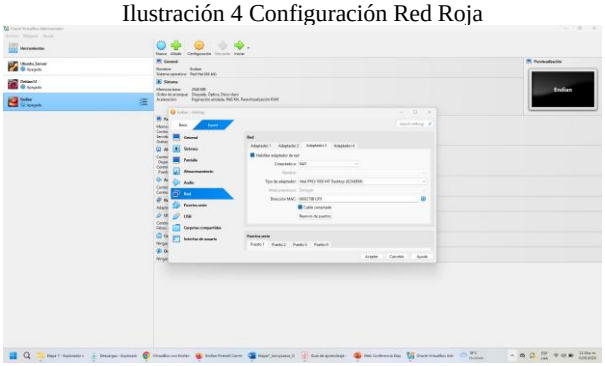
Fuente: Autoría Propia

Ilustración 3 Configuración Red Naranjada



Fuente: Autoría Propia

Ilustración 4 Configuración Red Roja



Fuente: Autoría Propia

Posteriormente, se añadieron dos máquinas virtuales complementarias: un cliente Debian 12 en la red Verde (IP 10.0.0.2) y un servidor Ubuntu en la red Naranja (IP 172.16.0.10). Estas VM facilitaron la validación de la conectividad y el control del tráfico en la red segmentada.

Ilustración 5 Máquinas virtuales

Fuente: Autoría Propia

Además de la creación de las máquinas, se configuró la IP estática en Ubuntu mediante el archivo /etc/netplan/01-netcfg.yaml, lo cual aseguró una conectividad permanente hacia el firewall.

Ilustración 6 IP fija en Ubuntu Server

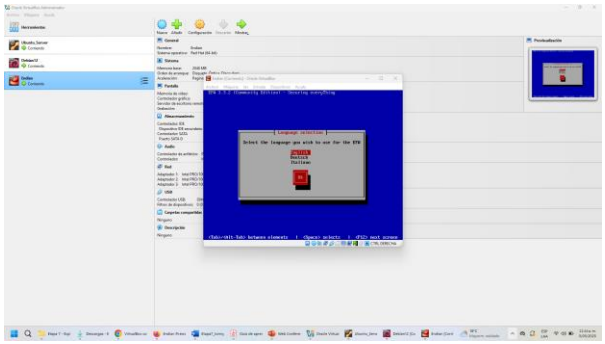
Fuente: Autoría Propia

En Debian, se usó el archivo /etc/network/interfaces para fijar la IP. Estas configuraciones permiten que los entornos se mantengan consistentes incluso después de reinicios.

2.2 INSTALACIÓN EFECTIVA DE ENDIAN Y CONFIGURACIÓN DE LAS ZONAS DE RED

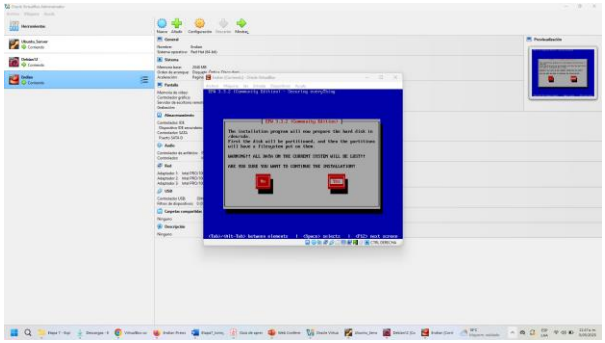
Durante la instalación del firewall, se seleccionó el idioma, se utilizó todo el disco disponible y se habilitó el puerto serial. Al finalizar, el sistema indicó la IP 10.0.0.1 para acceder a la interfaz web de configuración.

Ilustración 7 Idioma en Endian



Fuente: Autoría Propia

Ilustración 8 Almacenamiento Endian

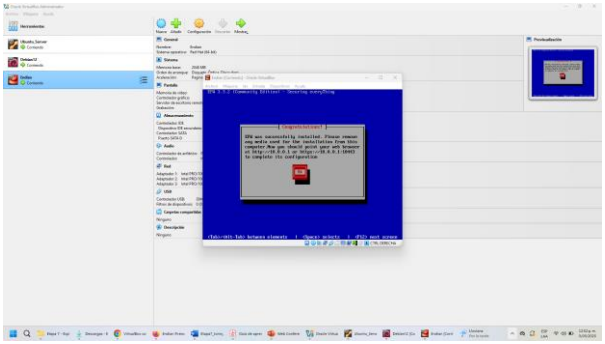


Fuente: Autoría Propia

Ilustración 9 Configuración Endian Red Verde

Fuente: Autoría Propia

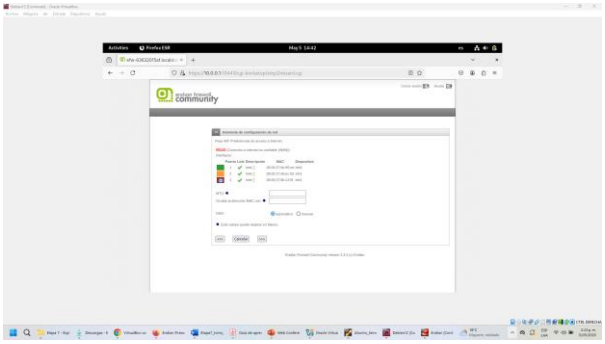
Ilustración 10 Finalización instalación Endian



Fuente: Autoría Propia

A través del asistente web, se configuraron los parámetros esenciales del sistema. Las interfaces se detectaron correctamente como eth0, eth1 y eth2, asignándose a las zonas Verde, Naranja y Roja respectivamente.

Ilustración 11 Interfaces en Endian



Fuente: Autoría Propia

La segmentación IP se estableció conforme a lo mostrado en la tabla 1. Se verificó que las reglas predeterminadas del firewall permitían navegación HTTP/HTTPS desde la LAN, pero bloqueaban ICMP desde la DMZ, como se espera en entornos de producción. La interfaz gráfica permitió configurar políticas de acceso entre zonas usando la sección "Firewall → Tráfico entre zonas", además de reglas de tráfico saliente.

Se realizaron pruebas de conectividad desde Debian y Ubuntu Server mediante los siguientes comandos:

ping 10.0.0.1 # Desde Debian ping 172.16.0.1 # Desde Ubuntu.

Ilustración 12 Ping desde Debian 12

Fuente: Autoría Propia

Ilustración 13 Ping desde Ubuntu Server

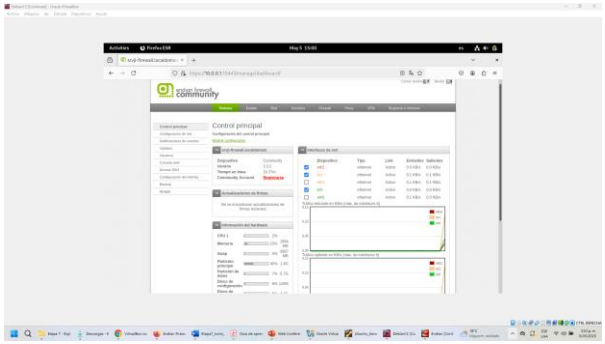
Fuente: Autoría Propia

Este tipo de pruebas permite asegurar que las políticas entre zonas permiten tráfico controlado según lo definido.

2.3 CONTROL Y MONITOREO DE LA RED ENDIAN

La consola de administración de Endian proporciona visibilidad en tiempo real sobre el estado del sistema, incluyendo uso de CPU, RAM, estadísticas de red y usuarios conectados. También permite administrar las reglas del firewall y realizar backups de configuración.

Ilustración 14 Consola de administración Endian

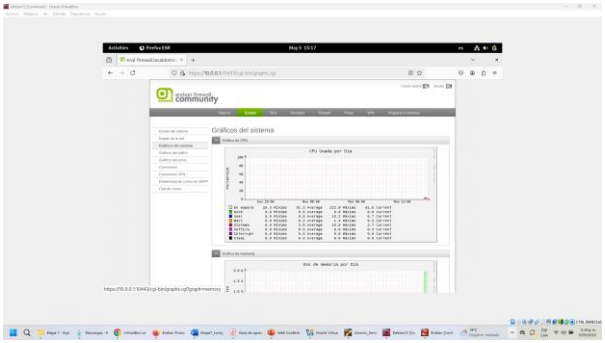


Fuente: Autoría Propia

Finalizada la configuración, se accedió al panel principal de Endian, desde el cual se puede:

- Monitorear todas las interfaces de red activas
- Visualizar estadísticas en tiempo real (uso de CPU, tráfico)
- Administrar usuarios, políticas de seguridad y actualizaciones
- Configurar servicios como proxy, VPN y acceso SSH

Ilustración 15 Gráficos del sistema Endian



Fuente: Autoría Propia

La sección de tráfico entre zonas es especialmente útil para definir reglas que permitan, por ejemplo, solo tráfico HTTP desde DMZ a WAN, pero bloqueen ICMP o acceso desde DMZ a LAN. Esto refuerza el principio de mínimo privilegio.

Además, la posibilidad de integrar filtros de contenido y autenticación de usuarios mediante proxy hace de Endian una solución integral para entornos escolares, universitarios o empresariales con presupuestos reducidos. Se logró implementar una red funcional, segmentada y monitoreada completamente con software libre y recursos de hardware limitados.

3 TEMÁTICA 2: CONFIGURACIÓN NAT

En el entorno de seguridad de redes, la configuración adecuada de NAT (Network Address Translation / Traducción de Direcciones de Red) representa un gran peso para permitir la comunicación controlada entre diferentes zonas de red. A continuación, se explorará la implementación práctica de reglas NAT en un firewall ENDIAN, permitiendo de este modo que tanto dispositivos en la red interna (LAN) como servidores en la zona desmilitarizada (DMZ) Tengan acceso a Internet (Red WAN) de una forma segura, mientras se mantiene un estricto control sobre el tráfico entrante y saliente de las redes.

3.1 ARQUITECTURA DE RED

Tabla 2.

Zona	Interfaz VirtualBox	Tipo de red VirtualBox	Rango IP
Verde (LAN)	Adaptador 1	Red interna	10.0.0.0/24

Naranja (DMZ)	Adaptador 2	Red interna	172.16.0.0/28
Roja (WAN)	Adaptador 3	Red NAT	10.0.2.0/24

Fuente: Autoría Propia

3.2 FUNDAMENTOS DE NAT Y REENVÍO DE PUERTOS

3.2.1 SOURCE NAT (SNAT)

NAT es una técnica fundamental que permite que múltiples dispositivos en una red privada compartan una única conexión a Internet con una dirección IP pública. NAT opera traduciendo las direcciones IP privadas de los dispositivos de la red interna a la dirección IP pública del firewall (o router con funcionalidad NAT) cuando el tráfico sale a Internet, y viceversa cuando el tráfico entrante regresa. Existen principalmente dos tipos de NAT relevantes para este contexto: Source NAT (SNAT) y Destination NAT (DNAT).

3.2.2 SOURCE NAT (SNAT)

También conocido como enmascaramiento, se utiliza para el tráfico que se origina en la red interna (la LAN o la DMZ) y se dirige hacia una red externa como Internet (WAN). Cuando un dispositivo en la red interna envía tráfico a Internet, su dirección IP privada, que no es enrutable en la red pública, se traduce a la dirección IP pública de la interfaz WAN del firewall Endian. Esto hace que parezca que todo el tráfico saliente se origina en el propio firewall, permitiendo que múltiples dispositivos compartan una única dirección IP pública. SNAT es esencial para proporcionar acceso a Internet a los dispositivos en la red privada, ya que enmascara las direcciones IP internas, presentando una dirección IP pública unificada a Internet.

3.2.3 DESTINATION NAT (DNAT)

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

3.2.4 REENVÍO DE PUERTOS

Es un servicio que permite un acceso limitado a las redes LAN internas desde el exterior. El reenvío de puertos es una forma de DNAT que permite que el tráfico de Internet llegue a servicios específicos que se ejecutan en servidores dentro de una red privada. Cuando se configura un reenvío de puertos en un firewall, se define una regla que especifica que el tráfico entrante a una determinada dirección IP pública y puerto debe redirigirse a una dirección IP privada y puertos específicos dentro de la red. Esto es fundamental para exponer servicios como servidores web, servidores de correo electrónico o servidores de juegos alojados en la DMZ o incluso en la LAN (aunque esto último generalmente no se recomienda por razones de seguridad). El reenvío de puertos actúa como una puerta virtual, dirigiendo tipos específicos de tráfico externo al servidor interno apropiado.

3.3 CONFIGURACIÓN DE LA REGLA NAT DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN

El propósito principal de SNAT en Endian es permitir que los dispositivos en la zona LAN (VERDE) accedan a Internet. Ya que las direcciones IP privadas utilizadas dentro de la LAN no son enrutables en la red pública de Internet, es necesario traducir estas direcciones a una dirección IP pública para que la comunicación con servidores externos sea posible. Endian Firewall realiza SNAT reemplazando la dirección IP de origen de los dispositivos en la LAN con su propia dirección IP pública, que está asignada a su interfaz WAN (ROJA), antes de reenviar el tráfico a Internet. Esto hace que parezca que todo el tráfico saliente se origina en el propio dispositivo Endian Firewall.

3.3.1 CONFIGURACION SOURCE NAT (SNAT)

Para configurar reglas de SNAT para el acceso a Internet desde la LAN a través de la interfaz web de Endian, se deben seguir los siguientes pasos:

- Acceder a la interfaz Web de Endian
- Ingresar al menú Firewall
- Dentro del menú "Firewall", seleccionar la opción "Port forwarding / NAT".
- Seleccionar la pestaña "Source NAT"
- Hacer clic en "Add a new source NAT rule": Para crear una nueva regla de SNAT.
- Configurar las opciones comunes:
    - Source or Incoming IP: Este campo define el origen del tráfico al que se aplicará NAT. Para permitir el acceso a Internet desde la LAN, en este caso será la red VERDE.
    - Destination or Target: Este campo define el destino del tráfico. Para el acceso a Internet, generalmente se selecciona la zona ROJA.
    - Service, Port, and Protocol: Estas opciones permiten especificar si la regla de NAT debe aplicarse solo a ciertos tipos de tráfico.
    - Policy: Este campo define la acción que se tomará sobre el tráfico después de que se haya aplicado NAT. Para la NAT de salida, generalmente se desea "Allow" el tráfico.
    - Enabled: Esta casilla debe estar marcada para activar la regla.
    - Remark: Añadir un comentario descriptivo para la regla (por ejemplo, "NAT de salida para la LAN").

Ilustración 16 Menu Firewall – Source NAT

Fuente: Autoría Propia

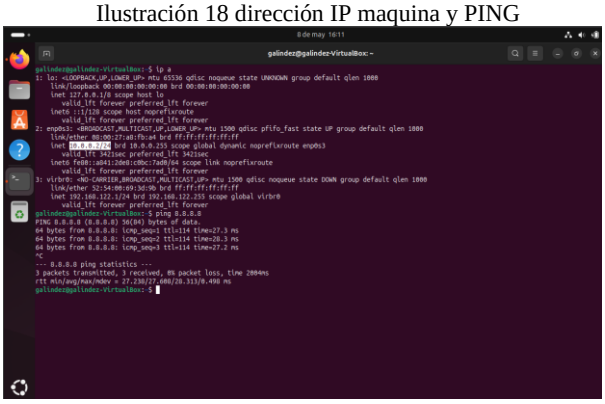
Ilustración 17 Creación Regla Source Nat

Fuente: Autoría Propia

3.3.2 VERIFICACIÓN DE CONEXIÓN Y SALIDA A LA ZONA ROJA DESDE EQUIPO EN LA RED VERDE

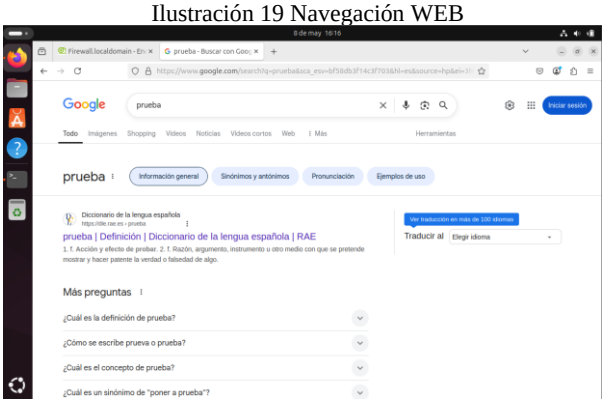
Desde la consola de la maquina se consulta la dirección IP de la máquina para demostrar que se encuentra dentro de la red verde y se realizan pruebas de conexión con PING y navegación en internet.

Ilustración 18 dirección IP maquina y PING



Fuente: Autoría Propia

Ilustración 19 Navegación WEB



Fuente: Autoría Propia

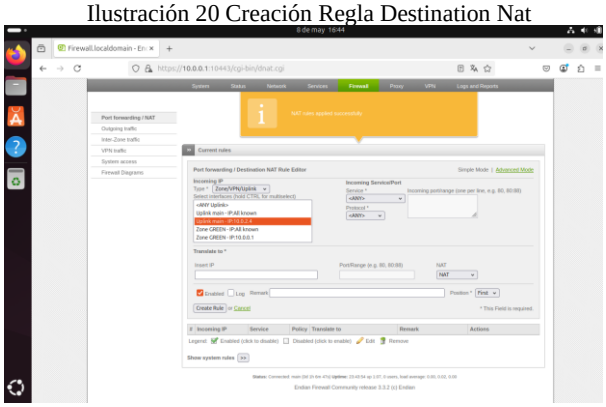
3.4 COMUNICACIÓN DESDE LA DMZ (ZONA NARANJA) HACIA INTERNET

DNAT, es esencial para permitir el acceso externo a servidores ubicados en la zona DMZ (Naranja). Los servidores en la DMZ suelen alojar servicios que deben ser accesibles desde Internet, como servidores web, servidores de correo electrónico o servidores FTP. Dado que estos servidores estan en una red privada con direcciones IP no enrutables públicamente, es necesario configurar reglas de reenvío de puertos en el firewall Endian para dirigir el tráfico entrante desde Internet a estos servidores internos.

3.4.1 CONFIGURACION DESTINATION NAT (DNAT)

- Acceder a la interfaz Web de Endian
- Ingresar al menú Firewall
- Dentro del menú "Firewall", seleccionar la opción "Port forwarding / Destination NAT".
- Hacer clic en "Add a new source NAT rule": Para crear una nueva regla de DNAT.
- Configurar las opciones comunes:
    - Incoming IP: Seleccionar "Zone/VPN/Uplink" del menú desplegable y luego elegir la red con la dirección IP de la red ROJA.
    - Service, Port, and Protocol: Definir el servicio al que se desea permitir el acceso externo. Se puede elegir un servicio predefinido del menú desplegable "Service" que establecerá automáticamente el puerto y el protocolo.
    - Policy: Elegir la acción que se tomará sobre los paquetes coincidentes. Para el acceso externo, generalmente se selecciona Allow para permitir que el tráfico pase.
    - Remark: Añadir un comentario descriptivo para la regla ("Reenviar HTTP al servidor web de la DMZ").
    - Position: Elegir la posición donde se debe colocar esta regla en la lista de reglas de firewall. Las reglas se procesan de arriba a abajo y se aplica la primera regla coincidente.

Ilustración 20 Creación Regla Destination Nat

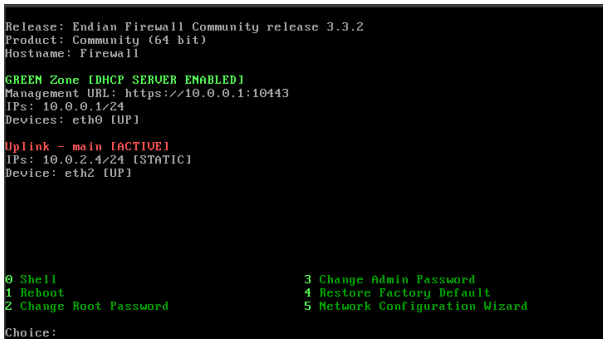


Fuente: Autoría Propia

3.4.2 VERIFICACIÓN DE CONEXIÓN Y SALIDA A LA ZONA ROJA DESDE EQUIPO EN LA RED NARANJA (DMZ)

Se ingresa a la Máquina Virtual de ENDIAN y se verifican las direcciones ip de cada red

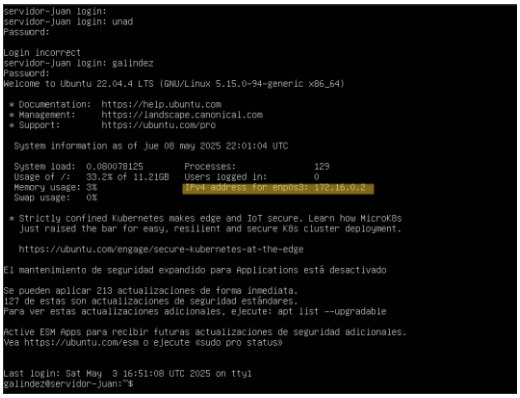
Ilustración 21 Verificación De direcciones IP redes VERDE y ROJA ENDIAN



Fuente: Autoría Propia

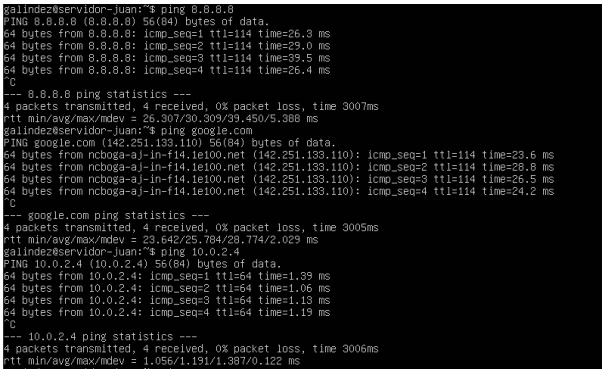
Se ingresa al servidor, se realiza consulta de la dirección IP de este y se hacen pruebas de conexión a internet desde el servidor.

Ilustración 22 Verificación IP Servidor



Fuente: Autoría Propia

Ilustración 23 Verificación Conexión a internet



Fuente: Autoría Propia

La correcta configuración de NAT y el reenvío de puertos en Endian es importante, para establecer un acceso seguro y controlado a los servicios de Internet para los equipos de la red interna y los servidores ubicados en la DMZ. Comprender la arquitectura de zonas de Endian Firewall, así como los fundamentos de SNAT y DNAT, es el primer paso para una implementación exitosa.

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

Como parte de la formación práctica en Administración de Servicios en Red, se desarrolló una serie de actividades para familiarizarse con la configuración de redes segmentadas y la aplicación de reglas de seguridad mediante herramientas basadas en GNU/Linux. Se llevó a cabo la configuración de una red segmentada utilizando el firewall Endian, abarcando desde la instalación del sistema hasta la validación de servicios permitidos y restringidos entre zonas.

4.1 IMPLEMENTACIÓN DE ENDIAN FIREWALL

4.1.1 CREACIÓN DE LA MÁQUINA VIRTUAL ENDIAN

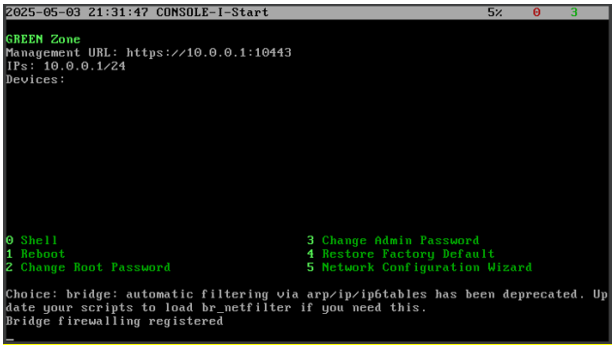
Se utilizó VirtualBox para crear la máquina virtual endian_byron, configurada con sistema operativo Linux (64-bit), 1024 MB de RAM y disco duro VDI de 4 GB. Se asignaron tres adaptadores de red:

1. Adaptador 1: red interna llamada LAN
2. Adaptador 2: red interna llamada DMZ
3. Adaptador 3: modo NAT para salida a Internet

4.1.2 INSTALACIÓN DEL SISTEMA ENDIAN FIREWALL

Se montó la ISO EFW-COMMUNITY-3.3.2.iso en la VM y se procedió con la instalación. Durante la configuración inicial, se asignó la zona verde con IP estática 10.0.0.1/24. Luego se accedió a la interfaz gráfica desde un navegador en una máquina cliente LAN.

Ilustración 24 Endian Firewall instalado.



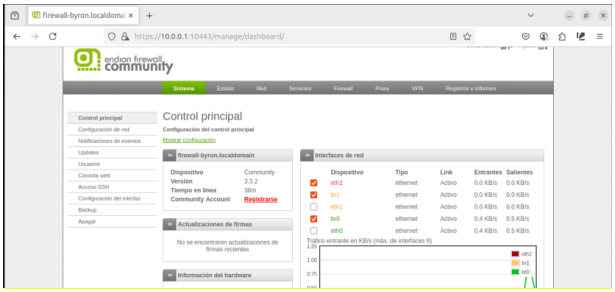
Fuente: Autoría Propia

4.1.3 ACCESO AL DASHBOARD Y CONFIGURACIÓN BÁSICA

Desde el navegador de una máquina cliente (con IP 10.0.0.2), se accedió a la dirección https://10.0.0.1 para iniciar sesión en el dashboard de Endian. Se completó el asistente de configuración inicial, se estableció zona roja como ETH02, zona verde como ETH00 y zona naranja como ETH01. Se configuraron las interfaces con IPs:

1. Verde: 10.0.0.1/24
2. Naranja: 172.16.0.1/24
3. Roja: automática por DHCP

Ilustración 25 Acceso a dashboard.



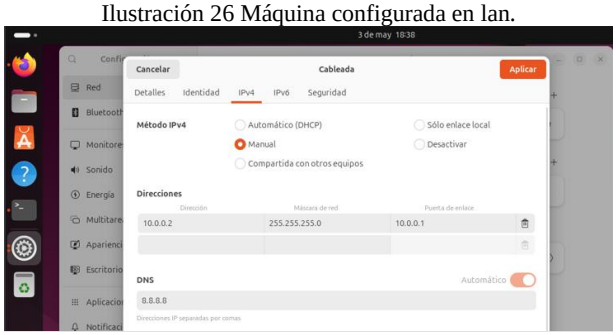
Fuente: Autoría Propia

4.1.4 CREACIÓN DE CLIENTES LAN Y DMZ

Se crearon dos nuevas VMs:

1. cliente_lan con IP 10.0.0.2, red interna LAN
2. cliente_dmz con IP 172.16.0.2, red interna DMZ
3. Ambas sin ISO, utilizando Ubuntu Server previamente instalado.

Ilustración 26 Máquina configurada en lan.



Fuente: Autoría Propia

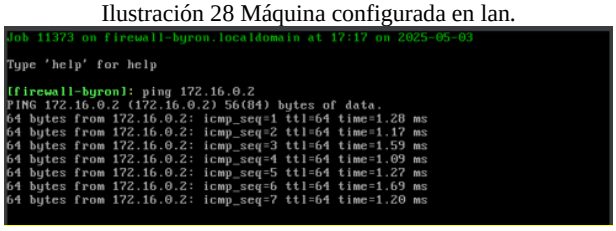
Ilustración 27 Máquina configurada en dmz.

Fuente: Autoría Propia

4.1.5 PRUEBAS DE CONECTIVIDAD

Se realizaron pings exitosos:
Desde endian_byron:
ping 172.16.0.2 (servidor byron3)

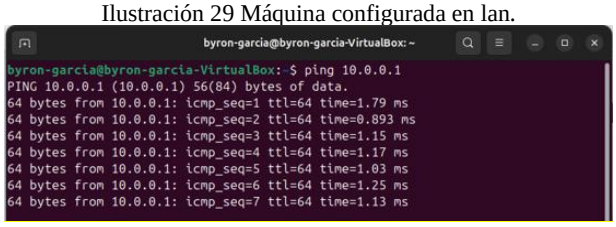
Ilustración 28 Máquina configurada en lan.



Fuente: Autoría Propia

Desde Byron_Garcia:
ping 10.0.0.1 (endian_byron)

Ilustración 29 Máquina configurada en lan.



Fuente: Autoría Propia

4.1.6 REGLAS DE FIREWALL Y FILTRADO DE SERVICIOS

Se activaron o bloquearon servicios específicos como HTTP, FTP y ICMP para ciertas zonas. Luego se probaron accesos:

Ilustración 30 Máquina configurada en lan.

Fuente: Autoría Propia

Regla 1: HTTP desde DMZ a LAN
Regla 2: FTP desde DMZ a LAN

Ilustración 31 Máquina configurada en lan.

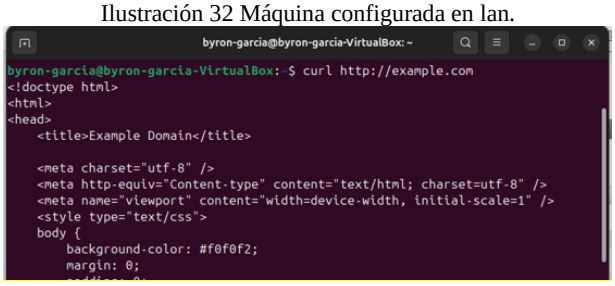
Fuente: Autoría Propia

Regla 3: Bloqueo ICMP (Ping)

4.2 PRUEBAS REALIZADAS PARA CADA REGLA

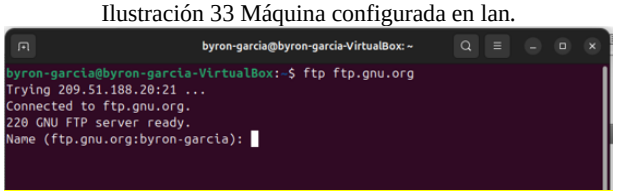
1. Desde Byron_Garcia: Regla 1: HTTP

Ilustración 32 Máquina configurada en lan.



Fuente: Autoría Propia

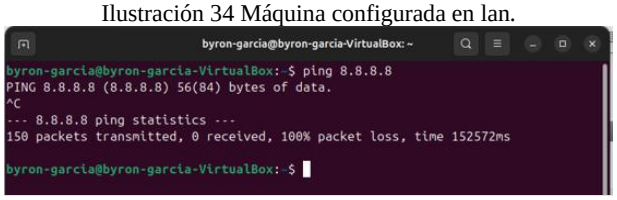
2. Desde Byron_Garcia: Regla 2: FTP
Ilustración 33 Máquina configurada en lan.



Fuente: Autoría Propia

3. Desde Byron_Garcia: Regla 3: Bloqueo ICMP

Ilustración 34 Máquina configurada en lan.



Fuente: Autoría Propia

4.3 RESULTADOS TEMÁTICA 3

La implementación permitió validar el aislamiento de zonas de red mediante el firewall. El acceso al dashboard solo fue posible desde la LAN, y se pudo controlar qué servicios se permiten entre zonas, simulando un entorno real con zona desmilitarizada y redes seguras internas.

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

5.1 INFRAESTRUCTURA DE RED CONFIGURADA

Para la implementación de la temática 5 la cual consiste en la configuración de un proxy HTTP no transparente con políticas de autenticación y filtrado de contenidos se estableció una infraestructura de red utilizando tres máquinas virtuales sobre VirtualBox, cada una configurada con un tipo de red interna específica para simular un entorno perimetral de seguridad basado en zonas LAN, DMZ y firewall. Las máquinas y sus configuraciones de red son las siguientes:

Ubuntu Desktop (Zona Verde - LAN):
Tipo de red: Red interna (internet) llamada verde.
Dirección IP: 10.0.0.2
Máscara de subred: 255.255.255.0

Esta máquina representa el cliente de red desde donde se accede a Internet a través del proxy configurado.

Endian Firewall:
Zona Verde (LAN):
Tipo de red: Red interna llamada verde.
Dirección IP: 10.0.0.1
Zona Naranja (DMZ):

Tipo de red: Red interna llamada naranja.
Dirección IP: 172.16.0.2
Endian actúa como cortafuegos entre la LAN y la DMZ, y aloja el servicio de proxy HTTP con filtrado de contenidos y autenticación.
Ubuntu Server (Zona Naranja - DMZ):
Tipo de red: Red interna llamada naranja.
Dirección IP: 172.16.0.1
Máscara de subred: 255.255.255.240

Esta máquina representa un servidor en la zona DMZ, accesible solo desde la red controlada por el firewall.

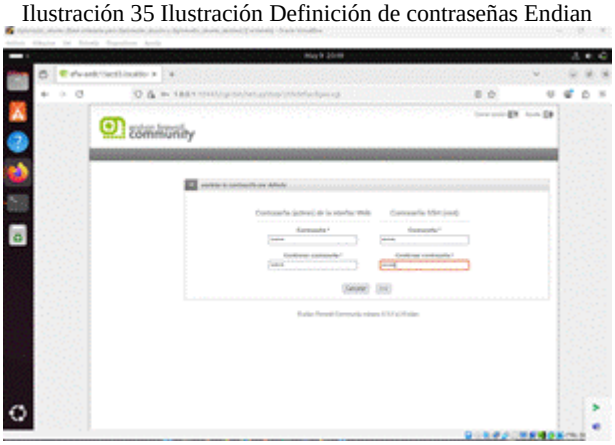
Esta configuración permite simular un entorno seguro con políticas de acceso controladas, en el cual el tráfico entre la LAN y el exterior debe pasar obligatoriamente por el firewall (Endian), quien actúa como proxy de salida.

5.2 CONFIGURACIÓN DE ENDIAN.

Una vez finalizada la configuración básica de las máquinas virtuales (Ubuntu Desktop y Ubuntu Server), se procede a la instalación y configuración inicial de Endian Firewall, accediendo a su interfaz web desde Ubuntu Desktop mediante la dirección https://10.0.0.1:10443. A través del asistente de configuración, se definen los parámetros esenciales de red para el funcionamiento del firewall perimetral.

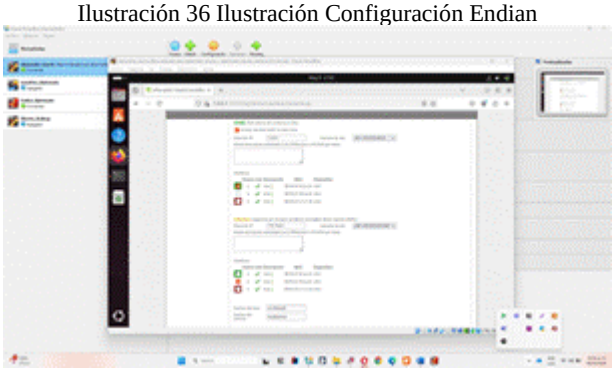
Durante este proceso, se asignan las interfaces correspondientes a las zonas Verde (LAN) y Naranja (DMZ), estableciendo sus respectivas direcciones IP previamente planificadas: 10.0.0.1 para la zona verde y 172.16.0.2 para la zona naranja. Asimismo, se define un nombre de host identificador para el sistema Endian dentro de la red, y se establece una contraseña de acceso para el usuario administrador (admin), garantizando así un acceso seguro a la consola de administración.

Ilustración 35 Ilustración Definición de contraseñas Endian



Fuente: Autoría Propia

Ilustración 36 Ilustración Configuración Endian



Fuente: Autoría Propia

Ilustración 37 Ilustración Configuración Endian

Fuente: Autoría Propia

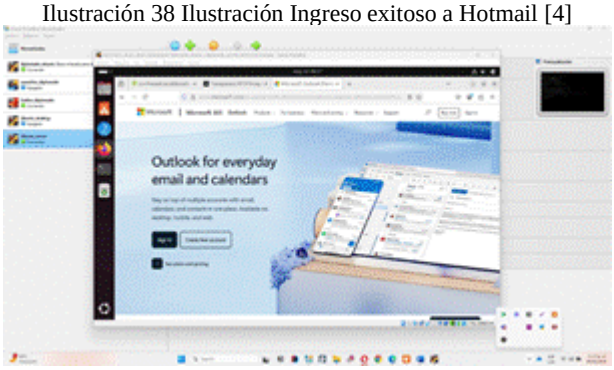
5.3 IMPLEMENTACIÓN DE PROXY HTTP CON AUTENTICACIÓN Y FILTRO DE NAVEGACIÓN

Una vez configurado el entorno de red con las zonas Verde (LAN) y Naranja (DMZ), se procede con la implementación del proxy HTTP no transparente a través de la interfaz de administración web de Endian Firewall (EFW). Esta etapa tiene como propósito aplicar restricciones de navegación mediante autenticación de usuarios y políticas de filtrado.

Como primer paso, se realizó una prueba de acceso desde el navegador web en la máquina Ubuntu Desktop para comprobar que era posible ingresar a los sitios web que más adelante serían bloqueados. Se confirmó el acceso exitoso a:

- www.hotmail.com [4]
- www.elnuevodia.com.co [5]

Ilustración 38 Ilustración Ingreso exitoso a Hotmail [4]



Fuente: Autoría Propia

Ilustración 39 Ilustración Ingreso exitoso a el nuevo día [5]

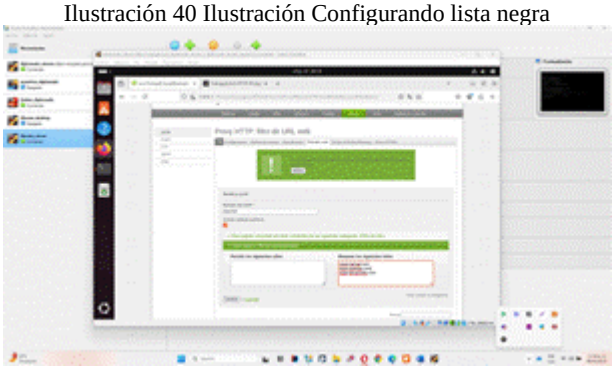
Fuente: Autoría Propia

5.4 CREACIÓN DEL PERFIL DE FILTRADO WEB

Desde el menú Proxy > HTTP > Filtrado Web, se creó un nuevo perfil de filtrado llamado "blacklist". Este perfil contiene una lista negra que bloquea el acceso a los siguientes sitios:

- www.hotmail.com [4]
- www.elnuevodia.com [5]
- www.youtube.com [6]

Ilustración 40 Ilustración Configurando lista negra

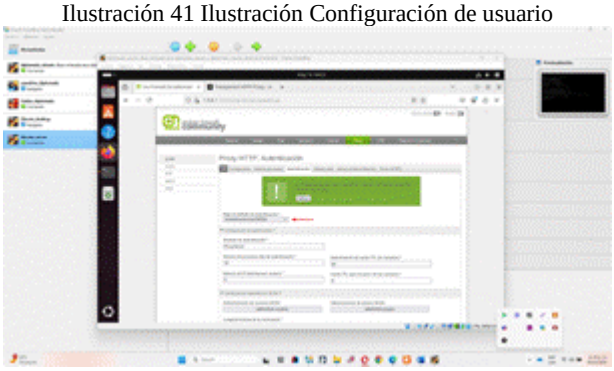


Fuente: Autoría Propia

Posteriormente, se definió el método de autenticación "en base a un usuario". Para ello:

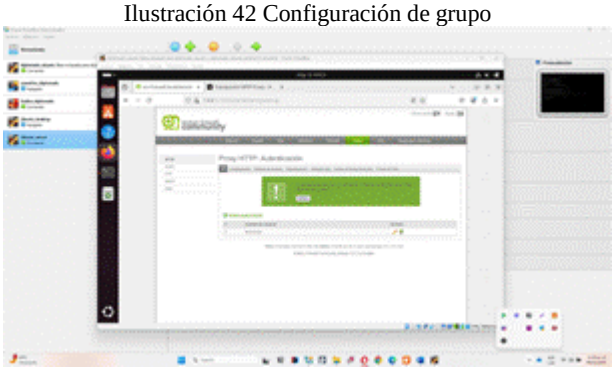
- Se creó un nuevo usuario llamado leonuranje.
- Se creó un grupo de usuarios llamado endian.
- El usuario leonuranje fue asociado a este grupo.

Ilustración 41 Ilustración Configuración de usuario



Fuente: Autoría Propia

Ilustración 42 Configuración de grupo



Fuente: Autoría Propia

Finalmente, se configuró una política de acceso que vincula todos los elementos anteriores:

- Se seleccionó autenticación en base a un usuario.
- Se seleccionó el usuario leonuranje.
- Se permitió el acceso bajo esta política.
- Se aplicó el perfil de filtrado "blacklist" como política de contenido web.

Después de guardar los cambios, el sistema mostró un mensaje indicando que la configuración del proxy había sido modificada, por lo que se hizo clic en "Aplicar" para que los cambios entraran en vigencia.

Ilustración 43 Creación de políticas de acceso

Fuente: Autoría Propia

Ilustración 44 Creación de registro políticas de acceso

#	Política	Origen	Destino	Grupo de autenticación/ usuario	Cuándo	Agente de usuario	Actions
1	filter using 'blacklist'	CUALQUIERA	CUALQUIERA	leonuranje	Siempre	CUALQUIERA	

Fuente: Autoría Propia

Como resultado, el sistema denegó el acceso a estas páginas, mostrando un time out por el bloqueo generado por las políticas de contenido web definido en el perfil "blacklist".

Ilustración 45 Pruebas de bloqueo

Fuente: Autoría Propia

6 CONCLUSIONES

6.1 TEMATICA 1

La implementación de Endian Firewall en VirtualBox permitió establecer un entorno virtual de red segmentado y funcional, emulando una infraestructura de seguridad perimetral con zonas Verde, Roja y Naranja. Esta segmentación favorece la administración del tráfico y la mitigación de riesgos, alineándose con los principios modernos de ciberseguridad.

Las configuraciones aplicadas, como la asignación de IPs fijas, el uso de NAT y las políticas de firewall, demostraron la versatilidad de Endian para entornos educativos o de pequeñas organizaciones. Además, la posibilidad de gestionar todo el sistema desde una consola web centralizada mejora notablemente la experiencia de administración.

6.2 TEMATICA 2

La correcta configuración de NAT y el reenvío de puertos en Endian es importante, para establecer un acceso seguro y controlado a los servicios de Internet para los equipos de la red interna y los servidores ubicados en la DMZ. Comprender la arquitectura de zonas de Endian Firewall, así como los fundamentos de SNAT y DNAT, es el primer paso para una implementación exitosa. La interfaz web de Endian proporciona las herramientas necesarias para configurar estas funcionalidades, ya sea a través del modo simple para tareas básicas o del modo avanzado para escenarios más complejos que requieren un control más granular.

Es de suma importancia aplicar el principio de mínimo privilegio al configurar las reglas de reenvío de puertos, limitando el acceso por direcciones IP de origen cuando sea posible y asegurando que las políticas de firewall complementen las reglas de NAT para una protección integral. La seguridad de los servidores en la DMZ es igualmente importante, requiriendo una gestión proactiva de parches y la implementación de medidas de seguridad adicionales a nivel de host.

6.3 TEMÁTICA 3

La configuración de Endian Firewall en un entorno virtualizado permite comprender de forma práctica el funcionamiento de un firewall perimetral, las zonas de red y la aplicación de reglas de seguridad específicas. Además, facilita la transición hacia infraestructuras seguras basadas en software libre. Junto al estudio de los fundamentos Linux con LPI, esta experiencia fortalece competencias clave en administración de redes y servicios en entornos corporativos.

6.4 TEMÁTICA 5

La configuración del servicio proxy con filtrado web en Endian permitió implementar de manera efectiva políticas de restricción de acceso a sitios específicos mediante el uso de perfiles personalizados y autenticación de usuarios. A través de la creación de una lista negra y su asociación a un grupo y usuario específico, se logró un control detallado del tráfico web desde la red interna, evidenciando cómo una herramienta de firewall y proxy puede fortalecer la seguridad y administración del acceso a Internet en entornos educativos o empresariales.

7 REFERENCIAS

[1] Endian Team. (s.f.). *Endian Firewall Community (Versión 3.3.2) [Software de código abierto]*. SourceForge. https://sourceforge.net/projects/efw/

[2] *Outbound NAT | PFSense Documentation*. (s. f.). https://docs.netgate.com/pfsense/en/latest/nat/outbound.html

[3] *Port forwarding / NAT — Endian UTM 3.2 Reference Manual*. (s. f.). https://docs.endian.com/3.2/utm/firewall/dnat.html

[4] Microsoft Corporation, "Hotmail," Outlook Live, [En línea]: https://www.hotmail.com.

[5] Editorial Aguasclaras S.A., "El Nuevo Día," El Nuevo Día, [En línea]: https://www.elnuevodia.com.co.

[6] YouTube, "YouTube," YouTube, [En línea]: https://www.youtube.com.

[7] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix . https://learning.lpi.org/es/learning-materials/101-500/102/

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

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

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

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