“IMPLEMENTACIÓN DE UNA ARQUITECTURA SEGURA DE RED LAN, DMZ Y WAN MEDIANTE GNU/LINUX FIREWALL EN ENTORNOS VIRTUALIZADOS “

John Fernando Mantilla Hernandez
Johnfmantillah@unadvirtual.edu.co
Carlos Sneyder Diaz Valderrama
csdiazv@unadvirtual.edu.co
Jesus Alberto Leon Salazar
jaleons@unadvirtual.edu.co
Francisco Javier Perez Solano
fjperezs@unadvirtual.edu.co
Jhon Anderson Lipez Esteban
jalipeze@unadvirtual.edu.co

RESUMEN: *Este proyecto presenta la implementación de una arquitectura de red segura basada en la distribución GNU/Linux Endian Firewall (EFW), configurada en un entorno virtualizado mediante VirtualBox. La solución integra tres zonas fundamentales: la red interna (LAN – Zona Verde), la zona desmilitarizada (DMZ – Zona Naranja) destinada a servidores, y la red externa (WAN – Zona Roja). Se desarrollan cinco temáticas orientadas a la configuración de la instancia, traducción de direcciones (NAT), gestión de servicios en DMZ, reglas de acceso interzona y la implementación de un proxy con autenticación. El propósito es fortalecer las capacidades de administración de seguridad perimetral, aplicando buenas prácticas y verificando el funcionamiento correcto de los servicios y políticas establecidas bajo un enfoque académico y profesional.*

PALABRAS CLAVE: Endian Firewall (EFW), Seguridad, DMZ, NAT, Proxy HTTP, Distribución de Linux, Virtualización..

1 INTRODUCCIÓN

La protección de la infraestructura tecnológica es un aspecto fundamental en cualquier organización que administre datos sensibles, aplicaciones críticas o servidores internos conectados a redes abiertas o externas. En el contexto del Diplomado de profundización en administración de sistemas operativos Open Source con certificación en Linux, se plantea como actividad final la implementación de un entorno seguro utilizando la distribución Endian Firewall (EFW). Esta plataforma de seguridad permitirá gestionar el tráfico entre la red interna (LAN), la zona desmilitarizada (DMZ) destinada a servidores, y la red externa (WAN), estableciendo políticas de control, filtrado y protección.

Esta actividad busca que cada integrante del grupo configure, desde un entorno virtualizado, las zonas Verde, Roja y Naranja de Endian, y además seleccione y desarrolle una de las cinco temáticas propuestas: configuración de la instancia, NAT, acceso a servicios en DMZ, reglas interzona y la implementación de un proxy con autenticación. El propósito es comprender a fondo el funcionamiento de un firewall perimetral profesional, sus políticas de red y las técnicas de protección en redes heterogéneas.

2 OBJETIVO GENERAL

Implementar una arquitectura de red segura utilizando Endian Firewall en un entorno virtualizado, configurando las zonas LAN, DMZ y WAN, y aplicando reglas de seguridad, NAT, acceso a servicios y autenticación para controlar el tráfico entre redes.

2.1 OBJETIVOS ESPECIFICOS

Configurar correctamente la instancia de Endian en VirtualBox con tarjetas de red para las zonas Verde, Roja y Naranja.

Implementar reglas NAT que permitan la comunicación controlada entre LAN, DMZ y WAN.

Habilitar y restringir servicios específicos en la zona DMZ, como HTTP y FTP, y bloquear ICMP.

Definir reglas de acceso interzona para permitir y denegar tráfico según políticas establecidas.

Implementar un Proxy HTTP no transparente con autenticación y listas negras para controlar la navegación.

3 DESARROLLO DE LA ACTIVIDAD

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

Integrante 1 John Fernando Mantilla Hernandez

Producto esperado:

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

3.1.1 DESARROLLO METODOLÓGICO

Se realizó la instalación de GNU/Linux Endian en VirtualBox, configurando tres adaptadores de red para simular tres zonas de seguridad:

- Zona Verde (LAN): Red interna para los usuarios.
- Zona Roja (WAN): Acceso simulado a Internet.
- Zona Naranja (DMZ): Red de servidores que requieren acceso controlado desde LAN e Internet.

3.1.2 TEMÁTICAS Y RESULTADOS

Se realizó la instalación de GNU/Linux Endian en VirtualBox, configurando tres adaptadores de red para simular tres zonas de seguridad:

- Zona Verde (LAN): Red interna para los usuarios.
- Zona Roja (WAN): Acceso simulado a Internet.
- Zona Naranja (DMZ): Red de servidores que requieren acceso controlado desde LAN e Internet.

A. Temática 1: Configuración de la instancia en VirtualBox

Procedimiento:

- Crear una máquina virtual para Endian en VirtualBox.

1. Instalación de VirtualBox

- Ingresar al sitio oficial: https://www.virtualbox.org
- Seleccionar Downloads.
- Escoger la versión para tu sistema operativo (Windows, Linux o macOS).
- Ejecutar el instalador descargado.
- Avanzar con la instalación predeterminada marcando:
  VirtualBox Application
  VirtualBox USB Support
  VirtualBox Networking
- Finalizar la instalación y abrir VirtualBox

2. Creación y configuración de la máquina virtual para Endian Firewall

Crear la VM

- Clic en Nueva.
- Nombre: Endian Firewall
- Tipo: Linux
- Versión: Other Linux (32-bit o 64-bit) según la ISO.
- Asignar memoria: 2 GB mínimo, recomendado 4 GB.
- Crear disco duro virtual: 20 GB tipo VDI, almacenamiento dinámico.

Agregar la ISO de Endian

- En la VM → Configuración.
- Ir a Almacenamiento.
- En “Controlador IDE”, seleccionar “Vacío”.
- Cargar la ISO de Endian descargada desde:
- https://www.endian.com/en/community/
- Aceptar

Configurar las tres tarjetas de red

Endian requiere 3 adaptadores para RED, GREEN y ORANGE.

A. Adaptador 1 Zona ROJA (WAN)

- Habilitar adaptador.
- Modo: NAT (o Adaptador Puente).
- Interfaz en Endian: eth0

B. Adaptador 2 Zona VERDE (LAN)

- Modo: Red interna
- Nombre: LAN_GREEN
- Interfaz en Endian: eth1
- IP sugerida: 192.168.10.1/24

C. Adaptador 3 Zona NARANJA (DMZ)

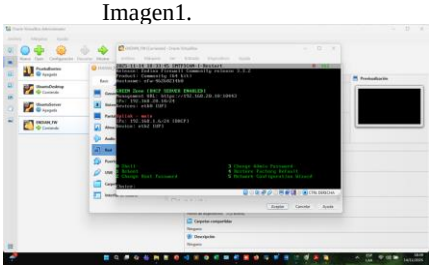
- Modo: Red interna
- Nombre: DMZ_ORANGE
- Interfaz en Endian: eth2
- IP sugerida: 192.168.20.1/24

3. Instalación de Endian Firewall

- Iniciar la máquina virtual.
- Seleccionar Install Endian.

- Aceptar licencia.
- Elegir disco para instalar.
- Configurar las zonas:
    - RED → eth0
    - GREEN → eth1
    - ORANGE → eth2
    - Asignar IPs:
    ○ GREEN: 192.168.10.1/24
    ○ ORANGE: 192.168.20.1/24
    ○ RED: automática por DHCP (si usas NAT)
    - Completar la instalación.Asignar IPs:
    - Al finalizar, Endian mostrará:
    ○ Su IP GREEN para administración web
    ○ Credenciales por defecto.

Imagen1.



Fuente: Autoria Propia

Acceso Web

Desde un navegador en la zona GREEN:

- URL: https://192.168.10.1:10443
- Usuario: admin
- Contraseña

4. Creación de la máquina virtual Ubuntu Desktop (cliente LAN)

A. Crear la VM

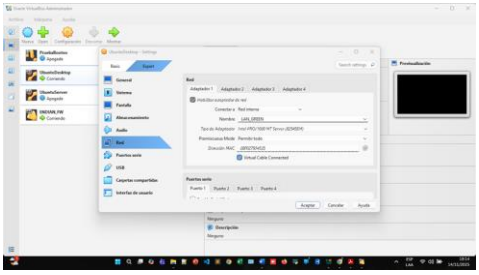
- Clic en Nueva.
- Nombre: Ubuntu Desktop.
- Tipo: Linux.
- Versión: Ubuntu (64-bit).
- Memoria: 2 – 4 GB.
- Disco duro: 20 GB.

B. Configurar el adaptador de red

Para que Ubuntu quede en la zona GREEN:

- **Adaptador 1 → Red interna**
- Nombre: **LAN_GREEN**

Imagen2.



Fuente: Autoria Propia

C. Agregar la ISO de Ubuntu

- Configuración → Almacenamiento.
- Montar ISO de Ubuntu Desktop.
- Iniciar e instalar normalmente.

5. Pruebas de Conectividad

A. Comprobar IP en Ubuntu

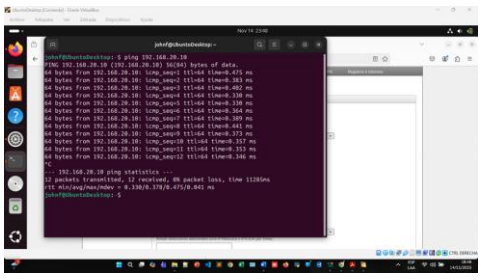
- En Ubuntu abrir una terminal:
- ip a

B. Probar conexión con Endian (zona GREEN)Comprobar IP en Ubuntu

ping 192.168.10.1

ping 192.168.20.1

Imagen3.



Fuente: Autoría Propia

Debe responder.

C. Probar salida a Internet

ping 8.8.8.8

D. Probar navegación

Abrir Firefox y cargar cualquier página

Resultados:

- La máquina Endian se inició correctamente.
- Cada zona obtuvo conectividad interna.

Se identificaron los interfaces y se asignaron correctamente los roles de Red Verde, Roja y Naranja

3.2 TEMÁTICA 2: CONFIGURACIÓN NAT.

Integrante 2 Carlos Sneyder Diaz Valderrama

Abstract—Este artıculo presenta la implementación práctica de un firewall perimetral basado en Endian Firewall Community 3.3, configurando tres zonas de red (RED, GREEN y ORANGE/DMZ) con traducción de direcciones (NAT) de origen para ambas redes internas. Se demuestra el aislamiento entre zonas y el acceso controlado a Internet desde la DMZ mediante reglas de firewall expl´ıcitas. Index Terms—Endian Firewall, NAT, DMZ, zonas de red, seguridad perimetral, firewall de código abierto

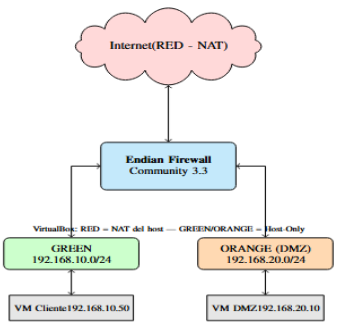
3.2.1 INTRODUCCION

En entornos reales las organizaciones requieren separar sus redes internas (LAN) de los servidores accesibles desde Internet (DMZ). Este trabajo implementa dicha arquitectura utilizando Endian Firewall Community como firewall perime-tral, configurando:

- Zona RED (Internet - NAT del host)
- Zona GREEN (LAN interna – 192.168.10.0/24)
- Zona ORANGE (DMZ – 192.168.20.0/24)

3.2.2 ARQUITECTURA DE RED PROPUESTA

Diagrama1.



Fuente: Autoria Propia

3.2.3 CONFIGURACIÓN DEL ENTORNO

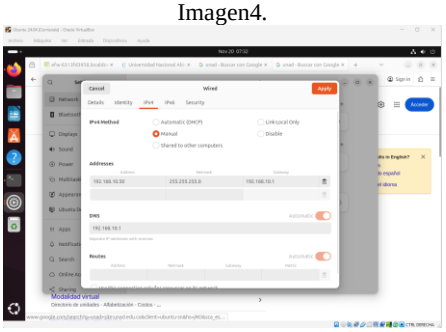
A. Configuración de interfaces en Endian Firewall

- RED: NAT (salida a Internet del host)
- GREEN: 192.168.10.1/24
- ORANGE: 192.168.20.1/24

B. Configuración de máquinas cliente

- Cliente LAN (GREEN): 192.168.10.50/24, gateway 192.168.10.1

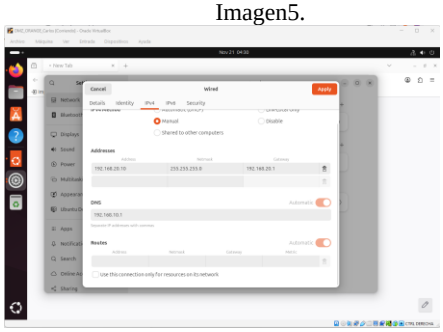
Imagen4.



Fuente: Autoría propia

- Servidor DMZ (ORANGE): 192.168.20.10/24, gateway 192.168.20.1

Imagen5.



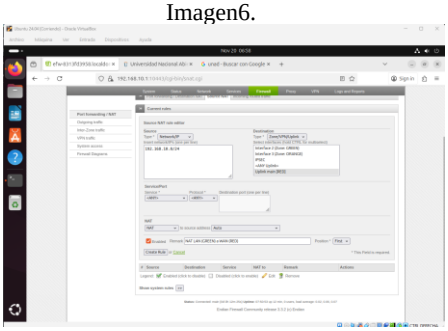
Fuente: Autoría propia

3.2.4 NAT Y POLÍTICAS DE ACCESO

A. NAT de origen (SNAT)

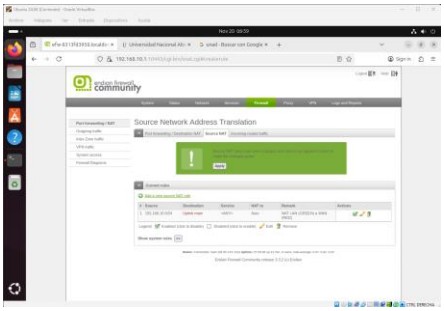
- Se configuraron dos reglas SNAT para ambas redes internas.

Imagen6.



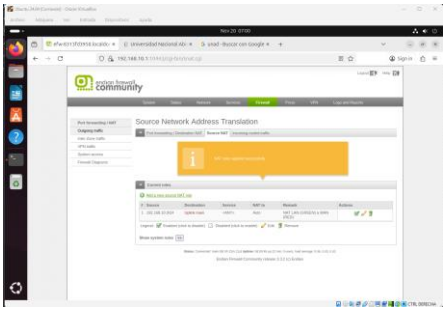
Fuente: Autoría propia

Imagen7.



Fuente: Autoría propia

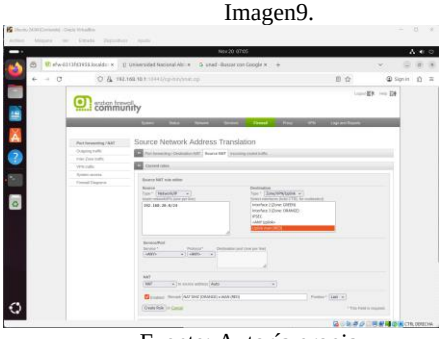
Imagen8.



Fuente: Autoría propia

B. Reglas de salida desde ORANGE

Imagen9.



Fuente: Autoría propia

Imagen10.

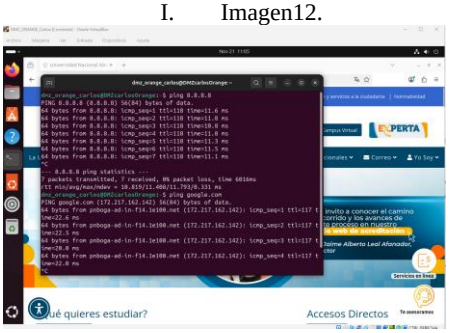
Fuente: Autoría propia

Imagen11.

Fuente: Autoría propia

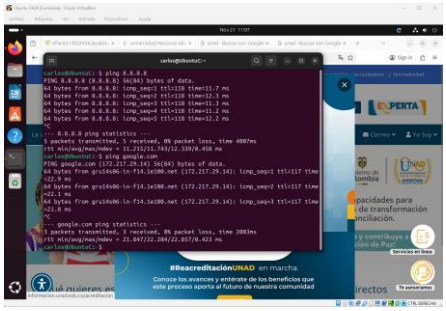
3.2.5 RESULTADOS Y PRUEBAS

I. Imagen12.



Fuente: Autoría propia

Imagen13.



Fuente: Autoría propia

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

Integrante 3 Jesus Alberto Leon Salazar

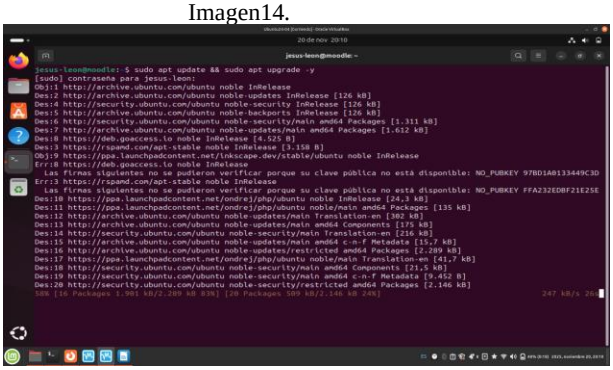
- Instalar servicios en Ubuntu Server (HTTP y FTP)

En la VM 192.168.20.1:

1. Actualiza e instala Apache y vsftpd:

sudo apt update && sudo apt upgrade -y
sudo apt install apache2 vsftpd -y

Imagen14.



Fuente: Autoría Propia

Imagen15.

Fuente: Autoría Propia

2. Verifica servicios:

Imagen16.

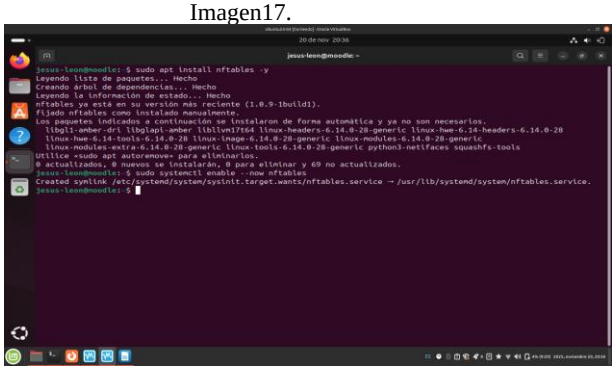
Fuente: Autoría Propia

- Configuración recomendada: nftables

En la VM servidor (192.168.20.1), instala nftables y aplica reglas:

1. Instala nftables:

Imagen17.



Fuente: Autoría Propia

2. Configurar reglas nftables

- Edita el archivo:

sudo nano /etc/nftables.conf

Imagen18.

Fuente: Autoría Propia

3. Carga las reglas y verifica:

Imagen19.

Fuente: Autoría Propia

Explicación:

• Política input = drop por defecto.

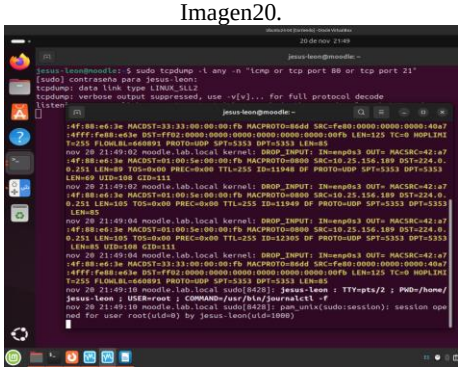
• Se acepta tráfico en lo y conexiones establecidas.

• Se permite TCP 80 y 21 solo desde la red 192.168.10.0/24.

• Se descartan paquetes ICMP con tipo echo-request (ping).

Ver tráfico en el servidor ORANGE

Imagen20.



Fuente: Autoría Propia

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

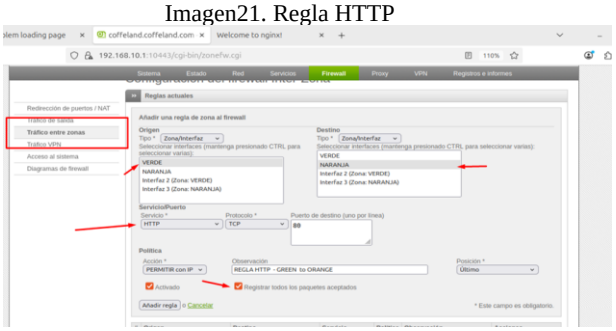
Integrante 3 Francisco Javier Perez Solano

En esta tematica se busca configurar e implementar diferentes reglas de firewall para los servicios HTTP y FTP los cuales se comunican a traves de distintas zonas LAN-GREEN,DMZ-ORANGE y WAM-RED. para el desarollo se configuro 2 VM simulando el comportamiento entre un cliente y servidor a los cuales se les aplican las distintas reglas de acceso creadas y validamos su comportamiento mediante las diferentes pruebas y registros identificados.

3.4.1 COMUNICAR LA ZONA VERDE CON LA ZONA NARANJA CON EL PROTOCOLO HTTP Y FTP CON SUS RESPECTIVOS PUERTOS.

Para poder habilitar la comunicación del HTTP entre las diferentes zonas GREEN-ORANGE se crearon una regla en la seccion de FIREWALL en el apartado de trafico de zonas donde permitio que el protocolo HTTP sobre el puerto 80 del equipo cliente el cual tenia una zona GREEN hacia el servidor de la zona ORANGE, una vez aplicada esta politica el servidor DMZ-ORANGE quedo accesible unicamente a traves del firewall.

Imagen21. Regla HTTP



Fuente: Autoría propia

Imagen22.Regla FTP

Fuente: Autoría propia

Durante el proceso de configuración y ambientación del entorno se implementó un servidor de nginx en el servidor asociado con la red de ORANGE el cual se implemento que su acceso sera unicamente a traves de los protocolos y reglas que se definieron en el proceso de configuración para acceder a la conexión mediante el protocolo FTP es necesario que previamente se instale en los equipos esta utilidad y a su vez debemos de configurar las reglas de reenvío de los puertos en nuestro entorno de virtualización.

Imagen23.Reglas de reenvío de puertos

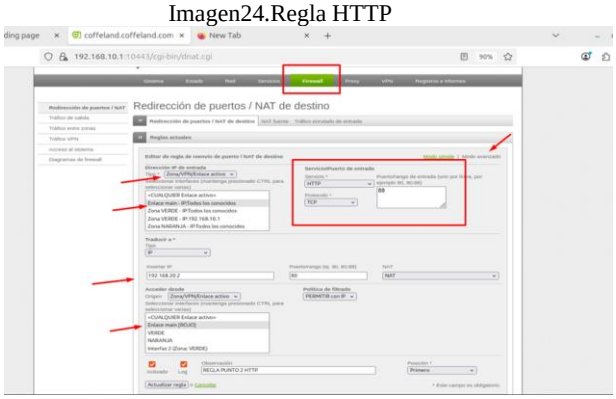
Fuente: Autoría propia

3.4.2 COMUNICAR LA ZONA INTERNET CON LA ZONA DMZ

Para el proceso de comunicacion de las zonas de internet WAN con la zona DMZ orange, acorde a los dos protocolos de conexion HTTP y FTP se implementaron dos reglas en la seccion de FIREWALL-redireccionamiento de puertos donde la primera regla seleccionamos el protocolo servicio HTTP por el protocolo de conexion TCP mediante el puerto 80 y

asignamos la ip de la zona ORANGE que fue la 192.168.20.2 y apuntando hacia la interfaz de la red RED la cual tiene habilitado el protocolo DHCP.

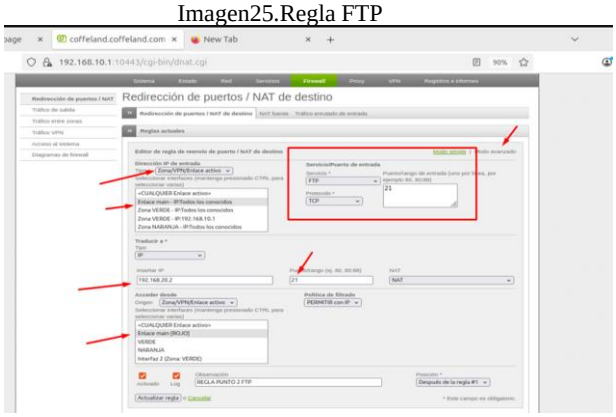
Imagen24.Regla HTTP



Fuente: Autoría propia

Para la configuración por el servicio FTP mediante el protocolo TCP se seleccionó en las zonas el enlace main y seleccionamos el servicio FTP por el protocolo TCP por el puerto 21 y le asignamos el puerto de la zona ORANGE 192.168.20.2 apuntando a la interfaz de la de zona RED la cual tiene el protocolo DHCP habilitado, cabe resaltar que para ambas instancias se habilito los logs para un monitoreo mas ameno.

Imagen25.Regla FTP

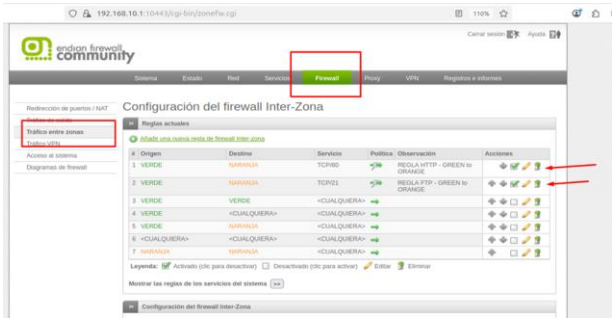


Fuente: Autoría propia

3.4.3 VERIFICAR EN EL TRAFICO INTER-ZONA, LA CREACIÓN DE LAS REGLAS

En el desarrollo de este punto de la tematica su interpretación hace alusión al validar que si entramos a la sección de FIREWALL en el modulo de trafico de zonas, la configuracion del firewall Inter zonas y corroborar que dichas reglas creadas anteriormente esten realmente creadas, cabe mencionar que para un mejor flujo de trabajo se deba inhabilitar las otras reglas y subir las que hemos creado recientemente.

Imagen25.Reglas definidas del trafico de zonas



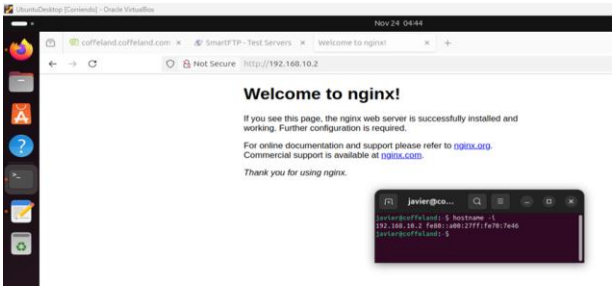
Fuente: Autoría propia

3.4.4 PROBAR DESDE UN NAVEGADOR WEB LAS SIGUIENTES DIRECTIVAS

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ

acceso al localhost donde instalamos nginx

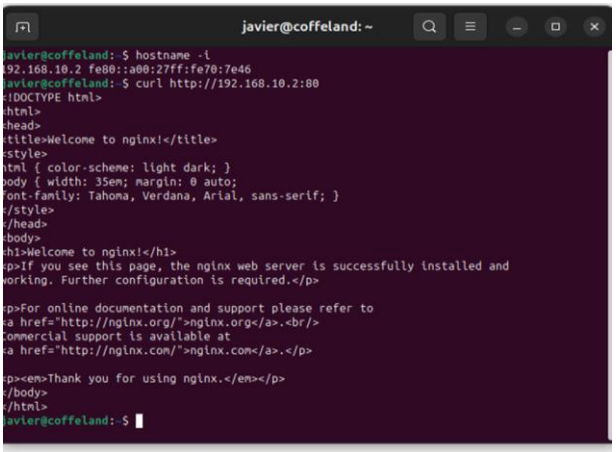
Imagen26.



Fuente: Autoría propia

curl al localhost, visualizando el html del nginx

Imagen27.



Fuente: Autoría propia

trafico del curl y acceso realizado, registrado

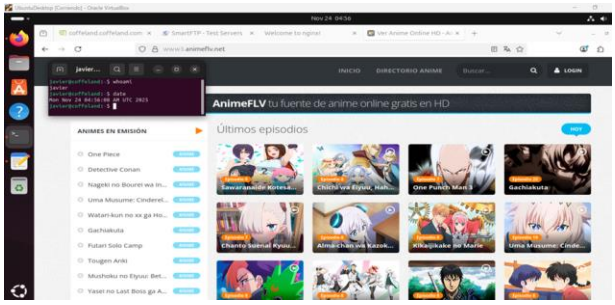
Imagen28.

Fuente: Autoría propia

..**El ingreso del servicio HTTP desde la LAN hacia la WAN**

accediendo a la pagina de animeflv con conexión

Imagen29.



Fuente: Autoría propia

El ingreso del servicio HTTP desde la zona DMZ hacia la WAN

wget realizado a la pagina de google.com

Imagen30.

Fuente: Autoría propia

lectura del index.html de google

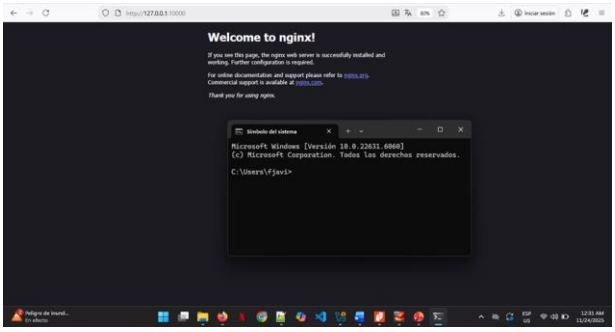
Imagen31.

Fuente: Autoría propia

El ingreso del servicio HTTP desde la WAN hacia la zona DMZ

acceso desde nuestro maquina física

Imagen32.



Fuente: Autoría propia

El ingreso del servicio FTP desde la LAN hacia WAN

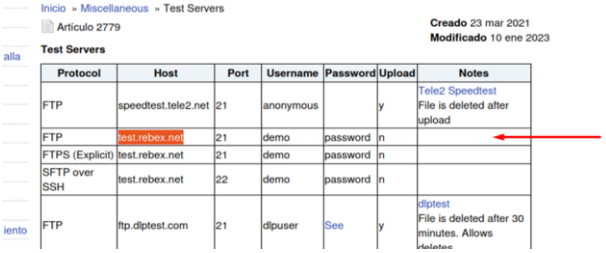
acceso por FTP a un host publico de FTP

Imagen32.

Fuente: Autoría propia

tabla del host publico utilizado

Imagen33.



Inicio » Miscellaneous » Test Servers

Artículo 2779

Creado 23 mar 2021
Modificado 10 ene 2023

Test Servers

Protocol	Host	Port	Username	Password	Upload	Notes
FTP	speedtest.tele2.net	21	anonymous		y	Tele2 Speedtest File is deleted after upload
FTP	test.rebex.net	21	demo	password	n	
FTPS (Explicit)	test.rebex.net	21	demo	password	n	
SFTP over SSH	test.rebex.net	22	demo	password	n	
FTP	ftp.dlptest.com	21	dlpuser	See	y	dlptest File is deleted after 30 minutes. Allows

Fuente: Autoría propia

El ingreso del servicio FTP desde la WAN hacia la zona DMZ

conexión realizada por ftp desde nuestra máquina física

Imagen34.

Fuente: Autoría propia

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

3.5.1 DESCRIPCIÓN GENERAL DE LA ACTIVIDAD

Integrante 5 Jhon Anderson Lipez Esteban

La temática 5 tiene como propósito implementar un Proxy HTTP no transparente en Endian Firewall (EFW), incluyendo políticas de autenticación, control de acceso y listas negras para restringir el uso de sitios web específicos desde la red LAN. Este ejercicio refleja un caso real de seguridad perimetral aplicado en organizaciones, donde el proxy actúa como punto de control obligatorio para la navegación hacia la Internet, asegurando trazabilidad, regulación de contenido y cumplimiento de políticas internas.

Endian Firewall permite integrar un proxy, administrado desde una interfaz gráfica centralizada Desktop Endian 13 Trixie, que controla el tráfico HTTP mediante perfiles, reglas y autenticación. La actividad describe cómo un firewall profesional puede aplicar filtros de contenido, gestionar usuarios y asegurar que solo tráfico autorizado acceda a la WAN.

2.6.2 APLICACIÓN DEL PROXY HTTP EN ENDIAN FIREWALL

El uso de Endian en esta actividad se basa en sus capacidades como plataforma de seguridad unificada, en particular su módulo de Web Proxy. La aplicación práctica de EFW en esta temática incluye:

Control de navegación desde la zona Verde (LAN) mediante la obligatoriedad de pasar por el proxy configurado.

Creación de perfiles de filtrado, donde se definen permisos y restricciones específicas para usuarios o grupos.

Implementación de una lista negra que bloquea el acceso a dominios no permitidos.

Autenticación por usuario, donde cada persona debe identificarse para navegar en Internet.

Monitoreo del tráfico, validando la aplicación de políticas de seguridad.

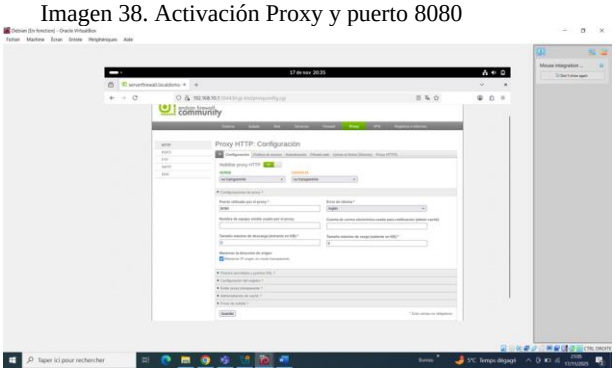
EFW se convierte en un punto centralizado donde todo el tráfico HTTP es inspeccionado y controlado, con registro detallado de accesos, bloqueos y usuarios autenticados.

2.6.3 DESARROLLO METODOLÓGICO

El primer paso consiste en habilitar el módulo de Proxy HTTP en Endian Firewall desde la interfaz web. Dado que se requiere autenticación, la modalidad utilizada es no transparente, es decir, el navegador debe configurarse manualmente para usar el proxy.

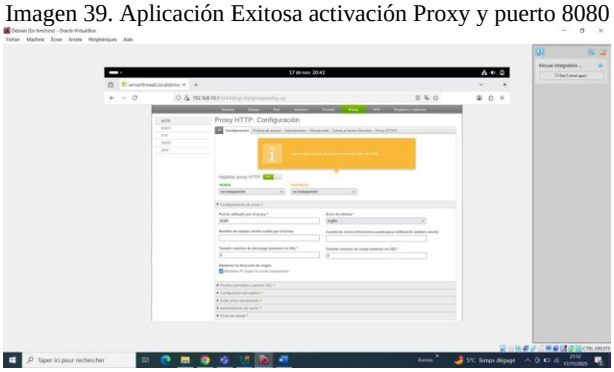
La configuración incluye: Habilitar el servicio. - Seleccionar el modo no transparente. - Definir el puerto del servicio (por defecto 8080). - Aplicar cambios y reiniciar el módulo.

Imagen 38. Activación Proxy y puerto 8080



Fuente: Autoría Propia

Imagen 39. Aplicación Exitosa activación Proxy y puerto 8080



Fuente: Autoría Propia

El segundo paso consiste en la Creación de Perfil de Filtrado y Lista Negra

En la sección Perfiles, se crea un perfil “Restriccion_algunas_paginas_web” dedicado para la LAN. Este perfil permite establecer políticas de acceso.

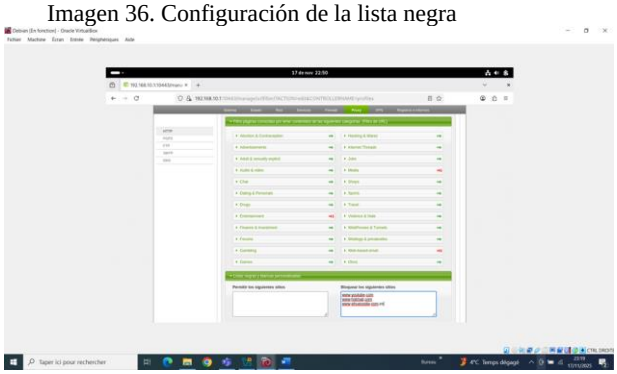
Imagen 35. Creación del perfil

Fuente: Autoría Propia

Posteriormente se configura la lista negra, especificando los dominios a bloquear en esta actividad:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

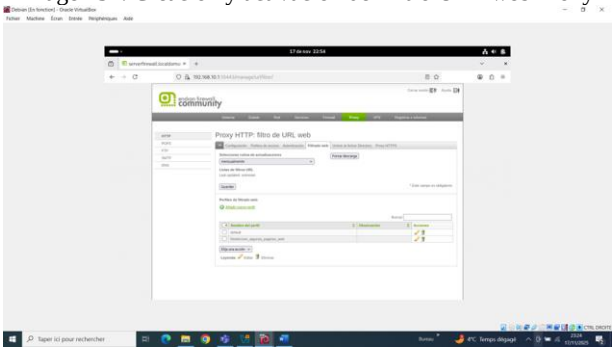
Imagen 36. Configuración de la lista negra



Fuente: Autoría Propia

Creación y activación del filtro URL web Proxy HTTP

Imagen 37. Creación y activación del filtro URL web Proxy



Fuente: Autoría Propia

El tercer paso consiste en Creación de un Usuario y Grupo para su Autenticación y una política de acceso

Desde el menú Proxy, Autenticacion, se habilita la autenticación local mediante usuarios administrados en EFW.

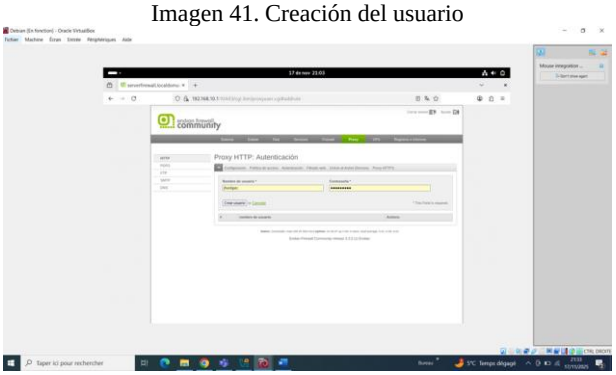
Creación del grupo “Usuarios_LAN”

Imagen 40. Creación del grupo

Fuente: Autoría Propia

Creación del usuario “jhonlipez”

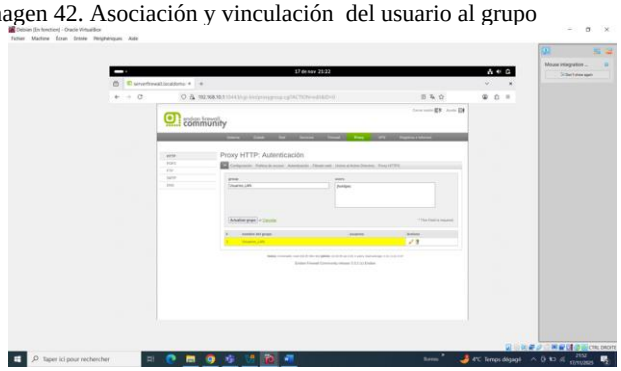
Imagen 41. Creación del usuario



Fuente: Autoría Propia

Asociación y vinculacion del usuario “jhonlipez” al grupo “Usuarios_LAN”

Imagen 42. Asociación y vinculación del usuario al grupo



Fuente: Autoría Propia

Política de acceso todos los agentes de usuario y luego selección del filtro del perfil creado “Restriccion_algunas_paginas_web”, primera posición y al final crear política.

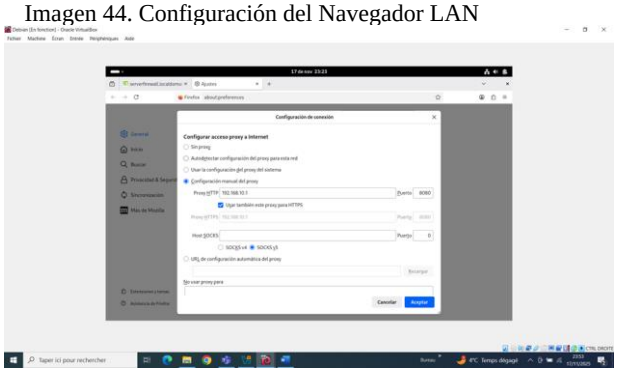
Imagen 43. Creación de Política de acceso

Fuente: Autoría Propia

El cuarto paso consiste en la configuración del Navegador en la LAN

La estación de trabajo ubicada en la zona Verde (LAN) debe configurar manualmente el proxy: Servidor proxy: 192.168.10.1 - Puerto: 8080. Una vez configurado, cualquier acceso HTTP exige credenciales.

Imagen 44. Configuración del Navegador LAN

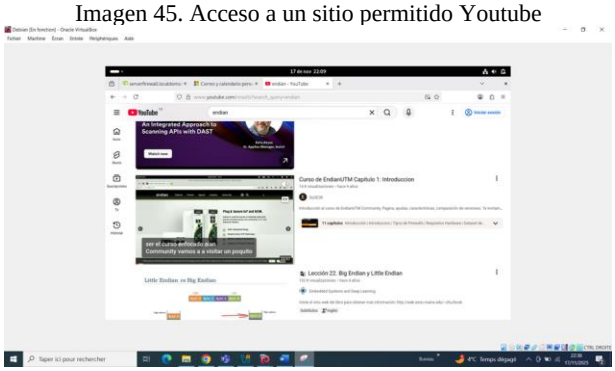


Fuente: Autoría Propia

El quinto paso consiste en pruebas de funcionamiento y evidencias

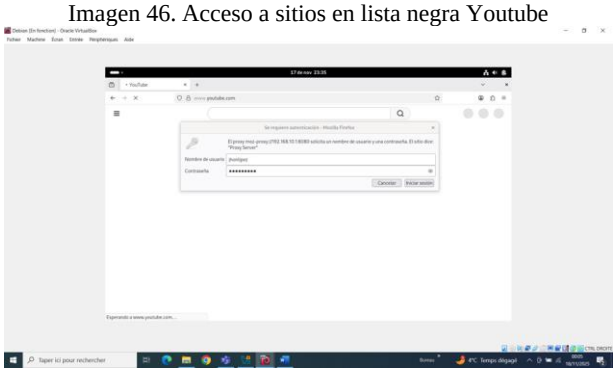
Se realizan pruebas desde un navegador: Acceso a un sitio permitido - Conexión exitosa. Acceso a sitios en lista negra - Acceso bloqueado. Verificación en logs del firewall.

Imagen 45. Acceso a un sitio permitido Youtube



Fuente: Autoría Propia

Imagen 46. Acceso a sitios en lista negra Youtube



Fuente: Autoría Propia

4 Conclusiones.

Tematica1

La instalación y configuración de GNU/Linux Endian en VirtualBox permitió comprender la importancia de la segmentación de redes mediante zonas de seguridad diferenciadas. La creación de las interfaces RED, GREEN y ORANGE facilitó la simulación de un entorno real donde el firewall actúa como núcleo de control y filtrado del tráfico. Esta práctica evidenció cómo un dispositivo perimetral puede gestionar eficientemente la comunicación entre la LAN, la DMZ y la red externa, garantizando tanto el acceso controlado como la protección de los recursos críticos. Asimismo, el uso de máquinas virtuales permitió replicar un laboratorio seguro y funcional para evaluar conectividad, asignación de IPs y pruebas de salida a Internet, estableciendo una base sólida para configuraciones más avanzadas como NAT, políticas de acceso y servicios proxy.

Temática 2

La configuración de NAT en Endian permitió comprender cómo el firewall gestiona la traducción de direcciones para controlar y optimizar el flujo de tráfico entre la red interna y el exterior. La creación de reglas de Port Forwarding y Masquerading evidenció la importancia de definir

adecuadamente qué servicios internos pueden ser expuestos y cómo los equipos de la LAN acceden a Internet mediante la IP pública del firewall. Esta práctica demostró que NAT no solo es esencial para proteger la topología interna, sino también para asegurar un enrutamiento eficiente, estable y seguro. Asimismo, trabajar con la interfaz administrativa de Endian facilitó una implementación ordenada y coherente, reforzando la comprensión de cómo un firewall perimetral aplica políticas de traducción y filtrado para mantener la integridad y disponibilidad de los servicios de red.

Temática 3

La configuración realizada permitió asegurar la comunicación entre la red GREEN (192.168.10.0/24) y la DMZ ORANGE (192.168.20.0/24) mediante reglas de firewall que autorizaron únicamente los servicios HTTP y FTP hacia el servidor Ubuntu, mientras que el bloqueo del protocolo ICMP evitó respuestas de ping y redujo la posibilidad de reconocimiento no autorizado. Las pruebas con curl, FTP y ping confirmaron el funcionamiento correcto de las reglas aplicadas, y el uso de nftables proporcionó un control granular y moderno del tráfico, fortaleciendo la seguridad perimetral y garantizando que solo los servicios estrictamente necesarios estén expuestos en la DMZ.

Temática 4

La creacion de las reglas entre las diferentes zonas GREEN, ORANGE y RED con el protocolo DHCP permite entender de manera más clara y estructurada como fluye el tráfico entre la LAN, el DMZ y la WAN a través de sus configuraciones cada equipo como cliente y servidor. Al probar los accesos mediante los servicios de HTTP y FTP por el protocolo TCP entre los distintos orígenes se evidencio la importancia de definir correctamente las políticas de firewall y validar que cada servicio esté activo y escuchando por los puertos adecuados.

Temática 5

La implementación del Proxy HTTP no transparente en Endian Firewall demostró la capacidad de controlar, filtrar y auditar el tráfico de navegación proveniente de la red LAN mediante políticas centralizadas basadas en usuarios y grupos. El uso de perfiles con listas negras y reglas de autenticación permitió establecer un modelo de acceso seguro y totalmente administrado, garantizando que solo usuarios autorizados puedan navegar y que los sitios restringidos sean efectivamente bloqueados. Esta temática evidenció además el valor del proxy como herramienta fundamental para el fortalecimiento de la seguridad perimetral, permitiendo a la organización aplicar normativas internas de uso aceptable y registrar la actividad web para fines administrativos o de

5 REFERENCIAS

[1] [1] Endian Firewall Community, Endian Firewall Community Edition, Endian.com. [En línea]. Disponible en: https://www.endian.com/en/community/. Accedido: 24-nov-2025.

[2] Oracle Corporation, Oracle VM VirtualBox – User Manual, VirtualBox.org. [En línea]. Disponible en: https://www.virtualbox.org/. Accedido: 24-nov-2025.

[2] Endian. (2023). Endian Firewall Community – NAT, Firewall & Routing Configuration Guide. Endian Documentation. https://www.endian.com/en/community/

[3] LPI LPIC-1 Exam 101. (2022). Tema 101: Arquitectura del Sistema. https://learning.lpi.org/es/learning-materials/101-500/101

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

[5] A. Tanenbaum y D. Wetherall, Computer Networks, 5th ed., Pearson, 2011. — (Referencia adicional para sustentar el uso de proxys dentro de arquitecturas de red)