SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNOS VIRTUALIZADOS

Luis Fernando Lopez Carranza
e-mail: lflopezcar@unadvirtual.edu.co
Nelson Guillermo Velasquez Triana
e-mail: ngvelasquezt@unadvirtual.edu.co
Viviana Orozco Perez
e-mail: vi49oro558@unadvirtual.edu.co
Jhon Stiven Murcia Vargas
e-mail: jsvargasmur@unadvirtual.edu.co

RESUMEN: *Este artículo presenta el desarrollo e implementación de un entorno de seguridad perimetral basado en la distribución GNU/Linux Endian Firewall Community. ejecutado sobre la plataforma VirtualBox. Se enfoca en la administración de zonas de red (verde, naranja y roja), reglas de traducción de direcciones (NAT), control de servicios (HTTP, FTP) y políticas de acceso entre segmentos LAN, DMZ y WAN. La labor cubrió dividir la red por partes. Se puso la configuración de NAT para salir a la web. Se activaron servicios en la DMZ. El ICMP se bloqueó en esa zona. Luego se revisaron las normas de paso de datos. Desde el punto de vista de estudios, se mira cómo ayudan estas cosas a la seguridad. Esto pasa en los lugares con máquinas virtuales. Se sigue lo que dice el 802.1 de IEEE sobre dividir redes. Los hallazgos muestran que las normas de borde funcionan bien. Esto aplica a los equipos que usan Linux. Así se refuerzan destrezas en manejo experto de redes.*

PALABRAS CLAVE: Autenticación, Endian Firewall, NAT, Seguridad Perimetral.

INTRODUCCIÓN

Las estructuras de hoy necesitan cimientos firmes para poder separar, mandar y vigilar el ir y venir entre trozos de red distintos. Los muros cortafuegos fronterizos tienen una función clave en esto, sobre todo si trabajan en diseños que juntan áreas separadas como la red local, la zona desmilitarizada y la web. En este marco, la versión Endian Firewall Community sobresale por su manera completa de actuar, dando opciones de filtrar, traducir direcciones, manejar servicios y un intermediario con comprobación de identidad.

El presente artículo documenta el proceso de implementación de un entorno de seguridad perimetral desarrollado como parte del diplomado en Linux. Se planeó y ajustó un lugar simulado en VirtualBox con Endian Firewall como aparato principal, uniendo las áreas Verde (LAN), Naranja (DMZ) y Roja (WAN). Después se ajustaron normas de traducción, servicios que pueden usarse, normas entre áreas y un intermediario de web sin que se note. La meta mayor fue solidificar saberes prácticos en manejar la guarda fronteriza bajo sistemas operativos de software libre, usando modelos que se ven en lugares verdaderos.

2. METODOLOGIA

La metodología aplicada se basó en cuatro fases:

- Análisis: comprensión de requerimientos perimetrales.
- Diseño: definición de direcciones IP, segmentación lógica, zonas y políticas iniciales.
- Implementación: despliegue del firewall, configuración de NAT, reglas de tráfico y servicios.
- Validación: pruebas funcionales, análisis de tráfico, verificación de seguridad y documentación.

Este enfoque permitió integrar teoría y práctica garantizando trazabilidad y coherencia entre los objetivos del proyecto y su ejecución.

2.1 CARACTERÍSTICAS GENERALES

El entorno implementado se basa en la distribución Endian Firewall Community, una plataforma orientada a la gestión de seguridad perimetral en redes corporativas. Su forma facilita dividir la red en partes distintas —VERDE (local), NARANJA (zona de paso) y ROJO (fuera)— para poner reglas claras de hablar y limitar quién entra entre ellas. El montaje se hizo en un lugar simulado con VirtualBox, dejando poner adaptadores de red separados para cada parte y copiar cómo funciona una estructura de verdad. Endian da una pantalla fácil de usar donde uno puede poner normas para parar cosas, mostrar servicios, manejar identidades y aplicar seguridades complejas. Además, el aparato trae dentro formas de mirar lo que viaja, apuntar lo que pasa, manejar el intermediario web y checar quién entra, logrando así un cuidado total del borde de la red. Estos puntos hacen que Endian Firewall sea una opción fuerte y que se adapta para poner defensas en sitios de estudio, negocios y pruebas.

3. TÍTULO PRINCIPAL

Implementación de Seguridad Perimetral con Endian Firewall Configuración de Zonas, NAT, Políticas de Acceso, Proxy Autenticados, Control de Servicios HTTP/FTP y Bloqueo de ICMP en Entornos Virtualizados.

4. INSTALACIÓN Y CONFIGURACIÓN

4.1 ARQUITECTURA DEL SISTEMA

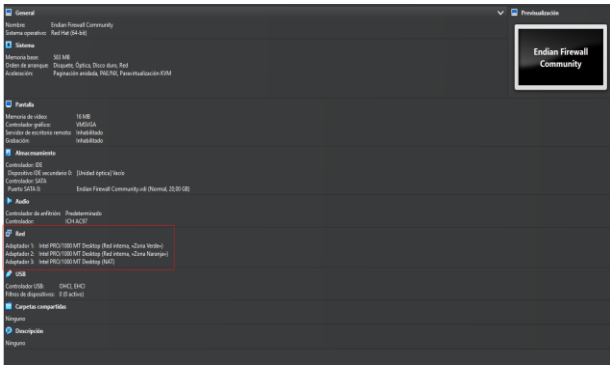
La segmentación de la red se basa en la separación lógica de las zonas GREEN y ORANGE, administradas por el firewall Endian. Esta división permite aislar los servicios expuestos al exterior y garantizar que únicamente el tráfico autorizado pueda circular entre los segmentos. Cada máquina virtual recibe una configuración IP manual que define su posición dentro de la arquitectura perimetral.

La arquitectura implementada se compone de tres zonas definidas según el modelo clásico de seguridad perimetral:

- Zona Verde (GREEN – LAN): red interna segura.
- Zona Naranja (ORANGE – DMZ): capa intermedia para exposición de servicios.
- Zona Roja (RED – WAN): red insegura o externa.

Configuramos en la máquina de Endian los 3 adaptadores de red que usaremos para configurar las diferentes zonas de red, Red interna (Zona Verde), Red interna (Zona Naranja) y NAT (Zona Roja).

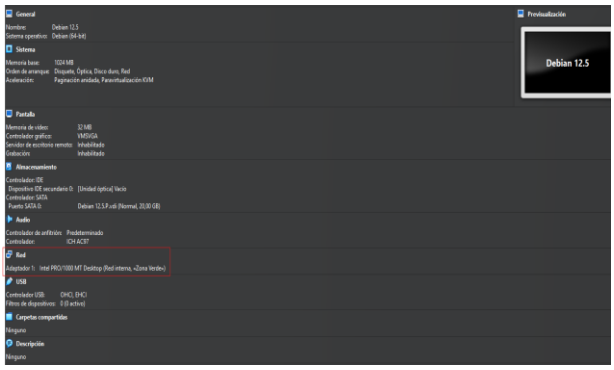
Figura 1. Configuración red endian



Fuente: Autoría Propia

Configuramos el adaptador de la máquina del cliente el Desktop en la zona verde, este se conectará a interne por medio de la maquina Endian del Firewall.

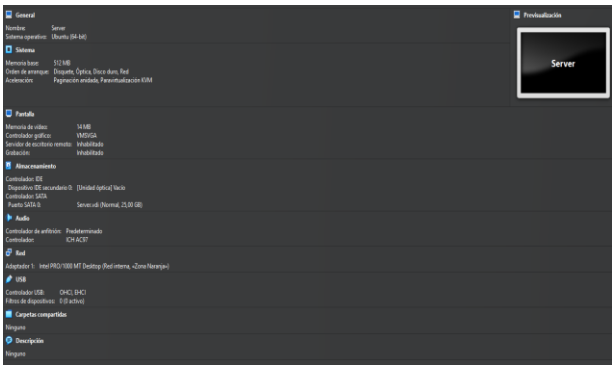
Figura 1. Configuración red desktop



Fuente: Autoría Propia

De igual manera configuramos el adaptador del servidor en la zona naranja.

Figura 1. Configuración red servidor



Fuente: Autoría Propia

Arranque e instalación de Endian desde ISO, Al momento de realizar la instalación nos pedirá la dirección IP de la zona verde esta se le asignará la IP del Gateway que el compañero de la temática 1 haya establecido la segmentación de las Red.

Figura 1. Arranque endian

Fuente: Autoría Propia

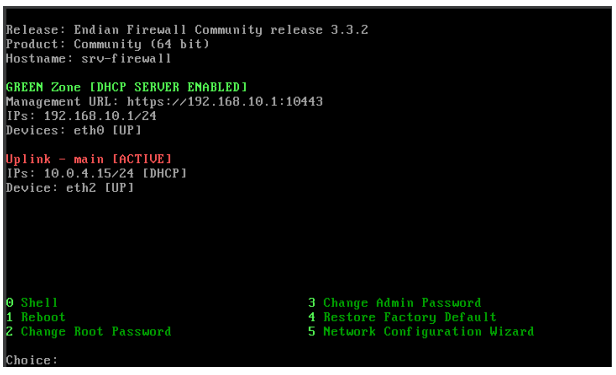
Figura 1. Arranque endian

Fuente: Autoría Propia

Figura 1. Arranque endian

Fuente: Autoría Propia

Figura 1. Interfaz de endian



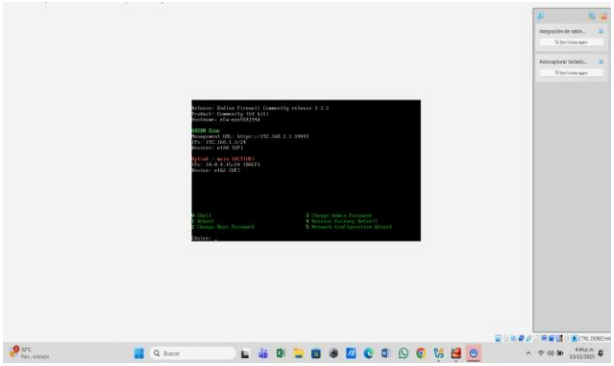
Fuente: Autoría Propia

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

Fundamento: La configuración inicial establece la base para segmentación, basada en IEEE 802.3 para interfaces Ethernet virtuales. Se instaló Endian desde ISO, asignando IP verde durante el wizard.

Desarrollo: Luego de haber asignado interfaces y zonas Network Setup Wizard, se configura el IPs de clientes y servidores.

Figura 1. Configuración inicial en endian

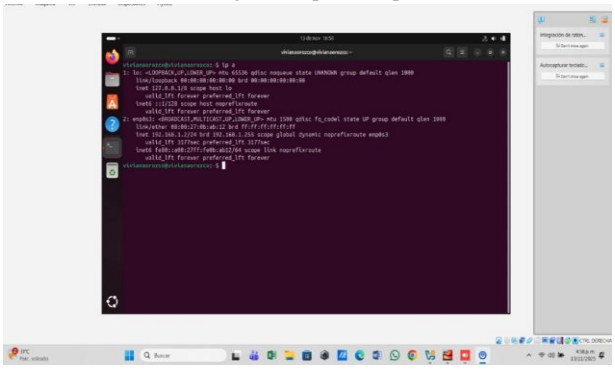


Fuente: Autoría Propia

En donde las VMs conectadas a las redes internas: Es, VM-Client (GREEN): asignando IP manual: 192.168.10.10/24, gateway 192.168.10.1 (la IP del Endian en GREEN).

VM-Server (ORANGE): asignando IP manual: 192.168.20.10/24, gateway 192.168.20.1 (Endian en ORANGE).

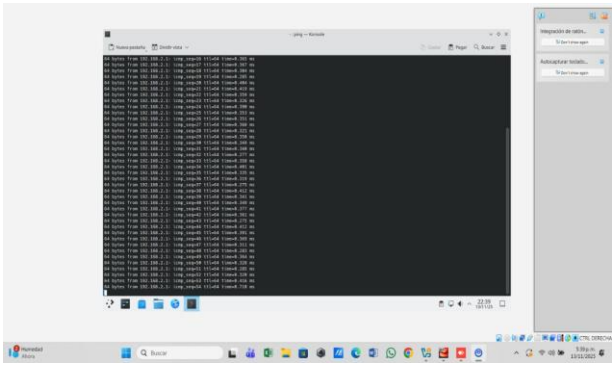
Figura 1. Ip desktop



Fuente: Autoría Propia

Se Comprueba la conectividad:
Desde VM-Client hacer ping 192.168.10.1.
Desde VM-Server hacer ping 8.8.8.8 (si en RED hay salida a Internet y NAT habilitado).

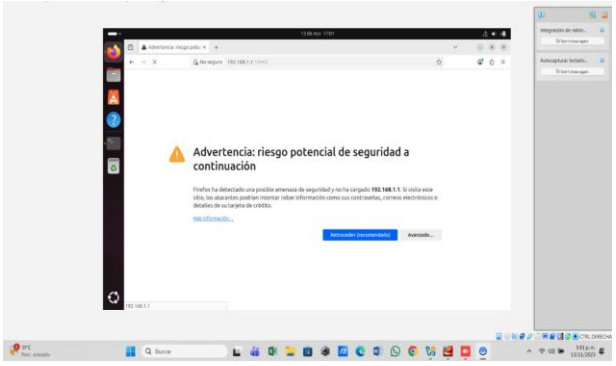
Figura 1. Comprobar conexión



Fuente: Autoría Propia

En una máquina en GREEN se abre el navegador con https://192.168.10.1 y autenticando con el usuario admin y la contraseña que se creó.

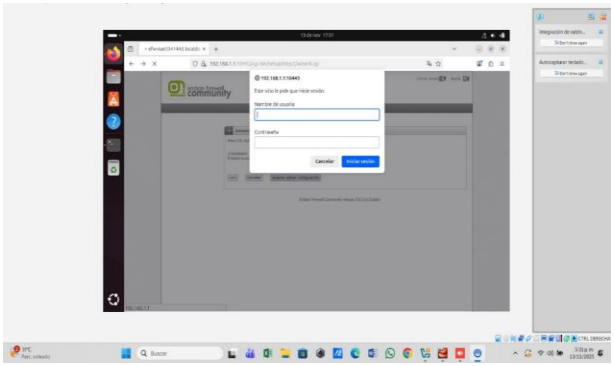
Figura 1. Entrar a endian en el navegador



Fuente: Autoría Propia

A partir de esto la GUI permite: Ver interfaces y zonas. Configurar reglas de firewall, NAT, VPN, contenido.
Ver logs y eventos. (Tutoriales GUI disponibles).

Figura 1. Ingresar a endian con usuario



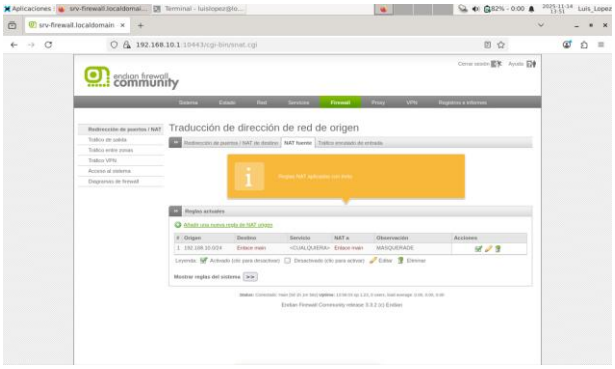
Fuente: Autoría Propia

6 TEMATICA 2 CONFIGURACIÓN NAT

6.1 CREACION DE REGLAS NAT

Nos dirigimos a la opción de Firewall redirección de puertos y NAT fuentes y creamos las reglas, en Origen: 192.168.10.0/24 Destino: Enlace main (ROJO) NAT a: Enlace main auto, en Observación Modo: MASQUERADE Estado → Activado.

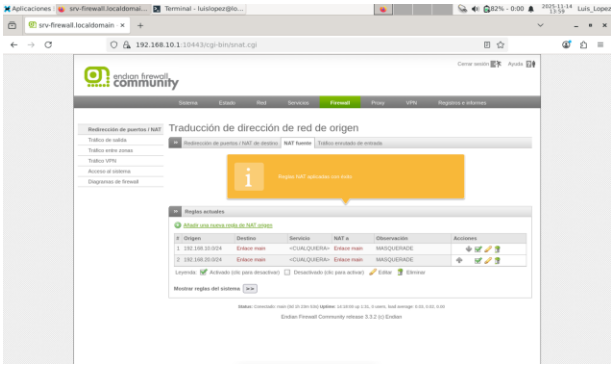
Figura 1. Crear reglas NAT (rojo)



Fuente: Autoría Propia

De igual manera con la regla en Origen: 192.168.20.0 de la zona Naranja para el server y le damos crear regla.

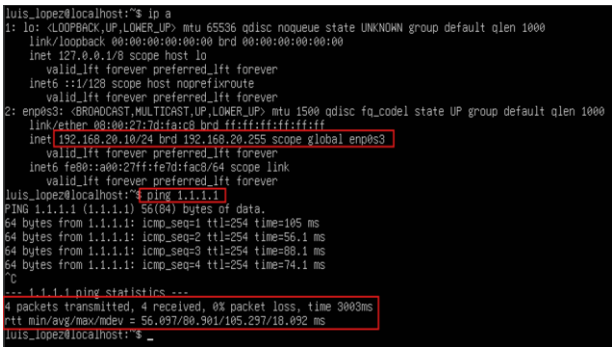
Figura 1. Crear reglas NAT (naranja)



Fuente: Autoría Propia

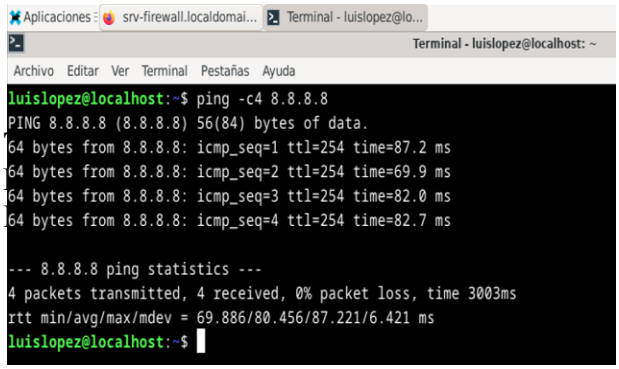
Validación De Comunicación Desde La LAN Hacia La WAN

Figura 1. Validar conexión



Fuente: Autoría Propia

Figura 1. Validar conexión



Fuente: Autoría Propia

7 TEMATICA 3 PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED. INSTALACIÓN DE FIREWALL DE ENDIAN

Endian con interfaces activas.

Se puede observar la actividad de las interfaces antes de validar trafico

Figura 1. Actividad de las interfaces

Fuente: Autoría Propia

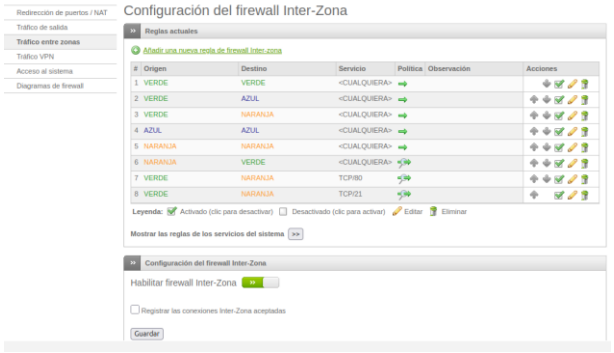
Reglas iniciales. Se verifican y se crea la regla para la zona NARANJA-VERDE y así confirmar comunicación general entre equipos. Se confirma ping entre los equipos cliente servidor y la red externa.

Figura 1. Crear regla naranja-verde

Fuente: Autoría Propia

Reglas de acceso a servicios HTTP (Puerto 80) y FTP (Puerto 21). Se crean 2 reglas para permitir acceso desde la zona verde a la naranja para los puertos 80 y 21, es decir para el acceso al servicio web y para el acceso via ftp para transferir archivos.

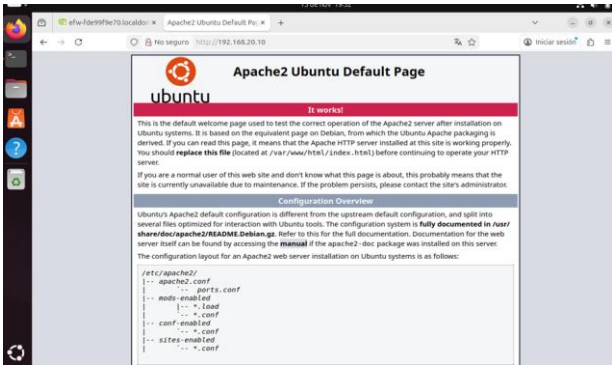
Figura 1. Regla http y ftp



Fuente: Autoría Propia

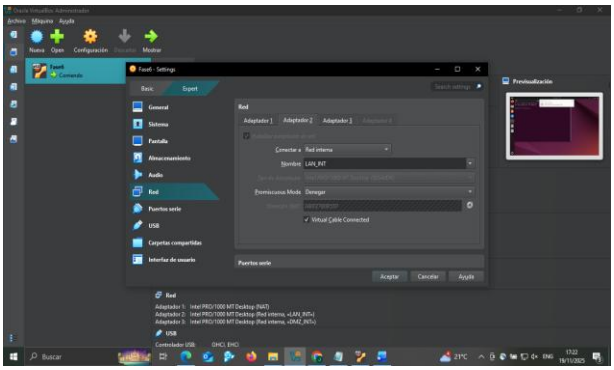
Acceso web desde el cliente. En este paso accedemos a Ubuntu que es la Comprobación de acceso a la web desde el cliente.

Figura 1. Ingresar desde el cliente



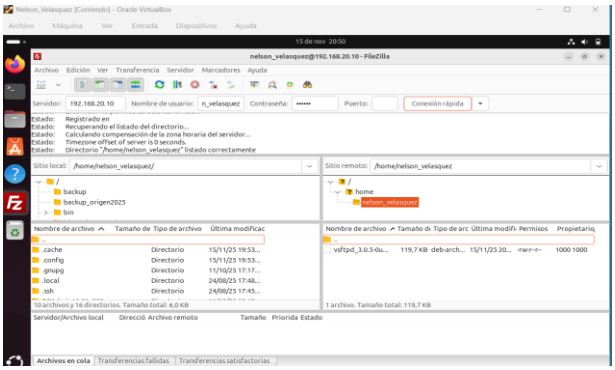
Fuente: Autoría Propia

Figura 1. Ingresar desde el cliente



Fuente: Autoría Propia

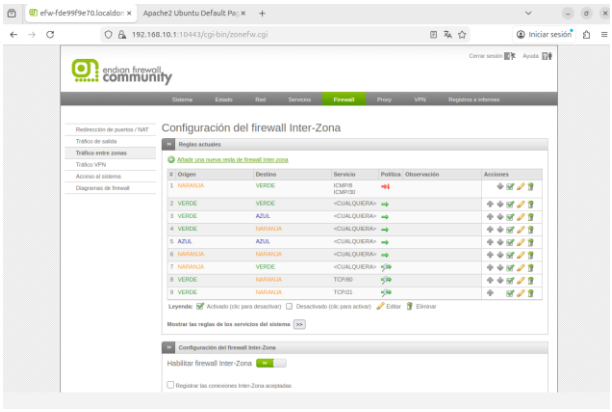
Figura 1. Ingresar desde el cliente



Fuente: Autoría Propia

Configuración regla de negación ICMP. Se crea la regla para no permitir el ping entre la zona naranja y la zona verde.

Figura 1. Configurar regla ICMP

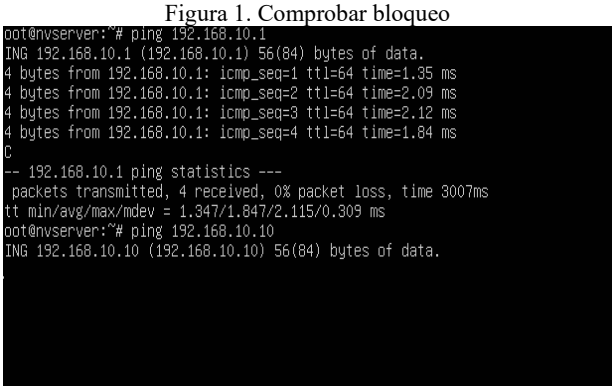


Fuente: Autoría Propia

Comprobación regla de bloque ICMP.

Se realiza ping al puerto Endian de la red verde y responde correctamente y se hace ping al equipo en esa red y no responde.

Figura 1. Comprobar bloqueo



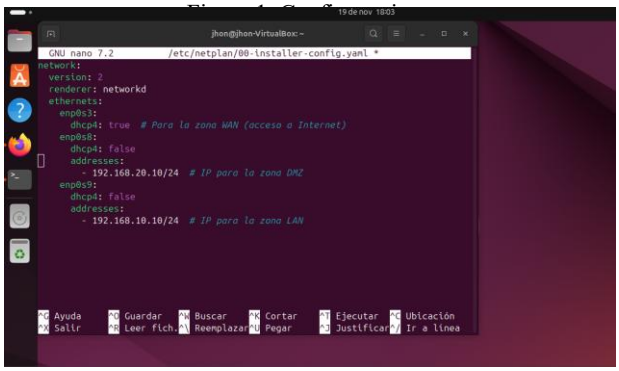
Fuente: Autoría Propia

8 TEMATICA 4 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO.

Se debe configurar la máquina virtual antes de iniciar la partición Ubuntu.

Configuramos la red y sus adaptadores.

Se configuran las interfaces con las IPs

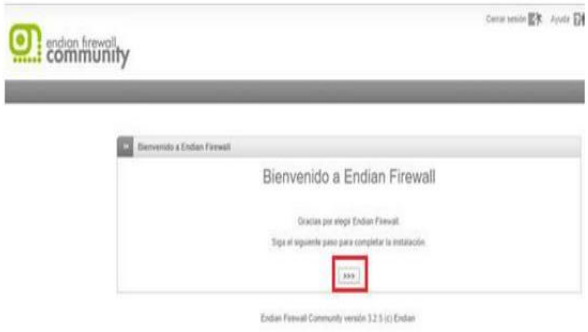


Fuente: Autoría Propia

Interfaz web de endian

Seleccionamos zona horaria, idioma y demás configuraciones básicas

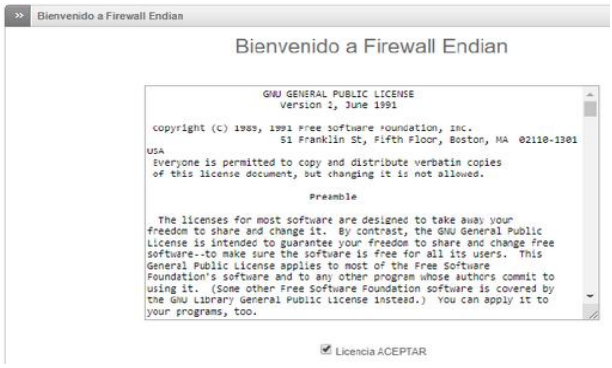
Figura 1. Configuración endian



Fuente: Autoría Propia

Se deben aceptar la licencia

Figura 1. Aceptar licencia

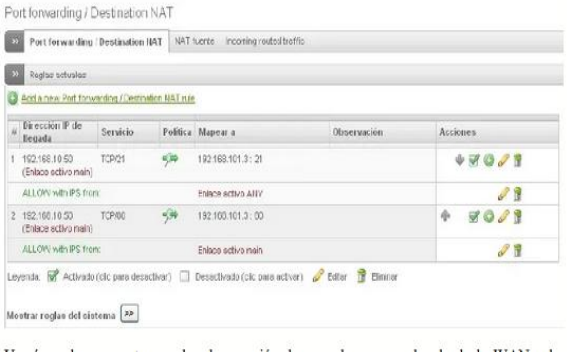


Fuente: Autoría Propia

Comunicamos la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos.

Comunicamos la zona Internet con la zona DMZ.

Figura 1. Comunicar http y ftp



Fuente: Autoría Propia

Verificar en el tráfico Inter - Zona, la creación de las reglas.

Figura 1. Verificar trafico

Fuente: Autoría Propia

9 DESARROLLO DEL PROYECTO

Configuración de la instancia Endian en VirtualBox

Se configuraron tres adaptadores de red en Endian Firewall:

- Adaptador interno para GREEN.
- Adaptador interno para ORANGE.
- Adaptador NAT para RED.

De igual manera, cada máquina virtual cliente/servidor recibió una configuración IP estática correspondiente a su zona.

La instalación inicial incluyó:

- selección de interfaces,
- configuración de direcciones,
- pruebas de conectividad entre zonas,
- acceso a la interfaz web del firewall como administrador.

Esta etapa permitió verificar que Endian actuara efectivamente como gateway y punto de control perimetral.

Configuración de NAT

La traducción de direcciones es indispensable para permitir que dispositivos internos accedan a Internet sin exponer su estructura. Se creó una regla **MASQUERADE** para habilitar el tráfico desde GREEN y ORANGE hacia RED.

NAT permite:

- ocultar direcciones internas,
- controlar el flujo hacia redes externas,
- mantener coherencia con políticas de seguridad modernas.

Las pruebas de validación incluyeron:

- ping a servidores externos,
- análisis de trazas mediante los logs del firewall,
- verificación de tablas de enrutamiento.

Servicios en la DMZ: HTTP y FTP

Uno de los objetivos centrales del proyecto fue demostrar la correcta exposición de servicios públicos mediante una DMZ. Se implementaron servidores **HTTP** y **FTP** dentro de ORANGE, y se crearon reglas para permitir el acceso desde GREEN y desde RED únicamente en los puertos autorizados.

Esto permitió analizar:

- seguridad aplicada mediante capas,
- funcionamiento de la DMZ como zona aislada,
- comportamiento del flujo interzona.

Se realizaron pruebas con navegadores y clientes FTP para validar el acceso.

Reglas de acceso y control de tráfico

Se asignaron reglas específicas para permitir o denegar el paso de protocolos entre zonas, incluyendo:

- HTTP (80),
- FTP (21),
- ICMP para diagnósticos.

El bloqueo de ICMP entre GREEN ↔ ORANGE permitió simular escenarios comunes de mitigación contra ataques de reconocimiento.

Resultados

Los resultados demostraron que la arquitectura perimetral implementada cumple los principios fundamentales de aislamiento, control de tráfico y protección de servicios. Las pruebas de los servidores en DMZ, el funcionamiento del NAT y el filtrado selectivo evidencian un comportamiento seguro y alineado con prácticas profesionales.

El análisis de tráfico mostró que Endian gestiona efectivamente el flujo entre zonas, bloqueando intentos no autorizados y permitiendo únicamente los servicios aprobados.

10 CONCLUSIONES

La implementación de un sistema de seguridad perimetral basado en Endian Firewall en un entorno virtualizado permitió comprender de manera integral los mecanismos de segmentación de red, control de tráfico, traducción de direcciones y exposición segura de servicios. El uso de zonas GREEN, ORANGE y RED demostró la importancia de aislar segmentos críticos y aplicar políticas diferenciadas que garanticen la protección de los recursos internos frente a redes externas o poco confiables. Los resultados evidencian que un diseño adecuado de reglas, sumado a la validación continua del tráfico, es esencial para asegurar un perímetro robusto y funcional en infraestructuras de red reales o simuladas.

La implementación de una DMZ en GNU/Linux, acompañada de la habilitación controlada de los servicios HTTP y FTP, permitió establecer un entorno perimetral seguro y segmentado. La aplicación de reglas de firewall, incluyendo el bloqueo del protocolo ICMP, fortaleció la protección contra actividades de reconocimiento y accesos no autorizados. Los resultados obtenidos evidencian que la segmentación adecuada y el control del tráfico son elementos esenciales para mantener servicios expuestos sin comprometer la integridad de la red interna.

La exposición controlada de los servicios HTTP y FTP dentro de la zona DMZ demostró la importancia de aislar servidores públicos del resto de la red. El ejercicio evidenció que una DMZ bien diseñada minimiza riesgos y facilita la administración del tráfico hacia servicios sensibles sin comprometer la integridad de la LAN.

La creación de reglas específicas para permitir o denegar protocolos como HTTP, FTP e ICMP mostró la importancia del filtrado granular dentro del firewall. La restricción selectiva del tráfico entre zonas permitió validar escenarios reales de seguridad y reforzó la necesidad de aplicar políticas basadas en el principio de mínimo privilegio.

REFERENCIAS

[1] B. Ward, *How Linux Works: *What Every Superuser Should Know*, 2nd ed. No Starch Press, 2014*.

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

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

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

[5] E. Nemeth, G. Snyder, T. Hein, and B. Whaley, **UNIX and Linux System Administration Handbook**, 5th ed. Pearson, 2017.

[6] LPI Linux Essentials, *"Tema 5: Seguridad y sistema de permisos de archivos," 2022*. [Online]. Available: https://learning.lpi.org/es/learning-materials/010-160/5/

[7] 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/

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