DISEÑO E IMPLEMENTACIÓN DE UNA ARQUITECTURA PERIMETRAL SEGURA CON DMZ Y NAT EN ENDIAN FIREWALL

Alexandra Maireth Villa Guerra
amvillagu@unadvirtual.edu.co
Diana Paola Santibañez Parra
dpsantibanezp@unadvirtual.edu.co
Gerson Andres Duenas Perez
gaduenasp@unadvirtual.edu.co
Hernan Camilo Losada Rivera
hclosadar@unadvirtual.edu.co
Jonathan Stivens Vargas Ramirez
e-mail: jsvargasra@unadvirtual.edu.co

RESUMEN: *En este artículo se diseñó e implementó una arquitectura de seguridad perimetral para proteger los servidores de intranet (LAN) y extranet (WAN) mediante el uso de una zona DMZ, empleando Endian Firewall Community como plataforma central en VirtualBox; se configuraron tres interfaces de red: GREEN para la LAN, ORANGE para la DMZ y RED para la WAN simulada, definiendo un direccionamiento IP coherente para toda la infraestructura y común para los integrantes del grupo; se instaló una estación de trabajo GNU/Linux en la LAN con puerta de enlace hacia Endian y un servidor GNU/Linux en la DMZ destinado a hospedar servicios web finalmente se corroboró en la interfaz de Endian la creación y funcionamiento de las reglas NAT, dejando la plataforma lista para continuar con las temáticas de habilitación/denegación de servicios, reglas inter-zona y proxy.*

PALABRAS CLAVE: Endian Firewall, NAT, GNU/Linux, DMZ, LAN.

1 INTRODUCCIÓN

La seguridad perimetral es un componente esencial para garantizar la protección de los recursos críticos en redes corporativas y académicas, especialmente cuando se dispone de servicios internos (LAN) y servicios expuestos hacia el exterior (WAN). En estos entornos, la segmentación de la infraestructura en zonas con diferentes niveles de confianza permite controlar de manera más efectiva el flujo de tráfico y reducir la superficie de ataque.

Una de las estrategias más utilizadas para este fin es la creación de una zona desmilitarizada (DMZ), en la cual se alojan servidores que deben ser accesibles desde múltiples redes sin comprometer la seguridad de la red interna. En este trabajo se implementa una arquitectura de seguridad perimetral basada en Endian Firewall Community sobre VirtualBox, configurando las zonas GREEN (LAN), ORANGE (DMZ) y RED (WAN) con direccionamiento IP definido y dispositivo GNU/Linux en cada segmento.

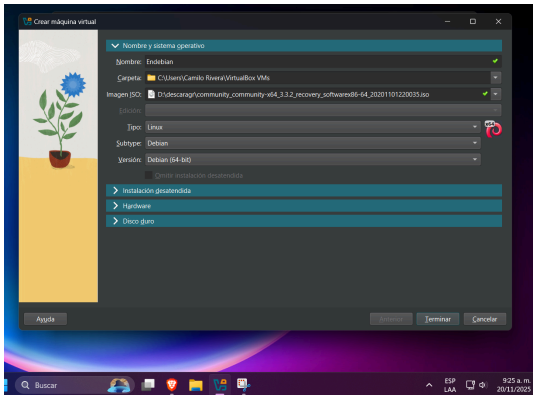
A partir de esta infraestructura, se desarrolla la configuración de NAT/SNAT (masquerading) y las reglas de tráfico necesarias para habilitar la comunicación controlada desde la LAN y la DMZ hacia Internet, verificando su funcionamiento mediante pruebas de conectividad y validación de servicios. De esta manera, se busca evidenciar el papel del firewall como elemento central en la administración segura del tráfico inter-zona y en la protección de aplicaciones y bases de datos alojadas en plataformas GNU/Linux.

2 TEMÁTICAS

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

Para dar inicio a esta sección del trabajo, es necesario descargar e instalar Endian Firewall. Se accede al enlace https://www.endian.com/en/community/ para obtener el software requerido, a continuación en VirtualBox se debe crear una nueva máquina virtual definiendo su nombre, el sistema operativo (Linux) y la versión correspondiente

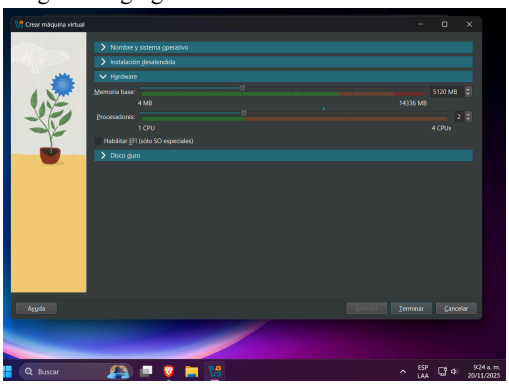
Fig. 1 asignación de nombre y sistema operativo en VirtualBox



Fuente: Autoría Propia

Procedimos a la sección de Hardware para determinar los recursos que utilizará la máquina virtual específicamente se ha realizado la asignación de la Memoria base (RAM) y de la cantidad de Procesadores (CPU), en este caso particular se ha configurado la máquina virtual para utilizar 3072 MB de memoria y se le ha asignado 1 CPU del sistema físico. Este paso es fundamental ya que garantiza los recursos operativos necesarios para el sistema antes de avanzar a la configuración del almacenamiento.

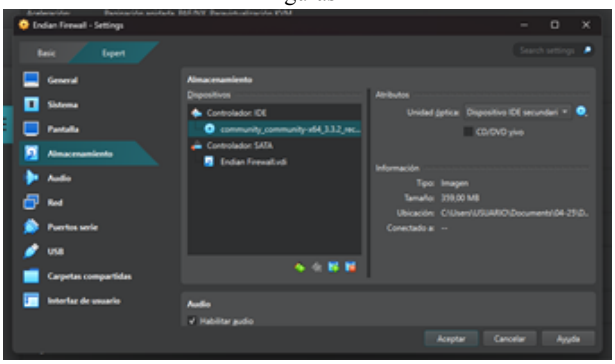
Fig. 2 Se agrega la memoria RAM en VirtualBox



Fuente: Autoría Propia

Accedemos a la configuración de Almacenamiento y, bajo el Controlador IDE, se asigna la imagen .iso luego se descarga como la Unidad óptica secundaria. Esta acción es vital ya que nos permite a la máquina virtual arrancar desde la imagen de instalación para iniciar el despliegue del sistema operativo en el disco virtual.

Fig. 3 Instalación de la OS ENDIAN. Ejemplo para todas las figuras



Fuente: Autoría Propia

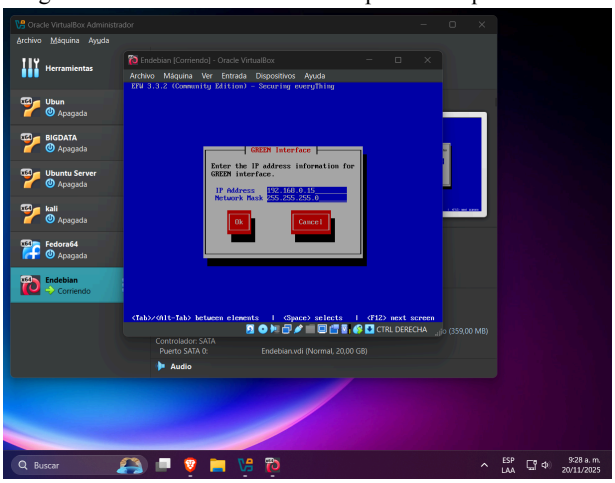
Tabla 1

Zona de Red	Descripción	Dirección IP / Máscara de Subred	Tipo de Conexión
GREEN (LAN)	Red de Área Local	192.168.0.15/24	Fija/Estática
ORANGE (DMZ)	Zona Desmilitarizada	192.168.20.1/24	Fija/Estática
RED (WAN)	Red de Área Extensa	Definida por DHCP	Dinámica

Fuente: Autoría Propia

En este punto, la instalación solicita los parámetros de red para la Interfaz GREEN (la red local). Se ingresa la dirección IP estática requerida, en este caso, 192.168.0.15 y se confirma la Máscara de red (255.255.255.0). Esta configuración es crucial para la segmentación y correcto funcionamiento del firewall.

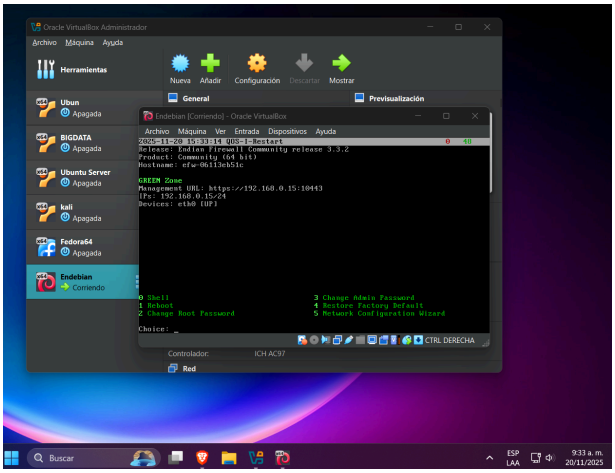
Fig. 4 Direccionamiento IP estático para la máquina virtual



Fuente: Autoría Propia

Esta pantalla confirma que la instalación del sistema operativo ha finalizado exitosamente, se muestra el estado de la GREEN Zone con la IP asignada (192.168.0.15) y la URL de gestión web (192.168.0.15:10443). Desde este menú el usuario puede acceder a shell para cambiar contraseñas o iniciar el asistente de configuración de red.

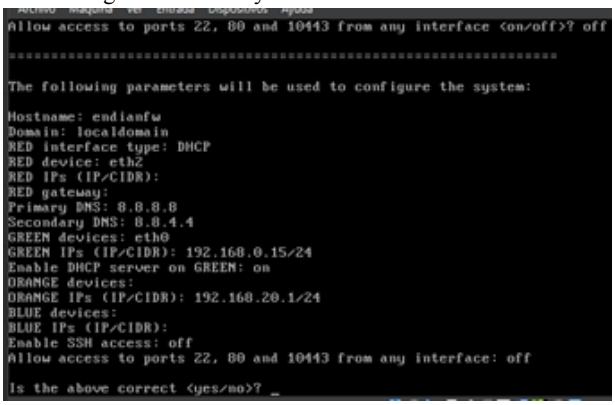
Fig. 5 Consola de gestión inicial del firewall instalado.



Fuente: Autoría Propia

Se procede a la visualización y confirmación de los parámetros del sistema definidos. En este resumen se verifica que la interfaz RED está configurada por DHCP, se validan los servidores DNS públicos y se comprueba el direccionamiento IP de las zonas GREEN (192.168.0.15/24) y ORANGE (192.168.20.1/24). La aceptación final se valida y aplica esta arquitectura de red al firewall.

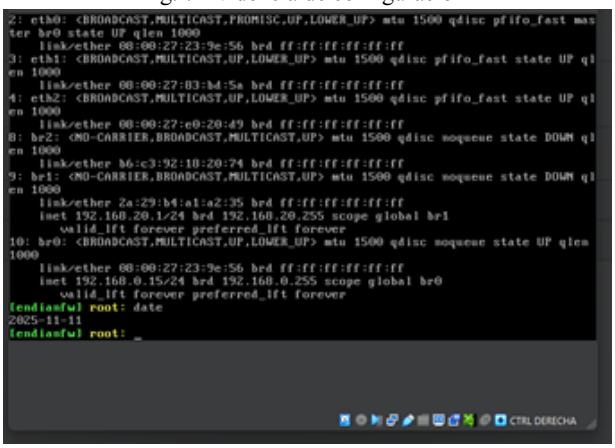
Fig. 6 Validación y resumen de las IPs de red.



Fuente: Autoría Propia

Posterior a la aplicación de la configuración se ejecutó una inspección directa a través de la interfaz de comandos. Esta acción permitió confirmar que las interfaces br1 (ORANGE) y br0 (GREEN) se encuentran en estado activo (UP). Crucialmente, se validó la correcta vinculación de sus respectivas direcciones IP (192.168.20.1/24 y 192.168.0.15/24), lo cual certifica el despliegue exitoso de la topología de red.

Fig. 7 Evidencia de configuración



Fuente: Autoría Propia

3 TEMÁTICA 2: CONFIGURACIÓN NAT

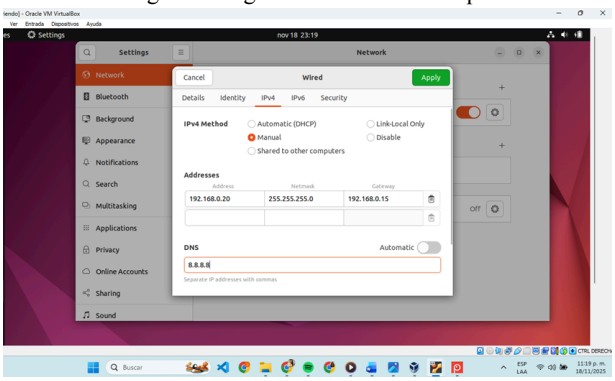
En esta temática el objetivo es demostrar la correcta configuración de NAT en Endian permitiendo que tanto la LAN como la DMZ establezcan comunicación hacia la red WAN, manteniendo la seguridad y aislamiento entre zonas.

3.1 CONFIGURACIÓN DE LA RED LAN (GREEN)

La estación de trabajo Ubuntu Desktop fue configurada con una IP estática perteneciente a la zona GREEN:

- IP: 192.168.0.20
- Máscara: 255.255.255.0
- Gateway: 192.168.0.15 (interfaz GREEN de Endian)
- DNS: 8.8.8.8

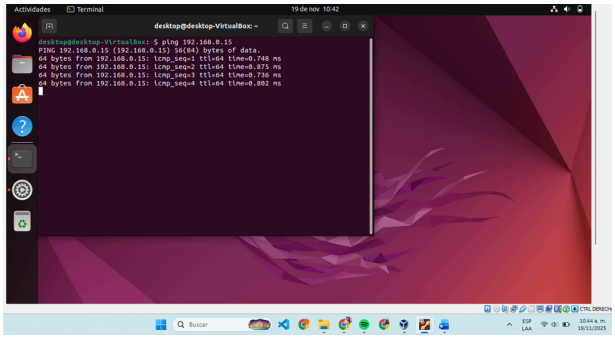
Fig. 8 Configuración de red Desktop



Fuente: Autoría Propia

Verificamos la conectividad al firewall ejecutando el comando ping 192.168.0.15

Fig. 9 Verificación de conectividad hacia el firewall



Fuente: Autoría Propia

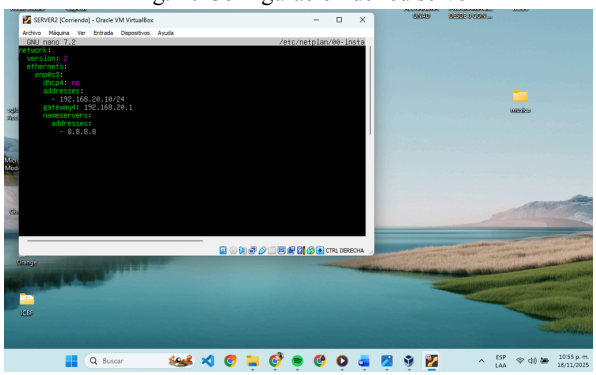
3.2 Configuración de la red DMZ (ORANGE)

El servidor Ubuntu Server asignado como DMZ se configuró con:

- IP: 192.168.20.10
- Máscara: 255.255.255.0
- Gateway: 192.168.20.1 (interfaz ORANGE de Endian)
- DNS: 8.8.8.8

Como lo podemos evidenciar en la figura 10

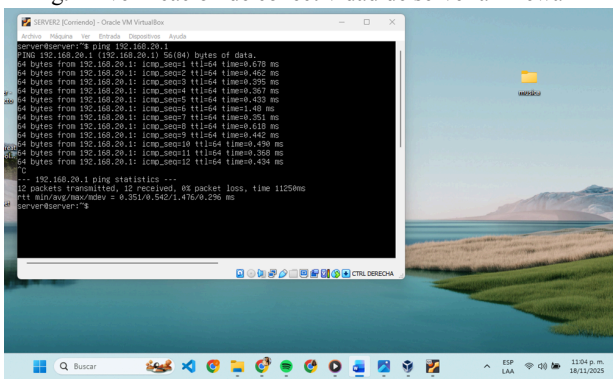
Fig. 10 Configuración de red server



Fuente: Autoría Propia

La comunicación con Endian la verificamos cuando ejecutamos el comando ping 192.168.20.1

Fig. 11 Verificación de conectividad de server al firewall

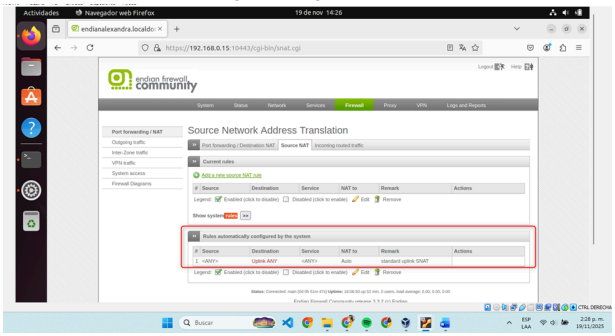


Fuente: Autoría Propia

3.3 VERIFICACIÓN DE NAT (SNAT / MASQUERADE)

Endian genera automáticamente una regla de NAT para todas las zonas internas, esta regla se verificó desde el apartado Firewall → Port forwarding / NAT → Show system rules

Fig. 12 Regla NAT



Fuente: Autoría Propia

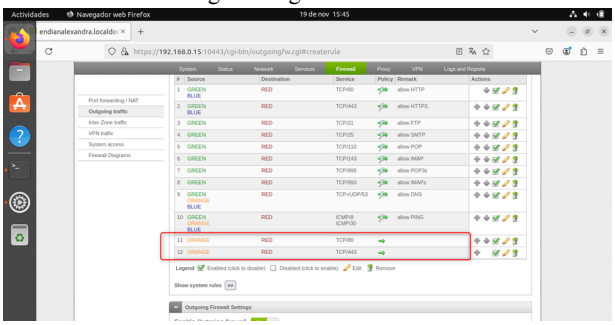
3.4 REGLAS DE SALIDA DESDE LA DMZ HACIA INTERNET

Como seguridad predeterminada, la DMZ no tiene acceso HTTP/HTTPS a la WAN, por lo que se crearon reglas en el apartado Firewall → Outgoing traffic

Reglas creadas:
ORANGE → RED → HTTP (ALLOW)
ORANGE → RED → HTTPS (ALLOW)

Esto habilita la navegación y actualización del servidor DMZ.

Fig. 13 Reglas de salida

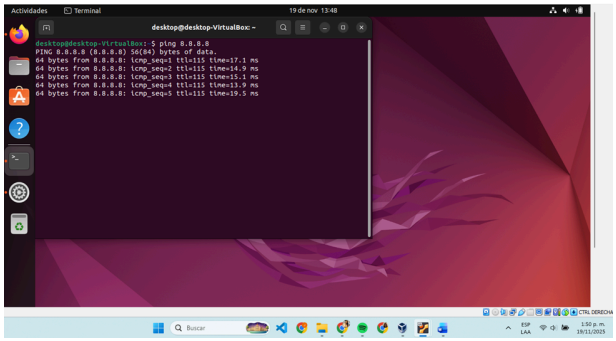


Fuente: Autoría Propia

3.5 PRUEBAS DE CONECTIVIDAD

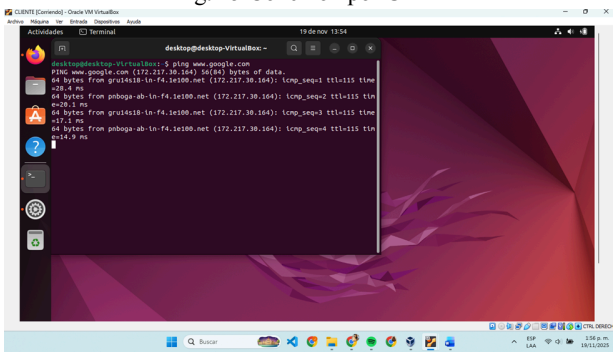
Verificamos la conexión de NAT desde LAN (Desktop), donde se evidencia a continuación de manera satisfactoria

Fig. 14 Conexión por ip



Fuente: Autoría Propia

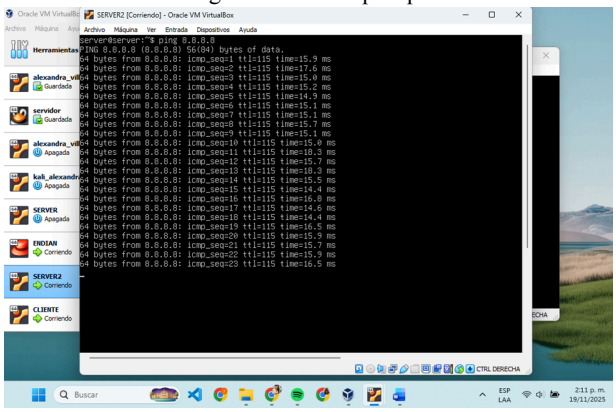
Fig. 15 Conexión por URL



Fuente: Autoría Propia

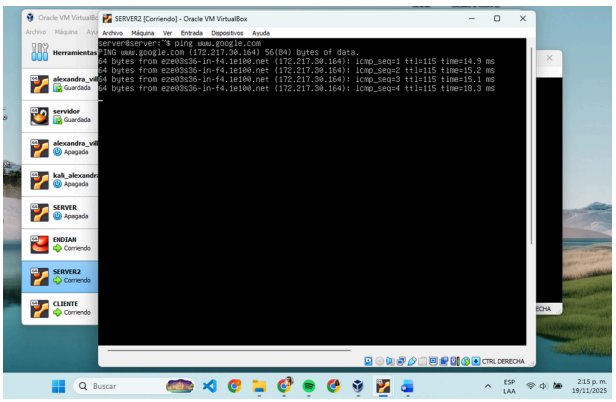
Verificamos la conexión de NAT desde DMZ(SERVER), donde se evidencia a continuación de manera satisfactoria

Fig. 16 Conexión por ip



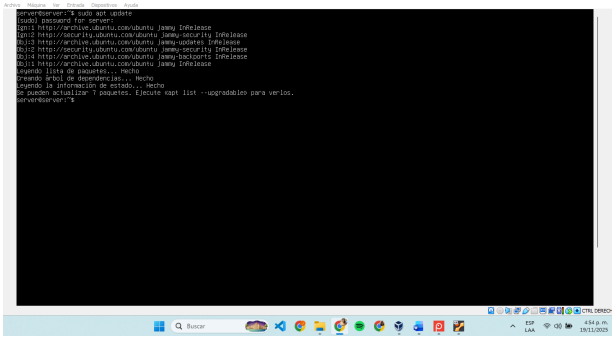
Fuente: Autoría Propia

Fig. 17 Conexión por URL



Fuente: Autoría Propia

Fig. 18 Conexión con sudo apt

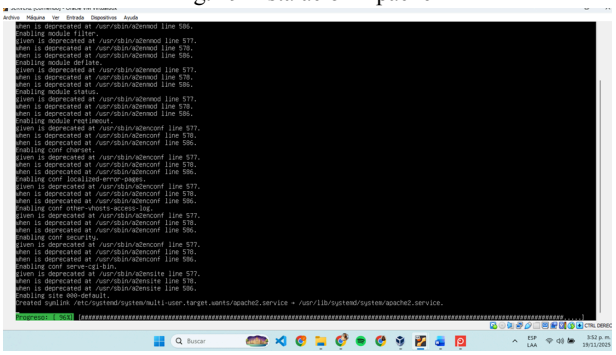


Fuente: Autoría Propia

3.5 INSTALACIÓN DE SERVICIO WEB EN DMZ

El servicio que instalamos es apache2 ejecutando el comando sudo apt install apache2

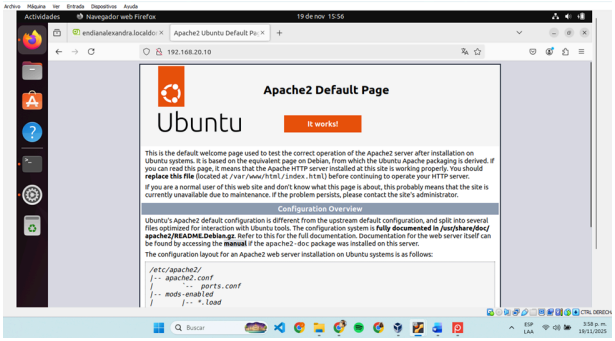
Fig. 19 Instalación Apache



Fuente: Autoría Propia

Para verificar el acceso de LAN hacia DMZ ingresamos al navegador del Desktop con la siguiente URL http://192.168.20.10 y evidenciamos que la página Apache fue accesible desde la LAN, evidenciando que la infraestructura interna opera de forma correcta.

Fig. 20 Ejecución de apache en Desktop



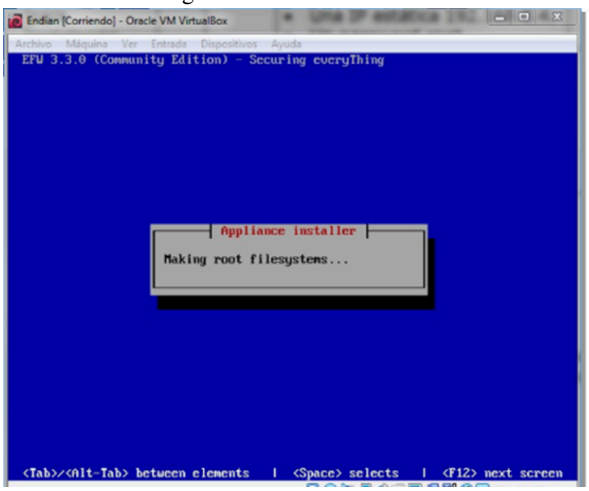
Fuente: Autoría Propia

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

4.1. INSTALACIÓN DE ENDIAN

Se continúa el trabajo del equipo instalando Endian Firewall Community una solución gratuita para seguridad perimetral, se explica cómo descargar y verificar la ISO, además de preparar el medio de instalación, esto se resume en los pasos para instalarlo en un servidor VM y hacer la configuración inicial de red, en pocas palabras cualquier usuario puede dejar funcionando un firewall robusto.

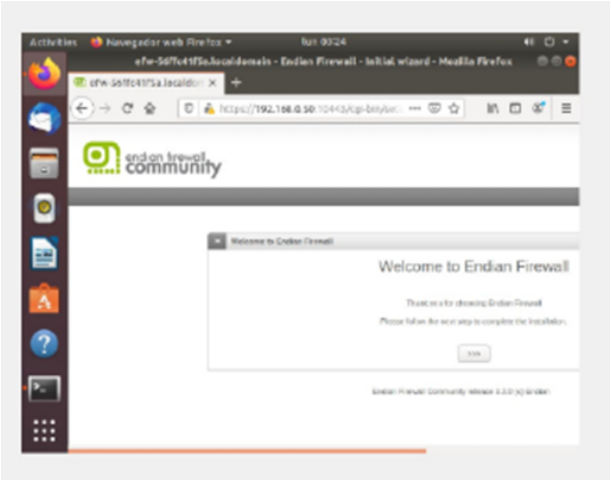
Fig. 21 Instalación de Endian



Fuente: Autoría Propia

En la imagen se ve Ubuntu con Firefox mostrando la página inicial de Endian Firewall. Es el asistente al que entras usando la IP interna y que confirma que la instalación ya quedó lista, desde ahí se sigue con lo más importante: la configuración de contraseñas, zonas de red y algunas opciones de seguridad, básicamente es la pantalla desde donde empiezas a dejar el firewall funcionando y a manejar todas sus herramientas.

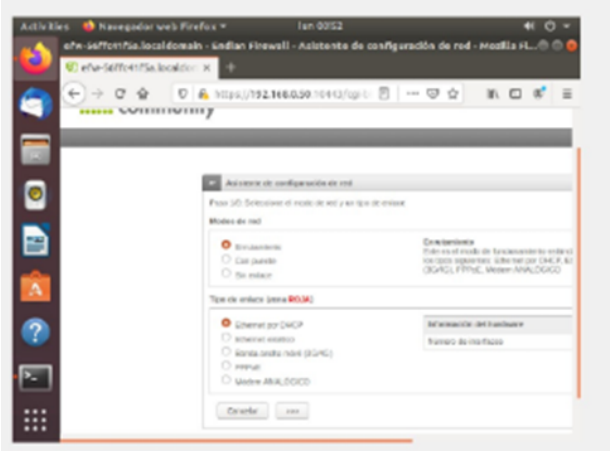
Fig. 22: Configuración de Endian



Fuente: Autoría Propia

La zona RED en Endian Firewall es la red externa, la conexión hacia Internet. En la configuración inicial se elige cómo se va a conectar (DHCP, IP fija, PPPoE, etc.) y se definen datos como la IP, la máscara y la puerta de enlace, esta parte es clave porque determina cómo el firewall se comunica con el proveedor. Al ser una zona “no segura”, Endian aplica reglas más estrictas para proteger la red interna.

Fig. 23 configuración de la zona roja

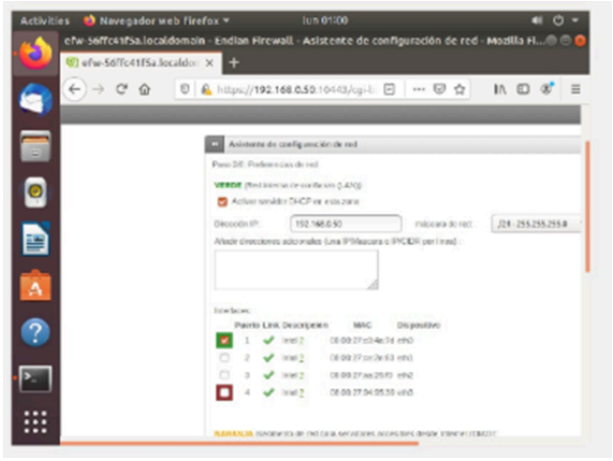


Fuente: Autoría Propia

La zona Verde en Endian Firewall es la red interna confiable donde están los equipos y servidores de los usuarios. En su configuración se asigna la IP del firewall y la máscara de subred porque será el punto de acceso para todos los dispositivos.

Esta zona es la base de la red protegida y permite que los equipos naveguen a través del firewall con sus filtros y medidas de seguridad, configurarla bien asegura una comunicación segura y estable dentro de la red.

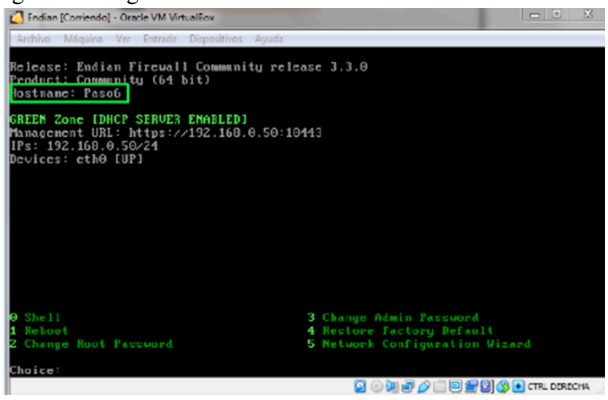
Fig. 24: configuración de la zona verde



Fuente: Autoría Propia

La imagen muestra la consola principal de Endian 3.3.0 corriendo en VirtualBox. Ahí se ve el estado de la zona GREEN, donde el DHCP está activo y también aparece la IP para entrar al panel web. En la parte de abajo salen opciones como abrir la Shell, cambiar contraseñas o reiniciar el asistente de red. Básicamente, es el panel básico del firewall antes de pasar a configuraciones más avanzadas.

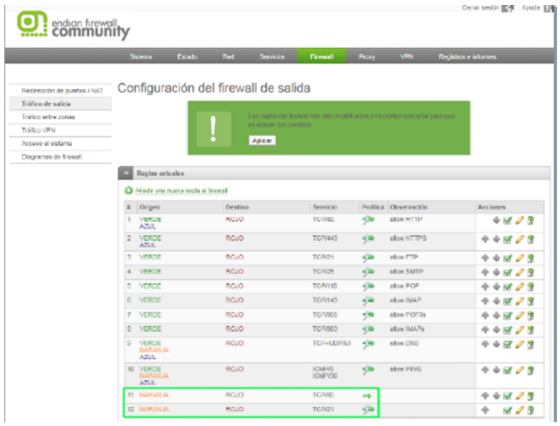
Fig. 25 Configuración de Endian



fuente. autoría propia

La imagen muestra la sección *Outgoing* del firewall de Endian donde se controlan las reglas de tráfico que salen desde la red interna, ahí se ven reglas como las de HTTP y FTP, que están permitidas para que los equipos de la zona GREEN puedan navegar y transferir archivos, la tabla también muestra datos como protocolo, origen, destino y puertos, además de opciones para editar o borrar reglas, en resumen esta es la parte que asegura la conectividad básica hacia Internet pero con control del tráfico saliente.

Fig. 26: permisos de http con puerto 80 y FTP con puerto 21



fuente: autoría propia

La imagen muestra la sección *Incoming* del firewall de Endian donde se gestionan las reglas de tráfico, se destaca una regla que bloquea ICMP, incluyendo ping y traceroute desde la red interna (GREEN) hacia Internet (RED), esta acción aplicada es DROP, esto ayuda a proteger la red evitando que dispositivos externos o internos puedan identificarla y descubrir sus equipos.

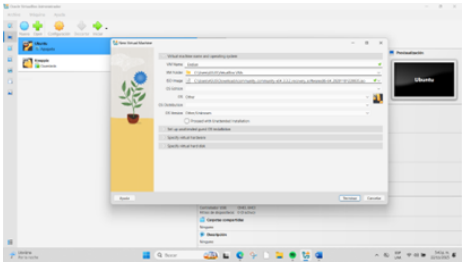
Fig. 27: bloqueo de protocolo ICMP PARA TIPO 8 Y 30

fuente: autoría propia

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

Continuando con lo realizado en los puntos anteriores continuamos con la creación de la VM de ENDIAN

Fig. 28: Creación de VM de Endian

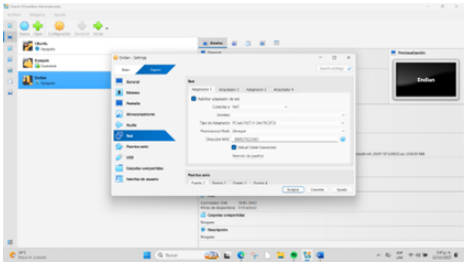


fuente: autoría propia

Realizamos el proceso de instalación con la ISO de Endian como se evidencia en la imagen fig. 28

Configuramos las zonas de Endian

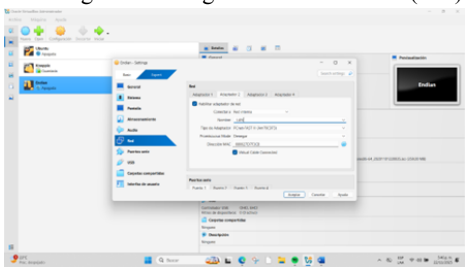
Fig. 29: Configuración Zona Roja (internet)



fuente: autoría propia

La imagen muestra la configuración de la Zona Roja (Internet) en una máquina virtual, donde se ajustan los parámetros de conexión y red para que el firewall se comunique correctamente con el exterior, esto es una parte fundamental para que el sistema funcione bien con Internet.

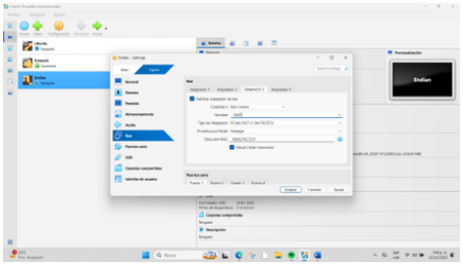
Fig. 30: Configuración Zona Verde (Lan)



fuente: autoría propia

La imagen muestra la configuración de la Zona Verde (LAN) en una máquina virtual donde se definen los detalles de la red interna para que el firewall controle correctamente el tráfico local, es fundamental para asegurar la comunicación segura dentro de la red.

Fig. 31: Configuración Zona Naranja (DMZ)

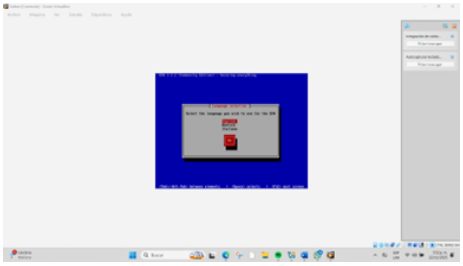


fuente: autoría propia

La imagen muestra la configuración de la Zona Naranja (DMZ) en una máquina virtual donde se establecen los parámetros para una red semi-segura que separa el tráfico entre la red interna y la externa. Esto ayuda a proteger los sistemas críticos manteniéndolos aislados.

Configuramos

Fig. 32: Configuracion instalacion Endian

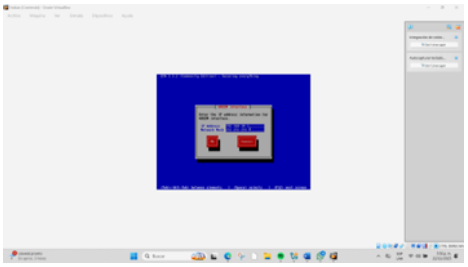


fuente: autoría propia

En la imagen de la Fig,32 se observa la configuración en la forma de instalación de envian, donde paso a paso se va realizando para su debido proceso de ejecución

Agregamos la IP Adrdress

Fig. 33: Configuración IP Addres

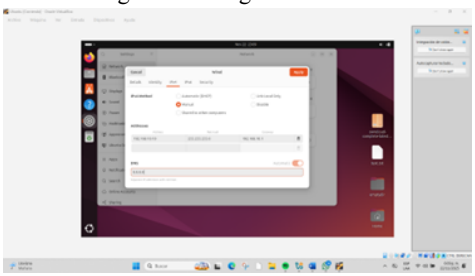


fuente: autoría propia

Posteriormente se configura como evidencia en la imagen fig 33 se muestra la ventana de configuración donde se agrega la dirección IP al sistema. Aparece un cuadro azul típico del instalador solicitando confirmar o editar el valor ya que es parte del proceso de ajuste de red durante la instalación o configuración del servidor.

Se configura la red dentro de Ubuntu

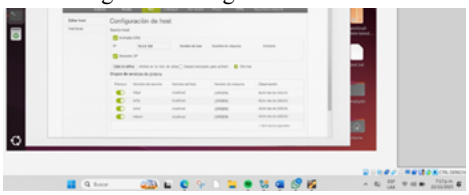
Fig. 34: Configuración de Red



fuente: autoría propia

Se realiza la configuración del Host

Fig. 35: Configuracion de Host

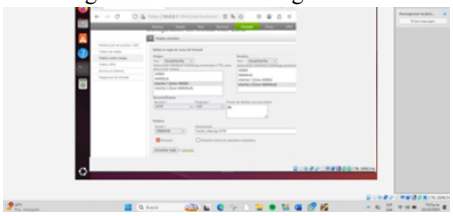


fuente: autoría propia

Se debe crear una nueva regla en el firewall para permitir la comunicación desde la zona Verde (LAN) hacia la zona Naranja (DMZ).

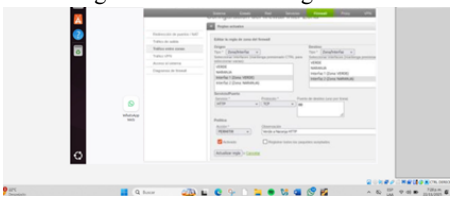
Detalles de la regla:
Nombre: Verde a Naranja HTTP y FTP
Protocolo: TCP
Puertos permitidos:
80 para tráfico HTTP
21 para tráfico FTP
Origen: Zona Verde (LAN)
Destino: Zona Naranja (DMZ)
Acción: Permitir el tráfico

Fig. 36: Creación de regla HTTP



fuente: autoría propia

Fig. 37: Creación de regla FTP

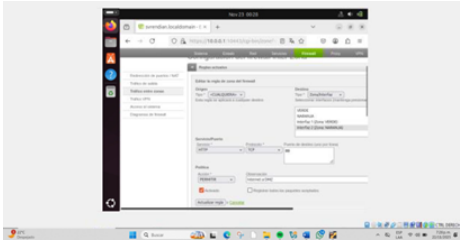


fuente: autoría propia

Se debe crear otra regla para permitir la comunicación desde la zona Internet hacia la zona DMZ.

Detalles de la regla:
Nombre: Internet a DMZ
Protocolo: TCP
Puerto permitido:
80 para tráfico HTTP
Origen: Zona Roja (WAN)
Destino: Zona Naranja (DMZ)
Acción: Permitir el tráfico

Fig. 38: regla comunicación zona naranja



fuente: autoría propia

Para verificar el tráfico entre zonas, se debe acceder a Seguridad > Firewall > Registros, donde es posible visualizar la información del tráfico de salida generado entre las distintas zonas del sistema.

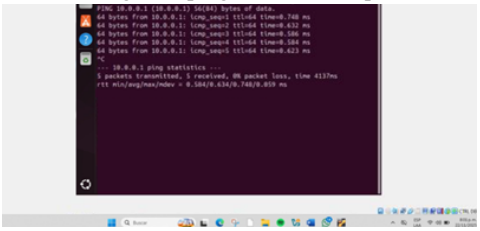
Fig. 39: Ilustración tráfico de salida

fuente: autoría propia

Una vez creadas las reglas de firewall en Endian, es esencial aplicarlas para que tengan efecto en la red. Después de configurar las reglas que permiten o bloquean el tráfico entre las zonas Verde, Naranja, DMZ y WAN para los servicios HTTP y FTP se deben guardar y aplicar los cambios para activar la nueva configuración.

El firewall garantiza la gestión correcta de las conexiones entre las distintas zonas, luego es necesario verificar el tráfico inter-zonas para confirmar que las reglas funcionan como se espera y que el tráfico permitido fluye adecuadamente.

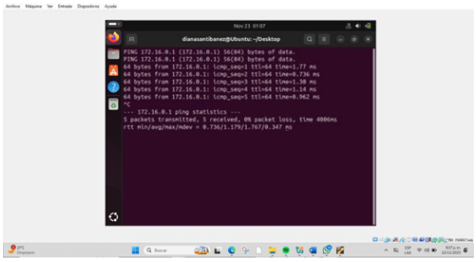
Fig. 40: ping desde Desktop



fuente: autoría propia

Desde un navegador web ubicado en la zona Verde (LAN), se debe intentar acceder a un servidor web alojado en la zona Naranja (DMZ) utilizando la dirección IP 172.16.0.1 para comprobar que la comunicación funciona correctamente.

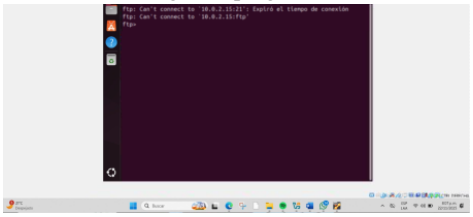
Fig. 41: ping



fuente: autoría propia

Para el protocolo FTP, se lleva a cabo la verificación de conectividad desde un equipo de escritorio utilizando el comando ping con el objetivo de confirmar que exista comunicación entre los dispositivos involucrados.

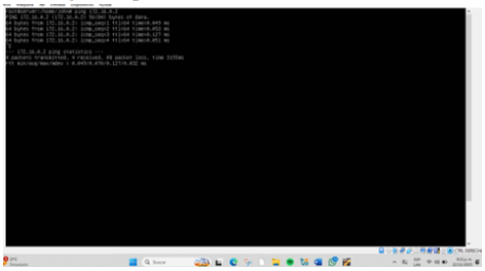
Fig. 42: ping FPT



fuente: autoría propia

Se realiza un ping desde la máquina ubicada en la LAN hacia la DMZ para confirmar que puede comunicarse con el servidor en dicha zona y que el tráfico ICMP está permitido entre ambas áreas de la red.

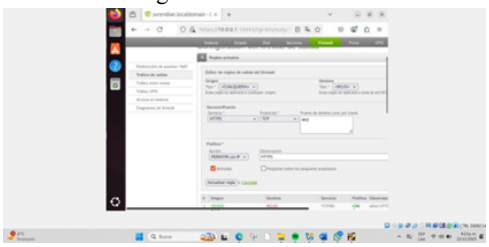
Fig. 43: prueba conexión desde servidor



fuente: autoría propia

La regla de firewall de salida permitirá el tráfico HTTP desde la zona LAN hacia Internet garantizando que los dispositivos internos puedan acceder a sitios web externos sin restricciones.

Fig. 44: tráfico HTTP



fuente: autoría propia

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

6.1 Configuración de red implementada.

Para la presente temática se implementará la configuración Proxy HTTP (no transparente) con políticas de autenticación utilizando el firewall Endian, esta configuración se llevará a cabo considerando la segmentación de red definida en la Temática 1 y aplicándola sobre las tres máquinas virtuales desplegadas en VirtualBox garantizando así un entorno controlado para la gestión del tráfico, la aplicación de filtros y la validación de credenciales de acceso.

La configuración de segmentación de red utilizada es la siguiente:
Ubuntu Desktop (Zona Verde - LAN):
Tipo de red: Red interna (internet) llamada verde.
Dirección IP: 192.168.0.15
Máscara de subred: 255.255.255.0

Ubuntu Server (Zona Naranja - DMZ):
Tipo de red: Red interna (internet) llamada naranja.
Dirección IP: 192.168.20.1
Máscara de subred: 255.255.255.0

Endian actúa como cortafuegos entre la LAN y la DMZ, y aloja el servicio de proxy HTTP con filtrado de contenidos y autenticación permitiendo 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.

6.2 Configuración de Endian.

Ingresamos a la interfaz de Endian desde Ubuntu Desktop por la ip 192.168.0.15:10443/, verificamos la configuración DHCP confirmando que se encuentre habilitado y configurado según lo establecido por la configuración de la temática 1

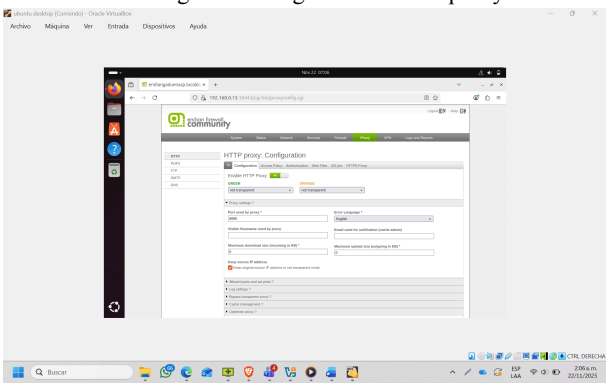
Fig. 45: Configuración DHCP Server

fuente: autoría propia

Se habilita la configuración Proxy HTTP en modo no transparente con el fin de gestionar el tráfico mediante el módulo de filtrado web (Web Filter). Dentro de este componente se definen dos políticas de filtrado: una destinada a usuarios con acceso a la mayoría de los recursos web y otra configurada con accesos restringidos limitando el alcance de navegación según las directrices operativas establecidas.

Cada política se implementa mediante ACLs (Access Control Lists) y parámetros específicos de control permitiendo aplicar selectivamente reglas de validación, inspección y restricción del tráfico de acuerdo al perfil asignado a cada grupo de usuarios.

Fig. 46: Configuración HTTP proxy

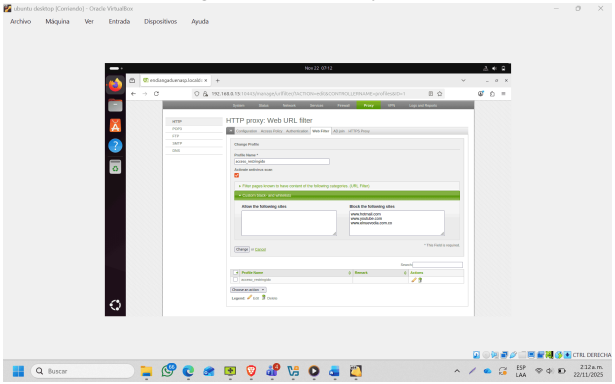


fuente: autoría propia

Se procede a crear un perfil de navegación específico dentro del módulo de Proxy HTTP de Endian en el cual se define una política de filtrado basada en listas negras tales como youtube.com, hotmail.com y elnuevodia.com.co

La lista negra es gestionada mediante reglas de control de acceso (ACL), lo que permite al proxy bloquear de forma automática cualquier solicitud HTTP/HTTPS dirigida a dichos portales, esta configuración garantiza que el tráfico generado por los usuarios asociados al perfil sea filtrado antes de abandonar la red, reforzando los mecanismos de restricción y cumplimiento de políticas de uso aceptable.

Fig. 47: HTTP Proxy filtro web



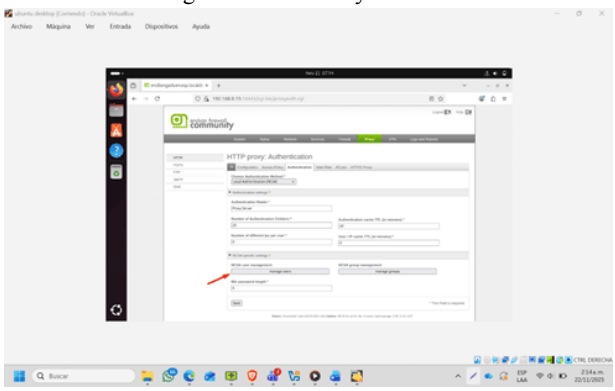
fuente: autoría propia

6.3 Autenticación por usuario

Se implementa la autenticación por usuario mediante el módulo de Proxy de Endian creando un usuario individual y asociándose a un grupo previamente definido a este grupo se le asigna una política de acceso específica la cual se le asigna el perfil de filtrado configurado en el punto anterior y lo vincula directamente con el mecanismo de autenticación.

El proxy valida las credenciales del usuario antes de permitir el establecimiento de sesiones HTTP/HTTPS, aplicando las restricciones, privilegios y reglas de filtrado correspondientes al perfil y al grupo asociado, esto garantiza un control sobre la navegación y una administración de los permisos de acceso dentro de la red segmentada.

Fig. 48: HTTP Proxy autenticación

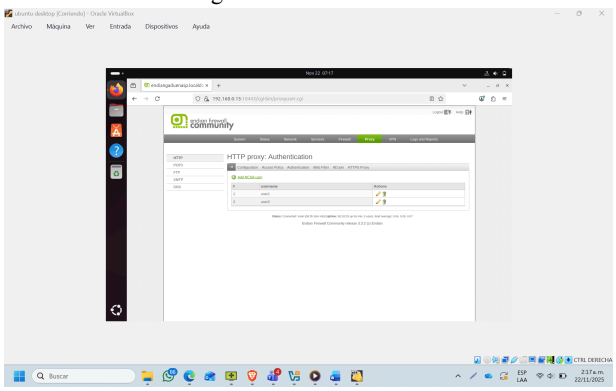


fuente: autoría propia

Una vez realizado la autenticación procedemos a crear los usuarios:

- User1, asociado al grupo con políticas de navegación restringida
- User2, vinculado al perfil con acceso libre.

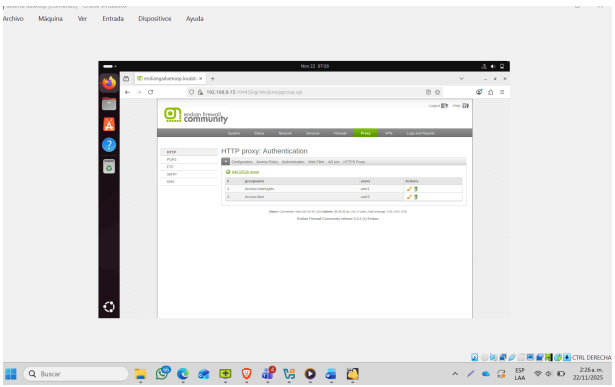
Fig. 49: Creación de usuarios



fuente: autoría propia

Se procede a la creación de los grupos de control dentro del módulo de administración del proxy HTTP

Fig. 50: Creación de grupos



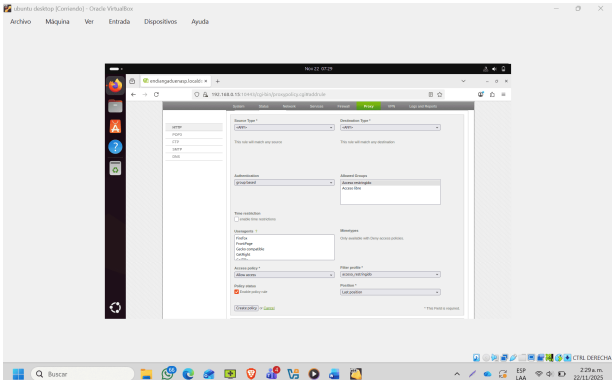
fuente: autoría propia

6.4 Políticas de Acceso para las restricciones

Se accede al módulo de políticas de acceso del Proxy HTTP con el fin de aplicar las restricciones correspondientes a los grupos creados, desde esta sección se definen las reglas que determinan el comportamiento de navegación para cada grupo vinculando los Usuarios para agregar listas negras y parámetros de autenticación configurados con anterioridad.

Una vez asignadas estas políticas el proxy establece qué recursos web pueden ser accedidos o bloqueados por los diferentes grupos, garantizando que las restricciones se apliquen en tiempo real sobre el tráfico HTTP/HTTPS generado desde la red segmentada

Fig. 51: configuración de políticas de acceso a los grupos

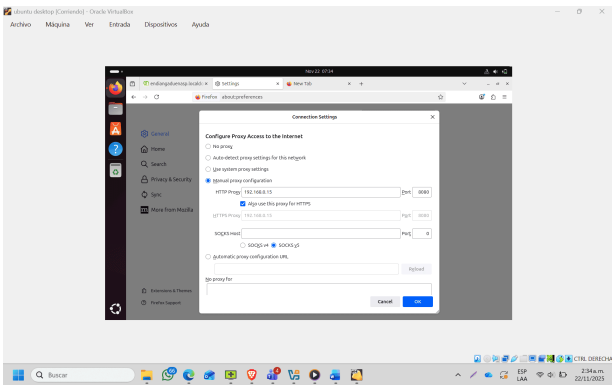


fuente: autoría propia

6.5 Verificación de restricciones desde la LAN

Para validar la correcta aplicación de las políticas de filtrado se realiza una prueba de navegación desde un host ubicado en la red LAN utilizando y configurando la entrada por ip estática (192.168.0.15) a un navegador web estándar para acceder a la red.

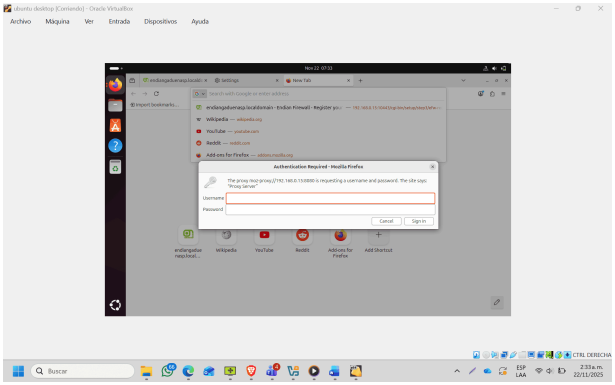
Fig. 52: Configuración del proxy del navegador



fuente: autoría propia

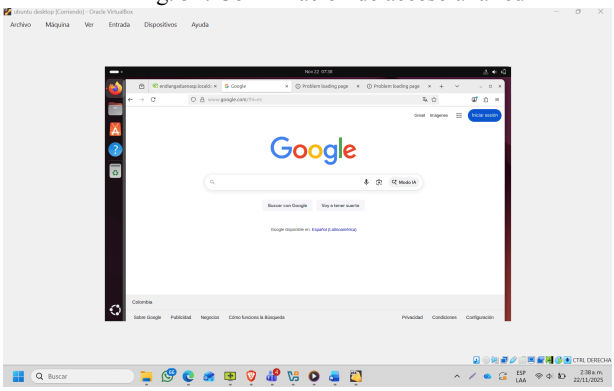
Al ingresar nos logueamos con el usuario User1 e intentamos acceder a los dominios incluidos en la lista negra configurada en el Proxy HTTP, como YouTube, Hotmail y Elnuevodía, el objetivo es confirmar que las solicitudes HTTP/HTTPS dirigidas a dichos portales sean interceptadas y bloqueadas por el proxy conforme a las reglas definidas.

Fig. 53: ingreso con un usuario de navegación



fuente: autoría propia

Confirmamos Normal conexión e ingreso a la red
Fig. 54: Confirmación de acceso a la red

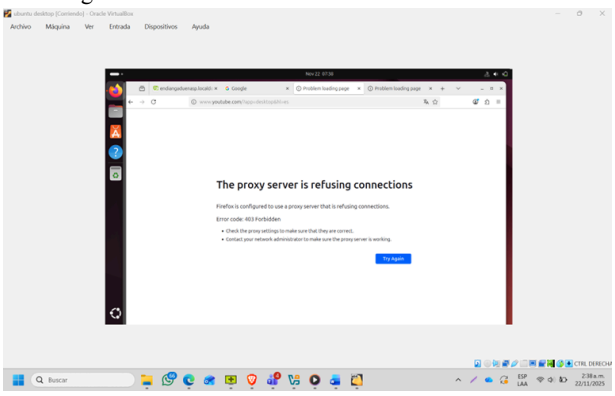


fuente: autoría propia

Se realiza una solicitud directa al portal a través del navegador para confirmar que el tráfico HTTP/HTTPS hacia Youtube.com en el que es interceptado y denegado por el firewall Endian, La cual nos muestra -El servidor proxy rechaza las conexiones- valida que las reglas de filtrado, el perfil asignado y la política de autenticación están siendo

aplicados correctamente confirmando la efectividad del mecanismo de restricción hacia youtube.com dentro del entorno segmentado.

Fig. 55: Confirmación de restricción hacia Youtube.com



fuente: autoría propia

7 CONCLUSIONEs

7.1. TEMÁTICA 1

El despliegue de la instancia GNU/Linux Endian en VirtualBox se ha validado, cumpliendo el objetivo de implementar una arquitectura de firewall segmentada.

Se configuraron exitosamente las zonas clave:

- Zona GREEN (LAN): 192.168.0.15/24.
- Zona ORANGE (DMZ): 192.168.20.1/24.
- Zona RED (WAN): Definida por DHCP para acceso a Internet.

La verificación final de la conectividad certifica el correcto funcionamiento y la operatividad de las interfaces, culminando con éxito la preparación del sistema de seguridad.

7.2. TEMÁTICA 2

El proceso permitió demostrar el funcionamiento adecuado de NAT en Endian Firewall para las zonas GREEN y ORANGE. Se verificó que ambas redes pueden comunicarse con la WAN, garantizando navegación completa y seguridad adecuada.

También se comprobó la funcionalidad del reenvío NAT (SNAT automático) y su impacto en el tráfico de salida. El aislamiento entre LAN y DMZ se mantuvo, respetando los principios de seguridad perimetral, mientras que el servicio web de la DMZ pudo ser accedido correctamente desde la LAN y desde Internet.

7.3. TEMÁTICA 3

Esta configuración permite que el servidor web en Ubuntu pueda ofrecer sus servicios HTTP y FTP desde la DMZ sin inconvenientes, asegurando que los usuarios puedan acceder a lo que necesitan, Además al bloquear los tipos de ICMP usados para hacer ping, se evita que otros equipos puedan detectar o explorar la red.

En conjunto, estas reglas permiten mantener los servicios accesibles sin sacrificar la seguridad también ayudan a reducir posibles intentos de reconocimiento por parte de atacantes; de esta forma la red se mantiene funcional, ordenada y mejor protegida frente a riesgos externos.

7.4. TEMÁTICA 4

La configuración de reglas en Endian Firewall permite controlar con precisión el tráfico entre LAN, DMZ y WAN, garantizando que solo las conexiones autorizadas fueran permitidas.

Las pruebas con HTTP y FTP confirmaron la efectividad del filtrado inter-zona, validando la comunicación permitida y bloqueando la no autorizada.

El análisis del tráfico evidenció la importancia del firewall como herramienta clave para proteger infraestructuras GNU/Linux y fortalecer habilidades de administración segura.

7.5. TEMÁTICA 5

La implementación del Proxy HTTP no transparente con autenticación evidencia la importancia de los controles de acceso en la red corporativa, ya que permite regular el tráfico, aplicar políticas de seguridad, segmentar usuarios y garantizar el cumplimiento de las restricciones definidas por la organización

8 REFERENCIAS

Aplicar las normas APA V7 ed

1. LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learningmaterials/101-500/101/101.1/
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. Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

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

6. Canonical (2023). Guía del Ubuntu desktop 20.04 LTS . Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html
7. Debian (2023). El manual del administrador de Debian 12.5.0 . Debian https://www.debian.org/releases/stable/amd64/index.es.html
8. Oracle (2020). Manual de usuario VirtualBox . VirtualBox. https://www.virtualbox.org/manual/
9. Endian (2016), Endian UTM 3.2 Manual referencia . Endian. http://docs.endian.com/3.2/utm/index.html
10. 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