REDES SEGURAS CON ENDIAN: UN ENFOQUE ACADÉMICO

Germán Padilla Useda
e-mail: gpadillau@unadvirtual.edu.co
Diana Marcela Castiblanco Sanchez
e-mail: dmcastiblancosa@unadvirtual.edu.co
John Fredy Tibagan Motavita
e-mail: jftibaganm@unadvirtual.edu.co
Diego Andres Sandoval Diaz
e-mail: dasandovald@unadvirtual.edu.co
Marcos Fernando Rios Cruz
e-mail: mfrioscr@unadvirtual.edu.co

RESUMEN: *Este trabajo presenta la implementación y configuración del sistema de seguridad perimetral GNU/Linux Endian Firewall dentro de un entorno virtualizado utilizando VirtualBox. El proyecto se divide en cinco temáticas, desarrollando progresivamente una solución de red segura y segmentada mediante la correcta administración de las zonas Verde (LAN), Roja (WAN) y Anaranjada (DMZ). En la primera temática se realiza la instalación efectiva del sistema Endian, junto con la asignación de interfaces de red para cada zona. La segunda temática aborda la configuración de reglas NAT, permitiendo la salida a Internet desde la LAN y desde la DMZ, incluyendo el reenvío de puertos. Posteriormente, se implementan reglas de firewall que permiten servicios HTTP y FTP en la zona DMZ y se bloquean protocolos como ICMP para reforzar la seguridad. En la cuarta temática se configuran políticas de acceso entre zonas, verificando el tráfico permitido y denegado, de acuerdo con distintos escenarios de prueba. Finalmente, se establece un proxy HTTP no transparente con autenticación por usuario y aplicación de políticas de filtrado de contenido web, demostrando el bloqueo de sitios específicos desde la red LAN. La ejecución de estas temáticas evidencia una arquitectura de red segura, flexible y controlada, alineada con las mejores prácticas en administración de sistemas y redes.*

PALABRAS CLAVE: DMZ, Endian Firewall, Linux, NAT

1 INTRODUCCIÓN

En el contexto de la seguridad perimetral y la gestión eficiente del tráfico de red, el uso de firewalls dedicados como Endian Firewall se ha convertido en una solución robusta y confiable para entornos empresariales y educativos. Este trabajo presenta el proceso de instalación y configuración del sistema GNU/Linux Endian sobre una máquina virtual en VirtualBox, implementando una topología de red dividida en tres zonas principales: zona verde (LAN), zona naranja (DMZ) y zona roja (WAN). A través de esta configuración, se busca garantizar la segmentación lógica de la red, así como establecer políticas de control y acceso entre las diferentes zonas.

Se desarrollan procedimientos orientados a la configuración de reglas de NAT, control de acceso basado en protocolos y puertos, y la implementación de un proxy HTTP no transparente con autenticación por usuario. Además, se verifica el funcionamiento de los servicios permitidos y restringidos, validando su efectividad mediante pruebas prácticas. Este ejercicio permite comprender de manera integral el funcionamiento de un firewall perimetral, su aplicación en entornos virtualizados y su rol en la protección de infraestructuras informáticas.

2 TEMÁTICA 1.

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).

2.1 DESARROLLO TEMÁTICA 1.

Implementación del Entorno de Virtualización y Diseño de Zonas de Red.

Con el fin de implementar una solución de seguridad perimetral mediante el sistema GNU/Linux Endian Firewall, se diseñó una arquitectura virtualizada compuesta por tres máquinas virtuales (MV) ejecutadas sobre VirtualBox.

La organización del entorno se realizó de la siguiente manera:

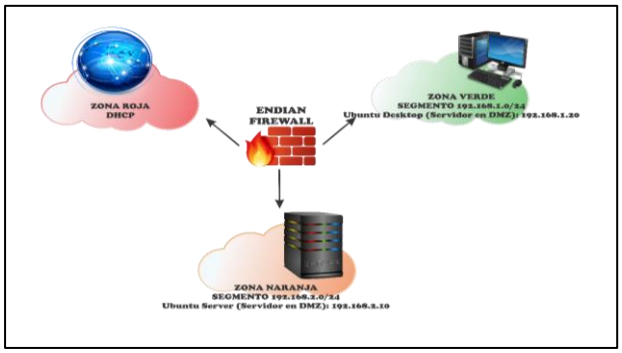
- MV1: Ubuntu Desktop, asignada a la Zona Verde (LAN).
- MV2: Ubuntu Server, asignada a la Zona Naranja (DMZ).
- MV3: Endian Firewall, encargado de gestionar y filtrar el tráfico entre las zonas.

Cada zona de red cumple un propósito específico dentro de la topología de seguridad:

- Zona Verde: Representa la red interna o LAN, desde donde se realiza la administración del firewall y se simula el acceso de los usuarios finales a los servicios disponibles.
- Zona Naranja: Corresponde a la DMZ (zona desmilitarizada), donde se ubican los servidores públicos como servicios web o FTP que deben ser accesibles desde la red externa y la interna con restricciones.
- Zona Roja: Simula la conexión a Internet o red WAN. Esta interfaz está configurada en modo NAT y obtiene su dirección IP mediante DHCP, facilitando el acceso a la red externa sin necesidad de configuración manual.

Esta configuración permite establecer un entorno controlado para la implementación, prueba y verificación de reglas de cortafuegos, traducción de direcciones (NAT) y políticas de acceso entre zonas, respetando los principios de segmentación de redes y defensa en profundidad.

Figura 1. Arquitectura de red virtual para implementación del firewall Endian

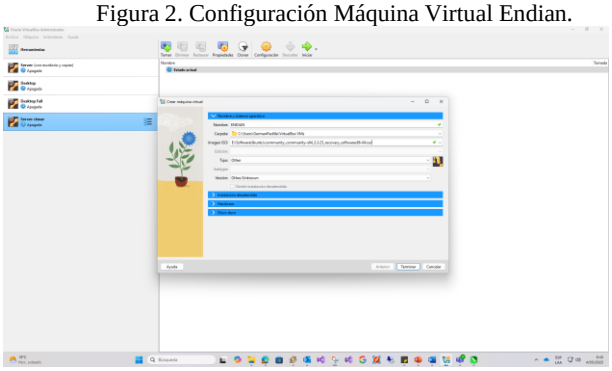


Fuente. Autoría Propia.

Instalación y Configuración de Endian Firewall en Entorno Virtualizado

Para la implementación del cortafuegos Endian Firewall, se procedió inicialmente a la descarga de la imagen ISO desde el sitio oficial en SourceForge (https://sourceforge.net/projects/efw). A continuación, se creó una máquina virtual (MV) en Oracle VM VirtualBox, seleccionando como tipo de sistema "Linux" y versión "Other Linux (64-bit)". Se asignaron los recursos necesarios a la MV, incluyendo memoria RAM, número de procesadores y capacidad de disco duro.

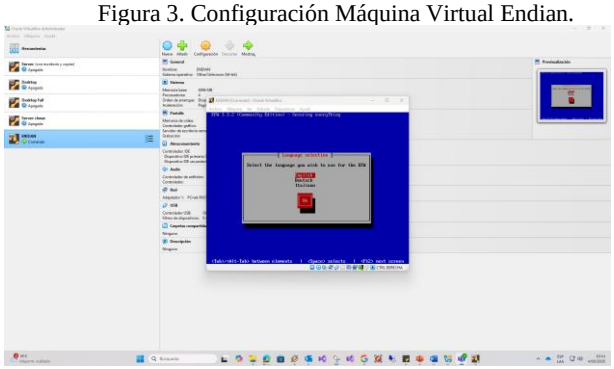
Figura 2. Configuración Máquina Virtual Endian.



Fuente. Autoría Propia.

Una vez creada la máquina virtual en VirtualBox, se procedió a iniciarla con la imagen ISO montada como medio de instalación. Durante el proceso, se seleccionó el idioma "inglés" como predeterminado para garantizar compatibilidad con documentación técnica global. Inmediatamente, el sistema mostró una advertencia crítica en una ventana emergente, alertando sobre la preparación y partición automática del disco principal (/dev/sda), enfatizando que todos los datos existentes serían eliminados irreversiblemente. Tras validar los términos, se aceptó la advertencia navegando con la tecla Tab para resaltar la opción "Yes" y presionando Enter para confirmar.

Figura 3. Configuración Máquina Virtual Endian.

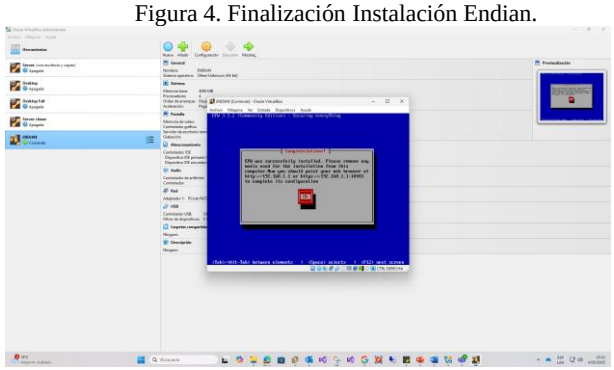


Fuente. Autoría Propia.

El instalador ofreció la opción de habilitar una consola a través del puerto serie, útil para conexiones mediante terminal serial y cable nullmodem. Posteriormente, se solicitó asignar una dirección IP para la interfaz correspondiente a la zona verde (Green Zone).

Finalizada la instalación, se indicó retirar el medio de instalación y se proporcionó la URL de gestión: https://192.168.1.15:10443.

Figura 4. Finalización Instalación Endian.



Fuente. Autoría Propia.

Desde la MV Ubuntu Desktop, accediendo a dicha URL mediante navegador web, se presentó la pantalla de bienvenida al sistema, seguida de la visualización de los datos de configuración de la zona verde: Management URL: https://192.168.1.15:10443, IPs: 192.168.1.15/24, Dispositivo: eth0 [up], así como el menú de opciones accesible por consola.

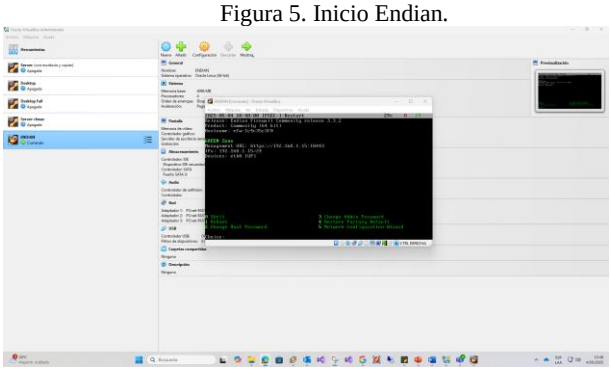
La configuración de red para cada máquina virtual se estableció de la siguiente manera:

- MV Endian:
  - Adaptador 1: Red Interna "RedVerde"
  - Adaptador 2: Red Interna "RedAnaranjada"
  - Adaptador 3: NAT (para acceso a Internet)
- MV Ubuntu Desktop:
  - Adaptador 1: Red Interna "RedVerde"
- MV Ubuntu Server:
  - Adaptador 1: Red Interna "RedAnaranjada"
  - Dirección IP estática asignada: 192.168.2.20/24

Al iniciar Endian Firewall, se confirmó que la zona verde estaba correctamente configurada con la dirección

192.168.1.15/24, y la zona roja (Red externa) obtenía una IP por DHCP: 10.0.2.15/24.

Figura 5. Inicio Endian.



Fuente. Autoría Propia.

Se intentó realizar ping desde las MV Ubuntu Desktop y Ubuntu Server a la IP 192.168.2.15 sin obtener respuesta inicial, lo cual indicaba que era necesario completar la configuración de zonas en Endian Firewall.

Accediendo nuevamente desde el navegador a https://192.168.1.15:10443, se aceptó el mensaje de advertencia de seguridad mediante la opción "Avanzado", se seleccionó el idioma y zona horaria, y se aceptó la licencia GNU General Public License. A continuación, se configuraron las contraseñas para el administrador de la interfaz web y para el usuario root por SSH.

En la siguiente sección, se mostró la configuración de la red roja con modo de red “Routing” y tipo de enlace “Ethernet por DHCP”. También se identificaron las tres interfaces de red correspondientes a los tres adaptadores configurados en VirtualBox para la MV de Endian.

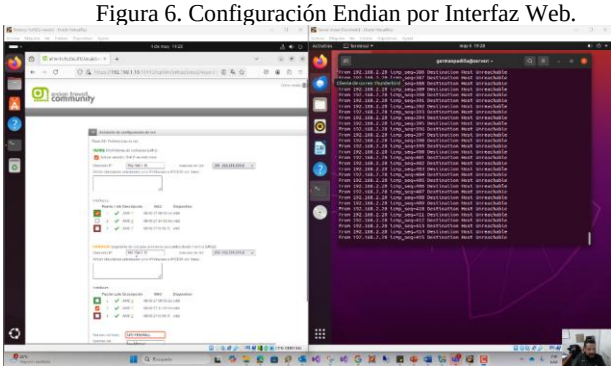
Finalmente, se accedió a la interfaz web introduciendo las credenciales de acceso (usuario: admin, contraseña previamente definida), completando así la instalación y habilitación del sistema para configurar reglas de firewall y servicios adicionales.

Una vez completada la instalación de Endian Firewall y accediendo a su interfaz web mediante la dirección https://192.168.1.15:10443 desde la máquina virtual Ubuntu Desktop, se visualizó que la zona verde (Green Zone) se encontraba configurada con la dirección IP 192.168.1.15/24.

Se procedió con la configuración de la zona anaranjada (Orange Zone), asignándole la dirección IP 192.168.2.15 con máscara de subred 255.255.255.0 (/24). La zona roja (Red Zone), correspondiente al acceso a Internet, permaneció configurada para obtener su dirección IP mediante DHCP.

Posteriormente, se definió el nombre del host como SVR-FIREWALL y se dejó el nombre del dominio como LOCALHOST. En el siguiente paso, se confirmó que las tres interfaces de red estaban correctamente detectadas y configuradas.

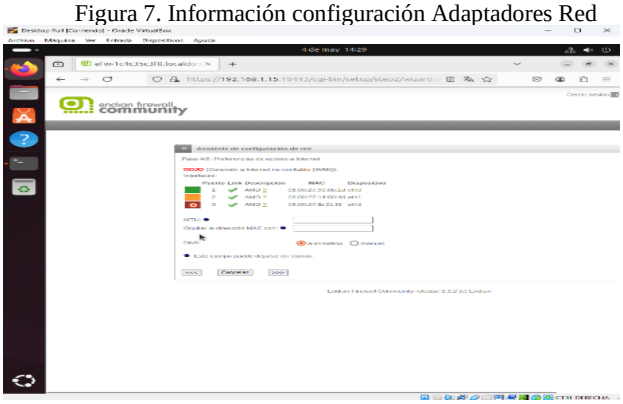
Figura 6. Configuración Endian por Interfaz Web.



Fuente. Autoría Propia.

La configuración del servidor DNS se estableció de forma automática. En la siguiente pantalla, se solicitó ingresar una dirección de correo electrónico para notificaciones del sistema; este campo se dejó en blanco para continuar. Finalmente, el asistente informó que la configuración inicial se había completado correctamente.

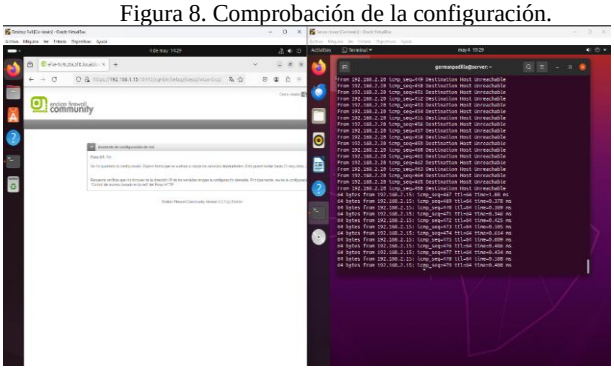
Figura 7. Información configuración Adaptadores Red



Fuente. Autoría Propia.

Durante este proceso, se mantenía activa una sesión de consola en una máquina virtual (Ubuntu Server) que intentaba realizar ping a la dirección IP 192.168.2.15 (interfaz anaranjada), sin obtener respuesta. Sin embargo, al hacer clic en “Aceptar y aplicar la configuración” en la interfaz web de Endian, el ping comenzó a responder, confirmando la disponibilidad de red y la correcta configuración de la interfaz.

Figura 8. Comprobación de la configuración.

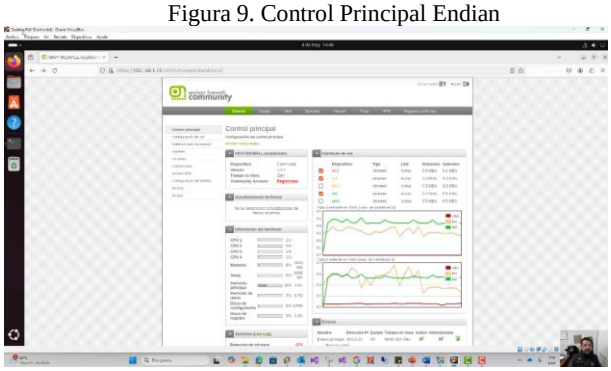


Fuente. Autoría Propia.

Al acceder nuevamente al panel principal de administración desde el navegador, se pudo verificar

gráficamente que las tres zonas estaban activas: zona verde (conectada al Ubuntu Desktop), zona anaranjada (conectada al Ubuntu Server) y zona roja (conectada a Internet mediante NAT). Además, se visualizaron estadísticas básicas de tráfico y estado de las interfaces de red.

Figura 9. Control Principal Endian



Fuente. Autoría Propia.

Este procedimiento completa la configuración inicial de red en la máquina virtual Endian Firewall y permite su operación como cortafuegos entre las distintas zonas de red configuradas.

3 TEMÁTICA 2.

Configurar la regla de NAT (Network Address Translation/Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet). Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia Internet. Verificar en el reenvío de puertos / NAT, la creación de las reglas.

3.1 DESARROLLO TEMÁTICA 2.

Para abordar la temática se adaptan tres máquinas virtuales en VirtualBox 7.1.6.

Allí mismo se configura una Red NAT en Herramientas > Red > Redes NAT, en este caso se crea con el nombre NAT-Endian, IPv4: 10.0.2.0/24.

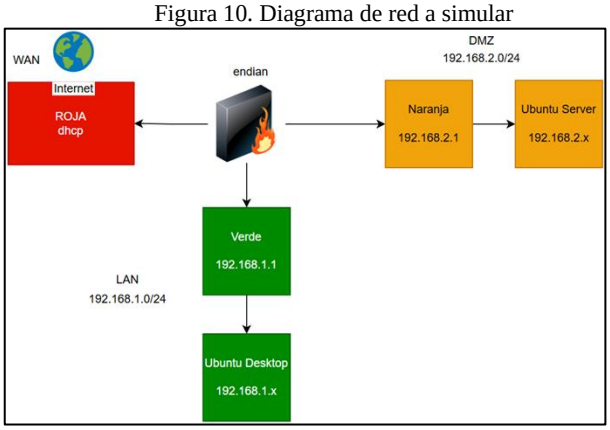
A continuación se define las imágenes, maquinas virtuales y configuraciones de red para abordar el desarrollo de la temática.

- Endian Firewall 3.3.2
- Ubuntu Desktop 24.04 (zona LAN)
- Ubuntu Server 24.04 (zona DMZ)

Las conexiones de red se configuran así:

- Endian:
  - Adaptador 1: Interno (Red Verde - LAN)
  - Adaptador 2: Interno (Red Naranja - DMZ)
  - Adaptador 3: RED NAT “NAT-Endian” (Red Roja - WAN)
- Ubuntu Desktop: Interno (Red Verde)
- Ubuntu Server: Interno (Red Naranja)

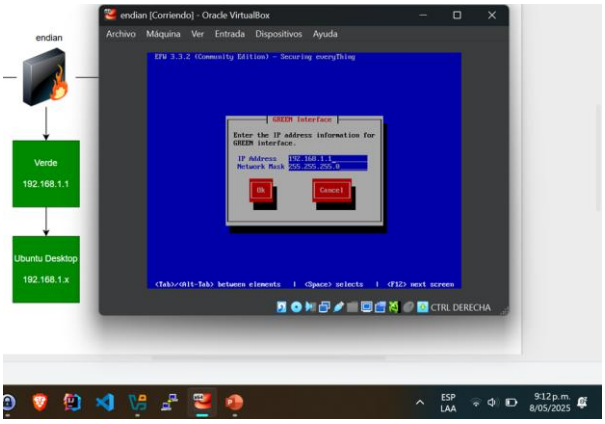
Figura 10. Diagrama de red a simular



Fuente. Autoría Propia.

La instalación de Endian se hace desde la imagen ISO, seleccionando idioma, particionando el disco y configurando las interfaces. Luego de aplicar la configuración, se accede al panel administrativo por el navegador desde la URL: https://192.168.1.1:10443

Figura 11. Configurando Interfaz GREEN en la instalación de Endian



Fuente. Autoría Propia.

Se inician las demás máquinas virtuales para terminar de configurar el portal, la zona DMZ y las reglas de navegación.

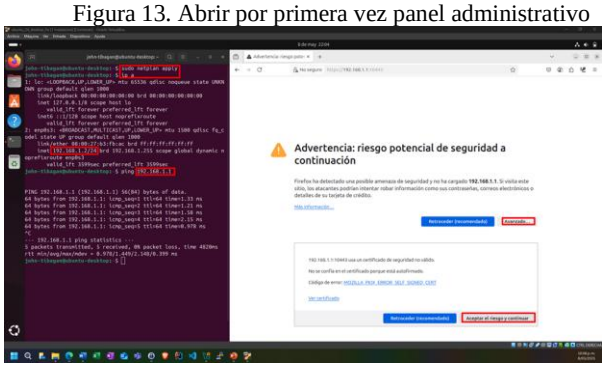
Figura 12. Máquinas virtuales activas

Fuente. Autoría Propia.

Para la zona GREEN, Endian configura automáticamente un servidor DHCP asignando automáticamente una IP al Ubuntu Desktop por estar en la misma red interna (RedVerde).

Por eso se tiene conexión y es posible ingresar a la IP que define el Firewall https://192.168.1.1:10443.

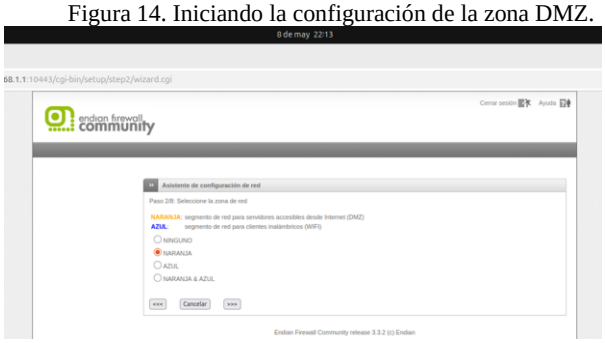
Figura 13. Abrir por primera vez panel administrativo



Fuente. Autoría Propia.

En el primer ingreso al panel administrativo se debe configurar el idioma y la zona horaria, luego se define las credenciales para el usuario admin y para el servicio SSH. Iniciando el paso 1/8 inicia el asistente para configurar la red, donde se continúa para configurar la zona Naranja (DMZ) que es el paso 2/8.

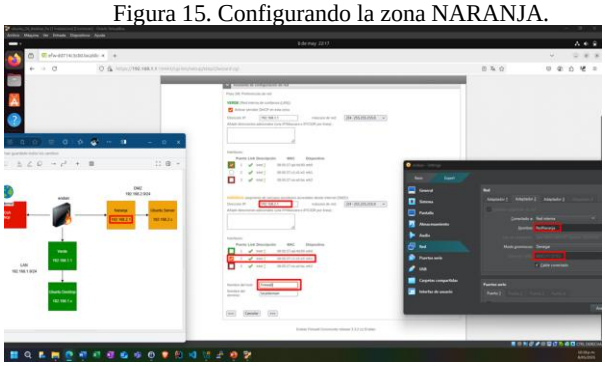
Figura 14. Iniciando la configuración de la zona DMZ.



Fuente. Autoría Propia.

Se procede a configurar la zona DMZ con el segmento de red definido 192.168.2.0/24, tomando como base la configuración de la MAC asignada en la máquina virtual para estar seguros del adaptador. De igual manera se cambia el host del Endian por "firewall".

Figura 15. Configurando la zona NARANJA.



Fuente. Autoría Propia.

Se finalizan los demás pasos del 4 al 8 por defecto sin cambios o ajustes adicionales, y luego de esto tarda un momento para que el panel solicite las credenciales del usuario admin, se ingresa y ya se puede continuar con las configuraciones de las reglas. Endian al ser un Firewall permisivo, contiene reglas por defecto para navegación entre zonas, incluso acceso a internet. Esto lo verificamos en el menú Firewall > Tráfico de salida y Tráfico entre zonas, por lo cual desde el desktop se debería tener acceso a internet, pero para abordar la temática se eliminan todas las reglas del tráfico de salida y se deshabilita el tráfico entre zonas. Con esto ya no se tendría acceso a internet desde la LAN o DMZ.

Figura 16. Deshabilitando el tráfico entre zonas.

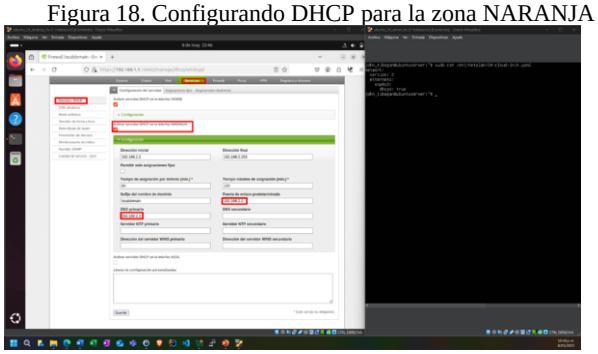
Fuente. Autoría Propia.

Figura 17. Eliminando reglas de salida

Fuente. Autoría Propia.

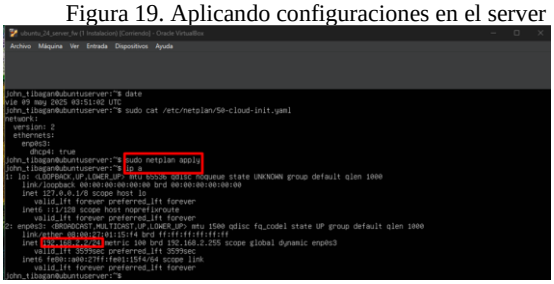
Para evitar configuraciones de IP manual en el server, desde el Firewall se va a configurar para que se asigne una IP automáticamente. En el server se debe tener por defecto la asignación por dhcp4: true.

Figura 18. Configurando DHCP para la zona NARANJA



Fuente. Autoría Propia.

Figura 19. Aplicando configuraciones en el server



Fuente. Autoría Propia.

En este punto se configura el primer punto de la temática e indirectamente parte del punto 2, el cual es habilitar tráfico entre la LAN a la WAN y entre la DMZ a la WAN. Es decir que tanto el desktop como el server tengan acceso a internet suministrado por el Firewall.

Para esto se configura desde Firewall>Tráfico de salida donde se crean 3 reglas habilitando navegación para los servicios: HTTPS, HTTP y DNS. Desde las Zonas VERDE y NARANJA a la zona ROJA.

Figura 20. Configurando regla HTTPS

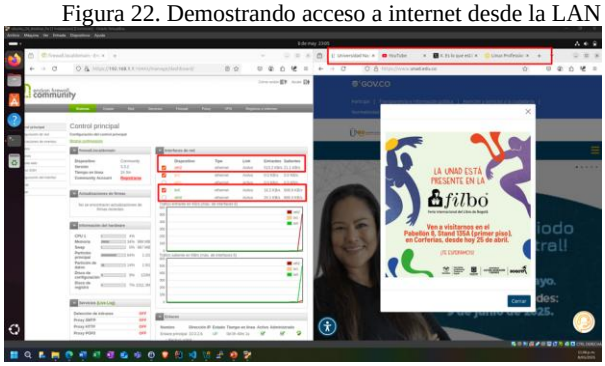
Fuente. Autoría Propia.

Figura 21. Configuración de las 3 reglas necesarias.

Fuente. Autoría Propia.

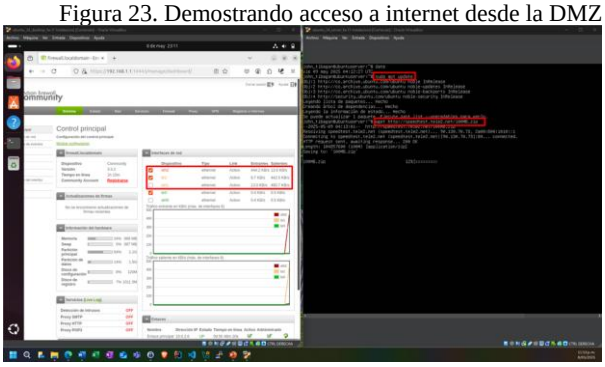
Con esto ya se tendría acceso desde la LAN (desktop) y desde la DMZ (server) a la WAN (Internet), lo cual se procede a generar tráfico, desde el desktop navegando a diferentes sitios web y desde el server actualizando librerías y generando una descarga de un archivo de 100 MB.

Figura 22. Demostrando acceso a internet desde la LAN



Fuente. Autoría Propia.

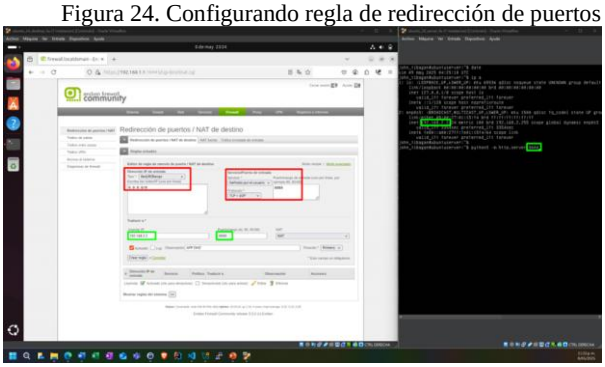
Figura 23. Demostrando acceso a internet desde la DMZ



Fuente. Autoría Propia.

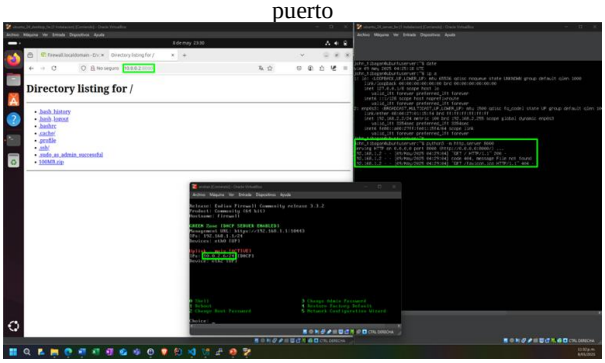
Para el siguiente punto, Verificar en el re-envió de puertos / NAT. En este paso se requiere exponer un servicio con un puerto y que sea consumido con la puerta de enlace del firewall, para esto se hará lo siguiente: Exponer un servicio en el server (DMZ) y que se consuma desde en Desktop (LAN) con la IP asignada al Firewall (Debido a que se deshabilito navegación entre zonas Imagen). La regla se configurará para que se acceda desde cualquier IP al puerto 8080 y que este redirija a la IP y puerto expuesto en el server.

Figura 24. Configurando regla de redirección de puertos



Fuente. Autoría Propia.

Figura 25. Demostrando la exposición y reenvío del puerto



Fuente. Autoría Propia.

La implementación de un firewall open-source como Endian permite crear mecanismos de seguridad centralizados, estableciendo niveles óptimos de confianza y previniendo vulnerabilidades mediante políticas granulares (filtrado de contenido, NAT, VPN) [5].

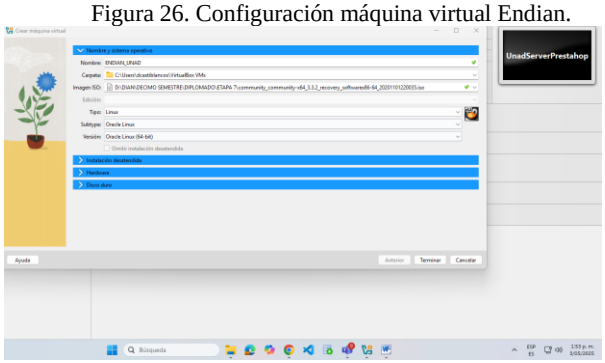
4 TEMÁTICA 3.

Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

4.1 DESARROLLO TEMÁTICA 3.

Se realiza la instalación y configuración de Endian firewall en un entorno virtualizado para esto se utilizó la versión 3.3.2 descarga de la imagen ISO desde el sitio oficial en SourceForge (https://sourceforge.net/projects/efw). De esta forma se procede con la configuración de la máquina en la herramienta de VirtualBox.

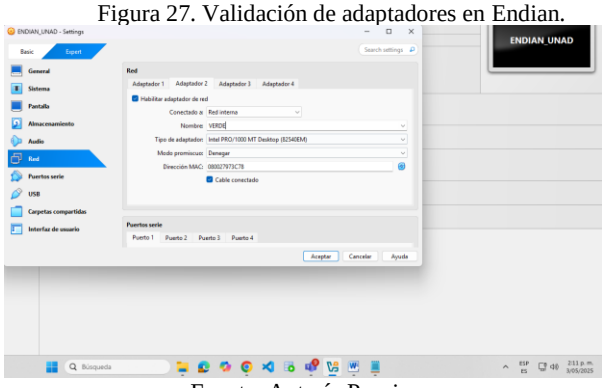
Figura 26. Configuración máquina virtual Endian.



Fuente. Autoría Propia.

Antes de realizar con el proceso de instalación de la máquina se realizó la configuración de los adaptadores de red que se utilizaran en el proceso para esto se tuvieron presentes las zonas roja, verde y naranja en el cual se validaron en el proceso de instalación.

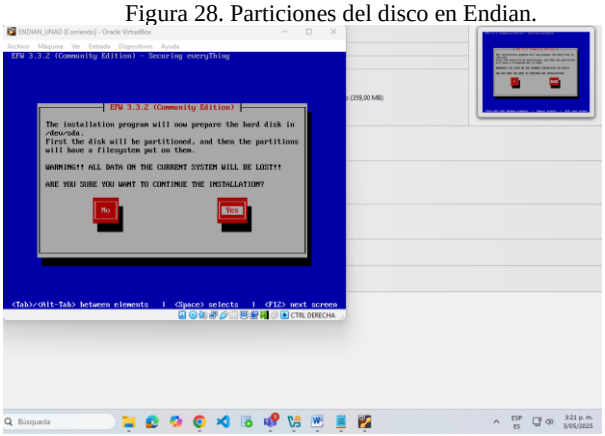
Figura 27. Validación de adaptadores en Endian.



Fuente. Autoría Propia.

Una vez realizadas dichas configuraciones se proceden con las validaciones de instalación del Endian en el cual se instala en idioma inglés, se procede con las configuraciones y particiones del disco duro de esta forma se procede con aceptar dichos procesos.

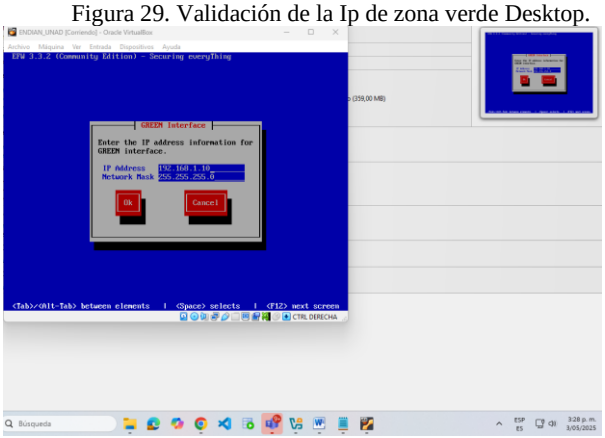
Figura 28. Particiones del disco en Endian.



Fuente. Autoría Propia.

Se realiza las configuraciones de la IP de la zona verde que este caso hace referencia a la máquina que tiene asignado el cliente el cual es el Desktop el cual se le asigno la IP 192.168.1.10/24 con una máscara de red 255.255.255.0 de esta forma se estará configurando la primera zona que necesita para el proceso del Endian.

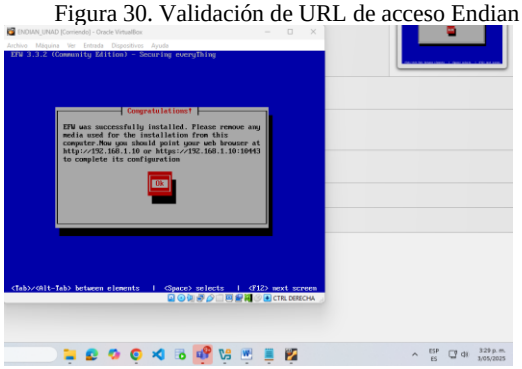
Figura 29. Validación de la Ip de zona verde Desktop.



Fuente. Autoría Propia.

De esta forma se obtiene la URL de acceso para la parte gráfica de la configuración del Endian esto quedando de esta forma http://192.168.1.10:40443 esto haciendo referencia a la zona verde configurada anteriormente y procedido se da Ok para confirmar dichas configuraciones necesarias para el proceso y utilización del servicio Endian.

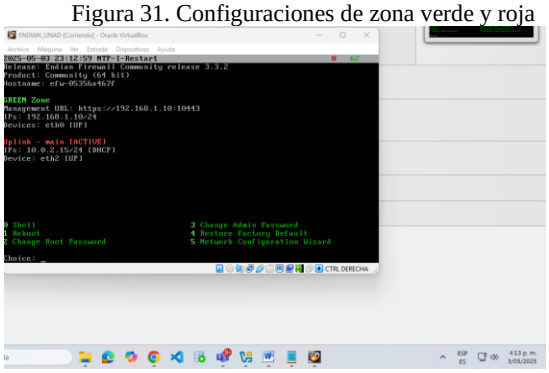
Figura 30. Validación de URL de acceso Endian



Fuente. Autoría Propia.

Mediante este proceso inicial se obtienen las configuraciones de la zona verde y roja que en este caso la IP se obtiene de manera automática por DHCP: 10.0.2.15/24.

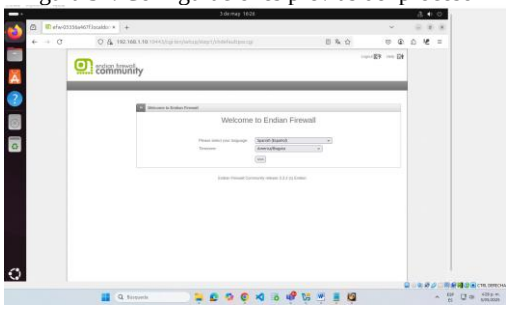
Figura 31. Configuraciones de zona verde y roja



Fuente. Autoría Propia.

Se accede a la URL asignada mediante el equipo Desktop el cual este está configurado por medio del adaptador verde validado en la máquina de Endian esta máquina tiene la IP 192.168.1.10 el cual se ingresa por medio del navegador y obtenemos respuesta de manera correcta esto con el fin de realizar las respectivas configuraciones de acceso desde la interfaz gráfica.

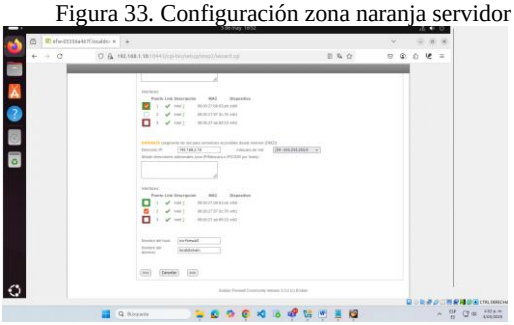
Figura 32. Configuraciones previas del proceso Endian



Fuente. Autoría Propia.

Una vez realiza el proceso de configuraciones iniciales se procede a validar las configuraciones de red en el cual este queda por medio del enrutamiento esto mediante la conexión DHCP se le da siguiente y se procede con la configuración del adaptador red faltante en este caso la zona naranja el cual cumple la función del servidor DMZ esto validado mediante la IP 192.168.2.10/24 y la máscara de red 255.255.255.0 de igual forma se permite visualizar las tarjetas de red de cada uno de los adaptadores configurados.

Figura 33. Configuración zona naranja servidor



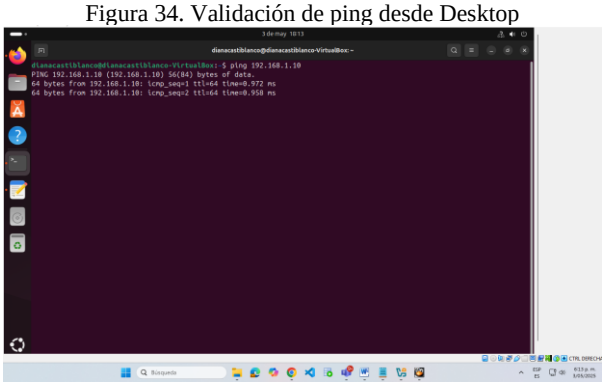
Fuente. Autoría Propia.

De esta forma se permitirá visualizar cada una de las configuraciones de adaptadores de red la zona roja es la conexión a internet esto validado mediante el tipo NAT. Se aceptan las configuraciones necesarias y se permitirá acceder de manera exitosa a las configuraciones del Endian en el cual podemos observar las previas configuraciones de las diferentes zonas de red.

Cada una de las validaciones realizadas permitirá acceder de manera correcta a las máquinas configuradas en este caso el Desktop y server que se tendrán en cuenta para este proceso se realizan las previas validaciones de acceso y ping en cada una de las máquinas esto con el fin de que en cada una esté tomando su Ip correspondiente. Se deben realizar configuraciones previas de las validaciones de los DNS en este caso se adicionan los accesos de Google.

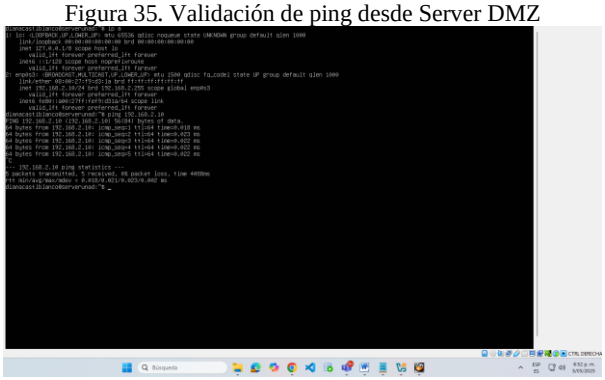
De esta forma se definió el nombre del host en este caso se deja svr-firewall y el nombre del dominio localdomain de esta manera se permiten visualizar de manera correcta los tres adaptadores.

Figura 34. Validación de ping desde Desktop



Fuente. Autoría Propia.

Figura 35. Validación de ping desde Server DMZ



Fuente. Autoría Propia.

Se procede a realizar la validación de permitir el acceso a los servicios HTTP mediante los puertos 80 y FTP por el puerto 21 esto mediante el servidor Web estas configuraciones se realizan mediante la opción de Firewall en el tráfico entre zonas. Esta validación se realiza mediante la creación de una nueva regla en el cual se seleccionará la zona naranja de origen y el destino la zona verde esto para el servicio HTTP con el protocolo TCP para el puerto 80 y de esta forma se permite.

Figura 36. Ingreso de regla de servicio HTTP puerto 80

Fuente. Autoría Propia.

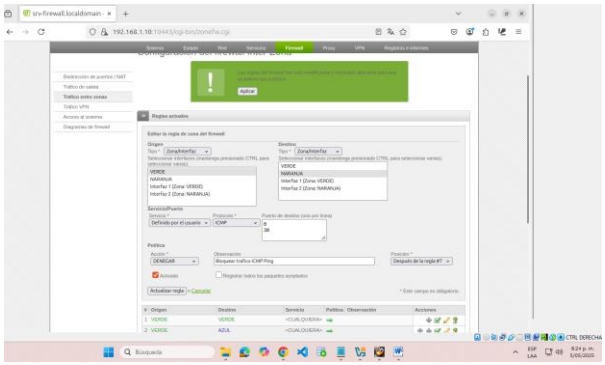
Para la realización del permiso de servicio FTP para el protocolo TCP mediante el puerto 21 esto para la zona naranja como origen y verde destino.

Figura 37. Ingreso de regla de servicio FTP puerto 21

Fuente. Autoría Propia.

Se realiza la configuración de la denegación del protocolo ICMP para los puertos 80 y 30 el cual no se permitirá realizar ping en el cual se procede a realizar la creación de la nueva regla en el cual se deja validado desde el origen como zona verde y destino naranja realizando la denegación del protocolo de esta manera si se realiza ping desde el equipo de Desktop no se permite realizar ninguna petición de ping a la Ip 192.168.2.10 una vez realiza estas configuraciones de creaciones de reglas se debe aplicar los cambios para que se ve han reflejados.

Figura 38. Creación de regla para denegación de protocolo ICMP



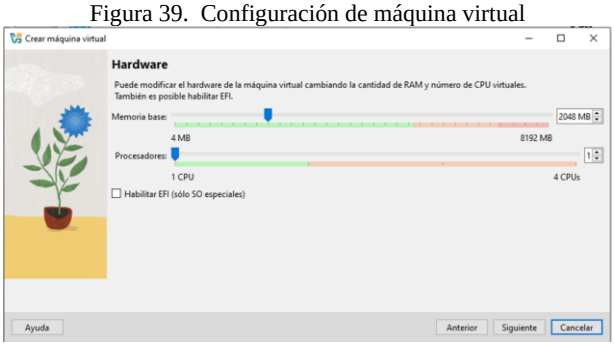
Fuente. Autoría Propia.

5 TEMÁTICA 4.

5.1 DESARROLLO TEMÁTICA 4.

Reglas de acceso para permitir o denegar el tráfico. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y FTP con sus respectivos puertos. Comunicar la zona Internet con la zona DMZ. Verificar en el tráfico Inter - Zona, la creación de las reglas. El ingreso del servicio HTTP desde la LAN hacia la zona DMZ.

Figura 39. Configuración de máquina virtual



Fuente. Autoría Propia

Previo a llevar a cabo el proceso de instalación de la máquina, se llevó a cabo la configuración de los adaptadores de red que se utilizarán en dicho proceso.

Para esto, se consideraron las zonas roja, verde y naranja, las cuales fueron validadas en el procedimiento de instalación.

Figura 40. Implementación de Puertos

Fuente. Autoría Propia

Se llevó a cabo la implementación y configuración detallada de Endian Firewall en un entorno virtualizado mediante Oracle VM VirtualBox 7.0. Para ello, se utilizó la versión estable 3.3.2, descargada como imagen ISO desde el repositorio oficial de SourceForge (https://sourceforge.net/projects/efw), tras verificar su integridad mediante el hash SHA-256. Posteriormente, se asignaron recursos específicos a la máquina virtual (2 GB de RAM, 2 núcleos de CPU) y se configuraron tres adaptadores de red para las zonas verde, naranja y roja, asegurando una segmentación inicial acorde a los requisitos del proyecto.

Figura 41. Instalación de Endian

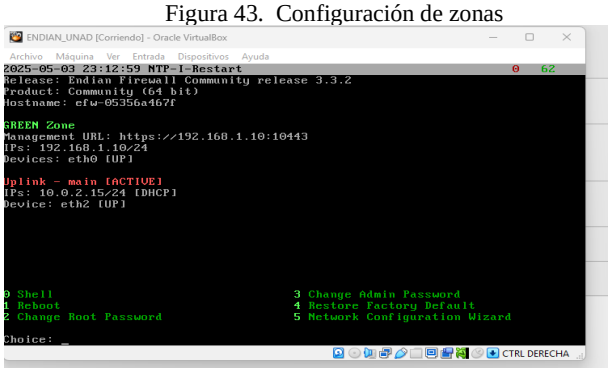
Fuente. Autoría Propia.

Una vez que se hayan completado las configuraciones se llevarán a cabo las validaciones de la instalación de Endian, Seguidamente, se procederá a las configuraciones y particiones del disco duro; de esta manera, se aceptarán los procesos correspondientes.

Figura 42. Particionado de disco duro

Fuente. Autoría Propia

Figura 43. Configuración de zonas



Fuente. Autoría Propia.

Se ingresa a la URL designada utilizando un equipo de escritorio que ha sido configurado mediante el adaptador verde validado en la máquina Endian, la cual posee la dirección IP 192. 168. 1. 10. Esta dirección se ingresa a través del navegador para obtener una respuesta adecuada, con el objetivo de llevar a cabo las configuraciones necesarias desde la interfaz gráfica.

Figura 44. Ingreso a interfaz Endian

Fuente. Autoría Propia

Con el fin de permitir el acceso interno a los servicios web en la DMZ, se estableció una regla específica en Endian Firewall que admite tráfico HTTP (puerto 80) proveniente de la LAN. Esta regla fue configurada al detallar las direcciones IP de origen (LAN: 192. 168. 1. 0/24) y de destino (DMZ: 10. 0. 0. 0/24), garantizando así una comunicación segura entre las diferentes zonas.

Figura 45. Configuración de la zona naranja con la zona verde

Fuente. Autoría Propia.

Las instrucciones de firewall se desarrollaron y aplicaron en la sección Inter-Zonas de Endian Firewall, siguiendo un enfoque estructurado para garantizar coherencia en las políticas. En los paneles de control, se configuraron tres reglas clave:

- HTTP LAN-DMZ: Se permitió el tráfico web (puerto TCP/80) desde las computadoras de la red interna (LAN) hacia los servidores alojados en la zona desmilitarizada (DMZ), facilitando el acceso a aplicaciones corporativas.

- FTP LAN-DMZ: Se habilitó la transferencia de archivos (puerto TCP/21) desde la red local hacia los servidores FTP en la DMZ, asegurando integridad mediante autenticación básica.

- HTTP WAN-DMZ: Mediante redirección de puertos (NAT), se permitió el acceso externo desde Internet (WAN) al servidor web en la DMZ a través de la URL http://www.Wichit.com, exponiendo únicamente el puerto 80.

Adicionalmente, se implementó una regla FTP WAN-DMZ para conexiones externas seguras, restringidas por geolocalización a direcciones IP del país predefinido. Estas pautas se diseñaron seleccionando protocolos específicos (HTTP/FTP), definiendo zonas origen-destino (LAN, DMZ, WAN) y activando filtros basados en políticas regionales, lo que aseguró un tráfico alineado con los requisitos de seguridad.

Figura 46. Creación de la regla ftp con el puerto 20 para comunicar el desktop con la zona naranja

Fuente. Autoría Propia.

Figura 47. Verificar la creación de las reglas

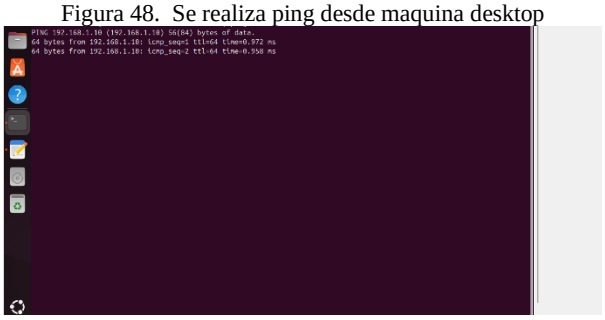
Fuente. Autoría Propia.

Auditoría aleatoria: Se verificó que las políticas de red estuvieran correctamente establecidas y aplicadas según los escenarios predefinidos. Para ello, se desarrolló una guía que garantiza la visibilidad del tráfico autorizado en cada caso. Como resultado, se confirmó que las pautas para el tráfico HTTP y FTP entre las zonas LAN, DMZ y WAN están operando correctamente, sin interrupciones y con el direccionamiento adecuado. Este informe respalda que el filtrado del tráfico se realiza conforme a las directrices definidas por los administradores de red.

De acuerdo con dichas directrices, se realizaron pruebas de conectividad utilizando un equipo con Ubuntu en una estación de trabajo de escritorio. Las pruebas confirmaron la comunicación en la zona verde mediante comandos de ping. También se evaluó el tráfico HTTP desde la LAN hacia la DMZ empleando la IP del servidor web en la zona naranja.

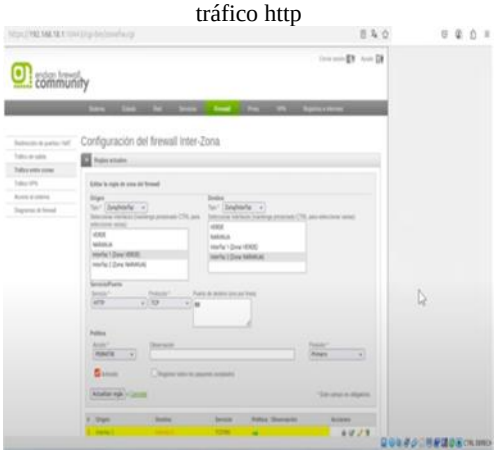
Asimismo, se validó la conexión de LAN a WAN mediante tráfico HTTP hacia sitios como YouTube. Esta simulación se llevó a cabo utilizando un equipo físico y NAT público de Endian, accediendo desde la WAN a la DMZ con conectividad HTTP. Finalmente, se realizó una prueba de acceso desde la LAN a la WAN usando direcciones públicas FTP, obteniendo resultados satisfactorios que confirman una conexión exitosa.

Figura 48. Se realiza ping desde maquina desktop



Fuente. Autoría Propia.

Imagen 49. Creación de la regla firewall para permitir el tráfico http



Fuente. Autoría Propia.

6 TEMÁTICA 5.

Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Producto esperado:

1. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios:
   - www.hotmail.com
   - www.youtube.com
   - www.elnuevodia.com.co

2. Autenticación por usuario: A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.
3. Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

6.1 DESARROLLO TEMÁTICA 5.

Ingresamos a la máquina virtual con Ubuntu en VirtualBox y procedimos a instalar Squid. Se instala para actuar como un servidor proxy, el cual se encarga de intermediar las

solicitudes entre los clientes (como navegadores web) y los servidores de Internet.

Figura 50. Actualizando e instalando Squid

```
diego-sandoval@diego-sandoval:~$ sudo apt update
[sudo] contraseña para diego-sandoval:
Obj:1 http://co.archive.ubuntu.com/ubuntu noble InRelease
Obj:2 http://co.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:3 http://co.archive.ubuntu.com/ubuntu noble-backports InRelease
Obj:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:5 https://ppa.launchpadcontent.net/inkscape.dev/stable/ubuntu noble InReleas
e
Obj:6 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 66 paquetes. Ejecute «apt list --upgradable» para verlos.
diego-sandoval@diego-sandoval:~$ sudo apt install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  fonts-tuffy libapache2-mod-php8.3 libatkmm-1.6-1v5 libblas3
  libboost-filesystem1.83.0 libcairomm-1.0-1v5 libcdr-0.1-1
  libdouble-conversion3 libgc1 libgfortran5 libglibmm-2.4-1t64 libgsl27
  libgslcblas0 libgtkmm-3.0-1t64 libgtksourceview-4-0
```

Fuente. Autoría Propia.

Con Squid instalado, procedemos a crear la lista negra, en la que se especifican los nombres de las páginas web que se desea bloquear para restringir su acceso desde la red.

Figura 51. Abriendo lista blanca

```
diego-sandoval@diego-sandoval:~$ sudo nano /etc/squid/blacklist.txt
```

Fuente. Autoría Propia.

Figura 52. Editando lista blanca

```
  GNU nano 7.2                  /etc/squid/blacklist.txt *
www.hotmail.com
www.youtube.com
www.elnuevodia.com.co
```

Fuente. Autoría Propia.

La creación del usuario se realizó utilizando la herramienta htpasswd, incluida en el paquete apache2-utils.

El paquete apache2-utils en sistemas basados en Debian (como Ubuntu) contiene varias herramientas útiles para la administración y configuración de servidores Apache. Algunas de las utilidades más comunes que incluye son:

htpasswd: Se utiliza para crear y actualizar archivos de contraseñas para la autenticación básica HTTP. Este archivo es utilizado para proteger áreas de un servidor web mediante usuario y contraseña.

Figura 53. Instalando apache

```
diego-sandoval@diego-sandoval:~$ sudo apt install apache2-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
apache2-utils ya está en su versión más reciente (2.4.58-1ubuntu8.6).
fijado apache2-utils como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  fonts-tuffy libapache2-mod-php8.3 libatkmm-1.6-1v5 libblas3
  libboost-filesystem1.83.0 libcairomm-1.0-1v5 libcdr-0.1-1
  libdouble-conversion3 libgc1 libgfortran5 libglibmm-2.4-1t64 libgsl27
  libgslcblas0 libgtkmm-3.0-1t64 libgtksourceview-4-0
  libgtksourceview-4-common libimage-magick-perl libimage-magick-q16-perl
  liblapack3 libmagick++-6.q16-9t64 libpangomm-1.4-1v5 libpotrace0
  librevenge-0.0-0 libsigc++-2.0-0v5 libvisio-0.1-1 libwpd-0.10-10
  libwpg-0.3-3 perlmagick php8.3 php8.3-bcmath php8.3-cgi php8.3-cli
  php8.3-curl php8.3-fpm php8.3-gd php8.3-intl php8.3-mbstring php8.3-mysql
  php8.3-opcache php8.3-readline php8.3-soap php8.3-xml php8.3-zip
  python-tinycss2-common python3-appdirs python3-bs4 python3-cachecontrol
  python3-cssselect python3-filelock python3-gi-cairo python3-html5lib
  python3-lxml python3-msgpack python3-numpy python3-packaging python3-scour
  python3-soupsieve python3-tinycss2 python3-webencodings
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 66 no actualizados.
```

Fuente. Autoría Propia.

Figura 54. Editando archivo users.txt

```
diego-sandoval@diego-sandoval:~$ sudo htpasswd -c /etc/squid/users.txt diego
New password:
Re-type new password:
Adding password for user diego
diego-sandoval@diego-sandoval:~$
```

Fuente. Autoría Propia.

Editamos el archivo de configuración de Squid para integrar tanto la autenticación del usuario creado como la lista negra de sitios bloqueados.

El archivo squid.conf es el archivo de configuración principal de Squid, donde se definen todas las reglas y parámetros que determinan cómo funciona el servidor proxy. A través de este archivo, puedes personalizar diversos aspectos del comportamiento de Squid. El uso de dstdomain permite bloquear o permitir el acceso a ciertos dominios http.

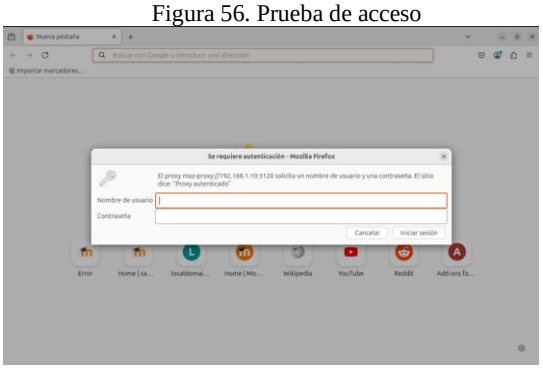
Figura 55. Modificando archivo squid.conf

```
http_access allow localhost


# Autenticacion por el usuario
auth_param basic program /usr/lib/squid/basic_ncsa/auth /etc/squid/users.txt
auth_param basic realm Proxy autenticado
acl usuarios_autenticados proxy_auth REQUIRED

# Sitios prohibidos
acl sitios_prohibidos dstdomain "/etc/squid/blacklist.txt"

# Reglas de acceso
http_access deny sitios_prohibidos usuarios_autenticados
http_access allow usuarios_autenticados
```

Fuente. Autoría Propia.

Procedemos a acceder al navegador y nos pide el usuario y contraseña creado.

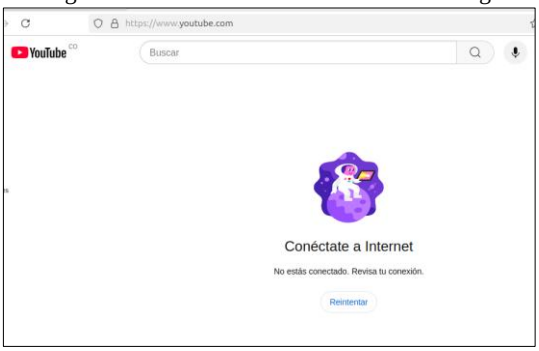
Figura 56. Prueba de acceso



Fuente. Autoría Propia.

El bloqueo se realizó para http pero el navegador toma como por defecto https entonces en esta ocasión no sale el bloqueo de página sino sale que no hay conexión a internet.

Figura 57. Prueba de acceso a YouTube denegada



Fuente. Autoría Propia.

Al intentar acceder a otra página si sale correctamente

Figura 58. Prueba de acceso a Wikipedia permitida

Fuente. Autoría Propia.

7. CONCLUSIONES

La instalación y configuración de Endian Firewall en una máquina virtual mediante VirtualBox permitió establecer de manera efectiva una arquitectura de red segmentada en tres zonas: verde, anaranjada y roja. Este proceso no solo facilitó la comprensión del funcionamiento de un firewall perimetral, sino que también demostró la importancia de la correcta asignación de interfaces de red para garantizar la seguridad, la conectividad interna y el acceso controlado a Internet. La interfaz web de administración ofreció una configuración guiada clara, lo cual permitió verificar el estado de cada zona y aplicar ajustes en tiempo real. En resumen, la implementación de Endian Firewall en entorno virtualizado es una herramienta didáctica eficaz para el aprendizaje y la simulación de redes seguras.

Se realizan las configuraciones y creaciones de reglas Firewall en el cual se permite la validación de las zonas origen a destino según la petición de servicio, protocolos y puertos de esta forma se realizó cada una de las peticiones de permisos para los servicios de HTTP, FTP y denegación del protocolo ICMP esto mediante la creación de las reglas en firewall.

La implementación de un proxy HTTP no transparente con autenticación de usuarios y filtrado de contenido mejora la seguridad y el control de acceso en una red. Al exigir autenticación, solo los usuarios autorizados pueden acceder a Internet, y las listas negras bloquean sitios web específicos. Esto optimiza la productividad y asegura el cumplimiento de políticas. Aunque la configuración de herramientas como Squid requiere conocimientos técnicos, ofrece flexibilidad para adaptarse a distintos entornos. Es crucial monitorear y probar regularmente el sistema para asegurar su efectividad y evitar afectar demasiado la experiencia del usuario. En resumen, es una solución eficaz para gestionar y proteger el acceso a Internet.

La implementación y gestión adecuadas de reglas de acceso para permitir o denegar el tráfico de red son fundamentales para establecer una postura de seguridad robusta y funcional. El producto esperado, que implica la comunicación controlada entre zonas de red específicas (Verde y Naranja mediante HTTP y FTP, e Internet con la DMZ), así como la verificación exhaustiva de estas reglas, subraya la importancia de segmentar la red y aplicar el principio de mínimo privilegio

8. REFERENCIAS

[1] Endian, “Endian Firewall Community – free open source security for home users,” Endian.com. [Online]. Available: https://www.endian.com/en/community/. [Accessed: May 7, 2025].

[2] Kifarunix, “Install and configure Endian Firewall on VirtualBox,” kifarunix.com, May 21, 2019. [Online]. Available: https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/. [Accessed: May 7, 2025].

[3] Espinosa, O. (2019, October 28). *Todo sobre DMZ: Para qué sirve y cómo configurarla en un router*. RedesZone. https://www.redeszone.net/tutoriales/configuracion-puertos/configurar-dmz-router/.

[4] Phipps, J. (2024, April 30). How to set up DMZ on servers: 7-step DMZ configuration. eSecurity Planet. https://www.esecurityplanet.com/networks/dmz-setup/.

[5] Zapata Escobar, D. E., Gómez Tangarife, I. L., Acevedo Munera, J. D., Obando Ibarra, C. H., & García Arango, D. A. (2023). Implementación de un sistema de control y seguridad Informático ENDIAN FIREWALL. INGENIERÍA: Ciencia, Tecnología e Innovación, 10(1), 98–115. https://doi.org/10.26495/icti.v10i1.2401

.