# “ IMPLEMENTACION DE SEGURIDAD PERIMETRAL EN ENTORNOS GNU/LINUX MEDIANTE SEGMENTACION DE REDES Y SERVICIOS DE FILTRADO CON ENDIAN FIREWALL “

Karen Valentina Bello Alvarado
kvbelloa@unadvirtual.edu.co
Luis Felipe Castillo Benavides
lfcastillobe@unadvirtual.edu.co
Francisco Jose Cepeda Amaya
fjcedpedaa@unadvirtual.edu.co
Jose Daniel Gutierrez Gutierrez
jdgutierrezgut@unadvirtual.edu.co
Ivonne Dayana Perez Rincon
idperezr@unadvirtual.edu.co

**RESUMEN:** *En el presente trabajo se abordan los procesos de instalación, configuración y puesta en marcha del sistema GNU/Linux Endian dentro de un entorno virtualizado, estableciendo adecuadamente sus zonas de red y las reglas necesarias para garantizar una comunicación segura y controlada. Asimismo, se implementan mecanismos de traducción de direcciones, políticas de acceso entre las diferentes zonas, habilitación y restricción de servicios según las necesidades de la red, y la configuración de un Proxy HTTP con autenticación y filtros de navegación. Todo esto con el fin de asegurar un funcionamiento óptimo del firewall, gestionar el tráfico de manera adecuada y fortalecer las medidas de seguridad en el entorno de red simulado.*

**PALABRAS CLAVE**: Endian Firewall, NAT, Proxy HTTP, Virtualización

## 1 INTRODUCCIÓN

La configuración de un entorno seguro dentro de una infraestructura de red requiere comprender y aplicar herramientas que permitan controlar, segmentar y proteger el tráfico entre diferentes zonas. En este contexto, GNU/Linux Endian se convierte en una solución fundamental para la gestión de seguridad perimetral, ofreciendo funcionalidades como firewall, NAT, filtrado de contenido y administración de servicios. A través de su implementación en un entorno virtualizado, es posible simular escenarios reales de comunicación, aplicar reglas de acceso, gestionar servicios y fortalecer los mecanismos de seguridad que garantizan un intercambio de información confiable. Este proceso permite desarrollar competencias clave en administración de redes y ciberseguridad, esenciales para entornos educativos y profesionales.

## 2 INSTALACIÒN

### 2.1. Instalación Edian

Instalación de Endian Firewall

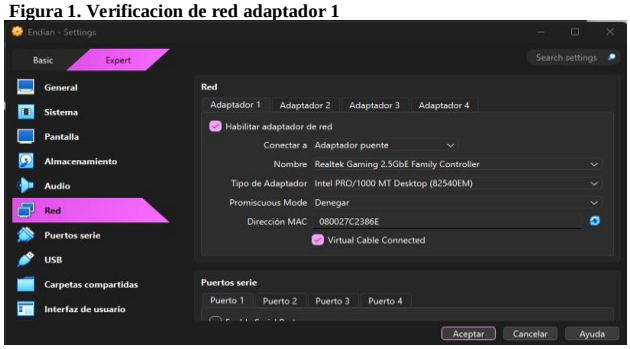
1. Clave de root
   - Clave por defecto: endian
   - Nueva clave asignada: contraseña

2. Configuración de adaptadores en la máquina virtual

Para garantizar la conectividad a internet durante la instalación y posterior funcionamiento:

Adaptador 1: Modo Adaptador puente (Bridge): Este modo permite que la máquina virtual tome una dirección IP desde la red local, actuando como si fuera un equipo físico más, lo que facilita el acceso a internet y la detección dentro de la red.

**Figura 1. Verificacion de red adaptador 1**




**Fuente: Los Autores**
**Comentario: Se realiza la configuración de los adaptadores de red.**

**Figura 2. Verificacion de red adaptador 2**


**Fuente: Los Autores**
**Comentario: Se realiza la configuración de los adaptadores de red.**

**Figura 3. Verificacion de red adaptador 3**


**Fuente: Los Autores**
**Comentario: Se realiza la configuración de los adaptadores de red.**

Se continúa con la verificación de Endian para activar la consola a través del puerto serial, permitiendo así el acceso directo a las opciones avanzadas de configuración desde la línea de comandos.

**Figura 4. Activación de la consola por puerto serial en Endian**

**Fuente: Los Autores**
**Comentario: La figura muestra la opción para habilitar la consola por puerto serial en Endian.**

Se selecciona No en la opción de activar la consola sobre el puerto serial. La dirección IP configurada para la interfaz es 192.168.0.15/24, con una máscara de red 255.255.255.0.

**Figura 5. Configuración de consola serial e IP en Endian**


Fuente: Los Autores
Comentario: Se muestra la desactivación de la consola serial y la asignación de la IP 192.168.0.15.

**Figura 6. configuración de consola en Endian**


Fuente: Los Autores
Comentario: Se evidencia que la consola serial no se habilita y que la interfaz de red queda configurada con la IP 192.168.0.15 y máscara 255.255.255.0.

**Figura 7. Confirmación de la configuración en Endian**


Fuente: Los Autores
Comentario: Se muestra la confirmación final de los parámetros establecidos para continuar con la instalación.

## 3. PLANTEAMIENTO Y CONTEXTUALIZACIÓN DEL PROBLEMA A RESOLVER:

**3.1.** Temática 1: Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

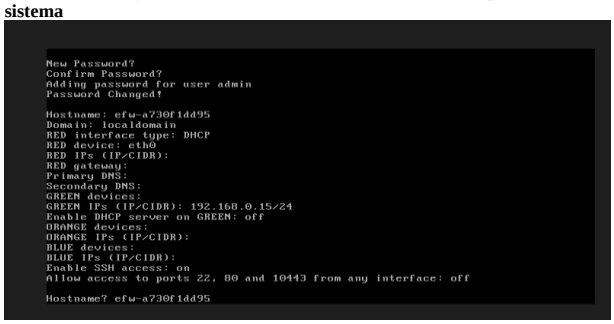
El proceso inicia con la preparación y configuración de la instancia destinada a GNU/Linux Endian dentro de VirtualBox, donde se definen correctamente las tarjetas de red necesarias para su funcionamiento. Posteriormente, se realiza la instalación del sistema, garantizando que cada componente quede operando de manera óptima para cumplir con los propósitos del firewall.

**Figura 8. Pantalla principal de administración de Endian Firewall**


Fuente: Los Autores

Comentario: La interfaz de consola de Endian, donde se visualiza la IP de administración (https://192.168.0.15:10443) y las opciones principales como Shell, reinicio y configuración de red.

**Figura 9. Configuración inicial de Endian: credenciales y parámetros del sistema**



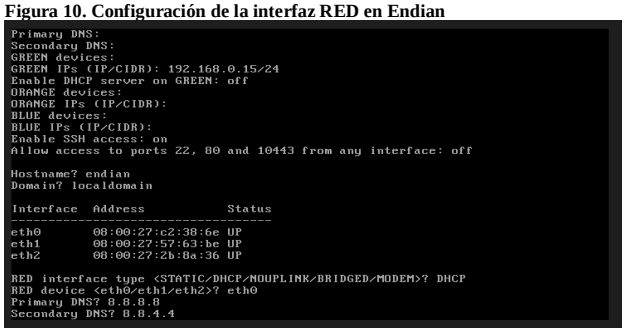

Fuente: Los Autores

Comentario: La configuración inicial de Endian, incluyendo el cambio de contraseña, los parámetros del sistema y la visualización de los tres adaptadores de red.

## CONFIGURACION RED

En el RED se Escribe DHCP si aparece una IP Si aparece DHCP solo ENTER y por la configuración hecha al comienzo se selecciona eth0 para RED. DNS Primario 8.8.8.8 DNS Secundario 8.8.4.4

**Figura 10. Configuración de la interfaz RED en Endian**



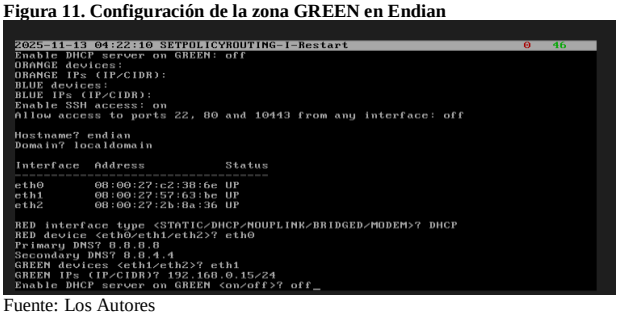

Fuente: Los Autores

Comentario: La selección de DHCP para la interfaz RED (eth0), junto con la asignación automática de IP y la configuración de los DNS 8.8.8.8 y 8.8.4.4.

## CONFIGURACION GREEN

Se selección eth1 en GREEN devices GREEN IPs se deja 192.168.0.15/24 y en Enable DHCP GREEN se pone off

**Figura 11. Configuración de la zona GREEN en Endian**




Fuente: Los Autores

Comentario: Se configura eth1 como interfaz GREEN, se mantiene la IP 192.168.0.15/24 y se desactiva el DHCP para esta zona.

## CONFIGURACION ORANGE

Se selecciona el eth2 en ORANGE devices
ORANGE IP que en nuestro DMZ dejamos 172.16.0.1/24
Y en BLUE devices dejamos en blanco asi endian sabe que no se va a usar

**Figura 12. Configuración de la zona ORANGE en Endian**

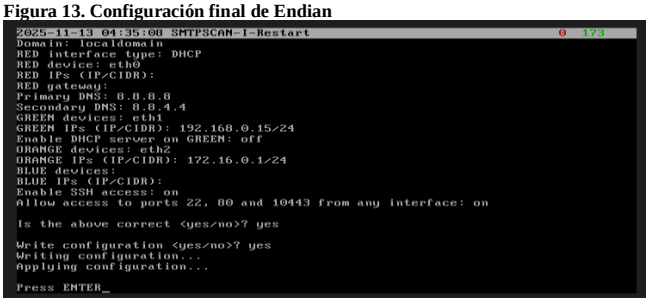

Fuente: Los Autores

Comentario:Se asigna eth2 a la zona ORANGE, se define la IP 172.16.0.1/24 para la DMZ y se deja vacío el campo BLUE devices para indicar que no será utilizado.

## CONFIGURACION FINAL

Para terminas seleccionamos:
Enable SSH Access on - Allow access to ports 22, 80 and 10443 from any interface? Ponemos ON - En Is the above correct ponemos YES y en Write configuration ponemos YES y terminamos la configuración

**Figura 13. Configuración final de Endian**




Fuente: Los autores

Comentario: Se habilita el acceso SSH, se permiten los puertos 22, 80 y 10443 desde cualquier interfaz, se confirma la configuración con YES, y finalmente se escribe la configuración para completar el proceso.

Por último, cambiamos la contraseña del usuario admin dejando
Usuario: admin
Contraseña: contrasena
Ya aquí viendo que la maquina quedo correctamente con el segmento Green y el segmento RED recibiendo una ip DHCP del proveedor de internet

**Figura 14. Cambio de contraseña del usuario admin**


Fuente: Los Autores

Comentario: Se actualiza la contraseña del usuario admin a contrasena, verificando que el sistema queda correctamente configurado con el segmento GREEN operativo y el segmento RED obteniendo una IP por DHCP del proveedor de internet.

## 3.2.Temática 2: Configuración NAT.

La segunda temática aborda la configuración de NAT, un proceso esencial para permitir que los equipos dentro de la red interna accedan a servicios externos mediante la traducción de direcciones. Este paso garantiza la comunicación efectiva entre las distintas zonas configuradas en Endian y la red pública.

**Figura 15. Preparación del entorno Ubuntu Desktop**

Fuente: Los Autores

Comentario: Se prepara Ubuntu Desktop como base de trabajo, asegurando que el sistema tenga las actualizaciones y herramientas necesarias para continuar con la configuración y posterior instalación de Endian.

Para esto se utilizaron los comandos:

• sudo nano /etc/netplan/01-netcfg.yaml

Dentro se ponen las siguientes líneas

network:

  version: 2

  renderer: NetworkManager

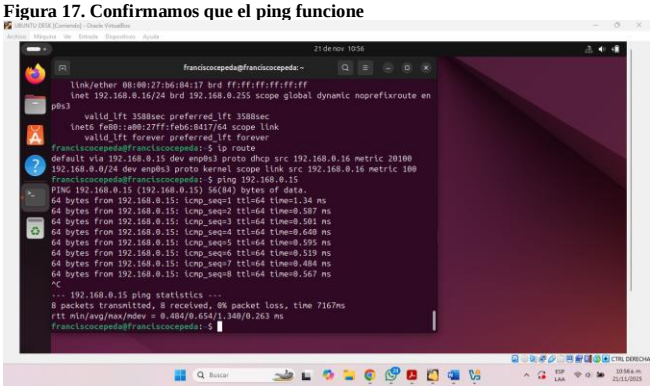
Se confirma que Ubuntu Desktop esté conectado a ENDIAN inet 192.168.10.10/24 brd 192.168.10.255 scope global dynamic ...

**Figura 16. Configuración en Ubuntu Desktop**

Fuente: Los Autores

Comentario: En este paso se realizan los ajustes necesarios dentro de Ubuntu Desktop para continuar con la instalación y configuración del entorno donde operará Endian.

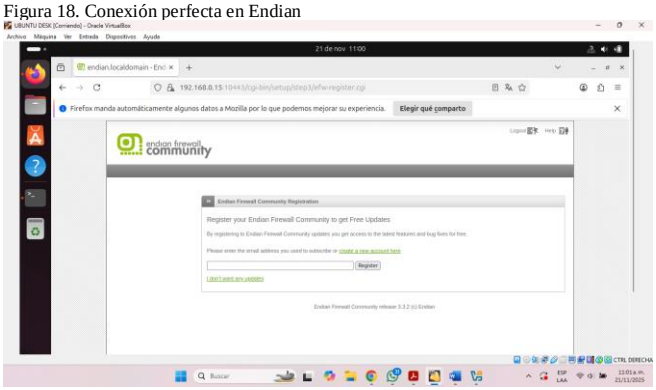
**Figura 17. Confirmamos que el ping funcione**



Fuente: Los Autores

Comentario: Se verifica la comunicación de red mediante un ping exitoso, confirmando que la conectividad está operativa.

Figura 18. Conexión perfecta en Endian

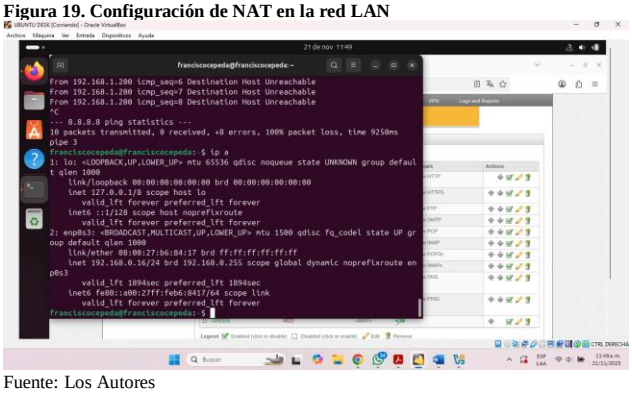


Fuente: Los Autores

Comentario: Se observa que la conexión en Endian opera correctamente, indicando que la configuración de red y los servicios están funcionando sin errores.

En este paso se realiza la habilitación y ajuste del mecanismo de traducción de direcciones (NAT) para la red LAN, permitiendo que los equipos internos accedan a recursos externos a través de la interfaz configurada en Endian. Esta configuración asegura la salida a internet desde la red local y garantiza un enrutamiento adecuado entre los distintos segmentos.

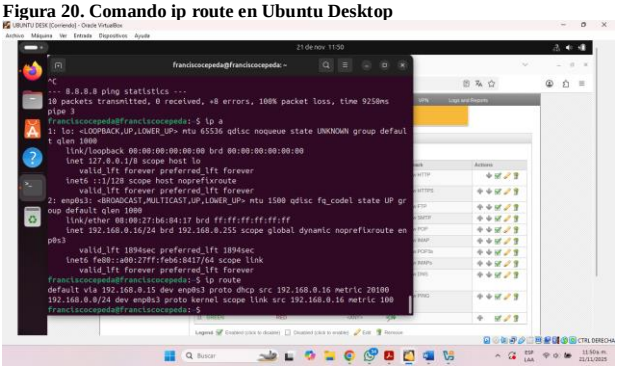
**Figura 19. Configuración de NAT en la red LAN**



Fuente: Los Autores

Comentario: Se habilita NAT para permitir que los equipos de la red LAN accedan a recursos externos mediante la traducción de direcciones realizada por Endian.

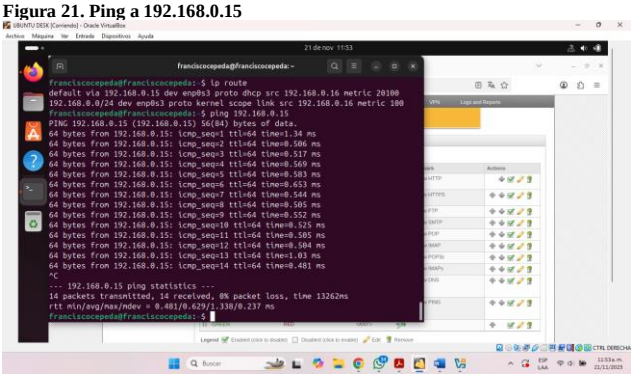
**Figura 20. Comando ip route en Ubuntu Desktop**



Fuente: Los Autores

Comentario: Se visualiza la tabla de rutas del sistema mediante el comando ip route, lo cual permite verificar el gateway, las interfaces activas y la correcta asignación de rutas dentro de la red.

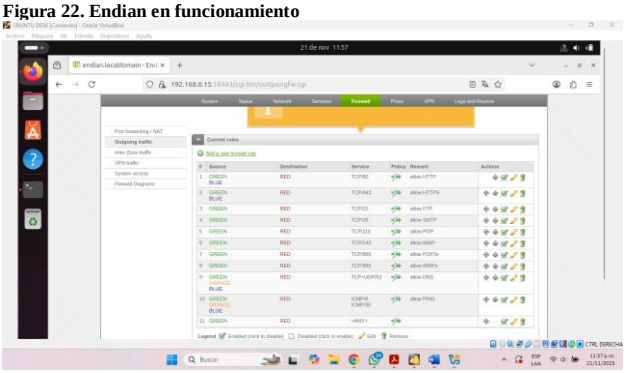
**Figura 21. Ping a 192.168.0.15**



Fuente: Los Autores

Comentario: Se realiza un ping a la dirección 192.168.0.15 para verificar la comunicación con el segmento GREEN, confirmando que la conexión es exitosa.

**Figura 22. Endian en funcionamiento**

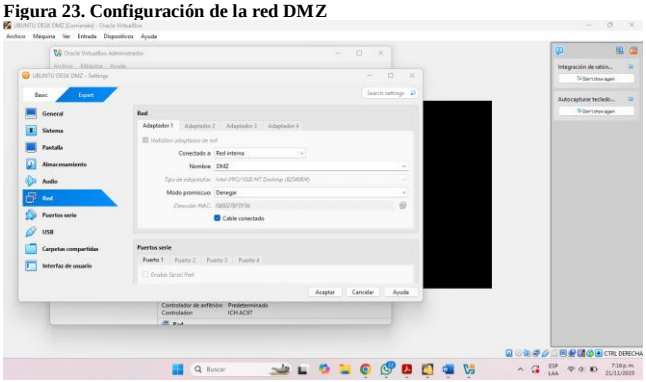


Fuente: Los Autores

Comentario: Se confirma que Endian está operando correctamente, mostrando estabilidad en los servicios y conectividad adecuada según la configuración realizada.

En esta etapa se configura el mecanismo de traducción de direcciones (NAT) para la zona DMZ, permitiendo que los servicios alojados en este segmento puedan comunicarse de manera controlada con redes externas. Esta configuración asegura que los servidores ubicados en la DMZ operen de forma segura, manteniendo el aislamiento respecto a la red interna mientras se habilita el acceso necesario hacia y desde el exterior.

**Figura 23. Configuración de la red DMZ**



Fuente: Los Autores

Comentario: Se establecen los parámetros de red correspondientes a la DMZ, asignando la interfaz y dirección configuradas para este segmento con el fin de aislar servicios y permitir su acceso controlado desde el exterior.

**Figura 24. Configuración de la conexión con Endian**

Fuente: Los Autores

Comentario: Se ajustan los parámetros necesarios para establecer la conexión con Endian, asegurando comunicación estable entre los segmentos de red y el firewall.

Para realizar esta configuración, se utiliza el comando **sudo nano /etc/netplan/01-netcfg.yaml**, que permite editar el archivo de parámetros de red en Ubuntu y ajustar manualmente las interfaces asociadas a la conexión con Endian.

**Figura 25. Comandos ip a e ip route en Ubuntu Desktop (DMZ)**

Fuente: Los Autores

Comentario: Se consultan las interfaces y rutas de red mediante los comandos ip a e ip route, verificando que la configuración aplicada para la DMZ coincida con los parámetros definidos para la conexión con Endian.

**Figura 26. Acceso al portal de Endian desde Ubuntu Desktop en la DMZ**


Fuente: Los Autores.
Comentario: Se accede correctamente al portal web de Endian desde la máquina ubicada en la DMZ, confirmando conectividad, enrutamiento adecuado y funcionamiento del segmento ORANGE.

### 3.3. Temática 3: Permitir servicios de la Zona DMZ para la red.

Se realizó la configuración de la forma correcta podremos conectarnos a la interfaz de endian por medio de la ip que se estableció con la configuración y la que aparece en la interfaz máquina de endian que es 192.168.0.15:10443

**Figura 27. Acceso a la Interfaz Web de Endian**


Fuente: Los Autores
Comentario: Se muestra el ingreso correcto al portal de Endian mediante la IP configurada 192.168.0.15:10443.

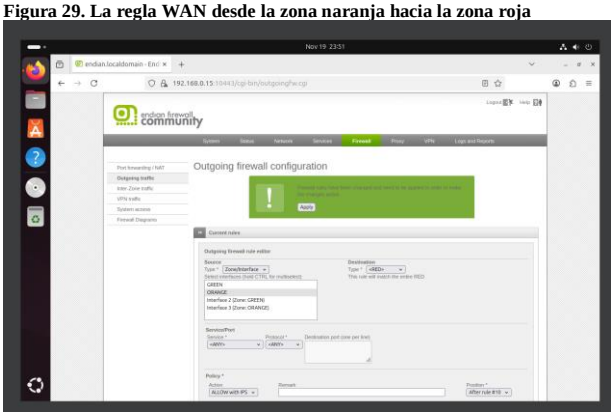
Permitir servicios de la Zona DMZ para la red. Producto esperado: 1. Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. Estando aquí vamos a ir a la selección de firewall y vamos a crear la configuración para el DMZ a la zona roja para la conexión a internet

**Figura 28. Configuración de Servicios HTTP y FTP en la Zona DMZ**


Fuente: Los Autores.
Comentario: Se inicia la creación de reglas en el firewall para permitir HTTP y FTP desde la DMZ hacia la zona roja.

Ya teniendo el puente configurado ahora vamos a crear la reglar para la conexión wan desde la zona naranja hasta la zona roja

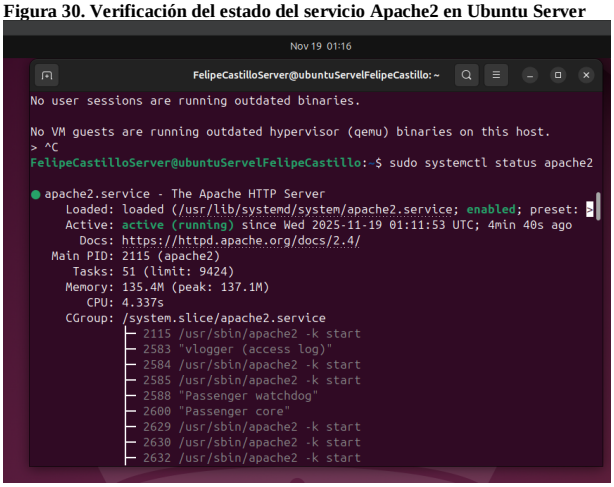
**Figura 29. La regla WAN desde la zona naranja hacia la zona roja**




Fuente: Los Autores.
Comentario: Se procede a generar la regla que permite la conexión WAN desde la zona naranja hacia la zona roja.

Para este paso iniciamos verificando que los paquetes necesarios estén instalados en nuestro Ubuntu Server. En este caso, se requiere Apache2 para el servicio HTTP y vsftpd para el servicio FTP. Dado que Apache2 ya había sido instalado en trabajos anteriores, procedemos a comprobar su estado actual ejecutando:
sudo systemctl status apache2

**Figura 30. Verificación del estado del servicio Apache2 en Ubuntu Server**




Fuente: Los Autores
Comentario: Se revisa el estado del servicio Apache2 para confirmar su correcto funcionamiento antes de configurar los servicios HTTP y FTP.

Para el servicio FTP se tiene que realizar la instalación por medio del comando *sudo apt install vsftpd -y*

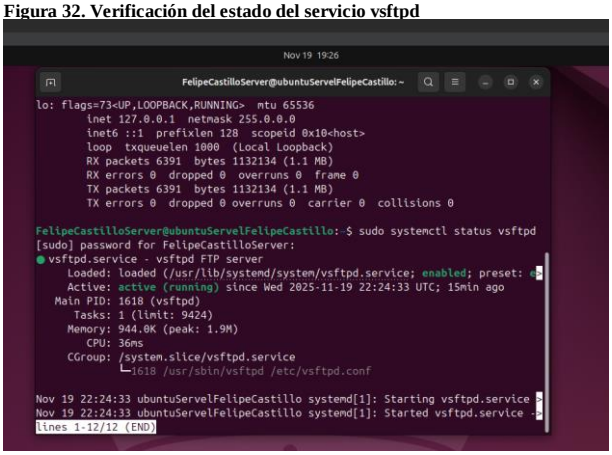
**Figura 31. Instalación del servicio FTP en Ubuntu Server**


Fuente: Los Autores

Comentario: Se instala el servicio FTP mediante el comando sudo apt install vsftpd -y.

Procedemos a ver el estado del servicio con el comando sudo systemctl status vsftpd

**Figura 32. Verificación del estado del servicio vsftpd**




Fuente: Los Autores

Comentario: Se comprueba el estado del servicio FTP utilizando el comando sudo systemctl status vsftpd.

Teniendo esto listo vamos a realizar la configuración de los puerto 80 y 21 desde endian, con esto volvemos a la interfaz de endian que teníamos en nuestra maquina desktop. En este punto vamos a ir a la sección de firewall y al módulo inter-zone traffic

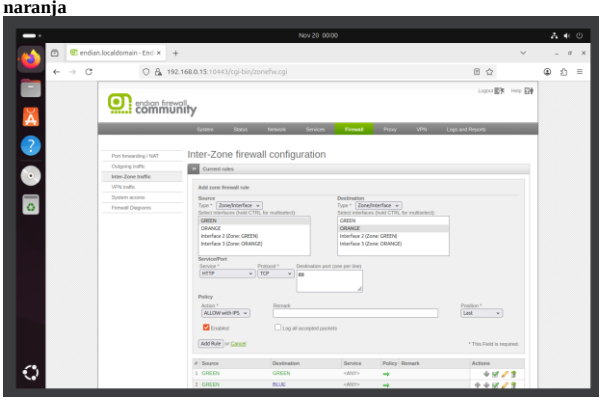
**Figura 33. Acceso al módulo Inter-Zone Traffic en el firewall**


Fuente: Los Autores.

Comentario: Se ingresa a la sección de firewall para configurar el tráfico entre zonas mediante el módulo Inter-Zone Traffic.

En este punto vamos a crear la primera regla que será para la conexión http la cual apuntara de la zona verde a la zona naranja ya que tenemos que consumir los servicios desde el desktop al servidor.

**Figura 34. Creación de la regla HTTP desde la zona verde hacia la zona naranja**




Fuente: Los Autores

Comentario: Se configura la regla que permite el tráfico HTTP desde la zona verde hacia la zona naranja para consumir los servicios del servidor.

Ya con esto podemos realizar la prueba de conexión al protocolo http desde el equipo desktop ingresando la siguiente dirección que corresponde a al servicio de apache 2 que esta en el servidor servidor http://172.16.0.10

**Figura 35. Prueba de acceso al servicio HTTP desde el equipo Desktop**


Fuente: Los Autores.

Comentario: Se verifica la conexión al servicio Apache2 del servidor ingresando la dirección http://172.16.0.10 desde el equipo de la zona verde.

De igual forma vamos a agregar la regla para la configuración del FTP o puerto 21

**Figura 36. Creación de la regla para el servicio FTP (puerto 21)**

Fuente: Los Autores.

Comentario: Se añade la regla que permite el tráfico FTP hacia el servidor mediante el puerto 21.

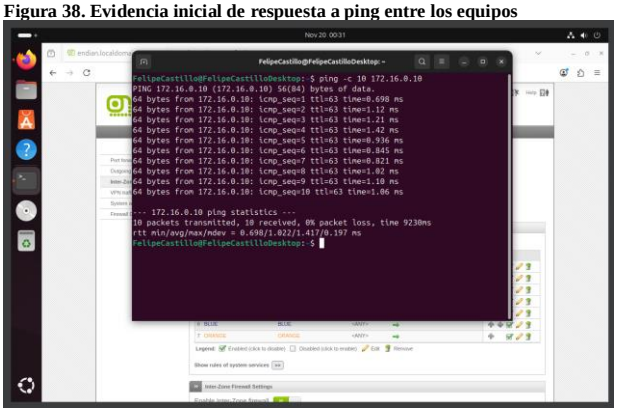
Con esto podríamos hacer las pruebas para comprobar la conexión al servicio FTP del servidor

**Figura 37. Prueba de conexión al servicio FTP del servidor.**

Fuente: Los Autores.
Comentario: Se realizan las pruebas necesarias para confirmar el acceso al servicio FTP en el servidor.

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. Como primera acción se tomará las evidencias de respuesta por ping entre los equipos.

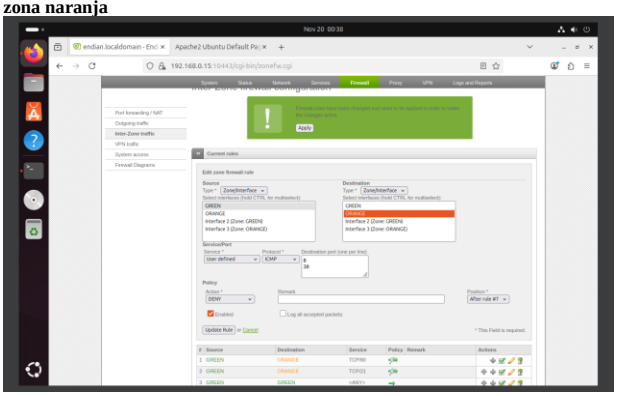
**Figura 38. Evidencia inicial de respuesta a ping entre los equipos**



Fuente: Los Autores.
Comentario: Se registran las respuestas exitosas al comando ping antes de aplicar la regla que bloqueará el protocolo ICMP en la red.

Validamos que tenemos conexión entre equipos lo que procedemos a hacer es agregar la reglas de bloqueo del servicio ICMP por lo puerto 8 /30, esta primera regla denegara el ping de la zona verde a la zona naranja.

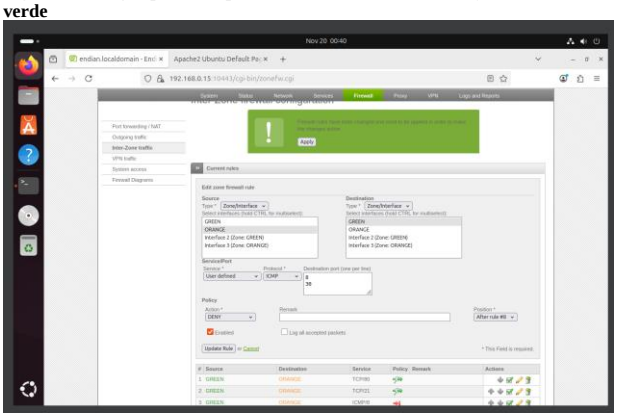
**Figura 39. Creación de la regla para bloquear ICMP de la zona verde a la zona naranja**



Fuente: Los Autores
Comentario: Se configura la regla que deniega el protocolo ICMP (puertos 8 y 30), impidiendo el ping desde la zona verde hacia la zona naranja.

De igual forma vamos a crear la regla que denegara de la zona naranja a la zona verde

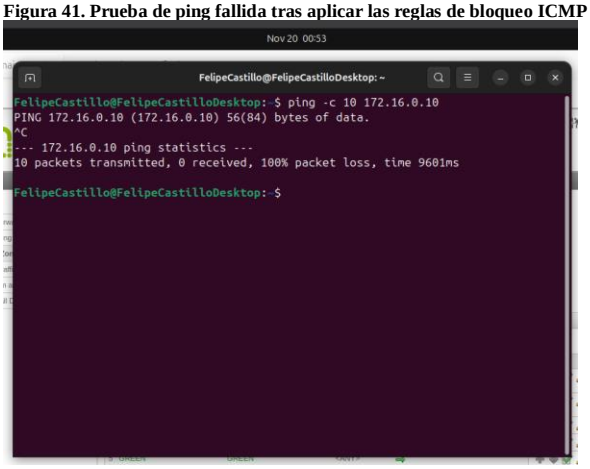
**Figura 40. Regla para bloquear ICMP de la zona naranja hacia la zona verde**



Fuente: Los Autores
Comentario: Se agrega la regla que deniega el protocolo ICMP desde la zona naranja hacia la zona verde.

Con esto ya configurado procedemos a realizar de nuevo la prueba de ping y nos daremos cuenta que ya no salga los ping del equipo desktop al servidor

**Figura 41. Prueba de ping fallida tras aplicar las reglas de bloqueo ICMP**

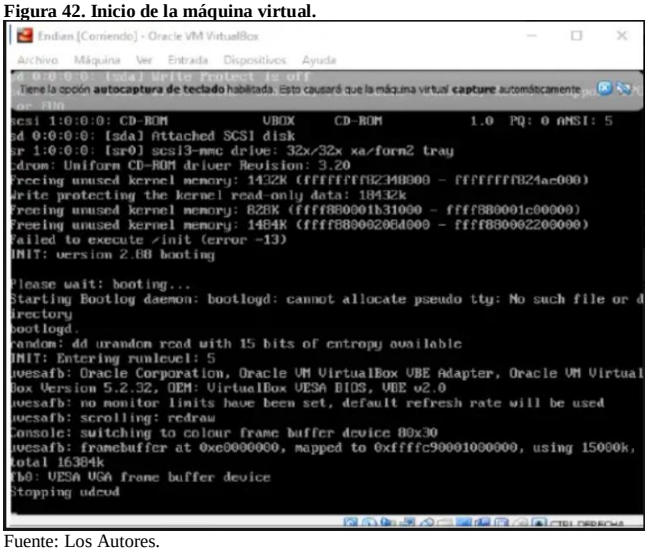



Fuente:Los Autores
Comentario: Se verifica que, después de aplicar las reglas, el equipo Desktop ya no puede hacer ping al servidor.

### 3.4. Temática 4: Reglas de acceso para permitir o denegar el tráfico.

Se inicia la máquina virtual.

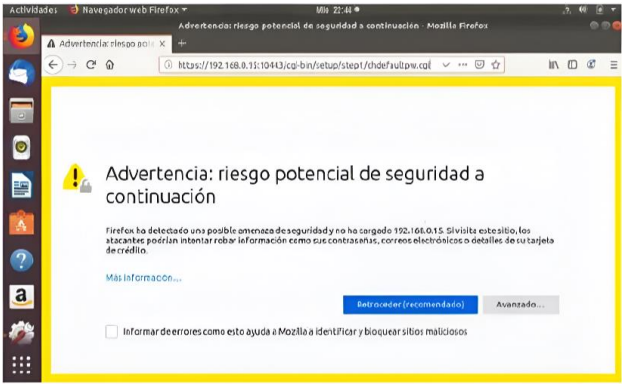
**Figura 42. Inicio de la máquina virtual.**




Fuente: Los Autores.
Comentario: Se procede a encender la máquina virtual para continuar con el proceso de configuración.

Se verifica la configuración de red de la máquina virtual GNU/Linux Ubuntu Server, la cual debe estar configurada en Red Interna. Luego se inicia la máquina virtual desde el sistema operativo Ubuntu Server. Del mismo modo, se inicia la máquina virtual que ejecuta Ubuntu Server y, desde su navegador web, se ingresa a la IP del servidor Endian, el cual redirigirá automáticamente a la página en modo seguro.

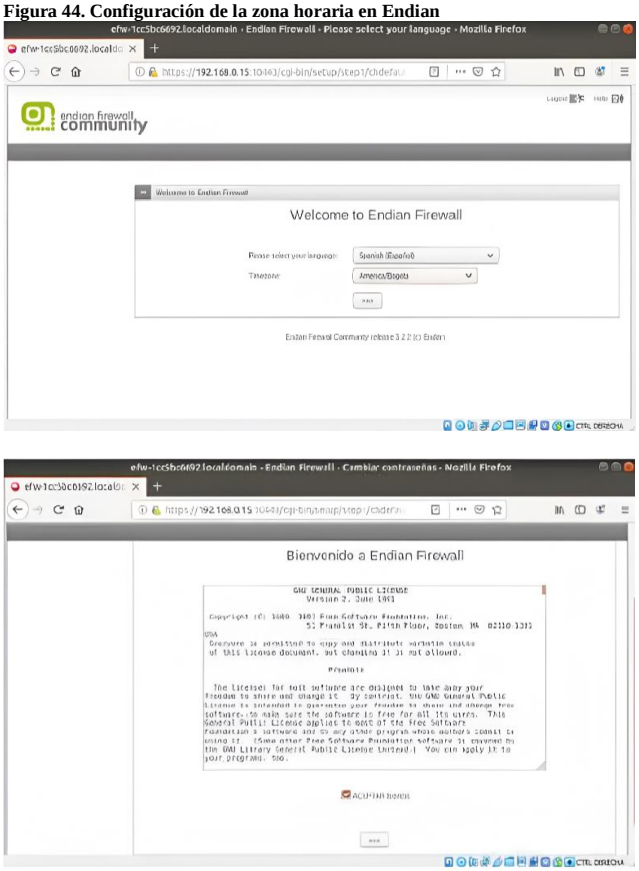
**Figura 43. Verificación de red y acceso al portal de Endian desde Ubuntu Server**




Fuente: Los Autores
Comentario: Se confirma que la máquina virtual está en Red Interna y, al iniciar Ubuntu Server, se accede desde el navegador a la IP del servidor Endian, que redirige automáticamente al modo seguro.

Se realiza la configuracion de la zona horaria de edian

**Figura 44. Configuración de la zona horaria en Endian**







Fuente: Los Autores.
Comentario: Se ajusta la zona horaria del sistema Endian según los parámetros requeridos.

Durante el proceso de configuración inicial de las máquinas virtuales, se procede a la creación y asignación de las claves de acceso para cada uno de los usuarios y servicios involucrados. En el caso del servidor GNU/Linux Ubuntu Server, se define una contraseña segura para el usuario administrador, garantizando que cumpla con los requisitos mínimos de seguridad recomendados (longitud adecuada, combinación de caracteres y no coincidencia con claves previas).

**Figura 45. Asignación de contraseñas en el proceso de configuración inicial**


Fuente: Los Autores.
Comentario: Se establecen las claves de acceso para los usuarios, incluyendo una contraseña segura para el administrador de Ubuntu Server.

Se selecciona la red de enrutamiento correspondiente y se configura el tipo de enlace utilizando el modo DHCP, permitiendo que la interfaz de red obtenga automáticamente su dirección IP, máscara de red, puerta de enlace y parámetros adicionales necesarios para la comunicación dentro de la infraestructura virtual. Esta configuración asegura que la máquina virtual se integre correctamente en la red definida y pueda interactuar con el resto de los servicios y dispositivos según la topología establecida.

**Figura 46. Configuración de la interfaz de red en modo DHCP**


Fuente: Los Autores.
Comentario: Se selecciona la red de enrutamiento y se habilita DHCP para que la interfaz obtenga automáticamente sus parámetros de red.

Se selecciona la red Naranja como el segmento destinado a la DMZ (Demilitarized Zone). Esta red se configura para alojar los servicios que deben ser accesibles tanto desde la red interna como desde el exterior, garantizando un entorno controlado y seguro. La asignación de la red Naranja permite aislar los servidores públicos del resto de la infraestructura, reduciendo riesgos y asegurando un manejo adecuado del tráfico que ingresa y sale hacia la DMZ.

**Figura 47. Selección de la red Naranja como segmento DMZ**


Fuente: Los Autores
Comentario: Se asigna la red Naranja para la DMZ, destinada a alojar servicios accesibles desde la red interna y el exterior.

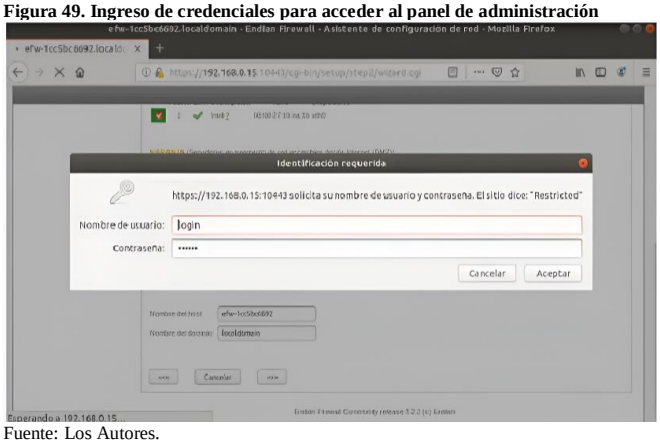
Posteriormente, se accede al asistente de configuración del sistema. Una vez revisadas las opciones iniciales, se selecciona la alternativa correspondiente y se hace clic en Continuar para avanzar con el proceso. Esto permite que el asistente aplique los parámetros definidos y prosiga con los siguientes pasos de la instalación o ajuste de la red.

Figura 48. Avance en el asistente de configuración del sistema


Fuente: Los Autores.
Comentario:Se revisan las opciones iniciales del asistente y se hace clic en Continuar para aplicar los parámetros y seguir con la configuración.

A continuación, se realiza el proceso de ingreso de datos necesarios para acceder al panel de administración del sistema. En esta etapa, el usuario debe proporcionar las credenciales previamente configuradas, incluyendo el nombre de usuario y la contraseña asignada. Una vez ingresada la información requerida, el sistema valida los datos y, si son correctos, permite el acceso al panel de control, desde donde se pueden gestionar y configurar los diferentes servicios y parámetros de la plataforma.

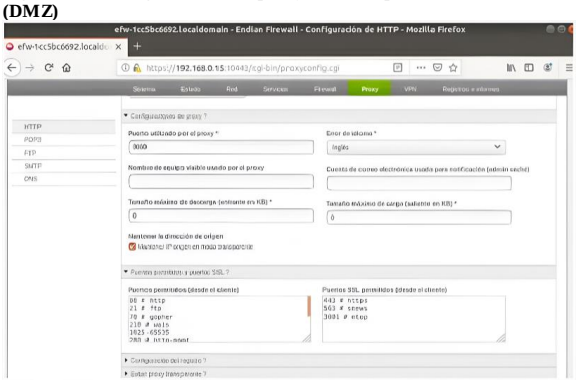
**Figura 49. Ingreso de credenciales para acceder al panel de administración**




Fuente: Los Autores.
Comentario: Se introducen el usuario y la contraseña configurados para acceder al panel de control del sistema.

Para permitir el manejo de archivos a través de los protocolos HTTP (puerto 80) y FTP (puerto 21) dentro de la infraestructura, se accede al módulo de Proxy del sistema. Desde esta sección, se habilita la configuración correspondiente al servicio HTTP Proxy y se especifica que dicha configuración debe aplicarse a la zona Naranja (DMZ).

**Figura 50. Configuración del proxy HTTP aplicado a la zona Naranja (DMZ)**



Fuente: Los Autores.
Comentario: Se accede al módulo de Proxy y se habilita el servicio HTTP Proxy para la zona Naranja.

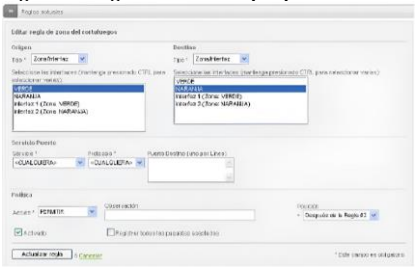
Se selecciona el tipo de regla Zona/VPN/Enlace activo y se elige el enlace activo de la WAN. Luego se configura la regla para el servicio FTP, indicando en Mapear a la IP del servidor en la DMZ y su puerto correspondiente, permitiendo el acceso desde cualquier enlace activo.
Finalmente, se crea una segunda regla idéntica, pero destinada al servicio HTTP (Web).

**Figura 51. Creación de reglas de mapeo para FTP y HTTP desde la WAN hacia la DMZ**

Fuente: Los Autores
Comentario:
Se configuran reglas Zona/VPN/Enlace activo para mapear los servicios FTP y HTTP hacia la IP del servidor en la DMZ.

Se selecciona el tipo de regla Zona/VPN/Enlace activo y se elige el enlace activo de la WAN. Luego se configura la regla para el servicio FTP, indicando en *Mapear a* la IP del servidor en la DMZ y su puerto correspondiente, permitiendo el acceso desde cualquier enlace activo.
Después se crea una segunda regla igual, pero para el servicio HTTP. Con esto se finaliza la prueba de reglas de reenvío, comprobando que desde la WAN ya se puede acceder a los servidores en la DMZ. Ahora se procede a configurar el tráfico entre zonas y a añadir las nuevas reglas necesarias.

**Figura 52. Reglas finales de mapeo para acceso WAN a servicios en la DMZ**



Fuente: Los Autores
Comentario: Se crean y validan las reglas de reenvío para FTP y HTTP desde la WAN hacia la DMZ, confirmando el acceso a los servidores.

### 3.5. Temática 5: Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet.

Crear un perfil y establecer una lista negra bloqueando los siguientes sitios: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.
Creación del perfil "lista_negra": En esta imagen se accede al menú Proxy → Web Filter → Add a Profile, donde se realiza la creación de un nuevo perfil. Le asignamos el nombre "lista_negra" en el campo Profile Name y se activa la opción Activate antivirus scan, lo cual permite aplicar un análisis antivirus al tráfico HTTP que pase por el proxy.

**Figura 53. Creación del perfil "lista_negra" en el Web Filter**

Fuente: Los Autores.
Comentario: Se crea el perfil "lista_negra" en el Web Filter y se activa el análisis antivirus para el tráfico HTTP.

**Adición de los sitios a bloquear (Blacklist):** Se despliega la opción Custom black- and whitelists, donde se especifica de forma manual qué sitios serán permitidos o bloqueados. Como se ve en la imagen en el recuadro **Block the following sites** se ingresan los tres dominios requeridos www.hotmail.com, www.youtube.com y www.elnuevodia.com.co.

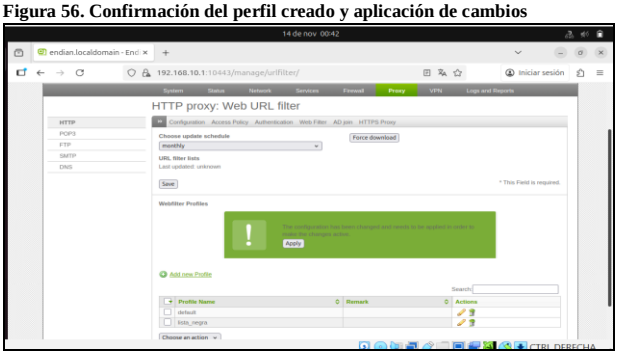
Esta configuración garantiza que el acceso a estas páginas sea denegado para los usuarios asociados a este perfil.

**Figura 54. Configuración de la lista negra en el Web Filter**

Fuente: Los Autores
Comentario: Se añaden los sitios a bloquear ingresando manualmente los dominios en la sección Custom black- and whitelists.

Confirmación del perfil creado y aplicación de cambios: En esta imagen se observa la lista de perfiles creados dentro del Web URL Filter. Damos clic en el botón Apply, lo cual habilita el perfil que creamos llamado lista_negra.

**Figura 56. Confirmación del perfil creado y aplicación de cambios**




Fuente: Los Autores
Comentario: Se observa la lista de perfiles del Web URL Filter y se habilita el perfil lista_negra mediante el botón Apply.

Creación de la regla de acceso en el Proxy HTTP: El perfil de blacklist tenga efecto sobre la red LAN, se debe asociar a una política de acceso. Como se ve en la imagen se configuro una regla desde **Proxy → Access Policy**, como se ve en la imagen.

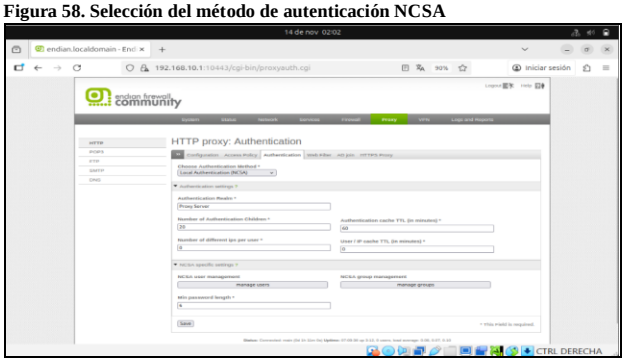
**Figura 57. Creación de la regla de acceso en el Proxy HTTP**


Fuente: Los Autores
Comentario: Se configura una política en Proxy → Access Policy para asociar el perfil de lista_negra a la red LAN.

Al crear esta política, el perfil "lista_negra" queda activo para todos los equipos de la red 192.168.10.0/24, bloqueando automáticamente los sitios previamente definidos.
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.

A continuación, se muestra el desarrollo de este segundo punto:
Selección del método de autenticación (NCSA): En el menú Proxy → Authentication, se seleccionó el método Local Authentication (NCSA). Este método permite gestionar localmente a los usuarios y grupos que podrán autenticarse en el proxy.

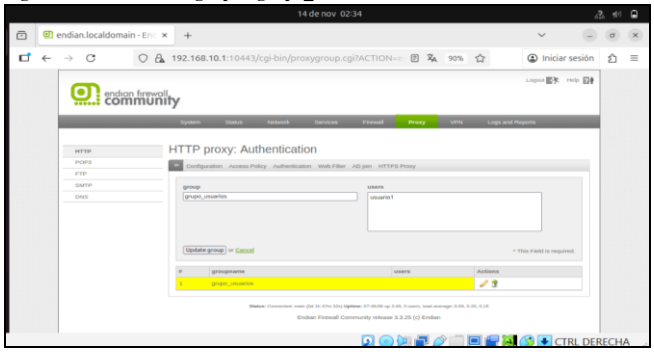
**Figura 58. Selección del método de autenticación NCSA**




Fuente: Los Autores
Comentario: En Proxy → Authentication se selecciona el método Local Authentication (NCSA) para gestionar usuarios y grupos de forma local.

**Creación del grupo "grupo_usuarios":** Desde la opción **NCSA group management** se agregó un nuevo grupo llamado **grupo_usuarios**. En este paso se dejó el espacio disponible para agregar posteriormente al usuario previamente creado. (El sistema lo coloco automáticamente apenas lo cree).

**Figura 59. Creación del grupo "grupo_usuarios" en NCSA**




Fuente: Los Autores
Comentario: Desde NCSA group management se añade el grupo grupo_usuarios, quedando disponible para asociar al usuario creado.

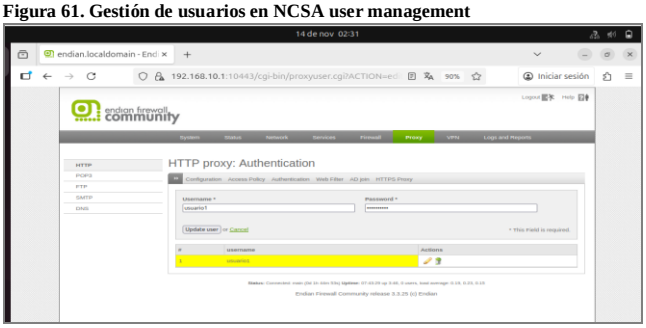
Grupo creado correctamente: La interfaz muestra el grupo "grupo_usuarios" ya registrado en el sistema. Aquí en la imagen se confirman el nombre del grupo y la disponibilidad para editarlo o asociar usuarios.

**Figura 60. Grupo creado correctamente en la gestión NCSA**


Fuente: Los Autores
Comentario: Se visualiza el grupo grupo_usuarios registrado, confirmando su nombre y la opción para editarlo o asociar usuarios.

Gestión de usuarios NCSA: En NCSA user management, se procedió a gestionar los usuarios que se autenticarán en el proxy. Ingresamos a la opción manage users donde allí nos aparece la siguiente imagen.

**Figura 61. Gestión de usuarios en NCSA user management**




Fuente: Los Autores
Comentario: Desde NCSA user management se accede a manage users para administrar los usuarios que se autenticarán en el proxy.

Alli se crea el usuario usuario1, definiendo también su contraseña. Como se ve en la imagen username: *usuario1* y el campo de contraseña completado.
Asignación del usuario al grupo: Una vez creado el usuario, desde la administración de grupos se agregó usuario1 al grupo grupo_usuarios.
La imagen demuestra la asignación correcta, mostrando ambos campos relacionados. (Esta es la misma imagen 2)

**Figura 62. Creación y asignación del usuario usuario1.**

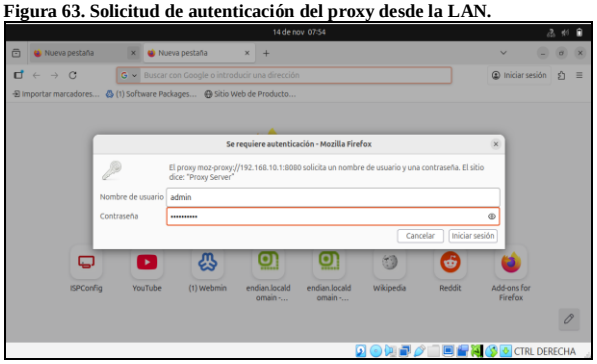

Fuente: Captura de pantalla del proceso en Endian.
Comentario: Se muestra la creación del usuario usuario1 y su asignación al grupo grupo_usuarios.

Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.
A continuación, se muestra el desarrollo de este tercer punto:

Solicitud de autenticación del proxy: En la primera imagen se evidencia que, al intentar navegar desde un equipo ubicado en la red LAN, el navegador Mozilla Firefox solicita autenticación para permitir el acceso a Internet.

El mensaje indica que el proxy configurado en Endian Firewall (192.168.10.1:8080) requiere un nombre de usuario y contraseña válidos, de acuerdo con la política de autenticación. Esta ventana confirma que el proxy está funcionando correctamente y que se debe autenticar antes de poder navegar.

**Figura 63. Solicitud de autenticación del proxy desde la LAN.**




Fuente: Los Autores
Comentario: Se solicita usuario y contraseña para navegar, confirmando que el proxy está activo.

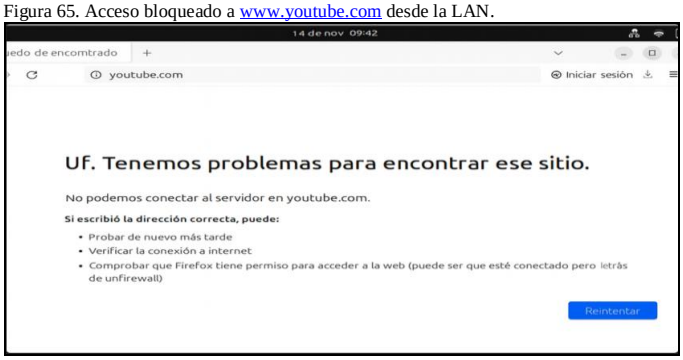
Acceso bloqueado a sitio de la lista negra: En la siguiente imagen se observa que, una vez autenticado el usuario, se intenta ingresar al sitio *hotmail.com*, el cual hace parte de la lista negra previamente configurada. El navegador muestra el mensaje "Tenemos problemas para encontrar ese sitio. No podemos conectar al servidor en hotmail.com". Este mensaje confirma que las políticas de filtrado del proxy están activas y que *hotmail.com* ha sido bloqueado exitosamente, evitando el acceso desde la LAN.

Evidencia www.hotmail.com

**Figura 64. Acceso bloqueado a www.hotmail.com desde la LAN.**


Fuente: Los Autores
Comentario: El sitio hotmail.com es bloqueado según la política de lista negra del proxy.

Evidencia www.youtube.com
Figura 65. Acceso bloqueado a www.youtube.com desde la LAN.




Fuente: Los Autores
Comentario: El sitio youtube.com es bloqueado según la política de lista negra del proxy.

Evidencia del estado aplicado de la política de Access Policy: La siguiente imagen muestra la sección HTTP Proxy > Access Policy, donde se visualiza la política creada, indicando: Source: 192.168.10.0/24 (la red LAN), Destination: hotmail.com, youtube.com y elnuevodia.com.co, Action: access denied, Useragent: ANY, Estado: aplicada correctamente.

## 4. CONCLUSIONES.

La implementación de GNU/Linux Endian en VirtualBox permitió establecer correctamente las zonas verde (LAN), roja (WAN) y naranja (DMZ), garantizando la segmentación de la red y el control del tráfico según los objetivos propuestos.

La configuración de NAT demostró la correcta comunicación entre la LAN y la WAN, así como entre la DMZ e Internet, verificando el reenvío de puertos y la efectividad de las reglas aplicadas.

La habilitación de servicios HTTP y FTP en la zona DMZ y la denegación del protocolo ICMP reforzaron la seguridad de la red, impidiendo accesos no autorizados y controlando la exposición de los servidores al tráfico externo.

Las reglas de acceso entre zonas garantizaron que los protocolos HTTP y FTP funcionaran de manera controlada, permitiendo el acceso legítimo desde la LAN hacia la DMZ y la WAN, y desde la WAN hacia la DMZ según la política definida.

La implementación de un Proxy HTTP con políticas de autenticación y lista negra permitió controlar la navegación en Internet, asegurando que los usuarios cumplieran con las políticas establecidas y bloqueando el acceso a sitios no autorizados, reforzando la seguridad y el control del tráfico web en la red LAN.

## 5. REFERENCIAS


[1] Endian. (2023). Endian Firewall Community Edition – Documentation. Recuperado de https://www.endian.com/documentation

[2] Ubuntu. (2023). Ubuntu Server Guide. Canonical Ltd. Recuperado de https://ubuntu.com/server/docs

[3] Stallings, W. (2020). Network Security Essentials: Applications and Standards (7.ª ed.). Pearson.

[4] Tanenbaum, A. S., & Wetherall, D. J. (2019). Computer Networks (6.ª ed.). Pearson.

[5] *VirtualBox. (2023). VirtualBox User Manual. Oracle Corporation. Recuperado de https://www.virtualbox.org/manual*

[6] Comer, D. E. (2021). Internetworking with TCP/IP Volume One (6.ª ed.). Pearson.