IMPLEMENTACIÓN Y CONFIGURACIÓN DE UN FIREWALL ENDIAN EN VIRTUALBOX: NAT, DMZ, REGLAS DE ACCESO Y PROXY HTTP

Edgar Miguel Delgado Ortiz
e-mail: jmcamargoq@unadvirtual.edu.co
Islein Bustamante Cruz
e-mail: ibustamantec@unadvirtual.edu.co
Laura Daniela Gonzalez Arias
e-mail: ldgonzalezar@unadvirtual.edu.co
María Angélica Fernández Masmela
e-mail: mafernandezma@unadvirtual.edu.co
Richard Javier Quintero Saavedra
e-mail: rjquinteros@unadvirtual.edu.co

RESUMEN: *Este artículo aborda el proceso completo de instalación, configuración y puesta en marcha de una instancia de GNU/Linux Endian en un entorno virtualizado mediante VirtualBox. Se detallan los ajustes necesarios en las tarjetas de red para garantizar el funcionamiento adecuado del firewall y de sus distintos servicios. Posteriormente, se explica la configuración de NAT para el manejo del tráfico de red, así como la habilitación de servicios en la zona DMZ, con el fin de permitir el acceso controlado desde redes externas. Asimismo, se establecen reglas de acceso que permiten o deniegan el tráfico según las políticas de seguridad definidas. Finalmente, se implementa un proxy HTTP no transparente con mecanismos de autenticación, lo que asegura un control eficaz de la navegación en Internet por parte de los usuarios.*

PALABRAS CLAVE: GNU/Linux, Endian Firewall, DMZ (Zona Desmilitarizada), Segmentación de Red.

1 INTRODUCCIÓN

La administración de redes y la implementación de sistemas de seguridad constituyen componentes esenciales en cualquier infraestructura tecnológica moderna [4]. En este trabajo se aborda el proceso completo de configuración y puesta en marcha de una instancia GNU/Linux Endian dentro de VirtualBox [7], con énfasis en la correcta asignación de las tarjetas de red y en su instalación efectiva [9].

A partir de esta base, se profundiza en la configuración de NAT como método de traducción de direcciones [5], con el fin de permitir una comunicación controlada entre los diferentes segmentos de la red. Posteriormente, se analiza la habilitación de servicios en la Zona Desmilitarizada (DMZ) [6], un entorno fundamental para alojar servidores accesibles desde el exterior [1], sin comprometer la seguridad interna. Asimismo, se estudian las reglas de acceso necesarias para permitir o restringir el tráfico entre redes, lo cual constituye el núcleo del control perimetral. Finalmente, se implementa un proxy HTTP no transparente con políticas de autenticación, una herramienta clave para gestionar la navegación de los usuarios y reforzar el control sobre el uso de Internet dentro de la red organizacional. En conjunto, estos elementos ofrecen una visión integral de la construcción y administración de un entorno seguro y funcional basado en Endian Firewall.

2 INSTALACIÓN ENDIAN 3.3.2

2.1 CARACTERÍSTICAS GENERALES

En primer lugar, se descarga la distribución Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Esta solución es compatible con arquitecturas x86.

Se utiliza el programa Oracle VM VirtualBox [3] para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

3 CONFIGURACIÓN DE LA INSTANCIA

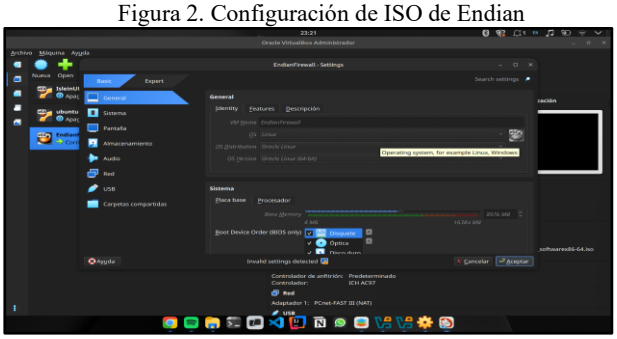
Instalación del firewall Endian a través de su sitio web oficial

Figura 1. Página oficial de descarga de Endian

Fuente: Autoría Propia

Se configuró ISO de Endian en una máquina virtual y se realizó la configuración necesaria para su correcta ejecución.

Figura 2. Configuración de ISO de Endian



Fuente: Autoría Propia

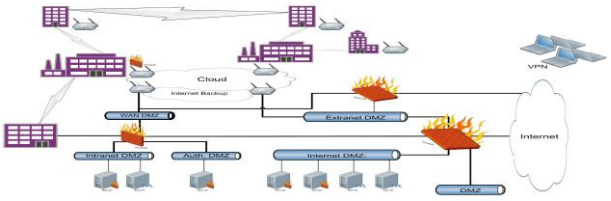
Se crean dos adaptadores de red, los cuales se configuran de la siguiente manera: Adaptador 1: Red NAT, con el fin de que la VM tenga acceso a Internet. Adaptador 2: Adaptador puente, destinado a la red LAN. Adaptador 3: Adaptador puente, utilizado para la red DMZ (opcional).

Figura 3. Configuración de red de Endian

Fuente: Autoría Propia

Configuraciones establecidas a lograr:

Figura 4. Diagrama de conexión con Endian



Fuente: Autoría Propia

Una vez dentro de Endian, se procedió a realizar la configuración del sistema.

Figura 5. Configuración de idioma Endian

Fuente: Autoría Propia

Figura 6. Instalación de paquetes

Fuente: Autoría Propia

Se acepta la configuración del login utilizando el número de serie de la terminal, con el fin de complementar el firewall.

Figura 7. Configuración de serial de terminal Endian

Fuente: Autoría Propia

4 DESARROLLO TEMATICAS

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

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, de la siguiente manera: Zona verde: red interna (LAN); zona roja: acceso a Internet (WAN); y zona naranja: servidores (DMZ).

Configuración IP de las zonas:

- GREEN (LAN): 192.168.10.1/24
- ORANGE (DMZ): 192.168.20.1/24
- RED (WAN): DHCP (automático)

Configuración de redes internas en cliente green lan y servidor orange DMZ

Figura 8. Máquinas virtuales de Endian, Cliente y DMZ

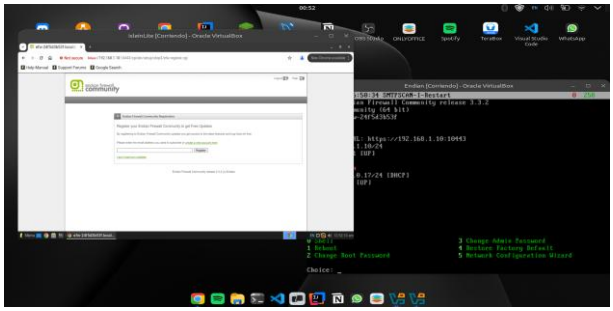
Fuente: Autoría Propia

Figura 9. Configuración de la ip de la green-zone

Fuente: Autoría Propia

Se ajustaron las redes internas verde y naranja para el cliente y la DMZ. En Endian se agregaron las direcciones IP en green (192.168.1.10:10443), desde donde el cliente se conecta y accede a la plataforma Endian.

Figura 10. conexión a Endian y acceso por cliente en la green-zone interna



Fuente: Autoría Propia

Las credenciales se configuraron directamente en la plataforma Endian mediante su menú de interacción, efectuándose posteriormente el cambio de la contraseña.

Figura 11. Acceso a la web de Endian

Fuente: Autoría Propia

Se accede al panel admin de Endian

Figura 12. Acceso a Endian

Fuente: Autoría Propia

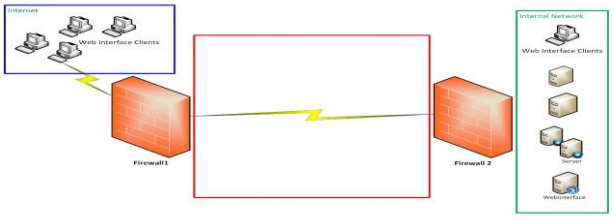
Se configura la zona naranja (Orange Zone) en el firewall con el fin de garantizar una conexión segura. Para ello, se crea una nueva regla especial destinada a esta zona, en la cual se especifica una dirección IP de conexión a través de la red interna previamente configurada en la máquina virtual de Endian.

Figura 13. Configuración firewall para conexión de máquina virtual

Fuente: Autoría Propia

Lo que logra la DMZ en la estructura de la red

Figura 14. configuración del DMZ



Fuente: Autoría Propia

Se configura la conexión de la zona naranja con la DMZ previamente establecida, la cual corresponde a un servidor Ubuntu, integrado con la red interna ya configurada en el sistema Endian.

Figura 15. configuración de red de las máquinas virtuales

Fuente: Autoría Propia

Se obtienen las redes ya configuradas y ubicadas en su zona correspondiente (roja, verde y naranja).

Figura 16. Vista de las redes de las máquinas virtuales

Fuente: Autoría Propia

Se ajustó el archivo Netplan con la dirección IP asignada y se configuró su conexión con el Gateway dentro de la configuración

Figura 17. configuración de ip de la DMZ

Fuente: Autoría Propia

Se realiza un ping para verificar la conexión y la habilitación del firewall mediante el comando ping 8.8.8.8, comprobando que el servidor DMZ cuenta con conectividad.

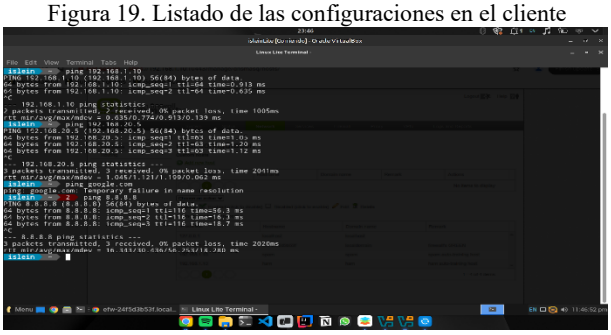
Figura 18. Conexión del servidor DMZ

Fuente: Autoría Propia

- ping 192.168.1.10 (Ping al Gateway).
- ping 192.168.20.5 (Ping al Servidor Ubuntu en la DMZ).
- ping google.com (Ping a Internet).

Descripción: "La red interna (Verde) tiene acceso al Firewall, al servidor en la DMZ y salida a Internet".

Figura 19. Listado de las configuraciones en el cliente



Fuente: Autoría Propia

Se comprueba el aislamiento de la DMZ. El servidor naranja no puede iniciar conexiones hacia la red interna verde, lo que protege los equipos de los usuarios en caso de un ataque al servidor.

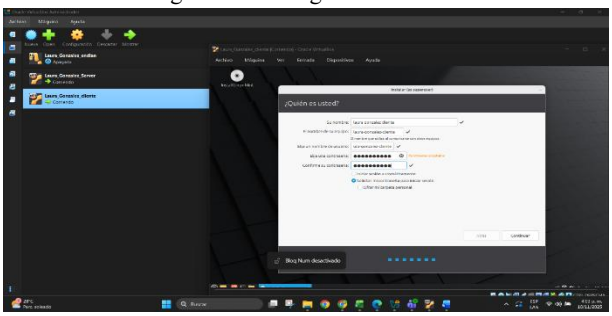
Figura 20. conexión de aislamiento de la DMZ

Fuente: Autoría Propia

4.2 TEMÁTICA 2: CONFIGURACIÓN NAT

La instalación del servidor y la configuración de la red se realizan mediante la instalación de tres máquinas virtuales (Endian, servidor y cliente). El proceso inicia con la selección del idioma y la ejecución de la instalación del servidor. A este equipo se le asigna la dirección IP 192.168.20.15 y el gateway 192.168.20.1. Posteriormente, se configura el nombre del servidor y la contraseña correspondiente. Una vez finalizada la instalación, el sistema se reinicia.

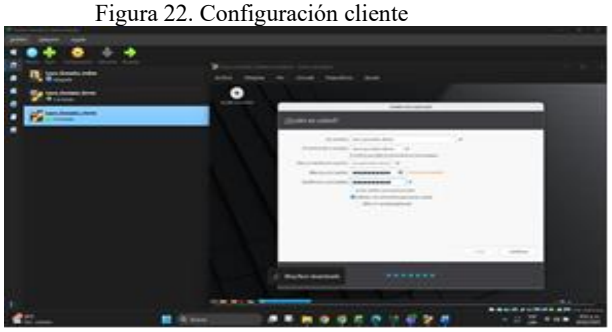
Figura 21. Configuración del servidor



Fuente: Autoría Propia

La instalación del servidor y la configuración de la red del cliente se realizan mediante la selección del idioma, el usuario y la contraseña; posteriormente, se efectúa un reinicio para completar el proceso.

Figura 22. Configuración cliente



Fuente: Autoría Propia

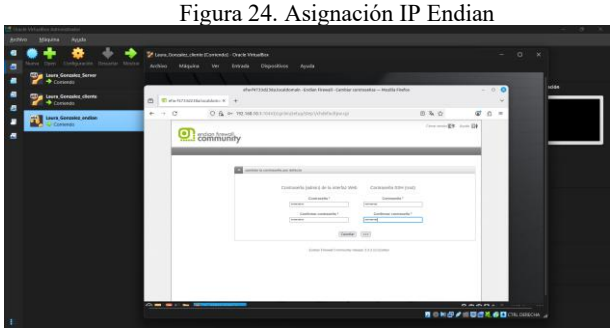
Figura 23. Reinicio del servidor

Fuente: Autoría Propia

4.2.1 CONFIGURACIÓN DE ENDIAN FIREWALL

Durante la instalación de Endian, se selecciona el idioma y se configura la dirección IP correspondiente. Al finalizar el proceso, se visualizan las zonas GREEN (red interna) y RED (salida hacia Internet).

Figura 24. Asignación IP Endian



Fuente: Autoría Propia

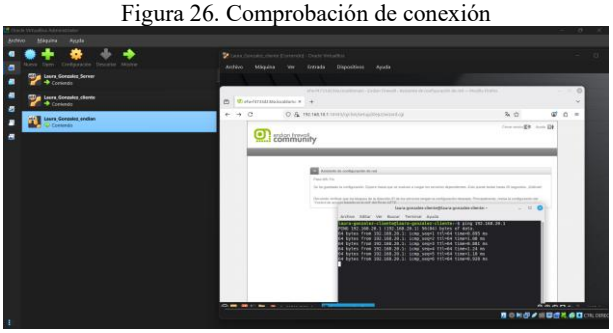
Como se observa en la Figura 25, la interfaz muestra que la zona verde ha obtenido la dirección IP 192.168.10.1, lo que confirma que la interfaz interna se encuentra activa.

Figura 25. IP de la red verde y naranja

Fuente: Autoría Propia

Desde el cliente se accede a Endian mediante la IP 192.168.10.1, realizando previamente una prueba de conectividad. En la interfaz gráfica se configuran el idioma, la zona y las credenciales del firewall.

Figura 26. Comprobación de conexión



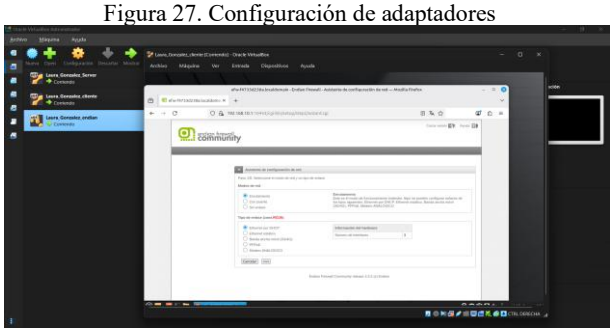
Fuente: Autoría Propia

Se validan tres adaptadores:

- Zona RED: configurada por DHCP
- Zona ORANGE: se asigna la IP 192.168.20.1, junto con el nombre de host y dominio
- Zona GREEN: conectada a la red de usuarios

Se comprobó la conectividad mediante un comando *ping* hacia la dirección IP 192.168.20.1.

Figura 27. Configuración de adaptadores

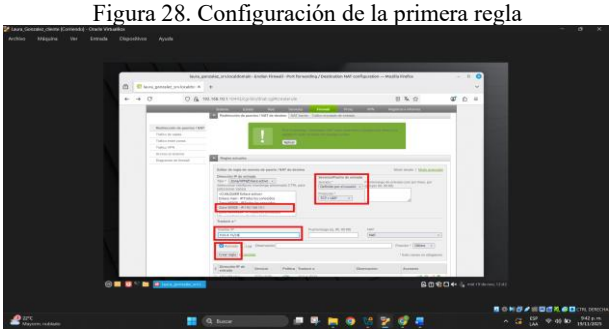


Fuente: Autoría Propia

4.2.2 CONFIGURACIÓN DE REGLAS NAT

Se establece una regla que permite el tráfico desde la zona ORANGE hacía GREEN, aplicando posteriormente dicha regla.

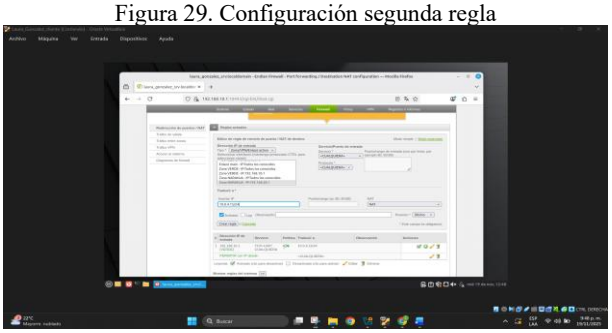
Figura 28. Configuración de la primera regla



Fuente: Autoría Propia

Se crea una segunda regla que permite el flujo desde GREEN hacia ORANGE. Estas reglas garantizan comunicación bidireccional bajo políticas controladas.

Figura 29. Configuración segunda regla



Fuente: Autoría Propia

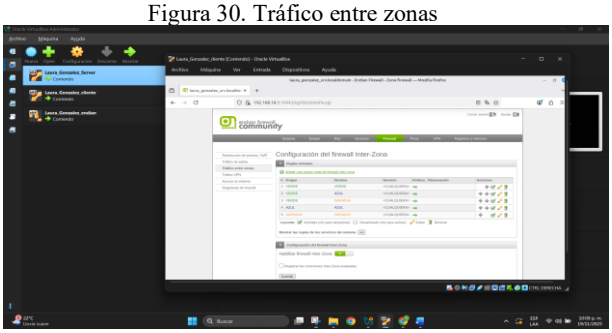
4.2.3 VALIDACIÓN DEL FUNCIONAMIENTO

Para las pruebas entre zonas se realizan pruebas de ping desde:

- Red ORANGE → Red GREEN
- Red GREEN → Red ORANGE

Ambas validaciones resultan exitosas.

Figura 30. Tráfico entre zonas

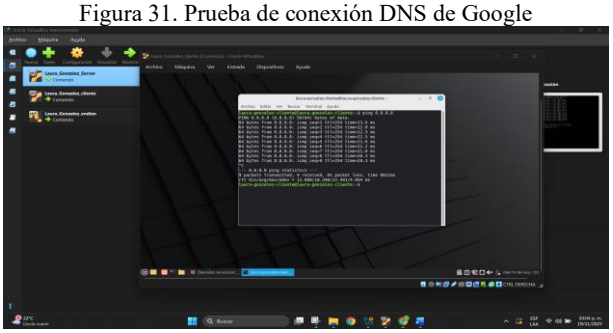


Fuente: Autoría Propia

4.2.4 VALIDACIÓN DE NAVEGACIÓN A INTERNET

Se realizó un ping hacia el DNS público de Google (8.8.8.8), lo que confirmó que la configuración NAT permite la salida a Internet.

Figura 31. Prueba de conexión DNS de Google



Fuente: Autoría Propia

4.2.5 VALIDACIÓN DE TRÁFICO

Se revisan los registros de tráfico saliente y las estadísticas entre zonas, confirmándose que NAT funciona de manera correcta según las reglas aplicadas.

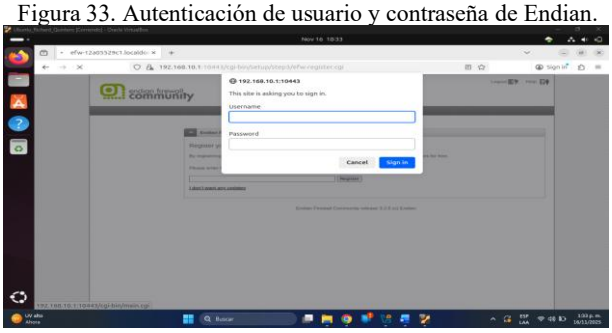
Figura 32. Tráfico de salidas

Fuente: Autoría Propia

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

El producto esperado consiste en habilitar los servicios HTTP y FTP en el servidor web bajo Ubuntu Server, permitiendo el acceso a los puertos 80 y 21 desde la zona DMZ. Además, se debe denegar el protocolo ICMP, bloqueando los puertos 8 y 30 para evitar respuestas de ping en la red. Finalmente, se verifica, en el tráfico de salida, la correcta creación de las reglas de firewall implementadas [8].

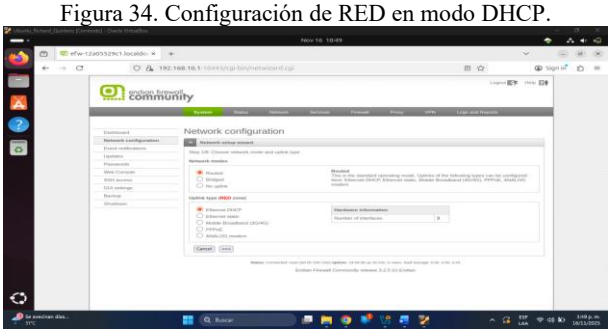
Figura 33. Autenticación de usuario y contraseña de Endian.



Fuente: Autoría propia

Se accede a la interfaz de administración web de Endian desde un equipo cliente ubicado en la red interna, utilizando el protocolo seguro HTTPS en la dirección 192.168.10.1 a través del puerto 10443. A continuación, se ingresan las credenciales administrativas para iniciar la sesión de configuración.

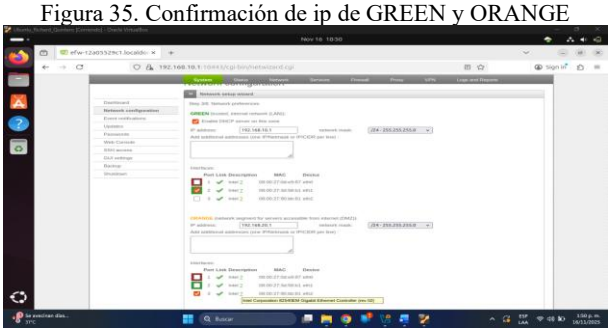
Figura 34. Configuración de RED en modo DHCP.



Fuente: Autoría propia

En el asistente de configuración de red, se selecciona el modo "Ethernet DHCP" para la interfaz ROJA (Uplink). Esto permite que el firewall obtenga automáticamente una dirección IP y salida a Internet desde el proveedor de servicios o la red externa

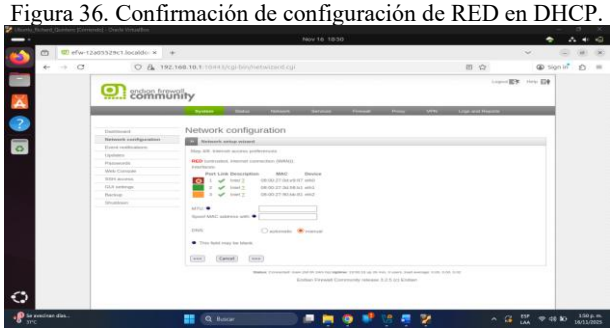
Figura 35. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia

Se definen y verifican las direcciones IP estáticas para los segmentos locales. La zona verde (LAN) se configura con la dirección IP 192.168.10.1 y la zona naranja (DMZ) con la dirección IP 192.168.20.1, estableciendo las puertas de enlace correspondientes para cada subred.

Figura 36. Confirmación de configuración de RED en DHCP.



Fuente: Autoría propia

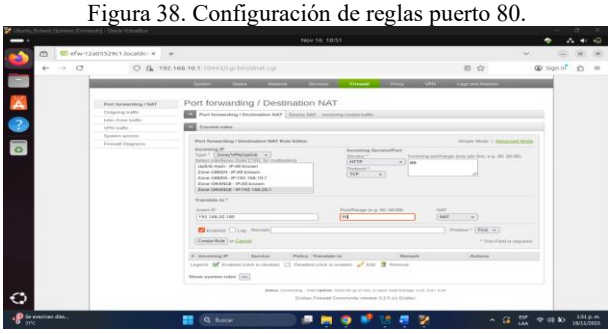
El sistema presenta un resumen de la configuración de las interfaces antes de aplicar los cambios. Se confirma que la interfaz física **eth0** está correctamente asignada a la zona **ROJA**, lo que permite gestionar adecuadamente el tráfico entrante de Internet.

Figura 37. Se ingresó al módulo Firewall.

Fuente: Autoría propia

Dentro del panel de administración, se navega a la sección Firewall > Port Forwarding / Destination NAT. Desde esta interfaz, se inicia el proceso para crear reglas que permitan el acceso desde el exterior a los servicios alojados en la DMZ.

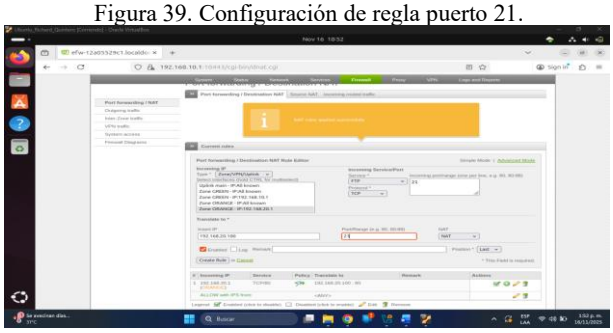
Figura 38. Configuración de reglas puerto 80.



Fuente: Autoría propia

Se configura una regla de reenvío de puertos (DNAT) para permitir el tráfico web. Se especifica que toda petición entrante por la interfaz de enlace (uplink), a través del puerto TCP 80, sea redirigida automáticamente hacia la dirección IP 192.168.20.100, correspondiente al servidor Ubuntu ubicado en la DMZ.

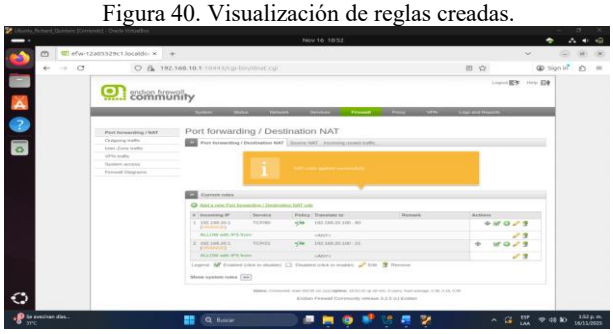
Figura 39. Configuración de regla puerto 21.



Fuente: Autoría propia

De manera similar, se habilita el acceso al servicio de transferencia de archivos. Se crea una regla que intercepta el tráfico en el puerto TCP 21 de la zona pública y lo reenvía al mismo servidor interno (192.168.20.100) en la zona naranja.

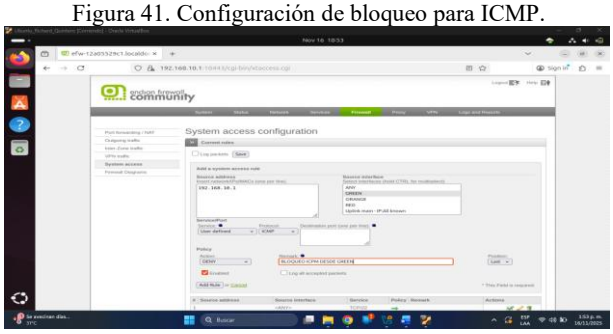
Figura 40. Visualización de reglas creadas.



Fuente: Autoría propia

El panel de "Reglas actuales" muestra las dos directivas DNAT creadas (HTTP y FTP) en estado activo. Esto confirma que el firewall está configurado para permitir y gestionar el tráfico externo hacia los servicios específicos de la DMZ sin exponer el resto de la red.

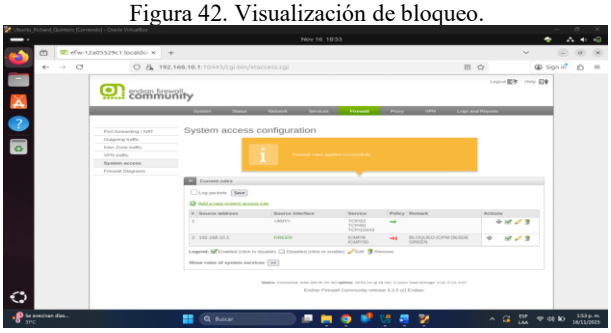
Figura 41. Configuración de bloqueo para ICMP.



Fuente: Autoría propia

Para reforzar la seguridad, se configura una regla de Acceso al Sistema. Se establece la denegación (DENY) del protocolo ICMP (ping) proveniente de la interfaz VERDE (192.168.10.1), evitando que el firewall responda a solicitudes de eco desde la red interna o la DMZ, según corresponda.

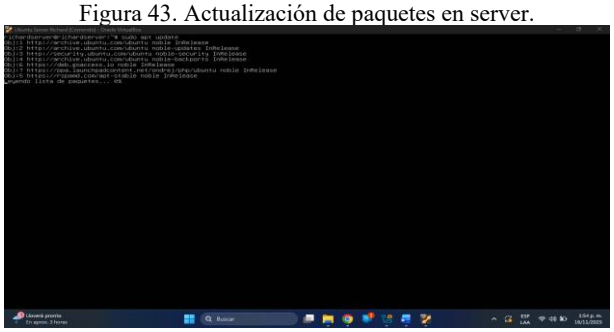
Figura 42. Visualización de bloqueo.



Fuente: Autoría propia

Se visualiza la lista de reglas de acceso al sistema, confirmando que la política de bloqueo ICMP ha sido guardada y aplicada correctamente. Esta medida ayuda a ocultar la presencia del dispositivo ante escaneos de red básicos.

Figura 43. Actualización de paquetes en server.



Fuente: Autoría propia

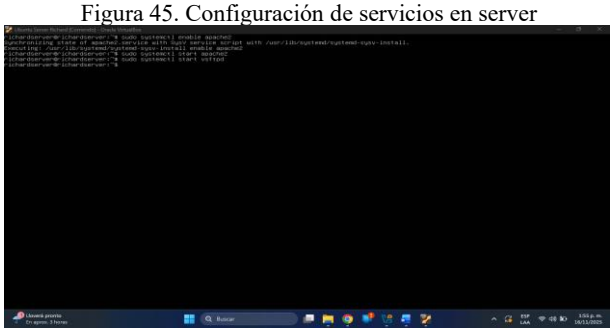
En la terminal del servidor Ubuntu, ubicado en la zona naranja, se ejecutan los comandos de actualización de paquetes (apt update) con el fin de garantizar que el sistema operativo disponga de las últimas definiciones de seguridad antes de la instalación de nuevos servicios.

Figura 44. Instalación de apache y FTP en server.

Fuente: Autoría propia

Se procede a la instalación de los paquetes de software necesarios mediante el comando apt install apache2 vsftpd. Este proceso permite desplegar el servidor web Apache y el servidor FTP en la máquina virtual, la cual actuará como servidor público.

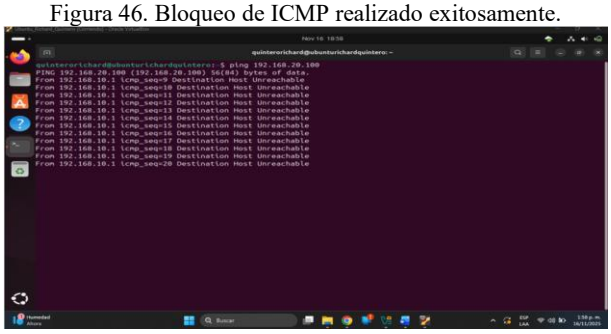
Figura 45. Configuración de servicios en server



Fuente: Autoría propia

Tras la instalación, se ejecutan los comandos systemctl para iniciar y habilitar los servicios HTTP y FTP, garantizando que estos se ejecuten automáticamente al arrancar el sistema y estén listos para recibir conexiones.

Figura 46. Bloqueo de ICMP realizado exitosamente.



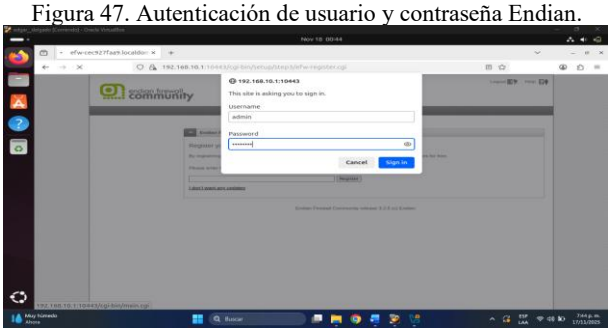
Fuente: Autoría propia

Se realizó una prueba de conectividad mediante el comando ping hacia la dirección IP de la red DMZ. Como se observa en la consola, se recibió el mensaje “Destination Host Unreachable”, lo cual valida que la regla de firewall creada anteriormente está bloqueando de manera efectiva el tráfico ICMP.

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

Producto esperado: Configuración de reglas de acceso en un firewall para controlar el tráfico de red, permitiendo servicios legítimos y bloqueando el tráfico no deseado. Este proceso incluye la definición de políticas de seguridad, la configuración de reglas por puerto y protocolo, el uso de NAT para la redirección de tráfico, la verificación de registros y la realización de pruebas de conectividad, con el fin de asegurar su efectividad y seguridad.

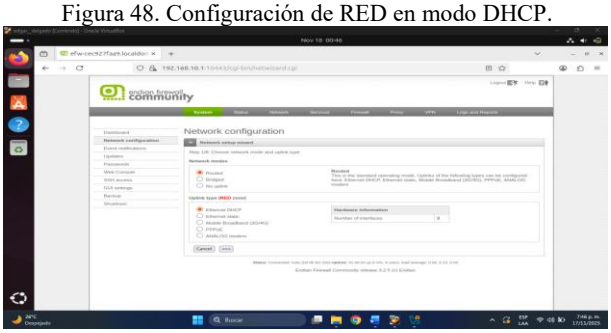
Figura 47. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

Se accede a la consola de administración web de Endian mediante la autenticación del usuario administrador, como paso previo necesario para modificar la configuración de las interfaces de red.

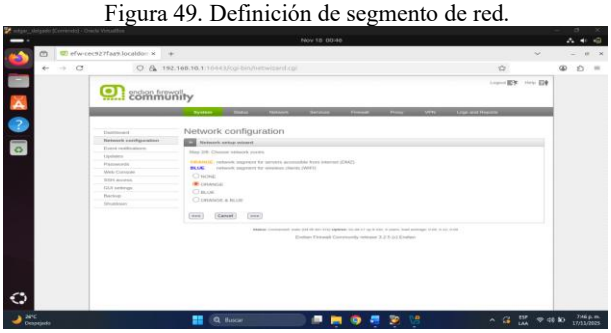
Figura 48. Configuración de RED en modo DHCP.



Fuente: Autoría propia

Selección del modo de conexión para la zona ROJA (Uplink). Se configuró como Ethernet DHCP con el fin de obtener direccionamiento dinámico desde el proveedor de Internet o desde la red externa.

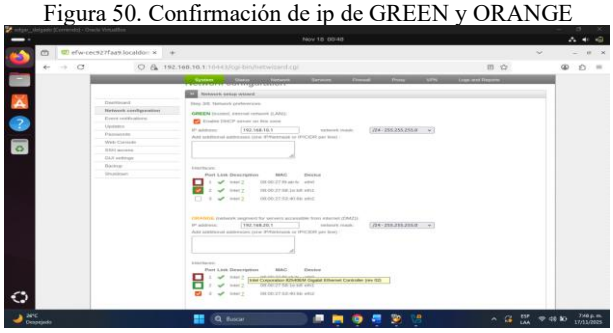
Figura 49. Definición de segmento de red.



Fuente: Autoría propia

En el asistente de configuración, se habilita la zona NARANJA (Orange) para establecer una Zona Desmilitarizada (DMZ), separándola lógicamente de la red inalámbrica (BLUE) o la red interna (GREEN).

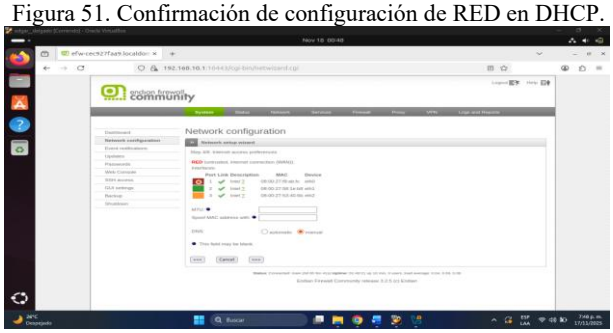
Figura 50. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia

Se realizó la confirmación de las direcciones IP asignadas a las interfaces locales: 192.168.10.1 para la zona VERDE (LAN) y 192.168.20.1 para la zona NARANJA (DMZ), estableciendo así la topología lógica de la red.

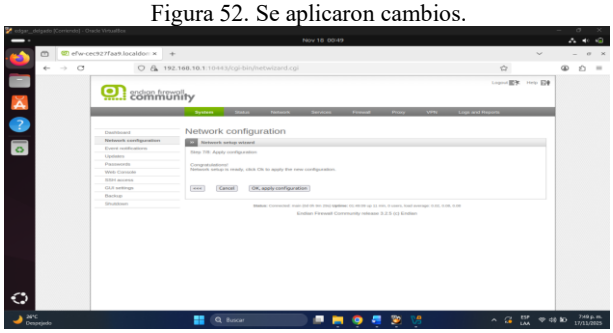
Figura 51. Confirmación de configuración de RED en DHCP.



Fuente: Autoría propia

Vista previa de la asignación de interfaces físicas a las zonas lógicas antes de aplicar los cambios. Se valida que la interfaz eth0 esté correctamente asociada a la zona ROJA para la salida a Internet.

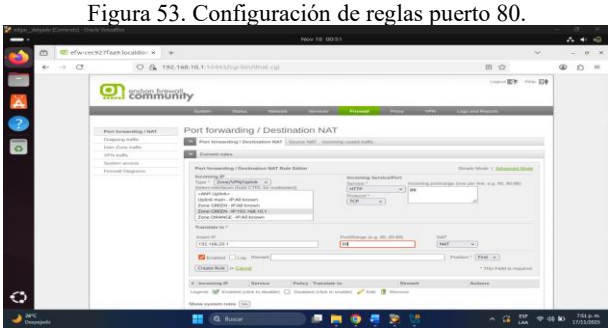
Figura 52. Se aplicaron cambios.



Fuente: Autoría propia

Finalización del asistente de configuración de red. El sistema aplica los cambios y reinicia los servicios de red necesarios para activar el nuevo esquema de direccionamiento y zonas.

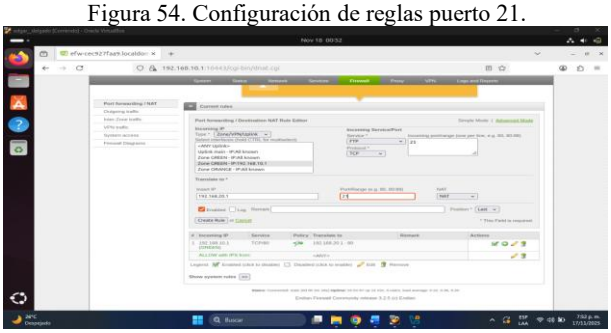
Figura 53. Configuración de reglas puerto 80.



Fuente: Autoría propia

Creación de una regla de Destination NAT (Port Forwarding) para redirigir el tráfico TCP entrante por el puerto 80 hacia el servidor web ubicado en la dirección IP 192.168.20.1 dentro de la zona DMZ.

Figura 54. Configuración de reglas puerto 21.



Fuente: Autoría propia

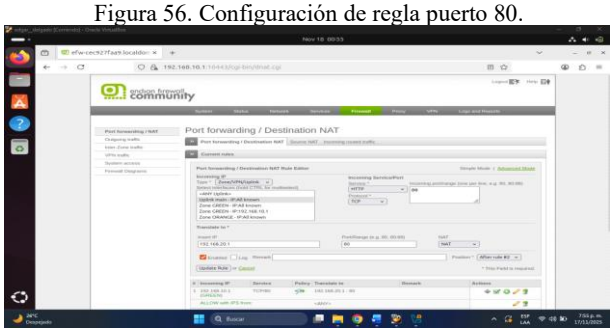
Configuración de la regla de reenvío de puertos para el protocolo de transferencia de archivos. Se permite el tráfico TCP en el puerto 21 destinado al servidor interno en la DMZ, garantizando el acceso a los servicios FTP desde la red externa.

Figura 55. Reglas guardadas y aplicadas.

Fuente: Autoría propia

Visualización del panel de reglas de firewall donde se confirman las políticas DNAT creadas. Se observa que tanto el tráfico HTTP como FTP está permitido y correctamente redirigido hacia el servidor objetivo en la zona naranja.

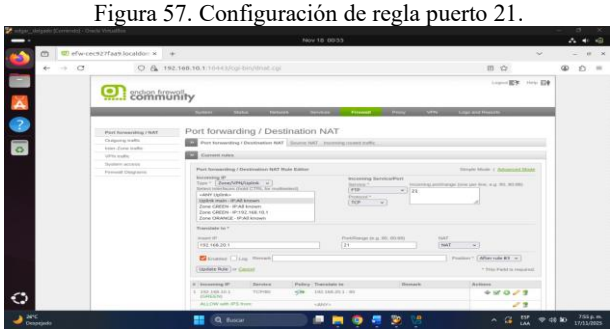
Figura 56. Configuración de regla puerto 80.



Fuente: Autoría propia

Detalle de la configuración de la regla de acceso para el puerto 80, en la cual se especifican la interfaz de origen, el protocolo (TCP) y la dirección de destino para la traducción de direcciones de red.

Figura 57. Configuración de regla puerto 21.



Fuente: Autoría propia

Vista detallada de los parámetros de la regla para el puerto 21, asegurando que el tráfico de control FTP sea gestionado adecuadamente por el firewall hacia la zona desmilitarizada.

Figura 58. Reglas guardadas y aplicadas.

Fuente: Autoría propia

Se confirmó en la interfaz de gestión que todas las reglas de acceso y de traducción de direcciones (NAT) para los servicios web y de archivos se encuentran habilitadas y en correcto funcionamiento.

Figura 59. Verificación de logs.

Fuente: Autoría propia

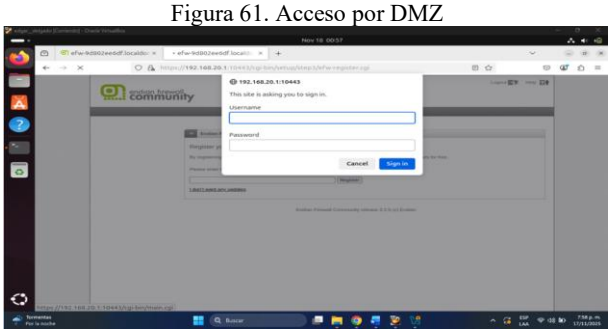
Inspección de los registros del firewall en vivo (Live Logs). Se evidencian las conexiones aceptadas y reenviadas, lo que valida que el tráfico hacia los puertos 80 y 21 fluye conforme a las reglas establecidas.

Figura 60. Verificación de tráfico exitoso.

Fuente: Autoría propia

Detalle de los registros (logs) del sistema, donde se corrobora la comunicación exitosa entre la zona de red local (LAN) y la zona externa (WAN), a través de las políticas de NAT configuradas.

Figura 61. Acceso por DMZ



Fuente: Autoría propia

Verificación de conectividad desde un cliente interno hacia la puerta de enlace de la DMZ (192.168.20.1) mediante navegador web, confirmando la accesibilidad a la zona naranja.

Figura 62. Proceso exitoso

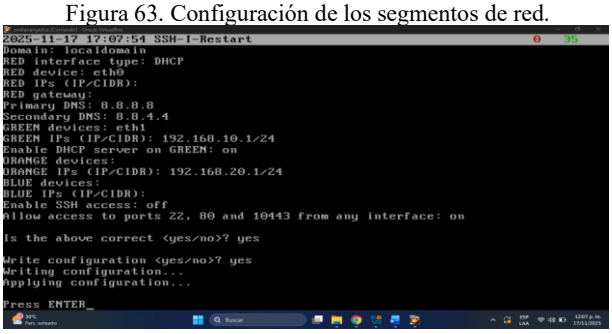
Fuente: Autoría propia

Se realizó una prueba exitosa de acceso a un sitio web externo (Google) desde un equipo de la red interna, demostrando que las reglas de enmascaramiento (SNAT) y la salida a Internet funcionan correctamente.

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

Producto esperado: El producto esperado consiste en crear un perfil y establecer una lista negra que bloquee los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe implementar la autenticación por usuario, creando un usuario y asignándole a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se debe probar el acceso a los sitios bloqueados desde la LAN utilizando un navegador web.

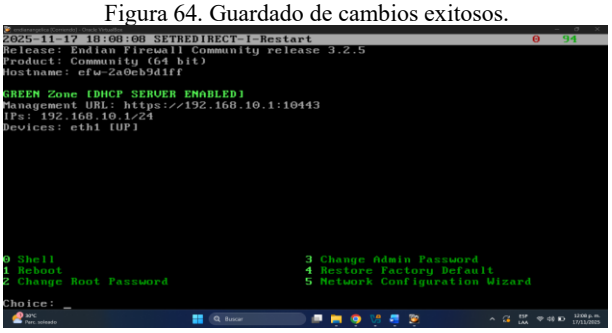
Figura 63. Configuración de los segmentos de red.



Fuente: Autoría propia

Mediante la visualización de la configuración de red a través de la interfaz de línea de comandos (CLI) de Endian, se confirma que el servidor DHCP se encuentra habilitado en la zona VERDE (192.168.10.1/24).

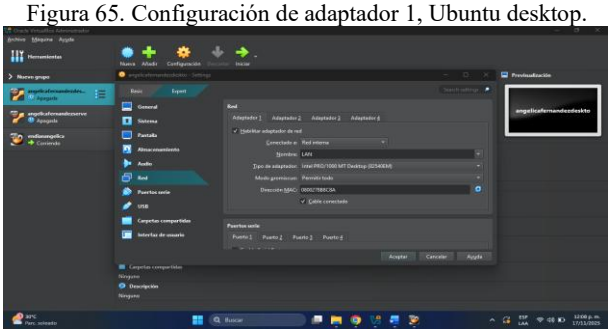
Figura 64. Guardado de cambios exitosos.



Fuente: Autoría propia

El sistema confirma, mediante la terminal, que la configuración de la zona VERDE es correcta y que la interfaz de gestión web se encuentra accesible.

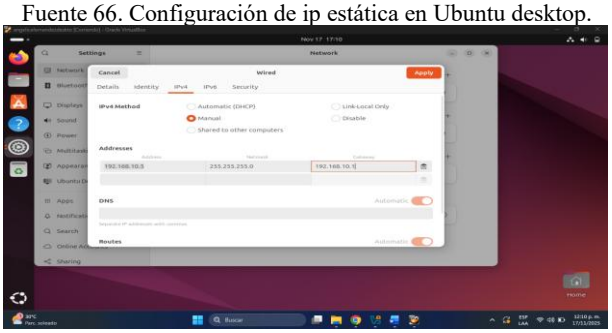
Figura 65. Configuración de adaptador 1, Ubuntu desktop.



Fuente: Autoría propia

Ajuste de las propiedades de la máquina virtual del cliente "Ubuntu Desktop". El adaptador de red se configura en modo "Red interna" con el nombre "LAN" para simular la conexión física a la zona VERDE del firewall.

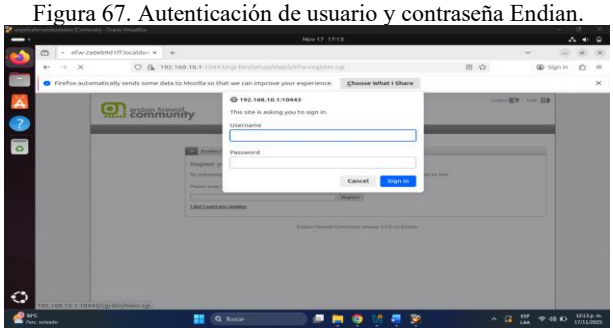
Fuente 66. Configuración de ip estática en Ubuntu desktop.



Fuente: Autoría propia

Configuración manual de la interfaz de red en el cliente Ubuntu. Se asigna la dirección IP 192.168.10.5, con puerta de enlace 192.168.10.1 (correspondiente a la IP interna de Endian), con el fin de asegurar la comunicación con el proxy.

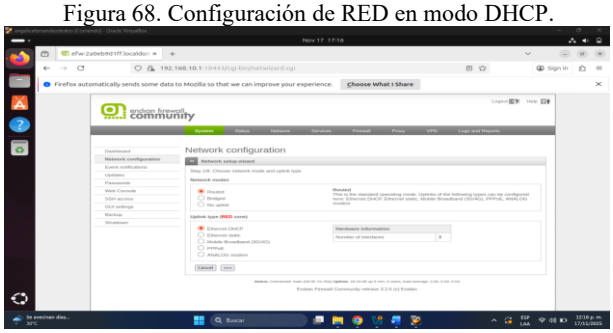
Figura 67. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia

Se realiza el inicio de sesión en el portal de administración de Endian para proceder con la configuración de los servicios de filtrado web y del proxy HTTP.

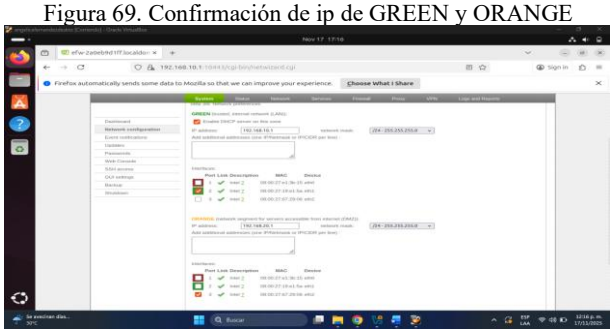
Figura 68. Configuración de RED en modo DHCP.



Fuente: Autoría propia

Paso de verificación dentro del asistente de red para confirmar que la interfaz de salida (ROJA) mantiene la configuración adecuada para permitir la navegación de los clientes a través del proxy.

Figura 69. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia

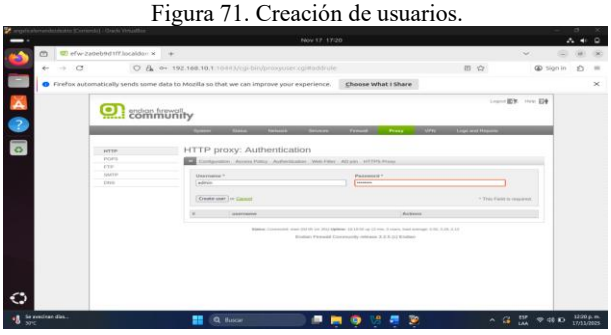
Se realizó la validación de las direcciones IP de las zonas VERDE y NARANJA en el panel de configuración, asegurando que coincidieran con la topología requerida para el filtrado de contenido.

Figura 70. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia

Pantalla de resumen del asistente de red, en la que se reitera la asignación de dispositivos físicos a las zonas lógicas antes de habilitar los servicios de la capa de aplicación.

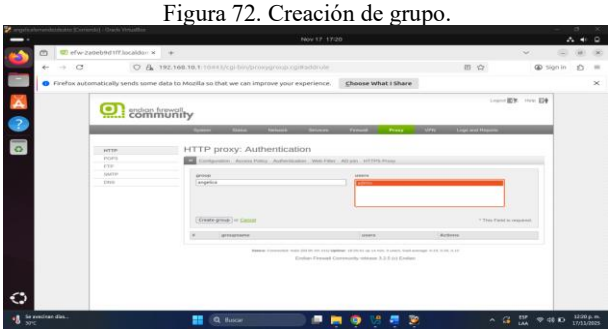
Figura 71. Creación de usuarios.



Fuente: Autoría propia

En la sección Proxy > Authentication, se crea un nuevo usuario local (admin) con su respectiva contraseña. Este usuario será requerido para autorizar la navegación en los equipos clientes.

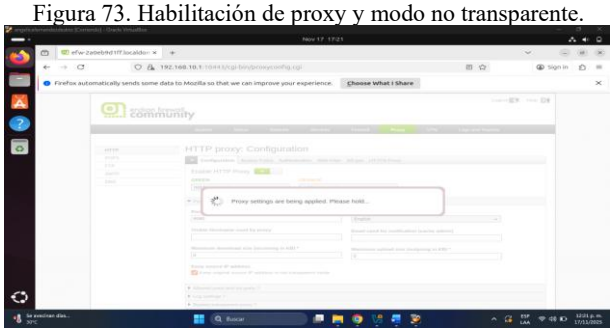
Figura 72. Creación de grupo.



Fuente: Autoría propia

Configuración de un grupo de acceso denominado "angelica", al cual se asocia el usuario creado anteriormente. Esto permite aplicar políticas de navegación diferenciadas por grupos.

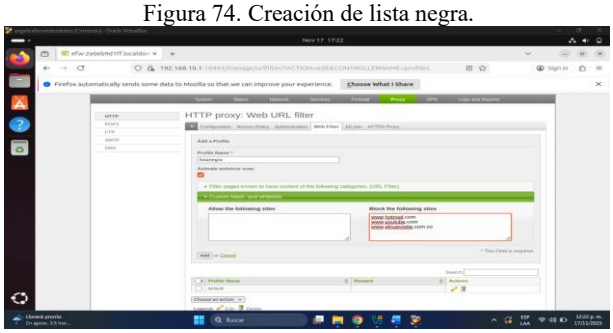
Figura 73. Habilitación de proxy y modo no transparente.



Fuente: Autoría propia

Activación del servicio de Proxy HTTP en modo no transparente. Se define el puerto de escucha 8080 en la interfaz VERDE, obligando a los clientes a configurar manualmente el proxy en sus navegadores.

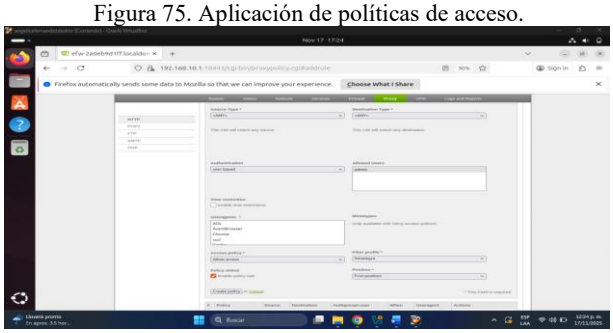
Figura 74. Creación de lista negra.



Fuente: Autoría propia

Creación de un perfil de filtro web llamado "listanegra". En la sección de bloqueo (Block the following sites), se añaden los dominios restringidos: hotmail.com, youtube.com y elnuevodia.com.co.

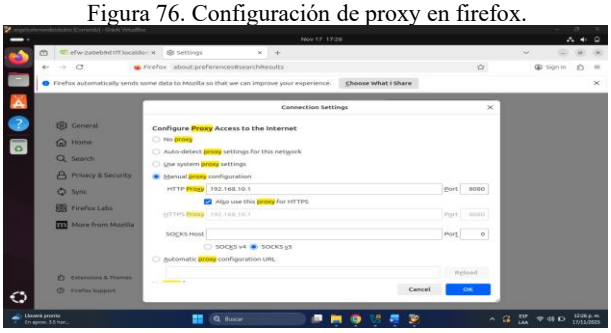
Figura 75. Aplicación de políticas de acceso.



Fuente: Autoría propia

Definición de una política de acceso que vincula el origen (cualquiera), la autenticación (basada en usuario), el usuario permitido (admin) y el perfil de filtro ("listanegra"), estableciendo las reglas de navegación

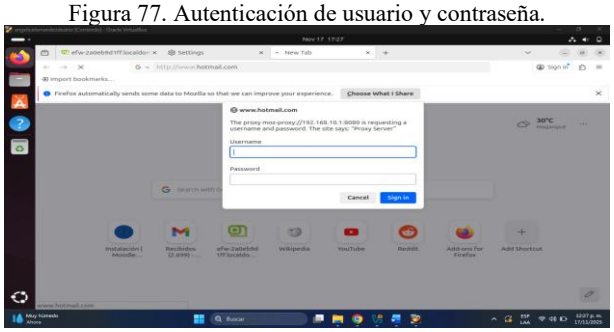
Figura 76. Configuración de proxy en firefox.



Fuente: Autoría propia

Configuración manual del proxy en el navegador Firefox del cliente Ubuntu. Se establece la dirección IP del firewall (192.168.10.1) y el puerto 8080 para los protocolos HTTP y HTTPS.

Figura 77. Autenticación de usuario y contraseña.



Fuente: Autoría propia

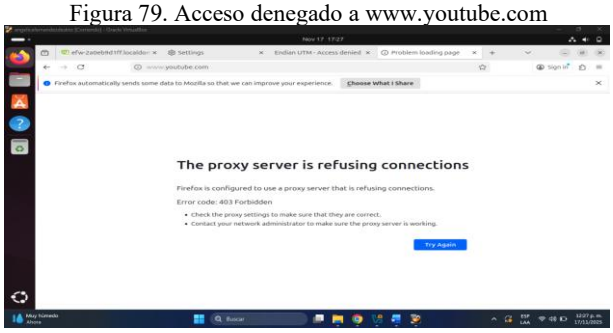
Al intentar navegar, el proxy intercepta la conexión y solicita las credenciales correspondientes. Se observa una ventana emergente en la que se requiere el nombre de usuario y la contraseña previamente configurados en el firewall.

Figura 78. Acceso denegado de www.hotmail.com

Fuente: Autoría propia

Verificación de la política de filtrado. Al intentar acceder a www.hotmail.com, el firewall deniega la conexión y muestra una página de advertencia indicando que el sitio se encuentra en la lista negra.

Figura 79. Acceso denegado a www.youtube.com



Fuente: Autoría propia

Prueba de acceso a www.youtube.com. El navegador muestra un error de conexión rechazada o denegada, lo que confirma que el **proxy** se encuentra filtrando el tráfico hacia este dominio multimedia.

Figura 80. Acceso denegado a www.elnuevodia.com.co

Fuente: Autoría propia

Prueba final de acceso a www.elnuevodia.com.co. Se visualiza la página de "Acceso Denegado" (Access has been denied) generada por Endian UTM, validando la efectividad del perfil de filtrado configurado.

5 CONCLUSIONES

Importancia de la Segmentación de Redes: La implementación exitosa de las tres zonas (Roja, Verde y Naranja) en Endian Firewall demostró ser una medida de seguridad crítica. Se evidenció que colocar servidores públicos en una DMZ protege eficazmente los activos de la red interna (LAN), ya que, aunque el servidor en la zona naranja sea comprometido, el firewall impide el acceso lateral hacia la zona verde.

La práctica de configuración NAT permitió comprender de manera integral el funcionamiento de la traducción de direcciones dentro de un entorno segmentado por zonas de seguridad. La implementación de Endian Firewall facilitó la creación de un esquema controlado en el que fue posible gestionar el flujo de tráfico entre redes internas y externas, garantizando conectividad eficiente y protección frente a accesos no autorizados. Las pruebas realizadas entre las zonas GREEN, ORANGE y RED confirmaron que las reglas de NAT y ruteo fueron aplicadas correctamente, asegurando la comunicación bidireccional y el acceso a Internet. En conjunto,

esta experiencia evidencia la importancia de los firewalls UTM y de la configuración adecuada de políticas de red para asegurar un funcionamiento estable, seguro y adaptable a las necesidades actuales de infraestructura.

El uso de herramientas GNU/Linux para la administración del cortafuegos y el filtrado de tráfico garantiza una mayor flexibilidad y un control preciso sobre los servicios expuestos. Este enfoque no solo mejora la integridad y disponibilidad de los datos, sino que también contribuye a una gestión más eficiente de los recursos y una seguridad perimetral robusta. En definitiva, la integración de estas estrategias representa un avance significativo hacia una infraestructura tecnológica confiable, escalable y alineada con las mejores prácticas de ciberseguridad.

La configuración de reglas de acceso para permitir o denegar el tráfico constituye un componente esencial en la arquitectura de seguridad de cualquier red. A través de estas políticas es posible controlar de manera precisa qué comunicaciones son autorizadas y cuáles deben ser restringidas, garantizando así la integridad, disponibilidad y confidencialidad de los recursos internos. La correcta definición de reglas basadas en criterios como dirección IP, puertos y protocolos permite no solo mitigar riesgos asociados a accesos no autorizados, sino también optimizar el flujo de datos según las necesidades operativas de la organización. En conjunto, la implementación rigurosa de estas reglas fortalece significativamente la postura de seguridad del sistema y asegura un entorno de red más confiable y eficiente.

La configuración de redes segmentadas es crucial para la seguridad y eficiencia operativa de cualquier infraestructura de TI. Al dividir la red en zonas diferenciadas, como LAN y DMZ, y establecer reglas de acceso específicas, es posible garantizar que los sistemas internos estén protegidos de accesos no autorizados mientras se permite la interacción controlada con recursos expuestos al público, como servidores web. El uso de herramientas como Endian Firewall facilita la implementación de estas configuraciones, asegurando que la red funcione de manera eficiente y segura. La correcta implementación y gestión de estas configuraciones proporcionan una mayor defensa contra posibles amenazas externas y mejor control sobre el tráfico interno.

6 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix. https://learning.lpi.org/es/learning-materials/101-500/102/

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

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

[4] Referencia sobre firewall, zonas y segmentación IETF. (2018). Firewall considerations for network security. https://www.ietf.org

[5] NAT y seguridad en redes Hunt, C. (2021). TCP/IP network administration (4.ª ed.). O'Reilly Media.

[6] Configuración de zonas en Endian. (2022). Network zone configuration in Endian Firewall. https://docs.endian.com

[7] Documento técnico sobre administración de redes Linux Nemeth, E., Snyder, G., Hein, T., Whaley, B., & Mackin, D. (2017). UNIX and Linux system administration handbook (5.ª ed.). Addison-Wesley.

[8] Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

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