IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN REDES VIRTUALIZADAS CON GNU/LINUX ENDIAN FIREWALL

Carlos Eduardo Choconta Campo
e-mail: cechocontac@unadvirtual.edu.co
Yeny Fernanda Buitrago Varela
e-mail: yfbuitragov@unadvirtual.edu.co
Jaime Rojas Cabrera
e-mail: jrojascab@unadvirtual.edu.co
Wilmar Coronado Solar
e-mail: wcoronados@ unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación de un sistema de seguridad de red basado en GNU/Linux Endian Firewall en un entorno virtualizado con VirtualBox. La arquitectura segmenta la red en zonas verde, naranja y roja, lo que facilita la gestión y protección de diferentes niveles de confianza. Se describe el proceso de instalación y configuración de interfaces, reglas de acceso y servicios en la DMZ, asegurando la separación entre redes internas y externas. Además, se implementa un proxy HTTP con políticas de autenticación y bloqueo de sitios específicos, reforzando la seguridad del acceso web. Los resultados evidencian una arquitectura segura y flexible que cumple con los principios de seguridad perimetral y control de tráfico en entornos virtualizados. Este enfoque permite gestionar servicios críticos y mejorar la protección contra amenazas externas, demostrando la viabilidad de los sistemas basados en GNU/Linux para la seguridad en entornos empresariales*.

PALABRAS CLAVE: VirtualBox, Endian firewall, LAN, WAN, NAT, HTTP, Zona DMZ.

1 INTRODUCCIÓN

En esta actividad grupal se implementan medidas de seguridad perimetral en una red que abarca zonas LAN, WAN y DMZ, utilizando la distribución GNU/Linux Endian Firewall (EFW) como herramienta principal. El objetivo principal es proteger los servicios y servidores ubicados en la DMZ, así como controlar el acceso entre la red interna y el exterior. Para lograrlo, se abordan varias temáticas clave, como la configuración inicial de Endian y sus zonas de red (verde, roja y naranja), la habilitación de servicios HTTP y FTP en la DMZ, la restricción del protocolo ICMP para aumentar la seguridad, y la implementación de un proxy HTTP no transparente con políticas de autenticación y filtrado web. Todo el proceso de configuración será documentado con evidencias prácticas que incluyen comandos, fechas y los resultados obtenidos desde la consola.

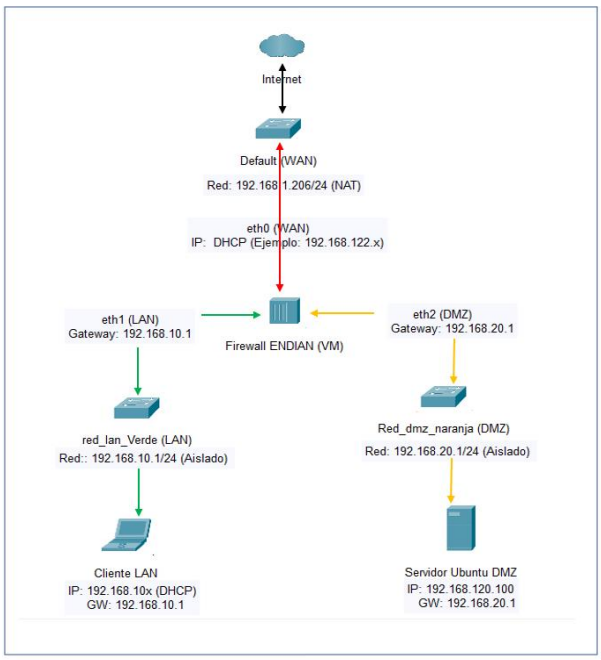
2 DESARROLLO

2.1 INSTALACIÓN DE ENDIAN FIREWALL EN VIRTUALBOX

Se presenta el proceso de la instalación y configuración de la distribución GNU/Linux Endian Firewall (EFW) el cual será el componente principal para la seguridad perimetral en redes que serán segmentadas, habrá tres redes que serán: la zona verde (LAN), la zona naranja (ZDM) y la zona roja (WAN). el sistema Endian se va a implementar en el software VirtualBox.

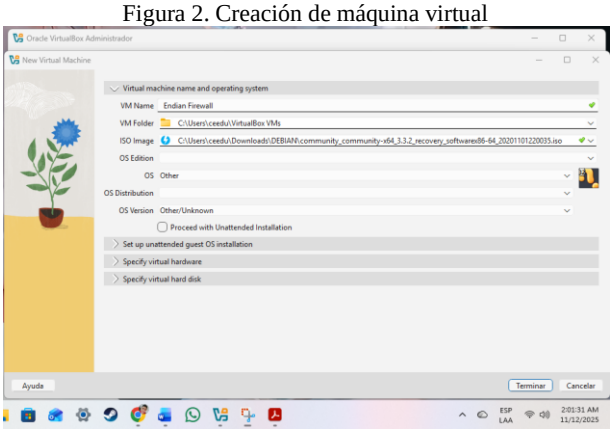
En la siguiente imagen se muestra cómo se van a dividir las IPs en cada una de las zonas.

Figura 1. Topología de red.



Fuente: Autoría propia (Jaime Rojas)

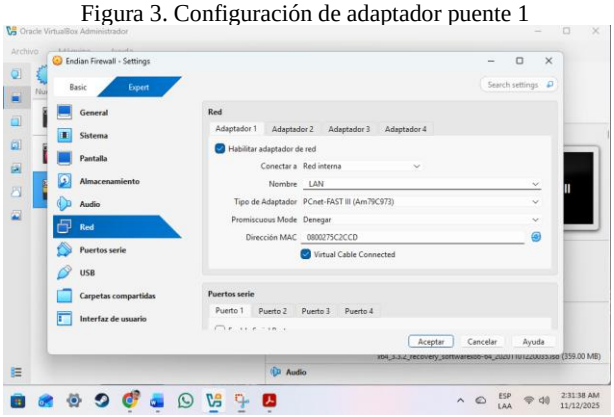
Figura 2. Creación de máquina virtual



Fuente: Autoría propia (Carlos Choconta Campo)

En el adaptador 1 de Endian lo configuramos como adaptador puente (WAN).

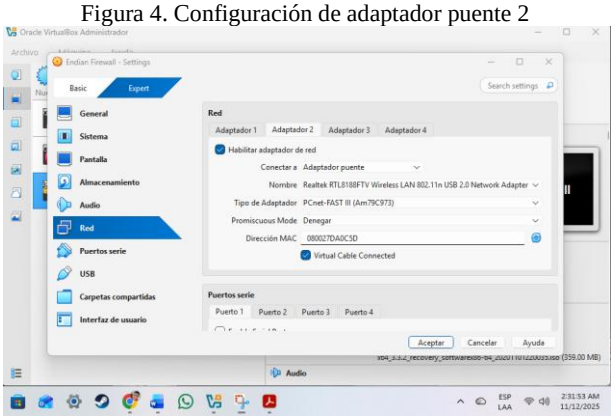
Figura 3. Configuración de adaptador puente 1



Fuente: Autoría propia (Carlos Choconta Campo)

En el adaptador 2 de Endian lo configuramos como red interna (LAN).

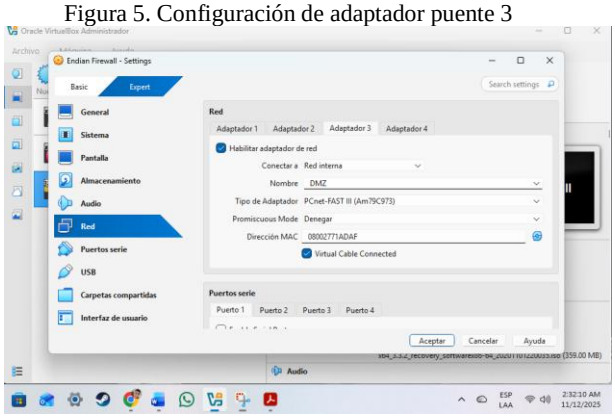
Figura 4. Configuración de adaptador puente 2



Fuente: Autoría propia (Carlos Choconta Campo)

En el adaptador 3 de Endian lo configuramos como red interna (DMZ).

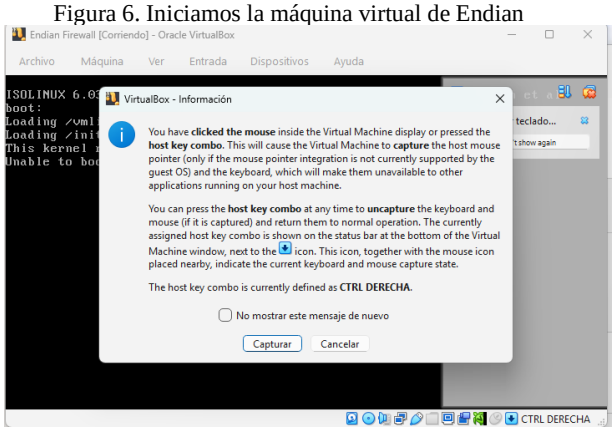
Figura 5. Configuración de adaptador puente 3



Fuente: Autoría propia (Carlos Choconta Campo)

Iniciamos la máquina virtual de endian.

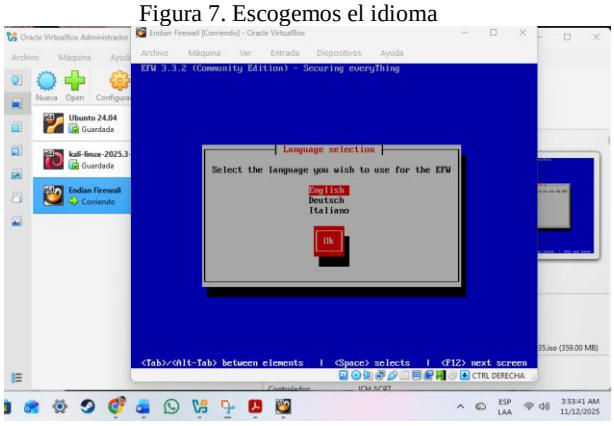
Figura 6. Iniciamos la máquina virtual de Endian



Fuente: Autoría propia (Carlos Choconta Campo)

Escogemos el idioma.

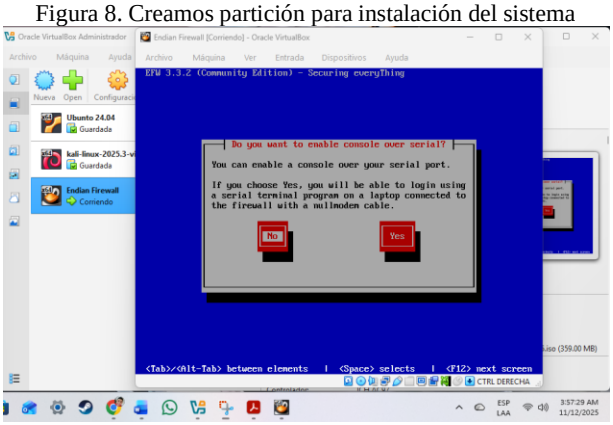
Figura 7. Escogemos el idioma



Fuente: Autoría propia (Carlos Choconta Campo)

Le damos yes para que cree una partición e instale el sistema.

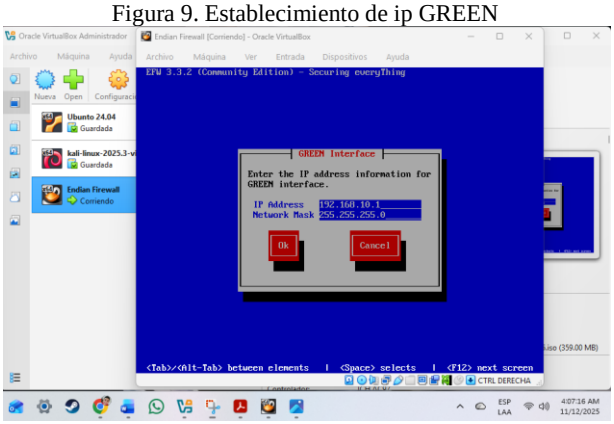
Figura 8. Creamos partición para instalación del sistema



Fuente: Autoría propia (Carlos Choconta Campo)

Establecemos la ip y la máscara de GREEN

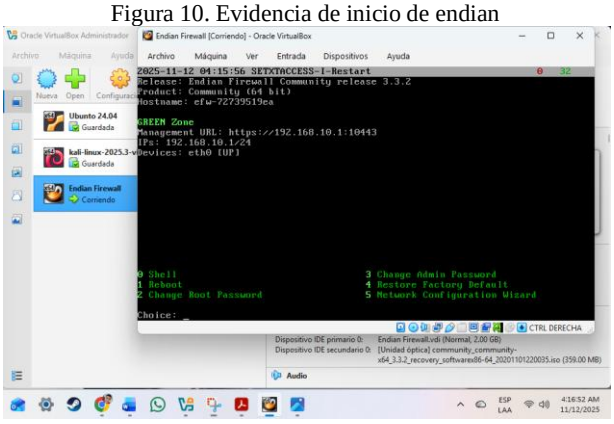
Figura 9. Establecimiento de ip GREEN



Fuente: Autoría propia (Carlos Choconta Campo)

De forma exitosa pudimos iniciar endian, donde nos muestra la ip de GREEN

Figura 10. Evidencia de inicio de endian

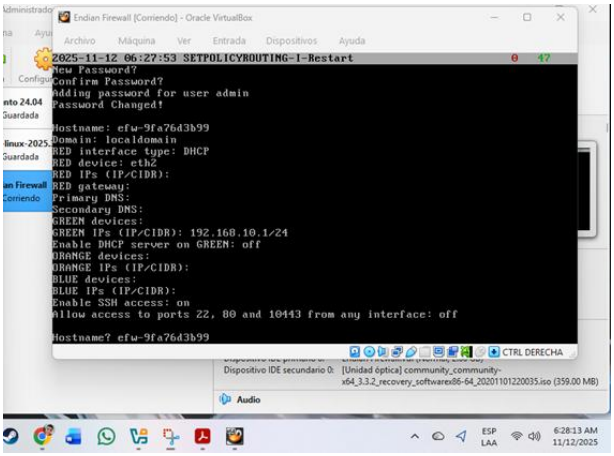


Fuente: Autoría propia (Carlos Choconta Campo)

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

El producto esperado es 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).

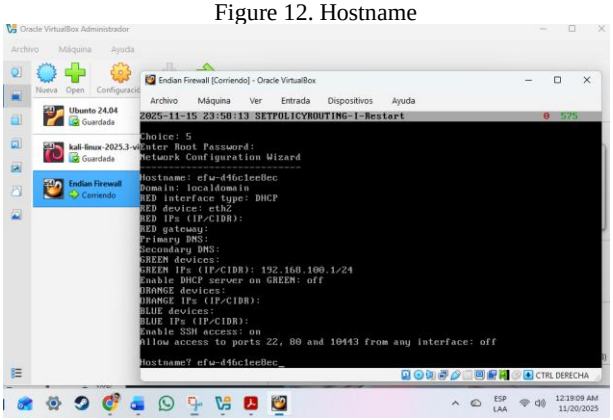
Figura 11. Zona Roja: Adaptador puente (WAN), Type: DHCP



Fuente: Autoría propia (Carlos Choconta Campo)

Desde Endian firewall configuramos Zona naranja: Servidores (DMZ) nos vamos a la opción 5 Network Configuration Wizard y seguimos los pasos para configurar.

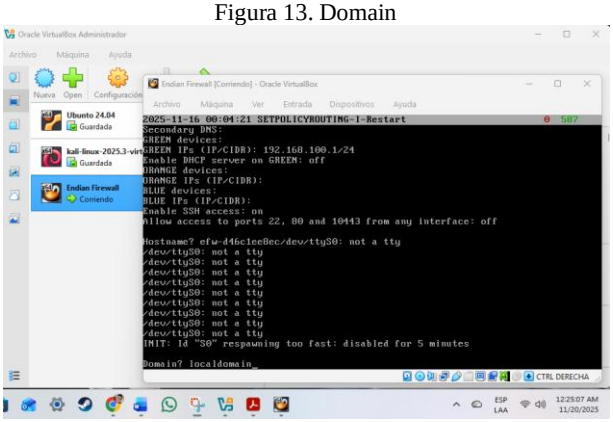
Figure 12. Hostname



Fuente: Autoría propia (Carlos Choconta)

Nos pedirá un Hostname podemos dejar el que se nos asigna por defecto o colocar el que nosotros queramos en este caso dejaremos el que se nos asigna por defecto.

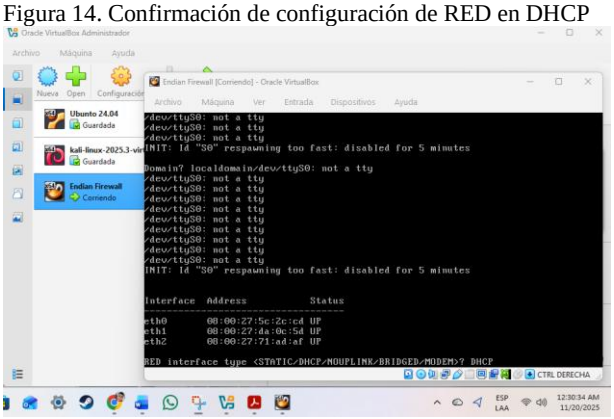
Figura 13. Domain



Fuente: Autoría propia (Carlos Choconta)

Después nos pedirá el nombre del dominio podemos colocar el que nosotros queramos o dejar el que nos da por defecto en este caso dejaremos el que nos da por defecto que es localdomain.

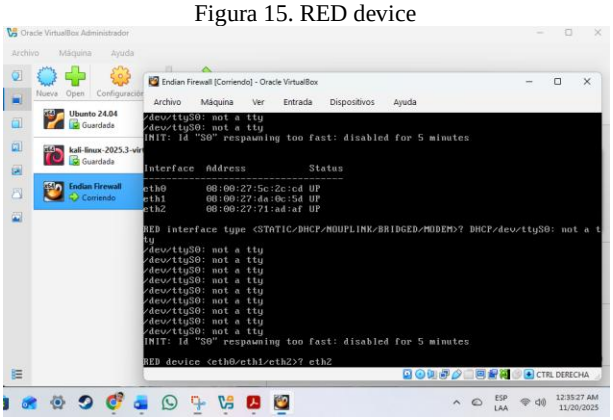
Figura 14. Confirmación de configuración de RED en DHCP



Fuente: Autoría propia (Carlos Choconta)

Confirmamos DHCP para RED.

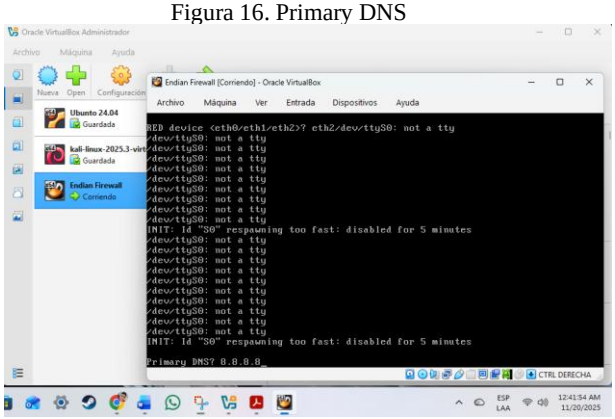
Figura 15. RED device



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pregunta que cual es el dispositivo rojo le damos enter ya que esta el eth2 por defecto eth2 es el dispositivo rojo.

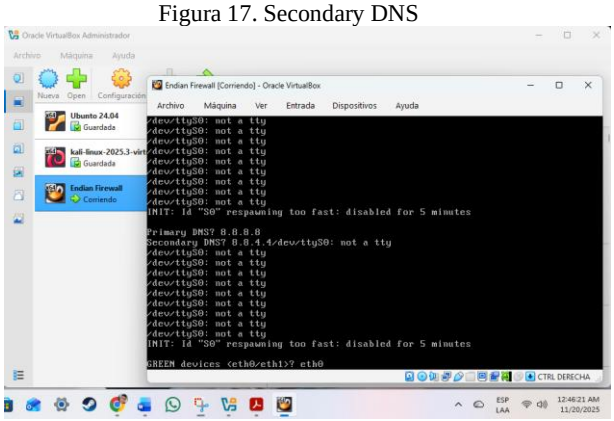
Figura 16. Primary DNS



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pide que cual es el DNS primario colocamos 8.8.8.8 y enter para confirmar

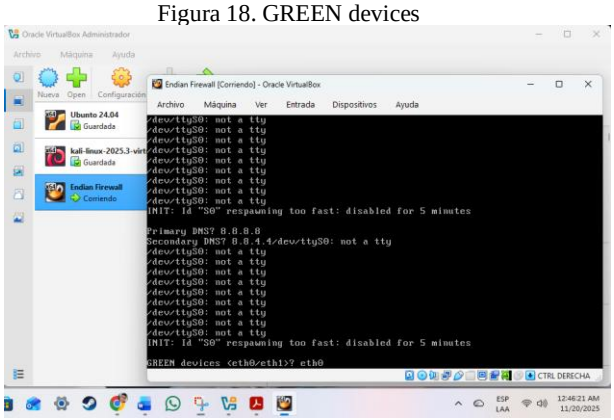
Figura 17. Secondary DNS



Fuente: Autoría propia (Carlos Choconta)

En DNS secundario colocamos 8.8.4.4 y enter para confirmar

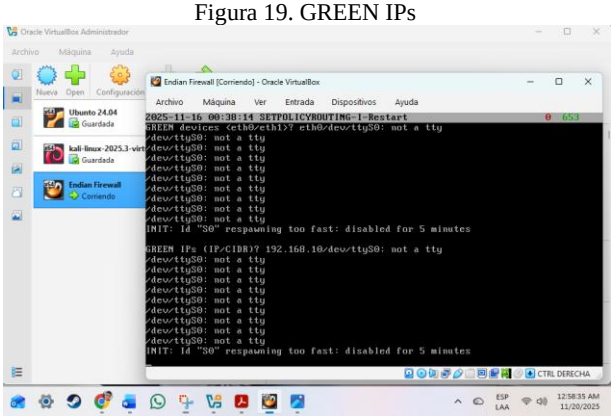
Figura 18. GREEN devices



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pregunta que cual es el dispositivo verde le decimos que es eth0 y enter para confirmar.

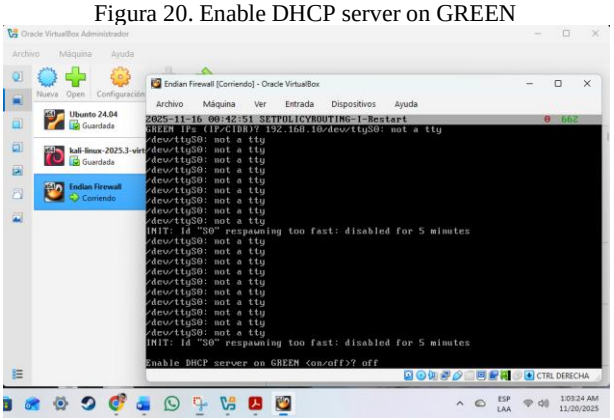
Figura 19. GREEN IPs



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pregunta para confirmar si la GREEN IPs es 192.168.10.1 le decimos que si precionando enter para confirmar.

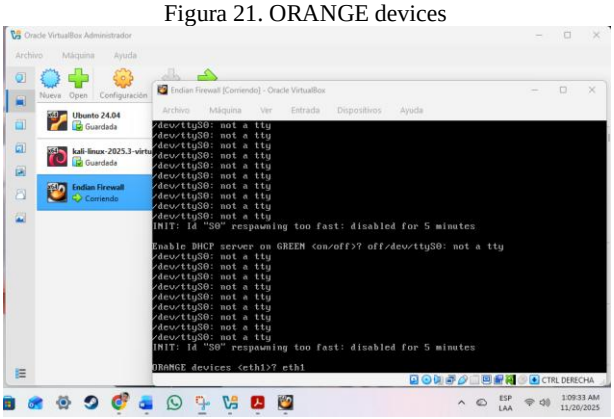
Figura 20. Enable DHCP server on GREEN



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pregunta que si habilitamos el servidor DHCP en la zona verde le damos enter ya que por defecto nos dice off.

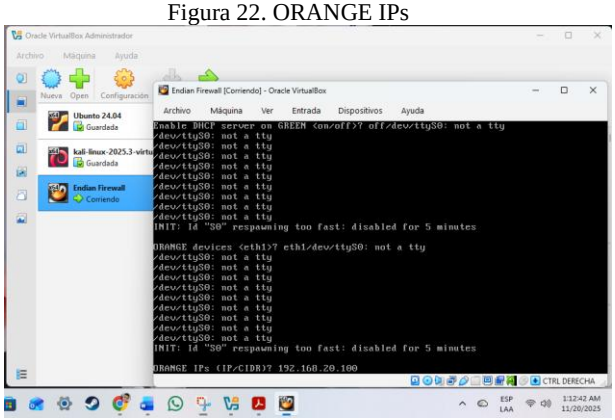
Figura 21. ORANGE devices



Fuente: Autoría propia (Carlos Choconta)

Aquí nos pregunta que cual es el dispositivo nananja le decimos que es eth1 y enter para confirmar.

Figura 22. ORANGE IPs



Fuente: Autoría propia (Carlos Choconta)

Finalmente nos pedira que cual IPs deseamos asignar a la zona naranja le ponemos 192.168.20.100 y le damos enter para confirmar y ya habremos configurado nuestra zona naranja de forma exitosa.

2.3 TEMÁTICA 2: CONFIGURACIÓN NAT

Configuración de las zonas NAT y DMZ con el fin de establecer la conexión a internet, mediante la implementación y creación de máquinas virtuales como Ubuntu, Ubuntu server y endian. Desde endian se configuran los puertos con el fin de realizar la configuración respectiva desde cada una de la otras maquinas para poder establecer la conexión.

Figura 23. configuración de puertos desde virtualBox

Fuente: Autoría propia (Yeny Buitrago)

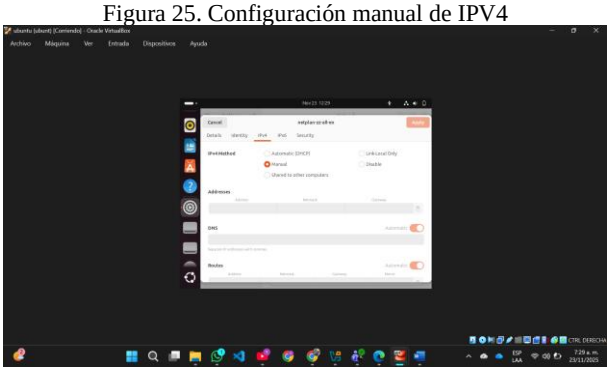
Al instalar la máquina virtual de server ubuntu, se debe realizar su respectiva configuración ya que es la máquina que se conecta en el puerto Green.

Figura 24. Configuración instalación server

Fuente: Autoría propia (Yeny Buitrago)

Se debe configurar desde la otra maquina la IPV4, de esta manera lograr la conexión.

Figura 25. Configuración manual de IPV4



Fuente: Autoría propia (Yeny Buitrago)

Mediante comandos permite validar la ip asignada.

Figura 26. Validación de ip

Fuente: Autoría propia (Yeny Buitrago)

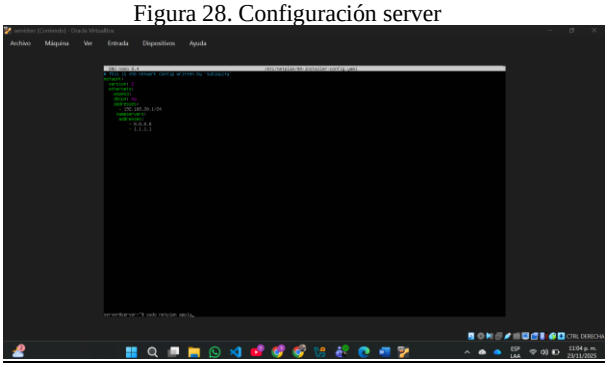
Desde el navegador mediante la ip se ingresa y validar que permita el acceso.

Figura 27. Validación de configuración

Fuente: Autoría propia (Yeny Buitrago)

Para la siguiente zona, se debe configurar desde otra maquina determinada Ubuntu server, mediante líneas de comandos se establece la ip designada a la zona.

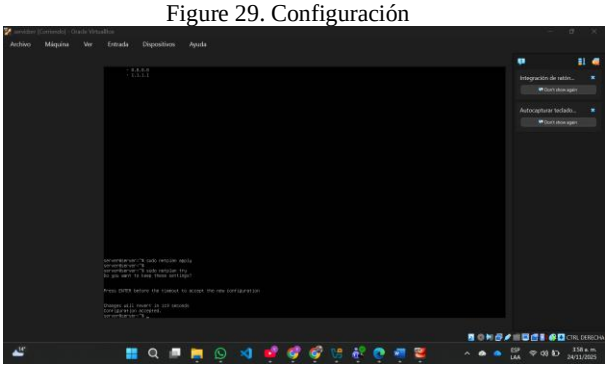
Figura 28. Configuración server



Fuente: Autoría propia (Yeny Buitrago)

Se debe agregar comandos para guardar los cambios para la red y validar que no presente inconveniente.

Figure 29. Configuración

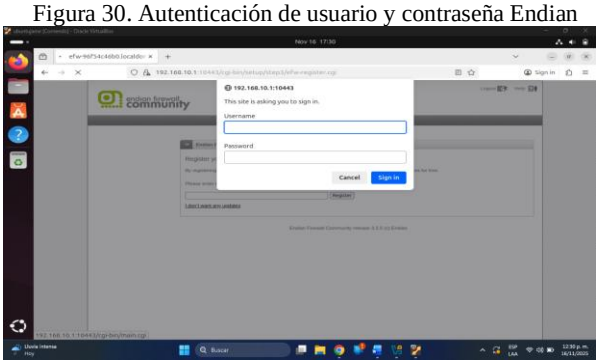


Fuente: Autoría propia (Yeny Buitrago)

2.4 TEMÁTICA 3: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED

El producto esperado es 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 debe verificar en el tráfico de salida la creación de las reglas de firewall implementadas.

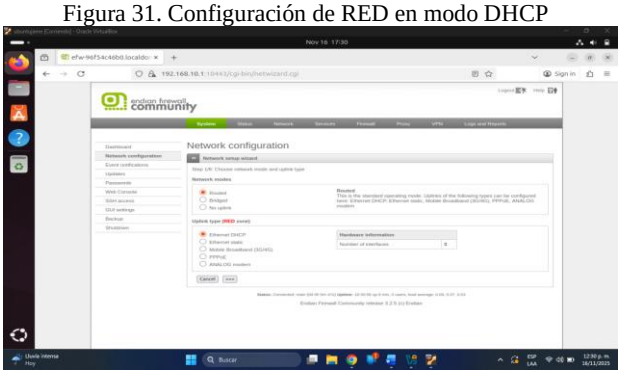
Figura 30. Autenticación de usuario y contraseña Endian



Fuente: Autoría propia (Jaime Rojas)

Desde desktop accedemos a Endian por medio de https://192.168.10.1:10443 y nos logueamos.

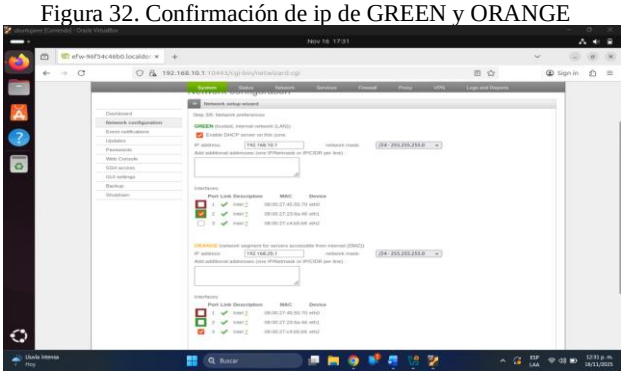
Figura 31. Configuración de RED en modo DHCP



Fuente: Autoría propia (Jaime Rojas)

Confirmamos la configuración de RED (WAN).

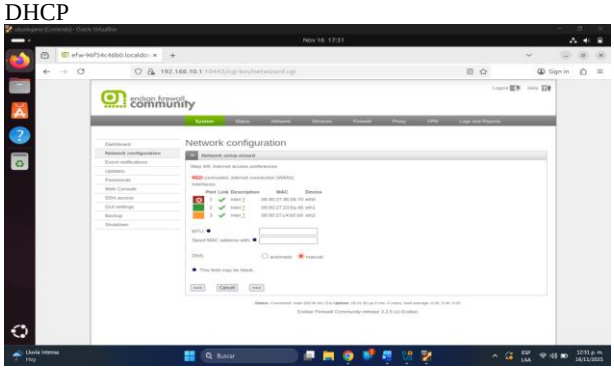
Figura 32. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia (Jaime Rojas)

Confirmamos la configuración de GREEN y ORANGE con sus respectivas ip.

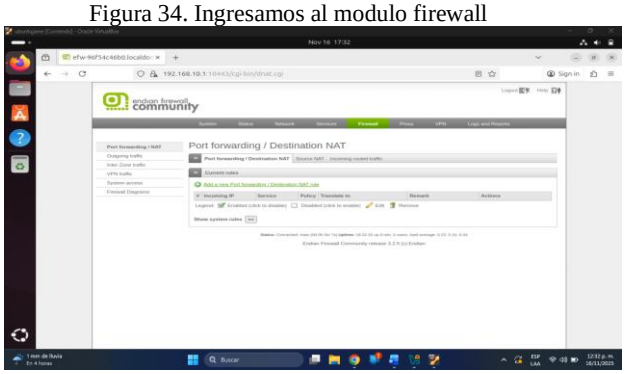
Figura 33. Confirmación de configuración de RED en DHCP



Fuente: Autoría propia (Jaime Rojas)

Confirmamos eth0 para RED.

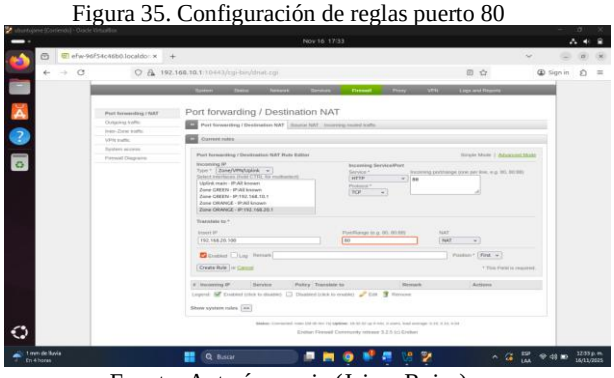
Figura 34. Ingresamos al modulo firewall



Fuente: Autoría propia (Jaime Rojas)

Nos dirigimos al modulo de firewall y le damos en botón de añadir una nueva regla.

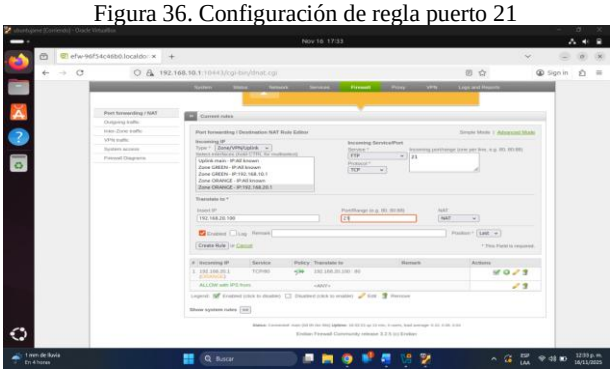
Figura 35. Configuración de reglas puerto 80



Fuente: Autoría propia (Jaime Rojas)

Configuración de port forwarding en Endian Firewall para permitir el tráfico HTTP (puerto 80) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

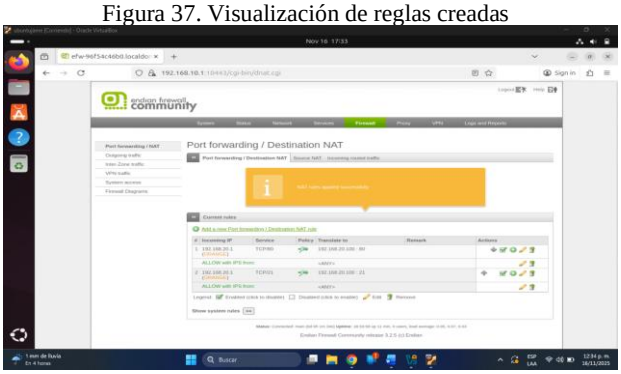
Figura 36. Configuración de regla puerto 21



Fuente: Autoría propia (Jaime Rojas)

Configuración de port forwarding para permitir el tráfico FTP (puerto 21) hacia el servidor Ubuntu en la zona DMZ con la IP 192.168.20.100.

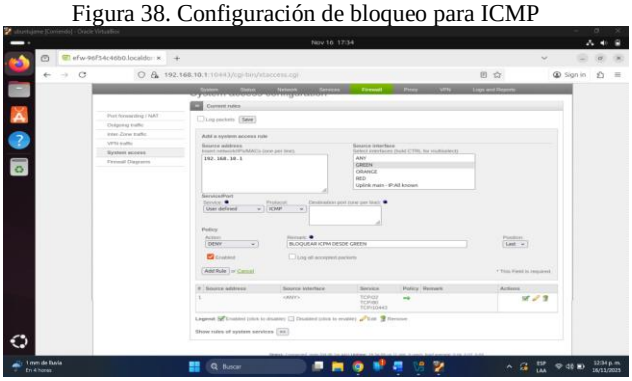
Figura 37. Visualización de reglas creadas



Fuente: Autoría propia (Jaime Rojas)

Reglas creadas correctamente.

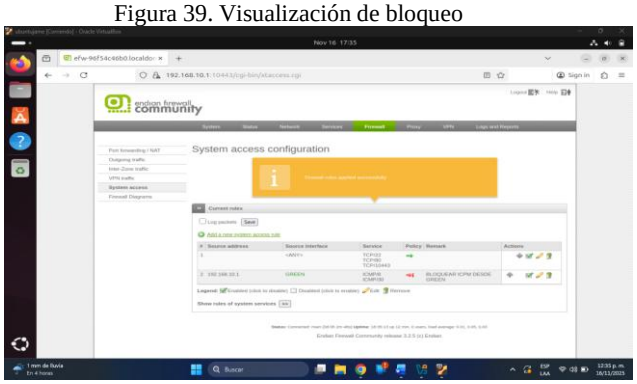
Figura 38. Configuración de bloqueo para ICMP



Fuente: Autoría propia (Jaime Rojas)

Regla de firewall en Endian Firewall para bloquear el tráfico ICMP desde la IP 192.168.10.1 en la interfaz GREEN (DMZ), con acción de denegar el tráfico. La regla está habilitada y aplicada.

Figura 39. Visualización de bloqueo



Fuente: Autoría propia (Jaime Rojas)

Bloqueo creado.

Figura 40. Actualización de paquetes en server

Fuente: Autoría propia (Jaime Rojas)

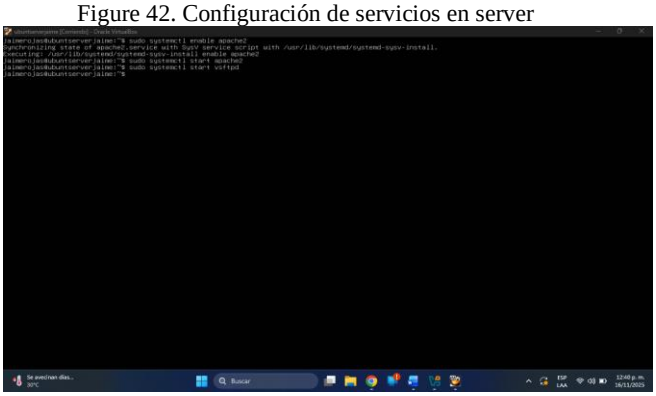
Se actualizan paquetes.

Figura 41. Instalación de apache y FTP en server

Fuente: Autoría propia (Jaime Rojas)

Instalación de Apache y FTP en Ubuntu Server

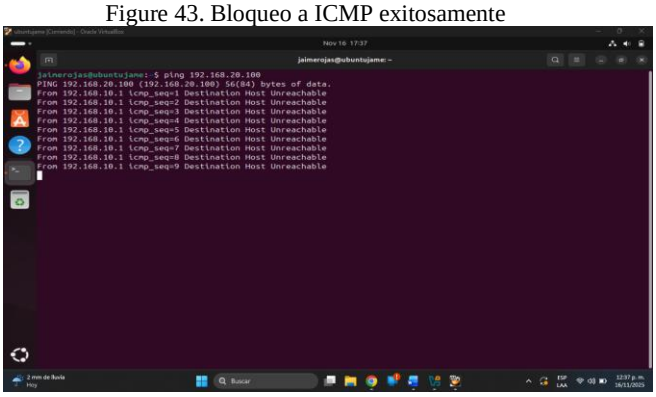
Figure 42. Configuración de servicios en server



Fuente: Autoría propia (Jaime Rojas)

Instalación de Apache y FTP en Ubuntu Server: Configuración de servicios HTTP y FTP.

Figure 43. Bloqueo a ICMP exitosamente



Fuente: Autoría propia (Jaime Rojas)

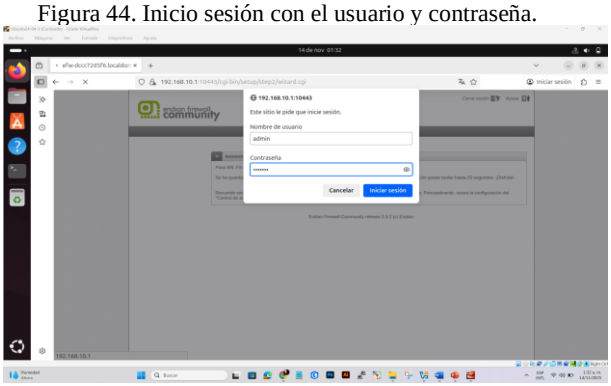
El ping a la dirección IP de la red DMZ está siendo bloqueado, mostrando "Destination Host Unreachable", lo que indica que la regla para bloquear ICMP está funcionando correctamente.

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

El objetivo final es desarrollar un perfil de seguridad que incluya una lista negra para restringir el acceso a los sitios web www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Posteriormente, se configurará un sistema de autenticación por usuario, donde se creará una cuenta específica, se asignará a un grupo determinado y se vinculó a una política de acceso asociada al perfil establecido. Para verificar el correcto funcionamiento, se realizan pruebas desde la red local (LAN) intentando acceder a las páginas bloqueadas mediante un navegador web.

En esta parte se muestra la interfaz de endian, se ingresa a la página proporcionando los campos de usuario y contraseña.

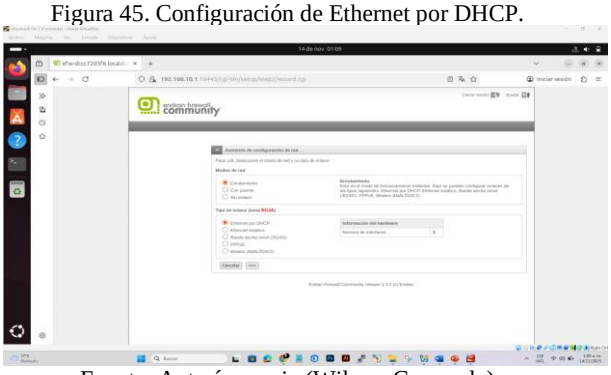
Figura 44. Inicio sesión con el usuario y contraseña.



Fuente: Autoría propia (Wilmar Coronado)

Se accede al apartado de configuración de red (Network Configuración) y se establecen los parámetros de la conexión RED en modo DHCP para asignación automática de direcciones IP.

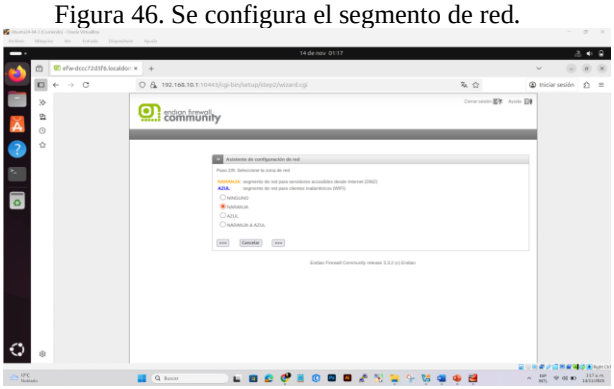
Figura 45. Configuración de Ethernet por DHCP.



Fuente: Autoría propia (Wilmar Coronado)

En esta parte, se procede a definir la configuración de red para las zonas del firewall. Se ha asignado el tipo ORANGE, correspondiente a la DMZ (Zona Desmilitarizada), con el fin de establecer un segmento de red accesible desde Internet y aislado de la red interna para mayor seguridad.

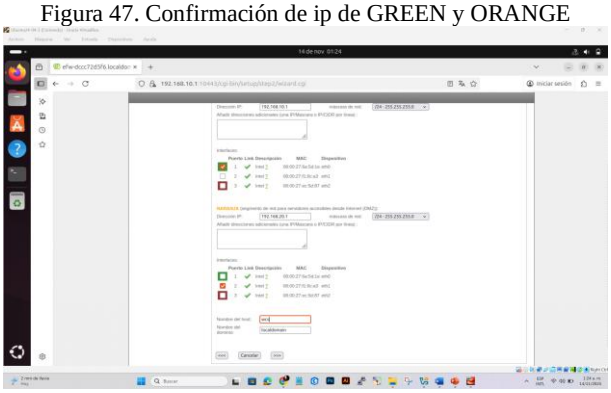
Figura 46. Se configura el segmento de red.



Fuente: Autoría propia (Wilmar Coronado)

Se verifican las direcciones IP asignadas a cada segmento: la red GREEN con la IP 192.168.10.1 y la red ORANGE con la IP 192.168.20.1, asegurando una correcta segmentación y conectividad según los parámetros de seguridad establecidos.

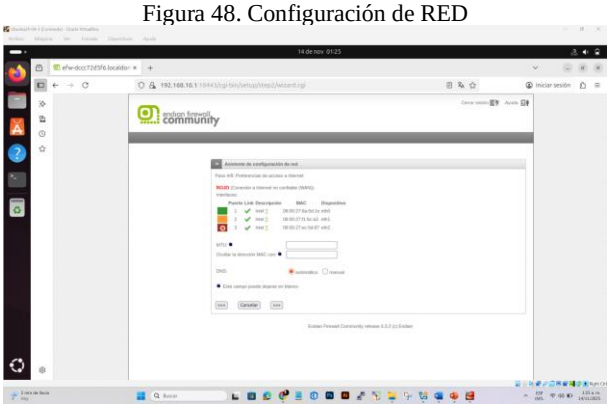
Figura 47. Confirmación de ip de GREEN y ORANGE



Fuente: Autoría propia (Wilmar Coronado)

De manera similar, se verifica que el segmento RED se encuentre configurado en modo DHCP, permitiendo la asignación automática de direcciones IP según los parámetros establecidos.

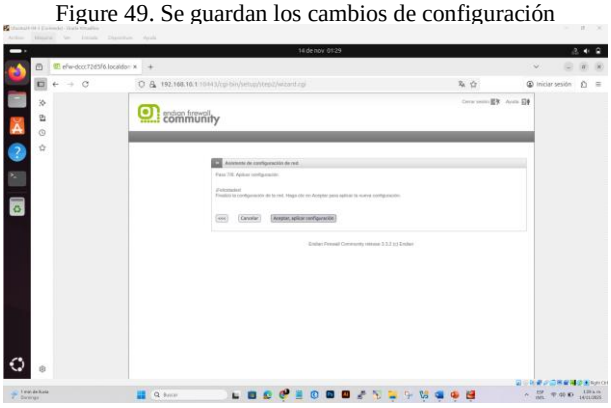
Figura 48. Configuración de RED



Fuente: Autoría propia (Wilmar Coronado)

En este punto, se aplican todas las configuraciones realizadas y se procede a guardar los cambios en el sistema.

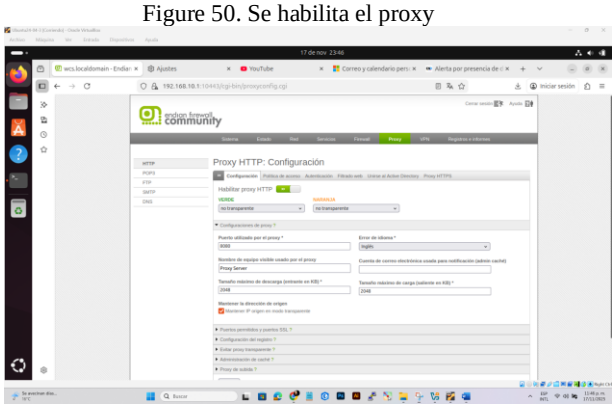
Figure 49. Se guardan los cambios de configuración



Fuente: Autoría propia (Wilmar Coronado)

Ingresamos al módulo Proxy, habilitamos dando clic en (Habilitar proxy HTTP), realizamos las configuraciones requeridas y damos guardar.

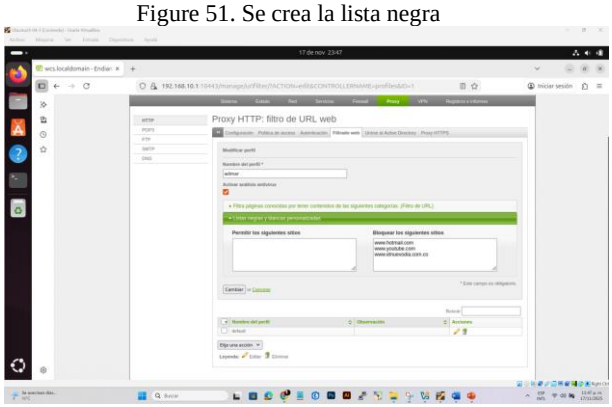
Figure 50. Se habilita el proxy



Fuente: Autoría propia (Wilmar Coronado)

En la pestaña (Filtrado web), creamos un perfil de filtrado, agregamos las páginas a bloquear a la lista negra y damos clic en añadir.

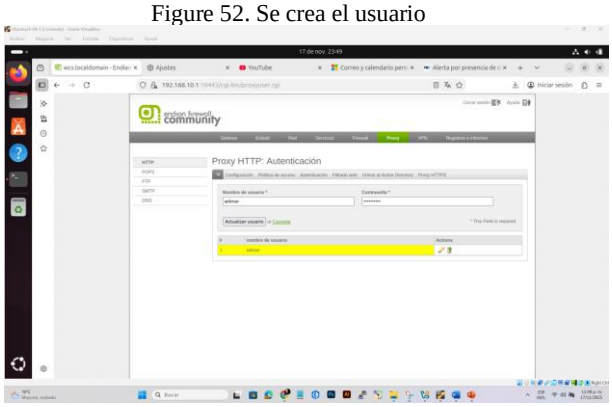
Figure 51. Se crea la lista negra



Fuente: Autoría propia (Wilmar Coronado)

En la pestaña (Autenticación), posterior en administrar usuarios y creamos uno nuevo “wilmar”.

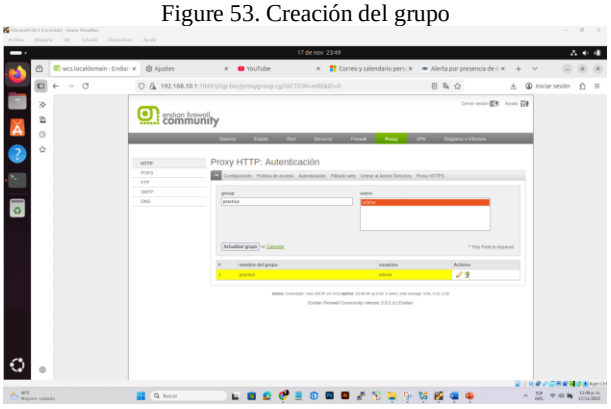
Figure 52. Se crea el usuario



Fuente: Autoría propia (Wilmar Coronado)

En la pestaña (Autenticación), posterior en administrar grupos, se crea un nuevo grupo de acceso llamado “practica” y se asigna el usuario “wilmar” como miembro de este, garantizando así los permisos de navegación y políticas de filtrado correspondientes.

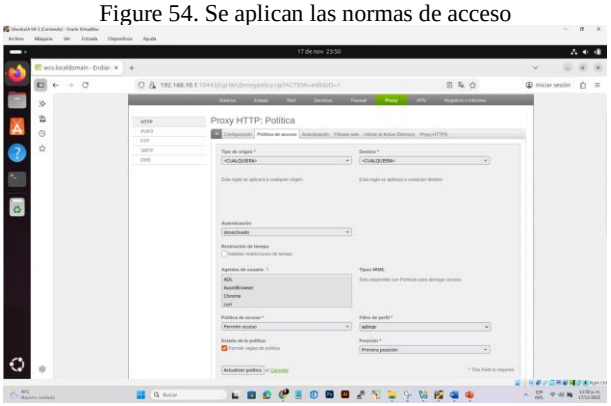
Figure 53. Creación del grupo



Fuente: Autoría propia (Wilmar Coronado)

En la pestaña (Política de acceso), en autenticación lo dejamos “desactivado” y le damos permitir acceso al usuario “wilmar” y damos clic en “Actualizar política”.

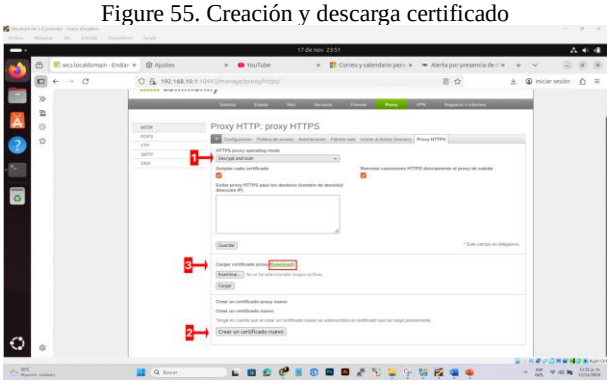
Figure 54. Se aplican las normas de acceso



Fuente: Autoría propia (Wilmar Coronado)

En la pestaña (Proxy HTTPS), desplegamos la opción “Decrypt and scan” le damos clic en “Crear un certificado” y posterior en “Dowload”.

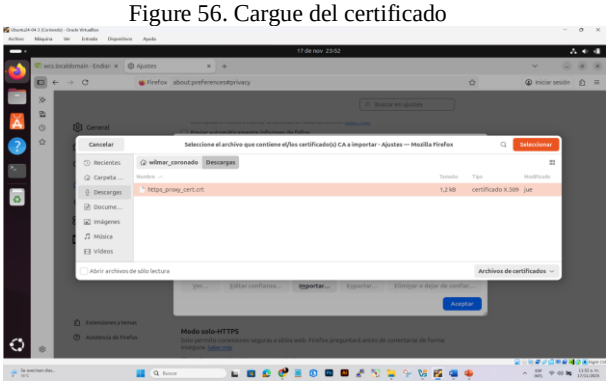
Figure 55. Creación y descarga certificado



Fuente: Autoría propia (Wilmar Coronado)

Después de descargar el certificado vamos al navegador Firefox, ingresamos por (Ajustes). (Privacidad & Seguridad). (Seguridad), (Ver certificados). (Importar). Lo seleccionamos, ubicado en (Descargas) y damos aceptar.

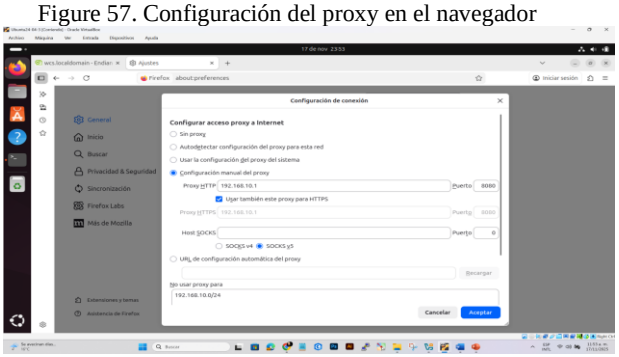
Figure 56. Cargue del certificado



Fuente: Autoría propia (Wilmar Coronado)

Se accedió a la configuración de proxy del navegador Firefox, donde se estableció manualmente la dirección IP 192.168.10.1 como servidor proxy para el tráfico HTTP. Además, se activó la opción para utilizar el mismo proxy en conexiones HTTPS, asegurando que todo el tráfico web pase por el servidor intermediario configurado.

Figure 57. Configuración del proxy en el navegador



Fuente: Autoría propia (Wilmar Coronado)

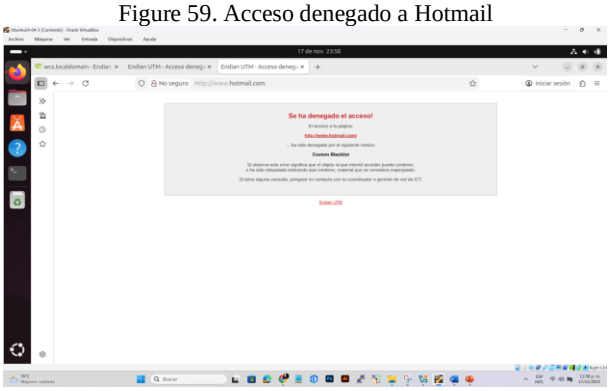
Al tratar de verificar el acceso a la página www.youtube.com aparece el mensaje previamente acceso denegado.

Figure 58. Acceso denegado a YouTube

Fuente: Autoría propia (Wilmar Coronado)

Al tratar de verificar el acceso a la página www.hotmail.com aparece el mensaje previamente acceso denegado.

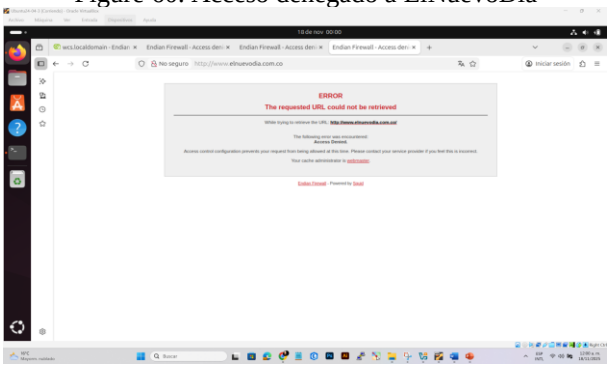
Figure 59. Acceso denegado a Hotmail



Fuente: Autoría propia (Wilmar Coronado)

Al tratar de verificar el acceso a la página www.elnuevodia.com.co aparece el mensaje previamente acceso denegado.

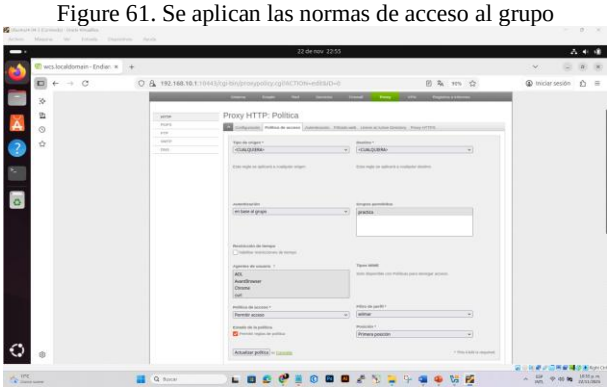
Figure 60. Acceso denegado a ElNuevoDia



Fuente: Autoría propia (Wilmar Coronado)

En el módulo Proxy ingresamos a la pestaña (Política de acceso), autenticamos en base al grupo creado (practica) y le damos permitir acceso al usuario (wilmar) y damos clic en (Actualizar política).

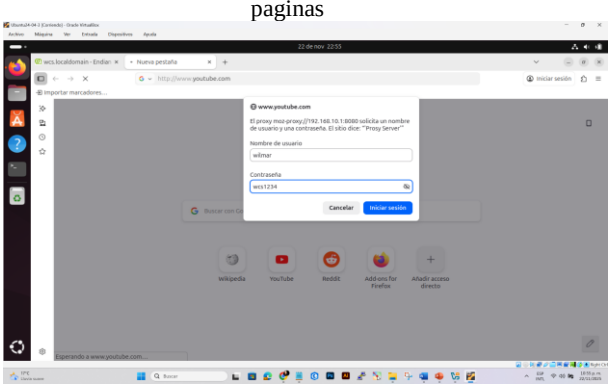
Figure 61. Se aplican las normas de acceso al grupo



Fuente: Autoría propia (Wilmar Coronado)

Despues de aplicar las politicas de acceso al grupo, vamos acceder a (www.youtube.com, www.hotmail.com y www.elnuevodia.comco) ingresamos el usuario y la contraseña y damos clic en (Iniciar sesión).

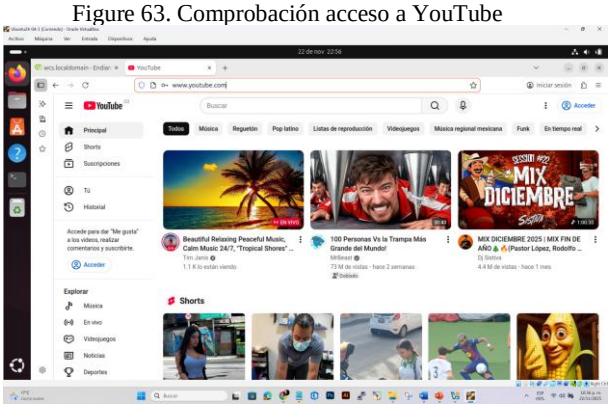
Figure 62. Acceso con usuario para la navegación a las paginas



Fuente: Autoría propia (Wilmar Coronado)

Una vez iniciado sesión, podemos verificar el acceso a las páginas web de (YouTube, hotmail y ElNuevoDia) que habíamos bloqueado.

Figure 63. Comprobación acceso a YouTube



Fuente: Autoría propia (Wilmar Coronado)

Figure 64. Comprobación acceso a Hotmail

Fuente: Autoría propia (Wilmar Coronado)

Figure 65. Comprobación acceso a ElNuevoDia

Fuente: Autoría propia (Wilmar Coronado)

3 CONCLUSIONES

La implementación de la instancia GNU/Linux Endian en el programa VirtualBox permite configurar de manera efectiva una arquitectura de red segmentada en tres zonas diferenciadas: verde, roja y naranja, estas zonas cumplen con los principios fundamentales de la seguridad perimetral, estableciendo barreras entre los diferentes niveles de confianza de la red. Además, la configuración de las interfaces de red y la asignación de direcciones IP privadas para cada una de las zonas ha resultado en la creación de un entorno controlado, lo que establece una base sólida para la protección de los servicios expuestos en la DMZ (zona desmilitarizada).

El objetivo fue configurar y verificar las reglas de NAT para permitir la comunicación de la LAN y la DMZ hacia Internet, habilitando servicios como HTTP y FTP desde la DMZ hacia la red interna. Además, se bloqueó el protocolo ICMP para evitar respuestas a ping y se comprobó que todas las reglas creadas aparecieran correctamente en el tráfico y en el reenvío de puertos. Asegurando una red funcional y controlada mediante la correcta gestión de permisos y restricciones.

Una de las configuraciones clave en este entorno fue la implementación de reglas de acceso para la zona DMZ, las cuales garantizan que únicamente los servicios necesarios, como HTTP y FTP, estén disponibles, este control estricto refuerza la seguridad del servidor web, que en este caso se ejecuta sobre Ubuntu Server. Además, se implementó una restricción en el protocolo ICMP para evitar la ejecución de comandos de diagnóstico, como el ping, lo cual reduce los vectores de reconocimiento utilizados por posibles atacantes, estas medidas, correctamente configuradas en Endian Firewall, destacan la importancia del control del tráfico en las redes perimetrales para la protección de la infraestructura.

La implementación de un proxy HTTP no transparente en la red segmentada mejora significativamente la seguridad y el control del tráfico web, esta solución permite bloquear el acceso a sitios específicos y gestionar de manera eficiente los recursos mediante políticas de acceso y autenticación. Asimismo, la integración de este proxy en entornos virtualizados, como VirtualBox, permite realizar pruebas en un entorno seguro, sin comprometer la infraestructura física. Además, la adecuada configuración de reglas NAT, zonas de confianza y servicios web refuerza la arquitectura de red, garantizando la seguridad perimetral y la protección de los servicios críticos.

4 REFERENCIAS

[1] D. Guzmán Arévalo, *Séptima Web académica etapa 7 DPL 16-04 2025*, 12 de noviembre de 2025. [En línea]. Disponible en: https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/daniel_guzman_unad_edu_co/EcFL2NIvmCNBgO7l50WpGIoBr4fkx6g5T_YWmltrNg1uUg?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D&e=AC6W53

[2] L. P. Learning, *LPIC-1 Exam 101 Version: 5.0*, 2025. [En línea]. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/

[3] J. Sanchez Giraldo, "VirtualBox con Endian 3.3.2, 3 Zonas: Verde, Naranjada y Roja," *YouTube*, 21 de noviembre de 2021. [En línea]. Disponible en: https://www.youtube.com/watch?v=Dvht5wCPIrI

[4] SOURCEFORGE, *Endian Firewall Community*. [En línea]. Disponible en: https://sourceforge.net/projects/efw/

[5] SuGE3K, "Diferencias entre un Firewall UTM y un NGFW," *YouTube*, 26 de octubre de 2016. [En línea]. Disponible en: https://www.youtube.com/watch?v=Uh1MeUaG_7s

[6] endian, *Endian UTM 3.2 Reference Manual*, 04 de octubre de 2016. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/index.html

[7] endian, *Getting Started*, 04 de octubre de 2016. [En línea]. Disponible en: https://docs.endian.com/3.2/utm/first.html#the-zones