CONFIGURACIÓN INTEGRAL DE ENDIAN FIREWALL EN VIRTUALBOX: SEGMENTACIÓN, NAT, REGLAS DE ACCESO Y PROXY

Ana María Gómez Oviedo
e-mail: amgomezov@unadvirtual.edu.co
Carlos Santiago Sierra Barrera
e-mail: cssierrab@unadvirtual.edu.co
Daniel Santiago Castellanos Cruz
e-mail: dscastellanosc@unadvirtual.edu.co
Gerardo Alexis Lemus Ramírez
e-mail: galemusr@unadvirtual.edu.co
Juan Camilo Chaves Hernandez
e-mail: jcchavesh@unadvirtual.edu.co

RESUMEN: *Este artículo presenta la implementación completa de un entorno de seguridad perimetral utilizando GNU/Linux Endian Firewall en VirtualBox, apoyado en las capacidades de estabilidad y seguridad del sistema operativo Linux (Free Software Foundation, 2024). Se configuraron las zonas Verde (LAN), Naranja (DMZ) y Roja (WAN), asignando tarjetas de red, direcciones IP y modos de conexión acordes con el diseño propuesto. Posteriormente, se desarrollaron configuraciones de traducción de direcciones (NAT), reglas de acceso entre zonas, publicación de servicios desde la DMZ y la implementación de un proxy HTTP no transparente con autenticación y filtrado de contenidos. Cada temática permitió validar conceptos fundamentales de segmentación de red, control de tráfico, seguridad por capas y administración de servicios. Los resultados muestran que es posible construir un entorno funcional que replica escenarios reales de protección perimetral, demostrando el comportamiento esperado de las reglas, la comunicación entre zonas y las restricciones aplicadas según los objetivos planteados.*

PALABRAS CLAVE: DMZ, Endian Firewall, NAT, Seguridad Perimetral, Virtualización

1 INTRODUCCIÓN

La seguridad perimetral es un elemento esencial en la administración de redes, ya que permite controlar el tráfico, aplicar políticas y proteger los recursos de una organización. En este sentido, un firewall se define como “a device or program that controls the flow of network traffic between networks or hosts that employ differing security postures” (Scarfone & Hoffman, 2009, p. 43). En este trabajo se implementó un entorno de firewall y segmentación utilizando GNU/Linux Endian en VirtualBox, con el objetivo de comprender cómo se configuran y administran las distintas zonas de seguridad en un sistema real.

Este proyecto se desarrolla en el contexto de los conocimientos de Linux LPI, que abarcan la administración básica del sistema, la gestión de servicios y las configuraciones de red necesarias para operar soluciones de seguridad basadas en Linux. Cada integrante del equipo abordó una temática especifica, incluyendo instalación del firewall, reglas de NAT, publicación de servicios en la DMZ, control de acceso entre zonas y configuración de un proxy HTTP con autenticación. Estos fundamentos permiten entender el comportamiento interno del sistema y facilitan la configuración de soluciones de seguridad basadas en Linux, ampliamente utilizadas en entornos profesionales debido a su estabilidad y flexibilidad, aspectos que se explican posteriormente.

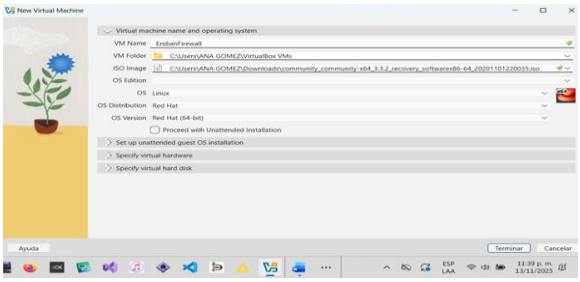
El propósito del artículo es documentar de forma clara las configuraciones realizadas y evidenciar el funcionamiento de los distintos mecanismos de seguridad aplicados demostrando su funcionamiento mediante diferentes verificaciones prácticas, de esta manera, se busca consolidar e integrar teórica y práctica para reforzar las competencias de administración y protección de redes además de aplicar los diversos conceptos que se han desarrollado a lo largo del desarrollo del curso.

2 TEMÁTICA 1: CONFIGURACIÓN DE LA INSTANCIA ENDIAN EN VIRTUALBOX

2.1 CONFIGURACIÓN INICIAL DE LA MÁQUINA VIRTUAL

Para la implementación del firewall se creó una nueva máquina virtual en Oracle VirtualBox utilizando como sistema operativo Linux y la distribución Red Hat. Se cargó la ISO de Endian Firewall 3.3 y se asignaron 2000 MB de memoria RAM, 16 MB de video y el controlador gráfico VMSVGA.

Figura 1. Creación de la máquina virtual Endian



Fuente: Autoría Propia

Se muestra la máquina virtual configurada en VirtualBox con la ISO de Endian Firewall.

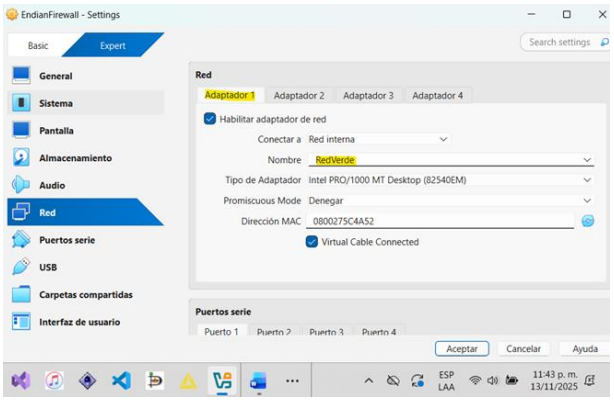
2.2 CONFIGURACIÓN DE LOS ADAPTADORES DE RED

Se configuraron tres tarjetas de red para representar las zonas del firewall:

- **Zona Verde (LAN):** Red interna con nombre *RedVerde*.
- **Zona Naranja (DMZ):** Red interna con nombre *RedNaranja*.
- **Zona Roja (WAN):** Modo NAT para salida a Internet.

Todas las tarjetas se configuraron con modelo Intel PRO/1000 MT Desktop.

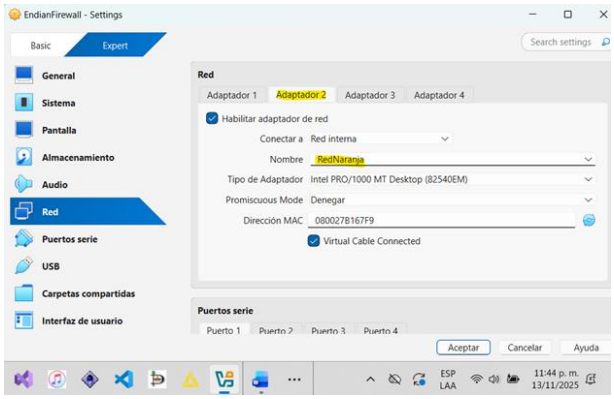
Figura 2. Adaptador de la Zona Verde



Fuente: Autoría Propia

Se observa la configuración del adaptador de red asignado a la Zona Verde mediante una red interna llamada *RedVerde*.

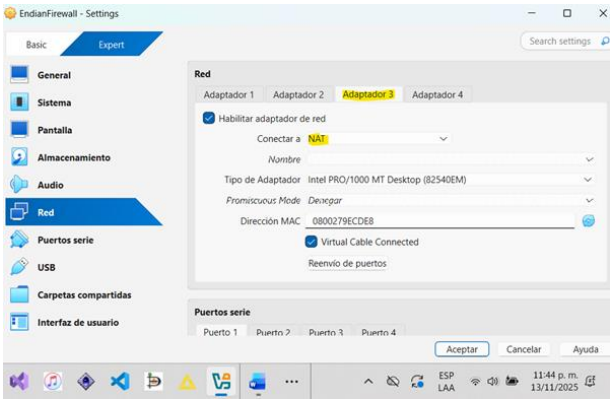
Figura 3. Adaptador de la Zona Naranja



Fuente: Autoría Propia

Se visualiza la asignación del adaptador de red correspondiente a la Zona Naranja, configurado como red interna *RedNaranja*.

Figura 4. Adaptador de la Zona Roja



Fuente: Autoría Propia

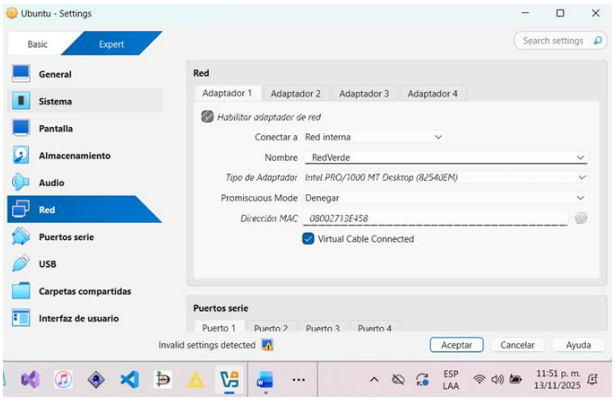
Se presenta la configuración del adaptador de la Zona Roja, definido en modo NAT para permitir acceso a Internet.

2.3 CONFIGURACIÓN DE LAS MÁQUINAS CONECTADAS AL FIREWALL

Se utilizaron dos máquinas virtuales adicionales:

- **Ubuntu Desktop:** conectada a *RedVerde*.
- **Ubuntu Server:** conectada a *RedNaranja*.

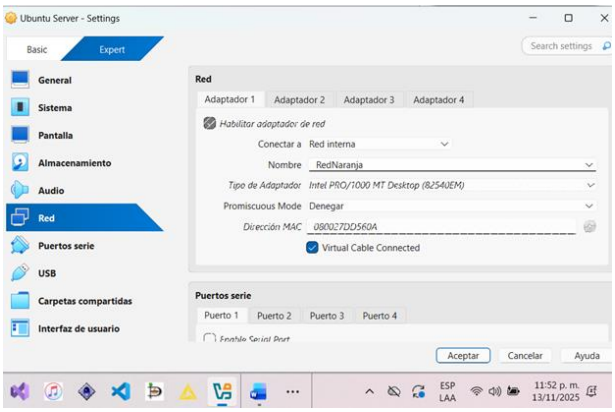
Figura 5. Configuración de red en Ubuntu Desktop



Fuente: Autoría Propia

Configuración de la interfaz de red del Ubuntu Desktop conectado a la Zona Verde del firewall.

Figura 6. Configuración de red en Ubuntu Server



Fuente: Autoría Propia

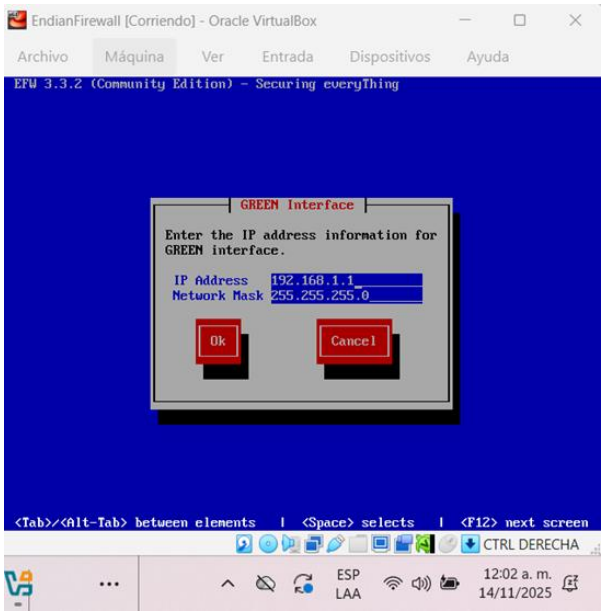
Vista de la configuración de red del Ubuntu Server conectado a la Zona Naranja del firewall.

2.4 PROCESO DE INSTALACIÓN DE ENDIAN

Se inició la instalación desde la ISO, seleccionando idioma, confirmando pasos del instalador y configurando las zonas del firewall:

- **Zona Verde:** 192.168.1.1/24
- **Zona Naranja:** 10.0.0.1/24
- **Zona Roja:** DHCP (Internet)

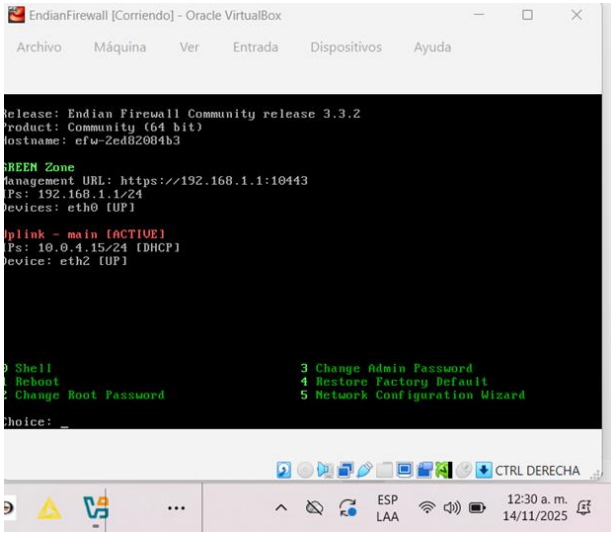
Figura 7. Configuración de la interfaz Green (Zona Verde)



Fuente: Autoría Propia

Se muestra la asignación de la dirección IP 192.168.1.1 a la interfaz Green durante la instalación de Endian.

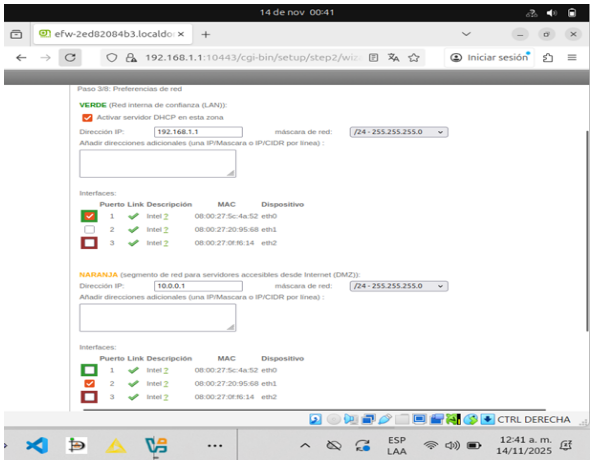
Figura 8. Visualización automática del estado de interfaces



Fuente: Autoría Propia

Pantalla de estado donde Endian muestra automáticamente las interfaces configuradas.

Figura 9. Configuración final de las zonas Verde y Naranja



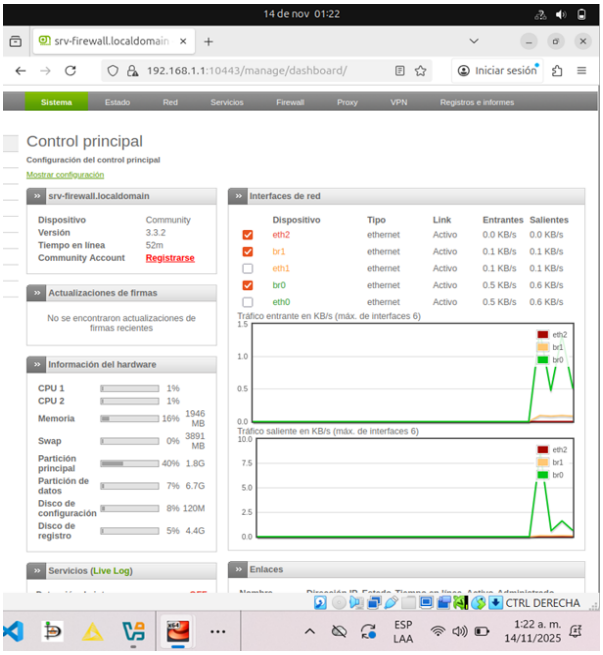
Fuente: Autoría Propia

Vista del resumen final de configuración de las zonas Green y Orange al finalizar la instalación.

2.5 ACCESO AL FIREWALL

Se realizaron pruebas de ping entre las máquinas y el firewall, confirmando la comunicación en las tres zonas. También se accedió a la interfaz web desde Ubuntu Desktop mediante https://192.168.1.1.

Figura 10. Inicio de sesión en la interfaz web de Endian



Fuente: Autoría Propia

Acceso a la consola web del firewall desde el navegador de Ubuntu Desktop.

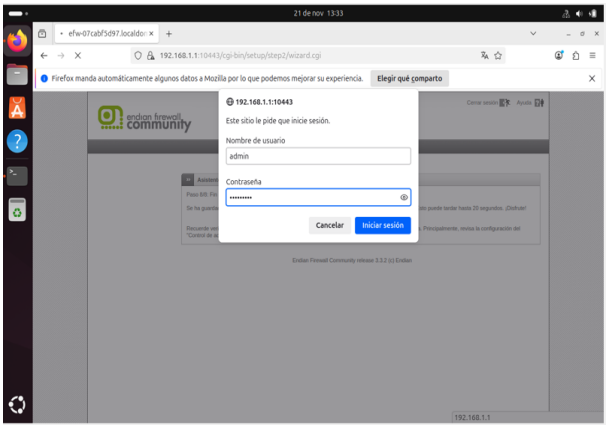
2.6 RESULTADOS DE LA CONFIGURACIÓN DEL FIREWALL

La configuración de Endian permitió establecer de manera correcta la segmentación de red entre las zonas Verde, Roja y Naranja. Las pruebas de conectividad mostraron un funcionamiento adecuado de la red, el firewall y el enrutamiento interno, permitiendo continuar con las temáticas siguientes.

3 TEMÁTICA 2: CONFIGURACIÓN DE NAT

Para habilitar el acceso a Internet desde la red local, se realizó la siguiente configuración mediante la interfaz web de administración del Endian Firewall: desde el Ubuntu Desktop (192.168.1.2/24), se ingresó al portal web de firewall mediante, https://192.168.1.1:10443 utilizando las credenciales de administrador, en este caso para el usuario "admin" y la contraseña que se cambió por "123456789"

Figura 11. Ingreso al portal web de Endian



Fuente: Autoría Propia

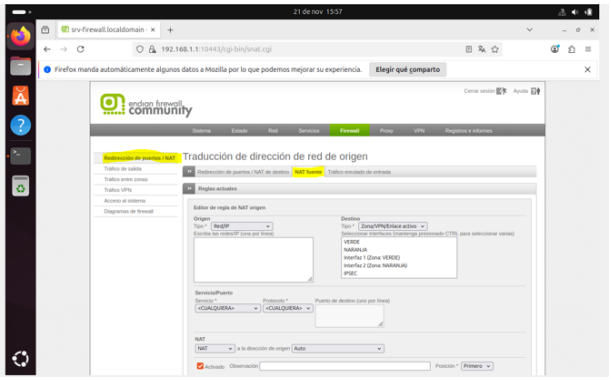
Ingreso al portal web Endian para la validación de los servicios y configuración de las reglas.

Desde el panel web de administración del Endian Firewall, se navega hasta el módulo NAT seleccionando Firewall > NAT > Source NAT (SNAT). Allí, se crea una nueva regla configurando los siguientes parámetros:

- **Source Type**: Network/IP (red 192.168.1.0/24 - Verde/LAN)
- **Destination Type**: Zone/VPN/Uplink (interfaz Uplink principal –RED)
- **NAT Action**: Auto (*Masquerading)*
- **Position**: First
- **Remark**: "NAT de red interna a internet"

Finalmente, se guarda la regla haciendo clic en *Add a new source NAT rule*, luego en *create Rule* y aplica cambios seleccionando *Apply*.

Figura 12. Ingreso al módulo firewall para configuración NAT

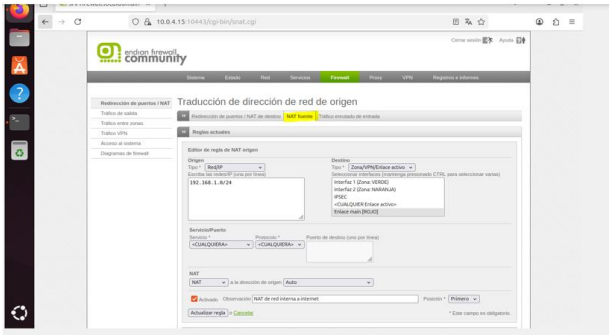


Fuente: Autoría Propia

Ingreso al módulo de firewall para la creación de las reglas NAT, en este caso se va a crear la regla LAN

Se procede a configurar y crear la regla para la zona Verde (LAN) dentro del formulario que se abre en la opción de crear nueva regla en la opción *Add a new source NAT*

Figura 13. Creación de la nueva regla NAT –Zona Verde

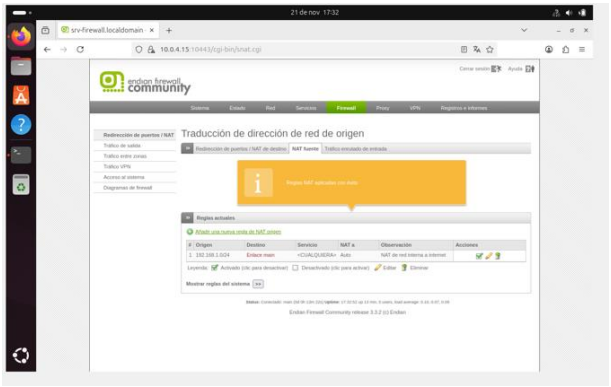


Fuente: Autoría Propia

Vista del módulo donde se realizan las configuraciones para la creación de la regla.

Luego de aplicar la regla se muestra la regla ya activa dentro del panel de la opción de Source NAT, en donde se puede visualizar la regla creada y configurada

Figura 14. Verificación de la regla creada y activa

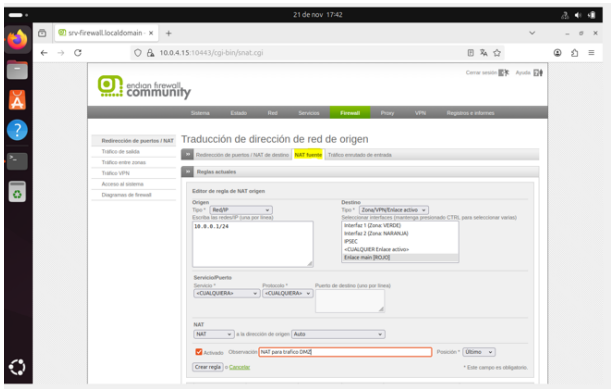


Fuente: Autoría Propia

Verificación de la regla creada, aquí se verifica si quedo creada y activa.

Luego dentro de la misma interfaz se agregó una regla adicional para la DMZ con los siguientes parámetros: en el campo Source, se seleccionó Network/IP con la dirección (10.0.0.1/24), correspondiente a la zona Naranja/DMZ. En Destination, se eligió Uplink main (Red).la acción NAT se estableció en Auto (masquerading). Además, la regla se posiciono como Last en la tabla para garantizar la prioridad del tráfico LAN. En el campo Remark, se añadió la nota "NAT para tráfico DMZ". Finalmente, se aplican los pasos para activar la regla: sé pulso en *Add a new source NAT rule*, luego en *Create Rule* y, por último, en *Apply*

Figura 15. Creación de la nueva regla NAT – Zona Naranja



Fuente: Autoría Propia

Creación de la segunda regla NAT, esta vez para la zona naranja.

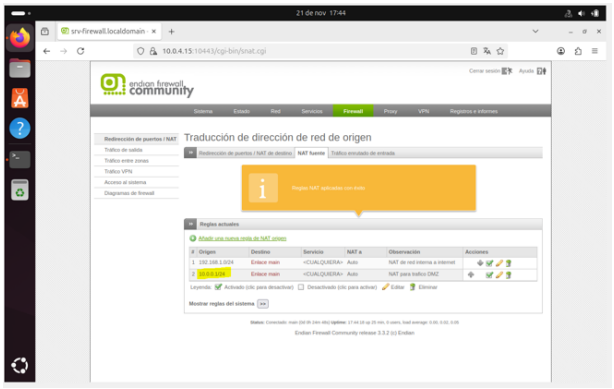
De manera similar a lo ocurrido con la regla aplicada en la zona verde, al finalizar la configuración, se puede verificar que la nueva regla esta activa en el panel de la opción Source NAT. En este panel, es posible visualizar todas las reglas creadas y configuradas.

Es importante tener en cuenta que la correcta priorización de las reglas NAT es fundamental para el correcto funcionamiento del sistema. la regla asociada a la LAN, ubicada

en posición *FIRST*, tiene mayor precedencia que la regla de la DMZ, situada en la posición *Last*. Además, el mecanismo de Masquerading automático utiliza la dirección IP publica asignada dinámicamente a la interfaz WAN (eth2).

Por último, cabe destacar que todos los cambios de configuración deben confirmarse mediante el botón *Apply* para que tengan efecto de manera definitiva en el firewall

Figura 16. Verificación de las reglas NAT configuradas



Fuente: Autoría Propia

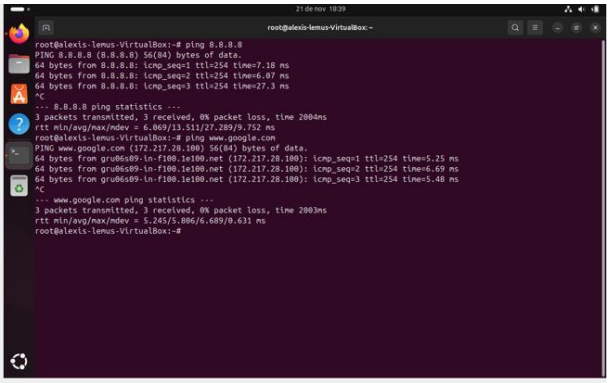
Validación de la regla creada, se identifica si queda activa y funcionando.

3.1 RESULTADOS Y VALIDACIÓN

Con el propósito de verificar la correcta implementación de las reglas NAT y la política de seguridad en el entorno de red configurado con Endian Firewall, se llevaron a cabo diversas pruebas de conectividad y acceso entre las zonas LAN, DMZ y WAN. Estas evaluaciones permitieron comprobar el cumplimiento de los objetivos establecidos, tales como la conectividad segura, el aislamiento adecuado de las zonas y la funcionalidad eficiente del reenvió de puertos.

Prueba de conectividad desde la LAN hacia internet: Se realizaron pruebas desde un equipo Ubuntu Desktop (192.168.1.2), se ejecutaron comandos ping hacia la dirección IP publica 8.8.8.8 y se realizaron consultas DNS a www.google.com. Los resultados confirmaron que el tráfico salía correctamente a través del firewall, asegurando una conectividad efectiva y segura hacia internet.

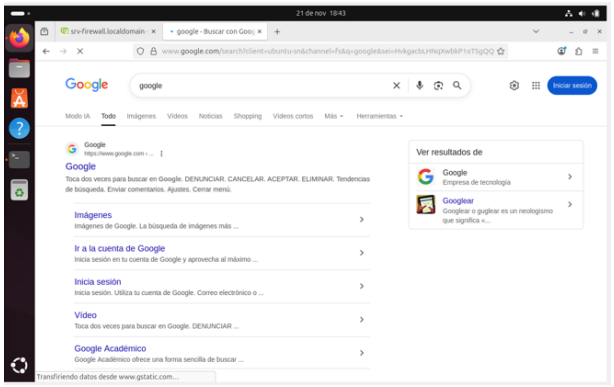
Figura 17. Prueba de conectividad desde la LAN



Fuente: Autoría Propia

Se realiza la prueba de conectividad desde la LAN, se valida que la regla se encuentre funcionado.

Figura 18. Prueba de acceso a Internet

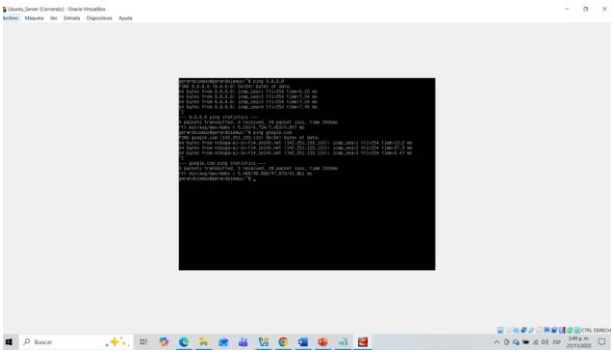


Fuente: Autoría Propia

Se realiza una segunda prueba esta vez ingresando a Internet para validar el acceso y funcionalidad de la regla creada

Prueba de conectividad desde la DMZ hacia internet: Desde el servidor Ubuntu ubicado en la zona Naranja (DMZ), se realizaron pruebas de conectividad utilizando comandos de ping hacia la dirección IP 8.8.8.8 y el dominio google.com. Estos testeos confirmaron la capacidad de acceso a internet y la adecuada resolución de nombres DNS, asegurando que las reglas del firewall permiten la comunicación saliente desde la DMZ hacia la red externa.

Figura 19. Prueba de conectividad desde la WAN a DMZ

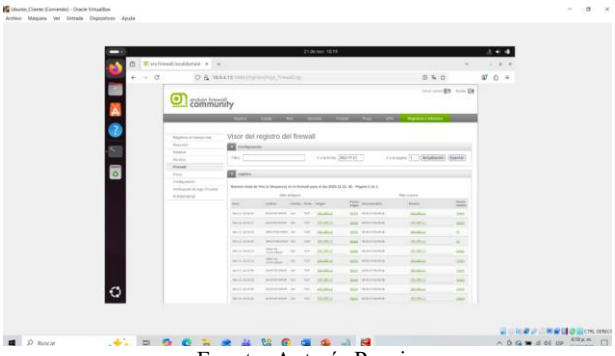


Fuente: Autoría Propia

Se realiza la prueba de conectividad y funcionalidad de la segunda regla NAT creada, desde la WAN a DMZ.

Pruebas de NAT y redirección de puertos (DNAT): Desde una red externa simulada en VirtualBox, se realizaron intentos de acceso al servidor web ubicado en la zona DMZ utilizando la dirección IP publica asignada a la interfaz WAN del firewall (10.0.0.4). las solicitudes provenientes desde esta red fueron correctamente redirigidas hacia el servidor interno, confirmando la correcta configuración de las reglas de DNAT. Además, se verificó la disponibilidad del servicio desde el exterior, permitiendo el tráfico en los puertos 80 y 443 en el servidor DMZ(10.0.0.1). Estos resultados validan la afectividad de la implementación y el funcionamiento adecuado de la redirección de puertos y reglas de NAT en el firewall.

Figura 20. Validación de tráfico por los puertos y redireccionamiento de estos



Fuente: Autoría Propia

Se realiza la validación de trafico de puertos y redireccionamiento de estos para la validación de las reglas creadas anteriormente.

La configuración de Endian Firewall, que incluye reglas de NAT y enmascaramiento de direcciones, ha establecido una red segura, eficiente y bien segmentada entre las zonas LAN, DMZ y WAN. Se han implementado políticas de filtrado de tráfico precisas que permiten un acceso controlado tanto a los servicios internos como a los públicos, garantizando una segmentación adecuada y protección contra accesos no autorizados.

Las pruebas de conectividad realizadas validaron que la red funciona según lo previsto, confirmando que los servicios son accesibles conforme a las reglas establecidas, al mismo tiempo que se mantienen estrictos controles de seguridad perimetral, contribuyendo a una infraestructura robusta y confiable.

4 TEMÁTICA 3: PUBLICACIÓN DE SERVICIOS EN LA DMZ

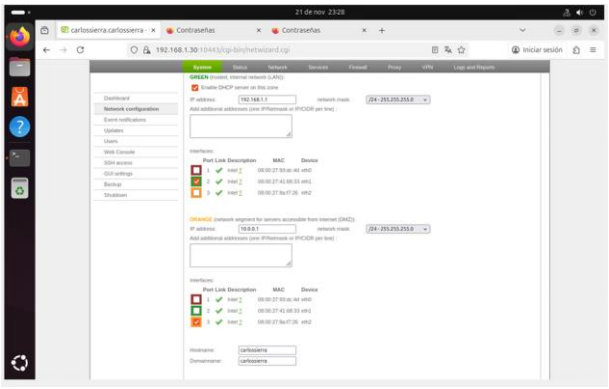
Para llevar a cabo la publicación o exposición de servicios a Internet utilizando la plataforma Endian, es fundamental comprender y establecer correctamente el esquema de direccionamiento de las diferentes zonas de seguridad. El firewall Endian gestiona el tráfico basándose en tres interfaces principales: la **Zona Verde** (red interna o LAN), la **Zona Roja** (Internet o WAN), y la crucial **Zona Naranja** o DMZ (Zona Desmilitarizada). Es necesario tener definido el direccionamiento IP de cada una de estas zonas antes de proceder con la configuración de reglas de tráfico.

4.1 PERMITIR SERVICIOS HTTP Y FTP

Ahora se permitirá la publicación de servicios HTTP y FTP desde el servidor Ubuntu (DMZ) hacia la zona *green* que es donde actualmente se tiene el equipo de escritorio ubuntu.

Para ello, se ingresa a la consola del firewall Endian por medio del navegador de un equipo de escritorio Ubuntu y posteriormente se verifica el apartado *System/Network configuration* y se valida que los direccionamientos de la zona *green, orange* y *red* estén configurados de manera correcta.

Figura 21. Validación de direccionamientos de las zonas *green, red, orange*.

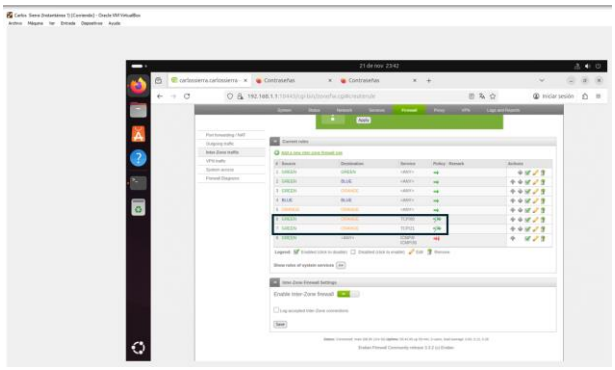


Fuente: Autoría Propia

Luego de validar las zonas, se procede a configurar la habilitación de servicios HTTP mediante el puerto 80 y FTP puerto 21, para ello se procede a verificar la consola de Endian y en el apartado de *Firewall/Inter-Zone traffic* y se selecciona *Add a new inter-zone* y se crea la política de habilitación de

tráfico mediante los protocolos mencionados anteriormente, si quedó configurado de manera correcta, se debería ver las reglas de la siguiente manera.

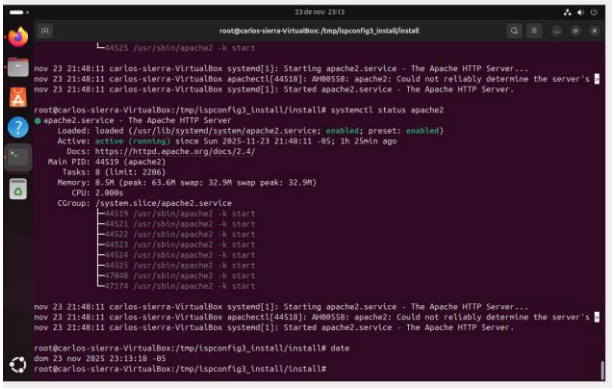
Figura 22. Configuración de tráfico entre zonas.



Fuente: Autoría Propia

Posteriormente se valida que el *server* tenga habilitado el servicio apache.

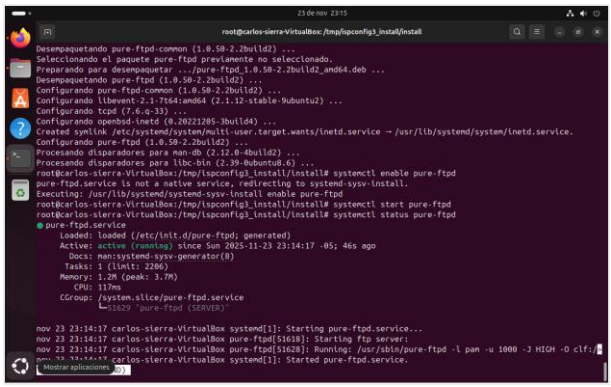
Figura 23. Verificación del estado del servicio HTTP.



Fuente: Autoría Propia

Se puede evidenciar el estado del servicio HTTP y su correcta funcionalidad.

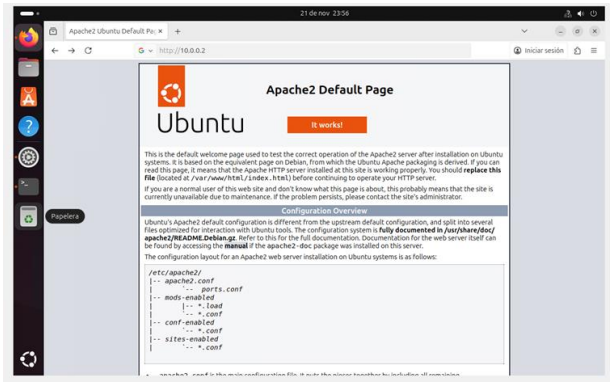
Figura 24. Verificación del estado del servicio FTP



Fuente: Autoría Propia

Como se evidencia en el server Ubuntu ya están activo los servicios HTTP y FTP. Posteriormente a esta validación se puede confirmar si el equipo de la zona *green* puede consumir el servicio apache, esto se logra mediante el cargue en el navegador de la url http://10.0.0.2, si carga una página que dice Apache2 Default page quiere decir que el servicio cargo de manera normal.

Figura 25. Consumo del servicio HTTP desde la zona *green*.



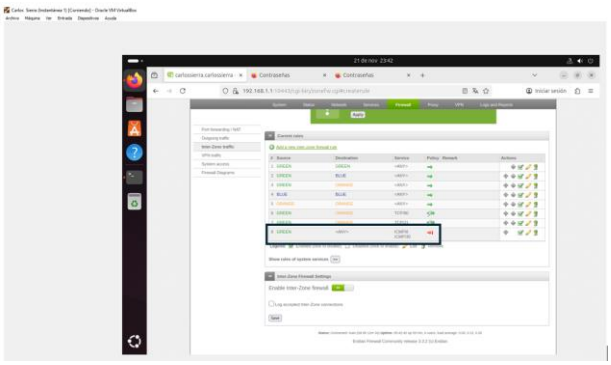
Fuente: Autoría Propia

Se evidencia el acceso al servicio HTTP configurado mediante Apache desde la zona verde.

4.2 DENEGACION DEL PROCOLO ICMP

Ahora se procede a realizar la denegación del protocolo ICMP con la finalidad de que cualquier equipo pueda hacer ping dentro de la red y el host responda. Para ello se dirige nuevamente a la consola de Endian y se selecciona en *firewall/ Inter Zone traficc/add* a *new inter-zone firewall rule* y posteriormente se configura la política de denegación del servicio ICMP por los puertos 30 y 80.

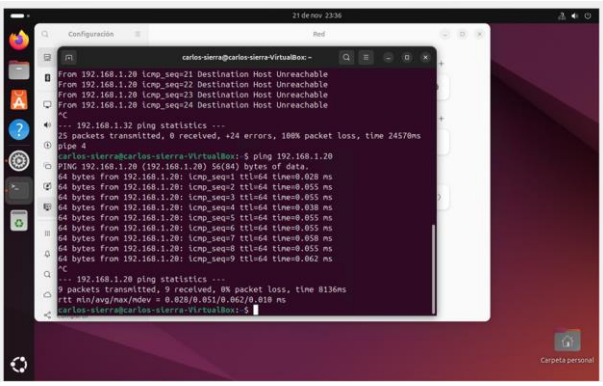
Figura 26. Restricción de tráfico ICMP.



Fuente: Autoría Propia

Antes de habilitar la regla configurada anteriormente se realiza una prueba de ping desde la zona *green* hasta la zona *orange* validando que responda ping de manera correcta.

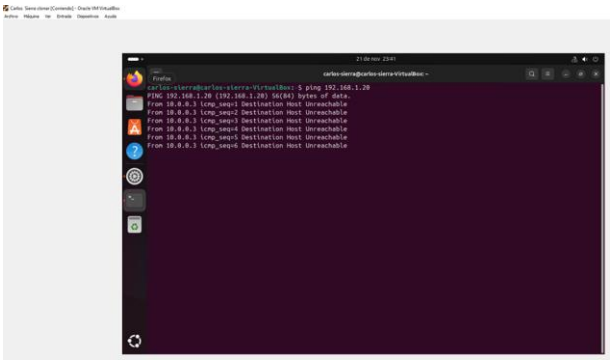
Figura 27. Validación de ping.



Fuente: Autoría Propia

Luego de habilitación de la regla, se procede a realizar nuevamente la prueba de ping y se evidencia que el destino no es accesible, lo que quiere indicar que la regla quedo configurada correctamente.

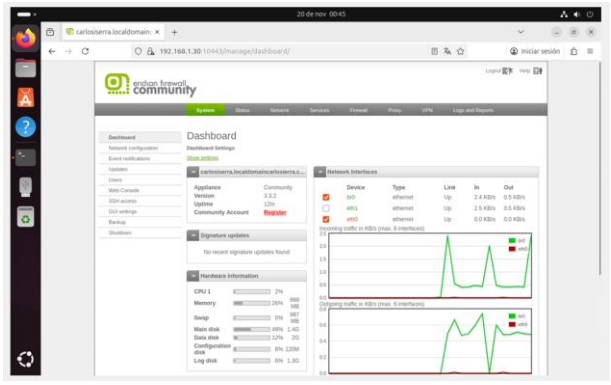
Figura 28. Denegación de respuesta de ping.



Fuente: Autoría Propia

Se evidencia la ejecución del comando ping y su posterior denegación.

Figura 29. Monitoreo de Zonas



Fuente: Autoría Propia

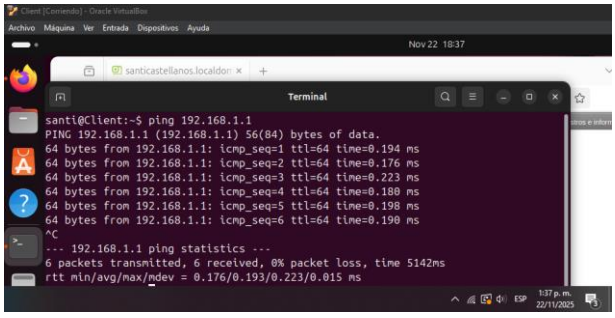
Se evidencia el *dashboard* correspondiente al monitoreo de zonas para su posterior uso.

5 TEMÁTICA 4: REGLAS DE ACCESO ENTRE ZONAS

5.1 CONFIGURACIÓN DE MÁQUINAS VIRTUALES

Para la configuración inicial de red se pretende alinear los parámetros establecidos en puntos anteriores, por lo que a continuación se efectúan los comandos correspondientes a las direcciones asignadas y su correcto funcionamiento tanto en el entorno de escritorio como en el entorno del servidor.

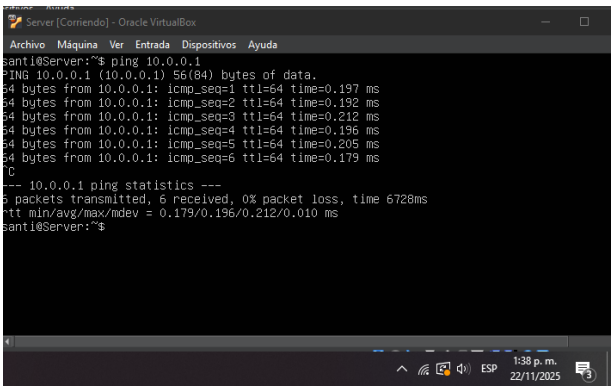
Figura 30. Verificación de ping desde el escritorio a Endian.



Fuente: Autoría Propia

Se evidencia la ejecución del comando ping desde el escritorio hacía el entorno de Endian para verificar su conectividad.

Figura 31. Verificación de ping desde el servidor a Endian.



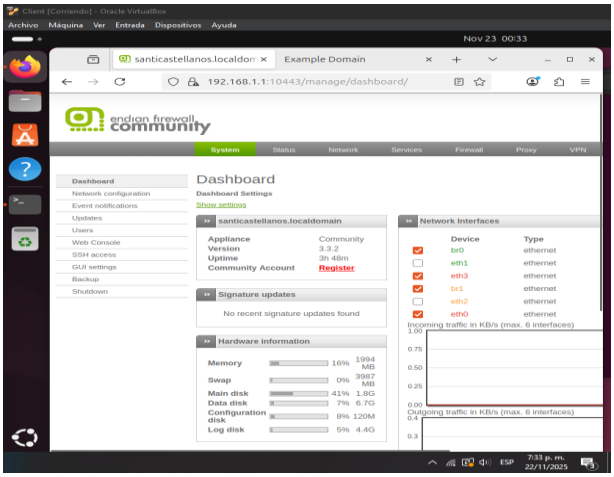
Fuente: Autoría Propia

Se evidencia la ejecución del comando ping desde el servidor hacía el entorno de Endian para verificar su conectividad.

5.2 ACCESO A ENDIAN DESDE EL ESCRITORIO

Una vez configurados los entornos correspondientes, se puede iniciar sesión desde el escritorio empleando la red de la zona verde.

Figura 32. Acceso a interfaz de Endian desde el escritorio.



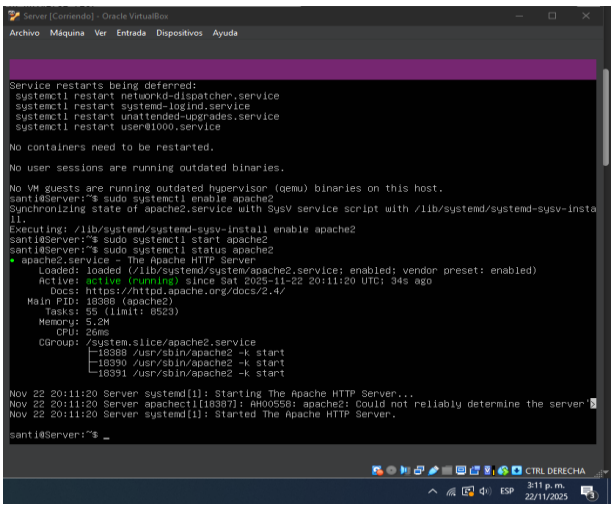
Fuente: Autoría Propia

Se evidencia la posibilidad de acceder al entorno Endian desde un navegador web en el entorno de escritorio.

5.3 CONFIGURACIÓN ENTORNO DE EL SERVIDOR

Con el objetivo de cumplir con los requerimientos solicitados, es fundamental configurar el entorno del servidor con servicios como Apache y un protocolo FTP.

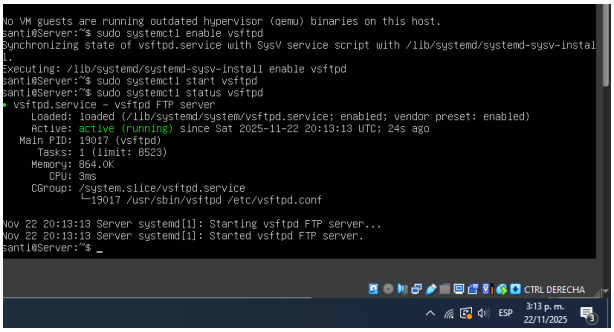
Figura 33. Instalación Apache en el servidor.



Fuente: Autoría Propia

Se evidencia la instalación y correcta ejecución de Apache para su posterior uso en HTTP.

Figura 34. Instalación servicio FTP en el servidor.



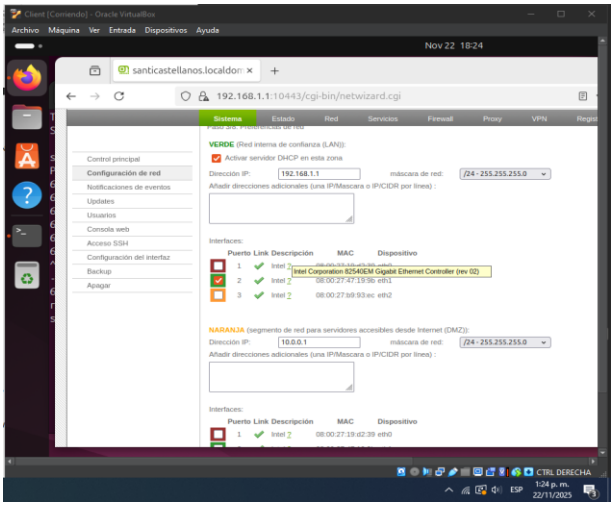
Fuente: Autoría Propia.

Se evidencia la instalación y correcta ejecución del servicio FTP.

5.4 CONFIGURACIÓN DE RED ENDIAN

Una vez culminado el proceso se puede verificar la configuración de la red en Endian corroborando que es idéntica a la propuesta en la temática 1.

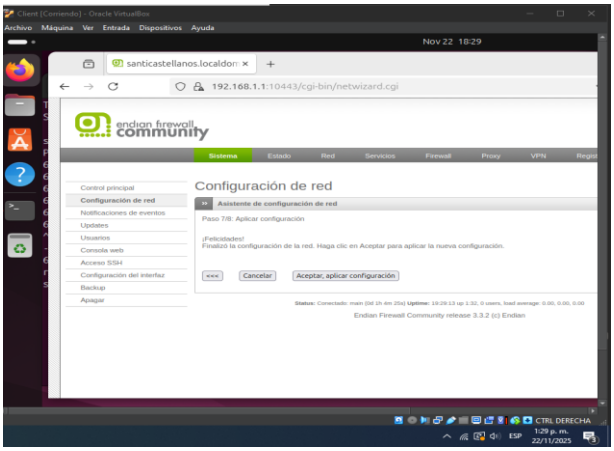
Figura 35. Validación de zonas y direcciones.



Fuente: Autoría Propia

Se evidencia que la configuración de las redes ha sido establecida alineándose a los parámetros establecidos en el documento.

Figura 36. Confirmación configuración de red.



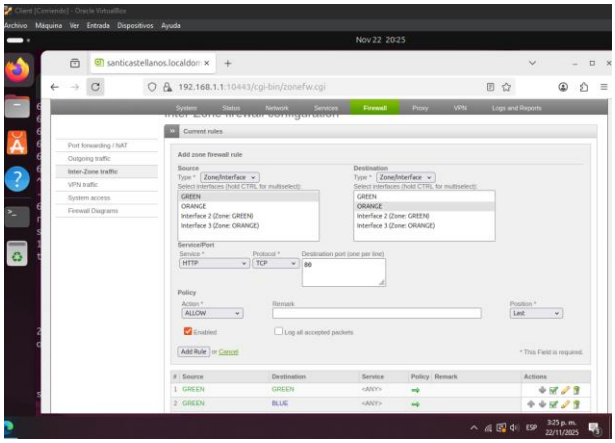
Fuente: Autoría Propia

Se evidencia la configuración completa de la red, necesario para poder gestionar los recursos de manera efectiva.

5.5 CREACIÓN DE REGLAS: PERMITIR LA CONECTIVIDAD DE LA ZONA VERDE CON LA ZONA NARANJA POR HTTP Y FPS.

Una vez se garantice que se establece la conexión y uso correcto de parámetros se procede a la creación de reglas de firewall que permitan la conectividad de los servicios previamente descargados en el entorno del servidor.

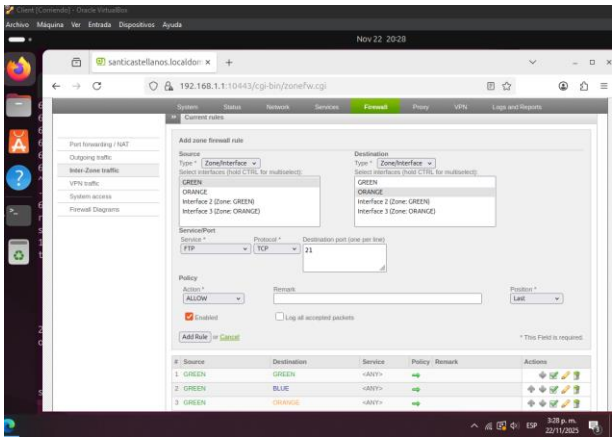
Figura 37. Configuración de la conectividad HTTP entre la zona verde con la zona naranja.



Fuente: Autoría Propia

Se evidencia la creación de la regla correspondiente a los accesos necesarios para el servicio HTTP con el puerto 80.

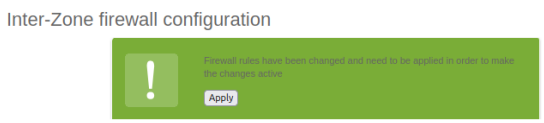
Figura 38. Configuración de la conectividad FTP entre la zona verde con la zona naranja.



Fuente: Autoría Propia

Se evidencia la creación de la regla correspondiente a los accesos necesarios para el servicio FTP con el puerto 21.

Figura 39. Aplicación de las reglas creadas.



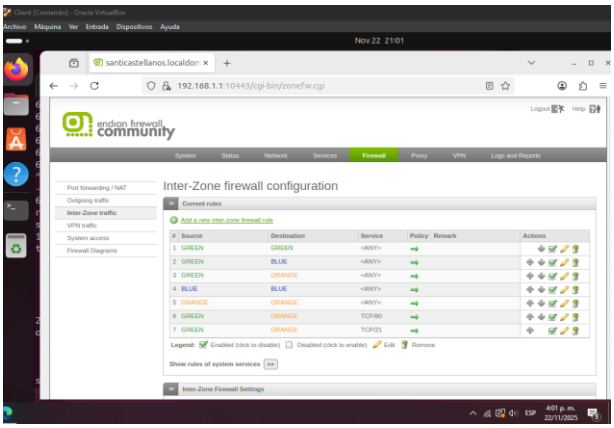
Fuente: Autoría Propia

Se evidencia el mensaje de aplicación necesario para guardar las reglas creadas.

5.6 VERIFICACIÓN DE REGLAS CREADAS EN LA INTER-ZONE.

Conforme se definen y se ajustan las reglas se verán reflejadas en la interfaz de Inter-Zone, donde podremos corroborar la creación y visualización de las reglas definidas previamente.

Figura 40. Visualización de la interfaz de reglas.



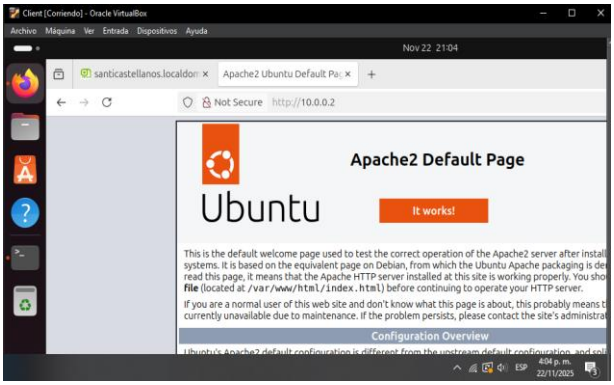
Fuente: Autoría Propia

Se evidencia el resumen de las reglas que han sido creadas y establecidas.

5.7 EVIDENCIA DE CONECTIVIDAD SEGÚN DIRECTIVAS.

Una vez establecido el proceso base, se procede con la verificación de conectividad entre servicios, a continuación, estarán listados en orden según las directivas solicitadas.

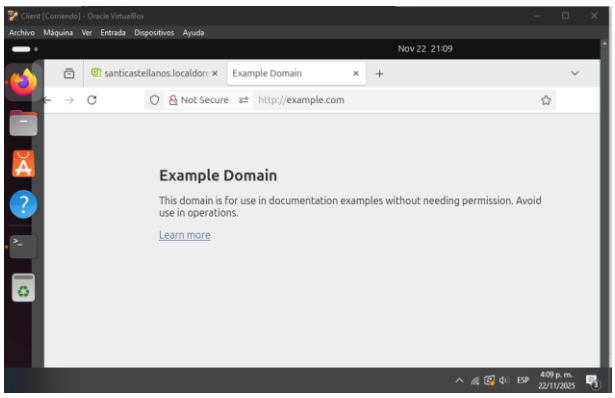
Figura 41. Conexión servicio HTTP desde LAN hacía zona DMZ.



Fuente: Autoría Propia

Se evidencia la accesibilidad del servicio HTTP desde el entorno de escritorio.

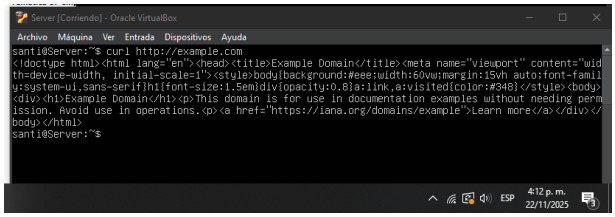
Figura 42. Conexión desde LAN hacía WAN por HTTP.



Fuente: Autoría Propia

Se evidencia la accesibilidad del servicio HTTP.

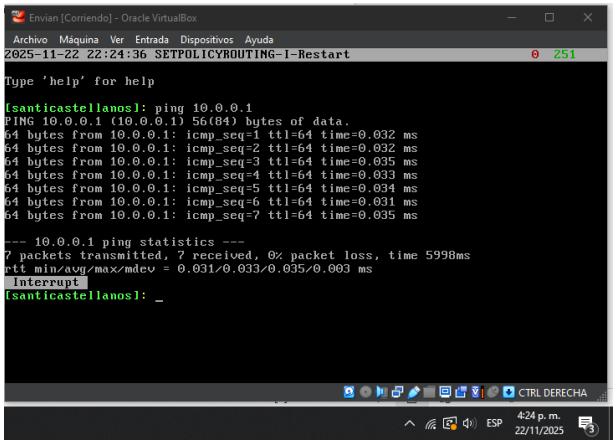
Figura 43. Ingreso del servicio HTTP desde la zona DMZ hacía la WAN.



Fuente: Autoría Propia

Se evidencia la ejecución del comando *curl* para verificar la accesibilidad del servicio HTTP desde la DMZ.

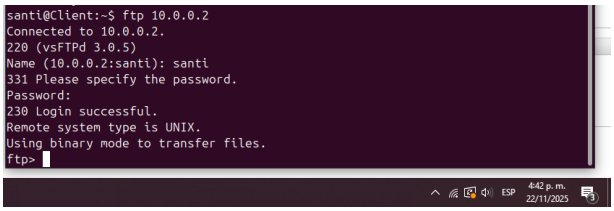
Figura 44. Ingreso del servicio HTTP desde la WAN hacía la zona DMZ.



Fuente: Autoría Propia

Se evidencia que el comando ping funciona de manera efectiva desde la WAN hacia la DMZ.

Figura 45. Ingreso del servicio FTP desde la LAN hacia la WAN.



Fuente: Autoría Propia

Se evidencia la conectividad del servicio FTP desde el entorno de escritorio hacía la zona WAN.

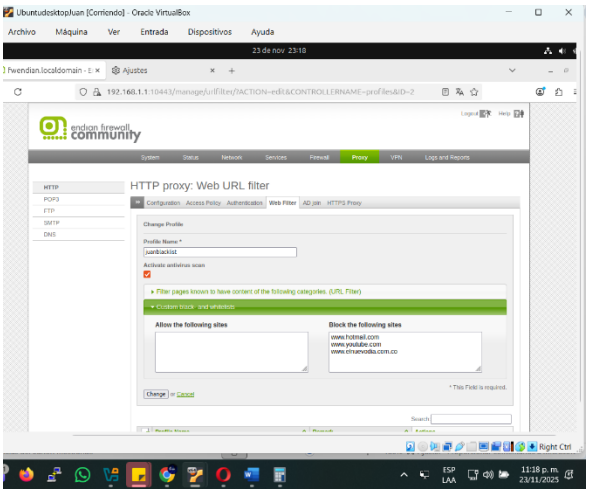
6 TEMÁTICA 5: PROXY HTTP CON AUTENTICACIÓN

Se realiza la configuración correspondiente de red Verde, naranja y roja respectivamente con su ip asignado, con la configuración e instalación idóneo de Endian firewall.

6.1 CREACIÓN DE PERFIL Y LISTA NEGRA DE SITIOS WEB

Desde Endian Firewall en la opción de Proxy se escoge HTTP y *Web filter* donde se realiza la creación de perfil con el nombre "juanblacklist".

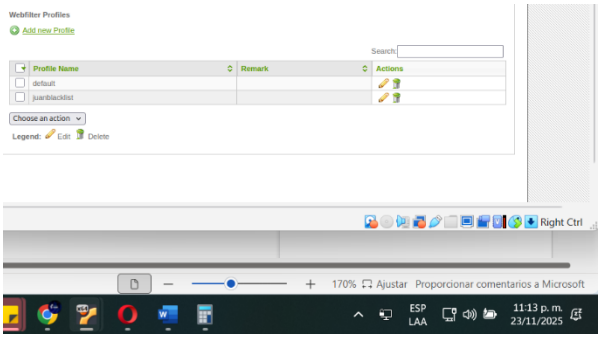
Figura 46. HTTP proxy: Web URL filter



Fuente: Autoría Propia

Para realizar la lista negra, en esta misma ventana en el espacio de *block the following sites* se agregan los tres sitios web que se desean bloquear; Hotmail, YouTube, Elnuevodía, como se ve en la figura 46

Figura 47. Perfil juanblacklist



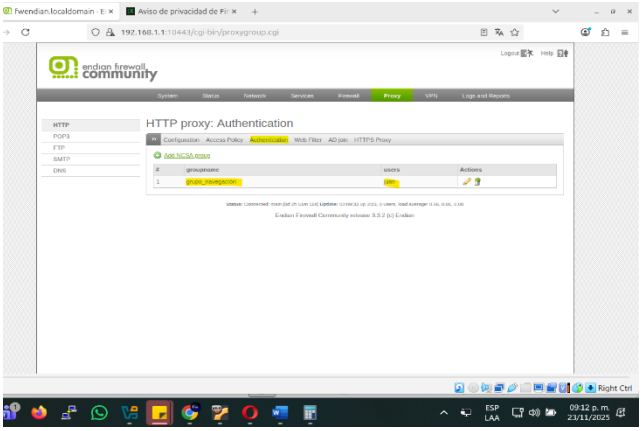
Fuente: Autoría Propia

En la figura 47 se puede ver el perfil creado como "juanblacklist" en la pestaña de filtro de webs.

6.2 CREACIÓN DE USUARIO PROXY Y VINCULACIÓN DE PERFIL

Desde la pestaña de Proxy dentro de la opción de Autenticación, se puede realizar la creación de grupo para relacionarlo con el usuario, en la parte de "administración de grupos".

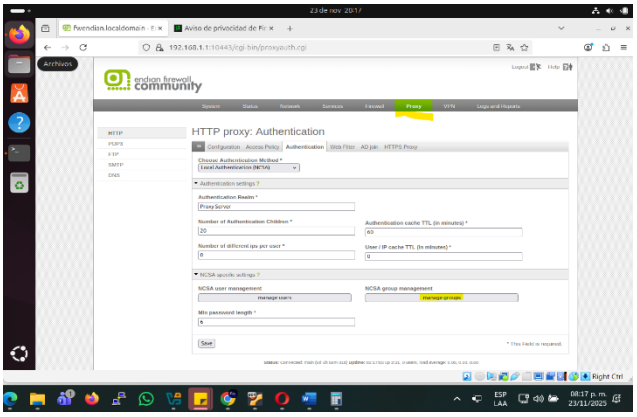
Figura 48. Creación de grupo



Fuente: Autoría Propia

En la creación del grupo se le asigna con el nombre "grupo_navegación" y se procede a relacionar el usuario "juan" creada como se puede visualizar en la Figura 49 dentro de la ventana *HTTP proxy: Authentication.*

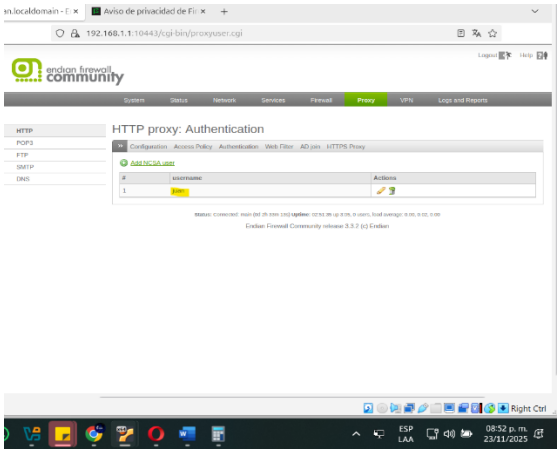
Figura 49. HTTP proxy: Autenticación



Fuente: Autoría Propia

Se puede realizar la creación del nuevo usuario regresando a la pestaña de autenticación dentro de proxy como "Juan" asignándole su contraseña correspondiente que será la que solicitará en el momento de ingresar a las páginas de navegación

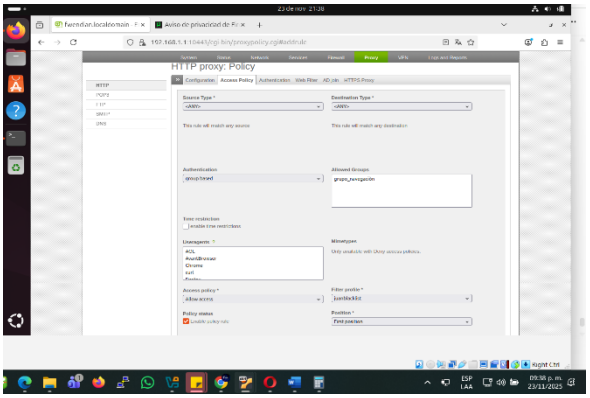
Figura 50. Creación de usuario



Fuente: Autoría Propia

Para proceder a realizar la configuración de proxy y que tenga en cuenta solo el perfil del grupo y la lista negra de las páginas a las que no se pueden ingresar se toma las opciones adecuadas en el acceso político.

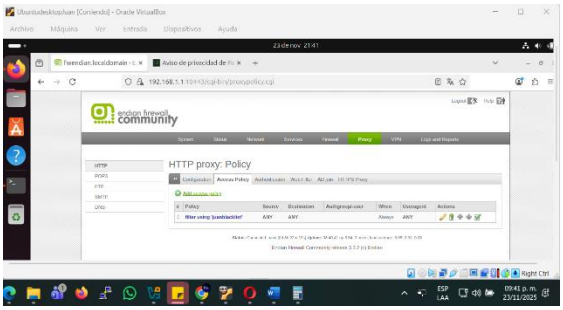
Figura 51. HTTP proxy: Política



Fuente: Autoría Propia

En la Figura 52 se evidencia que la política de HTTP proxy ya fue configurada

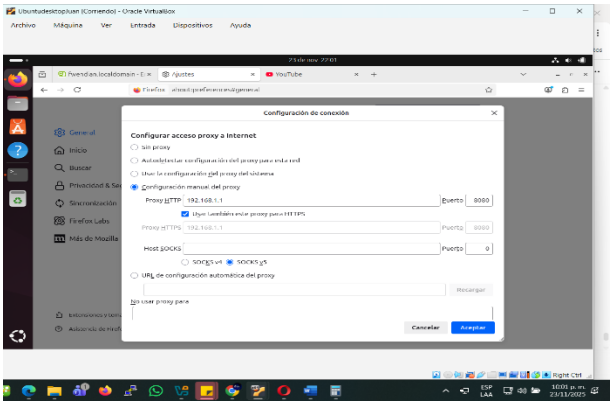
Figura 52. HTTP proxy: Política



Fuente: Autoría Propia

Enseguida para poder validar el funcionamiento de nuestra configuración se ingresa desde los ajustes del navegador de Firefox, encontrando la opción de red permitiendo abrir la configuración de conexión y modificando así mismo el acceso proxy, donde se ingresa la IP en la que fue realizada la configuración con su puerto 8080.

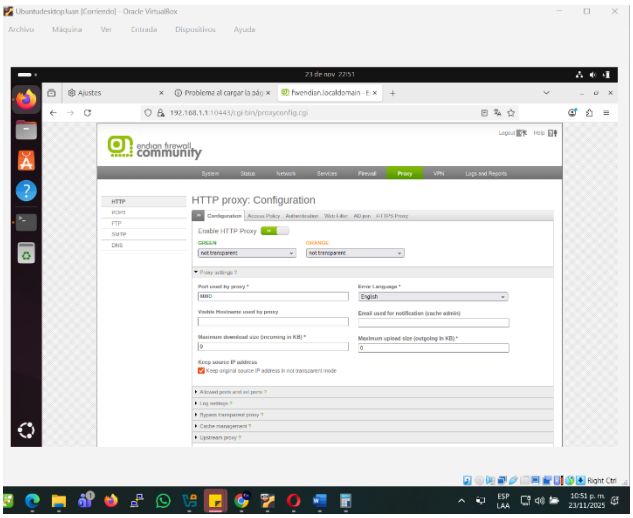
Figura 53. Configuración Proxy



Fuente: Autoría Propia

Se confirma en Endian que en la sección de HTTP en la pestaña de configuración debe estar habilitada la opción de *Enable HTTP Proxy* con el puerto 8080 fijándose que en las opciones Verde y Naranja.

Figura 54. Proxy habilitado en Debian



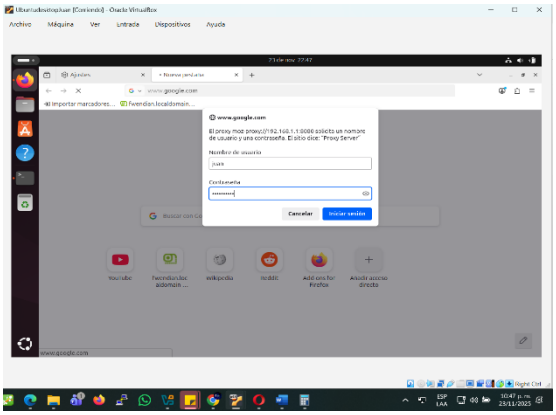
Fuente: Autoría Propia

Como se ve en la figura 54, la opción de no transparente debe estar marcado ya que esta opción es la que da el permiso de pedir autenticación al grupo y usuario.

6.3 PRUEBA DESDE LA LAN A LOS ACCESOS DE LA LISTA NEGRA

Para poder realizar la prueba de la configuración y verificar si está tomando en cuenta lista negra configurada con las direcciones de navegador solicitadas se procede a ingresar a Google como prueba donde se evidencia el hecho de que solicita la autenticación del usuario creado con la contraseña anteriormente configurada en la plataforma de Endian. Tal como se puede observar en la Figura.

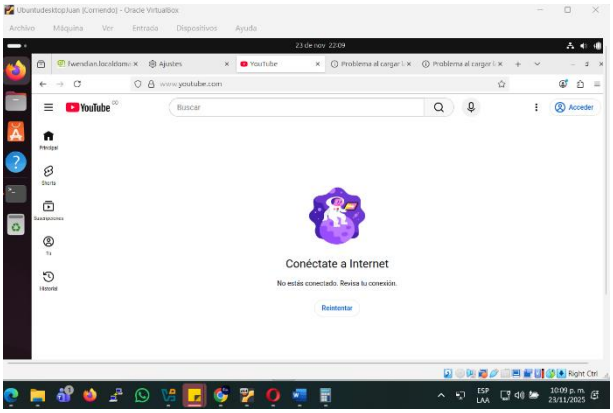
Figura 55. Proxy habilitado en Debian



Fuente: Autoría Propia

Y para la validación de la lista negra se procede abrir la ventana de los tres sitios web. YouTube, Hotmail, el nuevo día.

Figura 56. Proxy habilitado en Debian



Fuente: Autoría Propia

La figura 56 muestra que es posible modificar el bloqueo frente a estas páginas.

7 CONCLUSIONES

La implementación de Endian Firewall permitió comprender cómo se estructura un firewall real y cómo se realiza la segmentación de una red en distintas zonas de seguridad, principalmente para evitar ser víctimas de ataques y por consecuencia perdida y filtración de información que puede ser confidencial.

La configuración de NAT demostró la importancia de la traducción de direcciones para permitir la salida controlada hacia Internet desde redes privadas, siendo esta crucial para permitir el acceso solo a personal autorizado y por consecuencia evitar la navegación a sitios desconocidos desde dispositivos externos o internos.

La publicación de servicios desde la DMZ permitió evidenciar cómo se exponen recursos externos sin comprometer

la red interna, de esta manera se establece un control de seguridad más amplio que permite mantener y controlar los dispositivos que están siendo administrados en los diferentes entornos.

Las reglas de acceso entre zonas permitieron gestionar de manera adecuada el flujo de información y de qué manera se establecen las conexiones entre los distintos componentes que interactúan en un servidor.

La implementación del proxy con autenticación permitió establecer diferentes privilegios de acceso para el control de usuarios y los accesos que disponen cada uno de ellos, además, se establece un control de seguridad adicional que permite la verificación antes de la manipulación o visualización de información.

8 REFERENCIAS

[1] Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Revision 1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf

[2] Free Software Foundation. (2024) GNU/Linux: Free operating system. https://www.gnu.org/linux/