Seguridad Perimetral En Redes GNU/Linux Utilizando Edian Firewall

Yerson Leonardo Hurtado Diaz

RESUMEN: *En este artículo se realizó la implementación practica y teórica del firewall EDIAN, de forma virtualizada con ayuda de VirtualBox. Donde se realizó la configuración de las zonas solicitadas la cuales son zona verde en red LAN, roja en WAN y naranja DMZ, por consiguiente, también se definieron reglas de navegación y/o acceso, servicios permitidos y sus respectivas políticas de seguridad. Debido a las limitaciones técnicas que presenté durante el desarrollo de la actividad con la configuración de la NAT y otros intentos de los adaptadores, la totalidad de las pruebas practicas no pudo ser completadas de forma práctica, por lo cual decidí realizar la sustentación teórica de estas faltantes fundamentado en el comportamiento esperado del sistema es esos escenarios. Adicionalmente se documenta la implementación teórica de el proxy http con autenticación de usuarios y sus controles de acceso utilizando la lista negra como es solicitado. Los resultados permiten evidenciar la comprensión que se obtuvo sobre los principios y aplicación de seguridad perimetral, segmentación de red y el control del tráfico en entornos GNU/Linux..*

PALABRAS CLAVE: Firewall, GNU/Linux EDIAN, Proxy http, seguridad perimental.

1 INTRODUCCIÓN

La seguridad peri mental es fundamental para controlar la protección de las redes y subredes informáticas actuales, ya que al poder controlar el tráfico en todas las redes con las que se cuenten. En el contexto actual, un firewall que este basado en Linux representa la mejor solución y la más flexible para las políticas de seguridad que se deseen implementar. Este trabajo tiene como fin documentar la configuración del firewall EDIAN echo en las máquinas virtuales de VirtualBox donde también se nos permite realizar la visualización de los conceptos segmentación por zonas, reglas de acceso, servicios que se pueden controlar y uso de proxys para la navegación web. Aunque lastimosamente se presentaron las limitaciones de conectividad hacia internet, con el desarrollo teórico se permite justificar los funcionamientos esperados de cada configuración.

2 Configuración General del Entorno

2.1 Virtualización y zonas de red

Debido a que ya se contaba con el sistema operativo DEBIAN previamente instalado, se procedió a realizar la descarga de la imagen iso de EDIAN, el cual para su despliegue se configuro el VirtualBox con los requisitos necesarios para su correcta funcionalidad en un entorno simulado.

Una vez cargada la imagen iso se procede a arrancar la maquina y empieza a leer la imagen iso para su instalación inicial donde solicitara elegir un idioma para su previa instalación,

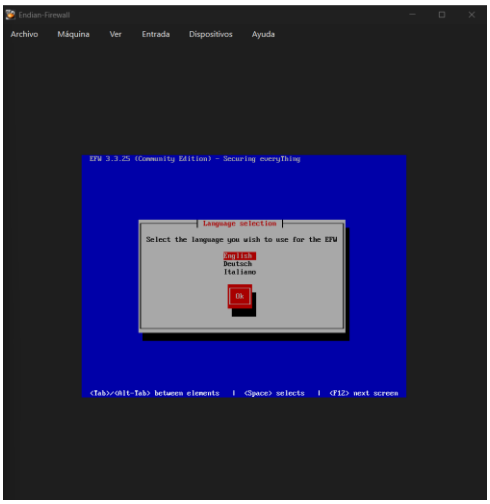


Fig.1. Selección de idioma

Luego se despliega una nueva ventana de instalacióon donde nos da la bienvenida, en esta das enter en ok para aceptar la instalción de EDIAN.

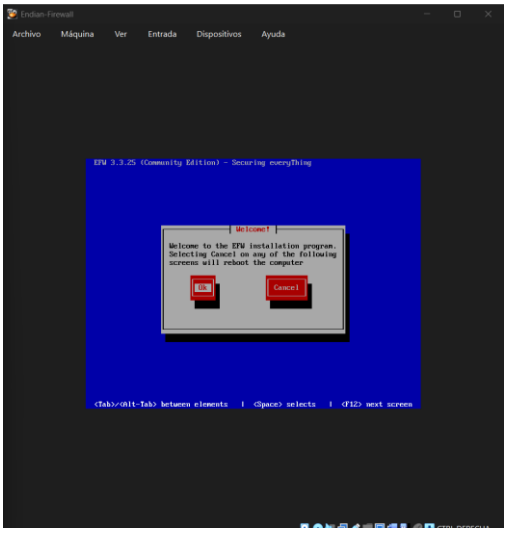


Fig.2. Aceptación de instalación

Luego se abre la ventana emergente donde dice que se realizara una partición donde se alojara los archivos necesarios para el correcto funcionamiento de EDIAN, en esta imagen damos enter en Yes para continuar la instalación.

Fig.3. Se acepta para inicar la instalación en el espacion designado.

Una de las ultimas ventanas que aparecen es la pregunta de habilitar la consola a través de puerto serial.

Fig.4. Se realiza enter sobre si y de esta forma se avanza a la siguiente ventana de configuración de red.

En la próxima pantalla se despliegan las opciones de configuración de la interfaz Green de Edian, que es la red local (LAN).

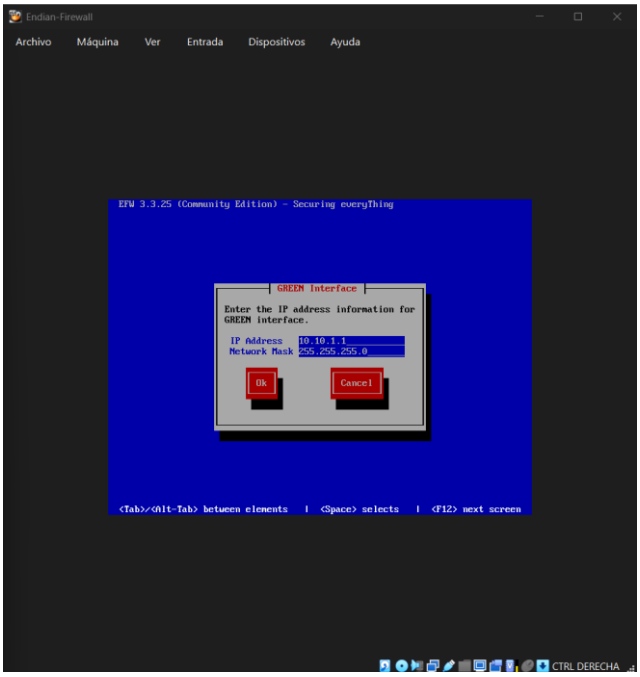


Fig. 5.Se asigna la ip y se da enter en ok para su asignación.

La ultima ventana de instalación nos indica que el despliegue de Edian firewall se realizó con equito a lo cual se confirma dando enter en ok.

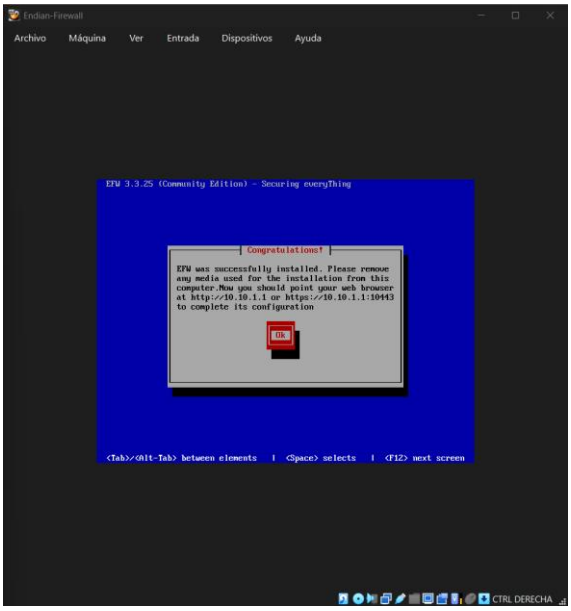
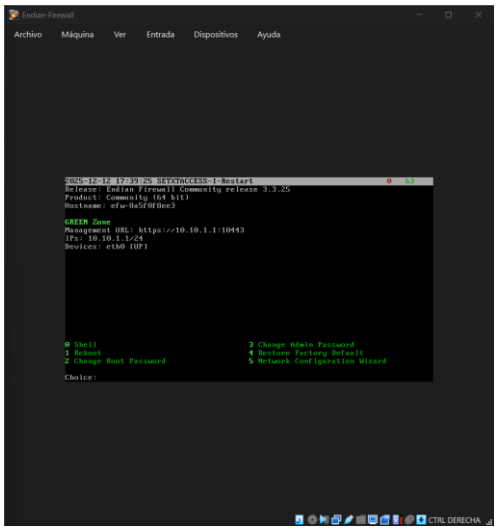


Fig.6. Enter en ok para ir a la pantalla de inicio

Cuando hemos realizado todos los pasos y estamos seguros de que todo fue exitoso nos mostrara la pantalla de inicio del sistema operativo Edian firewall.



Fg.7. Pantalla de inicio EDIAN.

Se realiza una prueba de conectividad desde el servidor Edian y el cliente donde se puede acceder a la configuración de forma más grafica

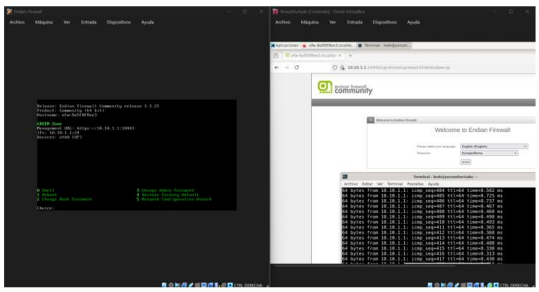


Fig.8. El ping responde a la conexión de forma exitosa.

Cuando iniciamos con la configuración previa se nos solicitara realizar la elección del idioma con el cual desearemos realizar el resto de la configuración.

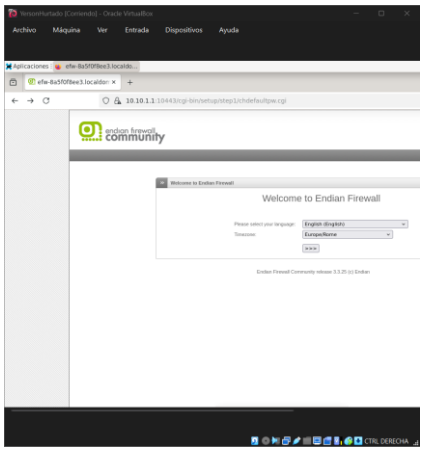


Fig.9.Eleción de idioma.

Una vez seleccionado el idioma se da clic en el signo de >>> para continuar la configuración en esta ventana aceptaremos la licencia de EDIAN para poder configurar las demás redes.

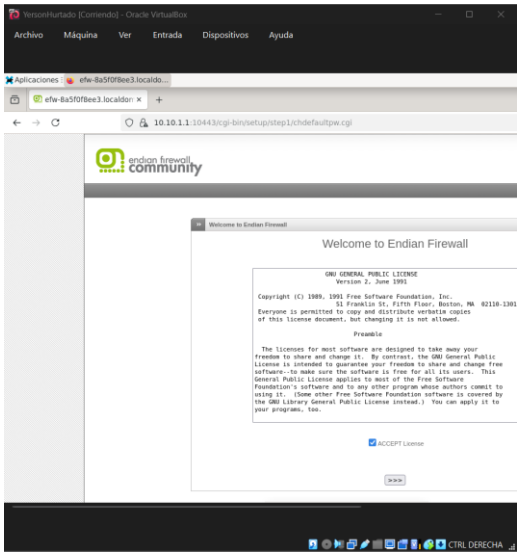


Fig.10. Lincencia por aceptar.

La siguiente ventana da la opción de importar una copia de seguridad de la configuración previa, pero dado que es la primera instalación no será necesario entonces se deja en **No.**

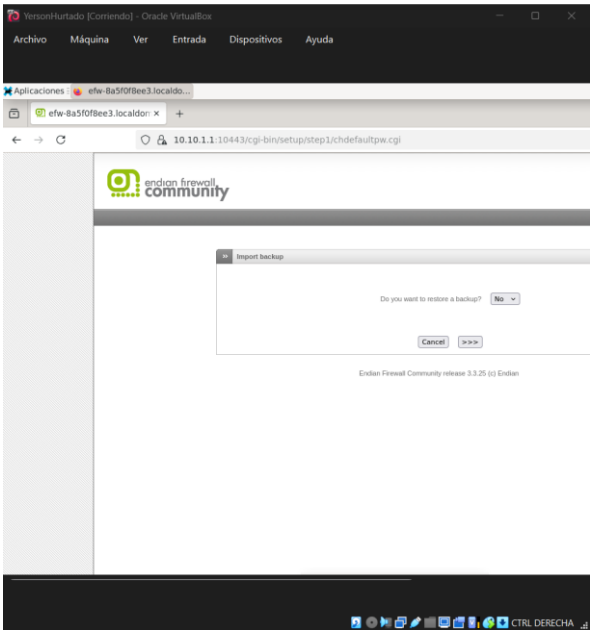


Fig.11. Selección de no al importe del backup.

El próximo paso es configurar los usuarios de Root y Admin se desplegará una ventana donde se nos pedirá asignar contraseña a los usuarios mencionados

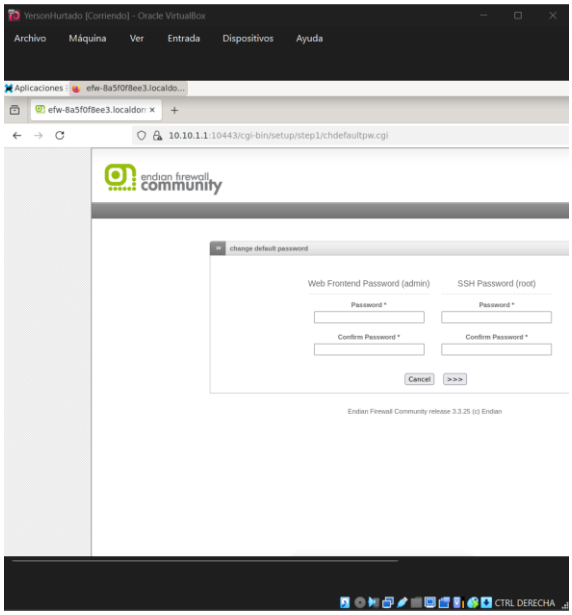


Fig.12. Asignación de contraseñas.

Se configura la zona roja donde se dejan los valores que trae por defecto si no son los de la imagen se deben reconfigurar para que queden de la siguiente manera, Network modes debe quedar cliqueado Routed y uplink type debe quedar en Ethernet DHCP

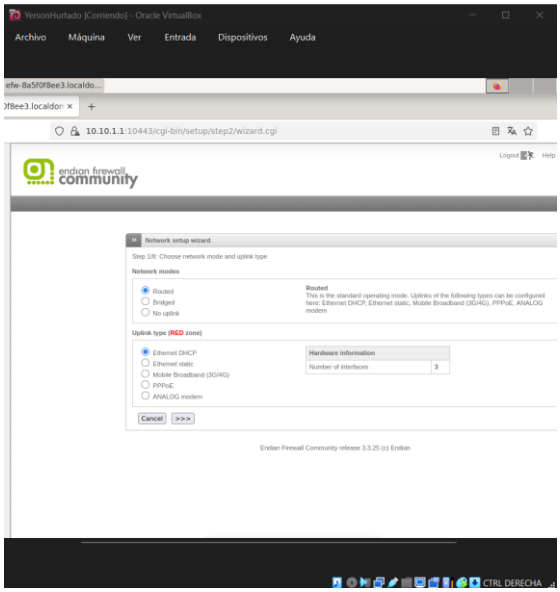


Fig.13. Configuración realizada para zona roja.

En la ventana siguiente nos indicara si deseamos crear otra zona de red, si no la necesitamos damos clic en siguientes para nuestro caso si vamos a seleccionar la zona Orange o DMZ.

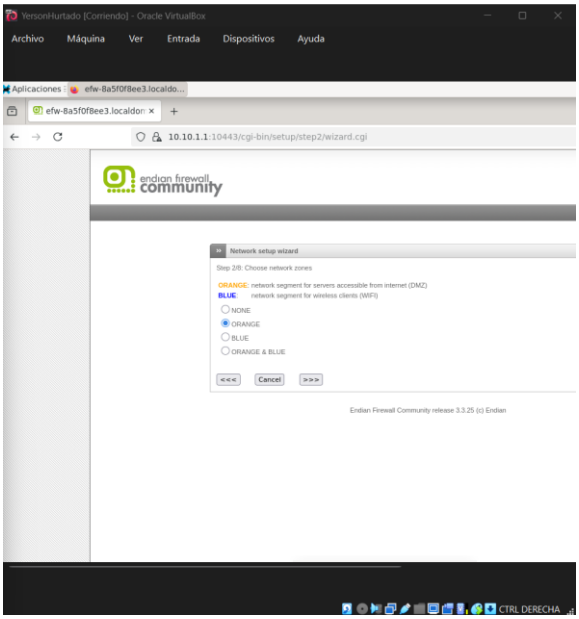


Fig.14. Creación de la zona Orange.

La siguiente imagen nos muestra una configuración predeterminada la cual solo le daremos siguiente y se aplica tal cual.

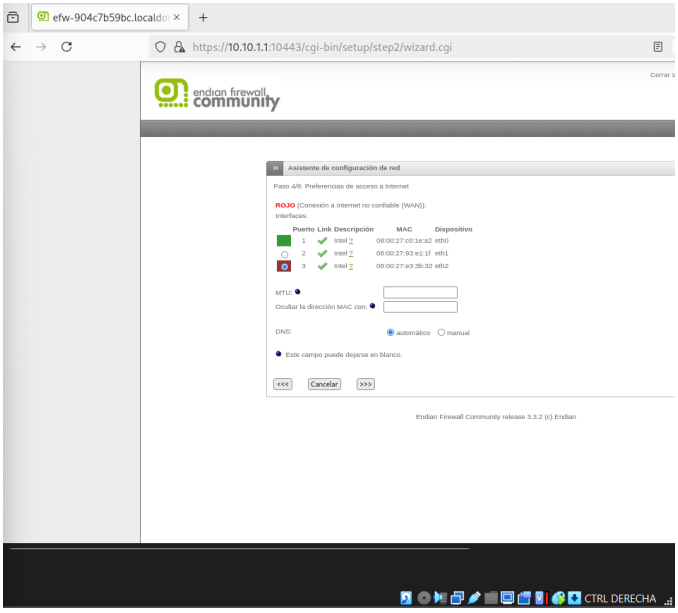


Fig.15.vusualización de la configuración predeterminada.

Se realiza la configuración de la zona Green y Orange asignando la ip a cada una de ellas para poder realizar las conexiones y configuraciones recomendadas.

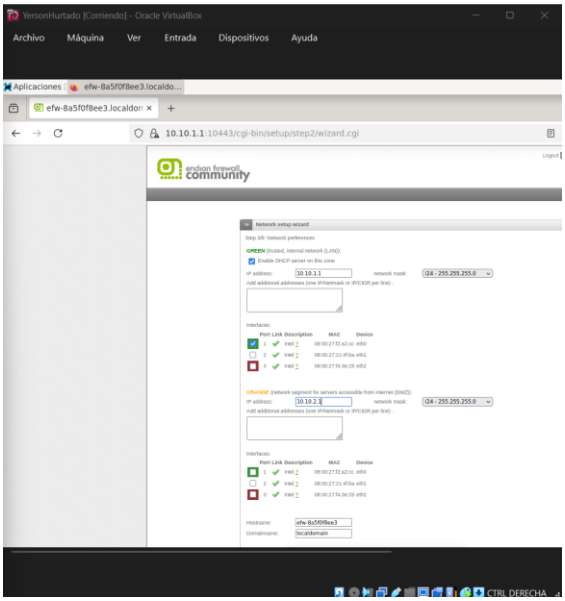


Fig.16. Configuraciones de las ip para cada zona.

La configuración de los DNS la dejaremos en automático como se puede apreciar en la figura 17.

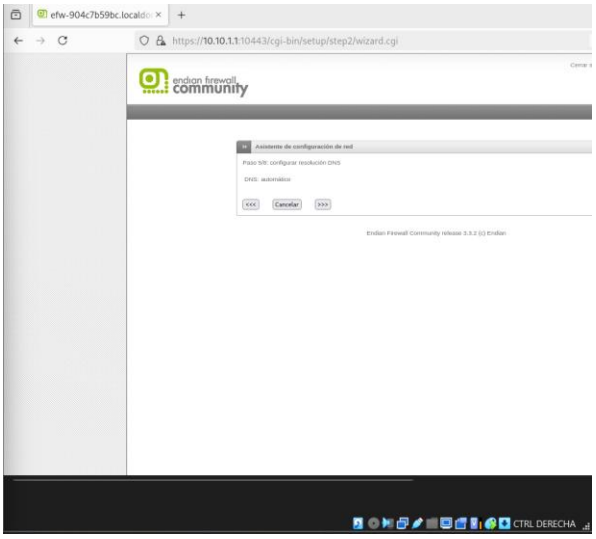


Fig.17. Configuracion final de DNS.

Por lo general este tipo de software (filware) solicita correos para poder realizar y eviar alertas a los administradores cuando detecta inconsistencias o trafico sospechoso en las redes.

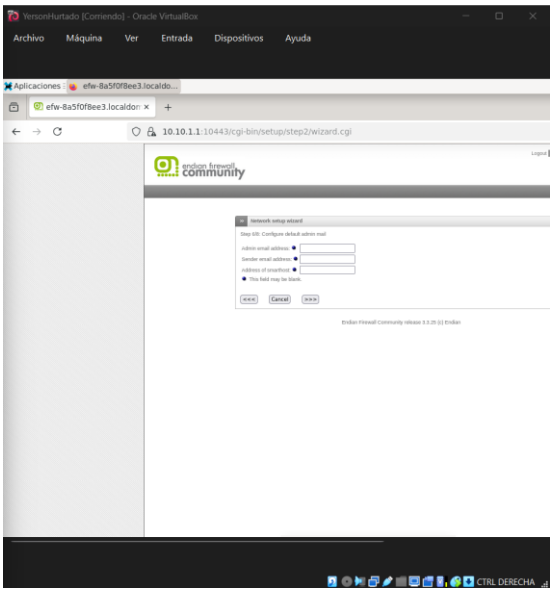


Fig.18.Solicitud de correos de alerta.

Por ultimo se visualiza la aplicación de la configuración en la parte 7/8 una vez termina se podra visualizar el dasbohar.

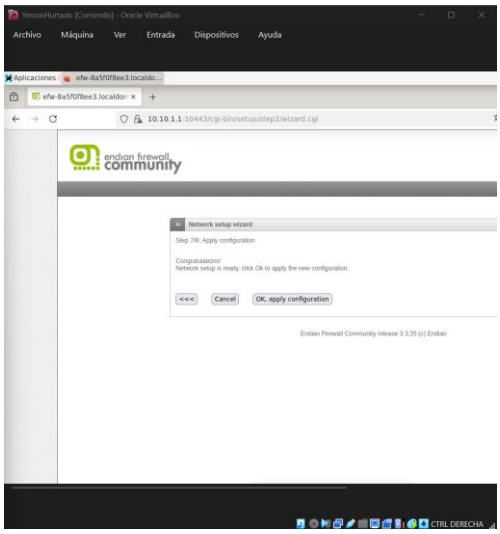


Fig.19. Configuración final de ingreso a EDIAN

Funcionamiento exitoso de Edian en su forma grafica el cual permite aplicar reglas y monitorear trafico.

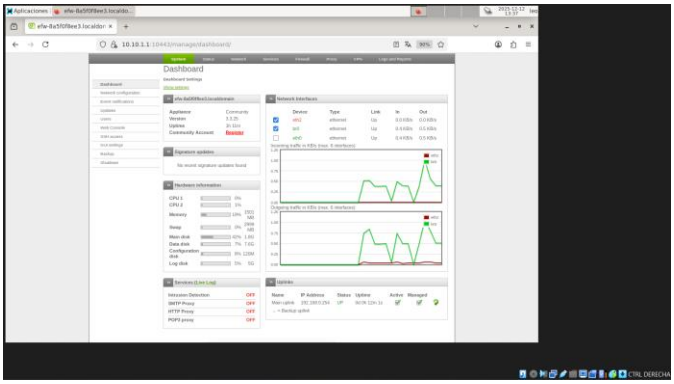


Fig.20. Presentación del Dashboard.

3 Configuración NAT (Masquerading)

Para aplicar las reglas nos dirigimos Firewall luego a Source Nat y por último Add a new source NAT rule.

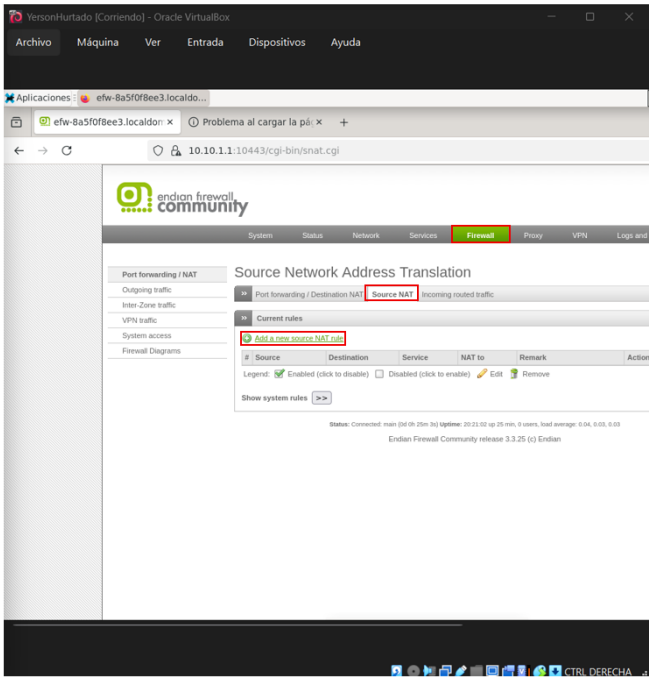


Fig.21.Interfaz para poder agregar las reglas.

El objetivo es crear una regla que permita que las redes internas (GREEN y ORANGE) salgan a Internet a través de la Zona RED, utilizando las ip utilizadas para las maquinas.

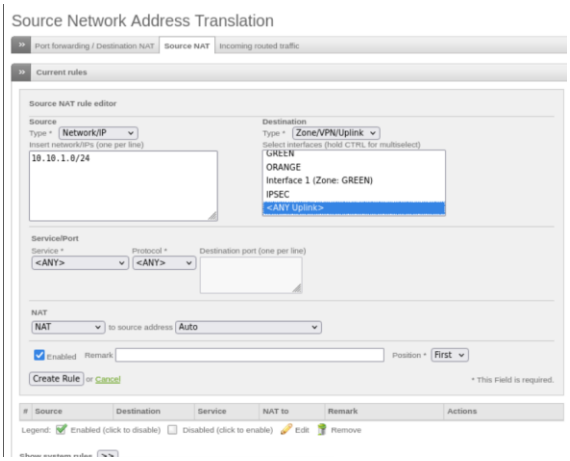


Fig.22.Reglas solicitadas para agregar las redes.

Se agregan las ip de la zona green y la orange y se aplican las reglas para su funcionamiento y se debe ver asi como la figura 23.

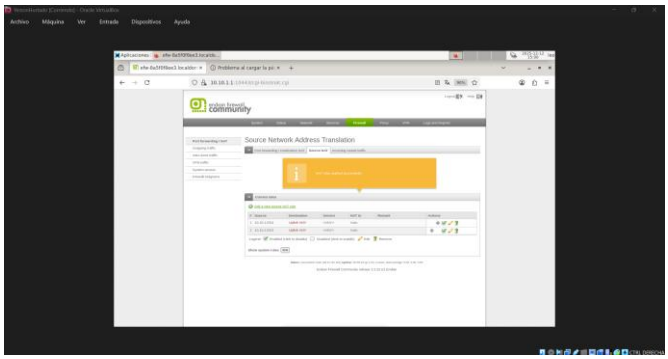


Fig.23. Reglas creadas

4 Sustentación Teorica de los puntos faltantes.

Los puntos 3, 4 y 5 se sustentara de forma teórica en el video adjunto debido a problemas técnicos que se me salen de las manos debido a los recursos con los que cuenta mi equipo de cómputo, los puntos faltantes están sustentados bajo el comportamiento normal que tendrían los software al momento de realizar pruebas de conexión, habilitación de protocolos, creación de reglas y de más complementos solicitados en el trabajo.

Link de la sustentación:
https://drive.google.com/file/d/1G4hgdiRyP7tRvLKr4_LACu_FJNMAxlCB/view?usp=drive_link

Conclusiones.

- Las configuraciones que permite realizar Edian con la segmentación son fundamentales para la seguridad perimental.
- Las reglas del firewall nos permiten tener el control sobre el acceso a servicios fundamentales como http y ftp forma segura.
- El bloqueo ICMP nos ayuda a realizar una reducción de la exposición de los dispositivos administrados frente a escaneos de red.
- El proxy HTTP con su respectiva autenticación proporcionara un mejor control sobre la navegación que realizan todos los usuarios.
- Pese a las limitaciones técnicas que tuve con la red Nat y puente, el desarrollo que se realizó de forma teórica se evidencia la correcta comprensión de los componente de seguridad que se implementaron.

REFERENCIAS

[1] Endian UTM 3.2 Reference Manual — Endian UTM 3.2 Reference Manual. (s. f.). Endian.com. Recuperado 16 de diciembre de 2025, de http://docs.endian.com/3.2/utm/index.html
.

[2]Guía Debian GNU/Linux de instalación. (s. f.). Debian.org. Recuperado 16 de diciembre de 2025, de https://www.debian.org/releases/stable/amd64/index.es.html
.

[3] *No title*. (s. f.). Edu.co. Recuperado 16 de diciembre de 2025, de https://repository.unad.edu.co/handle/10596/54230
.

[4] *Tema 102: Instalación de Linux y gestión de paquetes*. (s. f.). Lpi.org. Recuperado 16 de diciembre de 2025, de https://learning.lpi.org/es/learning-materials/101-500/102/
.

[5] *User guide for release 7.2. (s. f.). Virtualbox.org. Recuperado 16 de diciembre de 2025, de https://www.virtualbox.org/manual/*
.

[6] (S. f.-a). Ubuntu.com. Recuperado 16 de diciembre de 2025, de https://help.ubuntu.com/20.04/ubuntu-help/index.html
.

[1] [7] (S. f.-b). Ebsco.com. Recuperado 16 de diciembre de 2025, de https://research.ebsco.com/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952
.