IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Arley David Pinchao Cuatin
adpinchaoc@unadvirtual.edu.co
Gerzon Miguel Pino Herrera
gpinoh@unadvirtual.edu.co
Juana Valentina Leyton Gaitán
jvleytong@unadvirtual.edu.co
Miguel Darío Solano Romero
mdsolanor@unadvirtual.edu.co
Yorladys Suarez Arango
ysuarezar@unadvirtual.edu.co

RESUMEN: *La seguridad en sistemas GNU/Linux se ha convertido en un componente esencial para la administración de infraestructuras tecnológicas modernas. Este artículo presenta una visión integral de los mecanismos de protección disponibles en entornos Linux, abarcando desde la gestión de usuarios y permisos, hasta la implementación de firewalls, automatización de actualizaciones, políticas de auditoría y herramientas de endurecimiento del sistema. Se analizan estrategias que permiten fortalecer un servidor frente a amenazas comunes, utilizando herramientas nativas y complementarias que garantizan la integridad, confidencialidad y disponibilidad de la información.*

PALABRAS CLAVE: Endian, linux, regla, servidor.

1 INTRODUCCIÓN

GNU/Linux es reconocido como uno de los sistemas operativos más robustos y confiables en el ámbito de servidores. Su arquitectura basada en permisos, su transparencia y la naturaleza abierta del software lo convierten en una plataforma ideal para implementar políticas de seguridad flexibles y escalables. Sin embargo, ningún sistema es seguro por defecto. Es necesario aplicar medidas específicas para minimizar riesgos y asegurar que la infraestructura permanezca protegida frente a ataques internos y externos.

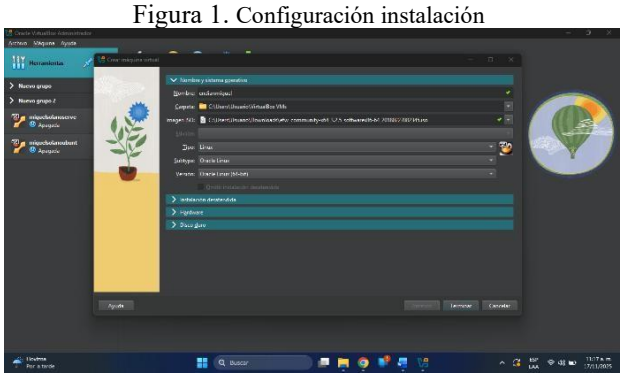
Este artículo describe buenas prácticas y herramientas para implementar una estrategia de seguridad sólida en un entorno GNU/Linux, orientado especialmente a administradores de sistemas, estudiantes y profesionales del área TI.

2 INSTALACIÓN ENDIAN

En primer lugar se descarga la distribución de endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86. Se utiliza el programa Oracle VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

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

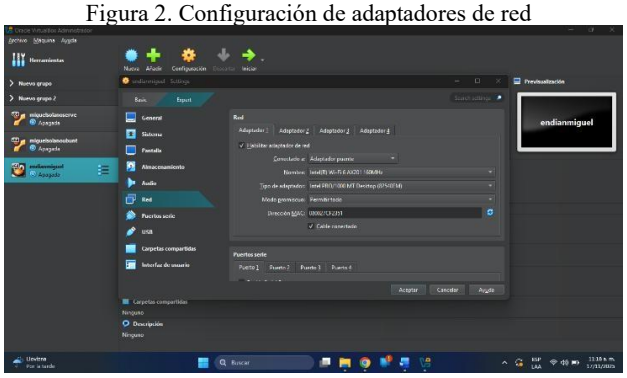
Figura 1. Configuración instalación



Fuente: Autoria Propia

En el apartado de red, de configuración de la máquina virtual, se establece cada una de las redes como GREEN, RED y ORANGE que vamos a utilizar para el desarrollo de cada una de las temáticas.

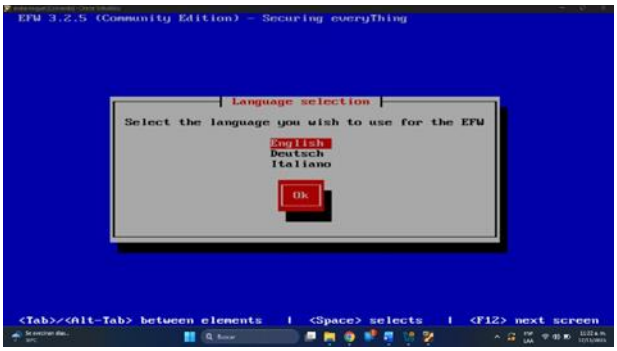
Figura 2. Configuración de adaptadores de red



Fuente: Autoria Propia

Con la configuración de virtual box ya terminada, ahora se procede a iniciar la maquina de endian, en donde inicia el proceso de la instalación, para lo cual podemos seleccionar el idioma.

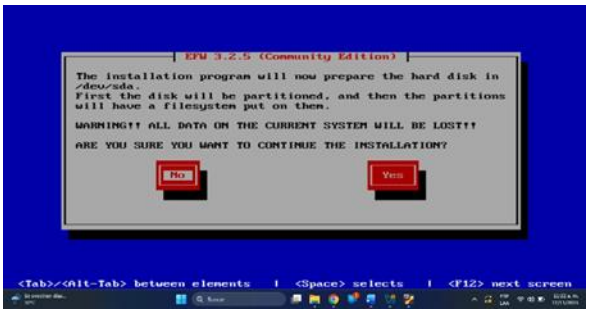
Figura 3. Selección de idioma de instalación



Fuente: Autoría Propia

Como siguiente paso se realiza la partición del disco asignado previamente en la configuración de VirtualBox y su formateo, haciendo clic en la opción de "yes" para que esta se haga de forma automática.

Figura 4. Particionamiento y formateo de disco



Fuente: Autoría Propia

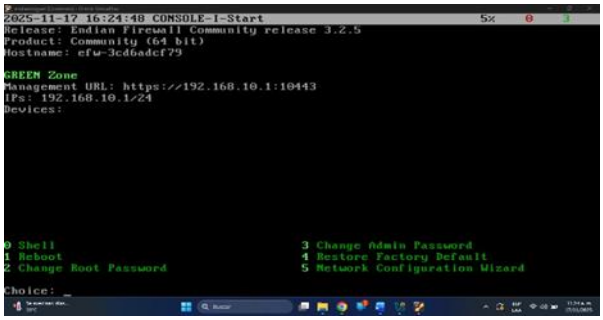
Se continúa estableciendo el segmento de red establecido por parte del grupo colaborativo para la red GREEN, es decir la 192.168.10.1/24 con su respectiva mascara de red.

Figura 5. Configuración red GREEN

Fuente: Autoría Propia

Si la instalación se realizo de forma correcta ya se tiene acceso a endian, en donde se puede visualizar una interfaz con la IP de la red GREEN, configurada previamente. En este apartado se realiza el cambio de las contraseñas de administrador y root para cuando sean necesarias.

Figura 6. Finalización instalación endian



Fuente: Autoría Propia

3 DESARROLLO DE TEMÁTICAS

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

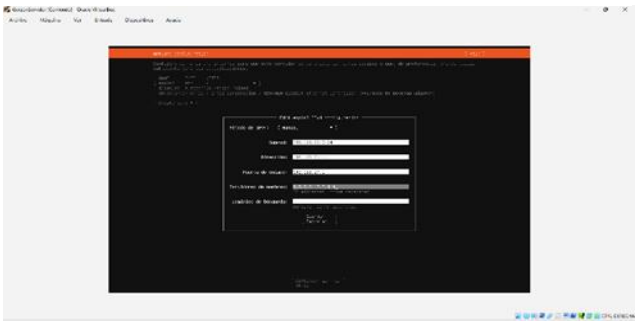
Para la configuración de la instancia para GNU/Linux endian en VirtualBox, iniciamos accediendo a la página oficial, por medio del siguiente enlace; https://sourceforge.net/projects/efw/ en donde podemos descargar la ISO para iniciar con el proceso de instalación:

Figura 7. Página oficial de endian

Fuente: Autoría Propia

Endian es un firewall de nivel empresarial basado en GNU/Linux que se utiliza para proteger redes, segmentarlas y controlar el acceso entre los diferentes dispositivos.

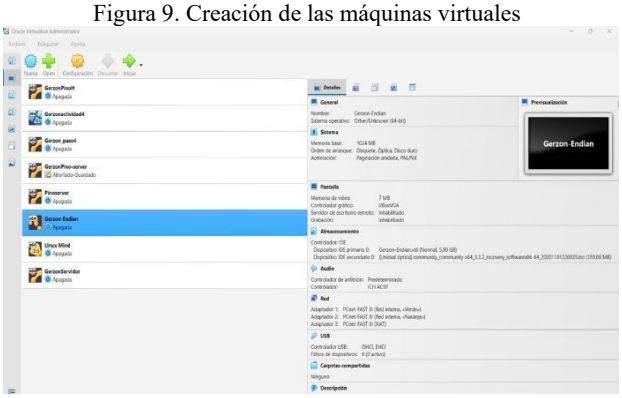
Figura 8. Configuración de IP



Fuente: Autoría Propia

Este sistema utiliza una arquitectura basada en zonas de seguridad.

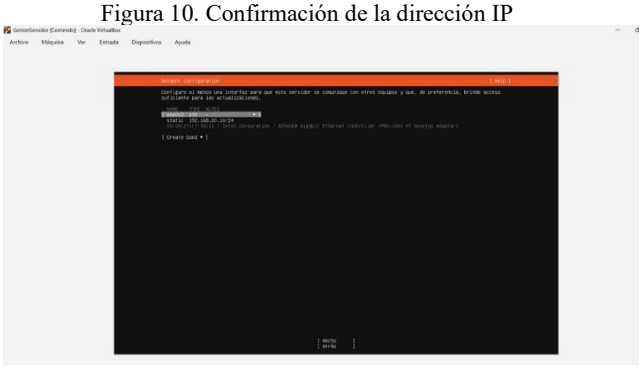
Figura 9. Creación de las máquinas virtuales



Fuente: Autoría Propia

En una infraestructura tecnológica moderna, es fundamental integrar soluciones que permitan controlar el tráfico de red, ofrecer servicios estables y, al mismo tiempo, brindar un entorno amigable para los usuarios. En este contexto, tres componentes juegan un papel clave: endian firewall, linux Mint y un servidor GNU/linux.

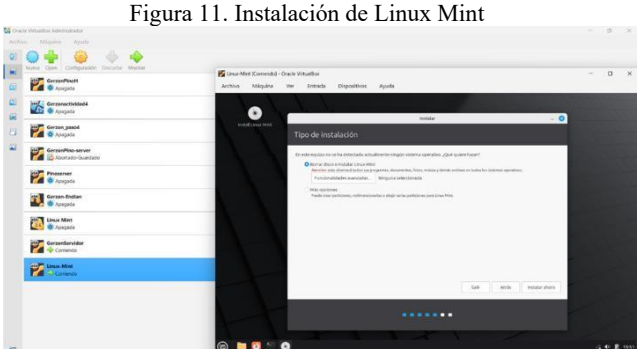
Figura 10. Confirmación de la dirección IP



Fuente: Autoría Propia

Herramienta que bloquea direcciones IP maliciosas tras varios intentos fallidos de autenticación.

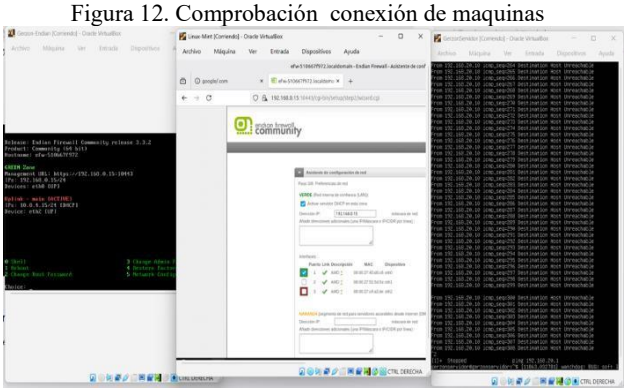
Figura 11. Instalación de Linux Mint



Fuente: Autoría Propia

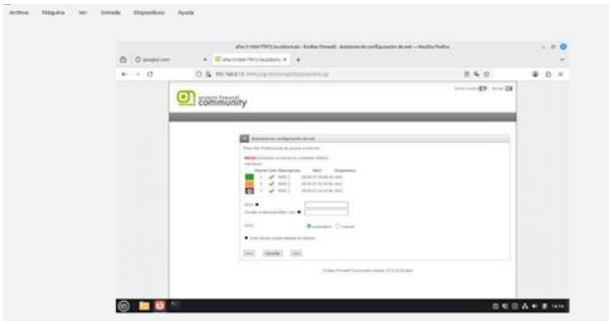
La implementación de seguridad en GNU/Linux debe abordarse como un proceso continuo. No existe una configuración única o definitiva, y cada entorno requiere ajustes específicos según las necesidades y el nivel de exposición al que esté sometido.

Figura 12. Comprobación conexión de maquinas



Fuente: Autoría Propia

Figura 13. Configuraciones de redes

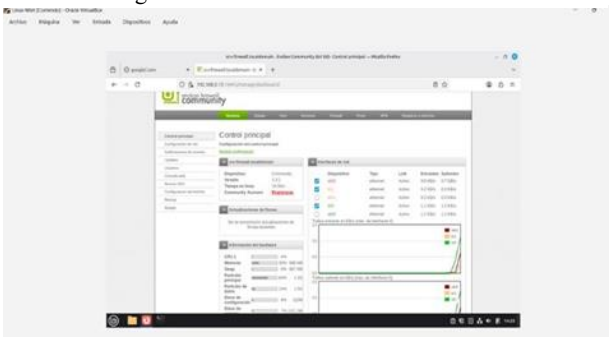


Fuente: Autoría Propia

Puedes ver y editar:

- Acceso entre GREEN ↔ ORANGE
- GREEN ↔ BLUE
- Acceso a internet desde cada red
- Publicación de servicios (DNAT/SNAT)

Figura 14. Visualización de Linux Mint



Fuente: Autoría Propia

Linux Mint trae varios escritorios:

- Cinnamon → el más moderno y completo
- MATE → más liviano
- XFCE → ultraligero

Linux Mint es una distribución GNU/Linux orientada al usuario final, conocida por ser:

- Intuitiva y fácil de usar.
- Liviana.
- Segura.
- Compatible con una amplia variedad de software.

En un entorno de red con endian, Linux Mint se emplea normalmente como estación de trabajo (Desktop) donde el usuario:

- Accede a servicios alojados en el servidor GNU/Linux.
- Navega con seguridad gracias a las políticas de Endian.
- Realiza pruebas de acceso mediante las diferentes redes (GREEN, BLUE, etc.)
- Puede conectarse mediante herramientas como SSH o navegadores web.

Gracias a su sencillez, Linux Mint es utilizado para validar conectividad, probar aplicaciones web internas y gestionar servicios a través de su interfaz gráfica.

Gestión de Usuarios y Permisos

La administración adecuada de usuarios es el primer paso para construir una base de seguridad.

Control de acceso básico

GNU/Linux utiliza un modelo de permisos que define acciones de lectura (r), escritura (w) y ejecución (x). Estos permisos se aplican al propietario del archivo, al grupo y a otros usuarios.

Ejemplo:
ls -l archivo.txt chmod 740 archivo.txt

El comando anterior limita el acceso únicamente al administrador.

Uso de sudo

El archivo /etc/sudoers permite controlar qué usuarios pueden ejecutar comandos administrativos. Esto evita el uso directo del usuario root, reduciendo riesgos por errores o accesos indebidos.

Gestión de contraseñas y políticas

Con herramientas como chage y el módulo PAM se pueden establecer políticas de caducidad, complejidad y reutilización de contraseñas.

Actualizaciones y Mantenimiento del Sistema

Las vulnerabilidades conocidas suelen ser explotadas rápidamente, por lo que se recomienda mantener el sistema actualizado.

En la terminal de Endian se selecciona la opción 5, solicita clave de acceso para ingreso luego muestra la red con los colores asignado y DHCP con herramientas como chage y el módulo PAM se pueden establecer políticas de caducidad, complejidad y reutilización.

3.2 TEMÁTICA 2: CONFIGURACION NAT

Con el desarrollo de la temática, se busca lograr establecer unas reglas de configuración NAT, haciendo uso de endian, un firewall usado por la comunidad de Linux para el despliegue en pequeñas y medianas empresas que lo requieran. Esto debido a que es un firewall tipo software, es decir no necesitas infraestructura fisca, más que la del equipo donde se vaya a realizar la instalación.

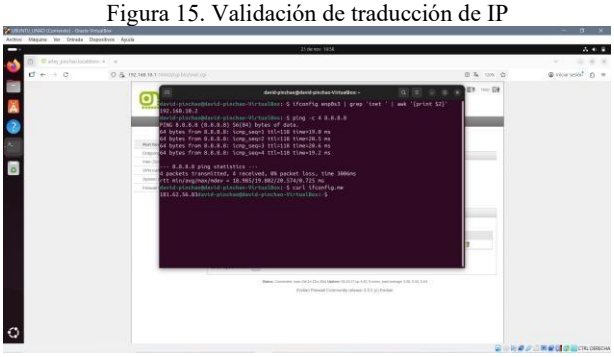
Una vez finalizada la instalación tal como se demostró en el punto 1 de este artículo, procedemos con el desarrollo de esta temática de la siguiente manera:

3.2.1 CONFIGURAR LA REGLA DE NAT (NETWORK ADDRESS TRANSLATION / TRADUCCIÓN DE DIRECCIONES DE RED), DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DESDE LA LAN HACIA LA WAN (RED SIMULADA DE INTERNET).

Para tener acceso a endian es necesario iniciar sesión con la cuenta de administrador y las credenciales configuradas durante la instalación. En el desarrollo de esta parte de la actividad, básicamente se espera que al finalizar la configuración de la regla NAT, se tenga salida a internet desde la red LAN a WAN, con NAT, es decir que se traduzca nuestra IP privada a una publica, para que esta sea la que es visible en la navegación web.

En el apartado de firewall > Source NAT, se hace clic en crear nueva regla, en donde se especifica desde la red GREEN hacia la RED para obtener salida a internet con la traducción de IP de NAT. Una vez realizada la creación de la regla de forma exitosa, podemos validar la traducción de la IP:

Figura 15. Validación de traducción de IP



Fuente: Autoría Propia

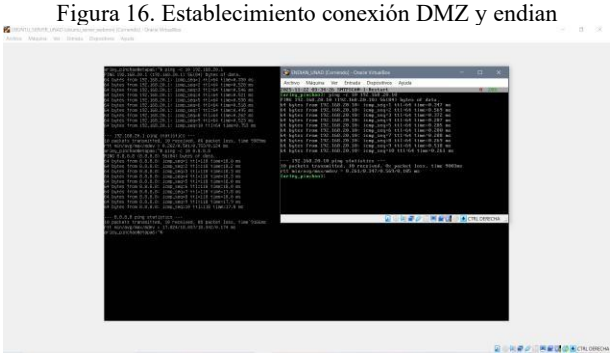
Como podemos evidenciar con el comando curl ifconfig.me se logra establecer que la regla funciona de forma correcta y se traduce la dirección IP 192.168.10.2 a una IP publica 181.62.56.83, es decir que somos visibles con esta última IP y nuestra IP de la LAN queda de forma protegida.

3.2.2 CONFIGURAR LA REGLA DE NAT, DEMOSTRANDO EL ESTABLECIMIENTO DE LA COMUNICACIÓN DE LA ZONA DMZ HACIA LA INTERNET. VERIFICAR EN EL RE-ENVIÓ DE PUERTOS / NAT, LA CREACIÓN DE LAS REGLAS.

Para dar cumplimiento a lo establecido en este ítem del desarrollo de la actividad, se conoce que nuestra red GREEN, RED ya tienen clientes previamente configurados, pero ahora es necesario tener un servidor DMZ es decir ORANGE con una dirección IP configurada dentro de ese mismo segmento en endian. Para esta actividad el grupo concertó establecer el segmento de red 192.168.20.0/24 para los equipos que estarán en la zona desmilitarizada.

Con nuestro servidor DMZ ya configurado en el mismo segmento de red, se procede a validar la comunicación existente entre este y endian, con ayuda del comando ping:

Figura 16. Establecimiento conexión DMZ y endian



Fuente: Autoría Propia

Ahora se realiza la creación de nuestra regla NAT, para la comunicación de DMZ a Internet, en donde en el apartado Source Network Address Translation en donde se permite que DMZ tenga salida Internet por medio de la traducción de IP, para ello configuramos la regla de la siguiente manera:

Figura 17. Creación de regla NAT

Fuente: Autoría Propia

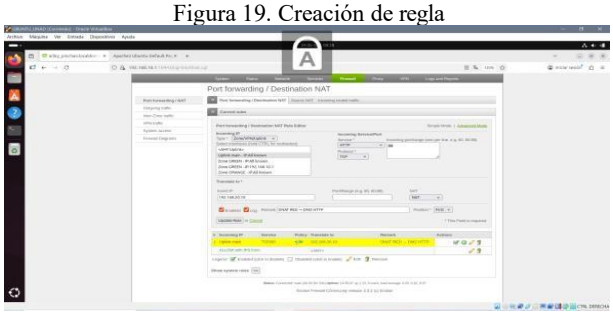
Ahora se comprueba que la salida a la RED desde el servidor DMZ por medio de la regla creada realizando ping al DNS, esto generar tráfico y en el apartado de logs and reports de la interfaz gráfica de Endian, se evidencia que la regla NAT se cumple porque traduce la dirección del servidor DMZ a una IP publica, así:

Figura 18. Validación de regla

Fuente: Autoría Propia

Continuando con el desarrollo de la actividad ahora se verifica el reenvío de puertos, para ello en el apartado de firewall – Port forwarding / Destination NAT, se realiza la creación de la regla que nos permitirá que desde un equipo en RED tener acceso a nuestro servidor DMZ configurado previamente, entonces se crea la regla y la aplicamos:

Figura 19. Creación de regla



Fuente: Autoría Propia

Con la regla ya creada, ahora desde un equipo en red (ubuntu desktop) se accede mediante la IP publica de endian que nos entrega por DHCP, si esta funciona, se puede acceder al servidor en la DMZ haciendo uso de esa IP y se confirma así el reenvío de puertos:

Figura 20. Validación regla DMZ

Fuente: Autoría Propia

Misma forma se puede validar en los logs and reports de endian y se evidencia que el cliente 192.168.20.2 accedió al puerto 80 y fue redirigido al servidor DMZ de IP 192.168.20.10, lo que nos indica que la regla DNAT está funcionando de forma correcta.

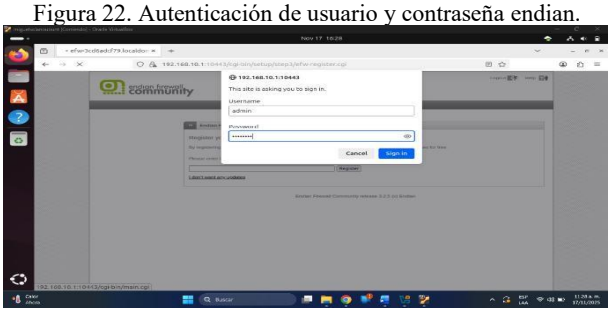
Figura 21. Validación regla DNAT

Fuente: Autoría Propia

3.3 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.

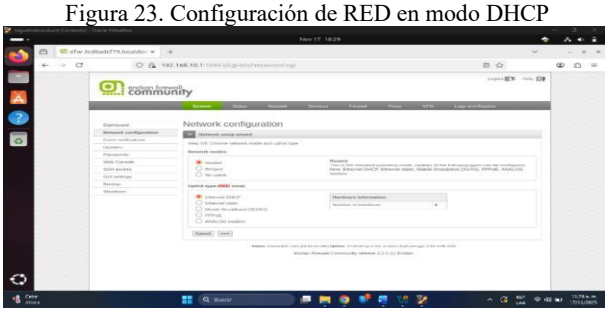
Figura 22. Autenticación de usuario y contraseña endian.



Fuente: Autoría Propia

Desde desktop accedemos a endian por medio de https://192.168.10.1:10443 y se inicia sesión con las credenciales.

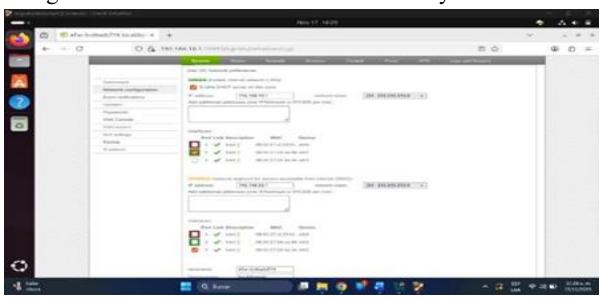
Figura 23. Configuración de RED en modo DHCP



Fuente: Autoría Propia

Se confirma la configuración de RED (WAN).

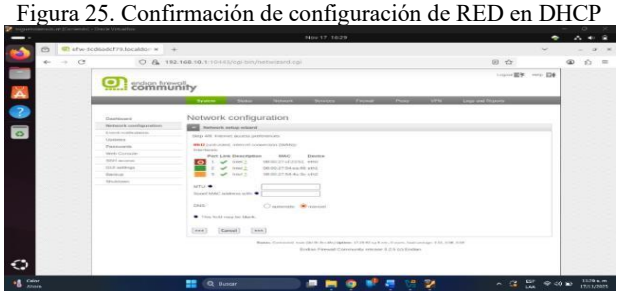
Figura 24. Confirmación de IP de GREEN y ORANGE



Fuente: Autoría Propia

Se valida la configuración de GREEN y ORANGE con sus respectivas IP.

Figura 25. Confirmación de configuración de RED en DHCP



Fuente: Autoría Propia

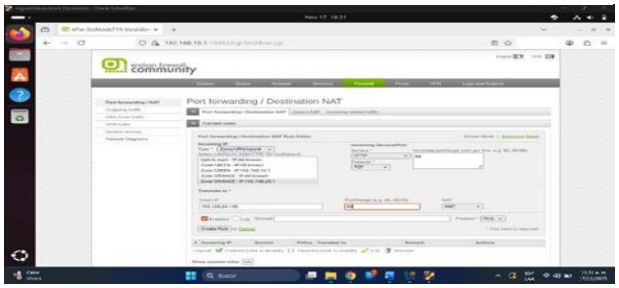
Confirmamos eth0 para RED.

Figura 26. Ingresamos al módulo firewall.

Fuente: Autoría Propia

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

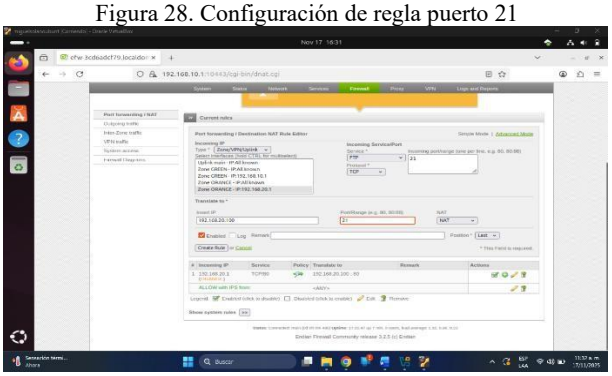
Figura 27. Configuración de reglas puerto 80



Fuente: Autoría Propia

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.

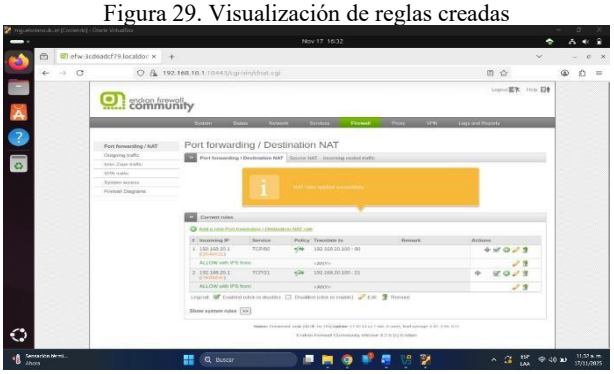
Figura 28. Configuración de regla puerto 21



Fuente: Autoría Propia

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.

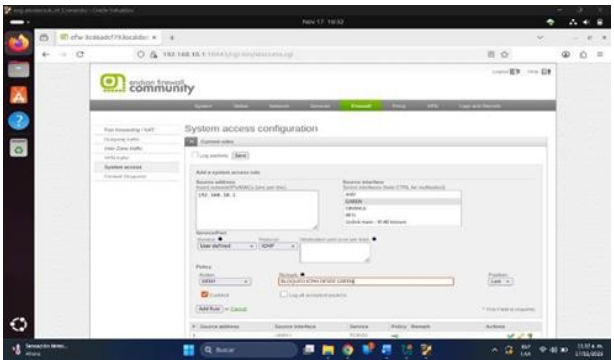
Figura 29. Visualización de reglas creadas



Fuente: Autoría Propia

Con las reglas creadas correctamente, ahora se procede a la configuración del bloqueo para ICPM.

Figura 30. configuración de bloqueo para ICMP



Fuente: Autoría Propia

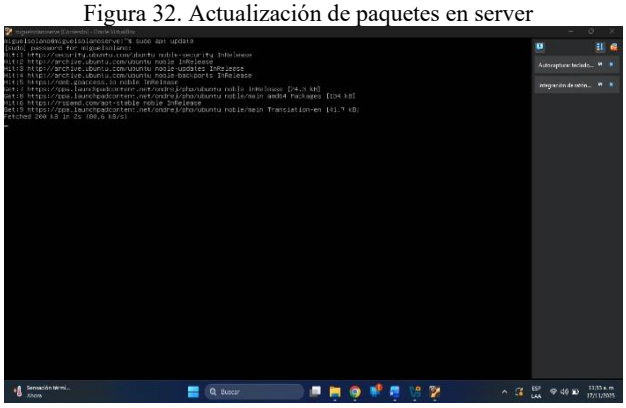
Regla de firewall en endian firewall para bloquear el tráfico ICMP desde la IP 192.168.10.1 en la interfaz GREEN (DMZ), con acción de denegar el tráfico. La regla está habilitada y aplicada.

Figura 31. Visualización de bloqueo

Fuente: Autoría Propia

El bloqueo fue creado de forma correcta, para realizar las pruebas respectivas, se procede a la actualización de paquetes en ubuntu server.

Figura 32. Actualización de paquetes en server



Fuente: Autoría Propia

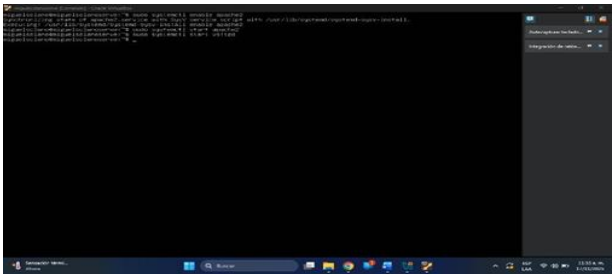
Al finalizar la actualización de paquetes, se continua con la instalación de paquete y el protocolo de transferencia de archivos denominado FTP.

Figura 33. Instalación de apache y FTP en server.

Fuente: Autoría Propia

Ahora con la instalación ya realizada de apache y FTP, se realiza la configuración de servicios en el servidor de ubuntu.

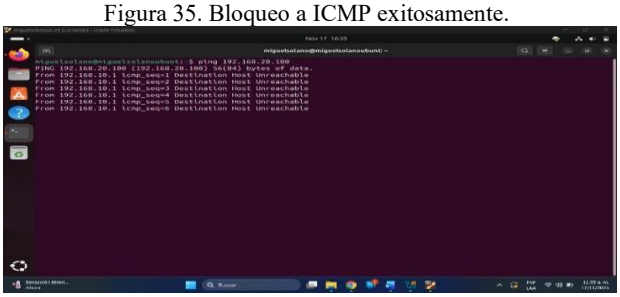
Figura 34. Configuración de servicios en server



Fuente: Autoría Propia

Ya con los servicios previamente configurados, se puede realizar la prueba del bloqueo del ICPM desde ubuntu desktop, por medio del comando ping.

Figura 35. Bloqueo a ICMP exitosamente.



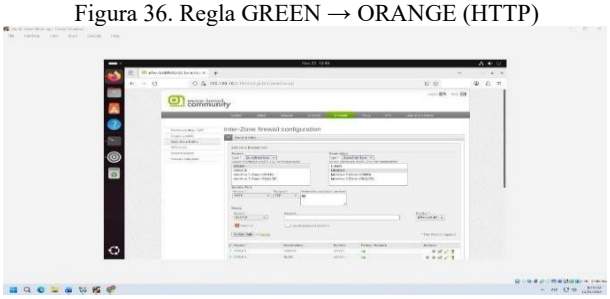
Fuente: Autoría Propia

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.

3.4 TEMÁTICA 4: REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO. PRODUCTO ESPERADO.

Se creó una regla de firewall inter-zona que permite el tráfico HTTP (puerto 80) desde la zona VERDE (LAN) hacia la zona NARANJA (DMZ). Esta regla garantiza que los equipos de la LAN puedan acceder al servidor web alojado en la DMZ.

Figura 36. Regla GREEN → ORANGE (HTTP)



Fuente: Autoría Propia

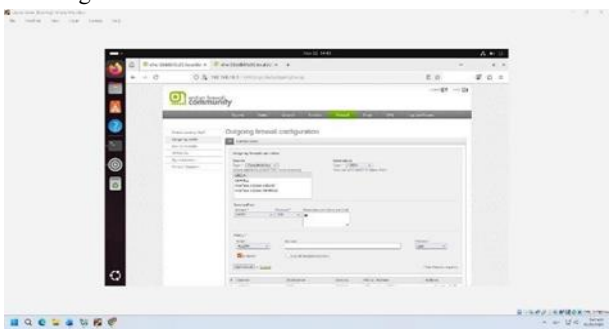
Se configuró una regla de firewall que permite el tráfico FTP (puerto 21) desde la zona VERDE hacia la zona NARANJA. Esta regla habilita el acceso de los equipos de la LAN al servidor FTP publicado en la DMZ.

Figura 37. Regla GREEN → ORANGE (FTP)

Fuente: Autoría Propia

En esta imagen se muestra la creación de la regla de tráfico saliente (Outgoing Traffic) que permite el servicio HTTP (puerto 80/TCP) desde la zona LAN (GREEN) hacia la zona WAN (RED). Esta configuración garantiza que los equipos de la red interna puedan acceder a páginas web.

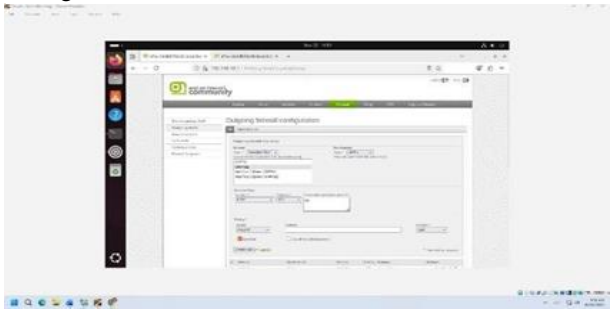
Figura 38. Permitir HTTP desde LAN hacia internet



Fuente: Autoría Propia

En esta imagen se muestra la creación de la regla de tráfico saliente (Outgoing Traffic) que permite el servicio HTTP (puerto 80/TCP) desde la zona DMZ (ORANGE) hacia la zona WAN (RED). Esta regla es necesaria para que el servidor ubicado en la DMZ pueda acceder a recursos externos, incluyendo servicios web en Internet, cumpliendo con el requerimiento de comunicación hacia la WAN.

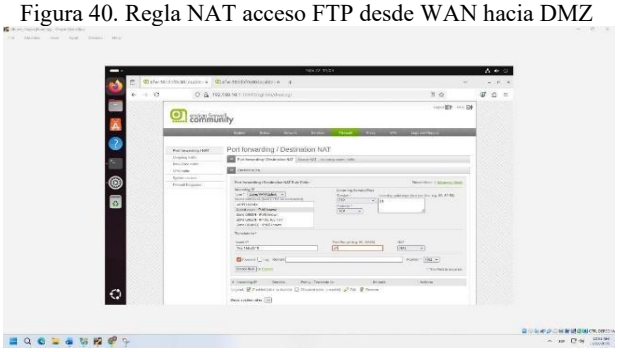
Figura 39. Permitir HTTP desde la DMZ hacia Internet.



Fuente: Autoría Propia

Se crea la regla de Destination NAT que permite el servicio FTP (puerto 21) desde la WAN hacia el servidor en la zona DMZ (192.168.20.10). Esta regla habilita que clientes externos accedan al servicio FTP ubicado en la DMZ.

Figura 40. Regla NAT acceso FTP desde WAN hacia DMZ



Fuente: Autoría Propia

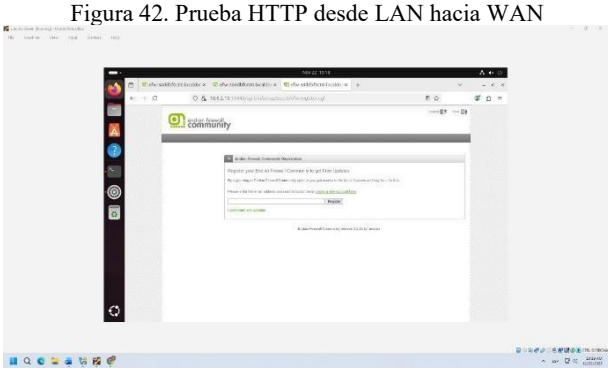
La imagen muestra la correcta visualización del servicio HTTP expuesto en la zona DMZ, accedido desde la zona WAN mediante la regla de Port Forwarding configurada en endian firewall.

Figura 41. Prueba HTTP desde WAN hacia servidor DMZ

Fuente: Autoría Propia

Prueba de acceso HTTP desde la LAN hacia la WAN, verificando que el tráfico HTTP generado desde la zona GREEN hacia la zona RED es permitido por las reglas de firewall configuradas.

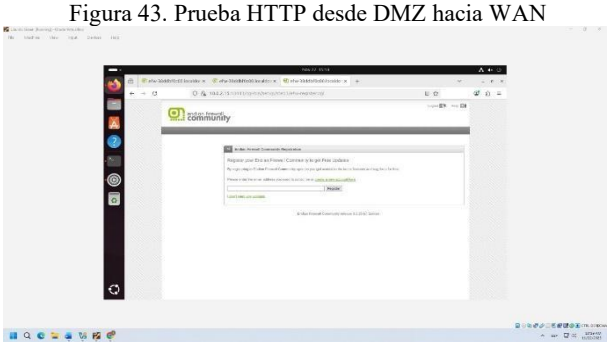
Figura 42. Prueba HTTP desde LAN hacia WAN



Fuente: Autoría Propia

La imagen evidencia que la zona ORANGE (DMZ) puede generar tráfico HTTP hacia la zona RED (WAN). Esto confirma que las reglas de salida permiten el acceso desde la DMZ hacia la WAN, según lo requerido en la temática.

Figura 43. Prueba HTTP desde DMZ hacia WAN



Fuente: Autoría Propia

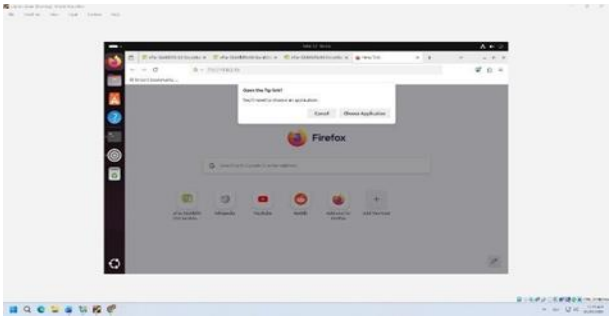
La captura muestra el intento de conexión desde la zona GREEN hacia la WAN (10.0.2.15) mediante el puerto FTP (21). El resultado “Connection timed out” evidencia que el tráfico FTP hacia la WAN está bloqueado por las reglas del firewall de endian, cumpliendo la directiva solicitada.

Figura 44. Prueba de conexión FTP desde LAN hacia WAN

Fuente: Autoría Propia

La imagen muestra el intento de conexión FTP (ftp://10.0.2.15:21) desde la zona WAN hacia el servidor en la zona DMZ. El navegador detecta el enlace FTP y solicita elegir una aplicación para abrirlo, evidenciando que el servicio FTP está siendo redirigido correctamente mediante la regla de Port Forwarding configurada en endian.

Figura 45. Acceso FTP desde la WAN hacia zona DMZ



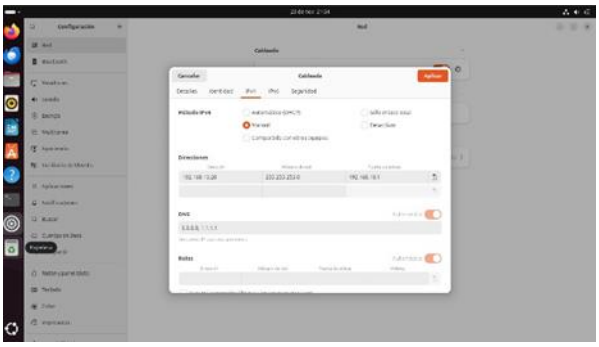
Fuente: Autoría Propia

3.5 TEMÁTICA 5: PERMITIR SERVICIOS DE LA ZONA DMZ PARA LA RED.

1. Crear un perfil y establecer una lista negra bloqueando los siguientes sitios como Hotmail, YouTube y el nuevo día.

En ubuntu Desktop, mediante la configuración de red, se procede a realizar la asignación de una dirección IP dentro de nuestro segmento de red.

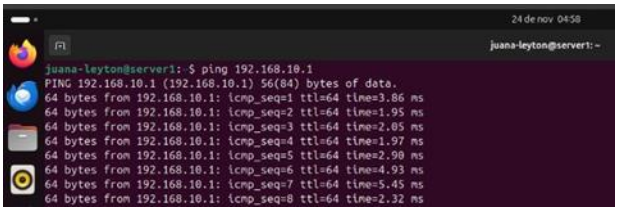
Figura 46. Se realiza configuración de red



Fuente: Autoría Propia

Se valida conexión desde ubuntu desktop por medio del comando ping con endian, obteniendo respuesta exitosa, lo que nos indica que la configuración de red es la correcta.

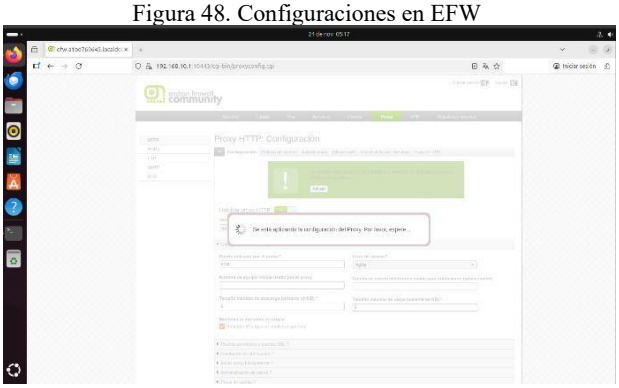
Figura 47. Comprobación de conexión



Fuente: Autoría Propia

Se accede a la interfaz gráfica de endian en donde se podrá hacer la configuración de la lista negra de los sitios establecidos.

Figura 48. Configuraciones en EFW

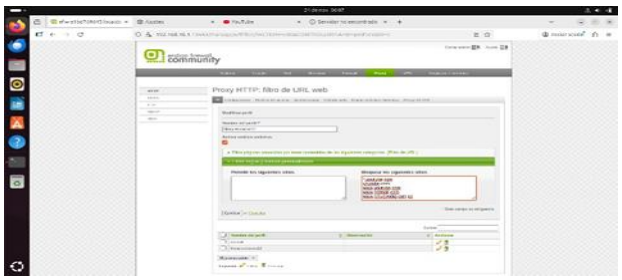


Fuente: Autoría Propia

2. Autenticación por usuario: A través de la opción proxy cree un usuario y asócielo a un grupo. Establezca una política de acceso y vincule el perfil creado en el punto anterior y relaciónelo también con la política de autenticación.

Se crea el perfil y la configuración de las páginas en la lista negra.

Figura 49. Creación de lista negra



Fuente: Autoría Propia

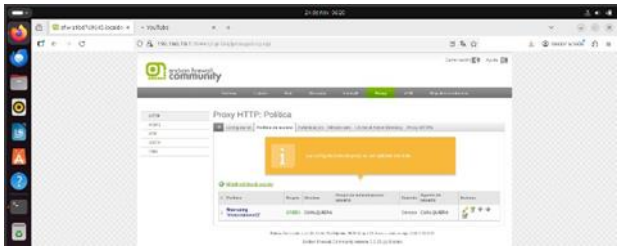
En el aparatado de proxy HTTP autenticacion de la interfaz grafica de endian, se crea el usuario y grupo.

Figura 50. Creación de usuario y grupo

Fuente: Autoría Propia

En proxy HTTP ploitica, se agrega una nueva la politica, para la negracion de servicios a lista negra.

Figura 51. Creación de política.



Fuente: Autoría Propia

Se realizan ajustes en ubuntu desktop, en el navegador Firefox, para poder realizar las respectivas pruebas.

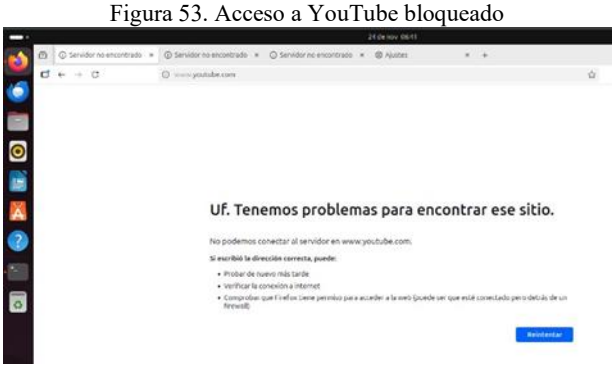
Figura 52. Configuración del navegador

Fuente: Autoría Propia

3. Probar desde la LAN a través de un navegador Web, el acceso a los portales referenciados en la lista negra.

Por medio de ubuntu desktop, que previamente fue configurado con una IP de la red LAN, procedemos acceder al navegador y intentamos acceder a uno de los portales de la lista negra, con el fin de realizar de la comprobación de este paso.

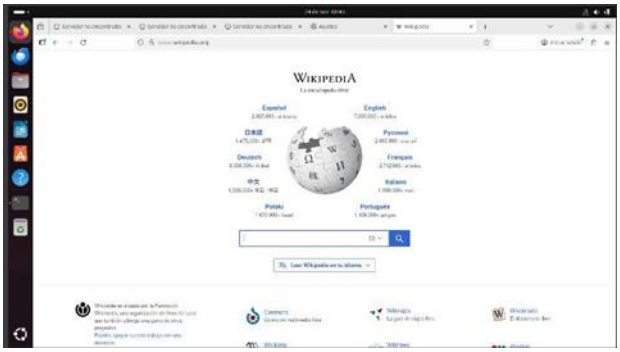
Figura 53. Acceso a YouTube bloqueado



Fuente: Autoría Propia

Desde este mismo navegador accedemos a otra página fuera de la lista negra y evidenciamos que esta accede sin problemas puesto que esta no está incluida en la lista negra.

Figura 54. Acceso a Wikipedia permitido.



Fuente: Autoría Propia

4 CONCLUSIONES

En la temática 1, GNU/Linux proporciona una base sólida para construir sistemas seguros, pero requiere la configuración adecuada para garantizar la protección de los servicios y de la información. La aplicación de buenas prácticas, el uso de firewalls, el monitoreo constante y las auditorías periódicas constituyen pilares fundamentales en la administración segura del sistema. Este artículo ha presentado procedimientos esenciales para fortalecer un servidor Linux, demostrando que la seguridad no es una función aislada, sino un conjunto de estrategias interrelacionadas. a aplicación de la seguridad. El marco de virtualización proporcionado por VirtualBox permitió un entorno de pruebas eficiente y controlado. La división de la red en zonas distintas mejora la seguridad al aislar servicios críticos y limitar la exposición.

En cuanto a la temática 2 correspondiente a la configuración NAT, fue necesario abordar las referencias bibliográficas con el fin de realizar la creación de las diferentes reglas NAT por medio del firewall de endian, en donde podemos establecer como queremos establecer comunicación con la traducción de IP en donde, podemos establecer conexión a internet por medio de una IP publica, sin exponer nuestro segmento de red. Con esto también podemos tener ahorros de IP, pues nuestros equipos harán uso de una sola IP para la conexión, esto en vista de las escasas direcciones de IPV4 que existen en la actualidad. Otra de las grandes ventajas de la configuración de reglas NAT, es que permite la redirección de puertos, permitiendo dirigir algún tráfico en específico hacia un servicio interno, esto debido al mapeo de puertos.

Para la temática 3, las pruebas de conectividad HTTP y FTP demostraron que es crucial revisar minuciosamente las reglas de firewall y NAT para garantizar que los servicios estén disponibles en la red. Los registros de tráfico mostraron que algunas conexiones fueron rechazadas, lo que indica que las reglas aún deben ajustarse para permitir ciertos tipos de tráfico. Garantizar una configuración correcta en las interfaces y servicios mejora tanto el acceso como la seguridad de la red, evitando bloqueos innecesarios y asegurando un control adecuado del tráfico entrante y saliente.

El desarrollo de la Temática 4 permitió comprender de forma integral la importancia del control de acceso entre zonas de seguridad dentro de una arquitectura perimetral basada en endian firewall. A través de la configuración de reglas entre las zonas GREEN, ORANGE y RED fue posible establecer un flujo de comunicación estructurado y restringido, donde únicamente los servicios autorizados pueden circular entre segmentos con diferentes niveles de seguridad. Este proceso evidenció cómo la segmentación y la creación de políticas adecuadas se convierten en pilares fundamentales para garantizar la protección de los recursos expuestos y evitar accesos indebidos.

El desarrollo de la temática 5 permitió fortalecer la comprensión del funcionamiento interno de GNU/Linux desde una perspectiva orientada a la seguridad del sistema. A través de ejercicios prácticos, se profundizó en temas como la identificación de dispositivos, el manejo de módulos del kernel, la interpretación del proceso de arranque y el uso de herramientas de diagnóstico como dmesg, journalctl y comandos del sistema. Asimismo, se consolidó el manejo de los esquemas de inicialización SysVinit y systemd, esenciales para la administración eficiente de servicios y la disponibilidad del sistema. En conjunto, estos conocimientos fortalecen las capacidades del administrador para anticipar fallos, responder a incidentes y aplicar configuraciones que garanticen un entorno seguro, estable y alineado con las buenas prácticas en sistemas operativos GNU/Linux.

5 REFERENCIAS

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

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

[3] Debian (2023). El manual del administrador de Debian 12.5.0.Debian https://www.debian.org/releases/stable/amd64/index.es.html
[4] Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/
[5] Endian (2016), Endian UTM 3.2 Manual referencia. Endian. http://docs.endian.com/3.2/utm/index.html
[6] Jay LaCroix. (2020). Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting.
[7] Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c- 94a8-f12e88b41952
[8] Nemeth, E., Snyder, G., Hein, T. UNIX and Linux System Administration Handbook. Addison-Wesley.
[9] Cooper, A., "Linux Hardening Techniques," Journal of Cybersecurity, vol. 12, 2023.
[10] Team, "Security Best Practices," Canonical Documentation.