IMPLEMENTACIÓN Y CONFIGURACIÓN DE UN CORTAFUEGOS MULTIZONA GNU/LINUX ENDIAN EN VIRTUALBOX CON SERVICIOS NAT, DMZ Y PROXY HTTP AUTENTICADO

María Celeste Muñoz Ibagon
e-mail: mcmunozi@unadvirtual.edu.co
Brayan Estiven Muñoz Semanate
e-mail: bemunozs@unadvirtual.edu.co
Juan David Delgado Macias
e-mail: jddelgadomac@unadvirtual.edu.co
Harold Andrés Salamanca Ortega
e-mail: hasalamancao@unadvirtual.edu.co

RESUMEN: *El presente proyecto describe la implementación de una infraestructura de red segura utilizando GNU/Linux Endian (EFW) como firewall principal y un servidor web ubicado en la zona DMZ. Se realizó la configuración de las zonas de red (verde, roja y naranja), estableciendo reglas específicas para permitir servicios HTTP y FTP, y negar el protocolo ICMP, reforzando así la seguridad perimetral. Además, se implementó un proxy HTTP no transparente con autenticación de usuarios y políticas de acceso, permitiendo el bloqueo de sitios web específicos mediante una lista negra. Se crearon perfiles de usuario y se asignaron permisos diferenciados, verificando el acceso desde la LAN para confirmar la efectividad de las restricciones. Los resultados obtenidos demuestran que la solución propuesta mejora significativamente el control de acceso, la segmentación de la red y la protección de los recursos internos, consolidando un entorno de red robusto, confiable y adaptable a las necesidades de la organización.*

PALABRAS CLAVE: Seguridad perimetral, Firewall, Red LAN, Red WAN, DMZ (Zona Desmilitarizada), GNU/Linux Endian (EFW), Proxy HTTP, Autenticación de usuarios, Política de acceso, Lista negra, Redes seguras, Endian, FTP, Servidor, Protocolo ICMP, Segmentación de red, Control de acceso, NAT, Port Forwarding, Virtualización, Ubuntu Server.

ABSTRACT: *This project describes the implementation of a secure network infrastructure using GNU/Linux Endian (EFW) as the main firewall and a web server located in the DMZ zone. The network zones (green, red, and orange) were configured, with specific rules established to allow HTTP and FTP services while blocking the ICMP protocol, thereby strengthening perimeter security. Additionally, a non-transparent HTTP proxy was implemented with user authentication and access policies, allowing the blocking of specific websites through a blacklist. User profiles were created with differentiated permissions, and access from the LAN was tested to confirm the effectiveness of the restrictions. The results obtained show that the proposed solution significantly improves access control, network segmentation, and the protection of internal resources, establishing a robust, reliable, and adaptable network environment tailored to the organization's needs.*

KEYWORDS: Perimeter security, Firewall, LAN, WAN, DMZ (Demilitarized Zone), GNU/Linux Endian (EFW), HTTP, Proxy, User authentication, Access policy, Blacklist, Secure networks, Endian, FTP, Server, ICMP protocol, Network segmentation, Access control, NAT, Port Forwarding, Virtualization, Ubuntu Server.

1 INTRODUCCIÓN

La protección de la infraestructura de red es esencial para cualquier organización que gestione información crítica. La seguridad perimetral, apoyada en la segmentación de la zona roja mediante como la DMZ, permite aislar servicios expuestos al exterior y proteger los activos internos. En este contexto, GNU/Linux Endian (EFW) se posiciona como una solución robusta para la gestión de firewalls y políticas de acceso, facilitando la administración de tráfico entre la LAN, la DMZ y la WAN. El presente trabajo aborda la instalación y configuración de Endian, la creación de reglas de firewall para habilitar servicios y restringir protocolos, y la implementación de un proxy HTTP con autenticación y filtrado de contenidos. A través de estas acciones, se busca fortalecer la seguridad, controlar el acceso a Internet y garantizar la integridad de los recursos internos, demostrando la importancia de una arquitectura de red bien segmentada y gestionada.

En el ámbito de la seguridad de redes, la implementación de una Zona Desmilitarizada (DMZ) se erige como una estrategia fundamental para proteger la red interna de una organización de posibles amenazas externas. La DMZ actúa como una zona de amortiguamiento que aloja servicios accesibles desde internet, separándolos de los activos críticos de la red interna. En esta temática, exploraremos la configuración de servicios específicos dentro de una DMZ, centrándonos en habilitar el acceso a los servicios web (HTTP en el puerto 80) y de transferencia de archivos (FTP en el puerto 21) desde un servidor Ubuntu Server ubicado en esta zona. Además, abordamos la importancia de restringir ciertos protocolos, como ICMP (puertos 8 y 30), para fortalecer la seguridad al evitar la detección y exploración de la red mediante la denegación de la respuesta a comandos ping. A través de la configuración de reglas de firewall, verificamos la correcta implementación de estas políticas de seguridad, tanto en la habilitación de los servicios deseados como en el bloqueo del tráfico no permitido.

2 INSTALACION ENDIAN

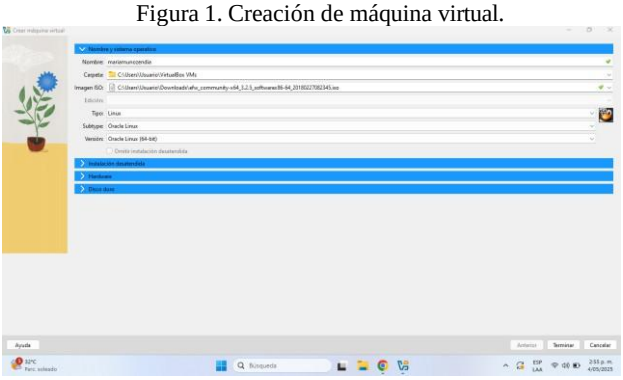
2.1 CARACTERÍSTICAS GENERALES

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 VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

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

2.2 INSTALACION

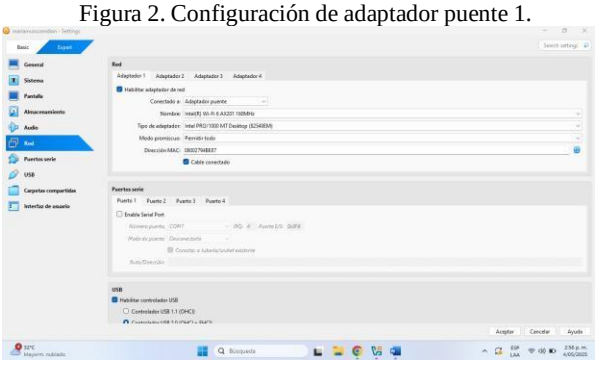
Figura 1. Creación de máquina virtual.



Fuente: Autoría propia (María Muñoz)

Creación de Máquina Virtual Endian.

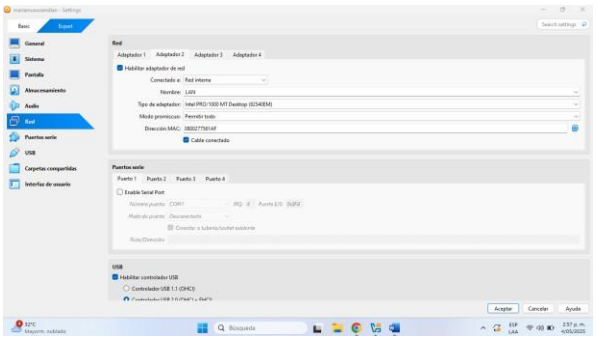
Figura 2. Configuración de adaptador puente 1.



Fuente: Autoría propia (María Muñoz)

En el adaptador 1 de red lo configuramos como adaptador puente RED.

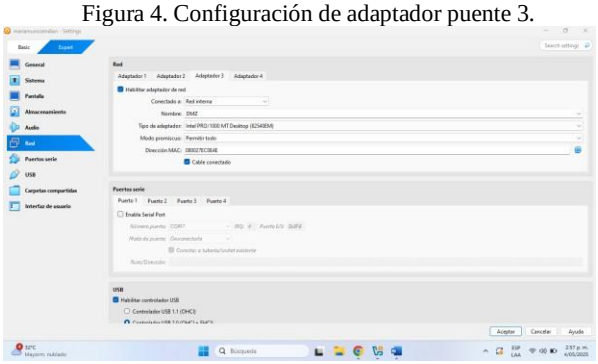
Figura 3. Configuración de adaptador puente 2.



Fuente: Autoría propia (María Muñoz)

Configuramos el adaptador 2 como red interna LAN GREEN.

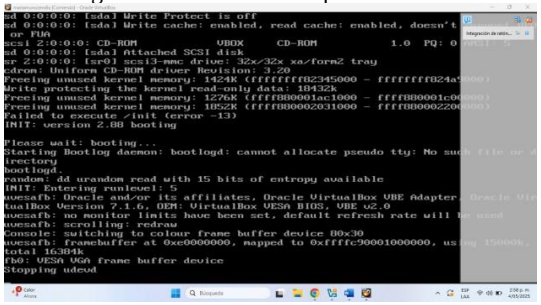
Figura 4. Configuración de adaptador puente 3.



Fuente: Autoría propia (María Muñoz)

Configuramos el adaptador 3 como red interna DMZ ORANGE.

Figura 5. Iniciamos la máquina virtual de Endian.

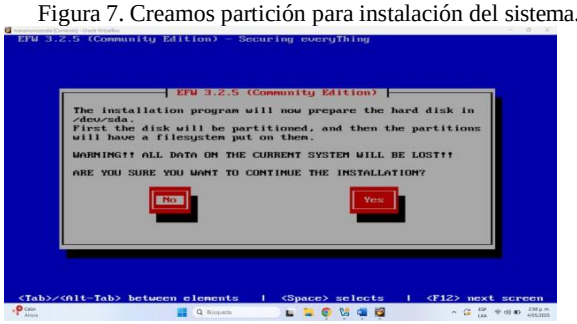


Fuente: Autoría propia (María Muñoz)
Iniciamos la máquina virtual de endian.

Figura 6. Escogemos el idioma.

Fuente: Autoría propia (María Muñoz)
Escogemos el idioma.

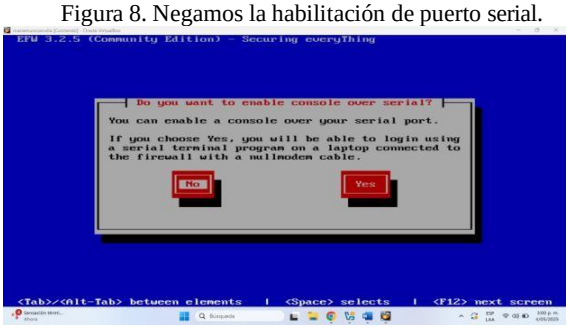
Figura 7. Creamos partición para instalación del sistema.



Fuente: Autoría propia (María Muñoz)

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

Figura 8. Negamos la habilitación de puerto serial.



Fuente: Autoría propia (María Muñoz)

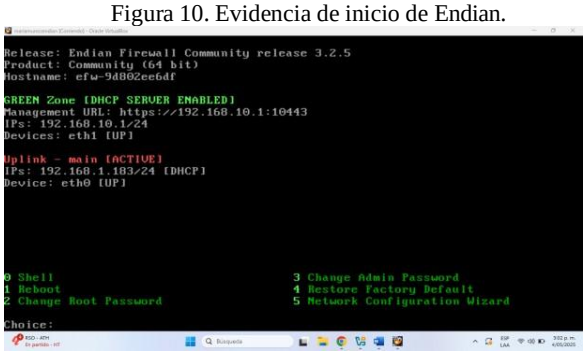
Seleccionamos "No" porque no necesitamos habilitar el acceso al firewall a través de un puerto serial.

Figura 9. Establecimiento de ip GREEN.

Fuente: Autoría propia (María Muñoz)

Establecemos la ip y la máscara de GREEN.

Figura 10. Evidencia de inicio de Endian.



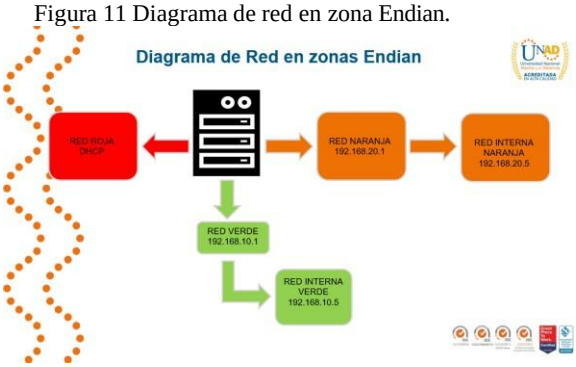
Fuente: Autoría propia (María Muñoz)

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

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

Producto esperado: Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

Figura 11 Diagrama de red en zona Endian.



Fuente: Autoría propia (Harold Salamanca)

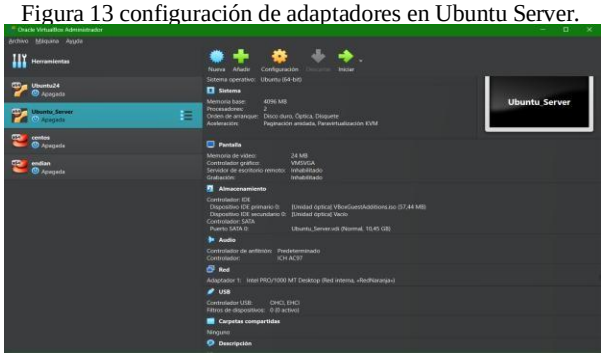
Nos enseña el diagrama con las direcciones ip, el cual se llevará a cabo en el ejercicio.

Figura 12 configuración de adaptadores en Endian.

Fuente: Autoría propia (Harold Salamanca)

Configuramos los adaptadores de red el servidor Endian, adaptador 1 con la red interna verde, adaptador 2 con red interna naranja y adaptador 3 con NAT de internet.

Figura 13 configuración de adaptadores en Ubuntu Server.



Fuente: Autoría propia (Harold Salamanca)

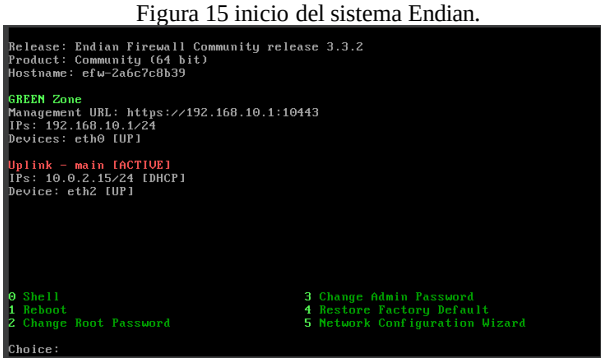
Configuramos los adaptadores de red el servidor Ubuntu, adaptador 1 con la red interna Naranja.

Figura 14 configuración de adaptadores en Ubuntu cliente.

Fuente: Autoría propia (Harold Salamanca)

Configuramos los adaptadores de red el cliente Ubuntu, adaptador 1 con la red interna verde.

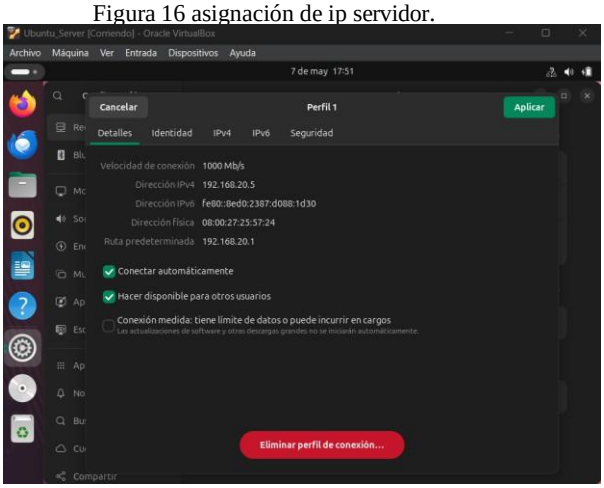
Figura 15 inicio del sistema Endian.



Fuente: Autoría propia (Harold Salamanca)

Se inicia el sistema Endian, cargando el kernel y los drivers de red, Muestra mensajes de arranque indicando detección de hardware de red. La cual la verde es 192.168.10.1.

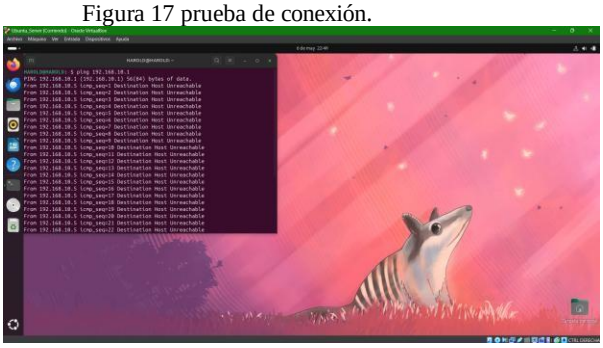
Figura 16 asignación de ip servidor.



Fuente: Autoría propia (Harold Salamanca)

Asignamos la dirección ip al servidor la cual estructuramos con la puerta de entrada 192.168.20.1.

Figura 17 prueba de conexión.



Fuente: Autoría propia (Harold Salamanca)

Probamos conexión en el servidor por medio de ping, dando como resultado una conexión sin datos.

Figura 18 prueba de conexión.

Fuente: Autoría propia (Harold Salamanca)

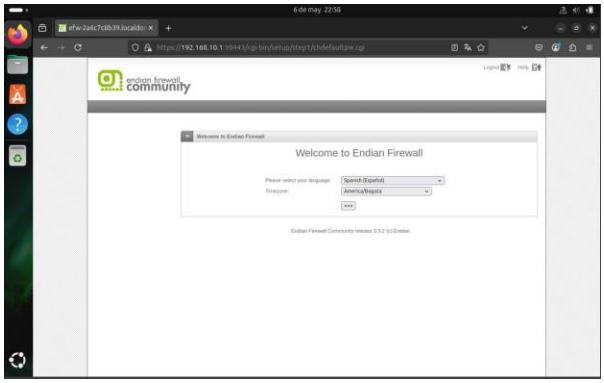
Se verificó la conectividad desde el cliente Ubuntu, lo que indica una conexión exitosa.

Figura 19 Proceso de instalación desde navegador.

Fuente: Autoría propia (Harold Salamanca)

En el navegador escribimos la ip recomendada 192.168.10.1 e ingresamos.

Figura 20 configuración.



Fuente: Autoría propia (Harold Salamanca)

Configuramos el idioma y la zona horaria, aceptamos términos.

Figura 21 contraseñas

Fuente: Autoría propia (Harold Salamanca)

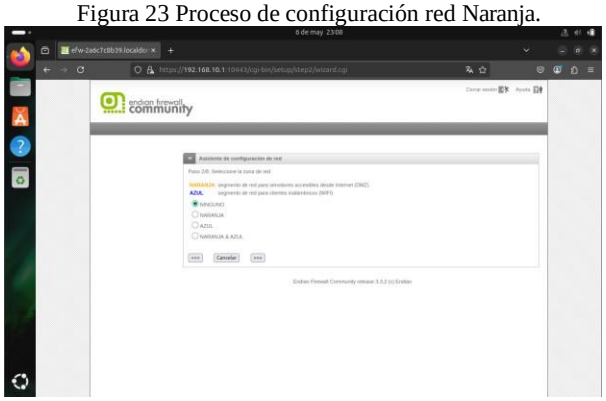
Se agregan contraseñas para el admin y para el root. E ingresamos.

Figura 22 Verificación de red roja.

Fuente: Autoría propia (Harold Salamanca)

Vamos a la instalación de las diferentes áreas, la cual nos muestra por donde ingresa el internet y vemos que es por la red roja, el modo de la red es enrutamiento y va recibir por ethernet el DHCP y tiene 3 tarjetas de red configuradas el servidor de Endian.

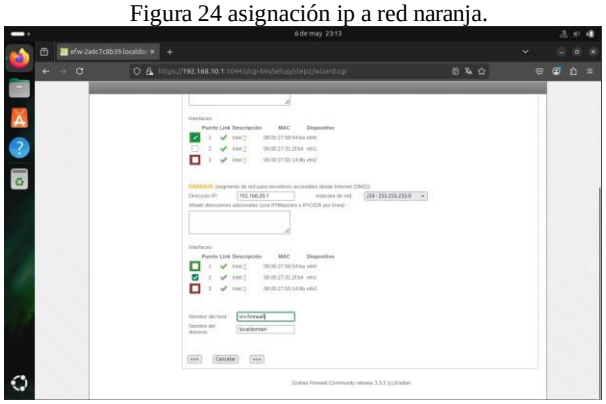
Figura 23 Proceso de configuración red Naranja.



Fuente: Autoría propia (Harold Salamanca)

Se selecciona la red a configurar, en este caso es la red naranja.

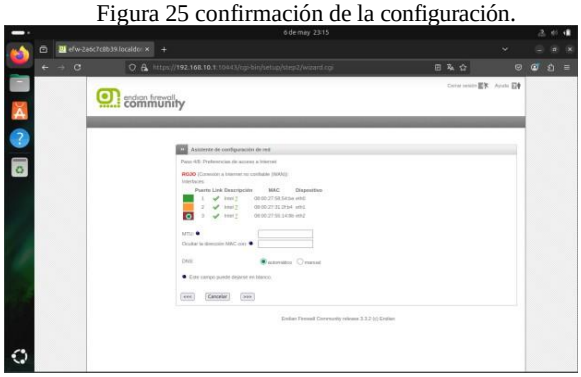
Figura 24 asignación ip a red naranja.



Fuente: Autoría propia (Harold Salamanca)

Esta interfaz nos muestra la configuración de nuestras redes y configuramos la red naranja con la ip 192.168.20.1 y el nombre del servidor como srv-firewall.

Figura 25 confirmación de la configuración.



Fuente: Autoría propia (Harold Salamanca)

Confirmamos la configuración de las redes la verde con su Mac, la red naranja, y la red roja que es el internet.

Figura 26 Endian Firewall en navegador

Fuente: Autoría propia (Harold Salamanca)

Al aceptar los cambios y configuraciones se direcciona la interfaz web de Endian Firewall Community, donde se ve: Estado del sistema y gráficos de uso de red.

Interfaces de red: eth0, eth1, br0, br1, etc.

Esto indica que se está usando Endian como cortafuegos/router, administrando las conexiones entre diferentes interfaces de red.

Figura 27 prueba Terminal de Ubuntu Server.

Fuente: Autoría propia (Harold Salamanca)

Se están recibiendo respuestas exitosas (64 bytes from 192.168.20.1) con tiempos de latencia (time=… ms). Esto indica que hay conectividad entre el servidor Ubuntu y el 6ateway o dispositivo con IP 192.168.20.1.

Se nota el cambio que ha realizado al momento de aceptar las configuraciones.

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

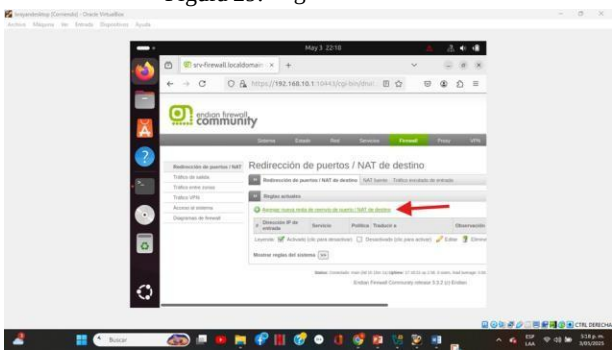
Producto esperado: Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Figura 28. Ingreso al panel Endian

Fuente: Autoría propia (Brayan Muñoz)

Ingresamos al panel para empezar a configurar nuestros permisos y restricciones de red.

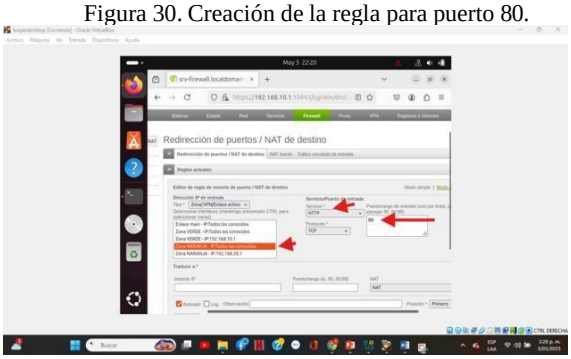
Figura 29. ingreso al firewall.



Fuente: Autoría propia (Brayan Muñoz)

Vamos a firewall y creamos una nueva regla de entrada.

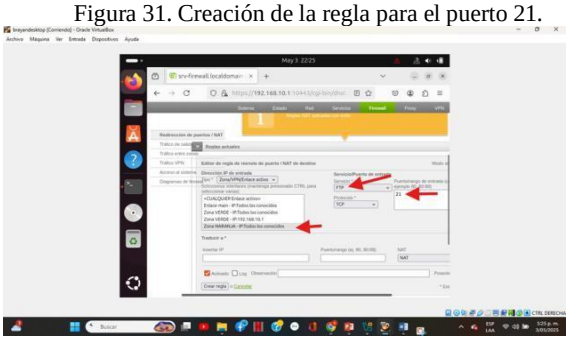
Figura 30. Creación de la regla para puerto 80.



Fuente: Autoría propia (Brayan Muñoz)

En este paso se observa cómo se permite los servicios http del puerto 80.

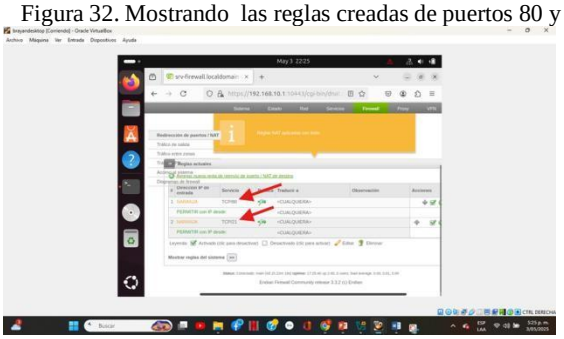
Figura 31. Creación de la regla para el puerto 21.



Fuente: Autoría propia (Brayan Muñoz)

En este paso se observó cómo se permiten los servicios ftp del puerto 21.

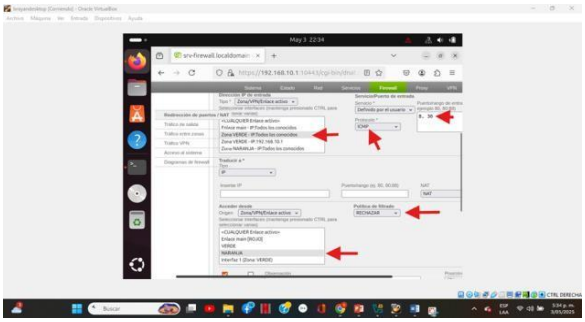
Figura 32. Mostrando las reglas creadas de puertos 80 y 21.



Fuente: Autoría propia (Brayan Muñoz)

Al finalizar estas dos primeras reglas se van a ver reflejadas como se observa en la imagen.

Figura 33. Creación de la regla del puerto ICMP.



Fuente: Autoría propia (Brayan Muñoz)

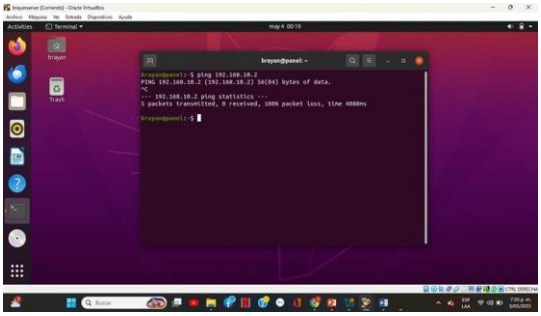
Ahora en esta imagen se observa cómo se está configurando una nueva regla para denegar el protocolo ICMP de los puertos 8 y 30 para bloquear y no hacer ping desde la red DMZ.

Figura 34. lista de reglas creadas.

Fuente: Autoría propia (Brayan Muñoz)

Al finalizar la creación de nuestra regla de restricción nos quedaría un resultado como se muestra en la imagen.

Figura 35. Comprobando la creación de la regla de restricción de la zona DMZ.



Fuente: Autoría propia (Brayan Muñoz)

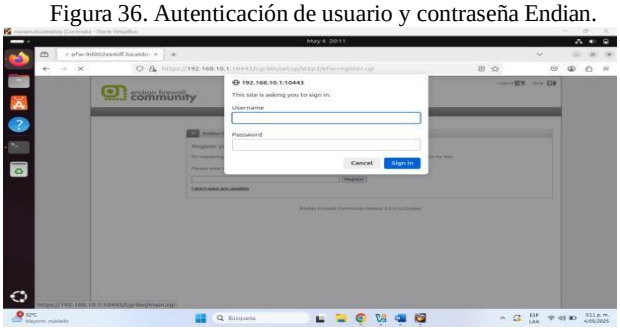
En esta imagen se comprobó que no se puede hacer ping desde la red naranja hacia la red verde todo por la regla de bloqueo que se creó anteriormente.

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

Producto esperado: Configuración de reglas de acceso en un firewall para controlar el tráfico, permitiendo servicios legítimos y bloqueando el no deseado. Incluye definir políticas de seguridad, configurar reglas por puerto y protocolo, usar NAT para redirección de tráfico, verificar registros y realizar

pruebas de conectividad para asegurar su efectividad y seguridad.

Figura 36. Autenticación de usuario y contraseña Endian.

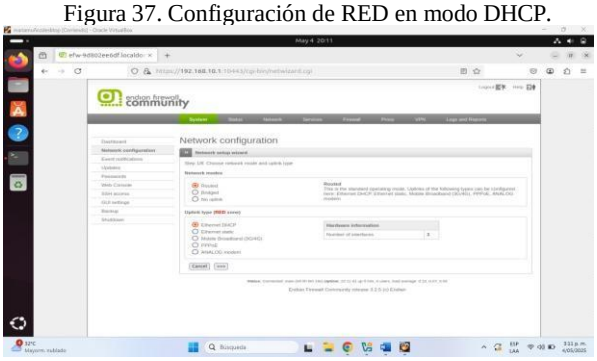


Fuente: Autoría propia (María Muñoz)

Nos pide usuario y contraseña y le damos en

sing in.

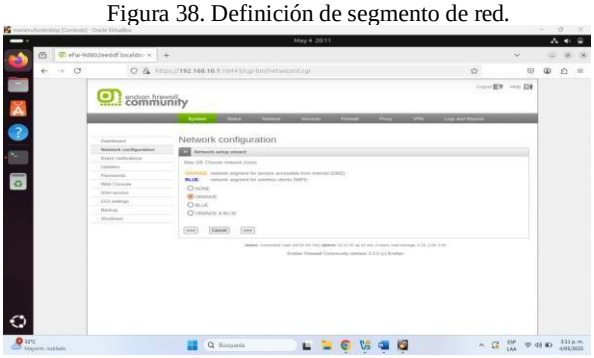
Figura 37. Configuración de RED en modo DHCP.



Fuente: Autoría propia (María Muñoz)

Nos dirigimos al módulo de Network configuración y procedemos a configurar RED de manera DHCP.

Figura 38. Definición de segmento de red.



Fuente: Autoría propia (María Muñoz)

En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado ORANGE para definir el segmento de red que será accesible desde Internet DMZ.

Figura 39. Confirmación de ip de GREEN y ORANGE

Fuente: Autoría propia (María Muñoz)

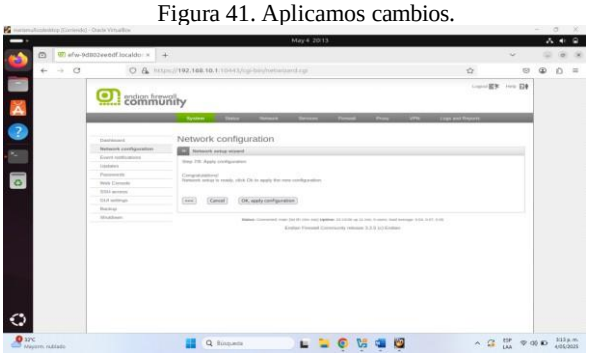
Confirmamos las ip de GREEN 192.168.10.1 y ORANGE 192.168.20.1.

Figura 40. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia (María Muñoz)

De igual forma confirmamos RED DHCP.

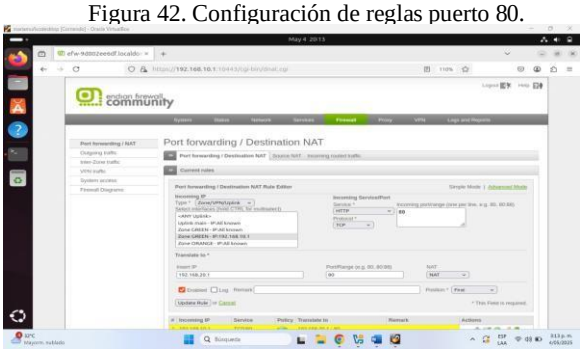
Figura 41. Aplicamos cambios.



Fuente: Autoría propia (María Muñoz)

Aplicamos cambios y guardamos.

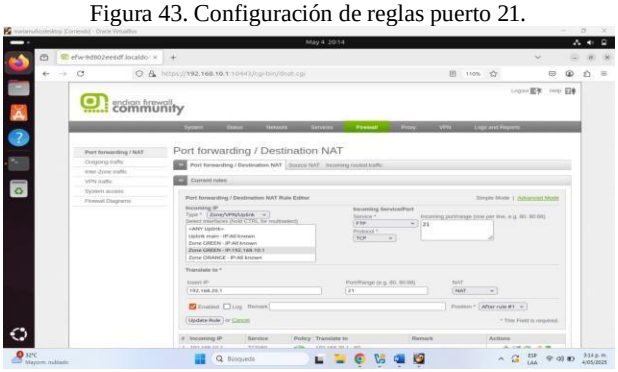
Figura 42. Configuración de reglas puerto 80.



Fuente: Autoría propia (María Muñoz)

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la LAN hacia la DMZ en un firewall Endian.

Figura 43. Configuración de reglas puerto 21.



Fuente: Autoría propia (María Muñoz)

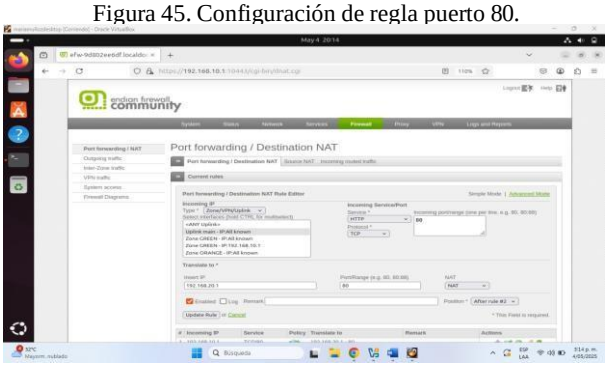
Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 21) desde la LAN hacia la DMZ en un firewall Endian.

Figura 44. Reglas guardadas y aplicadas.

Fuente: Autoría propia (María Muñoz)

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ.

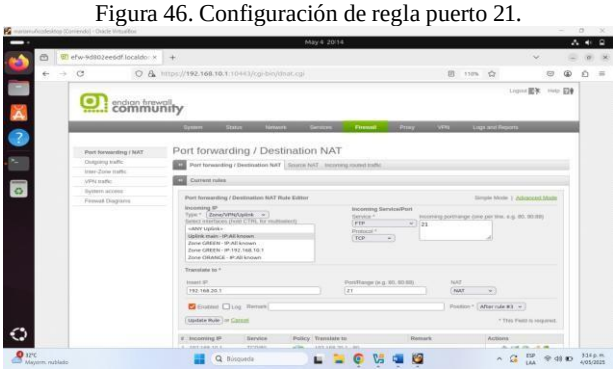
Figura 45. Configuración de regla puerto 80.



Fuente: Autoría propia (María Muñoz)

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 80) desde la RED hacia la DMZ en un firewall Endian.

Figura 46. Configuración de regla puerto 21.



Fuente: Autoría propia (María Muñoz)

Configuración de reglas de Port Forwarding para permitir tráfico HTTP (puerto 21) desde la RED hacia la DMZ en un firewall Endian.

Figura 47. Reglas guardadas y aplicadas.

Fuente: Autoría propia (María Muñoz)

Reglas NAT aplicadas para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) hacia la IP interna en la zona DMZ.

Figura 48. Verificación de logs.

Fuente: Autoría propia (María Muñoz)

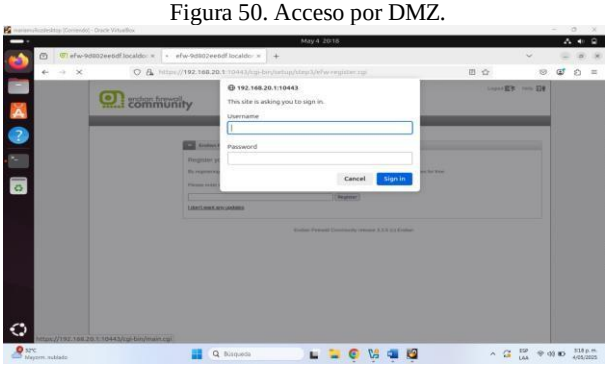
Verificación de los logs en tiempo real del tráfico del firewall para comprobar el acceso HTTP y FTP.

Figura 49. Verificación de tráfico exitoso.

Fuente: Autoría propia (María Muñoz)

De manera correcta se evidencia que se configuraron correctamente las reglas de NAT y Firewall para permitir el acceso HTTP desde la LAN hacia la WAN. Tras aplicar las reglas, se verificó que el tráfico HTTP se estaba gestionando adecuadamente sin bloqueos, lo que indica que las configuraciones fueron exitosas.

Figura 50. Acceso por DMZ.



Fuente: Autoría propia (María Muñoz)

Colocamos la ip de DMZ 192.168.20.1 y evidenciamos la conexión exitosa.

Figura 51. Acceso denegado a www.elnuevodia.com.co.

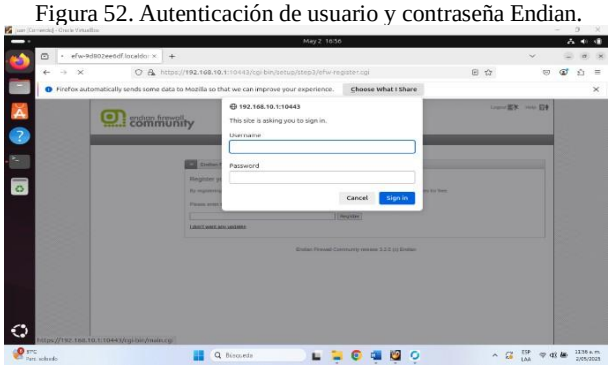
Fuente: Autoría propia (María Muñoz)

De igual forma evidenciamos la conexión HTTP desde la LAN hacia la WAN.

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

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

Figura 52. Autenticación de usuario y contraseña Endian.



Fuente: Autoría propia (Juan Delgado)

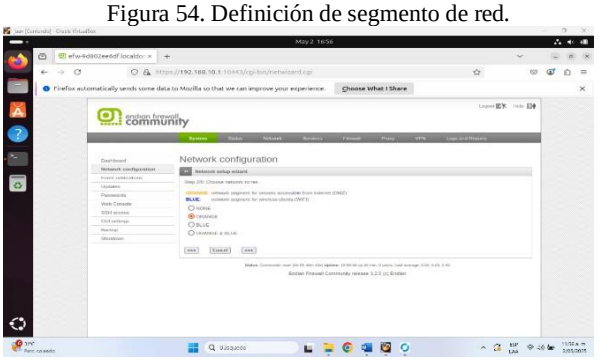
Nos pide usuario y contraseña y le damos en sing in.

Figura 53. Configuración de RED en modo DHCP.

Fuente: Autoría propia (Juan Delgado)

Nos dirigimos al módulo de Network configuración y procedemos a configurar RED de manera DHCP.

Figura 54. Definición de segmento de red.



Fuente: Autoría propia (Juan Delgado)

En este paso, se está configurando el tipo de red para las zonas del firewall. Se ha seleccionado ORANGE para definir el segmento de red que será accesible desde Internet DMZ.

Figura 55. Confirmación de ip de GREEN y ORANGE.

Fuente: Autoría propia (Juan Delgado)

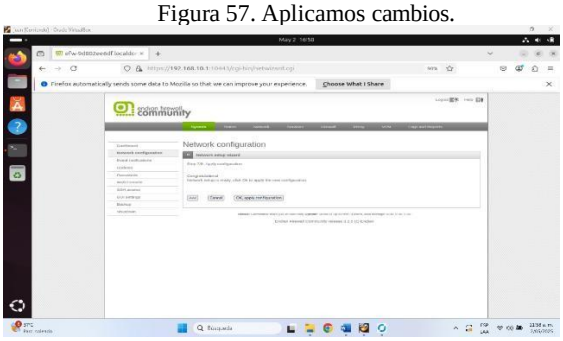
Confirmamos las ip de GREEN 192.168.10.1 y ORANGE 192.168.20.1.

Figura 56. Confirmación de configuración de RED en DHCP.

Fuente: Autoría propia (Juan Delgado)

De igual forma confirmamos RED DHCP.

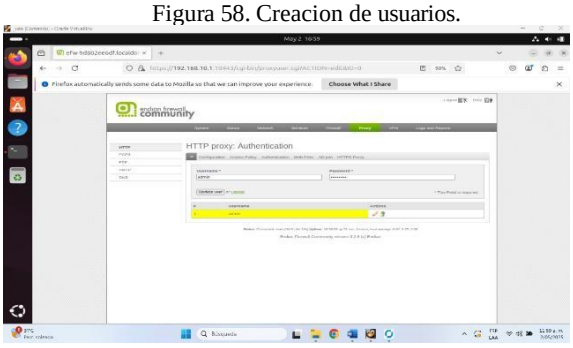
Figura 57. Aplicamos cambios.



Fuente: Autoría propia (Juan Delgado)

Aplicamos cambios y guardamos.

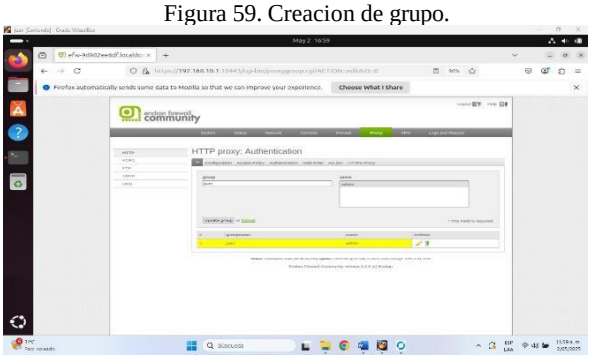
Figura 58. Creacion de usuarios.



Fuente: Autoría propia (Juan Delgado)

Creamos el usuario en el módulo de autenticación.

Figura 59. Creacion de grupo.



Fuente: Autoría propia (Juan Delgado)

Creamos el grupo llamado juan y asociamos nuestro usuario admin a dicho grupo.

Figura 60. Habilitacion de proxy y modo no transparente.

Fuente: Autoría propia (Juan Delgado)

Habilitamos el servicio de proxy.

Figura 61. Creacion de lista negra.

Fuente: Autoría propia (Juan Delgado)

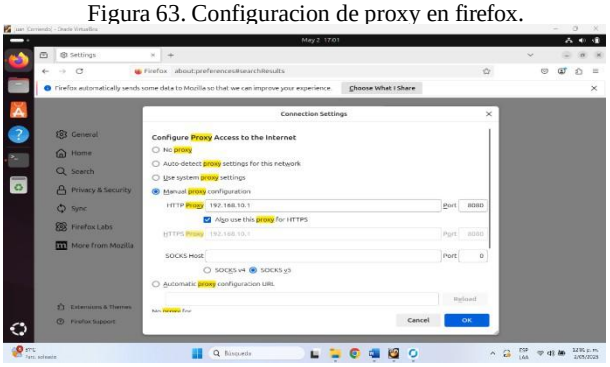
Creamos un nuevo filtro con el nombre listanegra, donde bloqueamos 3 páginas, www.hotmail.com, www.youtube.com, www.elnuevodia.com.co aplicamos y guardamos cambios.

Figura 62. Aplicación de politicas de acceso.

Fuente: Autoría propia (Juan Delgado)

Creamos una política de acceso donde asociamos nuestro usuario admin, le damos que apruebe la regla que se creó llamada listanegra y llenamos la demás configuración.

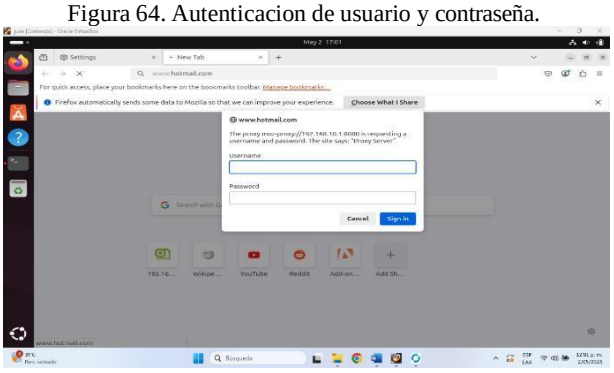
Figura 63. Configuracion de proxy en firefox.



Fuente: Autoría propia (Juan Delgado)

Vamos a la configuración de proxy en nuestro buscador Firefox y manualmente configuramos el Proxy donde colocamos 192.168.10.1 y le decimos que usemos el mismo proxy en HTTPS también.

Figura 64. Autenticacion de usuario y contraseña.



Fuente: Autoría propia (Juan Delgado)

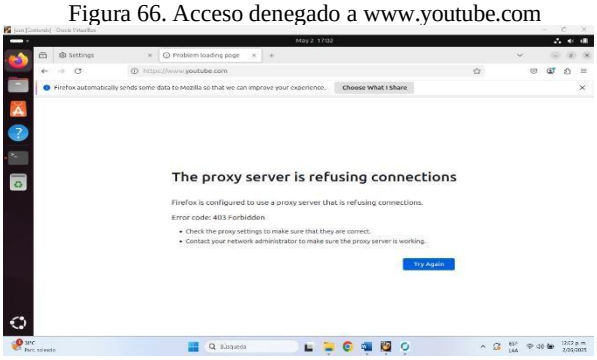
Intentamos ingresar a www.hotmail.com y nos pide autenticación de usuario.

Figura 65. Acceso denegado de www.hotmail.com

Fuente: Autoría propia (Juan Delgado)

Luego de colocar la autenticación nos muestra el siguiente mensaje.

Figura 66. Acceso denegado a www.youtube.com



Fuente: Autoría propia (Juan Delgado)

De igual forma intentamos entrar a www.youtube.com y nos sale el siguiente mensaje.

Figura 67. Acceso denegado a www.elnuevodia.com.co

Fuente: Autoría propia (Juan Delgado)

Y por último intentamos acceder a www.elnuevodia.com.co y también se deniega el acceso.

7 CONCLUSIONES

La implementación de GNU/Linux Endian como firewall y proxy en una infraestructura de red segmentada permitió establecer un entorno seguro y controlado. La correcta configuración de las zonas verde, roja y naranja, junto con la aplicación de reglas específicas para servicios y protocolos, garantizó la protección de los recursos internos y la adecuada gestión del tráfico. La integración de un proxy HTTP no transparente, con autenticación de usuarios y políticas de acceso basadas en listas negras, demuestra ser eficaz para restringir la navegación y reforzar la seguridad perimetral. Las pruebas realizadas evidenciaron la efectividad de las medidas adoptadas, permitiendo solo el tráfico autorizado y bloqueando accesos no deseados. En conclusión, la solución propuesta no solo mejora la seguridad y el control de acceso, sino que también proporciona una base sólida para la administración y escalabilidad de la red, adaptándose a las necesidades de protección de cualquier organización moderna.

La correcta configuración de GNU/Linux Endian en VirtualBox, segmentando la red en zonas verde (LAN), roja (WAN) y naranja (DMZ), es fundamental para establecer una infraestructura de red segura y eficiente. Este proceso permitió no solo la adecuada comunicación entre los diferentes segmentos de la red, sino también sentar las bases para la implementación de políticas de seguridad más avanzadas. La verificación de la conectividad y la asignación precisa de direcciones IP aseguraron que cada zona cumpliera su función específica, facilitando la administración y el control del tráfico. En resumen, la instalación y configuración inicial de Endian en un entorno virtualizado demuestra ser un paso esencial para garantizar la protección y el correcto funcionamiento de los servicios de red.

La habilitación controlada de servicios en la zona DMZ, como HTTP y FTP, junto con la restricción de protocolos como ICMP, evidencia la importancia de definir reglas claras en el firewall para proteger los recursos internos sin sacrificar la funcionalidad necesaria para los servicios expuestos. La creación y comprobación de reglas específicas permitió asegurar que solo el tráfico autorizado pudiera acceder a los servidores ubicados en la DMZ, mientras que los intentos de exploración o ataques mediante protocolos no permitidos fueron bloqueados de manera efectiva. Esta práctica refuerza la seguridad perimetral y demuestra que una gestión adecuada de la DMZ es clave para minimizar riesgos y mantener la integridad de la red interna.

La configuración de reglas de acceso en el firewall, permitiendo únicamente el tráfico legítimo y bloqueando el no deseado, resultó esencial para el control y la seguridad de la red. El uso de NAT y reenvío de puertos, junto con la verificación de registros y pruebas de conectividad, permitió validar la efectividad de las políticas implementadas. Este enfoque no solo garantiza que los servicios críticos estarían disponibles para los usuarios autorizados, sino que también previno accesos no autorizados y posibles amenazas externas. En conclusión, la gestión detallada de las reglas de acceso es un componente indispensable para mantener una red segura, eficiente y alineada con las necesidades de la organización.

La implementación de un Proxy HTTP con políticas de autenticación en un entorno de red gestionado bajo GNU/Linux Endian, refuerza las medidas de seguridad perimetral, controlando eficazmente el tráfico hacia y desde la red interna. Esta práctica permite no solo bloquear el acceso a sitios web específicos, sino también garantizar que la autenticación de usuarios sea una capa adicional de protección frente a accesos no autorizados. La segregación de redes mediante el uso de una DMZ, junto con un firewall como Endian, proporciona una infraestructura segura que limita los riesgos de posibles ataques externos. La solución propuesta es un paso significativo hacia la consolidación de un entorno de red robusto y confiable, lo que permite a la organización gestionar sus recursos tecnológicos de forma eficiente y segura.

8 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] LPI Linux Essentials.(2022). Tema 4: El sistema operativo Linux. https://learning.lpi.org/es/learning- materials/010-160/4/
[9] LPI Linux Essentials.(2022). Tema 5: Seguridad y sistema de permisos de archivos.
https://learning.lpi.org/es/learningmaterials/010-160/5/
[10] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD.
https://repository.unad.edu.co/handle/10596/53211