IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Juan Camilo Martínez Rozo
jcmartinezroz@unadvirtual.edu.co
Cristian Felipe Muñoz Betancourt
cfmunozbe@unadvirtual.edu.co
Jorge Isaac Ventura Sanchez
Jiventuras@unadvirtual.edu.co
Fabián Ricardo Guerrero Ballen
frguierrerob@unadvirtual.edu.co
Javier Alejandro Segura Rodríguez
jaseguraro@unadvirtual.edu.co

RESUMEN: *Este documento presenta la implementación de un entorno de red segmentado utilizando VirtualBox y el sistema de seguridad perimetral Endian Firewall. El proyecto se desarrolló con tres zonas diferenciadas —verde, naranja y roja— con el fin de simular un escenario real de control y protección del tráfico en una infraestructura de red. Durante la configuración se incorporaron mecanismos como reglas de NAT, filtrado mediante firewall, autenticación por proxy y restricción de navegación a través de listas negras, lo cual permitió aplicar políticas de seguridad específicas para cada segmento. Los resultados demuestran que Endian es una solución libre, flexible y eficaz para la gestión de redes y la protección perimetral, ofreciendo facilidad de administración y un alto nivel de control. La implementación realizada evidencia su utilidad en entornos académicos y organizacionales que requieren fortalecer su infraestructura sin incurrir en altos costos.*

PALABRAS CLAVE*: DMZ, Endian Firewall, FTP, HTTP, NAT, Proxy, Puerto, Seguridad perimetral, Segmentación de red.*

1. INTRODUCCIÓN

La seguridad perimetral constituye un pilar fundamental en el diseño y protección de cualquier infraestructura de red moderna. Con el propósito de comprender y aplicar estos principios en un entorno controlado, el presente trabajo aborda la configuración de una red segmentada mediante VirtualBox y el sistema Endian Firewall. A través de la implementación de tres zonas —verde, naranja y roja— se recrea un escenario cercano a la realidad, en el que es posible gestionar el tráfico, establecer políticas específicas y analizar el comportamiento de distintos servicios de seguridad.

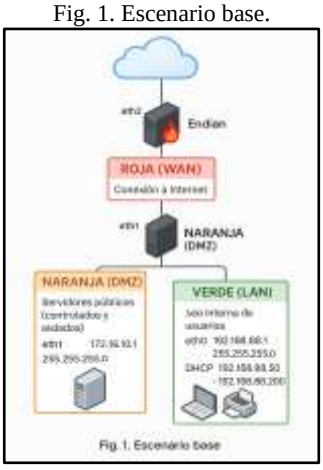
Durante el proceso se integraron funciones esenciales como reglas de NAT, filtrado de paquetes mediante firewall, autenticación de usuarios a través de proxy y control de navegación mediante listas negras, estas herramientas evidencian cómo una adecuada segmentación y administración del perímetro fortalecen la protección y disminuyen los riesgos dentro de la red, asimismo, se resalta la facilidad de uso y la eficiencia de Endian Firewall como solución libre y confiable para el aseguramiento de entornos corporativos y académicos.

2. DESARROLLO DE LA TEMÁTICA

2.1 CONFIGURACIÓN DE LA INSTANCIA PARA GNU/LINUX ENDIAN EN VIRTUALBOX (TARJETAS DE RED) E INSTALACIÓN EFECTIVA DEL MISMO - CARACTERÍSTICAS GENERALES

El escenario base se compone de una máquina virtual con GNU/Linux Endian configurada con tres interfaces de red: la red verde (LAN), que utiliza el direccionamiento 192.168.88.1/24 y aloja una máquina virtual con Ubuntu Desktop; la red naranja (DMZ), donde se encuentra una máquina virtual con Ubuntu Server destinada a servicios expuestos; y la red roja (WAN), que corresponde al equipo host desde el cual se ejecutan todos los entornos virtualizados. A continuación, se presenta una ilustración que permite visualizar mejor este escenario.

Fig. 1. Escenario base.



Fuente: Autoría propia.

El proceso inicia con la descarga de Endian Firewall 3.3 desde su repositorio oficial en SourceForge. Una vez obtenido

el instalador, se continúa con la preparación del entorno de trabajo, conformado por Ubuntu Desktop (como cliente), Ubuntu Server (como servidor) y el propio Endian, que actuará como cortafuegos y dispositivo de segmentación de redes.

Como primer paso, se procede a configurar las interfaces de red asignadas a Endian. El Adaptador 1 se establece como red interna bajo el nombre RED VERDE, destinada a la comunicación con los equipos de la LAN. El Adaptador 2 también se asigna a una red interna, identificada como RED NARANJADA, donde se conectará el servidor ubicado en la DMZ. Finalmente, el Adaptador 3 permanece en modo NAT, ya que es el encargado de proporcionar salida hacia Internet, representando la RED ROJA.

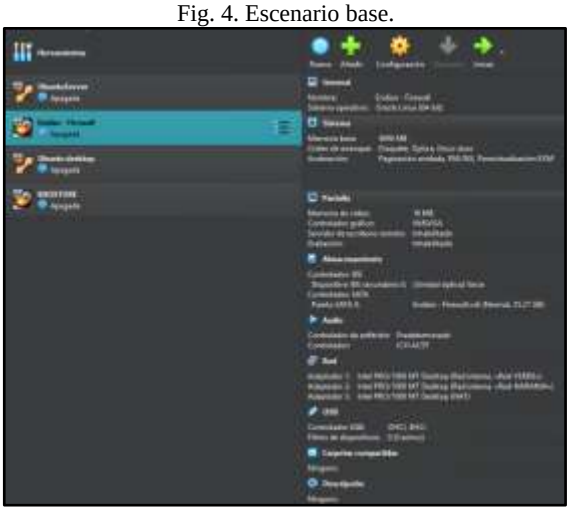
Fig. 2. Escenario base.

Fuente: Autoría propia.

Fig. 3. Escenario base.

Fuente: Autoría propia.

Fig. 4. Escenario base.



Fuente: Autoría propia.

Fig. 5. Escenario base.

Fuente: Autoría propia.

Posteriormente, se configuran las tarjetas de red de los equipos que interactuarán con el firewall. En el caso de Ubuntu Desktop, utilizado como cliente, se asigna el Adaptador 1 a la red interna RED VERDE, permitiendo que este equipo forme parte de la red local protegida por Endian.

Figura 6. Configuración del adaptador 1 del cliente.

Fuente: Autoría propia.

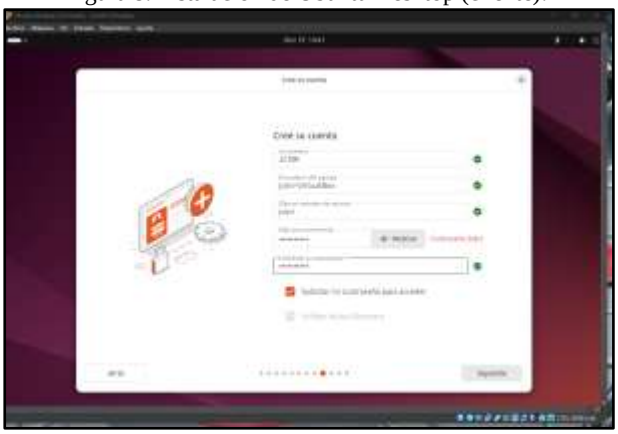
Para el Ubuntu Server, encargado de desempeñar funciones de servidor dentro de la DMZ, se configura su único adaptador como red interna asociada a la RED NARANJA.

Fig. 7. Configuración del adaptador 1 del servidor.

Fuente: Autoría propia.

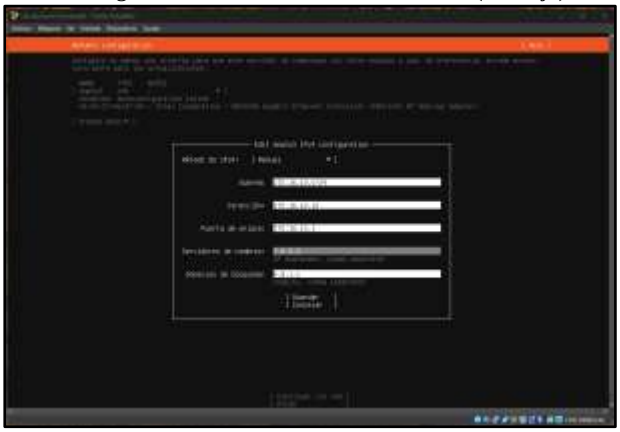
Una vez definidas las redes, se inicia el proceso de instalación de los sistemas operativos. Ubuntu Server y Ubuntu Desktop se instalan de manera convencional, mientras que para Endian Firewall 3.3 se sigue el asistente que guía la creación de las zonas de red y la carga de los módulos de seguridad.

Figura 8. Instalación de Ubuntu Desktop (cliente).



Fuente: Autoría propia.

Figura 9. Instalación de Ubuntu Server (Naranja).



Fuente: Autoría propia.

Figura 10. Instalación de Endian Firewall 3.3.

Fuente: Autoría propia.

Al finalizar la instalación, Endian muestra su interfaz inicial, en la cual se puede verificar que las zonas **VERDE** y **ROJA** aparecen activas. Esta vista confirma que la estructura básica del firewall quedó correctamente establecida durante el proceso de instalación.

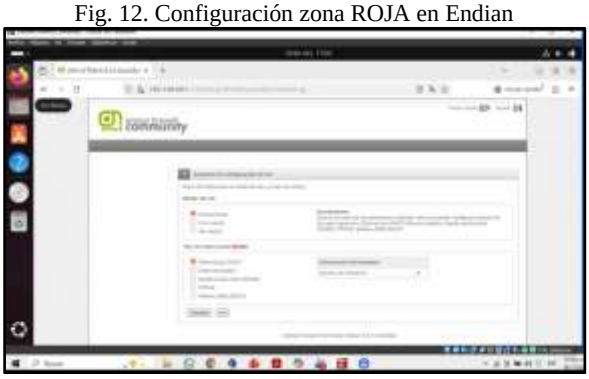
Figura 11. Vista general de la interfaz de Endian Firewall 3.3.

Fuente: Autoría propia.

2.2 Configuración NAT.

Para permitir la salida a Internet desde las redes internas en un entorno con Endian Firewall, es necesario configurar reglas de NAT, el primer paso consiste en habilitar el acceso a Internet desde la red LAN, que en este caso corresponde a la zona verde donde se encuentra el equipo Ubuntu Desktop con la IP 192.168.88.2, para esto, se accede a la interfaz web de Endian mediante la dirección https://192.168.88.1 desde el navegador y, donde se realizará la configuración inicial del sistema brindando la autorización de las políticas de uso del sistema y las contraseñas de administrador y del root para continuar con la configuración de la red roja utilizando el modo de red enrutamiento y el tipo de enlace de la zona ROJA como ethernet por DHCP.

Fig. 12. Configuración zona ROJA en Endian



Fuente: Autoría Propia.

Una vez se realiza la configuración de la zona roja realizamos la verificación de la que la zona verde se encuentre bien configurada con la dirección IP 192.168.88.1 y de la misma forma se realiza la configuración de la zona naranja, a la cual se le habilitará la IP 172.16.10.1.

Fig. 13. Configuración zona NARANJA en Endian

Fuente: Autoría Propia.

El siguiente paso es realizar una verificación de las modificaciones realizadas en el asistente de configuración de red verificando que se cumplan los requerimientos del sistema para una correcta asignación de red.

Fig. 14. Verificación de configuraciones realizadas

Fuente: Autoría Propia.

Una vez dentro de la interfaz Endian y la configuración de las zonas roja, naranja y verde se encuentran listas, se ingresa a la sección "Tráfico de salida" ubicada en el panel lateral izquierdo, estando ahí se crea una nueva regla con el nombre "Zona VERDE a zona ROJA", seleccionando como zona de origen la zona verde y como zona de destino la zona roja (Internet), marcando la acción como "Aceptar", esta configuración permite que los dispositivos de la LAN puedan salir a Internet utilizando la IP pública de la interfaz roja del firewall.

Figura 15. Configuración del firewall zona VERDE.

Fuente: Autoría Propia.

El siguiente paso es habilitar el acceso a Internet desde la zona DMZ, representada por la red naranja, donde se encuentra el servidor Ubuntu Server, desde la misma sección de "Tráfico de salida", se crea una nueva regla llamada "Zona NARANJA a zona ROJA", esta vez seleccionando como zona de origen la zona naranja y como destino nuevamente la zona roja. Al igual que en la regla anterior, se establece la acción como "Aceptar", con esta configuración, el servidor ubicado en la DMZ puede acceder a Internet de forma segura, sin exponer directamente su dirección IP interna.

Fig. 16. Configuración del firewall zona NARANJA

Fuente: Autoría propia.

Una vez configuradas correctamente las reglas, se realiza la verificación desde la consola de los equipos Ubuntu Desktop y Ubuntu Server que efectivamente tienen acceso a Internet, haciendo uso de un comandos que permiten confirmar tanto la conectividad como la traducción de direcciones, desde la terminal del Ubuntu Desktop, ubicado en la zona verde, se ejecuta el comando ping 8.8.8.8 para probar la conexión con un servidor DNS público de Google, luego, se utiliza el comando curl ifconfig.me para consultar la dirección IP pública con la que el equipo está saliendo a Internet, lo que permite confirmar que el enmascaramiento está funcionando correctamente.

Fig. 17. Comprobación de acceso LAN desde desktop

Fuente: Autoría propia.

Fig. 18. Comprobación de acceso LAN desde server

Fuente: Autoría propia

2.3 Permitir servicios de la Zona DMZ para la red:

Fig. 19. Servicios HTTP y FTP.

Fuente: Autoría propia

Se realiza una verificación dentro del entorno de Endian. Se configura para permitir servicios HTTP con puerto 80 y FTP con puerto 21.

En la figura 20, se observa el tráfico de inter-zona donde se crean 2 reglas para cumplir con los requerimientos de la primera parte de la temática 3.

Fig. 20. Servicio HTTP, puerto 80.

Fuente: Autoría propia

En la figura 20, se observa el tráfico de inter-zona donde la primer regla para permitir el servicio HTTP con un puerto 80 desde el servidor.

Fig. 21. Servicio FTP, puerto 21.

Fuente: Autoría propia

En la figura 21, se observa el tráfico de inter-zona donde la segunda regla para permitir el servicio FTP con un puerto 80 desde el servidor.

Fig. 22. Validación del servicio HTTP.

Fuente: Autoría propia

Fig. 23. Validación del servicio FTP.

Fuente: Autoría propia

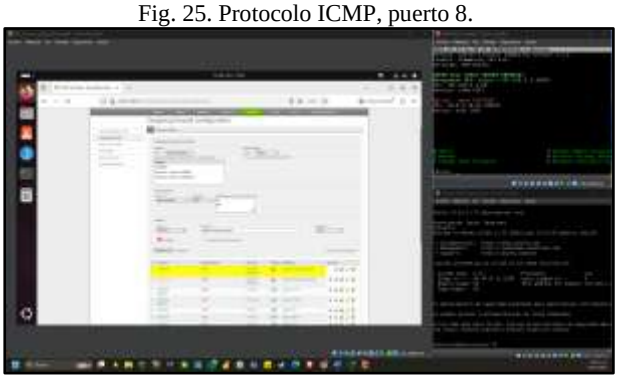
Se realiza la segunda parte de la temática 3, Denegando los protocolos ICMP (Puerto 8 y puerto 30) para no permitir ICMP Echo Request hacia una IP o host y una respuesta de la IP ICMP Echo Reply a través de la terminal. Configurando unas reglas en Endian.

Fig. 24. Protocolos ICMP.

Fuente: Autoría propia

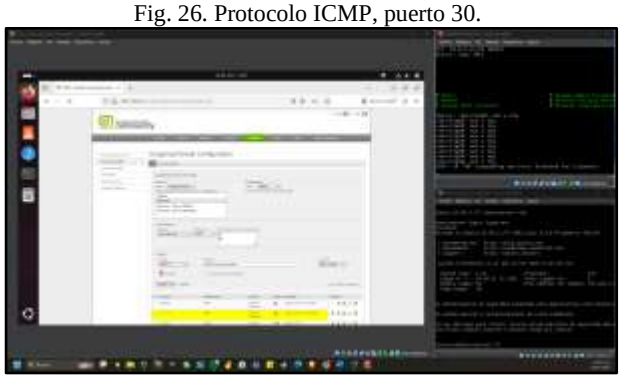
En la figura 24, se observan las reglas de tráfico saliente, donde se configuran 2 reglas para impedir el acceso y función del protocolo ICMP con un puerto 8 Y 30 desde el servidor.

Fig. 25. Protocolo ICMP, puerto 8.



Fuente: Autoría propia

Fig. 26. Protocolo ICMP, puerto 30.



Fuente: Autoría propia

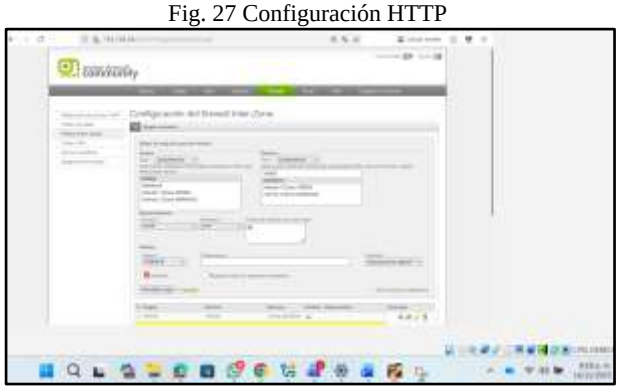
2.4 Reglas de acceso para permitir o denegar el tráfico

La navegación entre zonas es un factor importante, especialmente en procesos empresariales que requieren que sus empleados se conecten a las diferentes aplicaciones expuestas, ya sean web HTTP/HTTPS o FTP/SFTP, necesarias para la gestión de la compañía, no obstante la aplicación de reglas de acceso que permitan controlar las vías de comunicación es algo en el cual se debe prestar mucha atención en especial para cubrir todos los flancos y ofrecer una capa de seguridad muy necesaria en un entorno social en que la información se ha convertido en uno de los activos más importantes que tienen las compañías.

Esta temática permite realizar la aplicación de reglas que permitan controlar el tráfico dentro de una red, segmentada en tres zonas diferentes (Roja (WAN), Naranja (DMZ) y Verde (LAN), es importante aclarar que cada una de las redes se encuentra ubicada en segmentos diferentes de la red.

En primeras instancias, se realizará la configuración de una regla que permita establecer comunicación entre la zona verde (LAN) y naranja (DMZ), utilizando para ello los protocolos HTTP a través del puerto 80 y FTP mediante el puerto 21, desde el firewall Endian.

Fig. 27 Configuración HTTP



Fuente: autoría propia

La imagen anterior, nos permite visualizar la configuración de la regla que permite la comunicación entre las zonas verde y naranja, utilizando el puerto 80 (HTTP), de manera que ahora nuestro nodo cliente que se encuentra en la

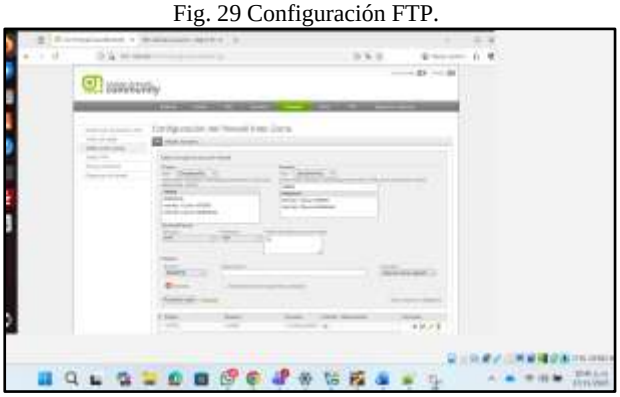
LAN, tiene acceso a las aplicaciones instaladas en el servidor que tengan acceso Web.

Fig. 28 Formulario PHP publicado en DMZ.

Fuente: autoría propia

Ahora que está configurado el servicio HTTP, se procede a crear la regla que permita la comunicación entre la zona verde y naranja mediante el puerto 21, el cual es utilizado por defecto para los servicios FTP

Fig. 29 Configuración FTP.



Fuente: autoría propia

Fig. 30 Acceso a FTP en DMZ mediante FileZilla

Fuente: autoría propia

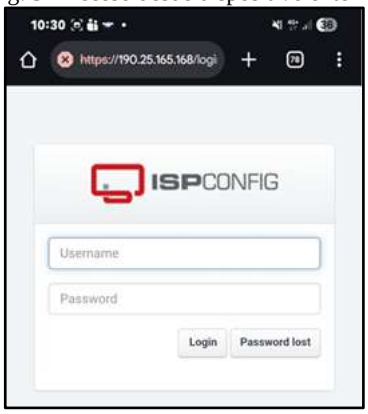
A nivel interno ahora se puede estar seguro de que la comunicación fue establecida correctamente, pero también es posible establecer reglas para que los clientes y externos, puedan acceder a las aplicaciones configuradas en mi servidor, para este escenario será habilitada una regla en Endian, para que cualquier persona desde internet tenga acceso a nuestro servidor de aplicaciones, dirigiendo el tráfico que llega desde la zona roja Internet mediante el puerto 443 HTTPS a la zona naranja, utilizando el puerto 8080

Fig. 31 Redirección tráfico Internet a DMZ

Fuente: autoría propia

La imagen ilustra la configuración, para que el tráfico que ingrese desde internet, mediante el puerto 443 HTTPS, sea dirigido a la zona DMZ, mediante el puerto 8080

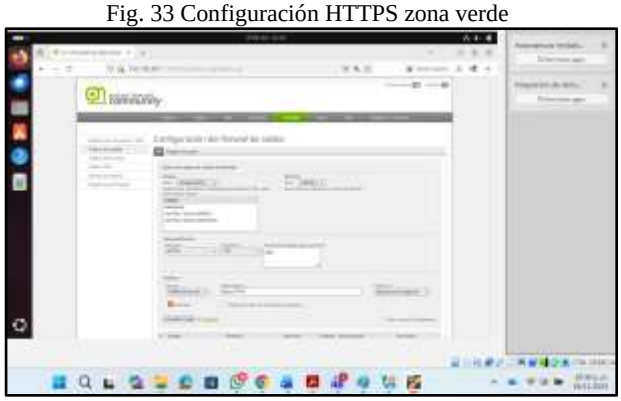
Fig. 32 Acceso desde dispositivo externo



Fuente: autoría propia

El acceso a internet debe ser permitido para mantener el sistema operativo actualizado y las herramientas a utilizar, en el siguiente paso se procede a crear una regla para permitir la navegación desde la zona verde LAN

Fig. 33 Configuración HTTPS zona verde



Fuente: autoría propia

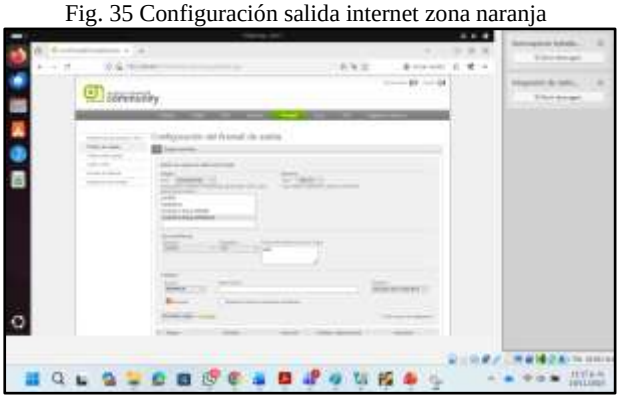
La imagen ilustra la configuración de la regla en el Firewall de Endian que le permitirá al host de mi red LAN zona Verde acceder a internet utilizando el protocolo HTTPS mediante el puerto 443

Fig. 34 Prueba navegación host zona verde

Fuente: autoría propia

En la imagen se evidencia que el host con la IP 192.168.88.20/24 tiene salida a Internet.

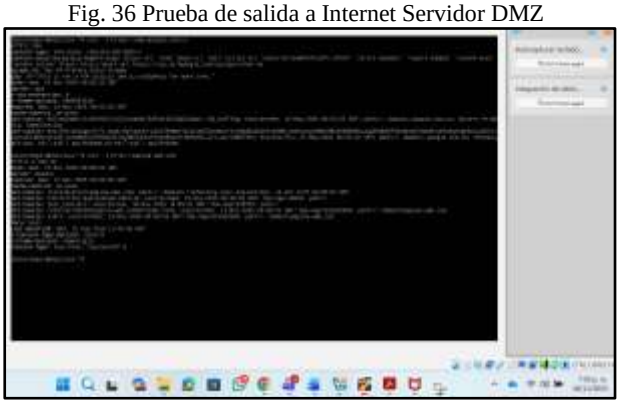
Fig. 35 Configuración salida internet zona naranja



Fuente: autoría propia

La imagen ilustra la configuración, para que nuestro servidor en la DMZ pueda tener navegación en internet

Fig. 36 Prueba de salida a Internet Servidor DMZ



Fuente: autoría propia

En la anterior imagen, vemos cómo podemos ingresar interactuar con una página, tanto HTTP, como HTTPS

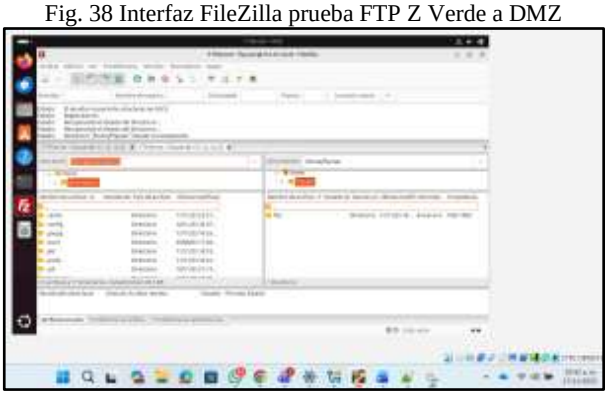
El servicio FTP, también además de ser útil para compartir archivos de forma local, también puede ser usado para interactuar con clientes y externos para compartir información de una forma rápida.

Fig. 37 Configuración FTP LAN a DMZ

Fuente: autoría propia

En la imagen anterior, se visualiza la configuración en el Firewall Endian entre la zona verde, hacia la zona naranja a través del puerto 21

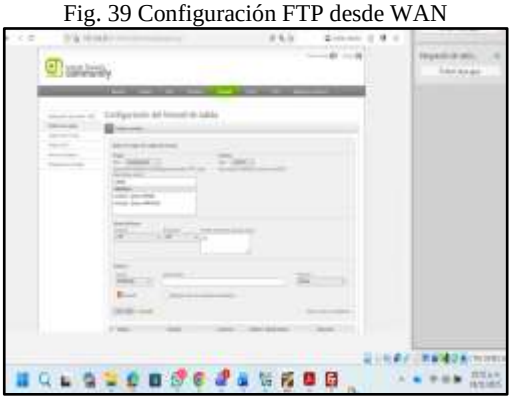
Fig. 38 Interfaz FileZilla prueba FTP Z Verde a DMZ



Fuente: autoría propia

La imagen ilustra el ingreso del host 192.168.88.20 que se encuentra en la red LAN accediendo a un directorio FTP creado y configurado en el servidor de la red DMZ. Pero las aplicaciones web, no son el único servicio que puede ser compartido, para este paso se requiere que el servicio FTP, pueda ser accedido desde cualquier lugar

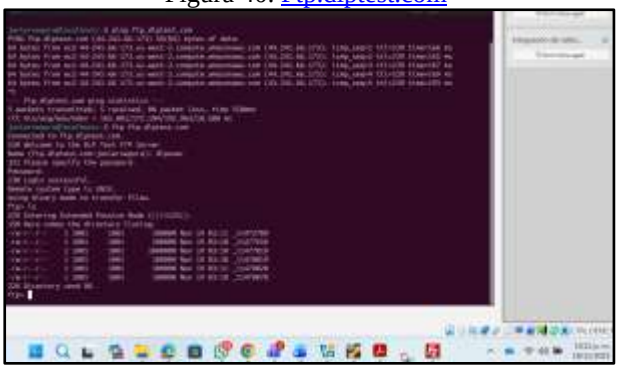
Fig. 39 Configuración FTP desde WAN



Fuente: autoría propia

Esta imagen representa la configuración que permite a cualquier host con acceso a internet, conectarse al servidor FTP configurado en el DMZ mediante el puerto 21

Figura 40. Ftp.dlptest.com



Fuente: autoría propia

2.5 Implementar un Proxy HTTP (No transparente) con políticas de autenticación para navegación en Internet

La implementación de proxys dentro de la infraestructura tecnológica de una organización constituye una práctica indispensable para fortalecer la seguridad y optimizar la gestión del tráfico de datos, un proxy permite al administrador de red tener un mejor control y más preciso sobre los sitios web a los que pueden acceder los equipos corporativos, aplicando políticas basadas en zonas, rangos de direcciones IP o perfiles de usuario. Este tipo de segmentación sirve para garantizar el uso adecuado de los recursos institucionales, evitando que los empleados accedan a contenido inapropiado o que pueda comprometer la productividad y la integridad de la información.

Los proxys contribuyen también a mejorar la protección contra amenazas externas al filtrar solicitudes maliciosas, bloquear dominios sospechosos y registrar de forma detallada las actividades de acceso otorgando al webmaster la capacidad de monitoreo y auditoría facilitando la detección temprana de comportamientos anómalos.

Implementar proxys y combinarlos con técnicas de segmentación de red, firewalls perimetrales y listas de control de acceso, permite construir ecosistemas tecnológicos más robustos, eficientes que cumplan mejor los lineamientos de la organización.

2.6 Activación del HTTP proxy

Primeramente, mediante la web de configuración del Endian en la opción de Proxy subsección Configuración-HTTP: se activa el HTTP proxy, seleccionando ambas zonas en este caso la verde y la naranja, aplicando el no transparente y configurando el puerto del proxy como 8080

Figura 41. Activación http proxy

Fuente: autoría propia

Posteriormente en el mismo menú proxy HTTP ahora en a sección Web filter se crea un perfil que se llamó “urlBloq”, en este apartado es en donde se crean las black and white lists, en este caso solo se hará uso de la black list en donde se procede a listar los sitios web que se bloquearán mediante proxy:

www.hotmail.com
www.youtube.com
www.elnuevodia.com.co

Figura 42. Creación del perfil web url filter

Fuente: autoría propia

En el menú Authentication se crea el perfil que se hará uso en pasos posteriores, además de la creación del grupo asignando al perfil “jorgev” como único miembro del grupo “grupo-proxy”

Figura 43. Creación del usuario “jorgev”

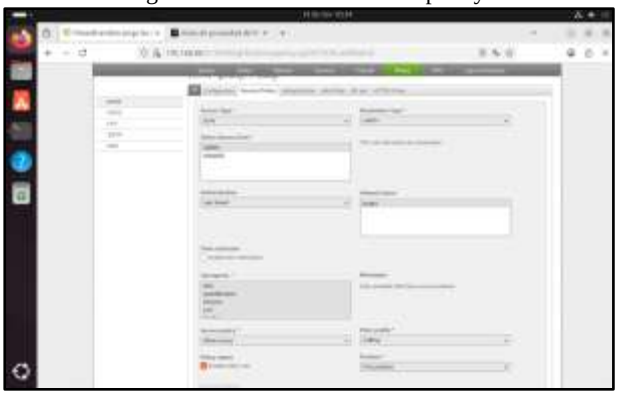
Fuente: autoría propia

Figura 44. Creación del grupo “grupo-proxy” y asignación miembro

Fuente: autoría propia

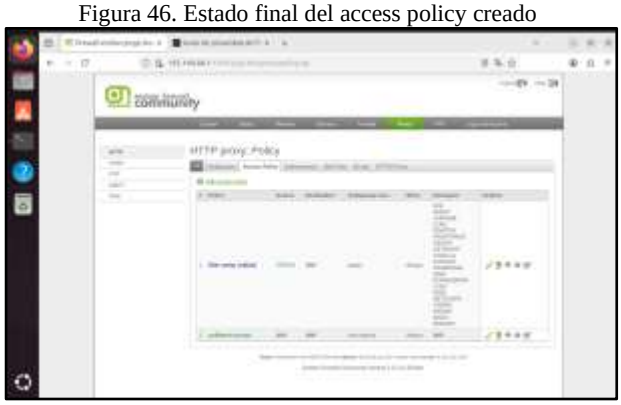
Finalmente, en el menú HTTP proxy, En la sección Access Policy se crea una nueva política seleccionando como zona de origen la zona verde hacia cualquier destino, pero asociando el usuario que se creó “jorgev” en autentication y el perfil que se creó de bloqueo hacia las urls listadas

Figura 45. Creación del access policy



Fuente: autoría propia

Figura 46. Estado final del access policy creado



Fuente: autoría propia

2.7 Prueba de funcionamiento del servidor proxy

Desde el equipo jorge_ventura_desktop2 conectado a la red interna VERDE mediante el navegador Firefox se comprueba conexión antes de aplicar el servidor proxy.

Figura 47. Navegación youtube.com

Fuente: autoría propia

Figura 48. Acceso a hotmail.com

Fuente: autoría propia

Figura 49. Acceso a elnuevodia.com.co

Fuente: autoría propia

Posteriormente, para hacer uso del servidor proxy configurado en la configuración web de Endian se selecciona Configuración manual del proxy poniendo la dirección ip del endian (192.168.88.1) con el puerto que se definió en la configuración web (8080).

Figura 50. Configuración proxy manual Firefox

Fuente: autoría propia

Al activar el servidor proxy ahora el navegador pasará por el Proxy antes de navegar, al iniciar el navegador solicita login para navegar:

Figura 51. Autenticación para acceder al proxy

Fuente: autoría propia

Ahora se bloqueará el acceso a las plataformas yutube.com, elnuevodia.com.co, y hotmail.com pero se permitirá navegación a todos los portales y webs

Figura 52. Acceso bloqueado a youtube.com mediante proxy

Fuente: autoría propia

Figura 53. Acceso bloqueado a hotmail.com

Fuente: autoría propia

Figura 54. Acceso bloqueado a elnuevodia.com.co

Fuente: autoría propia

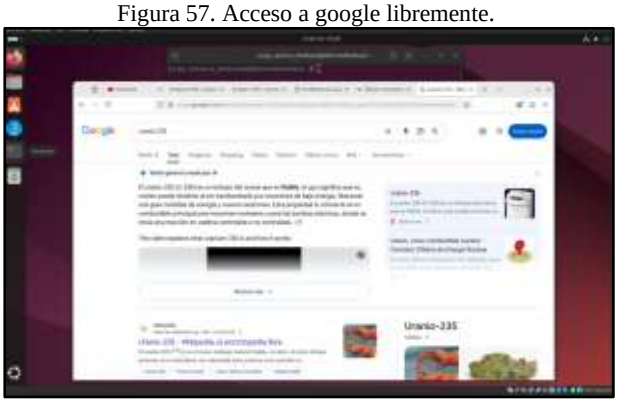
Figura 55. Acceso bloqueado a elnuevodia.com.co mediante búsqueda por Google.

Fuente: autoría propia

Figura 56. Acceso a wikipedia libremente.

Fuente: autoría propia

Figura 57. Acceso a google libremente.



Fuente: autoría propia

3. CONCLUSIONES

Las reglas de configuración son importantes, ya que permiten establecer parámetros y lineamientos para el correcto funcionamiento de la red basado en políticas que logran mantener la red segura, se pueden habilitar y deshabilitar servicios dependiendo de las necesidades del usuario.

En la temática 5 se realizó la configuración del proxy en Endian Firewall, estableciendo un control centralizado sobre la navegación de los equipos ubicados en la zona verde Se ejecutó la habilitación del proxy en modo no transparente y se definieron políticas de acceso basadas en autenticación, lo que permitió regular de forma precisa qué usuarios y dispositivos podían salir a Internet. Asimismo, se evaluó el funcionamiento filtrado mediante listas negras y restricciones por categorías, confirmando que el sistema bloqueó correctamente los sitios no autorizados. Durante las pruebas se verificó que todo el tráfico web fue canalizado a través del proxy, evidenciando su efectividad como mecanismo de control, auditoría y fortalecimiento de la seguridad perimetral.

La configuración de reglas NAT en Endian Firewall constituye un proceso esencial para garantizar la salida segura de las redes internas hacia Internet, permitiendo que tanto la LAN (zona verde) como la DMZ (zona naranja) utilicen la IP pública de la interfaz roja para enmascarar sus direcciones privadas. Este mecanismo asegura conectividad sin exponer directamente los equipos internos y refuerza la seguridad de la infraestructura, validado mediante pruebas de conectividad y traducción de direcciones. Tal como se señala en la guía oficial de Endian Firewall Community [4], la correcta implementación de estas reglas es un componente crítico dentro de la administración de redes segmentadas, ya que equilibra funcionalidad y protección de los recursos internos.

4. REFERENCIAS

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

[2] Cervelión, Á. J. (2023). *Instalación de Nagios Core 4.4 en Ubuntu 22.04* [Objeto virtual de información – OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/54230

[3] Debian. (2023). *El manual del administrador de Debian 12.5.0*. https://www.debian.org/releases/stable/amd64/index.es.html

[4] Endian. (2016). *Endian UTM 3.2: Manual de referencia*. http://docs.endian.com/3.2/utm/index.html

[5] LaCroix, J. (2020). *Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server*. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

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

[7] Oracle. (2020). *Manual de usuario VirtualBox*. https://www.virtualbox.org/manual/

[8] Firewall Basics: Understanding Network Security, RF Wireless World. [Online]. Available: https://www.rfwireless-world.com/terminology/networking-basics/firewall-basics-understanding-network-security

[9] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 6th ed., Pearson, 2021. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780136764052

[10] Red Hat, “Firewall and Network Security Basics,” 2023. [Online]. Available: https://www.redhat.com