Implementación de Seguridad Perimetral y Gestión de Zonas (LAN, WAN, DMZ) mediante Endian Firewall en entornos GNU/Linux

Mario Steven Barrera Restrepo
e-mail: mbarrerare@unadvirtual.edu.co
Santiago Calderón Méndez
e-mail: scalderonme@unadvirtual.edu.co
Sebastián Gamba Arredondo
e-mail: sgambaa@unadvirtual.edu.co
Camilo Montero Beltran
e-mail: cmonterob@unadvirtual.edu.co

ABSTRACT:

This article presents the implementation of a perimeter security environment based on GNU/Linux through the use of Open Source tools such as Endian Firewall, Ubuntu Server, Ubuntu Desktop, and VirtualBox. The development of the activity made it possible to configure a segmented network infrastructure in LAN, DMZ, and WAN zones, applying protection mechanisms aimed at the secure control and management of network traffic. During the process, NAT configurations, inter-zone access rules, traffic filtering, web and FTP services, as well as an HTTP proxy with authentication for Internet access were implemented. Connectivity tests and functional validation were also carried out to verify the correct operation of the established security policies. The practice strengthened competencies in GNU/Linux system administration, information security, and network management, promoting the use of best practices for protecting services and computing resources in virtualized environments.

KEYWORDS: GNU/Linux, Endian Firewall, perimeter security, NAT, DMZ, VirtualBox, HTTP proxy, firewall, segmented networks, authentication

RESUMEN:

Este artículo presenta la implementación de un entorno de seguridad perimetral basado en GNU/Linux mediante el uso de herramientas Open Source como Endian Firewall, Ubuntu Server, Ubuntu Desktop y VirtualBox. El desarrollo de la actividad permitió configurar una infraestructura de red segmentada en zonas LAN, DMZ y WAN, aplicando mecanismos de protección orientados al control y administración segura del tráfico de red. Durante el proceso se implementaron configuraciones NAT, reglas de acceso inter-zone, filtrado de tráfico, servicios web y FTP, así como un proxy HTTP con autenticación para el acceso a internet. Asimismo, se realizaron pruebas de conectividad y validación funcional para comprobar el correcto funcionamiento de las políticas de seguridad establecidas. La práctica fortaleció las competencias en administración de sistemas GNU/Linux, seguridad informática y gestión de redes, promoviendo el uso de buenas prácticas en la protección de servicios y recursos informáticos en entornos virtualizados.

PALABRAS CLAVE: GNU/Linux, Endian Firewall, seguridad perimetral, NAT, DMZ, VirtualBox, proxy HTTP, firewall, redes segmentadas, autenticación

1 INTRODUCCIÓN

La etapa 7 del diplomado en administración de sistemas operativos Open Source, tiene como propósito fortalecer las competencias de los estudiantes en la implementación de mecánicas de seguridad en entornos de GNU/Linux.

Esta actividad integra conceptos de seguridad perimetral, administración de servicios esenciales, segmentación de redes y control de tráfico mediante el uso de herramientas especializadas como lo son Endian Firewall, Ubuntu server, Ubuntu Desktop y VirtualBox.

A través del desarrollo de las cinco temáticas, los estudiantes se enfrentan a entornos de configurar un entorno funcional compuesto por una red LAN, una zona DMZ y una red WAN simulada, aplicando políticas de seguridad, reglas de acceso, servicios web, NAT, proxy y autenticación.

La actividad combina trabajo individual y colaborativo, permitiendo que cada estudiante documente sus procedimientos técnicos y participe en la construcción de un artículo grupal en formato IEEE.

Este proceso fomenta la comprensión integral de la seguridad en GNU/Linux, la administración de redes segmentadas y la aplicación de buenas prácticas en la protección de servicios y recursos informáticos.

2 JUSTIFICACIÓN

La seguridad informática es un componente esencial en la administración de sistemas operativos y redes corporativas. En entornos donde coexisten servicios internos, servidores expuestos y acceso a internet, es indispensable implementar mecanismos que garanticen la integridad, disponibilidad y confidencialidad de la información.

La etapa 7 permite al estudiante aplicar estos principios mediante la configuración de un entorno realista que incluyen firewall perimetral, DMZ, servicios web, reglas NAT, políticas de acceso y autenticación.

La actividad exige el uso de herramientas de administración en consola, promoviendo el dominio de comandos, l compresión del funcionamiento interno de los recursos y la capacidad de diagnosticar y resolver problemas de seguridad.

3 OBJETIVO GENERAL

Implementar y documentar un entorno de seguridad perimetral basado en GNU/Linux, configurando servicios esenciales, reglas de acceso, políticas de autenticación y mecanismos de protección en Endian Firewall y Ubuntu server y Ubuntu

Desktop, con el fin de garantizar la comunicación segura entre zonas LAN, DMZ y WAN establecidas en la etapa 7.

4 OBJETIVOS ESPECÍFICOS

Configurar la infraestructura de red requerida para la etapa 7, implementando las zona verde, naranja y roja mediante el uso de GNU/Linux, Endian Firewall, Ubuntu server, Ubuntu desktop y VirtualBox.
Implementar y asegurar los servicios esenciales en GNU/Linux, aplicando procedimientos administrativos en consola que permitan fortalecer la seguridad del sistema operativo.
Establecer políticas de seguridad perimetral mediante la configuración de reglas de acceso, NAT, filtrado de tráfico y mecanismos de autenticación, garantizando la comunicación controlada entre LAN, DMZ y WAN.
Ejecutar pruebas técnicas que validen el funcionamiento de los servicios, las reglas de seguridad y la conectividad entre los diferentes segmentos de red, evidenciando cada procedimiento mediante comandos y registros.
Documentar de manera detallada y detallada todos los procesos realizados, integrando los resultados individuales en un informe académico y el artículo colaborativo en formato IEEE.

5 INFORME DE LA ACTIVIDAD

1. **Temática 1: Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.**

2. **Temática 2: Configuración NAT**

Introducción

La traducción de direcciones de red (NAT, Network Address Translación) es una de las técnicas más utilizadas en la administración de redes modernas, debido a que permite establecer comunicación entre redes privadas y redes externas mediante la modificación de direcciones IP. En entornos corporativos y académicos, NAT constituye un mecanismo fundamental para optimizar el uso de direcciones IP, fortalecer la seguridad perimetral y controlar el acceso hacia internet.
En la presente práctica se implementó una configuración NAT utilizando GNU/Linux y herramientas Open Source como Endian Firewall, Ubuntu Server y VirtualBox. La actividad tuvo como propósito diseñar un entorno virtualizado compuesto por redes LAN, DMZ y WAN, permitiendo la comunicación entre diferentes segmentos mediante reglas de encaminamiento y traducción de direcciones.

Marco Teórico

La tecnología NAT permite modificar las direcciones IP de origen o destino de los paquetes de red mientras estos atraviesan un router o firewall. Este mecanismo es ampliamente utilizado para permitir que múltiples dispositivos de una red privada compartan una única dirección IP pública

Metodología

La implementación de la temática se desarrolló mediante las siguientes fases:

Configuración de la Topología de Red

Se diseñó una infraestructura virtual utilizando VirtualBox con tres segmentos de red:

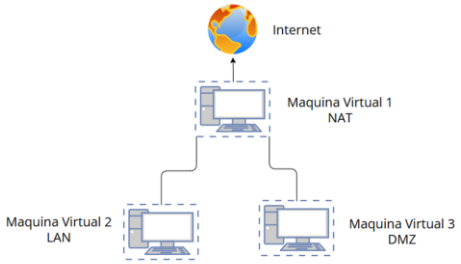
Zona LAN
Zona DMZ
Zona WAN simulada

Las máquinas virtuales utilizadas fueron: Endian Firewall, Ubuntu Server, Ubuntu Desktop

Topología Hardware

Figura 1. *Topología Configuración Nat*

Se muestra la topología general utilizada para la implementación de NAT en el entorno virtualizado, al igual que se observan las tres zonas definidas: LAN, DMZ y WAN.

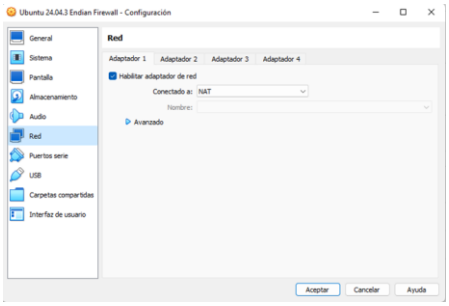


Fuente: Autoría Propia

Configuración Máquinas Virtuales

Figura 2. *Configuración Máquina Virtual NAT*

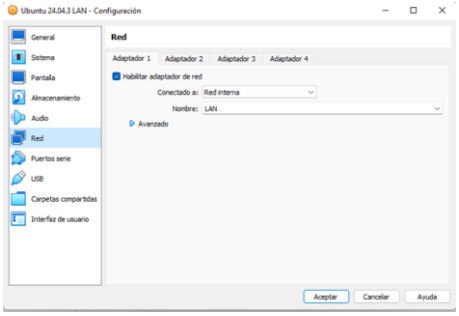
Se presenta la configuración de la interfaz de red asignada a la máquina virtual Endian Firewall en modo NAT dentro de Virtual Box.



Fuente: Autoría Propia

Figura 3. *Configuración Máquina Virtual LAN*

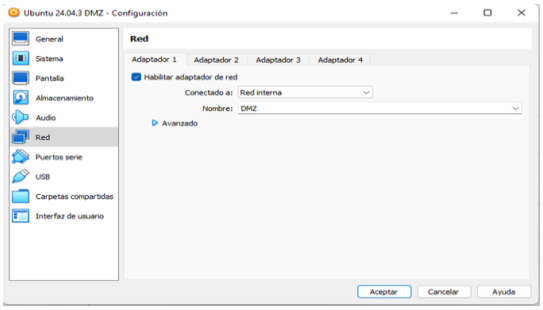
Se evidencia la configuración de la máquina virtual destinada a la zona DMZ. Se asigna una interfaz Host-Only , que permite la comunicación interna entra el cliente LAN y el firewall Endian.



Fuente: Autoría Propia

Figura 4. *Configuración Máquina Virtual DMZ*

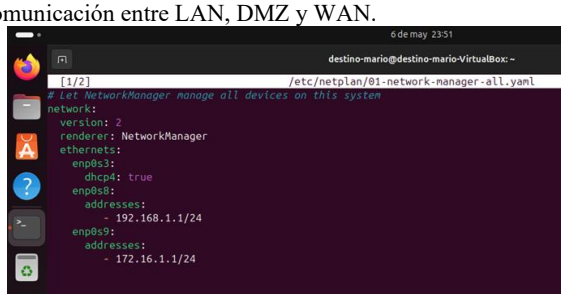
Muestra la configuración de la máquina virtual destinada a la zona DMZ. Se utiliza una interfaz Host-Only para aislar los servicios alojados en la DMZ y permitir si control mediante firewall.



Fuente: Autoría Propia

Figura 5. *Configuración Archivo YAML Firewall o NAT*

Se evidencia el archivo YAML utilizado para configurara las interfaces de red del servidor NAT mediante Netplan. Se asignaron las direcciones IP estáticas para garantizar la comunicación entre LAN, DMZ y WAN.



Fuente: Autoría Propia

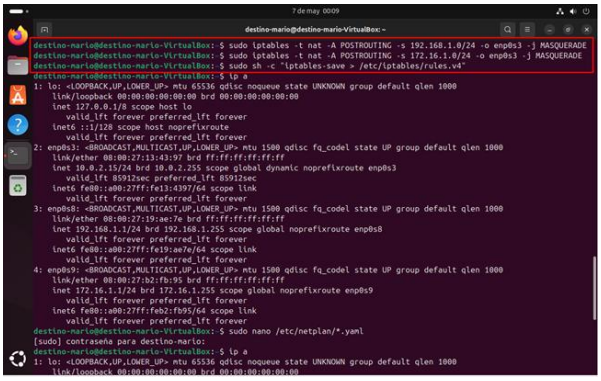
Figura 6. *Configuración Archivo Sysctl IP FORWARDING*

Habilitar el IP Forwarding para que Linux permite que los paquetes pasen de una interfaz a otra debemos activar el reenvío de ipv4 de forma definitiva.

Fuente: Autoría Propia

Figura 7. *Ejecución de comandos para agregar reglas al Firewall*

Muestra la ejecución de comando iptables utilizados para implementar la traducción de direcciones en la interfaz de salida. Esto permite que LAN y DMZ accedan a redes externas.

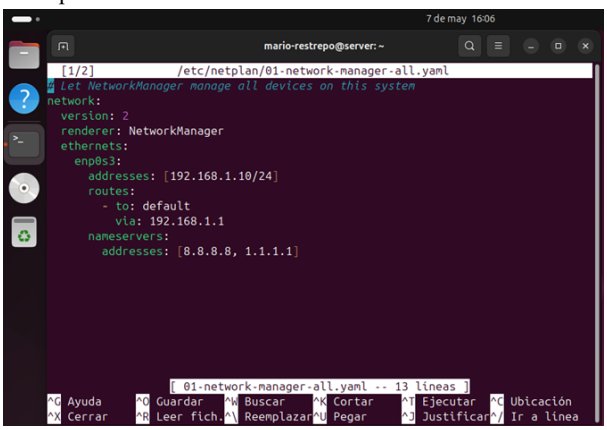


Fuente: Autoría Propia

Configuración LAN

Figura 8. *Configuración Archivo YAML LAN*

El uso del archivo YAML utilizado para configurar la interfaz de red del cliente LAN. Se asigna una IP estática y se define como puerta de enlace la IP del servidor NAT.



Fuente: Autoría Propia

Configuración DMZ

Figura 9. *Configuración Archivo YAML DMZ*

Se muestra el archivo YAML correspondiente ala configuración de la interfaz de red del servidor DMZ. Se asigna IP estática dentro del segmento 172.16.1.0/24.

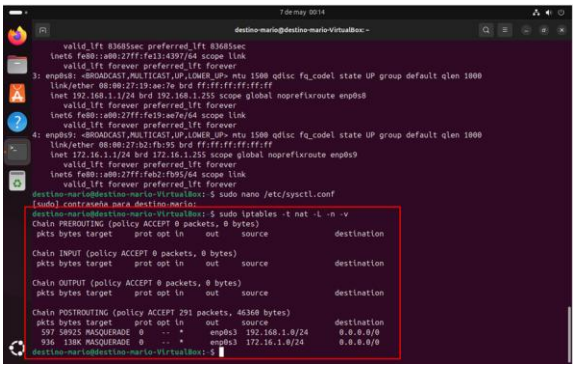
Fuente: Autoría Propia

Evidencias Configuración o Funcionamiento de NAT – LAN – DMZ

Mostrar Reglas NAT

Figura 10. *Ejecución Comando verificando las reglas creadas en iptables*

Se presenta la ejecución del comando utilizado para visualizar las reglas NAT configuradas en iptables. La salida confirma que las reglas de enmascaramiento están activas y funcionando correctamente.

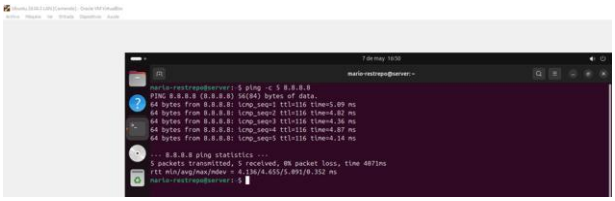


Fuente: Autoría Propia

Ping LAN

Figura 11. *Validación de conectividad a través de Ping Maquina LAN*

Se muestra la ejecución del comando 'ping' desde la maquina ubicada en la red LAN hacia el servidor NAT. La respuesta exitosa confirma que la comunicación entre LAN y el firewall está funcionando correctamente.

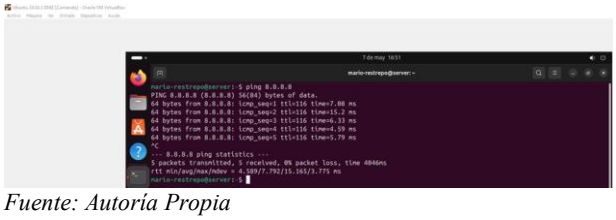


Fuente: Autoría Propia

Ping DMZ

Figura 12. ***Validación de conectividad a través de Ping Maquina DMZ***

Presenta la prueba de conectividad realizada desde la maquina ubicada en la DMZ hacia el servidor NAT. Las respuestas recibidas demuestran que la DMZ tiene comunicación estable con el firewall.



Fuente: Autoría Propia

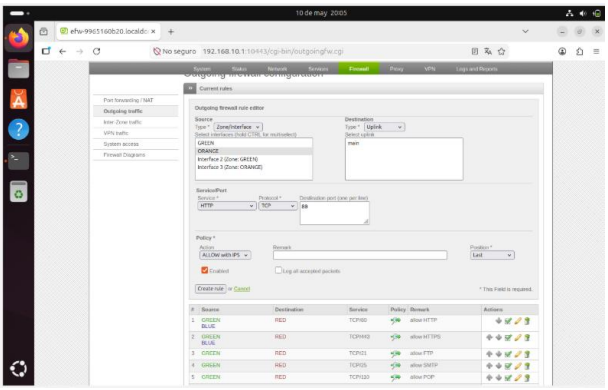
3. Temática 3: Permitir servicios de la Zona DMZ para la red.

La infraestructura implementada estuvo conformada por:
Una máquina virtual con GNU/Linux Endian Firewall.
Una máquina virtual Ubuntu Linux utilizada como cliente.
Una red interna configurada en VirtualBox.

Metodología Permitir HTTP y FTP y Bloquear ICMP para evitar respuestas de ping.

Figura 13. *Configuración para HTTP*

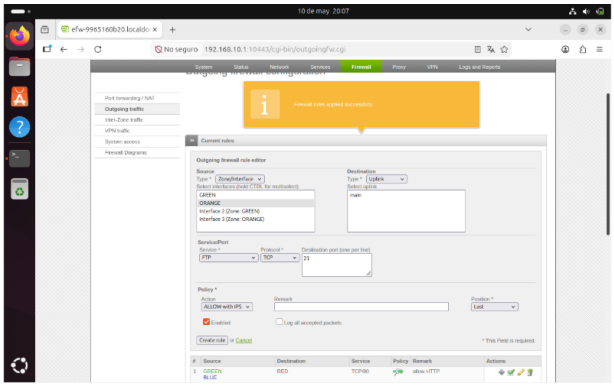
La primera regla implementada fue permitir tráfico HTTP mediante el puerto 80 desde la LAN hacia DMZ. Esta regla permite el acceso a servicios web alojados en el servidor DMZ.



Fuente: Autoría Propia

Figura 14. *Configuración para FTP*

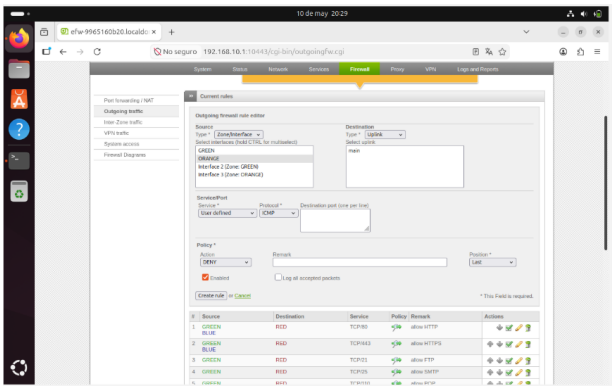
Posteriormente se configuró la regla para permitir tráfico FTP mediante el puerto 21 entre la LAN y la DMZ. Esta configuración habilita la transferencia de archivos hacia el servidor FTP ubicado en la DMZ.



Fuente: Autoría Propia

Figura 15. *Bloquear el ICMP*

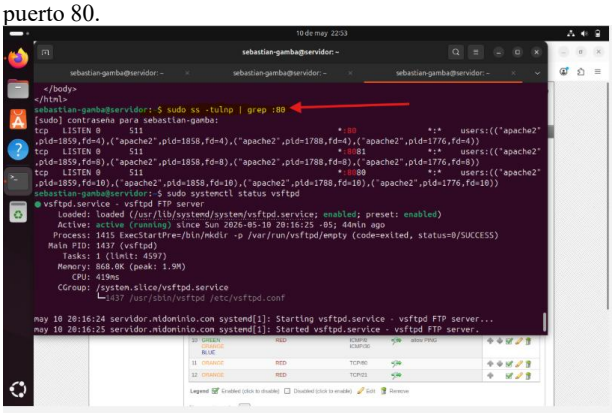
Finalmente se implementó una regla para bloquear el protocolo ICMP entre las zonas. Esta medida evita respuestas de ping, fortaleciendo la seguridad perimetral al reducir la visibilidad de los hosts.



Fuente: Autoría Propia

Figura 16. *Validamos HTTP con la IP*

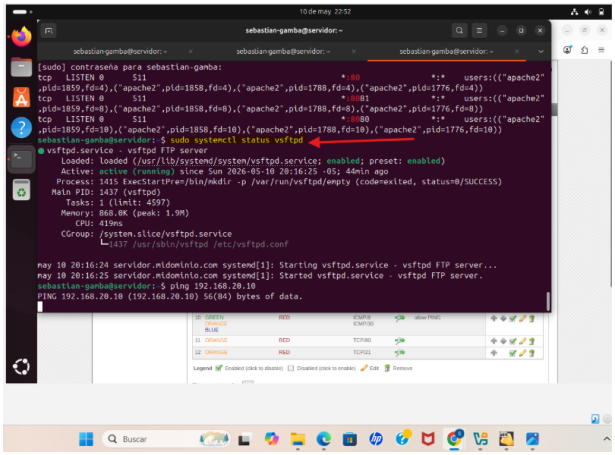
Se presenta la ejecución del comando: sudo ss -tulnp | grep :80 en el servidor DMZ. El resultado confirma que el servicio HTTP se encuentra activo y escuchando correctamente en el puerto 80.



Fuente: Autoría Propia

Figura 17. *Validamos el FTP*

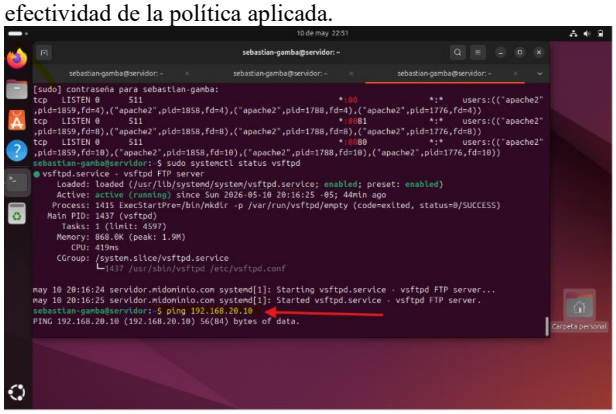
Muestra la ejecución del comando: systemctl status vsftpd, donde se verifica que el servidor FTP esta activo y funcionando correctamente en el servidor DMZ.



Fuente: Autoría Propia

Figura 18. *Bloqueo de ICMP*

Se evidencia la ejecución del comando: ping, desde LAN hacia la DMZ, donde no se recibe respuesta debido a la regla de bloqueo ICMP configurada en el firewall. Esto confirma la efectividad de la política aplicada.



Fuente: Autoría Propia

4. Temática 4: Reglas de acceso para permitir o denegar el tráfico.

Metodología

La ejecución de esta temática la realicé en tres partes:
Configuración de reglas Inter-Zona entre LAN y DMZ.
Implementación de reglas NAT para acceso WAN > DMZ.
Ejecución de pruebas de conectividad desde cada zona para validar el funcionamiento.

Configuración del firewall

Reglas Inter-Zona. Se configuran las siguientes reglas:

- HTTP (80) - Permitido
- HTTPS (443) - Permitido
- FTP (21) - Permitido
- ICMP - Denegado
- Reglas ANY predeterminadas entre zonas.

Figura 19. Reglas Inter-Zona configuradas en Endian Firewall.

Muestran las reglas Inter-Zona aplicadas entre la LAN y la DMZ, donde se permite el trafico HTTP, HTTPS y FTP, y se bloquea ICMP. Estas reglas controlan el flujo de tráfico entre segmentos según las políticas definidas.

Fuente: Autoría Propia

Creación de las reglas NAT para publicación WAN > DMZ.

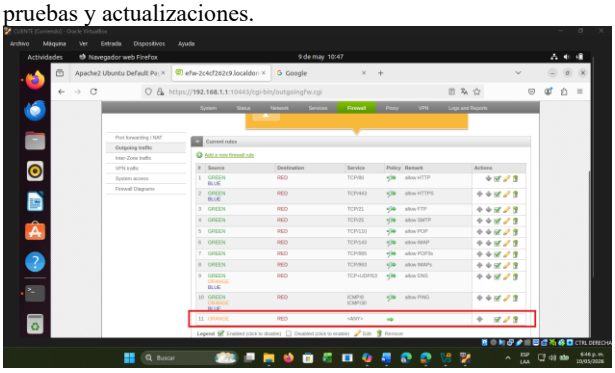
HTTP WAN > DMZ
FTP WAN > DMZ

Figura 20. Reglas NAT para publicación de servicios WAN > DMZ.

Las reglas NAT configuradas para redirigir soluciones provenientes de la WAN hacia los servicios HTTP y FTP alojados en la DMZ. Esta configuración permite la publicación segura de servicios hacia el exterior.

Fuente: Autoría Propia

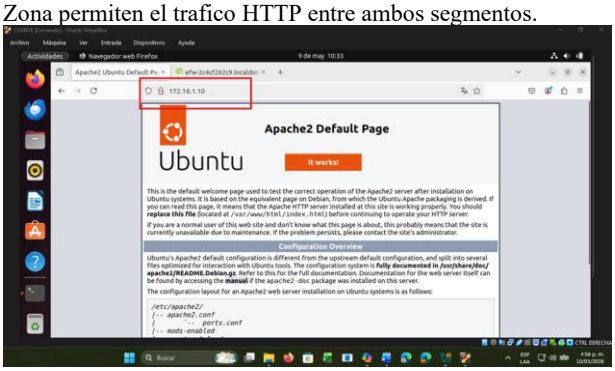
Figura 21. *Regla de salida a internet desde la DMZ.*
La regla configurada en el trafico saliente de Endian Firewall que permite quela zona DMZ tenga acceso a la WAN. Esta regla autoría la salida de cualquier servicio desde la DMZ hacia internet, garantizando la conectividad necesaria para pruebas y actualizaciones.



Fuente: Autoría Propia.

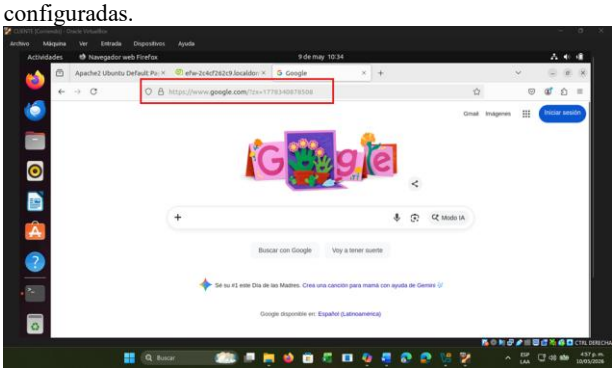
Pruebas de funcionamiento

Figura 22. *Prueba HTTP desde LAN hacia DMZ*
Presenta el acceso desde la LAN al servidor web ubicado en la DMZ mediante la dirección http://172.16.1.10. La carga correcta de la pagina Apache confirma que las reglas Inter-Zona permiten el trafico HTTP entre ambos segmentos.



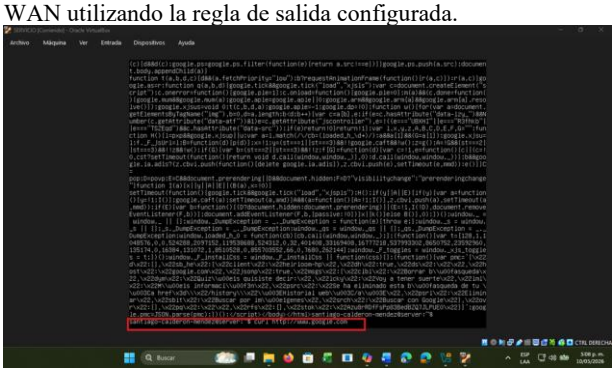
Fuente: Autoría Propia

Figura 23. Prueba *HTTP desde LAN hacia WAN*
Se muestra la navegación desde la LAN hacia el internet accediendo a Google. http://ww.google.com. Esto confirma que la LAN tiene salida a la WAN mediante las reglas NAT configuradas.



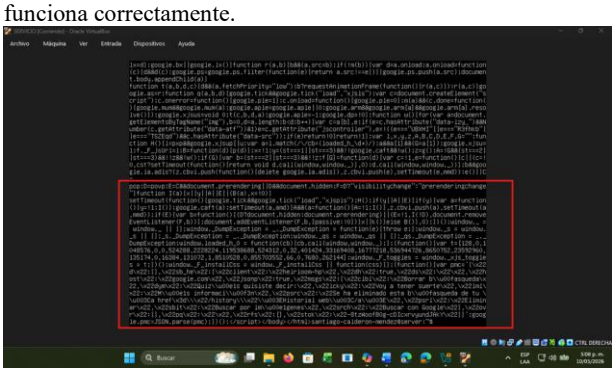
Fuente: Autoría Propia

Figura 24. *Prueba HTTP desde DMZ hacia WAN*
Evidencia la ejecución del comando curl http://www.google.com desde la DMZ. La solicitud enviada confirma que el servidor DMZ puede comunicarse con la WAN utilizando la regla de salida configurada.



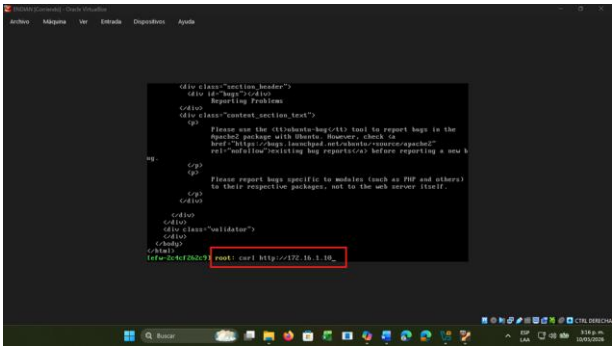
Fuente: Autoría Propia

Figura 25. *Respuesta HTML obtenida desde la DMZ hacia la WAN*
Muestra los encabezados y contenido HTML recibido tras ejecutar el comando curl desde la DMZ. Esto valida la DMZ tiene acceso completo a internet y que la regla de salida funciona correctamente.



Fuente: Autoría Propia

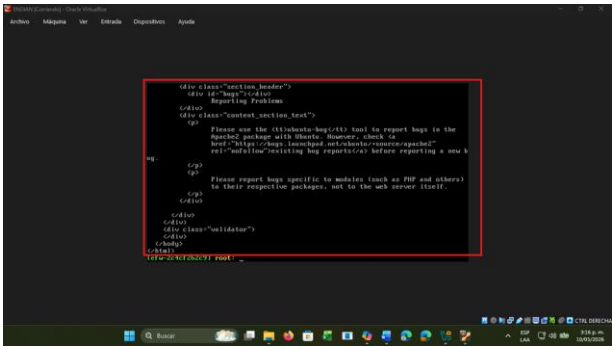
Figura 26. *Prueba HTTP desde WAN hacia la DMZ*
Presenta la ejecución del comando curl http://172.16.1.10 desde la zona WAN. La solicitud envía al servidor DMZ confirma que las reglas NAT permiten el acceso externo hacia el servicio web alojado en la DMZ.



Fuente: Autoría Propia

Figura 27. *Respuesta del servidor Apache ante solicitud desde la WAN*

Muestra la respuesta generada por el servidor Apache ubicado en la DMZ al recibir una solicitud desde la WAN. Esto confirma que el servicio esta correctamente publicado mediante NAT.

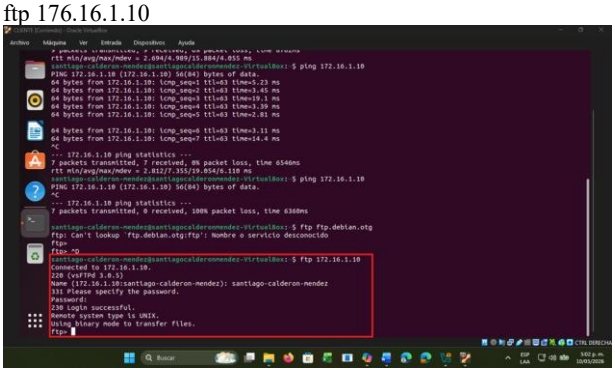


Fuente: Autoría Propia

Figura 28. *Prueba FTP desde LAN hacia WAN*

Evidencia la conexión FTP establecida desde la LAN hacia un servidor externo. La autenticación correcta demuestra que el servicio FTP funciona adecuadamente a través de la WAN.

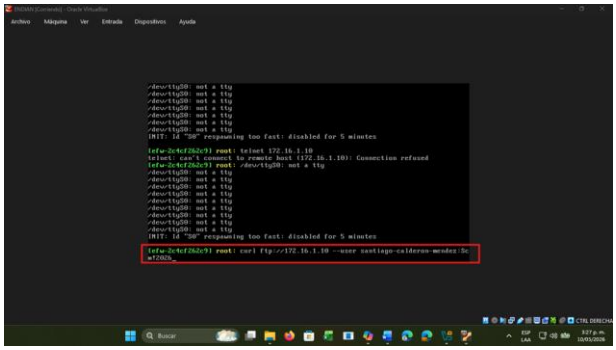
ftp 176.16.1.10



Fuente: Autoría Propia

Figura 29. *Prueba FTP desde WAN hacia DMZ con autenticación*

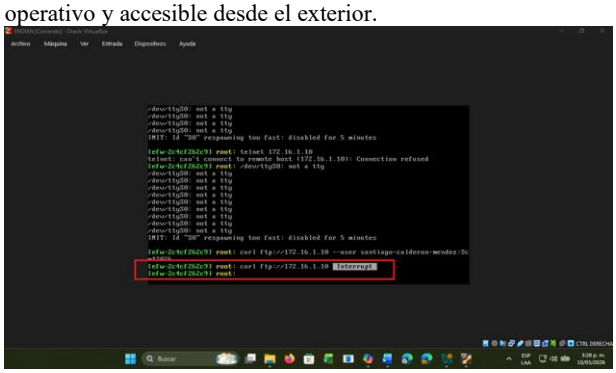
La ejecución del comando cur ftp://172.16.1.10 -- userr santiago-calderon-mendez: ¡Scm!2026 desde la WAN. La conexión y autenticación exitosa confirman que el servidor FTP esta publicado correctamente hacia la zona externa.



Fuente: Autoría Propia

Figura 30. *Confirmación de autenticación FTP desde la WAN hacia la DMZ*

Muestra la validación final el acceso FTP desde la WAN el servidor DMZ. La autenticación correcta confirma que el usuario configuración existe y que el servidor FTP este operativo y accesible desde el exterior.



Fuente: Autoría Propia

5. Temática 5: Implementar un Proxy HTTP (no transparente) con políticas de autenticación para navegación en internet.

Introducción

El proxy HTTP no transparente funciona como intermediario entre el usuario e Internet, pero a diferencia del transparente, requiere que el usuario lo configure manualmente en su navegador y se autentique antes de navegar. Esto permite saber exactamente quién accede a qué sitio y cuándo. Endian Firewall usa Squid para esto, integrando autenticación y filtrado de contenido en una sola herramienta.

Metodología

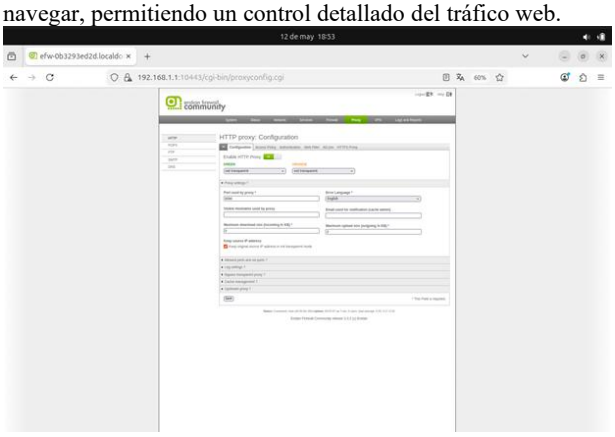
Para la implementación se usó Endian Firewall Community 3.3.2 en VirtualBox. Desde el panel web se configuró el proxy en modo no transparente para la zona GREEN en el puerto 8080. Se creó un perfil llamado Perfil Restringido con los sitios a bloquear: hotmail.com, youtube.com y elnuevodia.com.co. Luego se creó el usuario estudiante 1 y se le asignó una política de acceso vinculada a ese perfil. En el equipo cliente se configuró Firefox manualmente apuntando al proxy 192.168.1.1 puerto 8080.x manualmente apuntando al proxy 192.168.1.1 puerto 8080.

Pruebas de funcionamiento

Configuración del Proxy

Figura 31. *Configuración del Proxy HTTP no transparente en Endian Firewall*

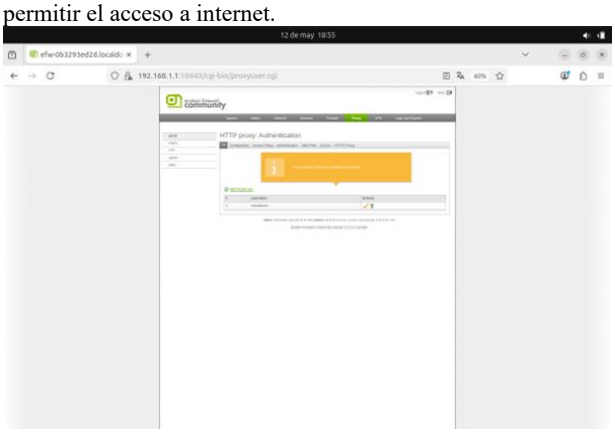
La activación del proxy HTTP en modo transparente para la zona GREEN, configurado en el puerto 8080. Esta configuración obliga a los usuarios a autenticarse antes de navegar, permitiendo un control detallado del tráfico web.



Fuente: Autoría Propia

Figura 32. *Creación del Usuario para autenticación en el Proxy HTTP*

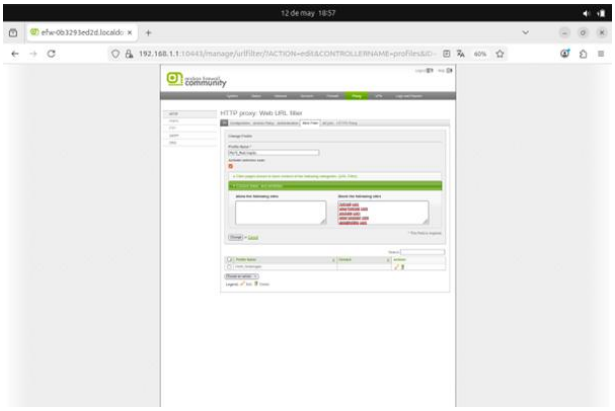
La creación del usuario destinado a autenticarse en el proxy. Este usuario será validado por el servicio Squid antes de permitir el acceso a internet.



Fuente: Autoría Propia

Figura 33. *Configuración de la lista negra personalizada en el Proxy HTTP*

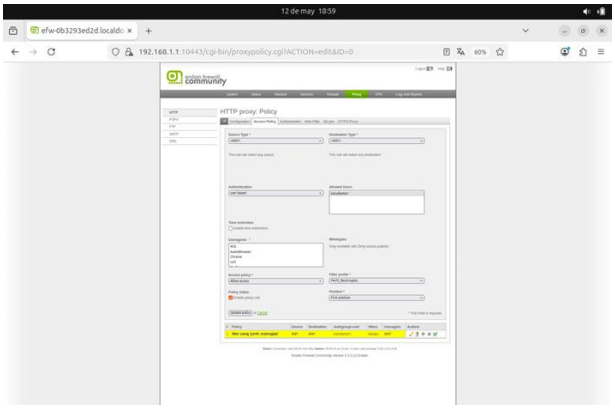
La creación del perfil del filtrado web denominado ‘perfil restringido’, donde se agregan los sitios bloqueados: hotmailo.com, youtube.com y elnuevodia.com.co. Este perfil se aplicará a los usuarios autenticados.



Fuente: Autoría Propia

Figura 34. *Configuración de la política de acceso vinculación al perfil de filtrado*

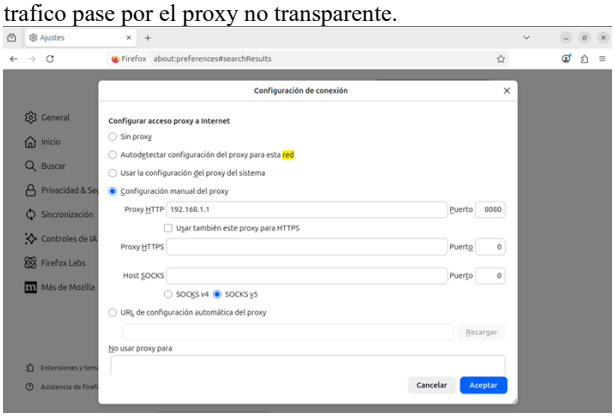
La creación de la política de acceso que asocia el usuario autenticado con el perfil de filtrado web. Esta política determina que contenido puede o no puede ser accedido por el usuario.



Fuente: Autoría Propia

Figura 35. *Configuración manual del proxy en el navegador del cliente*

La configuración del navegador Firewall, donde se establece manualmente el proxy HTTP con la dirección 192.169.1.1 y el puerto 8080. Esta configuración es necesaria para que el trafico pase por el proxy no transparente.



Fuente: Autoría Propia

Figura 36. *Autenticación del usuario en el Proxy HTTP*

Presenta la ventana de autenticación solicitada por el proxy al intentar acceder a internet. El usuario debe ingresar sus credenciales para que el proxy permita la navegación.

Fuente: Autoría Propia

Figura 37. *Bloqueo de acceso a sitio*

Muestra el mensaje de bloqueo generado por el Proxy al intentar acceder al sitio elnuevodia.com.co, incluido en la lista negra. Esto confirma el funcionamiento del filtrado web.

Fuente: Autoría Propia

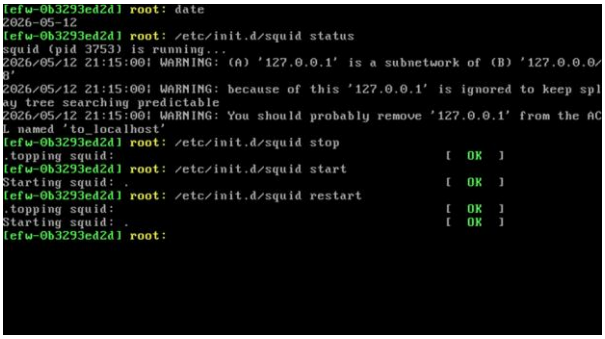
Figura 38. *Bloqueo de acceso al sitio 2*

Evidencia el boqueo exitoso del sitio hotmail.com, también incluido en la lista negra del perfil de filtrado. Esto demuestra aplicación de las políticas configuradas.

Fuente: Autoría Propia

Figura 39. *Gestión del Servicio Squid desde Consola de Endian*

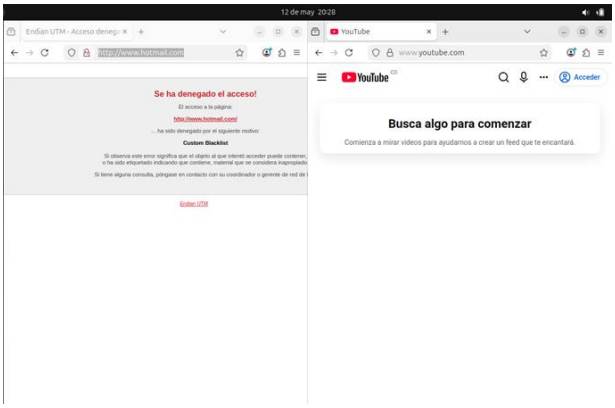
La administración del servicio Squid desde la terminal, mostrando que el servicio puede iniciarse, detenerse y reiniciarse correctamente. Esto confirma su funcionamiento estable.



Fuente: Autoría Propia

Figura 40. ***Limitación del proxy ante contenido HTTPS como YouTube***

Muestra YouTube no es bloqueado por el proxy debido a que el sitio redirige automáticamente las solicitudes HTTP hacia HTTPS. Esto evidencia una limitación del filtrado basado únicamente en HTTP.



Fuente: Autoría Propia

Conclusiones.

La implementación del entorno de seguridad perimetral basado en GNU/Linux permitió integrar y validar diferentes mecanismos de protección orientados al control seguro del tráfico entre las zonas LAN, DMZ y WAN. Mediante el uso de Endian Firewall, Ubuntu Server, Ubuntu Desktop y VirtualBox, fue posible diseñar una infraestructura funcional capaz de administrar servicios, segmentar redes y aplicar políticas de seguridad de manera centralizada.

La configuración de reglas NAT, filtrado de tráfico y políticas inter-zone permitió controlar el acceso entre segmentos de red, garantizando la comunicación únicamente entre los servicios autorizados. Las pruebas de conectividad realizadas evidenciaron el correcto funcionamiento de los servicios HTTP y FTP, así como la efectividad de las restricciones implementadas sobre protocolos como ICMP.

La implementación del proxy HTTP no transparente con autenticación permitió comprender la importancia del control de acceso y monitoreo de la navegación web en entornos corporativos. Asimismo, se identificaron limitaciones relacionadas con el filtrado de contenido HTTPS, evidenciando

la necesidad de mecanismos de inspección más avanzados para fortalecer la seguridad web.

El desarrollo de esta práctica fortalece las competencias técnicas en administración de sistemas GNU/Linux, virtualización, configuración de firewalls y gestión de servicios de red. Además, permitió comprender que la seguridad perimetral no depende de una única herramienta, sino de la integración de múltiples mecanismos de protección, monitoreo y control orientados a garantizar la disponibilidad, integridad y confidencialidad de la información.

Finalmente, la actividad permitió aplicar buenas prácticas de seguridad informática en un entorno virtualizado cercano a escenarios reales de infraestructura empresarial.

6 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). *Tema 102: Comandos GNU y Unix*. Disponible en: https://learning.lpi.org/es/learning-materials/101-500/102/
[2] Canonical. (2023). *Ubuntu Documentation*. Ubuntu. Disponible en: https://help.ubuntu.com/
[3] Debian Project. (2023). *Manual del Administrador Debian 12*. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html
[4] Oracle Corporation. (2020). *Oracle VM VirtualBox User Manual*. Disponible en: https://www.virtualbox.org/manual/
[5] Endian. (2016). *Endian UTM 3.2 Reference Manual*. Disponible en: http://docs.endian.com/3.2/utm/index.html
[6] J. LaCroix, *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*. Birmingham, UK: Packt Publishing, 2020.
[7] Netfilter Project. (2023). *iptables Documentation*. Disponible en: https://www.netfilter.org/documentation/
[8] Red Hat. (2022). *Security Guide for Red Hat Enterprise Linux*. Disponible en: https://access.redhat.com/documentation/
[9] W. Stallings, *Network Security Essentials: Applications and Standards*, 7th ed. Pearson Education, 2017.
[10] A. S. Tanenbaum y D. Wetherall, *Redes de Computadoras*, 5.ª ed. México: Pearson Educación, 2012.
[11] Squid Software Foundation. (2023). *Squid Proxy Server Documentation*. Disponible en: http://www.squid-cache.org/Doc/
[12] Cisco Networking Academy. (2021). *Introduction to Cybersecurity*. Cisco Press.
[13] E. Nemeth, G. Snyder y T. Hein, *UNIX and Linux System Administration Handbook*, 5th ed. Pearson, 2017.
[14] Open Web Application Security Project (OWASP). (2023). *OWASP Top Ten Web Application Security Risks*. Disponible en: https://owasp.org/www-project-top-ten/
[15] R. McMillan, *Linux Networking Cookbook*. O'Reilly Media, 2017.
[16] M. Rash, *Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort*. No Starch Press, 2007.
[17] Ubuntu Server Documentation Team. (2023). *Netplan Configuration Examples*. Disponible en: https://netplan.io/examples
[18] VMware y Virtualización Open Source. (2021). *Conceptos de Virtualización y Redes Virtuales*. Disponible en: https://www.vmware.com/topics/glossary/content/virtual-networking.html