IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL BASADO EN ENDIAN FIREWALL

Esteban Zapata Lotero
e-mail: ezapatal@unadvirtual.edu.co
Jonathan Arenas López
e-mail: e-mail: jarenasl@unadvirtual.edu.co
Juan Camilo López Galeano
e-mail: jclopezgal@unadvirtual.edu.co
Luis Guillermo Gallego Patiño
e-mail: lggallegop@unadvirtual.edu.co

RESUMEN: *Este articulo consolida el resultado del laboratorio practico desarrollado a lo largo de la fase 7 de la opción de grado diplomado de profundización en administración de sistemas operativos open source con certificación en Linux. Para ello se simuló una red virtualizada con el hipervisor VirtualBox; la red estaba constituida por un equipo desktop, un server y una máquina virtual que funciona como firewall gracias a la distribución Endian del sistema operativo Linux. Una vez la red estuvo funcional y se definió su topología, cada integrante del grupo implementó los mecanismos de seguridad perimetral propuestos en la guía, entre ellos la creación de reglas de Traducción de Direcciones de Red (NAT), de reglas de firewall para servicios HTTP y FTP, y la implementación de un proxy. Los resultados del laboratorio practico fueron el insumo a partir del cual se construyó el presente documento.*

PALABRAS CLAVE: Endian Firewall, NAT, Proxy, Linux.

1 INTRODUCCIÓN

La virtualización de infraestructuras de red en el ámbito académico y formativo ha abierto una oportunidad significativa para replicar escenarios de red complejos en entornos controlados, sin incurrir en los costos asociados al hardware físico. Herramientas como VirtualBox permiten construir topologías de red completas sobre un único equipo host, posibilitando la implementación de laboratorios orientados a la práctica de conceptos de administración y seguridad informática.

La seguridad perimetral constituye uno de los pilares fundamentales en la protección de infraestructuras de red. Su objetivo principal es establecer una frontera de control entre redes de diferente nivel de confianza (típicamente, la red interna de una organización y la red pública) mediante el uso de dispositivos como firewalls y zonas desmilitarizadas (DMZ). En este contexto, Endian Firewall es una solución de código abierto ideal para entornos de formación, gracias a su interfaz de administración intuitiva y su alto grado de personalización.

El presente artículo describe el diseño y construcción de una red virtual sobre VirtualBox que sirve como plataforma para la implementación de los ejercicios prácticos de seguridad perimetral propuestos en la guía de evaluación, utilizando Endian Firewall como dispositivo central de protección. Se detalla la configuración de los adaptadores de red virtuales, la segmentación en zonas de confianza (ROJA, VERDE y NARANJA), y la definición de reglas de firewall que permiten a los estudiantes experimentar con escenarios reales de control de tráfico

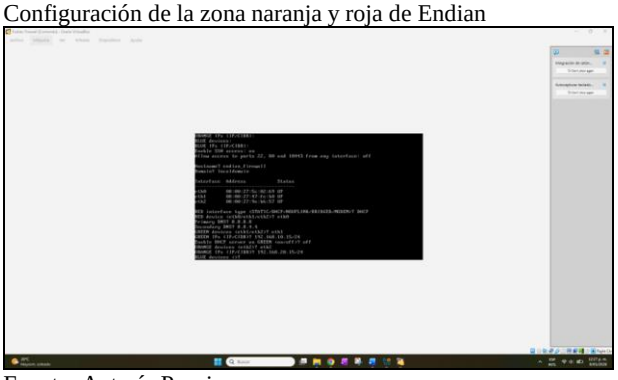
2 TEMÁTICA 1: CONFIGURACIÓN DE ENDIAN.

2.1 CARACTERÍSTICAS GENERALES

La configuración de la máquina Endian se realizó inicialmente durante el proceso de instalación mediante el asistente del sistema, para ello se utilizó un esquema GREEN + RED + ORANGE mediante VirtualBox, segmentando el entorno en tres zonas: LAN (Ubuntu Desktop), DMZ (Ubuntu Server) y WAN (Salida a Internet). En cuando al direccionamiento IP de la red, se asignó la dirección 192.168.10.15 a la puerta de enlace de la zona GREEN y la IP 192.168.20.15 a la zona ORANGE. La interfaz RED se configuró por medio del protocolo DHCP para la conectividad a internet.

Posteriormente, se asignaron las interfaces de red correspondientes a cada zona y se configuraron los tres adaptadores de red en VirtualBox.

Figura 1.
Configuración de la zona naranja y roja de Endian

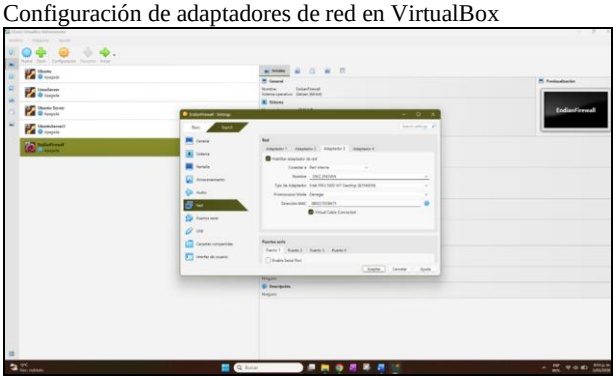


Fuente: Autoría Propia

2.2 CONFIGURACIÓN DE LA INSTANCIA DE GNU/LINUX ENDIAN

En el desarrollo individual de la Temática 1 se realizó la configuración integral de una instancia GNU/Linux Endian Firewall sobre VirtualBox, incluyendo la preparación de las tarjetas de red que dan soporte a la arquitectura de seguridad perimetral de tres zonas (verde, roja y naranja) requerida para el escenario colaborativo del curso. En consecuencia, se asignaron las interfaces de red a cada zona y se configuraron los adaptadores de red virtuales en el hipervisor VirtualBox.

Figura 2.
Configuración de adaptadores de red en VirtualBox



Fuente: Autoría Propia

2.3 PLANIFICACIÓN DE LA INFRAESTRUCTURA VIRTUAL

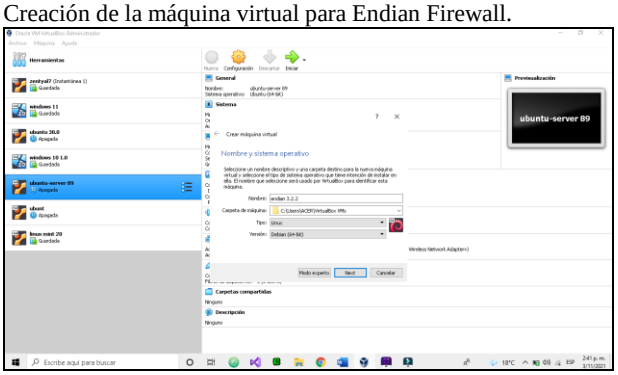
La arquitectura propuesta se compone de tres redes virtualmente aisladas conectadas a través de un firewall, cada una asociada a un nivel de confianza específico. La zona verde aloja la red interna de las estaciones de trabajo con segmento de red 192.168.10.0/24 y la interfaz interna del firewall en 192.168.10.1. La zona roja conecta el firewall con internet (red simulada para el ejercicio académico) con segmento 192.168.1.0/24 y la interfaz externa en 192.168.1.100 con puerta de enlace 192.168.1.1. La zona naranja, destinada a la DMZ donde se alojan los servidores web Ubuntu Server, recibe el segmento 192.168.20.0/24 con la interfaz del firewall en 192.168.20.1.

Esta planificación respeta la libertad operativa que la guía concede a los integrantes del grupo para definir el direccionamiento IP, manteniendo la consistencia entre todos los miembros del equipo durante el desarrollo de las temáticas subsiguientes.

2.4 CREACIÓN Y CONFIGURACIÓN DE LA MÁQUINA VIRTUAL

Deje un espacio en blanco después del título. En el hipervisor VirtualBox se crea la máquina virtual para Endian Firewall, asignándole los recursos mínimos necesarios para su operación, esto es 1 GB de memoria RAM y 20 GB de disco virtual de en formato VDI dinámico. Posteriormente se configuran tres adaptadores de red, cada uno asociado a una de las zonas planificadas (verde, roja y naranja).

Figura 3.
Creación de la máquina virtual para Endian Firewall.

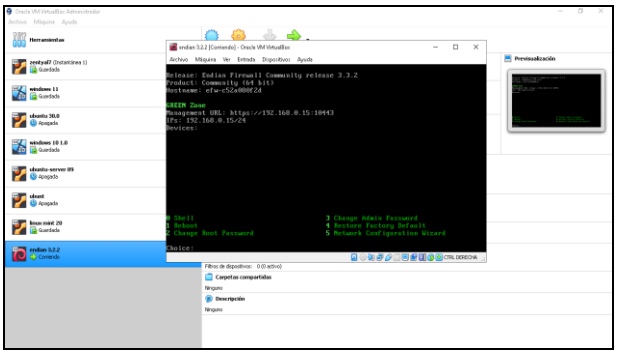


Fuente: Autoría Propia

2.5 INSTALACIÓN DE ENDIAN FIREWALL

Con la máquina virtual configurada se utiliza la imagen ISO del sistema operativo Endian Firewall Community Edition (versión 3.2.2) en la unidad óptica virtual. El instalador se ejecuta en modo consola siguiendo el flujo: i) selección de idioma, ii) aceptación del acuerdo de licencia, iii) particionamiento automático del disco virtual, iv) configuración del teclado, v) definición de la contraseña root y vi) configuración inicial de las interfaces de red.

Figura 4.
Pantalla final de la instalación de Endian Firewall.

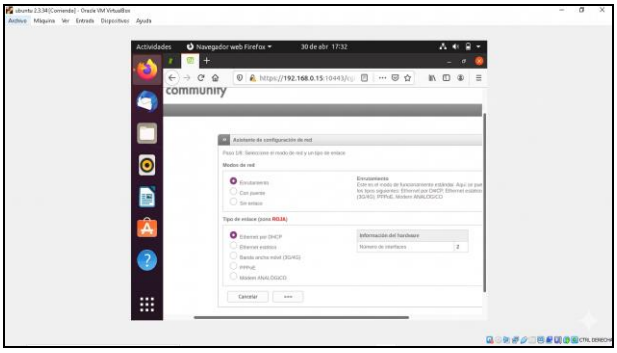


Fuente: Autoría Propia

2.6 CONFIGURACIÓN DE INTERFACES Y ZONAS

Una vez finalizada la instalación, se accede al asistente avanzado de Endian para parametrizar el modo de red, el tipo de enlace de la zona roja y la activación de la zona naranja DMZ. Se selecciona el modo de red “Enrutamiento” con enlace DHCP para la zona roja, garantizando la asignación automática de IP por parte del router de la red anfitriona. Posteriormente se habilita la zona naranja para que servirá como DMZ para alojar los servidores expuestos.

Figura 5.
Configuración del modo de red Enrutamiento con enlace DHCP



Fuente: Autoría Propia

2.7 VALIDACIÓN OPERATIVA POR CONSOLA

Una vez instalado el sistema, se ingresa al modo consola con las credenciales de usuario root y se ejecutan los comandos exigidos por la guía para verificar el estado de los servicios esenciales del firewall: i) inspección de la configuración de interfaces de red con los comandos *ifconfig* e *ip addr*, ii) verificación de la tabla de enrutamiento con los comandos *route -n* e *ip route*, y iii) consulta del estado de los servicios principales (firewall, dhcp, ntp) mediante el comando *service status*.

2.8 RESULTADOS DE LA IMPLEMENTACIÓN DE LA RED SIMULADA

La implementación de Endian Firewall sobre VirtualBox demuestra la viabilidad de construir un entorno de seguridad perimetral robusto utilizando exclusivamente software de código abierto. La arquitectura de tres zonas (verde, roja y naranja) permite segregar lógicamente los activos de la organización según su nivel de exposición y de confianza, y constituye la base para la implementación de las políticas de NAT, control de tráfico inter-zona y proxy's que se desarrollan en las siguientes temáticas.

La planificación previa del direccionamiento IP y de los tipos de adaptador en VirtualBox resulta crítica para el éxito de la instalación. El uso de la modalidad "Red interna" con nombres consistentes ("verde", "naranja") garantiza el aislamiento entre los segmentos virtuales y, al mismo tiempo, facilita la comunicación controlada entre las zonas a través del firewall.

La ejecución de los procesos en modo consola sin interfaces gráficas refuerza el aprendizaje propio de los administradores Linux profesionales. Los comandos de gestión de servicios *(start, stop, restart, status*) y de inspección de la configuración de red *(ifconfig, ip, route*) constituyen los fundamentos que deben tener los administradores, y que son reproducibles sobre cualquier distribución GNU/Linux, no solo sobre Endian

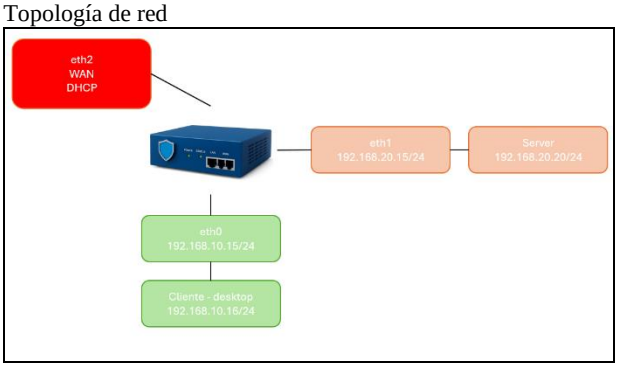
3 TEMÁTICA 2: CONFIGURACIÓN NAT.

3.1 CONSIDERACIONES PREVIAS

El desarrollo de esta temática se realizó en un entorno virtualizado con el hipervisor VirtualBox. Se desplegaron tres máquinas virtuales: i) equipo desktop con Linux mint, ii) servidor Ubuntu, y iii) firewall con distribución Endian. La comprobación funcional de los resultados esperados se realizó a través de capturas de pantalla del entorno simulado.

La topología de red se implementó de acuerdo con la propuesta realizada en la temática 1. Bajo esa perspectiva fue necesario concretar la asignación de direcciones IP a las subredes elegidas en la primera temática. Para ello se propuso una topología de red en estrella; según Cepeda - López "En una red estrella todos los nodos están conectados a un nodo central llamado nodo central neurálgico" (2008, p.12) [1]. En la red implementada, el nodo central es el firewall, al cual se conectan el servidor (Zona Naranja) y las estaciones de trabajo (Zona Verde) por sus respectivas interfaces.

Figura 6.
Topología de red

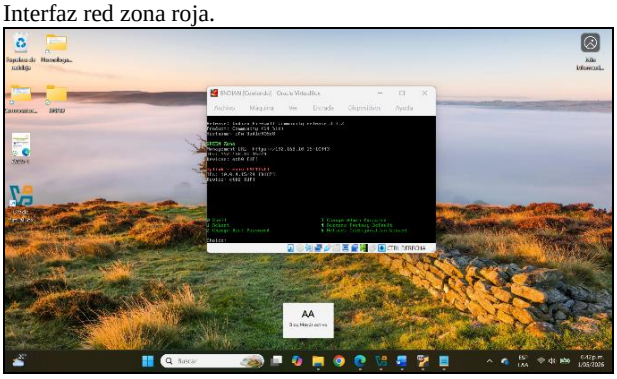


Fuente: Autoría Propia

El firewall "Es un servicio que permite filtrar información, a través del monitoreo constante del contenido entrante en la red, donde de acuerdo con las políticas establecidas" (Valencia *et al.*, 2020, p.88) [2]. Por ello, Endian es una herramienta valiosa para implementar soluciones de seguridad perimetral basadas en la delimitación de zonas según diferentes niveles de exposición y confianza.

Como último punto de las cuestiones que se deben documentar previo al desarrollo de la temática, se encuentra aquella relacionada con la asignación de la dirección IP mediante la cual la red privada se comunica con la red pública (Zona Roja). En esta actividad la interfaz de red de la zona roja se configuró con el servicio DHCP, por lo que existe una asignación aleatoria de dirección IP. Para el caso concreto el servidor DHCP asignó la dirección IP 10.0.4.15/24.

Figura 7.
Interfaz red zona roja.



Fuente: Autoría Propia

3.2 CONFIGURACIÓN DE REGLA NAT PARA COMUNICACIÓN DESDE LAN HACIA WAN

Para abordar desde la práctica este punto, primero debemos conceptualizar que es una NAT; Chimento 2015 establece que "Network Address Translation (NAT) o Traducción de Direcciones de Red es una técnica que modifica la información de dirección IP en la cabecera de un paquete IP mientras el mismo es transmitido de una red a otra por medio de un router" (2015, p.1) [3]. Esta técnica hace posible que todos los equipos de una red privada accedan a la red pública utilizando únicamente una dirección IP pública.

Una vez instalado Endian en la maquina desktop, y sin que se hayan configurado políticas de firewall, la comunicación entre el equipo y la red pública (Zona Roja) es imposible. Endian dispone de una interfaz de usuario que permite crear de manera visual políticas de salida para el tráfico desde la red privada hacia la red pública. Para ello se accede a la ruta Firewall > Trafico de salida > Añadir una nueva regla al firewall.

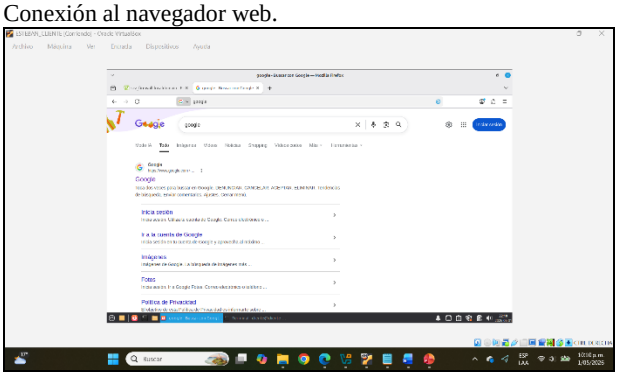
Figura 8.
UI para la creación de reglas de firewall.

Fuente: Autoría Propia

Allí se despliega un formulario donde se parametriza el origen y el destino del tráfico (agrupados por zonas), el tipo de servicio, el protocolo y el puerto del servicio; y finalmente el tipo de acción de la regla (permitir o denegar). Una vez la regla ha sido creada, el usuario puede establecer la prioridad que le asigna a la regla a través de un posicionamiento en lista descendente, mientras más cercana se encuentra una regla a la posición número 1, mayor prioridad se le asigna, y consecuentemente las reglas inferiores que le sean contrarias o incompatibles no se aplicarán.

Para dar cumplimiento al requerimiento de comunicación entre la Zona Verde (LAN) y la Zona Roja (WAN), se creó una regla que permite comunicación del servicio HTTPS a través del puerto 443, teniendo como origen la Zona Verde y como destino la Zona Roja. Una vez la regla fue creada y aplicada, el equipo desktop pudo establecer comunicación con la red pública, situación que se corroboró mediante la conexión al navegador web Google.

Figura 9.
Conexión al navegador web.



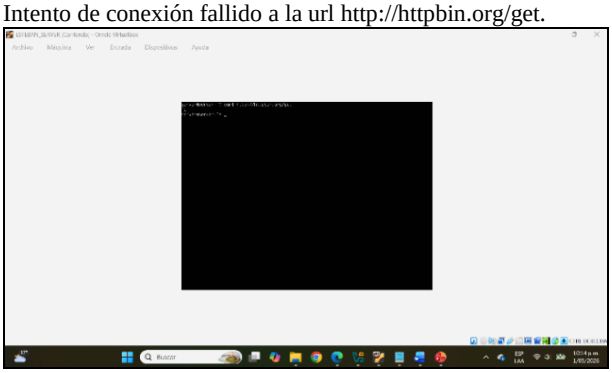
Fuente: Autoría Propia

3.3 CONFIGURACIÓN DE REGLA NAT PARA COMUNICACIÓN DESDE DMZ HACIA WAN

El servidor Ubuntu con el que se simuló la red propuesta en esta fase no tiene implementado ningún servicio. Por ello para comprobar si existe tráfico desde este equipo hacia la red pública se utilizó el comando *curl*, en la documentación de la empresa Canonical Ltd se ahonda sobre este comando "es una herramienta para transferir datos desde o hacia un servidor, utilizando uno de los protocolos compatibles (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET y TFTP)" [4], por ello se consideró pertinente el uso de este comando para validar conectividad con el servidor a pesar de no tener implementado ningún servicio en él.

En un primer momento se evaluó la falta de conectividad desde el servidor hacia internet al intentar establecer comunicación con la url http://httpbin.org/get, mientras no exista la regla de firewall o no se encuentre activa, el servidor no puede obtener el formato JSON esperado.

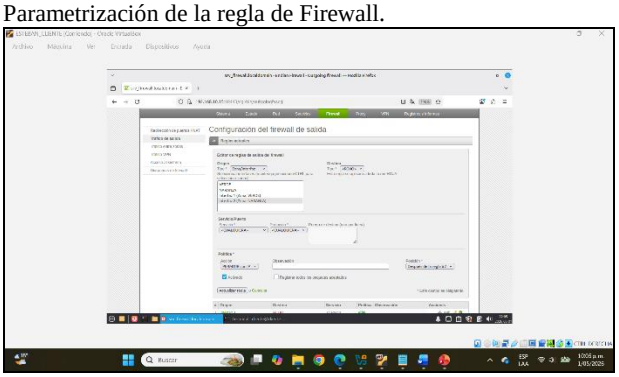
Figura 10.
Intento de conexión fallido a la url http://httpbin.org/get.



Fuente: Autoría Propia

Para establecer comunicación entre DMZ y WAN es necesario crear una regla de firewall, en consecuencia, se debe seguir la ruta expuesta en el numeral anterior (Firewall > Trafico de salida > Añadir una nueva regla al firewall). Allí se parametriza la Zona Naranja como origen, la Zona Roja como destino, y se permite el tráfico de los servicios que se estimen pertinentes; para el caso del ejercicio práctico se habilitó el tráfico de todos los servicios.

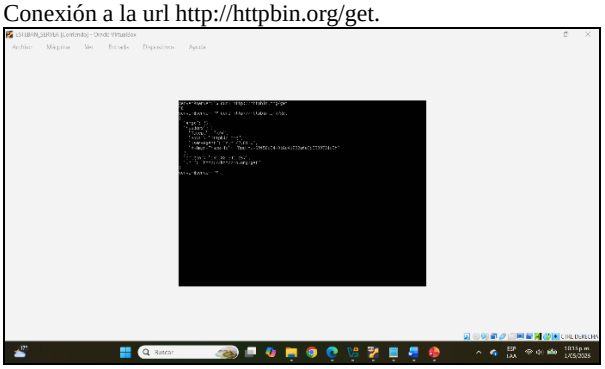
Figura 11.
Parametrización de la regla de Firewall.



Fuente: Autoría Propia

Finalmente se crea la regla de firewall y se aplica, una vez efectuada esta configuración, desde el servidor se ejecuta el comando curl http://httpbin.org/get; en esta oportunidad la url retorna un archivo en formato JSON, que es la respuesta esperada de acuerdo con la documentación de la url consumida.

Figura 12.
Conexión a la url http://httpbin.org/get.



Fuente: Autoría Propia

4 TEMÁTICA 3: PERMITIR LOS SERVICIOS DE LA ZONA DMZ.

Para el desarrollo de la actividad se utilizó VirtualBox para la creación de tres máquinas virtuales: un cliente Ubuntu Desktop, un servidor Ubuntu Server y un firewall Endian. Se configuraron redes internas para simular un entorno real con segmentación de red. Durante la instalación de Endian, se definieron tres zonas (GREEN, ORANGE y RED), asignando direcciones IP a cada interfaz. Luego, se accedió a la interfaz gráfica del firewall para configurar las reglas que permiten el acceso a servicios HTTP y FTP desde la LAN hacia la DMZ, y se bloqueó el protocolo ICMP para impedir la comunicación mediante el comando ping.

Figura 13.
Proceso de instalación de Endian en la máquina virtual.

Fuente: Autoría Propia

4.1 CONFIGURACIÓN DE REGLAS DE ACCESO (HTTP Y FTP).

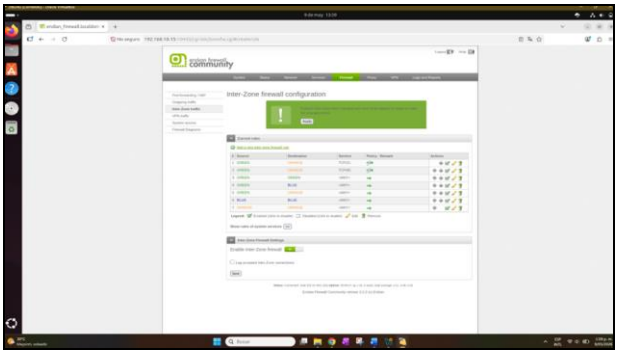
. En el dispositivo Ubuntu Server se instalaron los servicios HTTP y FTP. Para el servicio web se utilizó Apache, verificando su funcionamiento mediante el acceso desde un navegador en el cliente y para el servicio FTP se empleó el software vsftpd (Very Secure FTP Daemon) que es definido por Armijos como “un servidor de transferencia de archivos gratuito para sistemas operativos tipo Unix.” (2025, p.22) [5].

Para permitir el tráfico web y la transferencia de archivos hacia el servidor Ubuntu Server ubicado en la DMZ, se

configuraron reglas enfocadas en los protocolos TCP. Se habilitó el puerto 80 para el servicio HTTP, el cual permite la visibilidad de los aplicativos webs, y el puerto 21 para el servicio FTP el cual asegura la transferencia de datos. Las reglas de firewall que se implementaron en la interfaz web de Endian, utilizando la opción de tráfico entre zonas (Inter-Zone traffic) fueron:

- Margen izquierdo: 2.54 cm.Permitir tráfico HTTP (puerto 80) desde GREEN hacia ORANGE.
- Permitir tráfico FTP (puerto 21) desde GREEN hacia ORANGE.

Figura 14.
Panel de Endian donde se listan las reglas de los puertos 80 y 21 en estado "Allow"



Fuente: Autoría Propia

4.2 RESTRICCIÓN DEL PROTOCOLO ICMP

El protocolo ICMP es utilizado para verificar la conectividad entre equipos en una red, siendo el comando ping su principal aplicación, como señala Gil "ICMP es un protocolo empleado por los routers (encaminadores) y por los hosts (clientes, servidores, etc) para comunicar la información de control o de error de la red" (2009, p.2) [6]. En esta práctica se configuró una regla en el firewall Endian para bloquear el protocolo ICMP, impidiendo la comunicación mediante ping entre la red LAN y la DMZ. Las restricciones en el firewall se utilizan para proteger la red, controlar el tráfico y permitir únicamente los servicios necesarios; la regla configurada en Inter-Zone traffic fue:

- Denegar el protocolo ICMP entre GREEN y ORANGE

Figura 15.
Panel de Endian donde se observa la política de denegación del protocolo ICMP.

Fuente: Autoría Propia

4.3 RESULTADOS

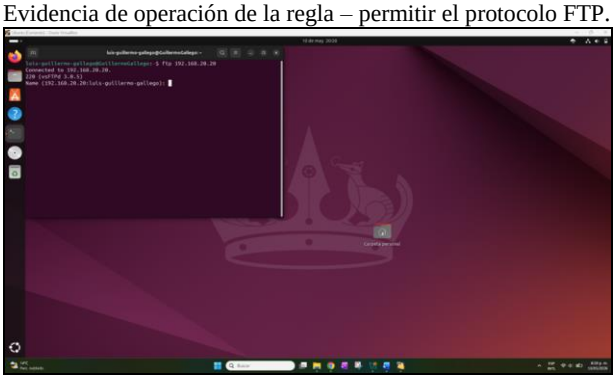
Como resultado de la implementación se logró establecer comunicación entre las máquinas virtuales a través del firewall Endian. Se verificó el funcionamiento del servicio HTTP mediante acceso web, así como el servicio FTP mediante autenticación de usuarios.

Figura 16.
Operación de la regla – permitir servicios HTTP.

Fuente: Autoría Propia

Las reglas configuradas en el firewall Endian permiten controlar el acceso a los servicios de forma específica. Se habilitaron los servicios necesarios como HTTP y FTP, mientras que se bloqueó ICMP para mejorar la seguridad, evitando que se pueda identificar fácilmente la red mediante herramientas como ping.

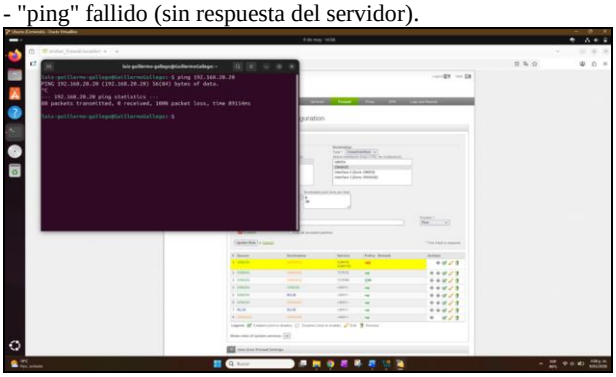
Figura 17.
Evidencia de operación de la regla – permitir el protocolo FTP.



Fuente: Autoría Propia

Se validó el funcionamiento del firewall mediante el análisis de logs, donde se evidenció el tráfico permitido y bloqueado. Como explica Bolaños, la seguridad perimetral en contextos de redes informáticas "es una forma de poner una barrera o frontera lo más inexpugnable posible entre nuestra red interna e internet" (2018, p.24) [7].

Figura 18.
Evidencia de operación de la regla denegar el protocolo ICMP - "ping" fallido (sin respuesta del servidor).



Fuente: Autoría Propia

5 TEMÁTICA 5: IMPLEMENTACIÓN DE PROXY HTTP NO TRANSPARENTE CON AUTENTICACIÓN

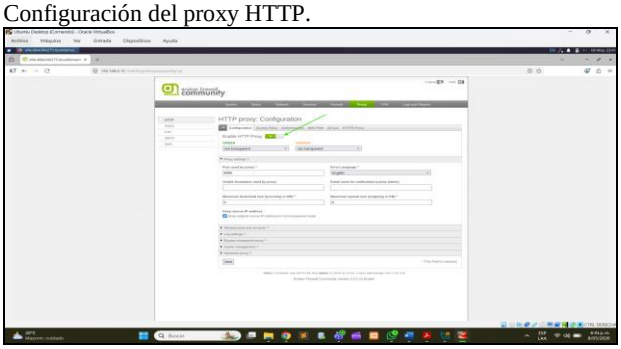
El uso de servidores proxy en infraestructuras de red empresariales permite mejorar el control, monitoreo y administración del tráfico de navegación de los usuarios. Además de optimizar el acceso a Internet, estas herramientas proporcionan mecanismos de seguridad orientados a la autenticación, filtrado de contenido y aplicación de políticas de acceso centralizadas.

Arismendy et al definen un proxy como "un punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo" (2019, p.5) [8], en ese orden de ideas la navegación mediada por un proxy permite implementar reglas de seguridad perimetral más complejas que protejan la red interna.

La implementación y validación de las políticas de acceso se realizaron en un entorno virtualizado que permitió la simulación de la infraestructura de red y ejecución de las pruebas de conectividad, autenticación y control de navegación desde los equipos cliente de la red LAN. Para la configuración del proxy HTTP no transparente se utilizó Endian Firewall Community, permitiendo que los equipos cliente establecieran conexión a Internet únicamente mediante autenticación previa.

Los mecanismos de filtrado y control de acceso a red implementados mediante firewalls y servidores proxy permiten fortalecer las políticas de seguridad dentro de las infraestructuras de red empresariales, facilitando la administración centralizada del tráfico y restringiendo el acceso a contenidos no autorizados. Para abordar el concepto de control de acceso a red acudimos a Ávila et al, quienes definen este tipo de medidas son "una aplicación del firewall que revisa los equipos que acceden a la red para comprobar que cumplan con todas las políticas de seguridad, como son actualizaciones de los antivirus, del sistema operativo y de aplicaciones." (2022, p.3) [9].

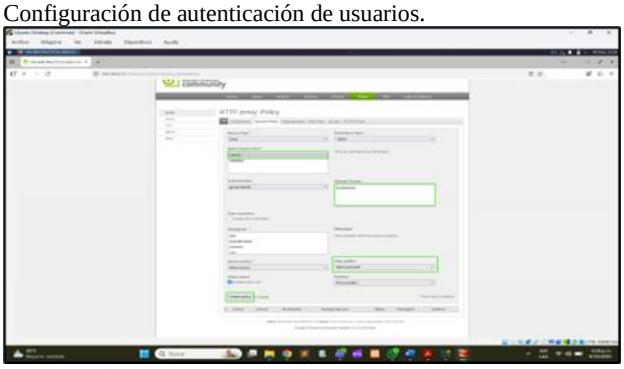
Figura 19.
Configuración del proxy HTTP.



Fuente: Autoría Propia

La configuración del mecanismo de autenticación de usuarios dentro del servicio proxy, permitió controlar el acceso a Internet únicamente mediante credenciales previamente registradas por el administrador, permitiendo de esta manera aplicar políticas de navegación diferenciadas y mejorar el control de acceso sobre los recursos de red, fortaleciendo las medidas de seguridad implementadas en la infraestructura.

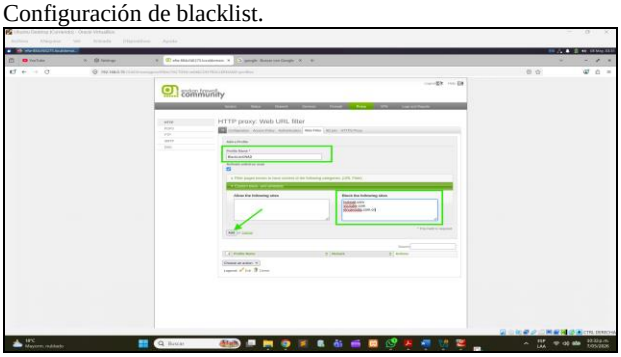
Figura 20.
Configuración de autenticación de usuarios.



Fuente: Autoría Propia

Asimismo, se aplicaron las políticas de filtrado mediante listas negras (blacklist), restringiendo el acceso a plataformas específicas definidas por el administrador de red. En cuanto a las listas negras, Álvarez propuso su importancia para la ciberseguridad de la siguiente manera “Las listas negras de IP son herramientas utilizadas para identificar y bloquear direcciones IP asociadas con actividades maliciosas, como el envío de spam, ataques DDoS y otras formas de cibercrimen” (2024, p.7) [10].

Figura 21.
Configuración de blacklist.

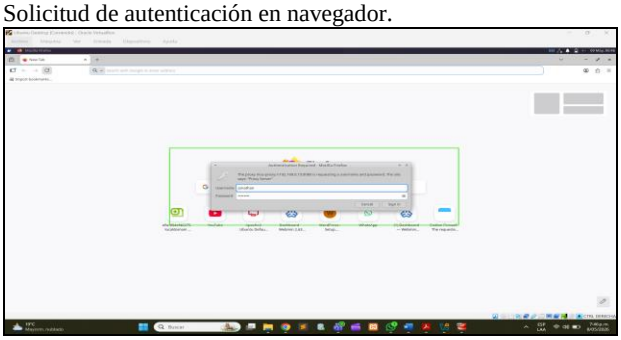


Fuente: Autoría Propia

5.1 RESULTADOS

Las pruebas realizadas permiten verificar el correcto funcionamiento del servicio proxy implementado. Inicialmente, los equipos cliente conectados a la red LAN fueron redireccionados al servicio de autenticación configurado en el firewall, validando las credenciales de acceso antes de permitir la navegación web.

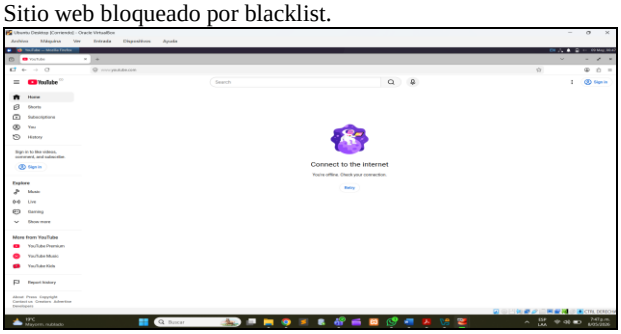
Figura 22.
Solicitud de autenticación en navegador.



Fuente: Autoría Propia

Posteriormente, se verificó el correcto funcionamiento de las reglas de filtrado implementadas mediante blacklist, evidenciando el bloqueo satisfactorio del acceso a los dominios restringidos previamente definidos dentro de las políticas de navegación. En las pruebas realizadas se puede observar que los usuarios autenticados no podían acceder a los sitios web incluidos en la lista negra, garantizando así el cumplimiento de las políticas de seguridad y control de contenido configuradas en el proxy.

Figura 23.
Sitio web bloqueado por blacklist.

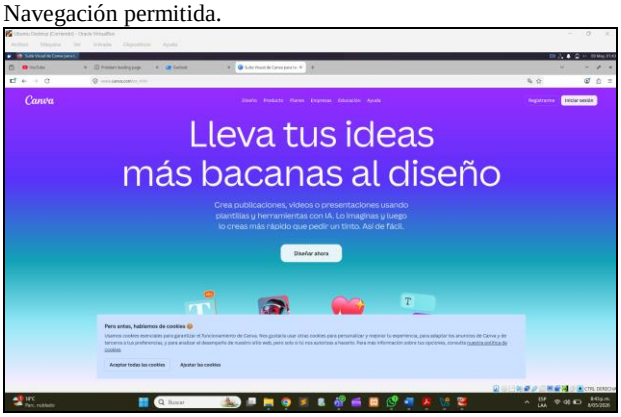


Fuente: Autoría Propia

A través de las pruebas realizadas se comprobó que los usuarios autenticados podían acceder correctamente a los sitios web autorizados dentro de las políticas configuradas en el proxy HTTP, comportamiento que permitió ver el correcto funcionamiento de las reglas de acceso implementadas, al habilitar la navegación controlada hacia recursos web desde la red LAN.

Todos los gráficos, fotografías y tablas se deben centrar. Todo debe de incluirse en el artículo. Recuerde que la calidad de los gráficos, fotografías y tablas debe ser mejor que los originales de origen.

Figura 24.
Navegación permitida.



Fuente: Autoría Propia

Adicionalmente, la implementación demuestra la importancia de los mecanismos de administración de tráfico web en entornos empresariales, toda vez que facilitan el monitoreo del acceso a Internet y contribuyen a la protección de los recursos de red frente a contenido no autorizado.

6 CONCLUSIONES

Las herramientas de virtualización como VirtualBox permiten simular infraestructuras de red complejas para probar soluciones funcionales en entornos reales complejos, sin incurrir en los costos asociados a la adquisición del hardware.

La seguridad perimetral basada en reglas de firewall es una herramienta para tener en cuenta por los administradores

de la red, a partir de la creación de políticas y reglas que segmenten el tráfico inter-zonas se protege a la red interna de la organización frente amenazas informáticas como ataques de denegación de servicio, accesos no autorizados a la red o tráfico malicioso proveniente de la red pública; por ello el uso de firewall debe ser un elemento central a la hora de implementar soluciones de ciberseguridad.

El desarrollo de esta actividad permite comprender el funcionamiento del firewall Endian en la gestión del tráfico de red entre diferentes zonas. Se logró establecer un acceso controlado a servicios como HTTP y FTP, al tiempo que se restringía el uso del protocolo ICMP. Además, se pudo verificar el comportamiento del firewall mediante pruebas prácticas y la revisión de logs.

La implementación del proxy HTTP no transparente permitió comprender la importancia de las políticas de seguridad y control de acceso dentro de las infraestructuras de red modernas. Mediante el uso de autenticación y filtrado web, fue posible restringir el acceso de usuarios autorizados y bloquear contenido definido por las políticas administrativas de la organización.

7 REFERENCIAS

[1] Cepeda-López, F. H. (2008). *La topología de redes como herramienta de seguimiento en el sistema de pagos de alto valor en Colombia*. Borradores de Economía, (Borradores de Economía; No. 513). https://www.researchgate.net/profile/Freddy-Cepeda/publication/4936800_La_topologia_de_redes_como_herramienta_de_Seguimiento_en_el_sistema_de_Pagos_de_Alto_Valor_en_Colombia/links/0912f50b37948320bd000000/La-topologia-de-redes-como-herramienta-de-Seguimiento-en-el-sistema-de-Pagos-de-Alto-Valor-en-Colombia.pdf

[2] Marín Valencia, J. J., Patiño Valencia, A., & Acevedo Bedoya, J. C. (2020). *Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS*. Revista Universidad Católica De Oriente, 31(45), 84–99. https://doi.org/10.47286/01211463.284

[3] Chimento, J. (2015). *Comunicaciones NAT* [Universidad Nacional de Rosario]. Repositorio institucional UNR. https://dcc.fceia.unr.edu.ar/sites/default/files/uploads/materias/nat.pdf

[4] Canonical Ltd. (s. f.). *curl*. Ubuntu Manpages. https://manpages.ubuntu.com/manpages/bionic/man1/curl.1.html

[5] Armijos Guillen, D. F. (2025). *Desarrollo de un sistema aprovisionador para reducir el tiempo de configuración de un servidor FTP, utilizando herramientas open source (Bachelor's thesis, Riobamba)*. http://dspace.unach.edu.ec/handle/51000/14793

[6] Gil, P. (2009). *Protocolo de Mensajes de Control de Internet (ICMP). Redes*. https://rua.ua.es/entities/publication/e6c16d9d-ceee-417b-8b52-77f03d5513b3

[7] Bolaños Botina, J. (2018). *Diseño de la arquitectura de seguridad perimetral de la red informática en la Industria de Licores del Valle. (trabajo de grado - maestría). Universidad Autónoma de Occidente*. Recuperado de http://hdl.handle.net/10614/10248

[8] Arismendy Sánchez, J, Suta Rincón, J y Parra Martínez, C. (2019). *Implementación de una herramienta de Firewall y Proxy para el control de las comunicaciones desde un entorno de red. Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Villavicencio*. Disponible en: https://hdl.handle.net/20.500.12494/12742

[9] Ávila, Á., Jiménez, T. E., Obando, C., & Zuleta, C. F. O. (2022). Directrices y políticas de firewall. *InGente Americana*, *2*(2), 15-28. https://publicaciones.americana.edu.co/index.php/inam/article/download/496/626

[10] Álvarez, F.H. (2024). Diseño de la investigación implementación de un sistema de protección y mitigación contra tráfico malicioso tipo web a través de filtros DNS, para prevenir la inclusión de IPs públicas en listas negras en un proveedor de servicios de internet [Trabajo de grado para optar por el título de ingeniería electrónica, Universidad de San Carlos de Guatemala]. Repositorio institucional Universidad de San Carlos de Guatemala. https://biblio.ingenieria.usac.edu.gt/protocolos/2024/TGP1656.pdf