IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD EN GNU/LINUX PARA ENTORNOS DE SERVIDOR

Andrés camilo cárdenas salcedo
e-mail: accardenassa@unadvirtual.edu.co

RESÚMEN: *Este artículo presenta la implementación y configuración de GNU/Linux Endian Firewall en VirtualBox, enfocada en la gestión segura de redes mediante zonas segmentadas: verde (LAN), roja (WAN) y naranja (DMZ). Se detalla la configuración de tarjetas de red y reglas NAT que permiten la comunicación controlada entre zonas, garantizando el acceso desde la LAN e Internet hacia la DMZ. Se habilitan servicios como HTTP y FTP, restringiendo protocolos como ICMP para reforzar la seguridad. Se definen reglas de acceso específicas que controlan el flujo de tráfico inter-zona, comprobando su funcionamiento mediante pruebas con navegador y terminal. Además, se implementa un proxy HTTP no transparente con autenticación de usuario, junto con políticas de filtrado que bloquean sitios web mediante listas negras. Esta solución simula un entorno empresarial básico, orientado a fortalecer la comprensión y aplicación de conceptos de seguridad en redes mediante software libre y herramientas de virtualización.*

PALABRAS CLAVE: Administración de redes, Proxy, Seguridad perimetral, VirtualBox.

1 INTRODUCCIÓN

En el contexto actual de la administración de sistemas operativos y la ciberseguridad, resulta imprescindible implementar mecanismos que garanticen la protección de la información y la continuidad operativa de los servicios de red. Este artículo presenta el desarrollo colaborativo de prácticas orientadas a la configuración y puesta en marcha de herramientas de seguridad utilizando la distribución GNU/Linux Endian Firewall (EFW). La actividad tuvo como propósito principal asegurar entornos LAN, DMZ y WAN, aplicando buenas prácticas de segmentación de red, reglas de acceso, servicios NAT, control de puertos y políticas de navegación.

Cada temática desarrollada abordó una funcionalidad esencial para proteger la infraestructura: desde la instalación inicial del firewall, la configuración NAT, la activación de servicios específicos en la DMZ, hasta la implementación de un proxy HTTP con autenticación. Todas las configuraciones fueron ejecutadas y validadas en un entorno virtualizado mediante VirtualBox, permitiendo simular una red empresarial con roles de servidor y cliente, fortaleciendo las competencias en administración de sistemas GNU/Linux.

2 METODOLOGIA

2.1 PREPARACIÓN DEL ENTORNO VIRTUAL

Se descargó la ISO oficial de Endian y se configuró una máquina virtual en VirtualBox. Se asignaron tres adaptadores de red para simular las zonas:

- verde (LAN).
- naranja (DMZ).
- roja (WAN).

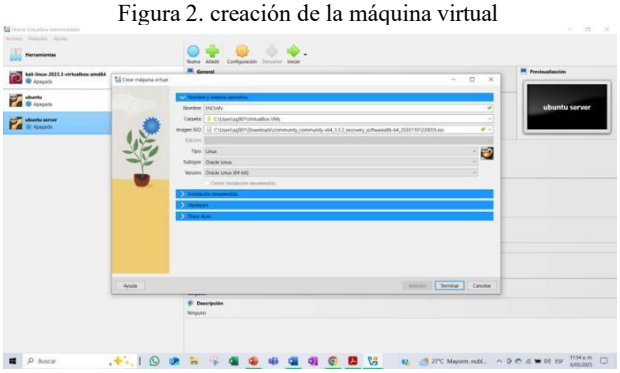
En la Figura 1, podemos observar el portal oficial de Endian, desde donde se descargó la imagen ISO utilizada para la instalación del firewall en el entorno virtualizado.

Figura 1. Sitio oficial de descarga

Fuente: Autoría Propia

En la figura 2, se muestra la creación de una nueva máquina virtual desde la Interfaz de VirtualBox, para instalar Endian Firewall, en donde se realiza la asignación de parámetros básicos como nombre, tipo de sistema operativo y memoria RAM.

Figura 2. creación de la máquina virtual

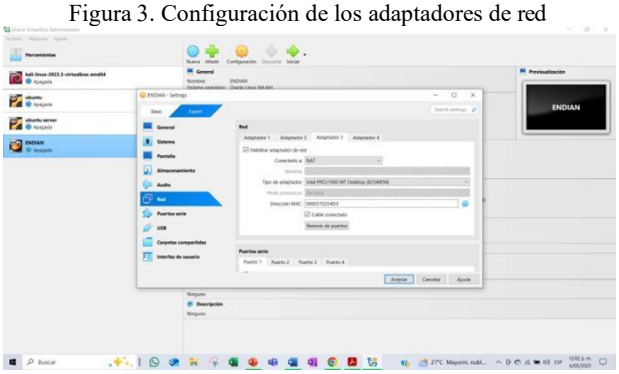


Fuente: Autoría Propia

2.2 CONFIGURACIÓN DE RED Y ACCESO INICIAL

Se configuraron las interfaces de red en VirtualBox y se accedió a la interfaz gráfica de Endian vía navegador web para la configuración inicial.

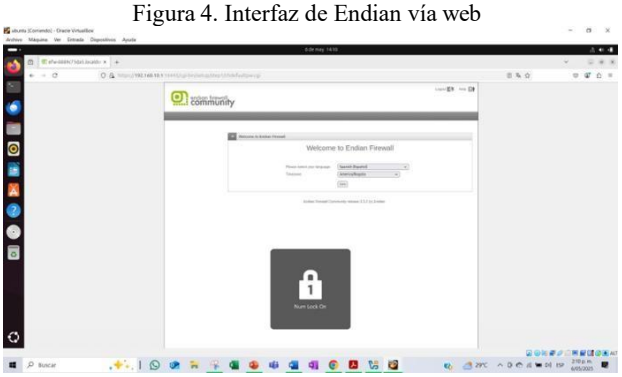
Figura 3. Configuración de los adaptadores de red



Fuente: Autoría Propia

En la figura 3, se observa el proceso de configuración de uno de los adaptadores de red en la máquina virtual, es decir, se realiza la configuracion de las tres zonas: zona verde (LAN), zona naranja (DMZ) y zona roja (WAN). Cada adaptador está asociado a un modo de red distinto para simular entornos de red reales.

Figura 4. Interfaz de Endian vía web



Fuente: Autoría Propia

En la figura 4, se observa Vista la interfaz web de administración de Endian Firewall, accesible desde un navegador mediante la dirección IP asignada a la zona verde. Desde aquí se realiza la configuración central del sistema.

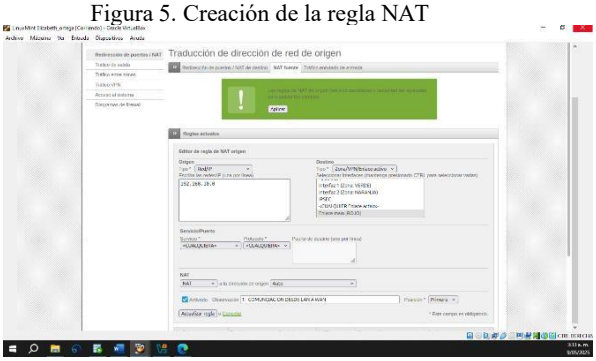
3 CONFIGURACIÓN NAT Y REGLAS DE SEGURIDAD

La configuración de la red se dividió en tres zonas: **LAN (zona verde), DMZ (zona naranja)** y **WAN (Internet)**. Para garantizar la conectividad y la seguridad, se implementaron reglas de traducción de direcciones de red (NAT) y políticas de firewall adecuadas a cada segmento.

3.1 NAT: LAN A LA WAN

Se creó una regla NAT de fuente para permitir que la red LAN acceda a Internet. Se verificó su funcionamiento con pruebas de ping antes y después de la configuración.

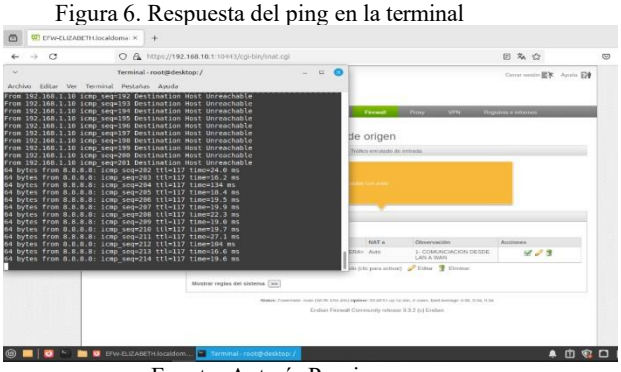
Figura 5. Creación de la regla NAT



Fuente: Autoría Propia

En la figura 5, se observa el proceso de la creacion de la regla NAT donde se accedió al panel del firewall y se configuró una regla NAT de fuente, especificando la interfaz de origen como LAN, la subred 192.168.10.2 y la traducción de origen como la IP pública de la interfaz WAN. Esto permite el acceso a Internet desde la red local.

Figura 6. Respuesta del ping en la terminal



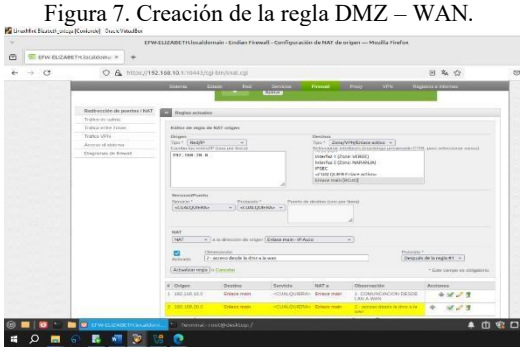
Fuente: Autoría Propia

En la figura 6, podemos observar que tyras aplicar la regla NAT, se realizaron pruebas con el comando ping desde un equipo en la LAN hacia dominios externos, confirmando el acceso exitoso a Internet.

3.2 NAT: DMZ HACIA WAN

Se configuró una regla NAT de fuente para permitir que los servidores en la DMZ accedieran a Internet. Se especificó la subred de la DMZ como origen y la IP pública de la interfaz WAN como dirección de traducción. garantizando conectividad con el exterior desde el servidor en la zona naranja.

Figura 7. Creación de la regla DMZ – WAN.



desde la DMZ donde podemos observar que la IP real de nuestros equipos está protegida y se observa es la IP pública y no la privada.

4. CONCLUSIONES.

La instalación y configuración de Endian Firewall en VirtualBox permitió establecer una red segmentada con zonas verde, naranja y roja, simulando un entorno empresarial. La interfaz gráfica facilitó la personalización de parámetros esenciales para una base de red segura.

La implementación de reglas NAT permitió habilitar el acceso a Internet desde la LAN y la DMZ, validando su efectividad mediante pruebas de conectividad y análisis de tráfico. Se comprobó el correcto enmascaramiento de las direcciones privadas mediante la IP pública asignada.

Las reglas de firewall configuradas permitieron la publicación segura de servicios HTTP y FTP desde la DMZ hacia la WAN. Se garantizó el acceso externo controlado sin comprometer la seguridad de la red interna.

5. REFERENCIAS

[1] Endian Documentation, “Firewall – In this page you find”.[En línea]. https://docs.endian.com/3.2/utm/firewall.html#in-this-page-you-find

[2] Endian Documentation, “Firewall – Inter-Zone Traffic”. [Enlínea]. https://docs.endian.com/3.2/utm/firewall.html#inter-zone-traffic

[3] Endian Documentation, “Firewall – Common Configuration Items”. [En línea]. https://docs.endian.com/3.2/utm/firewall.html#commonconfiguration-items

[4] Ubuntu, Ubuntu Server Documentation. [En línea]. https://documentation.ubuntu.com/server/

[5] J. LaCroix, Mastering Ubuntu Server: Gain Expertise in theArt ofDeploying,Configuring, Managing, and Troubleshooting Ubuntu Server, Packt Publishing, 2020. [En línea]. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952

[6] Endian Documentation, “Firewall – In this page you find”.[En línea]. https://docs.endian.com/3.2/utm/firewall.html#in-this-page-you-find

[7] Endian Documentation, “Firewall – Inter-Zone Traffic”. [En línea]. https://docs.endian.com/3.2/utm/firewall.html#inter-zone-traffic

[8] Endian Documentation, “Firewall – Common Configuration Items”. [En línea]. https://docs.endian.com/3.2/utm/firewall.html#commonconfiguration-items