IMPLEMENTACIÓN DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL CON ENDIAN FIREWALL EN ENTORNO VIRTUALIZADO UTM

Oscar Stiven Marulanda Otalvaro

RESUMEN: *Este proyecto consistió en la implementación y configuración de una solución de seguridad perimetral utilizando GNU/Linux Endian Firewall (EFW) dentro de un entorno virtualizado mediante VirtualBox.*

Se definieron y administraron tres zonas de red:

- *Zona Verde (LAN): red interna.*
- *Zona Roja (WAN): acceso a Internet.*
- *Zona Naranja (DMZ): servicios expuestos.*

Durante la configuración se aplicaron reglas de NAT, control de tráfico interzonal, y políticas de proxy HTTP con autenticación de usuarios. Las tareas se realizaron desde la consola, verificando la comunicación entre zonas y comprobando el bloqueo selectivo de servicios y sitios web según las políticas establecidas.

Los resultados evidenciaron una arquitectura segura, estable y funcional, capaz de aislar servicios críticos, gestionar eficientemente el tráfico y reforzar la protección del entorno. Esta implementación sirve como modelo replicable para proyectos de seguridad en ámbitos educativos y organizacionales.

1 INTRODUCCIÓN.

La creciente actividad de los actores maliciosos y su continua búsqueda de vulnerabilidades evidencian la exposición de los sistemas informáticos a riesgos externos e internos, lo que convierte a la seguridad perimetral en un componente crítico para la protección de infraestructuras de red. En entornos empresariales y académicos, la segmentación adecuada de la red mediante firewalls y zonas desmilitarizadas (DMZ) constituye una práctica indispensable para aislar servicios sensibles, como servidores web o bases de datos, y limitar el acceso no autorizado.

En este escenario, Endian Firewall (EFW) se posiciona como una solución de código abierto robusta para la implementación de políticas de seguridad avanzadas, tales como traducción de direcciones (NAT), filtrado de tráfico interzonal y administración de proxys con autenticación. Su uso en plataformas virtualizadas permite recrear infraestructuras reales de forma flexible y con bajos costos operativos.

2 CONFIGURACIÓN DE ENDIAN EN UTM.

2.1 Descarga del Software Endian.

Se ingresó al portal oficial de **Endian Firewall (EFW)** alojado en *SourceForge*, desde donde se descargó la imagen ISO necesaria para la instalación del sistema. Este repositorio proporciona versiones actualizadas y verificadas de la distribución, garantizando una obtención segura del software.

2.2 Configuración del Hardware Virtual en UTM.

UTM, se creó una nueva máquina virtual denominada “Endian”. Se asignaron los siguientes recursos:

- Memoria RAM: 4000 MB.
- Procesador: 4 núcleos.
- Disco duro virtual: 128 GB.

Se utilizó UTM/VirtualBox para crear una instancia de Endian con tres interfaces de red:

- Zona Green (LAN): Red interna para equipos locales.
- Zona Red (WAN): Puente hacia Internet.
- Zona Orange (DMZ): Segmento aislado para servicios públicos como web o FTP.

Cada interfaz fue configurada manualmente asegurando compatibilidad con la topología propuesta.

2.3 Instalación y Configuración Inicial de Endian.

Tras iniciar la máquina virtual, se siguió el asistente de instalación. Se seleccionó el idioma preferido y se confirmó la preparación del disco duro, aceptando la advertencia sobre la pérdida de datos. Se habilitó la conexión remota vía cable multipuerto y se asignó la dirección IPv4 192.168.2.15 con máscara 255.255.255.0 para la tarjeta de la zona verde. Al finalizar, el sistema proporcionó las direcciones de acceso a la interfaz web administrativa.

2.4 Configuración de las Zonas Roja, Verde y Naranja.

2.4.1 Dirección IP utilizada en la implementación

Para el funcionamiento del entorno se empleó el siguiente direccionamiento:

- **Zona Green (LAN):**
  - IP del Endian Firewall: **192.168.3.20**
  - Máscara: **255.255.255.0**
  - Rango de clientes: **192.168.3.21 – 192.168.3.254**
  - Gateway para los equipos LAN: **192.168.3.20**
- **Zona Red (WAN):**
  - IP asignada: **192.168.2.20** (según red externa disponible)
  - Máscara: **255.255.255.0**
  - Gateway principal: **192.168.2.20**
  - DNS: **8.8.8.8 / 1.1.1.1**
- **Zona Orange (DMZ):**
  - IP del Endian Firewall: **192.168.4.20**
  - Máscara: **255.255.255.0**
- **Zona Blue (WiFi):**
  - IP asignada: **192.168.5.20**
  - Máscara: **255.255.255.0**

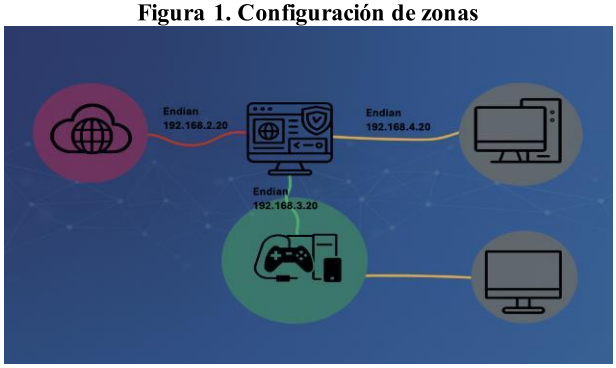
Para establecer la conexión de un servidor en la zona **Orange**, se implementó una máquina **Ubuntu Server** con su adaptador de red configurado en la interfaz interna correspondiente a dicha zona. Para asignar la configuración de red estática, se editó el archivo de Netplan ubicado en **/etc/netplan/xxxx.yaml**, aplicando los siguientes parámetros:

```
network:
  version: 2
  ethernets:
    enp0s8:
      dhcp4: no
      addresses: [192.168.4.21/24]
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Finalmente, se validó la conectividad ejecutando un **ping** hacia la dirección **192.168.2.20**, verificando así la correcta comunicación entre el servidor y el firewall ubicado en la zona Orange.

De este modo, se establecieron y verificaron las tres zonas de red propuestas: roja (WAN), verde (LAN) y naranja (DMZ).

Figura 1. Configuración de zonas



3 CONFIGURACIÓN DE REGLAS NAT PARA CONECTIVIDAD ENTRE ZONAS.

3.1 Establecimiento de Comunicación desde la LAN hacia la WAN.

La zona verde (LAN) se configuró con la subred definida por el grupo 192.168.3.0/24 la cual es administrada por el firewall Endian a través de la interfaz interna Verde. Para permitir que los desktops conectados en esta zona accedieran a la WAN (zona Roja) fue necesario implementar una regla de Source NAT (SNAT) haciendo uso de la funcionalidad de traducción automática de direcciones la cual fue provista por el firewall Endian. Esta regla asegura que el tráfico que se origina en la zona vede LAN sea enmascarado con la dirección IP de la zona roja (WAN) y así permitir la salida hacia internet de una manera controlada.

Se configuró una regla de NAT de fuente en la interfaz web de Endian Firewall, estableciendo como origen la subred 192.168.2.0/24 y como destino el enlace principal de la zona roja, utilizando la opción de enmascaramiento automático. Tras habilitar la regla, se verificó su funcionamiento mediante pruebas de navegación y conectividad desde una máquina Ubuntu Desktop. Los resultados confirmaron que el tráfico de la red LAN fue correctamente traducido y que el acceso hacia la zona WAN operó de manera adecuada.

Se logró habilitar la comunicación entre la LAN e internet, asegurando que todo el tráfico saliente fuera gestionado según las políticas del firewall, en cumplimiento con los principios de segmentación y control perimetral de la red.

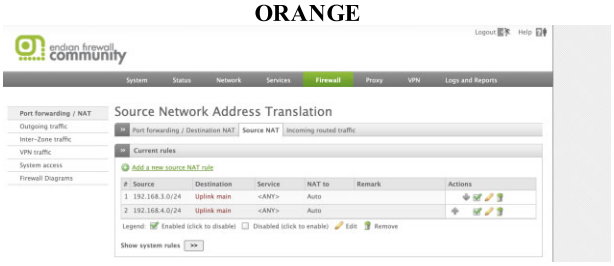
3.2 Configuración de NAT para la Zona DMZ y Verificación de Reglas de Reenvío de Puertos.

La zona naranja (DMZ) con la subnet definida 192.168.4.0/24 fue destinada para alojar servicios accesibles. En este escenario se usó un servidor Ubuntu con dirección IP estática 192.168.4.20 sobre la cual se configuró y habilitó un servicio web mediante Apache. Para otorgarle al servidor Ubuntu acceso controlado a la WAN.

En el firewall Endian, en la pestaña Firewall – NAT fuente se configuró el origen como 192.168.4.0/24 y el destino Enlace Esto permitió que el servidor Ubuntu ubicado en la DMZ alcanzara los repositorios de paquetes de actualización.

Con las configuraciones aplicadas anteriormente en Endian los servicios y red DMZ quedó correctamente integrado al esquema de seguridad del firewall Endian disponiendo una salida controlada hacia la zona roja WAN como la publicación selectiva de servicios hacia redes externas cumpliendo así con las buenas prácticas de aislamiento y exposición controlada de servidores.

Figura 2. Regla de NAT Fuente para zona LAN - ORANGE



4 CONCLUSIONES

La construcción del entorno de seguridad basado en Endian Firewall permitió validar de manera integral el funcionamiento de una arquitectura perimetral con múltiples zonas y políticas diferenciadas de acceso. La definición clara de las áreas LAN, WAN y DMZ, junto con el direccionamiento implementado, facilitó la creación de un entorno controlado en el que se comprobó el comportamiento del tráfico, el aislamiento de servicios expuestos y la correcta aplicación de reglas de traducción de direcciones.

El proceso de configuración evidenció la importancia de contar con mecanismos que centralicen el control del flujo entre redes y permitan administrar servicios de forma segura, especialmente cuando estos se ubican en segmentos críticos como la DMZ. Asimismo, la experiencia demostró la utilidad de Endian como plataforma de seguridad modular, capaz de integrarse a entornos virtualizados y responder adecuadamente a escenarios reales de gestión y filtrado de tráfico.

En conjunto, la práctica reafirmó la relevancia de las soluciones de código abierto como alternativas confiables para implementar medidas de protección perimetral. Además, fortaleció las habilidades operativas en administración de redes y servidores, resaltando el valor de la segmentación, el monitoreo y la correcta aplicación de políticas como pilares esenciales para salvaguardar infraestructuras modernas.

5 REFERENCIAS

[1] Endian. (2016). *Endian UTM 3.2 Manual de referencia*. https://docs.endian.com/3.2/utm/first.html#conventions-used-in-this-document

[2] Oracle. (2020). *Manual de usuario de VirtualBox*. https://www.virtualbox.org/manual/topics/networkingdetails.html#networkingdetails

[3] Stallings, W. (2021). Network Security Essentials: Applications and Standards (7th ed.). Pearson. https://api.pageplace.de/preview/DT0400.9781292154916_A37747529/preview-9781292154916_A37747529.pdf

[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.

[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.

[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.