Resumen

En la actualidad las PYMES se encuentran conectadas al Internet y exponen su red, información y aplicaciones a diferentes tipos de ataques, que pueden ser ejecutados a través de malware, spyware, accesos no autorizados y diversas combinaciones de amenazas externas e internas, en su mayoría no implementan sistemas de seguridad por los altos costos en licenciamiento. Una alternativa, para contrarrestar estas amenazas es la implementación de sistemas UTM Open-Source. Sin embargo, existen varias soluciones de UTMs Open-Source, y debido a la variedad y enfoque de los estudios comparativos disponibles, se dificulta determinar de manera objetiva la mejor opción que se ajuste a las necesidades de seguridad de las PYMES. El objetivo principal del presente proyecto, es el de realizar el análisis y selección de un UTM Open-Source, para fortalecer la seguridad de la información en las PYMES. A partir de la revisión sistemática de literatura de la documentación y de proyectos desarrollados sobre la implementación de los UTM Open-Source, se determinó los tres UTMs Open-Source con mejores prestaciones de seguridad. Se desarrolló una matriz comparativa, para analizar el funcionamiento de los servicios en un entorno de pruebas virtual, bajo diferentes tipos de ataques como la descarga de archivos maliciosos, escaneo de puertos y vulnerabilidades. Los resultados obtenidos determinaron que el UTM Open-Source Endian obtuvo los mejores resultados.

- Palabras Clave:
    - **UTM**
    - **FIREWALL**
    - **ANTIVIRUS**
    - **PROXY**
    - **OPEN-SOURCE**

Abstract

SMEs are currently connected to the Internet and expose their network, information, and applications to different types of attacks, such as malware, spyware, unauthorized access, and various combinations of external and internal threats, most of them do not implement security systems due to high licensing costs. An alternative to counteract these threats is the implementation of Open-Source UTM systems. However, there are several Open-Source UTM solutions, and due to the variety and focus of the available comparative studies, it is difficult to objectively determine the best option that fits the security needs of SMEs. The main objective of this project is to analyze and select an Open-Source UTM to strengthen information security in SMEs. We made a comparative matrix, based on a systematic literature review of the documentation and projects developed, on the implementation of UTMs Open-Source. From the systematic literature review of the documentation and projects developed on the implementation of Open-Source UTMs, the three Open-Source UTMs with the best security performance were determined. A comparative matrix was developed to analyze the performance of the services in a virtual test environment under different types of attacks such as malicious file downloads, port scanning, and vulnerabilities. The results obtained determined that the Open-Source Endian UTM obtained the best results.

- Keywords:

    - **UTM**
    - **FIREWALL**
    - **ANTIVIRUS**
    - **PROXY**
    - **OPEN-SOURCE**