Research and deployment of a network intrusion detection and prevention system using Suricata IDS and pfSense Firewall.

Ly Van Duy

Abstract: In the context of the increasing number of cyber attacks, this topic focuses on researching and deploying an Intrusion Detection System (IDS) based on Suricata combined with the pfSense firewall. The reason for choosing this topic is to meet the need for effective security for network infrastructure. The objective of the project is to build and evaluate the performance of this system, while providing a practical solution for organizations that need to enhance their network protection capabilities against potential threats. The research methodology includes both IDS theory and empirical analysis to verify the system's effectiveness. The expected outcome of this project is a comprehensive solution for early detection and prevention of network intrusions, while affirming the important role of Suricata technology in network security.

Keywords: Suricata IDS, pfSense Firewall, Network Security, Intrusion Analysis, Intrusion Prevention System