ABSTRACT

Distributed Denial of Service (DDoS) SYN Flood attacks pose a serious threat to networks based on Software-Defined Networking (SDN). This study analyzes the impact of such attacks using hping3 on network performance within a Supply Chain Management Network (SCMN) approach. The experimental topology includes an SDN controller, Open vSwitch, web server, PFSense router, and two additional networks acting as client and attacker. The security system is designed by integrating a Snort v2-based Intrusion Detection and Prevention System (IDPS), along with traffic filtering using iptables and ipset. Network performance is evaluated based on Quality of Service (QoS) parameters: throughput, packet loss, delay, and jitter. Results show that IDPS reduces throughput under attack from 1095.10 bit/s to 455.45 bit/s, and in minimal conditions from 3.33 bit/s to 1.34 bit/s. Packet loss was 0% in three scenarios, except for Non-IDPS Flooding (0.00075295%). The highest delay occurred in IDPS Minimal (381.72 ms), and the highest jitter in IDPS Flooding (1084.73 ms). These findings indicate that IDPS is effective in mitigating SYN Flood attacks despite increased latency. The system successfully maintains network stability and QoS during the attack..

Keywords: DDoS, SYN Flood, SDN, Snort v2, IDPS, iptables, ipset, Quality of Service, network security.