ABSTRACT

SDN architecture is vulnerable to DDoS attacks, particularly SYN Floods, which can paralyze network services. This study implemented and tested a firewall system with blacklisting methods on the Ryu Controller to mitigate these attacks. This defense mechanism works by monitoring the packet delivery rate, a parameter chosen after data analysis showed that attack packets have a fixed size of 54 bytes. The firewall was configured to automatically blacklist an IP address if it was detected sending more than 50 SYN packets in a one-second interval. Testing was conducted in a Mininet simulation environment comparing three scenarios. The test results showed that in the scenario without mitigation, attacks from 7 hosts caused Round-Trip Time (RTT) latency on normal traffic to spike to over 2700 ms. After the firewall system was implemented, RTT latency was successfully suppressed and remained stable at an average of 10-14 ms despite the ongoing attacks. Furthermore, the performance of the concurrent SVM detection model showed an F1-Score above 82%, indicating the system's ability to accurately distinguish between normal and malicious traffic. These results show that the firewall system with the implemented blacklisting method is able to maintain network stability and availability in the midst of a SYN Flood attack.

Keywords: SDN, SYN Flood, Attack Mitigation, Firewall, Blacklisting