ABSTRACT

SDN is a network architecture that separates control functions from data forwarding, enabling centralized traffic management through a controller. While flexible, this approach is vulnerable to DDoS attacks, including DNS Amplification. This type of attack exploits open DNS servers to send a large volume of responses to the target using IP spoofing techniques, with each packet averaging 72 bytes in size. If left unchecked, such traffic can overwhelm the controller and degrade network performance. This study implements a rate limiting mitigation technique controlled by the SDN controller, using a defined threshold of 20 DNS requests from a single IP address within a 10-second interval. When this threshold is reached, requests from the offending IP are restricted to prevent DNS responses from being generated. Testing was conducted under three scenarios: normal conditions, attack without mitigation, and attack with mitigation. Under the six-attacker scenario, the average RTT without mitigation reached 32,458 ms, which decreased to 14,860 ms with mitigation. The number of False Positives (FP) increased from 428 to 2,219, and False Negatives (FN) from 116 to 563 in the absence of mitigation. However, with mitigation in place, True Positives (TP) reached 21,781 and True Negatives (TN) reached 6,003. The model's accuracy declined from 94.70% (2 attackers) to 90.90% (6 attackers), and ranged from 90.88% to 94.55% after mitigation was applied. These results indicate that the implementation of rate limiting with a defined threshold can successfully reduce harmful traffic and help maintain SDN stability during attacks.

Keywords: SDN, DNS Amplification, Rate Limiting, Confusion Matrix