DDoS attack mitigation based on firewall in SDN environment

Abstract :

DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks are types of cyberattacks that aim to make a network or a service unavailable to its users by overwhelming it with a flood of traffic or requests. In this project, we will implement a firewall to help mitigate the effects of the attacks in software-defined networking (SDN)environment.

the proposed approach implements a layer 3 firewall module using the POX controller based on IP addresses. This module reads firewall policies based on IP addresses from a CSV file and installs flow rules in OpenFlow switches to block traffic according to these policies. The approach was implemented using Python, Mininet emulator, POX controller, and SDN control plane. The proposed approach filters traffic based on specific rules and can rate-limiting Firewalls can limit the rate of incoming traffic to prevent a flood of traffic from overwhelming a network or server.

This can help mitigate the impact of DoS and DDoS attacks. SDN- based firewalls can provide a flexible and scalable way to secure networks and can be easily integrated with other security solutions.