

Abstract

The problem raised in this study is guarantee the availability of a system to receive a DDoS HTTP Flood attack. Recently, attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) has become a major threat to the IT industry and the current computer network [1], this kind of attack aims to create network or system resources are not available to the user so they do not exist people who can access it [2]. An infrastructure on which the system is established Automated scalability is required to be able to take attacks DDoS, by creating a system that is always available, businesses can always running [3]. One platform that can be used to support the high availability of an application is a container orchestrator to be precise Kubernetes [4]. In this research, the focus is on designing cloud computing so that it can receive HTTP Flood attacks of 5,000, 10,000, 15,000, 30,000 which is done 10 times each. The results of this study show that even though there was an increase in the number of nodes/workers from 2 to 3, as well there is a significant increase in CPU and memory, the system built managed to deal with tens of thousands of attacks. So, it can be said that built systems are always available and reliable for production in working world.

Keywords: DDoS, EKS, Orchestrator.