Abstract

Voice over Internet Protocol (VoIP) is a technology for transmitting voice packets on an Internet Protocol (IP) network. VoIP service has a security risk, especially on the VoIP gateway. The most common attack is Denial of Service (DoS) attack. DoS attacks can turn off VoIP communication if it attacks the VoIP gateway performed for the signalling process, namely the Session Initiation Protocol (SIP). In this study, VoIP network is built using Amazon Web Service Elastics Compute Cloud (AWS EC2). The purpose of this study is to design VoIP network can handle DoS attack. The attacks is detected using CloudWatch an AWS feature to trigger VoIP gateway for reloading. As a result of the reloading, a softphone is needed so that the client still can communicate without re-registering when the VoIP gateway is transferred to other VoIP gateway. The result obtained, CloudWatch properly detects each incoming packet and performs a reloading on the VoIP gateway and the softphone works properly when the VoIP gateway is moved due to DoS attack. Data communication from the softphone to the other VoIP gateway can be done without re-registering for the softphone.

Keywords: VoIP, DoS, Sofphone, OpenSIPS, CloudWatch