Abstrak

Voice over Internet Protocol (VoIP) merupakan teknologi untuk mentransmisikan paket suara di jaringan *Internet Protocol (IP)*. Layanan *VoIP* memiliki risiko kemanaan terutama pada *VoIP gateway*. Serangan yang sering terjadi adalah serangan *Denial of Service (DoS)*. Serangan *DoS* bahkan dapat mematikan aliran komunikasi *VoIP* jika menyerang *VoIP gateway* yang ditujukan pada proses *signaling*, yaitu penyerangan pada protokol *Session Initiation Protocol (SIP)*. Pada penelitian ini dibangun jaringan *VoIP* menggunakan *Amazon Web Service Elastics Compute Cloud (AWS EC2).* Tujuan dari penelitian ini adalah untuk merancang jaringan *VoIP* yang dapat menangani serangan DoS. Serangan DoS pada *VoIP gateway* dideteksi dengan menggunakan *CloudWatch* yang merupakan fitur *AWS* agar memicu pemuatan ulang *VoIP gateway.* Akibat pemuatan ulang tersebut, maka diperlukan pembangunan *softphone* agar *client* dapat melakukan komunikasi tanpa *re-register* saat *VoIP gateway* sebelumnya dialihkan ke *VoIP gateway* lainnya. Hasil yang diperoleh, *CloudWatch* mendeteksi dengan baik setiap paket yang masuk dan melakukan aksi pemuatan ulang pada *VoIP gateway* dan *softphone* tetap dapat bekerja dengan baik saat *VoIP gateway* berpindah akibat serangan DoS. Komunikasi data dari *softphone* ke *VoIP gateway* yang baru dapat dilakukan tanpa perlu melakukan *re-register*.

Kata kunci : *VoIP, DoS, Softphone, OpenSIPS, CloudWatch*