1. Pendahuluan

1.1. Latar Belakang

VoIP (Voice over Internet Protocol) adalah teknologi untuk mentransmisikan paket suara di jaringan *IP (Internet Protocol).* Layanan *VoIP* memiliki mekanisme penyambungan *(signaling)* dan *data transport*. Celah keamanan layanan *VoIP* biasanya ada pada mekanisme tersebut. Salah satu risiko keamanan yang terjadi pada *VoIP gateway*, yaitu adanya serangan *Denial of Service (*DoS*)* yang merupakan serangan populer pada layanan *VoIP* [1]. Pada [2], dijelaskan bahwa serangan DoS yang dilakukan ke *server*, maka kedua *client* tidak dapat melakukan panggilan karena proses *signaling* pada *server* terpengaruh oleh serangan DoS. Sedangkan serangan DoS yang dilakukan ke *client*, maka kedua *client* masih dapat melakukan panggilan hanya saja panggilan yang dilakukan tidak lancar atau terputus-putus.

Pada penelitian ini dibangun jaringan *VoIP* pada *Amazon Web Service Elastic Cloud Compute (AWS EC2)* menggunakan *OpenSIPS* sebagai *VoIP gateway. VoIP gateway* akan bekerja sebagai *forwarder Client (softphone)* ke *server*, serta melakukan *re-routing* ke *VoIP server* lama menjadi *VoIP Server* yang tersedia (baru). Selanjutnya, jika terjadi serangan DoS ke *VoIP gateway* dan terdeteksi oleh *Cloudwatch*, maka *VoIP gateway* akan melakukan pemuatan ulang. Akibat pemuatan ulang tersebut, maka diperlukan pembangunan *Softphone* agar *Client* dapat melakukan komunikasi tanpa *re-registering* akibat *VoIP gateway* sebelumnya dialihkan ke *VoIP gateway* lainnya sebagai *trigger* penanganan serangan DoS. Pada studi ini juga dilakukan penghitungan MOS sebelum, sesaat, dan sesudah terjadinya serangan DoS.

1.2. Topik dan Batasannya

Sesuai dengan latar belakang yang dijelaskan, beberapa permasalahan yang diteliti diantaranya implementasi *cloud VoIP gateway* pada *Amazon EC2*. Mekanisme penanganan DoS pada *VoIP* gateway yang mengakibatkan perpindahan *VoIP gateway* lama ke *VoIP gateway* baru memerlukan pembangunan *softphone* agar komunikasi data yang ada tetap dapat dilakukan tanpa *re-registering.* Berdasarkan topik tersebut, terdapat beberapa batasan masalah, yaitu:

1. *Softphone* menggunakan sistem operasi *Android*.
2. *VoIP gateway* dibangun pada *Amazon Web Service Elastic Cloud Computing (AWS EC2).*
3. Protokol *signaling* yang digunakan adalah *Session Initiation Protocol (SIP).*
4. *VoIP gateway* yang dibangun sebanyak dua buah.
5. Semua *Instance VoIP gateway* harus dalam keadaan *standby*.
6. Panggilan yang sedang berlangsung akan mati sementara ketika server down, namun panggilan tetap dapat dilakukan setelah sekitar 1-2 menit tanpa perlu melakukan *re-registering*.

1.3. Tujuan

Tujuan dari penelitian ini yaitu tercapainya perancangan dan implementasi penanganan serangan *Denial of Service* pada *cloud VoIP gateway.* Penanganan dilakukan dengan menggunakan mekanisme perpindahan *instance* secara otomatis dan pembangunan *softphone* untuk c*lient* akibat perpindahan *instance* sebagai langkah penanganan.

1.4. Organisasi Tulisan

Penelitian ini ditulis menjadi beberapa bagian, bagian kedua merupakan studi literatur yang terkait dengan penelitian. Bagian ketiga menunjukkan sistem yang dibangun meliputi desain arsitektur jaringan dan spesifikasi kebutuhan sistem. Bagian keempat menunjukkan evaluasi yang berisi hasil pengujian dari beberapa skenario pengujian yang ada. Selain itu, bagian keempat juga berisi analisis hasil pengujian dari beberapa scenario. Bagian terakhir berisi kesimpulan dan saran untuk penelitian selanjutnya.