BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian, pembahasan dan interpretasi yang telah diuraikan pada bab-bab sebelumnya, dengan mengacu pada beberapa teori dan hasil penelitian sebelumnya, dapat ditarik kesimpulan sebagai berikut :

1. Teknologi *sFlow* dan *OpenFlow* terbukti, selain berfungsi untuk mempermudah konfigurasi jaringan dapat juga digunakan sebagai sistem keamanan jaringan dengan melakukan pengaturan seluruh trafik yang melalui perangkat jaringan berdasarkan pemodifikasian *flow table* pada setiap *OpenFlow switch*.
2. *sFlow* dapat digunakan sebagai alat untuk mendeteksi setiap trafik yang melalui perangkat jaringan sedangkan *OpenFlow* dapat digunakan sebagai alat untuk memitigasi serangan *ICMP flood* dengan cara memblok seluruh trafik yang berasal dari ip penyerang. Hal tersebut terbukti dari jumlah paket ICMP yang masuk ke *server* dapat berkurang secara signifikan yaitu menjadi 99 paket dibandingkan saat terjadi pengiriman *ICMP flood* yaitu 311130.2 paket.
3. Berdasarkan performa jaringan dalam hal ini *latency*, sistem keamanan yang digunakan juga dapat mengurangi nilai *latency* dari 42,822 *ms* menjadi 8.807 *ms* untuk kondisi 30 *user*. Untuk kondisi 60 *user* dan 90 *user* mengalami penurunan yang masing-masing dari 87.265 *ms* menjadi

17,557 *ms* serta 134,678 *ms* menjadi 28,724 *ms*. Sedangkan pada kondisi 120 *user* mengalami penurunan nilai *latency* dari 176,783 *ms* menjadi 36,409 *ms*. Hal tersebut menunjukkan bahwa kondisi jaringan atau trafik yang terjadi saat serangan berhasil di blok oleh sistem yang telah dibuat.

5.2 Saran

Berdasarkan kesimpulan dan analisis yang dilakukan selama melakukan penelitian perancangan sistem deteksi dan miligasi *ICMP flood* berbasis *software defined network* dan *sFlow-RT* di STMIK Amikom Yogyakarta, dapat dikemukakan saran-saran yang perlu ditindaklanjuti sebagai berikut :

1. Pengujian dilakukan menggunakan kontroler *Opendaylight*, sehingga masih bisa saja dikembangkan dengan menggunakan kontroler lain. Hasil yang berbeda bisa saja terjadi, dibandingkan dengan apa yang telah diperoleh pada penelitian ini.
2. Pada penelitian selanjutnya diharapkan untuk dapat menerapkan sistem kemanan ini terhadap beberapa jenis serangan lain seperti *UDP Attack, Smurf Attack, DNS Attack* dan lain-lain.