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. Implementasi IDS pada jaringan SDN dengan perangkat OpenWRT sebagai OpenFlow switch menjadikan jaringan lebih aman. Hal ini ditunjukkan pada hasil uji serangan yang telah dilakukan mampu untuk mendeteksi adanya serangan sesuai dengan *rule* yang ditambahkan pada IDS serta dapat mencegah serangan tersebut dengan memutus komunikasi perangkat penyerang.
2. Sistem yang dibangun dengan perangkat *Raspberry Pi 2* model B V1.1 yang dipasang sebagai server pada jaringan SDN secara keseluruhan belum mampu memenuhi layanan QOS sesuai dengan standar yang telah ditetapkan. Hal ini terlihat pada pengujian perfomansi yang menunjukkan data bahwa koneksi bandwidth yang dihasilkan tidak stabil baik sebelum dipasang IDS maupun setelah dipasang IDS. Meskipun secara umum masih bisa terkoneksi dengan baik pada jaringan SDN, namun dari segi pengukuran QOS menunjukkan performa yang buruk.
3. Berdasarkan hasil uji performansi terhadap sistem, penerapan IDS pada jaringan SDN dengan menggunakan perangkat OpenWRT dan *Raspberry Pi 2 model B v1.1* berpengaruh terhadap layanan QOS dari sistem yang

dibangun. Hal tersebut ditunjukkan dengan meningkatnya jumlah *delay* pada penambahan rule IDS sebanyak 1844 rule. Namun pengujian performansi yang menunjukkan pengaruh yang signifikan terhadap sistem adalah hasil dari pengujian besaran *bandwidth loss* dan *background traffic* yang dialirkan ke jaringan yang tidak stabil, sehingga berdampak pada layanan QOS yang diberikan.

5.2 Saran

Berdasarkan kesimpulan dan analisis yang dilakukan selama melakukan penelitian perancangan sistem analisis penerapan dan uji performa *Intrusion Detection System (IDS)* pada jaringan berbasis *Software Defined Network (SDN)*, dapat dikemukakan saran-saran yang perlu ditindaklanjuti sebagai berikut:

1. Pengujian dilakukan menggunakan kontroler *RYU dan* IDS Snort, sehingga masih bisa saja dikembangkan dengan menggunakan kontroler lain serta IDS yang berbeda. Hasil yang berbeda bisa saja terjadi, dibandingkan dengan apa yang telah diperoleh pada penelitian ini.
2. Menggunakan perangkat pendukung jaringan SDN yang berbeda selain OpenWRT dan Raspberry Pi seperti menggunakan Zodiac FX OpenFlow Switch, dll. Sehingga jaringan SDN bisa diterapkan serealistis mungkin dalam skala lab yang lebih besar atau organisasi tertentu.
3. Mengembangkan IDS menjadi *Intrusion Prevention System* (IPS) di lingkup jaringan SDN dan optimalisasinya.
4. Menerapkan penggunaan teknik *anomaly detection* dan mencegah serangan *IDS evasion* dari *hacker*, dengan IDS pada jaringan SDN.