Abstrak

Keamanan pada jaringan merupakan hal penting, semakin aman sebuah jaringan maka semakin baik jaringan tersebut. Pada jaringan dengan model SDN masih diperlukannya riset pada bagian keamanan (*security*) khususnya pada bagian hak akses dan monitoring paket. Salah satu solusi yang dapat digunakan adalah dengan menggunakan *firewall. Firewall* merupakan salah satu metode yang dapat digunakan untuk mengamankan lalu lintas data dan hak akses dalam sebuah jaringan. Dengan penerapan *firewall* pada SDN maka keamanan pada jaringan model tersebut akan lebih aman, akan dapat memonitoring paket keluar dan masuk serta hak akses pengguna akan dapat ditentukan.

Pada tugas akhir ini telah dilakukan penerapan *firewall* dengan menggunakan *controller* floodlight dengan menggunakan pendekatan *whitelisting*. Pengujian yang dilakukan adalah menguji penerapan *firewall* dengan skenario yang telah dibuat serta pengujian QoS jaringan ketika menggunakan *firewall* dan tidak menggunakan *firewall*, parameter pengujian QoS pada penelitian ini adalah *latency, packet loss, jitter* dan *throughput*.

Dari hasil pengujian yang dilakukan didapatkan hasil sebagai berikut. *Latency* layanan data sebelum *firewall* rata-rata 33,382 ms dan setelah *firewall* 34,369 ms, layanan video 56,186 ms dan 56,807 ms, layanan VoIP 41,062 ms dan 17.765ms. Jitter layanan data sebelum *firewall* 0,532 ms setelah *firewall* 0,586 ms layanan video 1,305 ms dan 1,336 ms, layanan VoIP 0,594 ms dan 0,615 ms. *Packet loss* layanan data sebelum *firewall* 4,098% setelah *firewall* 4,36%, layanan video 28,530% dan 30,768%, layanan VoIP 4,088% dan 4,698% dan *Throughput* layanan data sebelum *firewall* 36,929 Kbps setelah *firewall* 36,888 Kbps, layanan video 3649,08 Kbps dan 3645,11 Kbps, layanan VoIP 70,041 Kbps dan 69,610 Kbps.

Kata kunci: *Software Define Network* (SDN), *Firewall*, hak akses, Floodlight, *Whitelisting, QoS*.