

## ABSTRAK

Perkembangan teknologi berdampingan dengan berkembangnya jaringan komputer. Salah satunya perkembangan internet. Internet memiliki peran penting sehingga dapat mempengaruhi kehidupan manusia. Misalnya, agar informasi mudah diakses, ada beberapa faktor yang menentukan kinerja Internet, salah satunya adalah jaringan. Dalam perancangan infrastruktur jaringan yang optimal, dibutuhkan arsitektur jaringan yang *dynamic*, mudah untuk beradaptasi dan mudah dikelola dalam penyesuaian *hardware* atau *software*. Untuk memenuhi hal tersebut dibutuhkan konsep yang dikenal dengan *Software Defined Network* (SDN). SDN memungkinkan kita untuk membangun infrastruktur dan mengelola jaringan dengan membuat kontrol yang terpusat terlepas dari teknologi jaringan yang mendasarinya. Salah satu aspek yang harus diperhatikan dalam SDN itu adalah aspek keamanan. Keamanan pada SDN dikatakan komprehensif jika memenuhi 8 kriteria salah satunya *multi-tenancy*. Pada lingkungan *multi-tenant*, *tenant* dapat berbagi elemen jaringan, sehingga evolusi teknologi SDN memiliki beberapa kerentanan keamanan. Dalam penelitian ini, Peneliti menyajikan analisis keamanan *firewall* jaringan virtualisasi *multi-tenant* berbasis SDN, dengan menerapkan metode *network slicing* menggunakan FlowVisor untuk memperkuat isolasi setiap *slice* pada jaringan SDN. Simulasi jaringan *virtual* SDN menggunakan *mininet* serta POX *controller* sebagai komponen utama SDN. POX bertanggung jawab dalam melakukan tugas-tugas keputusan kontrol ketika mengeluarkan paket data. Selanjutnya Peneliti mengevaluasi kinerja jaringan simulasi SDN menggunakan tiga skario pengujian, diantaranya uji konektivitas dimana FlowVisor belum dijalankan sehingga antar *host* terkoneksi satu sama lain, uji fungsionalitas dimana pada uji ini sudah terjadi *network slicing* dengan menggunakan FlowVisor, hal ini akan menyebabkan *host* terkoneksi apabila terletak pada *tenant* yang sama. Dan terakhir uji *resource utilities*. Hasil penelitian ini diukur menggunakan parameter QoS (*throughput*, *packet loss*, *delay*, dan *jitter*) menggunakan *Transmission Control Protocol* (TCP) dan *User Data Protocol* (UDP). Nilai QoS yang dihasilkan pada setiap pengujian *throughput* TCP dan UDP digolongkan pada kategori sangat bagus kecuali pada skenario satu dengan *background traffic* 1Mbps, pada parameter *packet loss* beberapa pengujian dikategorikan sangat bagus, bagus dan sedang. Pada parameter *delay* hasil dari pengujian menunjukkan bahwa seluruh skenario berada pada kategorisasi sangat bagus. Pada parameter *jitter* memperoleh kategori bagus pada uji konektivitas dengan protokol UDP dan TCP dan sangat bagus pada uji fungsionalitas kecuali skenario satu. Pengkategorian *throughput*, *delay* dan *jitter* didasarkan pada standarisasi TIPHON, dan untuk *packet loss* didasarkan pada standarisasi ETSI 1999. Hasil pengujian *resource utilities* didapatkan performansi CPU pada jaringan SDN yang belum menerapkan FlowVisor cenderung lebih stabil dibandingkan pada jaringan SDN yang sudah menerapkan FlowVisor dan untuk performansi *memory* pada jaringan SDN yang sudah menerapkan FlowVisor cenderung lebih besar dibandingkan dengan performansi *memory* pada jaringan SDN yang belum menerapkan FlowVisor.

Kata kunci : *Software Defined Network* (SDN), *Network slicing*, FlowVisor, *Quality of Service* (QoS)