BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Semakin pesatnya perkembangan teknologi perangkat jaringan diberbagai perusahaan maka dibutuhkan teknologi jaringan komputer yang lebih fleksibel dan terpusat. *Software Defined Network* (SDN) merupakan salah satu solusi dari kebutuhan jaringan komputer saat ini. Dimana SDN menawarkan konsep jaringan yang efisen dan menjadi tersentralisasi. Dengan memisahkan *control plane* dan data *plane* dalam perangkat jaringan, menjadikan jaringan mudah diatur dan lebih fleksibel [1].

Konsep utama pada *Software Defined Network*ing adalah sentralisasi kendali jaringan dengan semua pengaturan berada pada *control plane* [2]. Namun konsep jaringan yang tersentralisasi tentunya memiliki kelemahan dari segi keamanan. *Software Defined Network* (SDN) memberikan kontrol penuh terhadap aktivitas yang ada dalam jaringan tersebut, sehingga dalam kinerja jaringan SDN semua dibebankan dan dikontrol oleh aplikasi *controller*. Dengan proses seperti itu, kecenderungan untuk mendapatkan serangan akan menjadi lebih besar [1].

Salah satu jenis serangan yang berbahaya adalah DDoS. Serangan DDoS adalah serangan yang sifatnya terdistribusi. Dimana serangan ini akan melumpuhkan jaringan bahkan dapat menghancurkan perangkat jaringan itu sendiri. Pada umumunya, serangan DDoS akan membanjiri jaringan atau *server* dengan mengirimkan paket *request* berupa TCP SYN, ICMP atau UDP dengan jumlah yang sangat banyak sehingga membuat lalu lintas pada jaringan menjadi padat [3]. Hal ini menjadikan sistem atau jaringan berkerja lebih keras dari biasanya. Selain itu apabila serangan terus menerus dilakukan tanpa henti akan menghabiskan sumber daya jaringan serta mengakibatkan kerusakan pada perangkat jaringan. Sehingga menyebabkan *controller* SDN tidak dapat lagi melayani permintaan pengguna SDN [4].

Maka dari itu dibutuhkan sistem keamanan yang berfungsi mencegah terjadinya serangan DDoS sekaligus memblokir serangan yang terdapat dalam jaringaan SDN. *Intrusion Prevention System* (IPS) merupakan suatu sistem yang memberikan keamanan pada jaringan dengan mengindetifikasi adanya aktivitas berbahaya, mencatat informasi serta mencegah dengan malakukan pemblokiran terdahap serangan [5]. Intergrasi IPS pada jaringan SDN akan memberikan keuntungan pada admininstrator dalam mengatur dan memonitoring keamanan jaringan secara terpusat.

Pada penelitian implementai IPS berbasis *athena* untuk Mencegah Serangan DDoS pada Arsitektur *Software Defined Network* (SDN) menyatakan bahwa IPS mampu mencegah dan mengenali karasteristik serangan DDoS dengan dibuktikan hasil *throughput* kembali ke keadaan normal. Saat keadaan normal, diserang dan diterapkan IPS didapatkan nilai *throughput transnmit* sebesar 3956 pps, 4045 pps, dan 3919 pps dan *receiver* sebesar 4720 pps, 4793 pps, dan 4692 pps [4]. Adapun penelitian Implementasi *Intrusion Prevention System* untuk mencegah serangan DDoS pada SDN berhasil memblokir serangan 1000 paket TCP SYN *Flood* dengan memanfaatkan *firewall* dari *Ryu*. Namun kinerja CPU meningkat saat terintegrasi IPS yaitu 21.5% untuk proses pengguna (us) dan 53.3% untuk besaran CPU yang digunakan sistem(sy) [6].

Berdasarkan penelitian sebelumnya, dibuatlah penelitian yang berjudul "Analisis Serangan *Distributed Denial Of Service* (DDoS) menggunakan *Intrusion Prevension System* (IPS) Pada Jaringan *Software Defined Network*" dengan metode dan pengambilan data yang berbeda pada penelitian sebelumnya. Pada penelitian ini penulis akan menerapkan sistem deteksi *Snort* berbasis log *alerts* pada terminal dan Telegram serta memanfaatkan *Ryu Controller* sebagai *firewall* dalam memblokir serangan. Penelitian ini juga menggunakan serangan DDoS tipe *TCP Syin Flood* dan UDP *Flood*. Data yang akan diambil pada penelitian ini berupa parameter nilai QoS *throughput* dan penggunaan CPU serta memori. Pengambilan nilai parameter tersebut bertujuan mengetahui kinerja jaringan SDN dalam kondisi normal, saat serangan maupun terintegrasi IPS

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1) Bagaimana merancang sistem keamanan *Intrusion Prevension System* (IPS) pada jaringan SDN dengan dalam mencegah serangan DDoS?
2) Berapa nilai QoS *throughput*, CPU *Usage* dan *Memory Usage* sebelum serangan, saat serangan DDoS tanpa *Intrusion Prevention System* dan saat dilakukan blokir serangan menggunakan *Intrusion Prevention System*?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Arsitektur jaringan *Sofware Defined Ne*work dan sistem keamanan *Intrusion Prevention System* hanya berupa simulasi pada OS Ubuntu
2) Sistem operasi menggunakan Linux Ubuntu 22.04.
3) Menggunakan Protokol *OpenFlow* sebagai penghubung *Switch* dengan *Controller*.
4) Rancangan jaringan SDN menggunakan *Controller Ryu*.
5) Sistem Keamanan jaringan IPS menggunakan *Snort* sebagai deteksi serangan dan *rest_firewall Ryu* sebagai mitigasi serangan.
6) Parameter yang akan di uji pada penelitian yaitu QoS *throughput* berupa nilai transfer dan bandwidth, CPU *usage* dan *Memory usage* dengan pengujian dilakukan pada kondisi jaringan normal tanpa serangan, saat serangan DDoS tanpa integrasi IPS dan setelah serangan DDoS diblokir oleh sistem IPS.
7) Penangkapan trafik data *Troughput* menggunakan *iperf3* sedangkan data CPU *usage* dan *Memory Usage* menggunakan aplikasi *top*.
8) Tipe serangan yang digunakan adalah UDP *flood* dan *TCP SYN Flood* yang dijalankan dengan variasi paket 10/detik, 100/detik, 1000/detik dan 10000/detik menggunakan metode *Hping3* pada host 3 yang akan bertindak sebagai *Attacker*

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Merancang sistem keamanan IPS menggunakan *Snort* untuk deteksi serangan dan *rest_firewal* pada *Controller Ryu* sebagai *firewall* dalam mencegah serangan DDoS pada jaringan SDN
2) Menganalisa nilai parameter QoS *throughput*, CPU *Usage* dan *Memory Usage* yang diperoleh saat sebelum serangan, saat serangan DDoS tanpa *Intrusion Prevention System* dan saat dilakukan blokir serangan menggunakan *Intrusion Prevention System*.

1.5 MANFAAT

Penelitian ini diharapkan dapat mengetahui bagaimana melakukan perancangan sistem keamanan *Intrusion Prevention System* pada jaringan *Software Defined Network* dalam mencegah serangan DDoS. Serta dapat mengetahui kinerja jaringan SDN dari nilai *throughput*, CPU *Usage* dan Memori *Usage* saat sebelum serangan, saat serangan dan saat integrasi IPS. Selain itu diharapkan dengan adanya penelitian ini dapat menjadikan perbandingan dalam menerapkan sistem keamanan pada jaringan SDN.

1.6 SISTEMATIKA PENULISAN

Penelitian ini tersusun menjadi beberapa bab yang mana masing-masing bab akan memiliki pembahasan yang berbeda - beda. Bab satu berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan. Bab dua berisi penjelasan mengenai kajian pustaka yang dijadikan rujukan dalam skripsi ini dan dasar teori mengenai jaringan *Software Defined Network*, DDoS, *Intrsuion Prevention System* dan teori pendukung yang akan digunakan dalam skripsi ini. Pada Bab tiga berisi tentang metode penelitian yang membahas mengenai alat data bahan yang digunakan, alur penelitan, topologi yang akan di rancang, perancangan jaringan SDN dan IPS serta alur serangan yang akan dilakukan. Pada Bab 4 membahas

mengenai hasil data yang diperoleh saat simulasi dan menganlisa dari hasi yang telah diperoleh. Pada Bab 5 membahas mengenai kesimpulan dan saran untuk penelitian selanjutnya.