BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi di era digital semakin berkembang pada setiap waktunya berbanding lurus dengan peningkatan perkembangan jaringan internet [1]. SDN merupakan suatu teknologi yang memisahkan antara *Control plane* dan Data *plane* atau forwarding *plane*. Pada jaringan tradisional kedua fungsi tersebut masih berada pada perangkat yang sama. *Control plane* sendiri berfungsi mengatur perangkat jaringan dan data *plane* berfungsi mengirimkan paket paket informasi [2]. Jaringan SDN bersifat dinamik dan *manageable* yang berarti memungkinkan jaringan komputer dapat di konfigurasi dengan konfigurasi atau perintah yang sama meskipun menggunakan vendor atau perangkat yang berbeda [3].

Pemisahan fungsi *data plane* dari *Control plane* pada SDN memudahkan konfigurasi perangkat secara terpusat. Jika pada jaringan tradisional perangkat dikonfigurasi satu persatu sehingga ada resiko human error sehingga kurang efektif pada jaringan skala besar sedangkan *Controller* SDN (*Control plane*) dapat melakukan konfigurasi lebih dari dua perangkat data *plane* secara langsung seperti switch sehingga jika terdapat perubahan data,struktur dan lalu lintas jaringan pada perangkat switch pusat tidak perlu mengkonfigurasi perangkat switch lainnya. *Control plane* dan data *plane* pada jaringan SDN dihubungkan dengan protokol openflow agar dapat saling terhubung. Jaringan SDN merupakan inovasi baru yang dapat meningkatkan kualitas jaringan komputer atau internet sehingga dapat membentuk lingkungan jaringan yang inovatif [4]. Namun kekurangan dari jaringan SDN terletak pada *avaibillity*.

Kekurangan tingkat keamanan jaringan SDN terletak pada *avaibillity* yang diatur oleh *Controller* . *Controller* merupakan kendali utama untuk jaringan dan bersifat tersentralisasi. Kelebihan tersensentralisasi adalah berkurangnya celah area untuk diserang tetapi jika bagian ini berhasil diserang maka seluruh jaringan dapat diambil alih.. Jika sumber daya SDN diserang dengan teknik *Denial Of Service* SYN *Flooding* akan menghabiskan sumber daya. [5]. Karena pengiriman paket data SYN yang termasuk dalam jenis paket TCP dengan jumlah besar ke *controller* SDN

sehingga menyebabkan *controller* tidak dapat melayani permintaan pengguna [6]. Diperlukan peningkatan kualitas keamanan perlu dilakukan untuk mencegah terjadinya kemungkinan serangan yang akan datang.

Salah satu upaya mengatasi hal itu sistem keamanan *Intrusion Prevention System* (IPS) digunakan. IPS adalah metode keamanan yang dapat mencegah serangan DoS dengan menggunakan aplikasi snort untuk memblokir paket data SYN yang dikirimkan penyerang secara *real time*. IPS berfungsi mengidentifikasi aktivitas lalu lintas jaringan yang mencurigakan, mencatat informasi tersebut dan akan memblokir ativitas yang dianggap mencurigakan [7]. Berdasarkan uraian di atas, maka penulis memilih penelitian tentang " IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* PADA *SOFTWARE DEFINED NETWORK* MENGGUNAKAN RYU *CONTROLLER*" sebagai judul tugas akhir, dengan harapan dapat meningkatan tingkat keamanan pada jaringan SDN dan nantinya dapat dikembangkan dan diimplementasi oleh perancang jaringan di indonesia.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah :

1. Bagaimana cara meningkatkan kualitas sistem keamanan pada jaringan SDN?
2. Bagaimana cara sistem keamanan IPS mengidentifikasi dan mencegah serangan denial of service?
3. Seberapa efektif sistem keamanan IPS mencegah serangan *Denial Of Service?*

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah

1. Perancangan dan simulasi jaringan SDN menggunakan Mininet
2. Percobaan serangan *Denial Of Service* untuk menguji sistem keamanan jaringan SDN menggunakan aplikasi Hping3.
3. Menggunakan sistem keamanan IPS dengan aplikasi Snort sebagai sistem keamanannya.
4. Menggunakan Aplikasi Ryu versi 4.3.4 sebagai *Controller* SDN untuk mengatur dan memonitoring jaringan SDN.

5. Parameter QoS yang diuji berupa *Throughput,Latency,* CPU *Load* dan penggunaan memori.

1.4 TUJUAN

Berikut merupakan tujuan dari pembuatan tugas akhir sebagai berikut **:**

1. Mengetahui efektivitas penerapan sistem keamanan IPS dalam mengidentifikasi dan mencegah terjadinya serangan DoS
2. Mengetahui kualitas QoS berupa *Throughput, Latency,* CPU *Load* dan penggunaan memori pada jaringan SDN sebelum dan sesudah penerapan keamanan IPS untuk mengetahui efektifitasnya.

1.5 MANFAAT

Penelitian ini diharapkan mampu memperkenalkan jaringan SDN dan meningkatkan keamanan jaringannya menggunakan IPS dan Ryu *Controller* untuk memudahkan untuk mengidentifikasi dan mencegah serangan pada jaringan sehingga lalu lintas jaringan tetap berjalan dengan baik.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian ini terbagi menjadi beberapa bab berdasarkan pengelompokan pokok-pokok pikiran yang tercantum dengan bab-bab sebagai berikut :

BABI PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan mssalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini berisi tentang kajian pustaka yang dijadikan rujukkan dalam tugas akhir ini dan berisi tentnag landasan-landasn teori pendukung yang digunakan pada tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentnag metode peneltian yang menjelaskan bagaimana perancangan sistem, pengujian sistem, alat yang digunakan, dan alur penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang pembahasan dan analisa berdasarkan hasil penelitian yang telah didapatkan melalui sistem yang telah dibuat.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan berdasarkan analisis yang telah dijelaskan pada bab sebelumnya dan saran yang ditunjukan untuk penelitian selanjutnya.