BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Pertumbuhan penggunaan teknologi informasi dan komunikasi bertambah pesat seiring dengan bertambahnya kebutuhan layanan data. Kebutuhan dari pengguna itu sendiri menyebabkan kenaikan trafik dan menambah kompleksitas jaringan. Namun, Infrastruktur jaringan saat ini masih dianggap belum mampu menangani kebutuhan tersebut sehingga muncul konsep jaringan baru yang disebut *Software Defined Network* (SDN). SDN merupakan sebuah paradigma baru dalam sebuah jaringan, berbeda dengan jaringan konvensional yang fungsi *forwarding* dan fungsi kontrol pada satu perangkat, konsep jaringan SDN yaitu memisahkan antara fungsi *forwarding* dan fungsi kontrol sehingga dapat dilakukan diperangkat yang berbeda[1].

Keamanan jaringan SDN, ada ancaman yang terjadi antara lapisan aplikasi dan jaringan yang terletak dibawahnya atau antara *control plane* dan *data plane*[2]. ada beberapa metode penyelesaianya yaitu menggunakan metode yang ditawarkan oleh *Intrusion Detection System* (IDS) dan *Intrusion Preventation System* (IPS). Pada implementasinya IDS hanya dapat memberikan deteksi jika terjadi ancaman namun tanpa melakukan *blocking* dan dalam hal ini membuat IDS rentan dari segi keamanan.

Implementasi IPS dapat dikatakan keamanan lebih unggul daripada IDS dengan melakukan tindakan pencegahan berupa blocking paket yang dianggap oleh sistem berbahaya. Namun IPS memiliki kekurangan yaitu dalam mengatasi *false positive* yang seringkali memproses data sebenarnya tidak perlu diblokir sehingga menambah waktu blokir yang mengakibatkan penurunan *bandwidth* dan *latency* yang tinggi, dan IPS memiliki durasi blokir yang lama untuk memproses suatu paet karena meakukan proses *detection* dan *prevention* paket yang berjalan di jaringan[3].

Permasalahan terjadi pada IDS dan IPS, masih dapat diselesaikan salah satunya dengan menggunakan metode *Deep Packet Inspection* (DPI). DPI dapat dikatakan lebih aman daripada IDS dan IPS karena mampu melakukan analyzing, monitoring serta traffic *controlling* dimulai dari layer 6 (*Presentation*) sampai ke layer 1 (*physical*)[4]. Penelitian tugas akhir ini penulis melakukan implementasi keamanan jaringan dengan metode DPI yang sudah terintegrasi pada arsitektur jaringan SDN untuk mencegah serangan DoS (*Denial of service*) dengan tipe SYN *Flooding*.

1.2 RUMUSAN MASALAH

Rumusan masalah dalam penelitian tugas akhir ini adalah :

1. Bagaimana jaringan pada SDN terintegrasi menggunakan metode *Deep Packet Inspection* ?
2. Pengaruh serangan DoS terhadap hasil dari nilai *latency* dan nilai *throughput* ?
3. Bagaimana sistem deteksi serangan dari kinerja *tools* ntopng dengan menggunakan metode DPI ?

1.3 TUJUAN

Adapun untuk tujuan dari penelitian Tugas Akhir ini yaitu sebagai berikut:

1. Dapat mengimplementasikan sistem keamanan jaringan SDN dengan menggunakan Metode *Deep Packet inspection*
2. Dapat mendeteksi dan melakukan *blocking* paket yang terindikasi berbahaya.

1.4 MANFAAT

Pada penelitian ini diharapkan mampu memaparkan implementasi arsitektur jaringan SDN dengan menggunakan metode *Deep Packet Inspection* (DPI) dimana metode ini dianggap mampu menyelesaikan masalah yang terjadi di IPS dan IDS yang tidak dapat diselesaikan. DPI mampu mengatasi *false positive* dengan mengklasifikasi level keamanan jaringan.

1.5 BATASAN MASALAH

Batasan masalah dalam penelitian Tugas Akhir ini yaitu :

1. Penggunaan arsitektur jaringan *Software defined network* (SDN).
2. Penggunaan emulator *Mininet* versi 2.2.2 yang digunakan untuk proses pengujian.
3. Teknik serangan yang dipakai yaitu *Denial of service* (DoS) *attack* tipe SYN *Flood*
4. Penggunaan *Controller* POX dengan versi 0.5.0 yang digunakan sebagai kontroller untuk menjalankan arsitektur jaringan SDN sekaligus untuk memblokir serangan DoS
5. Penggunaaan *Python* versi 2 sebagai bahasa pemrograman untuk menjalankan *controller* POX
6. Penggunaaan *tools* Ntopng sebagai *tools* deteksi dan monitoring dengan metode *Deep Packet Inspection.*

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian Tugas Akhir ini terbagi menjadi beberapa BAB. Adapun sistematika penulisannya yaitu :

BAB I PENDAHULUAN

Bab pendahuluan ini berisi tentang penjelasan latar belakang pada penelitian tugas akhir, rumusan masalah, batasan masalah, tujuan, manfaat dan kemudian berisi sistematika penulisan.

BAB II DASAR TEORI

Bab Dasar Teori ini membahas tentang teori-teori dan kajian pustaka dalam tugas akhir ini yang didapatkan dari berbagai sumber referensi terpercaya baik dari internet, paper dan lain-lain.

BAB III METODOLOGI PENELITIAN

Bab Metodologi Penelitian ini membahas tentang implementasi dari sistem, perangkat yang digunakan, dan alur penelitian yang akan dilakukan

BAB IV HASIL DAN PEMBAHASAN

Bab Hasil dan Pembahasan ini berisi tentang pengujuan-pengujian yang dilakukan terhadap sistem yang telah dibuat

BAB IV PENUTUP

Bab Penutup ini berisi tentang kesimpulan yang dilakukan selama penelitian tugas akhir berlangsung. Dan juga saran yang ditujukan untuk penelitian selanjutnya mengenai penelitian tugas akhir yang serupa.