BAB I

PENDAHULUAN

1.1 Latar Belakang

Traffic Engineering (TE) merupakan mekanisme penting yang digunakan untuk mengoptimalkan kinerja lalu lintas data pada jaringan yaitu dengan menganalisis, memprediksi, dan mengatur perilaku data yang ditransmisikan secara dinamis [1]. Telah banyak diterapkan di beberapa jaringan data konvensional, seperti penerapan *jaringan ATM* dan *MPLS*. Namun, paradigma jaringan konvensional dan solusi TE tersebut tidak cukup menguntungkan bagi paradigma dan manajemen jaringan pada generasi berikutnya karena dua alasan utama. Pertama, aplikasi internet sekarang ini memerlukan arsitektur jaringan yang mampu untuk bereaksi secara real time dan dapat diukur skalabilitasnya untuk lalu lintas data berskala besar. Arsitektur harus dapat mengklasifikasikan berbagai jenis lalu lintas data dari berbagai jenis aplikasi yang berbeda, serta menyediakan layanan yang sesuai dan spesifik untuk setiap jenis lalu lintas data dalam jangka waktu yang sangat singkat (misal dalam *milisecond*). Kedua, menghadapi pesatnya pertumbuhan *Cloud Computing* dan semakin besarnya permintaan kebutuhan *data center*, manajemen jaringan yang sesuai harus dapat meningkatkan pemanfaatan sumber daya untuk kinerja sistem yang lebih baik. Dengan demikian, arsitektur jaringan baru dan alat TE yang lebih cerdas dan efisien sangat dibutuhkan. Paradigma Software Defined Networking (SDN) yang muncul baru-baru ini memisahkan antara *Control plane* jaringan dari *Data*

forwarding plane, hal ini akan sangat memudahkan administrator dalam mengelola dan mengkonfigurasi jaringan secara terpusat sehingga jenis perangkat dari vendor yang berbeda dalam satu jaringan SDN dapat dikonfigurasikan dan dikelola dengan cara yang sama melalui sebuah controller **[2]**.

Perkembangan internet yang semakin pesat juga memicu perkembangan bidang keamanan jaringan sehingga keamanan jaringan menjadi faktor yang sangat vital saat ini. Namun, pada dasarnya jaringan SDN belum memiliki mekanisme khusus untuk mendeteksi serangan *cyber* sehingga diperlukan suatu mekanisme tertentu untuk bisa mendeteksi adanya serangan sedini mungkin. Salah satu cara untuk mendeteksi adanya serangan *cyber* pada suatu jaringan adalah dengan menggunakan teknik *Intrusion Detection System* (IDS). IDS merupakan suatu sistem yang mampu untuk memonitor paket-paket data yang melewati suatu perangkat jaringan dan melakukan analisa terhadap paket tersebut untuk mendeteksi adanya upaya serangan tertentu **[3]**. Sistem yang dibangun diharapkan dapat mendeteksi adanya usaha serangan *cyber* terhadap server *Raspberry* serta dapat melakukan tindakan pencegahan berupa pemblokiran terhadap pelaku serangan. Pemblokiran dilakukan dengan memanfaatkan kemampuan kontroler SDN dalam mengelola jaringan melalui modifikasi *flow entry* yang terdapat di kontroler tersebut. Setelah melakukan pemasangan IDS pada jaringan berbasis SDN, selanjutnya akan dilakukan pengujian performa jaringan SDN tersebut saat sebelum dan sesudah dipasang IDS serta melakukan pengujian deteksi serangan dari sistem yang telah dibuat dalam menghadapi beberapa jenis serangan *cyber* sehingga dapat diketahui efektifitas kinerja IDS

dalam mendeteksi serangan terhadap server *Raspberry*.

Pada penelitian ini, akan dibangun sebuah jaringan sederhana berbasis SDN pada perangkat OpenWRT dan kemudian jaringan tersebut akan diimplementasikan dengan *Intrusion Detection System*. Perangkat *Switch* yang digunakan pada jaringan merupakan *switch* yang mendukung protokol *Openflow*. Salah satu perangkat *Software-Based* yang dapat digunakan adalah dengan menggunakan OpenWRT yang memanfaatkan agen *OpenvSwitch* dalam perangkat tersebut yang mana pada hasil penelitian (Kartadie & Suryanto, 2015) menunjukkan performa OpenWRT mampu menggantikan *Dedicated Openflow Switch* dalam penerapan SDN **[4]**. *Controller* yang akan digunakan adalah *Ryu controller* karena update terbaru menunjukkan kontroler ini mendukung protokol *Openflow* v1.0, v1.2, v1.3, v1.4, v1.5 dan *Nicira Extension* **[5]**. Kemudian *Intrusion Detection System* akan dipasang pada jaringan tersebut untuk memonitor paket data yang melalui jaringan sehingga diharapkan sistem dapat mendeteksi adanya upaya serangan terhadap server di jaringan berbasis SDN.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah :

1. Bagaimana menerapkan *Intrusion Detection System* pada jaringan *Software Defined Network* di perangkat OpenWRT untuk mengatasi berbagai jenis serangan *cyber*?
2. Bagaimana pengaruh dari penerapan IDS pada jaringan SDN dilihat dari sisi performa dan keamanannya?

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Jaringan yang akan dibangun, menggunakan perangkat OpenWRT sebagai *Switch OpenFlow* dengan satu buah perangkat mini komputer *Raspberry Pi 2* sebagai *server* dan satu buah laptop sebagai Host serta *Controller SDN*.
2. *SDN Controller* yang akan digunakan adalah *RYU Controller*.
3. *Intrusion Detection System* yang akan digunakan adalah *Snort*.
4. Perangkat *software-base switch OpenFlow* yang digunakan adalah TP-LINK TL-MR3420 Ver. 1.2 dengan jumlah 1 buah.
5. Tidak dilakukan pembagian jalur koneksi dengan VLAN pada interface LAN perangkat OpenWRT nya.
6. Jalur koneksi yang digunakan untuk menghubungkan antar perangkat menkombinasikan antara koneksi kabel dan wireless.
7. Parameter uji performansi yang akan diukur adalah *Throughput*, *Delay*, *Jitter*, dan *Packet Loss Ratio*.
8. Penelitian ini tidak membahas mengenai perbandingan antar *SDN Controller*.
9. Server menyediakan layanan *http, ftp dan ssh*.
10. Percobaan penyerangan pada sistem tidak menggunakan teknik *IDS Evasion*.

11. Percobaan-percobaan serangan yang akan dilakukan adalah *SQL Injection*, *Cross Site Scripting(XSS Attack)*, *NMAP Host Discovery*, dan *DOS Syn Flood*.
12. Pengalamatan IP yang digunakan adalah IPv4
13. Aplikasi web yang digunakan sebagai percobaan serangan adalah *Damn Vulnerable Web Application* (DVWA) yang dikonfigurasi pada tingkat keamanan rendah.
14. Jaringan yang akan dibangun masih dalam satu subnet yang sama dan tidak terhubung dengan jaringan internet maupun intranet.
15. Metode pengembangan sistem menggunakan metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*). Penelitian ini hanya sampai membahas pada tahap *Operate*, tahap *Optimize* tidak dibahas.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Adapun maksud dari penelitian ini antara lain :

1. Sebagai prasyarat untuk kelulusan program studi Strata 1 Universitas Amikom Yogyakarta.

1.4.2 Tujuan

Adapun tujuan dari penelitian ini antara lain :

1. Mengimplementasikan *Intrusion Detection System* pada jaringan SDN berbasis OpenWRT agar dapat mengatasi serangan *cyber*.

2. Melakukan analisis pengaruh dari penerapan *Intrusion Detection System* pada jaringan SDN berbasis OpenWRT dari sisi performa dan keamanannya.

1.5 Metode Penelitian

Langkah-langkah dalam melakukan penelitian yang berjudul "Analisis Penerapan dan Uji Performa *Intrusion Detection System* (IDS) pada Jaringan Berbasis *Software Defined Network* (SDN)" ini dilakukan dengan metodologi sebagai berikut :

1.5.1 Studi Kepustakaan

Studi pustaka dilakukan untuk mempelajari dan mendapatkan pengetahuan dari buku, jurnal, internet atau literatur yang berhubungan dengan *Software Defined Network* dan pendeteksian serangan *cyber* dengan *Intrusion Detection System* sebagai dasar teori dalam perancangan sistem.

1.5.2 Metode Studi Sejenis

Metode pengumpulan data dengan mempelajari penelitian-penelitian sebelumnya yang memiliki karakteristik sama, baik dari segi teknologi maupun objek penelitian.

1.5.3 Metode Pengembangan Sistem

Metode pengembangan sistem menggunakan metode *PPDIOO life cycle* yang terdiri dari *Prepare, Plan, Design, Implement, Operate, Optimize.* Adapun rincian dari masing-masing proses tersebut antara lain :

1. *Prepare*

   Tahap yang pertama adalah *prepare* atau persiapan. Dimulai dari analisis alur dari penelitian yang akan dilakukan kemudian melakukan persiapan mengenai gambaran umum dari sistem yang akan dibangun.

2. *Plan*

   Pada tahap ini mengidentifikasi kebutuhan dari sistem yang akan dibangun seperti kebutuhan perangkat keras dan kebutuhan perangkat lunak.

3. *Design*

   Dalam tahapan ini membahas tentang detil logis perancangan arsitektur topologi yang sesuai dengan mekanisme sistem. Pada tahap ini akan dibuat perancangan menggunakan *flowchart* untuk menggambarkan mekanisme kerja serta topologi jaringan sistem deteksi serangan *cyber* dengan IDS berbasis *software defined network* pada perangkat *software-based OpenFlow* OpenWRT yang akan dibuat berdasarkan analisis.

4. *Implementation*

   Tahap selanjutnya adalah tahap implementasi, pada tahap ini menerapkan semua yang telah direncanakan. Dalam tahap ini mencakup instalasi serta konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat yang telah ditentukan.

5. *Operate*

   Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibangun serta pembahasan terhadap hasil pengujian yang telah dilakukan.

1.5.4 Penarikan Kesimpulan

Pada tahap ini dilakukan penarikan kesimpulan berdasarkan analisis pada data hasil pengujian.

1.5.5 Pembuatan Laporan

Pada tahap ini dilakukan penyusunan laporan yang memuat seluruh proses pengerjaan Tugas Akhir yang disesuaikan dengan ketentuan yang telah ditetapkan.

1.6 Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan disajikan dalam bentuk bab, antara lain sebagai berikut :

BAB I. PENDAHULUAN

Bab ini akan membahas latar belakang, perumusan masalah, maksud dan tujuan penelitian, batasan-batasan masalah dalam penelitian, metode penyelesaian masalah serta sistematika penulisan.

BAB II. LANDASAN TEORI

Pada bab ini akan membahas dan menjelaskan mengenai dasar teoritis yang menjadi landasan dan mendukung pelaksanaan penulisan laporan penelitian.

BAB III. ANALISIS DAN PERANCANGAN

Pada bab ini dibahas mengenai analisis rancangan sistem yang akan dibangun serta skenario pengujian yang akan dilakukan pada sistem.

BAB IV. HASIL DAN PEMBAHASAN

Bab ini membahas tentang proses implementasi mulai dari instalasi dan konfigurasi serta pengujian terhadap sistem yang telah dibangun. Pengujian dilakukan berdasarkan skenario-skenario yang telah dibahas pada bab 3.

BAB V. PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilaksanakan dan saran-saran dari masalah yang terkait untuk mengembangkan sistem yang lebih baik lagi terhadap penelitian selanjutnya.