

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Jaringan tradisional adalah perangkat jaringan yang memiliki *control plane* dan *data plane* didalam perangkat yang sama. Sedangkan *Software Defined Networks* merupakan arsitektur yang memisahkan antara control plane dan data plane, serta kemudian melakukan abstraksi sistem dan meng-isolasi kompleksitas yang ada pada komponen atau sub-sistem dengan mendefinisikan antar-muka (*interfaces*) yang standard. Dengan menerapkan arsitektur SDN bertujuan untuk membuat jaringan menjadi lebih fleksibel dan mempermudah dalam mengontrol jaringan apabila terdapat perubahan dalam *business requirement*. Pada *Software Defined Network*, network administrator atau network engineer dapat membentuk lalu lintas jaringan melalui sebuah central console, sehingga tidak perlu mengkonfigurasi masing-masing switch atau perangkat yang terdapat pada topologi.

Dalam konsep SDN, di perkenalkan dengan adanya *open interface* yang memungkinkan sebuah entitas software atau aplikasi dapat mengelola konektivitas yang disediakan oleh sejumlah sumber-daya jaringan, mengendalikan aliran traffic yang melewatinya serta melakukan inspeksi terhadap atau memodifikasi traffic tersebut. Sedangkan OpenFlow merupakan salah satu komponen dari arsitektur SDN. OpenFlow merupakan pionir standard terbuka yang di definisikan oleh *Open Networking Foundation* (ONF) untuk protocol komunikasi antara *control* dan *forwarding* atau *data plane*. OpenFlow memungkinkan pengaturan *routing* dan pengiriman paket melalui sebuah switch. Dalam sebuah jaringan tradisional, setiap switch hanya meneruskan paket data yang diterima kemudian dikirimkan ke tujuan tanpa mampu membedakan tipe protocol data yang dikirimkan. Dengan menggunakan *OpenFlow* memungkinkan untuk dapat mengakses dan memanipulasi *forwarding plane* secara langsung dari perangkat-perangkat jaringan seperti switch dan router baik secara fisik maupun virtual.

sFlow merupakan salah satu protocol yang digunakan untuk monitoring perangkat dalam jaringan. sFlow memiliki kemampuan untuk dapat melihat penggunaan jaringan, kinerja dan beserta informasi-informasi lain mengenai kondisi jaringan yang sedang di monitoring. Selain itu, sFlow memiliki dukungan multivendor lebih banyak dibanding protokol monitoring lain seperti NetFlow, RMON dan RMON II.

Dengan menggabungkan sFlow dan OpenFlow memberikan kemampuan yang lebih baik dalam SDN. OpenFlow memungkinkan sebuah aplikasi *Controller* untuk dapat melakukan konfigurasi terhadap *forwarding tables* didalam sebuah jaringan yang ada pada perangkat switch. Sementara *sFlow* dapat memberikan instrument standard kedalam *forwarding tables* perangkat switch tersebut yang kemudian dapat di akses melalui API untuk dapat memberikan gambaran *real-time* jaringan yang ada. Dengan menggabungkan keduanya, artinya kita dapat membuat sebuah aplikasi yang sifatnya *feedback control system* atau dapat melakukan adaptasi seketika bila dibutuhkan suatu perubahan kepada suatu jaringan.

Berdasarkan ulasan hasil sebelumnya, maka penelitian ini akan melakukan analisis dan penerapan OpenFlow dan sFlow untuk deteksi dan mitigasi DOS pada *Software Defined Network*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, maka didapatkan perumusan masalah yaitu :

- a. Bagaimana mengimplementasikan OpenFlow dan sFlow untuk melakukan deteksi terhadap serangan DOS pada *Software Defined Network*.
- b. Bagaimana mitigasi serangan DOS pada *Software Defined Network* dengan menggunakan OpenFlow dan sFlow.

1.3 Tujuan Tugas Akhir

Adapun tujuan yang hendak dicapai dalam penelitian tugas akhir adalah sebagai berikut :

- a. Merancang jaringan *Software Defined Network* menggunakan Mininet.
- b. Implementasi ONOS sebagai *OpenFlow Controller* dan *Network Topology*.
- c. Menggunakan sFlow-RT untuk monitor route dan traffic dalam jaringan.
- d. Melakukan pengujian dan analisa terhadap deteksi dan mitigasi bila terjadi serangan DOS pada *Software Defined Network*.

1.4 Manfaat Tugas Akhir

Adapun manfaat yang dapat diambil dari penelitian tugas akhir adalah :

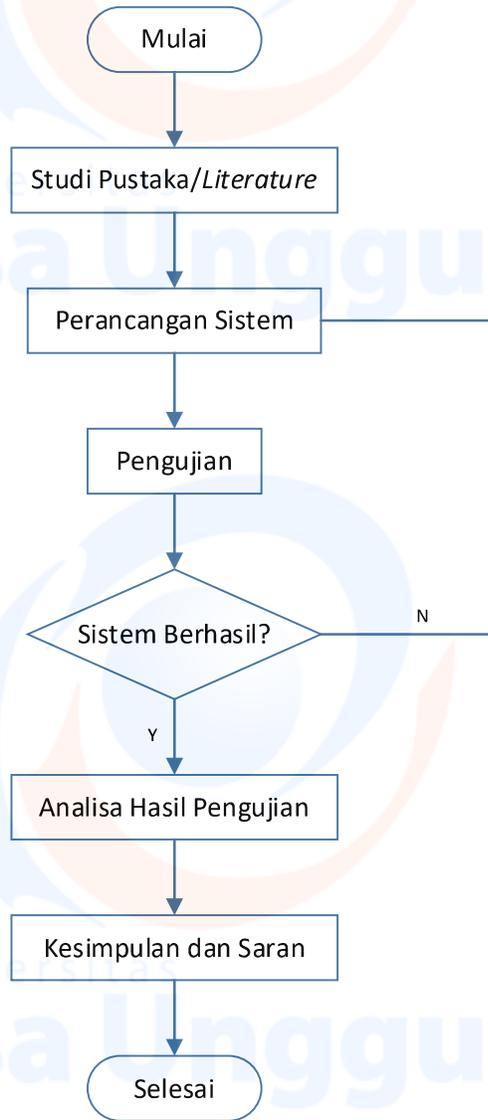
- a. Dapat menjadi solusi pencegahan DOS terhadap *Software Defined Network* yang lebih mudah dan terjangkau.
- b. Dapat menjadi referensi untuk penelitian atau pengembangan selanjutnya.

1.5 Lingkup Tugas Akhir

Selain perumusan masalah diatas, juga terdapat batasan masalah pada tugas akhir ini, antara lain :

- a. Topologi *Software Defined Network* dibangun secara simulasi
- b. *Tools* yang digunakan untuk membangun Topologi *Software Defined Network*, yaitu Mininet emulator yang bertindak sebagai data plane, ONOS sebagai *OpenFlow Controller*, sFlow digunakan untuk monitor route atau traffic dalam jaringan serta Nodejs dan Python digunakan sebagai bahasa pemrograman yang digunakan dalam pembuatan script untuk deteksi dan mitigasi serangan DOS.
- c. Protokol yang digunakan untuk komunikasi antara *Controller plane* dan *data plane* pada jaringan *Software Defined Network* adalah OpenFlow.
- d. Pengujian serangan DOS dilakukan dengan metode serangan *DNS Amplification*.
- e. Dalam pengujian saat ini Mininet belum mendukung multiple session dalam melakukan pengujian, sehingga pengujian potensi kesalahan (*false positive*) terhadap *traffic DNS legitimate* tidak dapat dilakukan.

1.6 Metodologi Penelitian



Gambar 1-1 Metodologi Penelitian

Pada Gambar 1-1, berikut ditampilkan metodologi penelitian secara visual dalam bentuk diagram alir yang merepresentasikan proses pelaksanaan penelitian. Metodologi yang akan digunakan dalam penelitian tugas akhir akan melewati beberapa tahap, yaitu :

1. Tahap Pertama (Studi Pustaka atau *Literature*)

Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk dijadikan sebagai penelitian, dengan membaca artikel atau makalah penelitian yang berhubungan langsung dengan tugas akhir.

2. Tahap Kedua (Perancangan Sistem)

Pada tahapan ini merupakan tahapan mengenai bagaimana proses membangun system dengan menggunakan metode atau pendekatan tertentu. Selain itu, apa saja perangkat keras ataupun perangkat lunak yang digunakan, kemudian bagaimana proses perancangan system, selanjutnya bagaimana pula penerapan metode pada penelitian tugas akhir.

3. Tahap Ketiga (Pengujian)

Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan. Dengan melakukan pengujian berdasarkan metodologi penelitian sehingga didapatkan data hasil uji yang sesuai dan tepat secara konsep ataupun praktis.

4. Tahap Keempat (Analisa)

Pada tahap ini adalah menganalisa data hasil pengujian berdasarkan parameter yang telah ditentukan, sehingga didapat hasil yang objektif dimana data diperoleh dari proses pengujian.

5. Tahap Kelima (Kesimpulan dan Saran)

Pada tahap ini akan dirumuskan suatu kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian dan analisis hasil pengujian. Kemudian beberapa saran yang dapat dijadikan landasan untuk lanjutan.

1.7 Sistematika Penulisan

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari setiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, tujuan tugas akhir, dan manfaat tugas akhir, lingkup tugas akhir, metodologi penelitian serta sistematika penulisan.

BAB II TINJUAN PUSTAKA

Bab ini berisi mengenai dasar teori dari penelitian tugas akhir tentang sejarah *Software Defined Network*, definisi *Software Defined Network*, arsitektur *Software Defined Network*, konsep protokol OpenFlow, ONOS sebagai *OpenFlow Controller*, mininet sebagai perangkat lunak untuk simulasi *Software Defined Network*, *sFlow-RT* sebagai monitor route dan traffic dalam jaringan, iperf sebagai *traffic generator* serta parameter pengujian deteksi dan mitigasi DOS.

BAB III METODE

Bab ini berisi penjelasan sistematis, mengenai bagaimana penelitian dilakukan. Penjelasan pada bab ini tentang tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang hasil pengujian yang dilakukan serta analisis dari data yang didapat dari hasil pengujian. Analisis data yang akan dilakukan yaitu berdasarkan parameter yang telah ditentukan sebelumnya yaitu *delay*, *packet counter* dan *packet trend*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan hasil penulisan dan saran yang dituliskan untuk penulisan dan penyempurnaan selanjutnya pada penelitian.