BAB 1

PENDAHULUAN

1.1 Latar Belakang

Internet merupakan suatu teknologi yang sudah menjadi kebutuhan vital masyarakat pada era saat ini. Sudah mulai bermunculan teknologi-teknologi baru yang sangat membutuhkan akses dari *internet* itu sendiri. Salah satu teknologi yang membutuhkan akses dari *internet* adalah teknologi *cloud computing*. Berbicara mengenai *cloud computing* tentu tidak akan lepas dari istilah yang biasa disebut dengan virtualisasi. Teknologi virtualisasi ini dapat diciptakan dengan menggunakan sebuah aplikasi yang biasa disebut dengan *hypervisor*, dengan bantuan *hypervisor* inilah maka mesin-mesin *virtual* dapat dibuat di dalam 1 *data center* fisik. Salah satu teknologi yang sangat dibutuhkan dalam virtualisasi adalah peran dari *software switch* yang dapat berfungsi menghubungkan mesin-mesin *virtual* di dalam *hypervisor*. *Software switch* tersebut adalah *openvswitch*, dengan digunakannya *software switch* yang mendukung protokol *openflow*, maka teknologi virtualisasi ini dapat memanfaatkan teknologi *SDN* sebagai orkestrasi jaringan di dalam teknologi virtualisasi ini.

Terdapat 3 jenis layanan atau service yang ditawarkan oleh *cloud computing*, salah satunya adalah *IAAS* atau *infrastructure as a service*. Layanan ini dapat menawarkan kepada pelanggan yang memiliki *data center* secara *virtual* atau *virtual data center*. Dengan menggunakan sebuah *virtual data center* maka kebutuhan akan *server* fisik akan berkurang dan hal tersebut akan sangat mengurangi biaya dari sebuah perusahaan. Namun masalah keamanan masih menjadi suatu persoalan dengan digunakannya layanan *virtual data center* ini. Masalah keamanan tersebut muncul mengingat digunakannya ip public untuk mendapatkan akses terhadap *virtual data center* tersebut yang sangat rentan terhadap serangan-serangan hacker melalui jaringan *internet*. Salah satu serangan yang saat ini masih menjadi salah satu serangan yang tidak dapat diatasi adalah serangan *syn flood attack* yang masuk ke dalam kategori serangan dos *attack* dengan mengincar aspek *availability* dari sebuah *server*. *Syn flooding attack* merupakan jenis serangan yang menitikberatkan kepada protokol TCP. Penyerang akan membanjiri korban dengan paket-paket *syn* palsu yang terdapat pada TCP protokol. Dengan *syn flooding attack* ini membuat suatu jaringan mengalami tidak adanya *availability* atau ketersediaan, yang merupakan salah satu aspek dari keamanan jaringan. Dalam *virtual data center* aspek

availability merupakan hal yang sangat penting untuk dijaga, dikarenakan dalam *virtual data center* terdapat suatu *server* yang merupakan pusat dari suatu jaringan computer Sudah terdapat banyak cara untuk mengatasi masalah keamanan tersebut antara lain, *DMZ, SYN Cookies* dan *SYN*Defender namun semua cara tersebut harus dilakukan di dalam *server* dan pada umumnya hanya dibangun pada satu point, hal tersebut tentu akan menghabiskan *resource* dari server dan perangkat jaringan.

Pada penelitian ini akan dibuat sistem pertahanan dengan memanfaatkan teknologi *SDN* yang saat ini sedang menjadi *trend* dalam dunia jaringan. Tujuan dari *SDN* sendiri adalah untuk memudahkan konfigurasi pada seluruh perangkat jaringan agar dapat dibuat secara terpusat. Untuk menerapkan hal tersebut dibutuhkan protokol *openflow* yang dapat memisahkan *control plane* dengan *data plane*. Dengan protokol *openflow* semua trafik yang melewati perangkat jaringan dapat dikontrol dengan mudah melalui *openflow* controller. Dengan manfaat tersebut, sistem keamanan mitigasi dapat diterapkan pada sisi perangkat jaringan dengan cara memodifikasi *flow table* pada *data plane*. Selain protokol *openflow* terdapat protokol *sflow* yang berfungsi sebagai monitoring jaringan. Protokol ini merupakan multi-vendor *sampling* teknologi yang dapat digunakan pada berbagai jenis *switch*. Dengan menggunakan protokol pemonitoraan pada setiap perangkat jaringan dapat dilakukan dengan membutuhkan *resource* yang sangat minimal.

Sistem keamanan akan diterapkan pada *virtual router* yang akan menghubungkan *virtual data center* dengan eksternal *network*, mengingat perangkat tersebut merupakan perangkat paling awal yang akan dilewati oleh paket-paket dalam *hypervisor*, selain itu perangkat jaringan merupakan lokasi yang tepat untuk memonitor setiap trafik yang melewati jaringan. Untuk menerapkan sistem keamanan pada *virtual router* maka diperlukan sebuah teknologi yang dapat memonitoring jaringan yang nantinya akan digunakan sebagai pendeteksi serangan, teknologi yang akan digunakan pada penelitian ini adalah *sflow*. Setelah serangan berhasil terdeteksi maka langkah selanjutnya adalah pemblokiran *ip address* penyerang, langkah tersebut akan dilakukan dengan memanfaatkan protokol *openflow* dengan melakukan *drop* trafik yang berasal dari penyerang. Pada penelitian sebelumnya [1] [2] [3] [4] telah dilakukan penelitian yang menggunakan sFlow dan openFlow dan terbukti dapat melakukan deteksi dan mitigasi dengan lebih cepat.

Dalam tugas akhir ini, penulis akan mengimplementasikan dan menganalisis sistem keamanan dengan menggunakan *sflow* dan *openflow* seperti pada penelitian sebelumnya pada jaringan *virtual data center* yang sudah menjadi *trend* untuk menggantikan *data center* konvensional.

1.2 Perumusan Masalah

Berdasarkan deskripsi latar belakang, maka dapat dirumuskan beberapa masalah di tugas akhir ini yaitu :

1. Bagaimana cara memanfaatkan *Sflow* dan *Openflow* dalam mendeteksi dan *memitigasi SYN FLOOD ATTACK* dalam jaringan *Virtual data center* ?
2. Bagaimana cara menguji keamanan jaringan *Virtual data center* dengan menggunakan *tools* untuk *hacking*?
3. Bagaiaman pengaruh metode keamanan yang digunakan terhadap aspek keamanan jaringan?
4. Bagaimana pengaruh metode keamanan yang digunakan terhadap performansi jaringan ?
5. Bagaimana pengaruh metode keamanan yang digunakan terhadap performansi dari sebuah server?

1.3 Tujuan Penelitian

Untuk menjawab beberapa permasalahan yang ada, maka tujuan dari penelitian ini adalah :

1. Memanfaatkan *Openflow* dengan *Sflow* sebagai sistem keamanan untuk mendeteksi dan memitigasi suatu serangan *SYN FLOOD ATTACK* di dalam jaringan *Virtual data center.*
2. Mensimulasikan suatu serangan ke *server* dalam *virtual data center* dengan metode serangan *SYN FLOOD ATTACK* agar dapat menganalisa sistem keamanan yang telah dibuat.
3. Menganalisis aspek keamanan dalam hal ini *availability* pada *virtual data center* dengan memanfaatkan *Sflow* dan *Openflow*.
4. Menganalisis aspek performansi jaringan dalam hal ini paket *loss* dan *round trip time* dengan sistem keamanan yang digunakan.
5. Menganalisis aspek performansi terhadap *server* dalam hal ini *cpu utilization* dan *memory utilization* dengan sistem keamanan yang digunakan.

1.4 Batasan Masalah

Batasan-batasan yang digunakan untuk mempermudah permasalahan dalam penelitian ini antara lain :

1. Implementasi *virtual data center* menggunakan *OPENSTACK*

2. Jaringan berjalan di jaringan IPv4

3. *Controller* yang digunakan adalah *controller Opendaylight*

4. Pada tugas akhir ini penulis tidak membahas performansi *SDN Controller*

5. Protokol yang digunakan adalah *Openflow* Protokol

6. Serangan ke *server* tidak sampai *server down*

7. *Virtual data center* hanya sebatas *instance tenant* dan tidak membahas secara mendalam mengenai openstack

8. Serangan hanya sebatas *Layer 3,* yaitu pada *TCP*

9. Jaringan *cloud computing* tidak dapat diakses melalui *internet*

10. Projek dikerjakan menggunakan *Virtual Machine*

1.5 Metodologi Penelitian

Metodologi dalam proses penyelesaian penelitian ini terdiri dari beberapa tahapan yaitu :

1. Studi Literatur

   Pada tahap ini, akan dilakukan pencarian, pengumpulan, dan mempelajari informasi referensi yang bersumber dari buku, jurnal maupun sumber lain dari *internet* sebagai landasan teori dalam pengerjaan dan penyusunan tugas akhir ini. Referensi yang dicari berkaitan dengan *Openflow protokol*, *Sflow,* dan *Virtual data center.*

2. Perancangan dan realisasi

   Merupakan tahap percobaan atau mencoba untuk membuat sistem dengan menerapkan hasil dari tahapan sebelumnya.

3. Analisis

   Pada tahap ini dilakukan pengimplementasian keamanan jaringan dengan memanfaatkan *openflow* dan *sflow* pada jaringan *virtual data center* yang telah dirancang sebelumnya.

4. Pengumpulan data dan analisis data

Menganalisis waktu yang dibutuhkan untuk mendeteksi dan memitigasi *syn flood attack* dalam jaringan *virtual data center* dan menganalisis pengaruh metode tersebut terhadap performansi jaringan.

5. Penyimpulan hasil

   Tahap penentuan kesimpulan penelitian berdasarkan data-data hasil percobaan dan capaian performansi untuk menjawab permasalahan dan pertanyaan penelitian.

1.6 Sistematika Penulisan

Sistematika yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, perumusan masalah, tujuan dan manfaat penelitian, pembatasan masalah dan asumsi penelitian, serta sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab ini berisi teori-teori yang digunakan dalam analisis pemecahan masalah.

BAB III PERANCANGAN SISTEM

Bab ini berisi tahapan-tahapan penelitian mulai dari persiapan hingga penyusunan laporan tugas akhir.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi analisis hasil pengolahan data dan pemecahan masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil pemecahan masalah dan saran-saran yang diberikan kepada pihak perusahaan

1.7 Jadwal Kegiatan

Untuk Memudahkan Penulis dalam pengerjaan agar selesai pada waktu yang diinginkan, maka diperlukan sebuah timeline atau jadwal kegiatan sebagai berikut :

Tabel 1. 1 Jadwal Kegiatan

No	Kegiatan	Bulan 1				Bulan 2				Bulan 3				Bulan 4				Bulan 5				Bulan 6			
1	Studi Literatur																								
2	Pengumpulan Data																								
3	Perancangan Sistem																								
4	Implementasi Sistem																								
5	Analisis Hasil Implementasi Sistem																								
6	Penyusunan Laporan																								