BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini perkembangan jaringan komputer sangatlah pesat dan semakin meningkatnya kekompleksitasan jaringan. Dengan pesatnya perkembangan jaringan komputer tersebut dalam dunia bisnis, perusahaan yang memiliki cabang banyak menginginkan sebuah teknologi yang dapat melakukan pengelolaan jaringan secara terpusat sehingga perusahaan tersebut dapat memonitoring atau mengelola cabang perusahaannya secara instan dan tidak mengeluarkan biaya yang terlalu besar Dengan adanya tantangan tersebut munculah suatu teknologi yaitu *Software-Defined Network* (SDN). SDN adalah sebuah terobosan terbaru dalam pemodelan jaringan modern dimana *control plane* dan *data plane* telah dibuat terpisah, pada dasarnya konsep SDN adalah sentralisasi dimana pengelolaan, konfigurasi, dan pengaturan jaringan dilakukan pada sisi *controller*[1], pada SDN terdapat beberapa controller yang dapat dipakai, yaitu Floodlight, OpenDayLight, POX, NOX, RYU dan yang terbaru adalah ONOS. Karena pada arsitektur SDN menggunakan sebuah perangkat kontrol untuk mengelola jaringan dengan skala besar hal tersebut dapat menimbulkan masalah *bottleneck*. Dengan demikian, konsep pengontrol SDN terdistribusi sedang diusulkan untuk menyelesaikan masalah tersebut seperti penggunaan konsep Open Network Operating System (ONOS) controller. Onos *controller* adalah sebuah platform yang terdistribusi sehingga memudahkan dalam pengelolaan penyebaran perangkat lunak, perangkat keras & layanan baru yang disederhanakan. ONOS merupakan kontrol jaringan pada perangkat lunak SDN berbasis Bahasa pemrograman java.

Namun bersamaan dengan berkembang pesatnya internet banyak juga serangan-serangan melalui internet, jaringan, dan lain-lain. Seiring dengan berjalannya waktu, serangan-serangan tersebut semakin banyak digunakan untuk hal-hal yang negatif, bahkan bisa sampai membuat komputer target menjadi lelet. Serangan *Denial Of Service* (DOS) adalah serangan yang sangat berbahaya bagi SDN karena konsep sentralisasinya. DOS adalah jenis serangan pada arsitektur jaringan komputer *modern* yang menargetkan pada perangkat atau server yang terdapat di dalam jaringan internet tersebut dengan tujuan yaitu untuk menghabiskan *resource* yang dimiliki oleh perangkat

tersebut hingga akhirnya perangkat atau *device* tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung membuat perangkat lain yang ingin memperoleh akses layanan menuju perangkat tersebut gagal atau *down service*. Dengan adanya masalah tersebut *firewall* adalah salah satu sistem keamanan jaringan yang dapat memblokir akses yang tidak sesuai dengan sistem *filtering* yang telah diatur oleh *system* administrator[1]. Pada penelitian [2] dilakukan simulasi dan analisis kinerja *Stateless* dan *Stateful Firewall* lalu membandingan masing-masing skema *firewall* pada SDN menggunakan RYU *Controller*, kinerja yang diukur berdasarkan parameter QoS (*Quality of Service*). Pada penelitian [1] dilakukan analisis performa *Centralized Firewall* pada SDN lalu menguji teknologi tersebut dengan melakukan penyerangan terhadap teknologi tersebut dengan tipe atau jenis serangan *Distributed-Denial Of Service* (DDos), performa diukur berdasarkan bitrate (Kbps), cpu using (%), waktu deteksi serangan (s), dan waktu penanganan serangan (s). Pada penelitian [3] dilakukan implementasi firewall pada jaringan SDN dengan *controller* Floodlight lalu merekomendasikan bahwa penelitian tentang SDN sangat penting karena banyak perusahaan IT besar menggunakan SDN untuk mengelola lalu lintas di antara pusat data mereka.

Pada proyek akhir ini diterapkan *firewall* pada *controller* ONOS, lalu dilakukan pengujian serangan DOS ke *controller* ONOS, dengan parameter yang digunakan sebagai pedoman dalam menganalisis adalah *throughput, respon time, packet loss,* dan CPU *utilization*.

1.2 Tujuan dan Manfaat

Adapun tujuan dari penulisan Proyek Akhir ini, sebagai berikut.

1. Membuat perancangan *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *syn flood*.
2. Membuat perancangan *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *icmp flood*.
3. Menganalisis kinerja firewall dengan parameter *throuthput, respon time, packet loss,* CPU *utilization*.

Manfaat dari penulisan Proyek Akhir ini, sebagai berikut.

1. Dapat merancang *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *syn flood*.

2. Dapat merancangan *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *icmp flood*.
3. Dapat memaksimalkan *throughput*, meminimalkan *respon time, packet loss,* dan CPU *utilization*.

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut.

1. Bagaimanakah perancangan *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *syn flood*?
2. Bagaimanakah perancangan *stateless firewall* pada jaringan SDN dengan *controller* ONOS yang dapat mengantisipasi serangan *icmp flood*?
3. Bagaimanakah kinerja firewall dengan parameter *throuthput, jitter, packet loss,* CPU *utilization*?

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini, sebagai berikut.

1. Untuk membangun jaringan SDN diperlukan perangkat jaringan yang *support Openflow*
2. Perangkat jaringan yang digunakan adalah mikrotik RB941-2nD-TC.
3. Penggunaan fitur aplikasi *reactive forwading* pada ONOS *Controller* sebagai konsep dasar SDN
4. Sistem kerja *firewall* menggunakan iptables.
5. Layanan yang digunakan adalah web server
6. Attacker menggunakan software hping3
7. Parameter yang di ujikan *throuthput, respon time, packet loss,* CPU *utilization*.
8. Pengujian dilakukan menggunakan jaringan local IPv4.

1.5 Metodologi

Adapun metodologi pada penelitian Proyek Akhir ini, sebagai berikut.

1. Studi Literatur

   Pencarian informasi yang terkait bersumber dari buku, media, jurnal dan diskusi yang bertujuan menunjang selesainya Proyek Akhir ini

2. Perancangan dan Implementasi sistem

   Melakukan perancangan dan pengimplementasian sistem sesuai dengan parameter yang diinginkan.

3. Analisis sistem

Mengamati hasil dari sistem yang dikerjakan sesuai dengan skenario yang telah ditetapkan serta menyimpulkan masalah yang ada.

4. Penarikan kesimpulan

Dari seluruh tahapan yang telah dilakukan diatas ditambah dengan masukkan dari dosen pembimbing maka dapat diambil kesimpulan dari hasil yang telah dilakukan.

1.6 Sistematika Penulisan

Dalam penulisan proyek akhir terdiri atas lima bab, dengan keterangan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan proyek akhir.

BAB III PERENCANAAN SISTEM

Pada bab ini membahas tentang deskripsi pengerjaan dan proses perancangan sampai implementasi sistem proyek akhir.

BAB IV PENGUJIAN DAN ANALISIS

Pada bab ini membahas tentang hasil pengujian perangkat berdasarkan parameter yang telah di tentukan

BAB V PENUTUP

Pada bab ini membahas tentang kesimpulan dari pengerjaan proyek akhir dan saran untuk pembaca yang akan mengambil penelitian dengan topik yang sama.