BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam teknologi jaringan komunikasi komponen keamanan jaringan merupakan suatu hal yang penting. Sifat dari jaringan adalah melakukan komunikasi data, untuk itu tidak ada jaringan yang benar – benar aman dari proses penyadapan [1]. Salah satu metode yang dipakai untuk membantu menjaga keamanan jaringan dari serangan luar adalah *firewall* [2].

Firewall adalah sebuah program perangkat keamanan jaringan yang memonitor lalu lintas yang masuk dan keluar pada jaringan dan memutuskan apakah akan mengizinkan atau memblokir lalu lintas tertentu berdasarkan aturan keamanan yang telah ditetapkan [3]. Implementasi *firewall* pada jaringan tradisional dinilai kurang efisien dalam penerapannya, hal ini dikarenakan perlu adanya konfigurasi pada setiap router yang akan digunakan. Untuk itu perlu adanya inovasi dalam penerapan firewall yaitu dengan menggunakan konsep *Software Defined Network* (SDN) [4].

Software Defined Network (SDN) merupakan sebuah konsep baru dalam perkembangan teknologi jaringan telekomunikasi di Indonesia, SDN dapat memudahkan pengguna dalam hal mendesain, mengelola, dan mengimplementasi jaringan. Konsep dasar SDN adalah dengan memisahkan antara *control plane* dan *data plane* dengan menggunakan protocol OpenFlow [5]. Dengan adanya SDN maka pengguna akan lebih mudah dalam mengatur aturan dalam satu perangkat kontrol sehingga lebih efisien dan mengurangi biaya konfigurasinya [6]. Saat ini *firewall* tradisional rentan terhadap banyak masalah, masalah utama yang dihadapi adalah luapan *firewall* yang disebabkan oleh pengguna yang terus menerus memperbarui aturan firewall, hal ini dapat menyebabkan firewall akan mengalami *overload* dan tidak bisa memproses lebih banyak paket. Hal itulah yang mendorong penggunaan layanan *virtual firewall*. Dengan menggunakan *virtual firewall* maka pengguna dapat membuat system firewall yang fleksibel dan dinamis dalam implementasinya, untuk dapat memonitoring *trafik* data dan mengatur keluar masuknya paket, serta menentukan hak akses oleh pengguna [7].

Selanjutnya, 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* [8]. 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.

Dalam karya buku tugas akhir ini, telah dilakukan analisa hasil implementasi *pfsense firewall* pada ONOS *controller* dengan model jaringan SDN.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka dapat dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana implementasi *virtual firewall* pada jaringan SDN menggunakan *controller* ONOS?
2. Mengapa penggunaan *pfsense firewall* saat ini lebih di unggulkan dibandingkan penggunaan *firewall* tradisional?

1.3 Batasan Masalah

Adapun batasan masalah pada proposal tugas akhir ini sebagai berikut :

1. Implementasi sistem berupa simulasi dengan menggunakan mesin virtual box menggunakan server HTTP.
2. Jenis *controller* yang digunakan pada penelitian ini adalah *controller* ONOS.
3. Penelitian ini tidak membahas mengenai perbandingan antar jenis *controller.*
4. Pengalamatan yang didukung adalah Ipv4.
5. Jenis *virtual firewall* yang digunakan pada penelitian ini adalah *virtual firewall* jenis *pfSense.*
6. Pengujian *firewall* dilakukan dengan menggunakan layanan iperf.

7. Topologi yang digunakan berupa 1 buah *controller,* 4 *virtual switch*, dan 4 *host*.
8. Server akan di install pada host 1 dalam topologi jaringan.
9. Pengambilan data menggunakan *iperf*.
10. Simulasi serangan menggunakan DoS *attack* yang dijalankan pada aplikasi *command prompt*.
11. *Background trafik* yang dikirimkan dari salah satu host sebesar 3Mb, 5Mb, 7 Mb, dan 10 Mb *connection.*
12. Pengambilan data dilakukan dalam interval waktu 10s.

1.4 Tujuan dan Manfaat

Tujuan dan manfaat dalam penelitian tugas akhir ini adalah dapat merancang sistem *pfsense firewall* pada jaringan SDN menggunakan *controller* ONOS dan menganalisa kinerja (*packet loss, jitter, throughput*) pada jaringan SDN yang menggunakan *firewall* maupun dengan yang tidak menggunakan *firewall* yang akan diuji dengan jenis serangan DoS *attack*.

1.5 Metodologi Penelitian

Metode yang digunakan untuk menyelesaikan penelitian tugas akhir ini adalah:

1. Studi Literatur

   Mempelajari konsep dasar dan teori mengenai jaringan SDN, *pfsense firewall* dan controller yang digunakan. Referensi yang digunakan berasal dari buku, jurnal, *paper,* maupun media online.

2. Perancangan sistem

   Pada penelitian ini akan dilakukan perancangan sistem yang akan digunakan dalam mengimplementasikannya. Sistem yang dibuat meliputi desain sistem jaringan SDN, *tools* yang digunakan, pengujian dan keluaran sistem. Sistem dibuat dengan cara melakukan simulasi SDN menggunakan *controller* ONOS dan mengimplementasikan *pfsense firewall* pada konsep SDN.

3. Simulasi

   Proses simulasi dilakukan menggunakan mesin *virtual box* adalah implementasi *pfsense firewall* pada jaringan SDN menggunakan *controller* ONOS

4. Analisis statistik

   Analisis dilakukan setelah proses simulasi selesai dilakukan. Data hasil simulasi akan diukur berdasarkan parameter yang telah ditentukan.

5. Kesimpulan

   Setelah semua proses diatas selesai maka dapat diperoleh sebuah kesimpulan berdasarkan data yang diperoleh.