BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era teknologi saat ini, penggunaan teknologi informasi mengalami peningkatan yang signifikan, terutama dalam mendukung berbagai aktivitas sehari-hari. Peningkatan ini mencakup berbagai aspek, mulai dari komunikasi, pendidikan hingga bisnis, yang semuanya bergantung pada infrastruktur teknologi yang handal. Namun, di balik kemudahan yang ditawarkan, perkembangan ini juga membawa tantangan baru, terutama dalam hal keamanan jaringan. Ancaman terhadap keamanan jaringan semakin meningkat, dan salah satu yang paling sering dihadapi adalah serangan *Distributed Denial of Service* (DDoS). Serangan DDoS merupakan salah satu jenis serangan yang paling umum dan kritis, yang menargetkan baik jaringan konvensional maupun jaringan generasi baru [1]. Serangan DDoS bertujuan untuk menguasai jaringan atau server dengan membanjiri target dengan traffic berlebihan, sehingga pelayanan menjadi lambat atau tidak dapat diakses oleh pengguna sah. Biasanya, serangan ini dilakukan oleh botnet yang terinfeksi perangkat lunak berisi kode berbahaya. Dalam konteks ini, *Software Defined Networking* (SDN) muncul sebagai solusi yang fleksibel dan andal untuk mengatasi tantangan ini, memungkinkan pengelolaan dan kontrol lalu lintas jaringan yang lebih efisien serta meningkatkan kemampuan deteksi dan mitigasi terhadap serangan DDoS [2].

Software Defined Networking (SDN) adalah pendekatan jaringan inovatif yang diperkenalkan untuk menyederhanakan konfigurasi dan administrasi jaringan, arsitektur SDN merupakan paradigma baru dalam manajemen jaringan yang memisahkan control plane dan data plane, serta membawa abstraksi ke lapisan kontrol jaringan dengan menyediakan antarmuka terbuka. Secara umum SDN memiliki pengendali terpusat dan kemampuan pemerograman jaringan yang dinamis. Fleksibilitas dan kemudahan konfigurasi yang ditawarkan oleh SDN menjadikannya pilihan utama dalam infrastruktur jaringan masa kini [3]. Dengan SDN, sistem keamanan jaringan dapat merespon anomali dan status lalu lintas

dengan cepat [4]. Meskipun arsitektur SDN menawarkan fleksibilitas, controller terpusat menjadi titik kritis yang rentan terhadap serangan DDoS, di mana controller menjadi target para penyerang yang berpotensi untuk meluncurkan serangan sehingga mengakibatkan server down [5].

Oleh karena itu, diperlukan strategi mitigasi serangan *Distributed Denial of Service* DDoS yang efektif, adaptif, dan responsif, terutama dalam lingkungan dinamis seperti SDN. penelitian sebelumnya telah menyoroti berbagai pendekatan mitigasi, termasuk *Intrusion Detection System* (IDS) yang mendeteksi serangan DDoS secara real-time, serta penerapan teknik load balancing untuk pengalihan paket pada pusat data dan memberikan pendekatan yang tepat untuk menangani dampak serangan DDoS [6][7]. Untuk mendemonstrasikan efektifitas teknik mitigasi tersebut secara realistis, penelitian ini menerapkan metode experimental dengan pendekatan kuantitatif, memanfaatkan emulator jaringan mininet untuk mensimulasikan jaringan nyata. Seperti yang dicatat dalam beberapa studi sebelumnya, Mininet memungkinkan pembuatan jaringan virtual yang kompleks dan dapat diadaptasi dengan berbagai kontroler SDN. Selain itu, mininet menyediakan dokumentasi lengkap dan kemudahan dalam pengaturan, sehingga memfasilitasi pengujian dan evaluasi sistem deteksi serangan DDoS secara inline dalam skenario yang menyerupai lingkungan nyata [1][8].

Menurut literatur, integrasi teknik mitigasi seperti firewall untuk memblokir lalu lintas berbahaya, IDS untuk deteksi dini anomali jaringan, dan load balancing untuk mendistribusikan beban traffic ke server yang lebih optomal, dinilai lebih efektif dibandingkan penggunaan teknik tunggal. Hal ini terbukti dari studi implementasi sistem pertahanan gabungan berbasis SDN yang menunjukan penurunan signifikan dalam dampak serangan DDoS saat diterapkan secara terpadu [9][10].

Berdasarkan permasalahan tersebut, penelitian ini berfokus pada penerapan strategi mitigasi serangan DDoS pada jaringan SDN dengan tiga pendekatan utama, yaitu *Intrusion Detection System* (IDS), firewall, dan load balancing (dengan pendekatan round robin, riku, dan pastest response). Penelitian ini menguji

efektivitas bagaimana ketiga teknik dalam menangani serangan DDoS jenis ICMP Flood, dengan tujuan akhir untuk menjaga ketersediaan dan performa jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah seperti di 1.1, maka beberapa permasalahan yang harus diselesaikan dalam penelitian ini:

1. Bagaimana efektivitas penerapan teknik mitigasi gabungan firewall, IDS, dan load balancing dalam mengurangi dampak serangan DDoS tipe ICMP Flood pada jaringan SDN?

1.3 Batasan Masalah

Berikut beberapa batasan masalah dalam penelitian ini, agar lebih terarah adalah sebagai berikut:

1. Penelitian ini menggunakan jaringan SDN dengan menerapkan topologi bawaan dari emulator mininet yaitu topologi single,3 dan Ryu controller sebagai pengendali utama jaringan.
2. Serangan yang digunakan ICMP Flooding dengan menggunakan tool hping3.
3. Menggabungkan tiga teknik mitigasi yaitu: Firewall, Intrusion Detection System (IDS), dan Load Balancing. Load Balancing diuji dengan tiga metode: round robin, riku, dan pastest response.
4. Pengecekan keberhasilan mitigasi diukur berdasarkan hasil pingall mininet, dengan parameter utama berupa persentase packet loss sebelum serangan, saat serangan, dan setelah mitigasi aktif.
5. Menggunakan Ubuntu Lts yang dijalankan di VirtualBox.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini sebagai berikut:

1. Menganalisis efek serangan DDoS ICMP Flooding terhadap kinerja jaringan SDN yang dikendalikan oleh Ryu controller.

2. Mengukur efektivitas dari ketiga teknik mitigasi Firewall, IDS, dan Load Balancing terhadap serangan DDoS
3. Menguji kinerja jaringan sebelum serangan, saat serangan, dan pada saat mitigasi aktif berdasarkan persentase packet loss dari hasil pengujian pingall

1.5 Manfaat Penelitian

Berikut ini adalah manfaat penelitian baik dari secara teoritis maupun praktis:

1. Meningkatkan pengetahuan terhadap strategi mitigasi serangan DDoS pada jaringan SDN.
2. Dengan menggabungkan tiga teknik mitigasi Firewall, IDS, dan Load Balancing, penelitian ini dapat menangani kinerja jaringan SDN dari ancaman serangan DDoS
3. Mengindikasikan pentingnya penggabungan ketiga teknik sebagai solusi pertahanan berlapis (defense in depth) pada infrastruktur masa kini.
4. Jadikan referensi untuk penelitian selanjutnya dalam meningkatkan performa jaringan SDN dari dampak serangan DDoS.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab pertama ini membahas mengenai bagian dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Penjelasan dalam bab ini bertujuan untuk menguraikan permasalahan yang diteliti, termasuk bagaimana permasalahan tersebut muncul, serta struktur penyajian laporan ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini mencakup studi literatur dan dasar teori, studi literatur akan membahas bagian-bagian penting serta melakukan perbandingan dan perbedaan dari beberapa jurnal atau referensi sebelumnya, sedangkan dasar teori

membahas konsep-konsep kunci yang relevan dengan penelitian ini

BAB III METODE PENELITIAN

Bagian bab ini menyajikan penjelasan secara detail mengenai objek yang diteliti, termasuk karakteristik dan konteks yang relevan dengan penelitian. Selain itu, bagian ini juga akan menguraikan langkah-langkah metodologis yang diambil dalam proses penelitian, mulai dari perencanaan hingga pelaksanaan. Serta menguraikan alat dan bahan yang digunakan dalam penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi terkait hasil-hasil pengujian dari rancangan sistem yang dikembangkan oleh penulis. Dalam bagian ini, penulis akan menguraikan hasil dari serangkaian pengujian yang dilakukan untuk mengukur kinerja dan efektivitas sistem. Setiap hasil pengujian akan disajikan dengan jelas, disertai dengan analisis yang mendalam mengenai data yang diperoleh.

BAB V PENUTUP

Bab penutup ini mencakup kesimpulan dan saran yang diperoleh dari penelitian yang telah dilaksanakan. Dalam bagian ini, penulis akan merangkum temuan-temuan kunci yang dihasilkan serta proses penelitian, serta memberikan saran yang relevan berdasarkan hasil yang diperoleh