BAB I PENDAHULUAN

I.1 Latar Belakang

Software-Defined Networking (SDN) adalah arsitektur jaringan modern yang bertujuan mempermudah pengelolaan jaringan melalui pemisahan antara fungsi kontrol dan data. Dalam arsitektur ini, control plane terpusat bertugas mengelola status jaringan dan mengirimkan instruksi ke data plane, sementara perangkat di data plane meneruskan paket data sesuai arahan tersebut. Model ini memungkinkan pengelolaan jaringan yang lebih fleksibel dan efisien, serta membuka ruang bagi inovasi dalam teknologi jaringan (Farooq et al., 2023) . Pemisahan *control plane* dan *data plane* dalam arsitektur terpusat SDN memungkinkan *controller* diprogram langsung, memberikan network administrator kemudahan dalam mengatur dan memelihara jaringan. SDN juga mendukung pemantauan *real-time* dan pengaturan lalu lintas yang dinamis, sehingga pemanfaatan sumber daya dan keamanan jaringan dapat dioptimalkan dengan kebijakan yang konsisten di seluruh jaringan (Le et al., 2020).

Namun, meskipun SDN memiliki berbagai keunggulan, kerentanannya terhadap serangan siber tetap menjadi perhatian utama. *Controller*, sebagai komponen utama dalam SDN, rentan terhadap serangan siber, terutama serangan *Distributed Denial of Service (DDoS)*. Dalam serangan ini, setiap lalu lintas jaringan yang tidak dikenal harus diteruskan ke *controller* untuk dianalisis lebih lanjut, yang membuka peluang bagi pelaku serangan untuk membanjiri *controller* dengan lalu lintas berbahaya. Tujuan serangan DDoS adalah mengganggu akses pengguna sah dengan cara membebani sumber daya jaringan hingga layanan menjadi tidak tersedia. Ketika *controller* terkena serangan DDoS, kapasitas lalu lintas menjadi kelebihan beban, yang akhirnya mengakibatkan gangguan pada *server* atau bahkan membuatnya tidak dapat diakses (Ulfa et al., 2024). Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) (2020), serangan DDoS adalah upaya pelaku serangan untuk menghabiskan sumber daya sistem sehingga sistem tersebut tidak mampu berfungsi optimal.

Salah satu jenis serangan DDoS yang perlu diperhatikan dalam konteks SDN adalah serangan *HTTP Flood*. Dalam serangan ini, penyerang membanjiri server dengan berbagai permintaan HTTP untuk menghabiskan sumber daya yang ada. Serangan *HTTP Flood* terdiri dari beberapa tipe, antara lain: *session flooding*, di mana botnet mengirimkan permintaan koneksi tinggi yang menguras sumber daya server; *requests flooding*, yang memanfaatkan sesi tunggal dengan banyak permintaan untuk melewati batas keamanan; *asymmetric attacks*, di mana permintaan dengan beban kerja tinggi atau celah aplikasi tertentu menyebabkan server terbebani; dan *slow request/response attacks*, seperti *Slowloris*, yang mengunci koneksi dengan permintaan yang berjalan lambat dan memaksa *server* kehabisan slot koneksi (Nisa & Ramadona, 2023). Serangan-serangan ini sangat berpotensi merusak jaringan SDN jika tidak ada tindakan mitigasi yang tepat.

Untuk menghadapi ancaman ini, teknik mitigasi yang efektif dan relevan dalam konteks serangan DDoS seperti *HTTP Flood* adalah penggunaan *Rate Limiting*. *Rate Limiting* adalah teknik yang bertujuan mengontrol jumlah permintaan yang dapat dilakukan oleh pengguna atau alamat IP dalam periode waktu tertentu. Dengan menerapkan batasan ini, organisasi dapat mencegah satu pengguna atau IP dari mengirimkan terlalu banyak permintaan yang berisiko membebani server, sehingga membantu mengurangi dampak serangan DDoS (Joque, 2022). Dalam menghadapi serangan DDoS seperti *HTTP Flood, Rate Limiting* memainkan peran penting karena mampu menurunkan beban yang ditimbulkan oleh permintaan tidak sah, sehingga sumber daya jaringan dapat dikelola lebih efisien untuk melayani pengguna sah.

Diharapkan, penelitian ini dapat mengidentifikasi solusi mitigasi yang efektif untuk menjaga kinerja, integritas, dan ketersediaan jaringan SDN dari serangan *HTTP Flood*. Selain itu, penelitian ini bertujuan memastikan bahwa layanan jaringan tetap optimal bagi pengguna sah melalui penerapan teknik *Rate Limiting* sebagai langkah mitigasi yang dapat mengurangi dampak serangan tersebut.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana implementasi serangan *HTTP Flood* pada SDN

b. Bagaimana cara mitigasi serangan *HTTP Flood,* pada SDN menggunakan *Rate Limiting*?

c. Bagaimana hasil perbandingan performa jaringan sebelum dan sesudah diterapkan mitigasi rate limiting terhadap serangan *HTTP Flood*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan, tujuan penelitian ini adalah sebagai berikut:

a. Menganalisis implementasi serangan *HTTP Flood* pada jaringan SDN.
b. Menerapkan mitigasi serangan *HTTP Flood* dengan menggunakan teknik *Rate Limiting* pada SDN melalui *Ryu Contoller*.
c. Mengevaluasi strategi mitigasi terhadap performa jaringan dalam menghadapi serangan *HTTP Flood* ada arsitektur SDN.

I.4 Batasan Penelitian

Batasan-batasan yang menjadi fokus dalam penelitian ini adalah sebagai berikut:

a. Jenis Serangan: Fokus penelitian hanya pada serangan DDoS tipe *HTTP Flood*, tanpa mempertimbangkan jenis serangan DDoS lainnya.
b. Metode Mitigasi: Penelitian ini hanya akan menggunakan strategi *Rate Limiting* sebagai metode mitigasi, tanpa membandingkan dengan metode mitigasi lain.
c. Penelitian ini dilakukan pada Linux Ubuntu 20.04 di VMware 17.
d. Topologi yang digunakan pada penelitian ini mencakup 4 switch dan 15 host.
e. Lingkungan Uji Coba: Pengujian dilakukan pada SDN simulasi, sehingga hasilnya mungkin berbeda jika diterapkan pada SDN nyata dengan variasi trafik yang lebih kompleks.
f. Skala Serangan: Skala serangan DDoS yang diuji dibatasi sesuai dengan kapasitas infrastruktur uji coba, sehingga hasilnya mungkin berbeda pada skala yang lebih besar.

g. Pengujian mitigasi serangan dilakukan menggunakan Mininet sebagai emulator jaringan untuk mensimulasikan kondisi SDN.
h. Metodologi PPDIOO *(Prepare, Plan, Design, Implement, Operate, Optimize),* dalam penelitian ini peneliti membatasi sampai tahap *design*.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini meliputi:

a. Meningkatkan pemahaman tentang dampak serangan *HTTP Flood* terhadap kinerja SDN.
b. Memperluas pengetahuan tentang teknik mitigasi serangan *HTTP Flood* menggunakan *Rate Limiting* pada SDN.
c. Menjadi referensi untuk pengembangan metode mitigasi serangan DDoS yang lebih efektif dan efisien.