BAB I
PENDAHULUAN

1.1 Latar Belakang

Software Defined Network (SDN) merupakan teknologi jaringan yang terus berkembang untuk mengatasi inkonsistensi dan kompleksitas dalam teknologi jaringan tradisional, hal ini mengakibatkan pengguna sulit dalam menyesuaikan pembaharuan yang dikeluarkan oleh vendor dan mengelola perbedaan aturan serta kebijakan teknologi (Yasin, 2020), (Abhilash & Divyansh, 2018). SDN hadir sebagai paradigma jaringan masa depan, yang menawarkan fleksibilitas dalam konfigurasi dan layanan (Syahputra dkk., 2020), (Lee dkk., 2020). Namun, perkembangan teknologi ini juga meningkatkan ancaman terhadap keamanan jaringan, salah satunya terhadap serangan *Distributed Denial of Service* (DDoS). Serangan tersebut mengancam stabilitas dan performa jaringan SDN dengan membanjiri lalu lintas jaringan menggunakan sejumlah besar paket (Boukria & Guerroumi, 2019), (Perwira dkk., 2019), (Quingueni & Kitsuwan, 2019).

Serangan DDoS berdasarkan Kaspersky DDoS *Intelligence* pada *Quartal* ke dua (Q2) tahun 2020 meningkat sekitar 30% dibandingkan dengan *Quartal* ke satu (Q1). Pada Q2 pada 9 April 2020 ini terdeteksi rata-rata serangan setiap harinya hampir 300 serangan dan Q1 terjadi 242 serangan. Peningkatan terus berlanjut hingga tahun 2021 berdasarkan salah satu perusahaan *cyber security* yaitu Tech Radar Pro. Kemudian berdasarkan *Securelist* pada Q1 tahun 2020 adanya peningkatan 80% dibandingkan dengan tahun sebelumnya yaitu 2019, dengan beberapa perusahan besar yang menjadi korbannya yaitu seperti *Github*, *Amazon Web Service*, *CloudFlare*, sampai *Bank of America* (Yudhana dkk., 2021).

Serangan DDoS menjadi kerentanan kritis dalam jaringan SDN yang harus segera di mitigasi, terutama melihat penelitian yang dilakukan oleh (Ananta dkk., 2023) yang menunjukan bahwa serangan DDoS menggunakan hping3 dengan PPDIOO dapat melumpuhkan jaringan SDN jika paket dikirimkan dalam jumlah yang besar dan cepat. Jaringan SDN ini dapat lebih cepat *down* pada saat jumlah penyerangan meningkat dan durasi serangan diperpanjang, mengakibatkan jaringan tidak dapat digunakan oleh pengguna yang sah. Meskipun SDN dapat dilindungi dengan *Firewall* yang terdapat pada *Controller*, serangan DDoS masih menjadi

suatu tantangan yang belum dapat diatasi sepenuhnya. Hal ini disebabkan karena *firewall* tradisional sering kali tidak mampu mendeteksi serangan kompleks seperti seperti DDoS, apalagi adanya keterba

tasan kapasitas dan skalabilitas dalam menangani volume lalu lintas yang besar dan durasi serangan yang lama (Thomas, 2005), (Alamsyah dkk., 2020). Melihat permasalahan tersebut, maka *Intrusion Prevention System* (IPS) hadir sebagai solusi dalam mengatasi kelemahan *Firewall* tradisional pada jaringan SDN.

Terdapat penelitian yang dilakukan oleh (Arifwidodo dkk., 2022) yang menunjukan efektivitas IPS menggunakan Snort yang mendeteksi dan memblokir serangan DoS dengan teknik SYN *Flood* pada jaringan SDN. Namun penelitian tersebut terbatas hanya dengan satu jenis serangan DoS dan tidak mencakup serangan DDoS yang lebih kompleks serta tidak melihat dampak dari serangan DDoS terhadap parameter *delay* dan *packet loss*. Melihat kekurangan tersebut Penulis tertarik membuat penelitian "Analisis Implementasi *Intrusion Prevention System* (IPS) untuk Mitigasi Serangan *Distributed Denial of Service* (DDos) pada Jaringan *Software Defined Network* (SDN)" yang mensimulasikan tiga jenis serangan DDoS yaitu SYN *Flood*, UDP *Flood*, dan ICMP *Flood*. Penelitian ini mengukur parameter yang terdiri atas *throughput*, *delay*, *packet loss*, CPU, dan memori dalam tiga kondisi yaitu sebelum serangan, saat terjadi serangan tanpa IPS, dan saat terjadi serangan dengan Snort IPS aktif. Hasil pengukuran ini kemudian dibandingkan untuk memantau performa jaringan SDN, dengan tujuan mengevaluasi efektivitas Snort IPS dalam menjaga kestabilan jaringan di tengah ancaman serangan DDoS.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan sebelumnya, maka penulis merumuskan masalahnya yaitu sebagai berikut:

1. Bagaimana analisis performa jaringan *Software Defined Network* (SDN) sebelum dan saat terjadinya serangan DDoS tanpa IPS?
2. Bagaimana analisis performa jaringan *Software Defined Network* (SDN) terhadap serangan DDoS yang sedang berlangsung tanpa dan dengan adanya implementasi *Intrusion Prevention System* (IPS) pada jaringan *Software Defined Network* (SDN)?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah dan batasan masalah maka terdapat beberapa tujuan dalam melakukan penelitian ini yaitu sebagai berikut:

1. Melakukan analisis performa jaringan *Software Defined Network* (SDN) sebelum dan saat terjadinya serangan DDoS tanpa IPS.
2. Melakukan analisis performa jaringan *Software Defined Network* (SDN) terhadap serangan DDOS yang sedang berlangsung tanpa dan dengan adanya implementasi *Intrusion Prevention System* (IPS) pada jaringan *Software Defined Network* (SDN).

1.4 Batasan Masalah

Berdasarkan Rumusan masalah yang telah disebutkan, maka penulis mempunyai batasan masalah sebagai berikut:

1. Implementasi IPS pada Arsitektur *Software Defined Network* (SDN)
2. Pada penelitian ini hanya menggunakan satu jenis IPS yaitu NIPS.
3. IPS *Tools* yang digunakan pada penelitian yang akan dilakukan Penulis yaitu menggunakan Snort3.
4. Jenis serangan yang digunakan yaitu *Distributed Denial of Service Attack* (ICMP *Flood*, SYN *Flood*, UDP *Flood*).
5. Pengukuran performa jaringan *Software Defined Network* (SDN) dalam penelitian yang akan dilakukan yaitu *Quality of Service* (QoS) terdiri atas *throughput*, *delay*, *packet loss*, pemakaian CPU, dan Memori.
6. Hanya melakukan 3 Pengukuran pengujian yaitu sebelum terjadinya serangan, ketika terjadi serangan tanpa IPS, dan ketika serangan dengan adanya IPS.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian yang akan dilakukan oleh penulis yaitu diantaranya:

1.5.1 Manfaat Teoritis

Secara teoritis, diharapkan penelitian yang akan dilakukan ini dapat menjadi sumber referensi bagi penelitian-penelitian selanjutnya dalam melakukan pengamanan dan pencegahan serangan terhadap jaringan dengan menggunakan IPS.

1.5.2 Manfaat Praktis

Penelitian yang akan dilakukan oleh penulis diharapkan dapat memberikan pengetahuan bagi berbagai pihak seperti:

1. Bagi penulis, diharapkan dapat memberikan manfaat berupa pengetahuan dan pemahaman terkait pentingnya mengamankan jaringan dengan menggunakan IPS.
2. Bagi Pengembangan Ilmu, diharapkan dapat memberikan manfaat berupa pengetahuan terkait pentingnya penelitian dalam menjaga keamanan jaringan dengan menggunakan IPS.
3. Bagi Perusahaan, diharapkan dapat memberikan manfaat berupa rujukan untuk solusi pengamanan bagi perusahaan dengan menggunakan IPS *tools* untuk mengamankan jaringan dari serangan.

1.6 Struktur Organisasi Skripsi

Struktur Organisasi yang ditulis guna mengetahui keseluruhan dari skripsi yang telah disusun. Adapun bagian-bagian strukturnya tersebut yaitu:

1. BAB I: Pendahuluan

   Bagian ini mencakup latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, serta struktur organisasi skripsi.
2. BAB II: Dasar Teori

   Bagian ini mencakup terkait dengan dasar ilmu atau teori yang mendukung untuk penelitian.
3. BAB III: Metode Penelitian

   Bagian ini mencakup penjelasan aspek-aspek penelitian terkait instrumen penelitian, prosedur penelitian yang terdiri atas, alur penelitian, alur percobaan, perancangan sistem, dan pengukuran data.
4. BAB IV: Hasil dan Pembahasan

   Bagian ini mencakup hal-hal terkait pengujian sistem, serta hasil dan pembahasan penelitian yang diperoleh melalui proses pengambilan data, analisis data, dan pengolahan data.
5. BAB V: Penutup

   Bagian ini mencakup kesimpulan dari seluruh hasil penelitian, implikasinya, dan rekomendasi yang dapat dikembangkan kembali.