BAB V
PENUTUP

5.1 Kesimpulan

Kesimpulan yang didapatkan dari penelitian Analisis Implementasi IPS untuk mitigasi serangan DDoS pada jaringan SDN, diantaranya:

1. Analisis performa jaringan *Software Defined Network* (SDN) ketika sebelum serangan dan saat terjadinya serangan tanpa aktivasi IPS menunjukkan adanya dampak negatif yang diberikan dari serangan DDoS terhadap jaringan SDN. Sebelum serangan DDoS, kondisi jaringan berada dalam kategori "Cukup Baik" untuk *throughput* dan "Sangat Baik" untuk *delay*, tanpa adanya *packet loss*, yang mencerminkan efisiensi dalam pengelolaan trafik. Namun, saat serangan DDoS terjadi, terutama dengan jenis serangan ICMP *Flood*, performa jaringan mengalami penurunan drastis, kondisi *throughput* dan *delay* berubah menjadi kategori "Buruk" dan terdapat *packet loss* yang masuk dalam kategori yang sama. Serangan lain, seperti SYN *Flood* dan UDP *Flood*, juga menurunkan performa jaringan, tetapi dampaknya sedikit lebih ringan, dengan penilaian performa jaringan yang dilakukan tersebut mengacu pada standar TIPHON. Kemudian pada penggunaan CPU serta memori mengalami peningkatan nilai rata-rata selama serangan DDoS menunjukkan beban yang lebih tinggi pada sumber daya sistem. Pada penggunaan CPU peningkatan drastis terjadi ketika serangan SYN *Flood* dilakukan sedangkan pada penggunaan memori peningkatan dratis terjadi ketika serangan UDP *Flood* dan ICMP *Flood*.
2. Analisis performa jaringan *Software Defined Network* (SDN) ketika serangan DDoS dilakukan dengan aktivasi IPS menunjukkan adanya dampak positif dari aktivasi IPS yang diberikan terhadap performa jaringan SDN. Serangan DDoS tanpa aktivasi IPS menunjukkan jaringan sangat terpengaruh berat oleh serangan DDoS, seperti SYN *Flood*, UDP *Flood*, dan ICMP *Flood*, dengan nilai rata-rata *throughput*, *delay*, dan *packet loss* berada dalam kategori "Buruk" menurut standar TIPHON. Sama halnya dengan penggunaan CPU dan memori yang nilai rata-ratanya mengalami lonjakan ketika serangan DDoS berlangsung pada jaringan SDN dengan nilai rata-ratanya tergolong cukup tinggi. Sebaliknya, ketika serangan DDoS terjadi setelah aktivasi IPS, nilai rata-rata

pada dua parameter yang mengukur performa jaringan SDN yaitu *throughput* dan *delay* menunjukkan hasil yang lebih baik. Meskipun *throughput* mengalami sedikit peningkatan saja dan tetap tergolong "kurang baik" untuk semua jenis serangan, namun nilai *packet loss* menurun secara signifikan, terutama pada serangan UDP *Flood* dan ICMP *Flood* yang berada dalam kategori "Baik". Namun, pada serangan SYN *Flood*, penanganannya hanya mencapai kategori "Cukup Buruk". Sementara itu, *delay* masih tetap dalam kategori "Buruk" akibat proses inspeksi paket oleh IPS yang menambah latensi. Penggunaan CPU dan memori juga meningkat secara drastis setelah aktivasi IPS, peningkatan nilai rata-rata tersebut terlihat pada setiap jenis serangan yang dilakukan dengan aktivasi IPS, mencerminkan beban kerja tambahan dalam memilih dan memproses paket mencurigakan.

5.2 Implikasi

Berdasarkan penelitian yang dilakukan oleh penulis dalam melihat dampak serangan DDoS dan aktivasi IPS terhadap jaringan SDN memberikan beberapa implikasi penting diantaranya:

1. Implementasi IPS dalam mitigasi serangan DDoS pada jaringan SDN dapat secara signifikan meningkatkan *throughput* dan mengurangi *packet loss*. Hal ini menunjukkan bahwa setelah aktivasi IPS, jaringan SDN dapat lebih efisien dalam menangani trafik yang besar akibat dari serangan DDoS. Namun di samping itu, implementasi IPS juga dapat menyebabkan peningkatan *delay* serta peningkatan penggunaan CPU dan memori.
2. Pada penelitian ini jenis serangan ICMP *Flood* merupakan jenis serangan DDoS yang paling berbahaya dibandingkan dengan jenis serangan SYN *Flood* dan UDP *Flood*. Hal tersebut dikarenakan jenis serangan ini dapat menyebabkan penurunan yang signifikan pada *throughput* serta peningkatan yang signifikan pada *delay*, *packet loss*, dan penggunaan memori.

5.3 Rekomendasi

Berdasarkan penelitian yang telah dilakukan, terdapat rekomendasi yang dapat dilanjutkan untuk penelitian selanjutnya yaitu terkait dengan penggunaan *tools* IPS lain seperti Suricata, agar dapat membandingkan efektivitas *tools* IPS dalam memitigasi serangan DDoS pada jaringan SDN.