BAB V
PENUTUP

5.1 Kesimpulan

1. Sebelum terjadinya serangan DDoS, performa jaringan SDN berada pada kondisi optimal dengan *throughput* tinggi, *delay* rendah, dan *packet loss* minimal. Nilai rata-rata *throughput* tanpa serangan adalah 750,54 Kbps. Namun, saat terjadi serangan DDoS, terjadi penurunan drastis dalam *throughput*. Pada serangan SYN *Flood*, *throughput* turun menjadi 463,44 Kbps, pada UDP *Flood* menjadi 456,51 Kbps, dan pada ICMP *Flood* menjadi 430,61 Kbps. Selisih *throughput* antara kondisi tanpa serangan dan selama serangan mencapai 287,10 Kbps untuk SYN *Flood*, 294,03 Kbps untuk UDP *Flood*, dan 319,93 Kbps untuk ICMP *Flood*, menunjukkan dampak negatif serangan terhadap *bandwidth* jaringan. *Delay* sebelum serangan sangat rendah dengan nilai rata-rata 0,156 ms. Selama serangan, *delay* meningkat signifikan, dengan nilai 461,79 ms pada SYN *Flood*, 469,40 ms pada UDP *Flood*, dan 475,55 ms pada ICMP *Flood*. Selisih *delay* mencapai 461,64 ms untuk SYN *Flood*, 469,24 ms untuk UDP *Flood*, dan 475,39 ms untuk ICMP *Flood*, menggambarkan peningkatan penundaan yang sangat besar akibat overload trafik serangan. Kemudian untuk *packet loss* sebelum serangan adalah 0,00%. Selama serangan, *packet loss* meningkat tajam, mencapai 37,05% pada SYN *Flood*, 37,94% pada UDP *Flood*, dan 39,26% pada ICMP *Flood*, menunjukkan bahwa *buffer* jaringan tidak mampu menangani volume trafik yang berlebihan. Terakhir pada penggunaan CPU dan memori juga mengalami peningkatan yang signifikan selama serangan. Penggunaan CPU meningkat dari 1,89% menjadi 38,72% pada SYN *Flood*, 30,54% pada UDP *Flood*, dan 30,91% pada ICMP *Flood*. Penggunaan memori meningkat dari 24,37% menjadi 45,41% pada SYN *Flood*, 55,30% pada UDP *Flood*, dan 55,54% pada ICMP *Flood*. Selisih penggunaan CPU dan memori menunjukkan beban tambahan yang berat pada sistem selama serangan DDoS.
2. Dengan adanya IPS, performa jaringan SDN selama serangan DDoS menunjukkan perbaikan yang signifikan dibandingkan tanpa IPS. *Throughput*

mengalami peningkatan yang signifikan, dengan nilai *throughput* lebih tinggi selama serangan. Misalnya, pada serangan SYN *Flood*, *throughput* meningkat dari 463,44 Kbps menjadi 528,93 Kbps; pada UDP *Flood*, dari 456,51 Kbps menjadi 562,23 Kbps, dan pada ICMP *Flood*, dari 430,61 Kbps menjadi 558,02 Kbps. Selisih *throughput* menunjukkan peningkatan 65,49 Kbps untuk SYN *Flood*, 105,72 Kbps untuk UDP *Flood*, dan 127,41 Kbps untuk ICMP *Flood*, yang menunjukkan bahwa IPS membantu memitigasi dampak serangan pada *bandwidth* jaringan. *Delay* selama serangan juga menunjukkan peningkatan, tetapi peningkatan ini lebih terkendali dibandingkan tanpa IPS. *Delay* untuk SYN *Flood* meningkat dari 461,79 ms menjadi 531,87 ms, untuk UDP *Flood* dari 469,40 ms menjadi 535,70 ms, dan untuk ICMP *Flood* dari 475,55 ms menjadi 593,92 ms. Selisih *delay* menunjukkan kenaikan 70,08 ms untuk SYN *Flood*, 66,3 ms untuk UDP *Flood*, dan 118,37 ms untuk ICMP *Flood*. Peningkatan *delay* ini sebagian besar disebabkan oleh proses tambahan yang dilakukan oleh IPS, yaitu pemeriksaan dan inspeksi paket untuk mendeteksi serta memitigasi serangan. Proses ini menambah latensi karena setiap paket harus melalui analisis tambahan sebelum diteruskan, meskipun penambahan *delay* ini lebih terkendali dibandingkan tanpa adanya IPS. Kemudian untuk *packet loss* berkurang secara signifikan dengan adanya IPS, menunjukkan perbaikan dalam pengelolaan *buffer*. *Packet loss* untuk SYN *Flood* turun dari 37,05% menjadi 18,07%, untuk UDP *Flood* dari 37,94% menjadi 13,51%, dan untuk ICMP *Flood* dari 39,26% menjadi 8,95%. Selisih *packet loss* menunjukkan pengurangan 18,98% untuk SYN *Flood*, 24,43% untuk UDP *Flood*, dan 30,31% untuk ICMP *Flood*, yang menunjukkan bahwa IPS efektif dalam mengurangi jumlah paket yang hilang selama serangan. Sedangkan pada penggunaan CPU meningkat dengan adanya IPS, yang menunjukkan tambahan beban dari proses analisis dan mitigasi. Penggunaan CPU meningkat dari 38,72% menjadi 94,74% pada SYN *Flood*, dari 30,54% menjadi 94,58% pada UDP *Flood*, dan dari 30,91% menjadi 94,38% pada ICMP *Flood*. Selisih penggunaan CPU menunjukkan peningkatan 56,02% untuk SYN *Flood*, 64,04% untuk UDP *Flood*, dan 63,47% untuk ICMP *Flood*, yang menandakan bahwa IPS membutuhkan sumber daya CPU yang signifikan. Peningkatan juga

terjadi pada penggunaan memori, meskipun kenaikan ini lebih kecil dibandingkan dengan penggunaan CPU. Penggunaan memori meningkat dari 45,41% menjadi 49,29% pada SYN *Flood*, dari 55,30% menjadi 80,40% pada UDP *Flood*, dan dari 55,54% menjadi 61,95% pada ICMP *Flood*. Selisih penggunaan memori menunjukkan kenaikan 3,88% untuk SYN *Flood*, 25,10% untuk UDP *Flood*, dan 6,41% untuk ICMP *Flood*, yang mengindikasikan bahwa IPS membutuhkan lebih banyak memori untuk menangani data trafik selama serangan.

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. *Throughput*: Aktivasi IPS meningkatkan *throughput* dibandingkan dengan Pengukuran tanpa IPS, namun tidak sepenuhnya mengembalikan *throughput* ke dalam kondisi semula, menunjukkan bahwa IPS efektif dalam mengurangi dampak serangan dengan sedikit penurunan performa.
2. *Delay*: IPS menambah *overhead* yang meningkatkan *delay*, meskipun *throughput* membaik, menandakan bahwa mekanisme perlindungan IPS menambah latensi pada jaringan.
3. *Packet loss*: Penurunan *packet loss* signifikan saat IPS diaktifkan, terutama pada serangan ICMP *Flood*, menegaskan efektivitas IPS dalam mengendalikan serangan DDoS.
4. Penggunaan CPU dan Memori: Aktivasi IPS meningkatkan penggunaan CPU dan memori secara drastis, menunjukkan perlunya peningkatan kapasitas sumber daya sistem untuk menjaga performa jaringan.

Implikasi ini menunjukkan bahwa meskipun IPS efektif dalam menjaga stabilitas jaringan dari serangan DDoS, ada konsekuensi dalam hal peningkatan *delay* dan penggunaan sumber daya, sehingga optimalisasi konfigurasi IPS dan peningkatan kapasitas sistem sangat diperlukan.

5.3 Rekomendasi

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa rekomendasi yang dapat diperbaiki dan dilanjutkan untuk penelitian berikutnya, yaitu:

1. Tambahkan *tools* IPS untuk membandingkan IPS yang lebih baik dalam implementasi pada jaringan SDN.
2. Menambahkan kembali parameter yang lain untuk mengukur performa IPS merespon serangan.
3. *Upgrade hardware* untuk meningkatkan kapasitas CPU dan memori pada perangkat yang menjalankan keseluruhan jaringan SDN.