ABSTRAK

Arsitektur SDN rentan terhadap serangan DDoS, khususnya *SYN Flood*, yang dapat melumpuhkan layanan jaringan. Penelitian ini mengimplementasikan dan menguji sebuah sistem *firewall* dengan metode *blacklisting* pada *Ryu Controller* untuk mitigasi serangan tersebut. Mekanisme pertahanan ini bekerja dengan memonitor laju pengiriman paket, sebuah parameter yang dipilih setelah analisis data menunjukkan bahwa paket serangan memiliki ukuran yang tetap sebesar 54 *byte*. *Firewall* dikonfigurasi untuk secara otomatis memasukkan alamat IP ke dalam *blacklist* jika terdeteksi mengirimkan lebih dari 50 paket SYN dalam interval satu detik. Pengujian dilakukan dalam lingkungan simulasi Mininet dengan membandingkan tiga skenario. Hasil pengujian menunjukkan bahwa pada skenario tanpa mitigasi, serangan dari 7 *host* menyebabkan latensi *Round-Trip Time* (RTT) pada lalu lintas normal melonjak hingga melebihi 2700 ms. Setelah sistem *firewall* diterapkan, latensi RTT berhasil ditekan dan tetap stabil di angka rata-rata 10-14 ms meskipun serangan terus berjalan. Selain itu, kinerja model deteksi SVM yang aktif bersamaan menunjukkan *F1-Score* di atas 82%, yang mengindikasikan kemampuan sistem untuk membedakan antara lalu lintas normal dan berbahaya secara akurat. Hasil ini menunjukkan bahwa sistem *firewall* dengan metode *blacklisting* yang diimplementasikan mampu menjaga stabilitas dan ketersediaan jaringan di tengah serangan *SYN Flood.*

Kata kunci: SDN, *SYN Flood*, Mitigasi Serangan, *Firewall, Blacklisting*