

Analisis kinerja sistem pendeteksi dan pencegahan serangan DDOS berbasis flow pada jaringan software defined networking openflow = Performance analysis for flow based prevention and mitigation systems denial of services attacks on openflow software defined networking

Dedi Gunawan, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20433421&lokasi=lokal>

Abstrak

Jaringan yang berbasis SDN, Software Defined Network kedepan secara perlahan akan menjadi alternatif sistem jaringan yang digunakan saat ini. Salah satu kelebihan utamanya adalah dalam satu box dapat diprogram untuk memiliki fitur apapun yang diinginkan, misalnya untuk dapat menjadi router, switch, access point, firewall dll. Pada penelitian ini akan dilakukan implementasi fitur firewall karena pada switch biasa seperti sekarang hal tersebut tidak dapat dilakukan, namun dengan SDN, maka hal tersebut dapat diterapkan. Yakni dengan memasukkan suatu instruksi kedalam openFlow switch untuk mendeteksi serangan DDoS sekaligus melakukan penanganan terhadap serangan tersebut.

Pengujian dilakukan dengan tool perangkat lunak network simulator mininet, floodlight controller dan SFlow. Setelah dilakukan pengujian, dapat dibuktikan bahwa suatu switch dapat juga berfungsi sebagai firewall untuk mengatasi serangan yang muncul pada jaringan. Berdasarkan pengujian tersebut telah dibandingkan kinerja sebuah jaringan SDN pada saat kondisi normal dan pada saat kondisi serangan berdasarkan pengukuran throughput dan latency. kemudian selanjutnya ketika fitur firewall diaktifkan untuk mengatasi serangan tersebut.

Dari penelitian tersebut didapatkan bahwa serangan DDoS menyebabkan delay paket semakin tinggi dan throughputnya menjadi semakin rendah. penambahan delay nya dari rata2 1,6 s naik menjadi 7,1 s dan penurunan nilai throughput dari rata-rata 66,5 Mbps turun menjadi 16,1 Mbps. Pada Penelitian ini telah dilakukan simulasi serangan secara bersama-sama dilakukan oleh banyak host menuju pada 1 server target dengan berbagai macam jenis serangan seperti udp, icmp dan tcp.

Network based on SDN, Software Defined Network in the future will be alternate network system which is already used from now. One of the main advantages is in one box we can create program to make any feature what we want, such as router, switch, access point, firewall, etc. In this research will be implementation some firewall feature because in normally switch like today that thing couldn't be done. But with SDN, that thing could be implemented. We can insert some instruction into openFlow switch to detection DDoS attack and how to prevent it.

The test will use software network to test DDoS with Mininet, Floodlight Controller and SFlow. After the research, we can proof that a switch could be function as a firewall to prevent attack our network. Based on research we already compare performance a network based SDN in normal condition and condition when our network attacked based on throughput and latency. Then when we activated firewall feature to prevent that attack.

From the research we can get information that DDoS attack cause delay packet much higher and throughput will be more slower. The average of delay increased from 1,6s to 7,1s. And the throughput decrease from 66,5 Mbps into 16,1 Mbps. In this research we have done attack simulation with many host to one specified server in one time with different method and protocol such as udp, icmp, and tcp.