Analisis Pengembangan Deteksi dan Mitigasi DDoS Attack pada Software Defined Network = Analysis Development of Detection and Mitigation DDoS Attack on Software Defined Network

Muhammad Farhan, author

Abstrak

Penelitian ini akan membahas proses pengujian terhadap serangan DDoS Attack pada jaringan virtual Software Define Network (SDN). Software Defined Network merupakan sebuah arsitektur jaringan yang memisahkan antara control plane dan data plane, berbeda dengan arsitektur jaringan pada umumnya. Pengujian dilakukan pada jaringan SDN memanfaatkan fitur OpenFlow switch, menggunakan aplikasi Mininet dan POX sebagai controller untuk OpenFlow switch dengan beberapa skenario dan arsitektur, yang menguji keamanan jaringan dengan protokol OpenFlow switch serta pencegahan dari controller POX. Pengujian tersebut akan membuktikan bahwa controller dapat mendeteksi traffic yang masuk dengan cara menganalisis traffic pada OpenFlow switch, serta mencegah penyerangan dengan melakukan drop paket pada OpenFlow switch. Dengan menggunakan metode ini, sistem deteksi dan mitigasi mendapatkan hasil yang cukup akurat dengan waktu rata-rata deteksi sekitar 17 detik untuk arsitektur 1 dan 48 detik untuk arsitektur 2. Sistem mitigasi ini juga memungkinkan pemantauan lebih mudah karena penurunan nilai entropi yang cukup signifikan ketika terdeteksi serangan, sebesar 15% - 22% pada arsitektur 1 dan 3% - 18% pada arsitektur 2.

<hr>This research will discuss the testing process for DDoS Attack attacks on the virtual network Software Define Network (SDN). Software Defined Network is a network architecture that separates between control plane and data plane, in contrast to network architecture in general. Tests were performed on SDN networks utilize the OpenFlow switch feature, using the Mininet and POX applications as controllers for OpenFlow switches with several scenarios and architectures, which test network security with OpenFlow switch protocols and prevention from POX controllers.

The test will prove that the controller can detect incoming traffic by analyzing traffic on the OpenFlow switch, and preventing attacks by dropping packets on the OpenFlow switch. Using this method, the detection and mitigation system gets quite accurate results with an average detection time of about 17 seconds for architecture 1 and 48 seconds for architecture 2. This mitigation system also allows easier monitoring because of a significant decrease in entropy value when detected attacks, by 15% - 22% on architecture 1 and 3% - 18% on architecture 2.