Analisis mitigasi dan deteksi serangan DDOS yang menggunakan openflow dan sflow pada jaringan berbasis software-defined network = Analysis of DDOS attack mitigation and detection system using openflow and sflow on software-defined network

Adhyatma Abbas, author

Abstrak

Software-Defined Network (SDN) merupakan sebuah teknologi baru pada jaringan komputer. Teknologi ini memungkinkan user untuk mengontrol alur data pada jaringan yang dibangunnya. Isu keamanan jaringan saat ini menjadi isu penting terutama untuk melindungi sistem dari berbagai serangan pada jaringan. Serangan ping flood merupakan salah satu dari jenis serangan Distributed Denial of Service yang banyak terjadi dan berkembang dengan cepat di dunia jaringan komputer. Untuk memproteksi sistem itu sendiri dapat dilakukan dengan berbagai cara seperti dengan menggunakan firewall dan IDS. Namun, meskipun firewall didesain untuk memproteksi sebuah sistem, akan tetapi firewall tidak dapat memitigasi serangan dengan kategori Distributed Denial of Service karena memang perangkat tersebut tidak didesain untuk jenis serangan ini. Untuk dapat meningkatkan kinerja dalam memproteksi sebuah sistem terutama untuk memitigasi serangan DDoS, maka dapat digunakan teknologi SDN dengan membangun suatu mekanisme mitigasi yang memanfaatkan OpenFlow dan sFlow. Dengan pemanfaatan teknologi ini, didapatkan sistem deteksi dan mitigasi serangan ping flood yang cukup akurat dengan rata-rata waktu akses normal sebesar 0,26636 ms dan waktu mitigasi dan deteksi sebesar 10,5 detik. Sistem mitigasi dan deteksi ini juga tidak akan menggunakan sumber daya yang banyak dan mampu menurunkan penggunaan CPU sistem yang terkena serangan ping flood dengan selisih kenaikan dan penurunan penggunaan CPU sebesar 0,001% yang berarti sistem ini mampu mendeteksi dan memitigasi serangan ping flood dengan cukup efisien.
.....Software-Defined Network (SDN) is a new technology in computer network which is make an users can control data flow in network that build by users. At this time, network security issues be more important issue especially for protect the systems from any attackers in the computer network. Ping flood attack is one of Distributed Denial of Service attacks type that happened more than other network computer attacks and this attack growth fastest in computer network area. There are many methods to protects the system from attacker, i.e. using firewall and IDS. However, although firewall designed for protect the system, but firewall cannot mitigating the Distributed Denial of Service attack type because it not designed for that case. So, to improve performance of DDoS mitigation, we can use SDN technology with build a mitigation mechanism using OpenFlow and sFlow. Using this technology, we can get a ping flood attack mitigation and detection system more accurate with time average for normal access 0,26636 ms and time for mitigation and detection 10,5 second. This mitigation and detection system is not going to use much CPU resources and have ability for decrease CPU resources from attacks with difference 0,001%. It means, this system is more efficient for mitigation and detection ping flood attacks.