RINGKASAN

PERANCANGAN SISTEM DETEKSI DAN MITIGASI SERANGAN *DENIAL OF SERVICE* PADA JARINGAN BERBASIS *SOFTWARE DEFINED NETWORKING*

Fian Visiardhana

Pengembangan jaringan perlu dilakukan agar kebutuhan kinerja, keandalan, dan keamanan jaringan dapat terpenuhi. Dalam pengembangan jaringan dilakukan dengan memisahkan *control plane* dengan *data plane* sehingga pengendalian perangkat jaringan menjadi terpusat, fleksibel, *automation* dan *programmable*, konsep tersebut merupakan *Software Defined Network* (SDN). Pada jaringan tradisional maupun jaringan berbasis SDN, keamanan menjadi permasalahan utama yang terus dikembangkan untuk mencegah terjadinya serangan yang semakin meningkat. Serangan yang sering terjadi pada jaringan, khususnya pada jaringan inti adalah *Denial of Service* (DoS) yang mana serangan DoS membanjiri trafik ke *server* tujuannya sehingga fungsionalitas jaringan dan *server* akan terhenti.

Pada jaringan yang berbasis SDN pun serangan DoS tersebut masih belum dapat ditangani dengan tepat jika hanya mengandalkan kontroler SDN dasar saja, maka penelitian ini akan merancang sistem yang mampu mendeteksi dan melakukan mitigasi terhadap serangan tersebut di jaringan berbasis SDN, salah satu aplikasi yang dapat dimanfaatkan untuk mengamati aktivitas dalam jaringan yaitu sFlow-RT, maka dengan integrasi antara sFlow-RT (yang dirancang sebagai pendeteksi serangan) dengan kontroler SDN dapat menjadi solusi keamanan jaringan berbasis SDN dalam menangani serangan DoS. sFlow-RT akan menganalisis trafik dan mendeteksi jika terjadi serangan kemudian memberikan intruksi kepada kontroler SDN untuk memblokir trafik dari penyerang sehingga serangan dapat dimitigasi dengan tepat, cepat dan otomatis.

Sistem yang dibangun mampu untuk mendeteksi 3 jenis serangan DoS yaitu ICMP Ping Flood, TCP SYN Flood, dan DNS Flood secara tepat dengan tindakan mitigasi berupa men-*drop* semua paket dari penyerang di *switch* yang terdekat sumber serangan, dan memiliki respons sistem yang cepat dengan rata-rata waktu deteksi sebesar 0.713 detik dan waktu mitigasi sebesar 4.947 detik pada karakteristik jaringan inti, serta mengonsumsi sumber daya rata-rata sebesar 52.2% untuk prosesor, dan 31.2% untuk memori dari virtual mesin dengan spesifikasi prosesor 4 *Core* dan memori 4 GByte.

Kata kunci : sFlow-RT, sFlow, serangan *Denial of Service*, *Software Defined Network*, jaringan inti topologi segitiga

SUMMARY

DESIGN OF DETECTION AND MITIGATION SYSTEM FOR DENIAL OF SERVICE ATTACKS IN SOFTWARE DEFINED NETWORKING-BASED NETWORKS

Fian Visiardhana

Network development is needed so that network performance, availability and security can be fulfilled. In network development is done by separating the control plane from the data plane so that network device control becomes centralized, flexible, automation and programmable, the concept is a Software Defined Network (SDN). In traditional networks and SDN-based networks, security is a major problem that continues to be developed to prevent increasing attacks. Frequent attacks on networks, especially in core networks, is Denial of Service (DoS) attack where DoS attacks will flooded the traffic to the server so that the functionality of network and server will stop.

In SDN-based networks, DoS attack still not able to handled properly if only using basic SDN controllers, so this study will design a system that can detect and mitigate DoS attacks on SDN-based networks, one application that can be used to monitor network activity, is sFlow-RT, with integration between sFlow-RT (which is designed for attacks detection) with SDN controllers, it can be a solution for SDN-based networks to mitigate DoS attacks. sFlow-RT will analyze the traffic and detect if an attack occurs then give instructions to the SDN controller to drop traffic from the attacker so that it can be mitigated appropriately, quickly and automatically.

The system built is capable to detect 3 types of DoS attacks, is ICMP Ping Flood, TCP SYN Flood, and DNS Flood precisely with mitigation actions is dropping all packets from the attacker on the switch closest to the source, and having a fast response system the average detection time is 0.713 seconds and the mitigation time is 4.947 second on the core network characteristics, and the average resource consumption is 52.2% for the processor, and 31.2% for the memory from the virtual machine with 4 Core processor and memory 4 GByte.

Keywords: sFlow-RT, sFlow, Denial of Service attacks, Software Defined Network, the core network of triangular topologi