ABSTRAK

Judul	:	Deteksi dan Mitigasi DOS pada *Software Defined Network* dengan menggunakan Openflow dan sFlow
Nama	:	Randy Mukti
Program Studi	:	Teknik Informatika

Software Defined Network (SDN) adalah arsitektur jaringan yang memisahkan control plane dan data plane. Fokus menelitian ini membahas tentang penerapan sFlow dan OpenFlow pada *Software Defined Network* untuk mendeteksi dan melakukan pencegahan serta packet capture terhadap packet besar atau DOS yang masuk ke dalam jaringan SDN. sFlow dan OpenFlow diimplementasikan pada sistem operasi Ubuntu 20.04, mininet sebagai virtual node, ONOS sebagai *OpenFlow Controller* dan network topology, sFlow-RT sebagai monitor route atau traffic dalam network, NodeJS dan phyton sebagai bahasa pemrograman yang digunakan untuk aplikasi SDN ini. Skenario pengujian dilakukan dengan cara switch mengirim sample packet dan mengirimkan header dari sample packet tersebut ke sFlow-RT. sFlow-RT kemudian memetakan packet yang sudah diterima kedalam bahasa atau flow yang lebih terstruktur. Jika paket sudah melewati batas *threshold* yang sudah ditentukan kemudian akan mentrigger event. Event tersebut kemudian yang akan dapat diakses dari aplikasi external melalui REST-API. Adapun hasil dari simulasi ini menunjukan bahwa ONOS dan Mininet dapat digunakan untuk pengembangan dan pengujian serangan DOS terhadap jaringan yang mengadopsi paradigma SDN.

Kata kunci : SDN, Deteksi dan Mitigasi DOS, OpenFlow

Title	:	*DOS Attack Detection and Mitigation with OpenFlow*
Name	:	Randy Mukti
Study Program	:	*Information Technology*

ABSTRACK

A Software Defined Network (SDN) is a network architecture that separates the control plane and data plane. The focus of this research discusses the

application of sFlow and OpenFlow in the Software Defined Network to detect and prevent as well as packet capture of large packets or DOS that enter the SDN network. sFlow and OpenFlow are implemented on the Ubuntu 20.04 operating system, Mininet as a virtual node, ONOS as an OpenFlow Controller and network topology, sFlow-RT as a route or traffic monitor in the network, NodeJS and Python as programming languages used for this SDN application. The test scenario is done by means of the switch sending sample packets and sending the header of the sample packet to sFlow-RT. sFlow-RT then maps the received packets to a more structured language or flow. If the packet has passed the predetermined threshold then it will trigger an event. The event will then be accessible from external applications via the REST-API. In the result from following simulation showing that ONOS and Mininet able to be used for development and testing DOS attack for SDN Networks.

Keywords: *SDN, DOS Detection and Mitigation, OpenFlow.*