INTISARI

IMPLEMENTASI FIREWALL PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN) DENGAN PENDEKATAN *WHITELISTING* DAN ALGORITME K-MEANS

Seiring bertumbuhnya pengguna internet, maka tingkat kompleksitas jaringan yang ada di dalamnya juga meningkat, seperti *firewall*. Pada kondisi lain, saat ini tengah berkembang teknologi SDN yang merupakan teknologi jaringan baru yang di dalamnya dilakukan pemisahan bagian infrastruktur perangkat jaringan menjadi *control plane* dan *data plane*. Hal ini berdampak pada pembuatan kebijakan hak akses user pada firewall yang di pusatkan pada kontroler yang nantinya diizinkan oleh *switch OpenFlow*. Pengontrolan jaringan terpusat oleh SDN membuat pengaturan dan konfigurasi lebih mudah. Pada makalah ini dilakukan implementasi *firewall* pada jaringan SDN dan melakukan perizinan pengiriman paket dalam komunikasi antar *host* yang terhubung dengan *OpenFlow* menggunakan perangkat Mikrotik. Hasil uji hak akses dari kriteria akses yang diizinkan akan dilakukan pengelompokan /*clustering* pada sebuah *database* dengan algoritme K-Means. Penerapan firewall ini dilakukan dengan menggunakan pendekatan *whitelisting* pada penerapan hak akses. Hal ini dilakukan karena *firewall* akan menolak semua paket data yang tidak memenuhi kriteria dalam daftar tersebut dan hanya mengizinkan paket data yang memenuhi kriteria dalam daftar. Parameter yang digunakan dalam pengujian *firewall* adalah *frame time, ip-src, ip-dst, eth-src, eth-dst* dan *protocol*. Penelitian ini akan dihasilkan keluaran paket data pada komunikasi jaringan SDN pada saat diterapkan *firewall* dengan pendekatan *whitelisting* yang dikelompokan pada sebuah *database* untuk memudahkan dalam melakukan analisa paket berdasarkan parameter yang digunakan.

Kata Kunci : SDN, *Firewall, OpenFlow, Floodlight, Whitelisting, K-means.*

ABSTRACT

IMPLEMENTATION OF FIREWALL ON SOFTWARE DEFINED NETWORK (SDN) WITH WHITELISTING APPROACH USING K-MEANS ALGORITHM

Due to increasing of internet users, the level of complexity of the existing network also increased, such as firewalls. By now, currently developing SDN technology is a new network technology which in separation of the network infrastructure part of the device into a control plane and data plane. This has an impact for the creation of user permissions policies on firewalls that are centralized by the controllers that are allowed by the switch of OpenFlow. Centralized network control by SDN makes setting and configuration easier. In this paper, the implementation of the firewall on the SDN network and do the filtering package in communication between connected hosts and OpenFlow using Mikrotik devices. The permission test results of the allowed access criteria will be clustered on a database with the K-Means algorithm. Application of this firewall are using whitelisting approach in applying the permissions. The firewall will reject all data packets that are out of criteria list and only allow data packets that on criteria list. The parameters used in firewall testing are frame time, ip-src, ip-dst, eth-src, eth-dst and protocol. This research will produce the output of data packets in SDN network communications on the use of firewalls with whitelisting approach that has been grouped in a database to facilitate in conducting packet analysis based on generated parameters.

***Keywords**: SDN, Firewall, OpenFlow, Floodlight, Whitelisting, K-means*