ABSTRACT

The development of technology is accompanied by the development of computer networks. One of them is the development of the internet. The Internet has an important role that can affect human life. Such as providing information. Several factors affect the performance of the Internet. One of them is the network. When configuring hardware or software, designing the best network infrastructure requires a dynamic, adaptable and easy-to-manage network architecture. To achieve this goal, a concept known as Software Defined Network (SDN) is needed. SDN allows us to build infrastructure and manage networks by creating centralized control regardless of the underlying network technology. One of the aspects that should be considered in sdn is the security aspect. The safety of SDN is said to be comprehensive if it meets 8 criteria, one of which is multi-tenancy. In a multi-tenant environment, tenants can share network elements, so the evolution of SDN technology has several security vulnerabilities. This study presented a security analysis of SDN-based multi-tenant virtualization network firewalls, by applying network slicing methods using FlowVisor to strengthen the isolation of each slice on sdn networks. SDN virtual network simulation uses mininet and POX controller as the main components of SDN. POX is responsible for performing control decision tasks when issuing data packets. Furthermore, the author evaluates the performance of SDN simulation network using three test scenarios, including connectivity tests where FlowVisor has not been run so that between hosts are connected to each other, functionality tests where in this test there has been network slicing using FlowVisor, this will cause the host to be connected if it is located in the same tenant. And lastly test the resource utilities. The results of this study were measured using QoS parameters (throughput, packet loss, delay, and Jitter) on Transmission Control Protocol (TCP) and User Data Protocol (UDP) packets. The QoS result generated in each TCP and UDP throughput test is classified in the very good category except for scenario one with 1Mbps background traffic, in the packet loss parameters some tests are categorized as very good, good and moderate. In the delay parameter, the results of the test show that all scario are in very good categorization. In the jitter parameter, it obtained a good category on connectivity tests with UDP and TCP protocols and very good on functionality tests except for scenario one. throughput, delay and jitter categorization is based on TIPHON standardization, and packet loss is based on the 1999 ETSI standard. The results of resource utilities testing show that CPU performance on SDN networks that have not implemented FlowVisor tends to be more stable than SDN networks that have implemented FlowVisor and for memory performance on SDN networks that have implemented FlowVisor tend to be greater than memory performance on SDN networks that have not implemented FlowVisor.

Keywords : *Software Defined Network* (SDN), *Network slicing, FlowVisor, Quality of Servive* (QoS)