ABSTRACT

Network security is the most important component in the communication network, without network security then a network system that we will create will be vulnerable to being hacked by irresponsible people. One of the techniques of network security is to use a firewall. The implementation of firewalls on traditional networks is considered less efficient in its application, this is due to the need for configuration on each router, in addition traditional firewalls are vulnerable to many problems, the main problem faced is the overflow of firewalls caused by users constantly updating firewall rules, this can cause firewalls to overload and not be able to process more packages. That's what drives the use of virtual firewall services. By using a virtual firewall, users can create a flexible and dynamic firewall system in its implementation. In addition, there needs to be innovation in the application of the network in a place so that it is easy to carry out maintenance and supervision of incoming data traffic. In this case the concept of Software Defined Network in value is the right solution to solve the problem. By using SDN, the existing network will be easily managed in one control device.

In its implementation, based on the test results of throughput, jitter, and packet loss parameters in sdn network using DoS attack. It can be concluded that at the time of measurement of data using traffic background. The use of Pfsense firewall in SDN network has better performance compared to SDN network without firewall. In addition, packet loss measurements are performed when there is an attack without a firewall the data obtained is worth 0 or no packets are lost during package delivery. This is caused by the controller that has been down so that the communication between the client and the server fails so that even along with the increase in the amount of traffic given though.

Keywords: Network security, SDN, firewall, virtual firewall