ABSTRACT

In the era of globalization technological developments have provided many benefits to the community. One is the development of digital technology, especially in the network connectivity sector. With the development of technology makes people able to do many things at a great distance though. The development of network connectivity would require security guarantees, so that data sent is not lost or stolen.

In this final project will be analyzed and simulated IPSec vpn tunnel. The simulation process is done by using GNS3 software and for the analysis performance done using NS2 software by making two scenarios, among others the first scenario on the network added a security and then given blackhole and rushing attack. As for the second scenario using blackhole and rushing attacks, but the network is not added a security.

Based on the result of simulation show that IPSec vpn tunnel work well. The results of the simulation can be seen using wireshark software. As for the results of network performance test, the network by using additional security has better results than the network that does not use it when an attack occurs. In the perfomance test scenario with blackhole attack and given additional security to change the number of nodes produce the average value for throughput of 1253.16 kbps, delay 394.17ms, and packet loss 9.22%. As for the results of QoS given blackhole attacks without additional security has decreased. For scenario test using rushing attack and without additional security to change the number of nodes produce the average throughput value of 740.76 kbps, packet loss of 2.2%, and delay of 233.53ms. Meanwhile the scenario with additional security has increased QoS value.

Keywords: IPsec, VPN, Tunneling Mode, Network Security , Blackhole, Rushing.