Abstract

Dynamic Multipoint Virtual Private Network (DMVPN) technology is one of Cisco's solutions to overcome the limitations of scalability in VPNs. DMVPN has a combination of components: Next hop resolution protocol (NHRP), Multipoint Generic Routing Encapsulation (mGRE) and Routing protocol. This research implements a simple network consisting of Hub, Spoke1, Spoke2, Lan1, Lan2 and Lan3 using the GNS3 simulator. This study compares the performance of IPSec and without IPsec on DMVPN using the BGP Routing protocol on performance parameters namely delay, throughput, jitter and packet loss to evaluate the security impact of the DMVPN network. The results of this study indicate that IPSec DMVPN has an effect on sending UDP packets which have a throughput value of No. IPSec is 4582.40 kbit/s while the IPSec throughput value is 4466.32 kbit/s. The packet loss value and the jitter value have the same value so it has no effect. The No IPSec delay value has a value of 0.295s while the IPSec delay value is 0.761s. TCP packet delivery has a throughput value of No. IPSec is 4598.72 kbit/s while the IPSec throughput value is 4515.44 kbit/s. The packet loss value and the jitter value have the same value so it has no effect. No IPSec delay value has a value of 0.301s while the IPSec delay value is 0.766s.

Keywords: DMVPN, VPN, Routing BGP, IPSec, network performance