ABSTRACT

Virtual Private Network (VPN) technology has become a popular solution for extending private networks over public connections such as Internet. A site-to-site VPN connects two separate local networks over Internet, and usually requires strong safeguards to protect the data exchanged between the two parties. One of the most recent VPN protocols today is WireGuard. WireGuard is a VPN protocol that runs at layer 3, which is built with sophisticated cryptography and makes it claimed to have the ability to provide strong security and better performance than other protocols. Therefore, this research analyzed the security and performance of a site-to-site VPN network using the WireGuard protocol. Testing was carried out on a site-to-site network, which connected the server's local network at site A and the client's local network that had been infiltrated by attackers at site B. The client accessed webserver A, then uploaded a files. The attacker on site B launched a DDoS attack on the webserver to then measure network performance with parameter availability, throughput, delay, and packet loss. The results of this study demonstrate the reliability of WireGuard in mitigating DDoS attacks. Increase the percentage of successful uploads, packet size and average packets sent per second, as well as provide consistent and optimal quality of service performance with an average throughput value of around 5 MB/s, 0.4 ms delay, and only 0.006% packet loss.

Keywords: *Network Security, VPN, site-to-site, WireGuard, DDoS*