ABSTRACT

The development of information technology has increased the need for flexible and secure remote access to home server data. Still, the combination of Virtual Private Network and reverse proxy usage poses performance challenges because security mechanisms such as encryption and tunneling can introduce overhead on data packets that increase latency and reduce throughput. This research is important because various VPN protocols have different characteristics in handling overhead and processing efficiency that directly impact system performance. At the same time, current conditions show that VPN protocol selection and system configuration are still based on theoretical assumptions without comprehensive empirical evaluation. This research implements an empirical analysis approach to the performance of home server access configuration using VPN combinations by comparing WireGuard and OpenVPN protocols as well as Nginx-based reverse proxy implementation, where the system is designed with a network topology consisting of two Virtual Private Servers as gateways and testing units as well as two Raspberry Pi units as target home servers with four testing scenarios focused on Quality of Service parameters namely response time, latency, and CPU and RAM resource utilization. Testing results show that OpenVPN with reverse proxy produces the best response time of 9ms and the lowest latency of 69.656ms. In contrast, WireGuard without reverse proxy is most efficient in CPU usage with consumption of only 16.7%, where reverse proxy implementation proves to provide a positive impact on response time for both protocols with OpenVPN showing better adaptation to reverse proxy architecture. Hence, this research contributes to providing empirical guidance in selecting appropriate VPN protocols for home server implementation with reverse proxy architecture.

***Keywords**: WireGuard, OpenVPN, Reverse Proxy, Home Server, Performance Analysis, VPN*