

ABSTRACT

The need for secure remote access to services and personal data drives the use of solutions such as reverse proxy and Virtual Private Network (VPN) in home server management. This research analyzes the performance of two popular web servers, NGINX and Apache, as reverse proxies integrated with OpenVPN for home server access, with a focus on performance in restricted environments such as Virtual Private Server (VPS) and Raspberry Pi. Four test scenarios were designed to measure and compare response time, latency, and CPU and RAM consumption: NGINX and Apache as reverse proxy with OpenVPN, and direct access without reverse proxy on each platform. Measurements were performed using curl, ping, top, and free to obtain valid empirical data. The evaluation results show that Apache reverse proxy with OpenVPN produces the fastest response time (0.1062 seconds) but with higher CPU consumption (6.1%), while NGINX reverse proxy offers efficient resource usage (CPU 3.1%, RAM 8.3%) with consistent response time. The direct access scenario indicates a trade-off between efficiency and access stability. These findings provide empirical recommendations regarding the selection of the optimal reverse proxy in a VPN-based home server environment, as well as a practical reference for network administrators in configuring and optimizing an efficient and secure remote access infrastructure.

Keywords: Apache, home server, latency, Nginx, OpenVPN, response time, resource usage,