BAB 5
SIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan komprehensif yang ditarik berdasarkan sintesis data kuantitatif hasil pengujian performa dan validasi keamanan (*Blue Teaming*), serta memberikan saran konstruktif untuk pengembangan penelitian selanjutnya.

5.1 Simpulan

Berdasarkan rumusan masalah yang diajukan pada Bab 1 dan hasil analisis data empiris pada Bab 4, penelitian ini menyimpulkan hal-hal sebagai berikut:

1. Perbandingan Kinerja Jaringan (*Network Performance*)
   Metode *Nginx Reverse Proxy* terbukti memberikan kinerja paling responsif dengan rata-rata *latency* terendah sebesar 20,58 ms, lebih unggul dibandingkan VPN WireGuard yang mencatat 37,23 ms. Mengacu pada standar *Quality of Service* (QoS) ETSI TIPHON TR 101 329, kedua nilai *latency* tersebut diklasifikasikan ke dalam kategori "Sangat Bagus" karena berada jauh di bawah ambang batas 150 ms, yang mengindikasikan kelayakan sistem untuk mendukung interaksi *real-time*. Namun, ditinjau dari segi *throughput* dan kecepatan transfer berkas, seluruh skenario akses jarak jauh mengalami penurunan performa signifikan sebesar $\pm$97% dibandingkan akses lokal (*Baseline* 889,34 Mbps), dengan kecepatan rata-rata konvergen pada kisaran 23–26 Mbps. Hal ini mengindikasikan bahwa *bottleneck* utama kinerja bukan disebabkan oleh *overhead* enkripsi, melainkan oleh limitasi kapasitas *upload bandwidth* pada jaringan ISP rumah.

2. Efektivitas Mekanisme Keamanan
   Validasi keamanan menggunakan standar NIST *Special Publication* (SP) 800-115 membuktikan bahwa kedua metode akses efektif melindungi kerahasiaan dan integritas data. Analisis *Deep Packet Inspection* (DPI) mengonfirmasi bahwa protokol WireGuard (menggunakan ChaCha20-Poly1305) dan Nginx (menggunakan TLS 1.2 AES-GCM) berhasil mengenkripsi 100% *payload* menjadi *ciphertext*, sehingga memitigasi risiko serangan *sniffing*. Selain itu, arsitektur *Hub-and-Spoke* terbukti efektif meminimalkan permukaan

serangan (*attack surface*) dengan menyembunyikan topologi jaringan internal dan menutup seluruh *port* non-esensial pada *gateway* publik.

3. Analisis *Trade-off* dan Rekomendasi
   Berdasarkan keseimbangan antara performa dan keamanan, Skenario Nginx merupakan metode paling optimal untuk penggunaan umum berbasis web. Hal ini didasarkan pada capaian kualitas layanan kategori "Sangat Bagus" menurut standar ETSI TIPHON serta kemudahan akses tanpa memerlukan instalasi klien tambahan. Sebaliknya, untuk kebutuhan administrasi sistem atau akses data sensitif, Skenario Hybrid (VPN + Nginx) lebih direkomendasikan karena memberikan lapisan pertahanan ganda (*Defense-in-Depth*) dengan stabilitas kecepatan transfer yang tetap terjaga pada angka 25,03 Mbps.

5.2 Saran

Berdasarkan keterbatasan penelitian dan temuan yang diperoleh, penulis mengajukan beberapa saran konstruktif untuk pengembangan penelitian di masa depan:

1. Peningkatan Sumber Daya Komputasi Gateway
   Mengingat penggunaan VPS dengan spesifikasi rendah (1 vCPU) berpotensi menjadi *bottleneck* saat menangani beban enkripsi ganda (*Hybrid*), penelitian selanjutnya disarankan menggunakan spesifikasi VPS yang lebih tinggi (minimal 2 vCPU). Hal ini diperlukan untuk memverifikasi apakah *throughput* enkripsi dapat ditingkatkan secara linear dan untuk mengisolasi variabel pembatas performa antara kapasitas CPU dan *bandwidth* jaringan.

2. Eksplorasi Protokol Transport Modern (HTTP/3)
   Penelitian selanjutnya dapat mengevaluasi penerapan protokol HTTP/3 (QUIC) pada implementasi Nginx Reverse Proxy. Protokol berbasis UDP ini memiliki potensi untuk menggabungkan keunggulan *latency* rendah (seperti WireGuard) dengan keamanan TLS 1.3, sekaligus mengatasi masalah *Head-of-Line Blocking* yang sering terjadi pada implementasi TCP konvensional di jaringan yang tidak stabil.

3. Pengembangan Arsitektur High Availability (HA)
   Untuk memitigasi risiko *Single Point of Failure* (SPOF) pada satu

VPS Gateway, disarankan untuk meneliti implementasi arsitektur *High Availability*. Pengembangan ini dapat melibatkan penggunaan teknik *Load Balancing* atau *DNS Failover* dengan melibatkan dua penyedia layanan VPS yang berbeda (*Multi-Cloud*), guna menjamin ketersediaan layanan (*availability*) yang lebih tinggi.