BAB I
PENDAHULUAN

1.1 Latar Belakang

Pengembangan teknologi informasi dan komunikasi telah secara signifikan meningkatkan kebutuhan akan akses data dan layanan secara fleksibel dan aman, tidak terbatas pada lokasi fisik [1]. Fenomena ini mendorong peningkatan adopsi solusi yang memungkinkan pengguna untuk terhubung ke jaringan pribadi dari jarak jauh, termasuk akses ke sumber daya personal seperti *home server* [2]. Kebutuhan akan kemampuan mengakses data dan aplikasi di *home server* dari luar jaringan lokal semakin umum, baik untuk keperluan kerja jarak jauh maupun pengelolaan data pribadi [3].

Akses jarak jauh yang aman ke jaringan pribadi, *Virtual Private Network (VPN)* adalah solusi yang sudah mapan untuk menciptakan kanal komunikasi yang aman melalui infrastruktur publik seperti internet [4]. Dengan teknik enkripsi dan *tunneling*, *VPN* menjamin kerahasiaan, integritas, dan otentikasi data yang ditransmisikan [5]. Selain *VPN*, *reverse proxy* juga makin populer sebagai lapisan di depan *home server* untuk mengelola koneksi masuk, memberikan fitur keamanan tambahan seperti terminasi *SSL/TLS*, otentikasi, dan *load balancing* [6]. Penggunaan *reverse proxy* juga menyederhanakan akses ke berbagai layanan internal melalui satu titik masuk *public* [7].

Kombinasi penggunaan *VPN* dan *reverse proxy* menimbulkan tantangan kinerja. Mekanisme keamanan yang diterapkan oleh *VPN*, seperti enkripsi dan *tunneling*, secara alami menimbulkan *overhead* pada paket data, yang dapat meningkatkan latensi dan mengurangi *throughput* [8]. Penambahan lapisan *reverse proxy* di atas koneksi *VPN* berpotensi menambah kompleksitas dalam alur data dan memengaruhi kinerja secara keseluruhan [9]. Hal ini terlihat pada peningkatan waktu *response*, peningkatan latensi dalam transmisi data, serta peningkatan konsumsi sumber daya sistem pada perangkat yang terlibat. Setiap protokol *VPN* memiliki karakteristik berbeda dalam efisiensi pemrosesan yang memengaruhi kinerja [10]. Oleh karena itu, evaluasi empiris terhadap kinerja berbagai konfigurasi menjadi krusial untuk mengidentifikasi solusi yang paling

optimal.

Solusi umum mengatasi masalah kinerja potensial melibatkan pemilihan protokol *VPN* yang efisien dan konfigurasi sistem yang tepat. Dua protokol *VPN* yang saat ini banyak digunakan dan diakui karena efisiensi dan keamanannya adalah WireGuard [11] dan OpenVPN [12]. Keduanya menawarkan pendekatan berbeda terhadap *tunneling* dan kriptografi, yang berdampak pada kinerja. Penggunaan *reverse proxy* bersamaan dengan *VPN* merupakan salah satu pendekatan arsitektur yang banyak diimplementasikan untuk meningkatkan keamanan dan fungsionalitas akses *home server* dari jarak jauh [13].

Penelitian ini mengusulkan pendekatan analisis empiris terhadap kinerja konfigurasi akses *home server* menggunakan kombinasi *VPN*, dengan membandingkan protokol WireGuard dan OpenVPN serta penerapan *reverse proxy*. Fokus analisis diarahkan pada parameter utama *Quality of Service* (QoS), yaitu *response time*, *latency*, dan penggunaan sumber daya seperti *CPU* dan *RAM*. Hasil pengujian akan diperoleh melalui serangkaian skrip pengujian terotomatisasi dan divisualisasikan dalam bentuk grafik metrik, sehingga memungkinkan analisis kinerja secara komprehensif dan akurat berdasarkan data yang telah dikumpulkan.

Penelitian ini menyediakan data kuantitatif perbandingan kinerja antara implementasi WireGuard dan OpenVPN ketika digunakan bersama *reverse proxy* pada skenario akses *home server*. Dengan menampilkan hasil pengujian secara terstruktur dan menampilkan metrik kinerja dalam bentuk grafik, penelitian ini memberikan gambaran jelas mengenai dampak *overhead* dan interaksi antar komponen. Hasil penelitian ini akan memberikan panduan yang jelas bagi pengguna dalam memilih arsitektur *VPN* dan protokol yang paling sesuai untuk kebutuhan akses *home server* mereka, mencapai keseimbangan keamanan dan efisiensi. Analisis ini diharapkan dapat membantu mengoptimalkan konfigurasi akses jarak jauh, memastikan pengalaman pengguna yang lebih baik dan pemanfaatan sumber daya sistem yang lebih efisien dibandingkan mengandalkan asumsi teoretis.

1.2 Rumusan Masalah

Berikut rumusan masalah yang diambil dari latar belakang di atas:

1. Bagaimana pengaruh penggunaan *reverse proxy* terhadap kinerja akses *home server* melalui protokol *VPN* WireGuard dan OpenVPN berdasarkan parameter *Quality of Service*, meliputi *response time, latency,* dan penggunaan sumber daya CPU dan RAM?
2. Protokol VPN manakah (WireGuard atau OpenVPN) yang memberikan kinerja optimal untuk implementasi *home server* dengan arsitektur *reverse proxy* berdasarkan parameter *response time, latency,* dan penggunaan CPU dan RAM?
3. Bagaimana perbandingan efisiensi penggunaan sumber daya CPU dan RAM antara implementasi WireGuard dan OpenVPN ketika dikombinasikan dengan *reverse proxy* untuk akses *home server*?

1.3 Tujuan dan Manfaat

Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja protokol WireGuard dan OpenVPN dalam akses *home server* dengan menggunakan *reverse proxy*, khususnya dalam hal *response time*, latensi, serta penggunaan sumber daya *CPU* dan *RAM*. Tujuan utama penelitian adalah mengidentifikasi protokol *VPN* yang memberikan kinerja optimal untuk implementasi *home server* dengan arsitektur *reverse proxy* sebagaimana diuraikan pada Tabel 1.1.

Tabel 1.1 Tabel Keterkaitan Antara Tujuan, Pengujian Dan Kesimpulan

No.	Tujuan	Pengujian	Kesimpulan
1	Menganalisis hasil kinerja *response time* serta *latency* protokol WireGuard dan OpenVPN melalui *reverse proxy*	Pengukuran *response time dengan curl, latency* menggunakan *ping* pada akses ke Pi01 WireGuard dan Pi02 OpenVPN melalui *reverse proxy* VPS01	Penentuan protokol yang memberikan *response time* dan *latency* optimal dalam konfigurasi *reverse proxy*
2	Mengevaluasi	Pemantauan	Identifikasi protokol

	dampak penggunaan WireGuard dan OpenVPN terhadap utilisasi *CPU* dan *RAM*	penggunaan *CPU* dan *RAM* pada VPS01, Pi01, dan Pi02 selama operasional VPN, menggunakan *top* dan *free* sebagai *tools* utama.	dengan *overhead* sumber daya terendah dan analisis dampak *reverse proxy* terhadap beban sistem
3	Menganalisis hasil kinerja akses langsung dengan *reverse proxy* untuk setiap protokol *VPN*	Pengujian komparatif metrik kinerja antara akses langsung dan melalui *reverse proxy* untuk WireGuard dan OpenVPN	Evaluasi *overhead reverse proxy* dan manfaat implementasi arsitektur tersebut untuk *home server*

Berdasarkan Tabel 1.1, penelitian ini dirancang dengan pendekatan sistematis yang menghubungkan tujuan penelitian dengan metode pengujian spesifik untuk menghasilkan kesimpulan yang komprehensif. Setiap tujuan penelitian memiliki metode pengujian yang terukur dan menghasilkan kesimpulan yang dapat diaplikasikan secara praktis dalam implementasi infrastruktur *home server*.

Manfaat dari penelitian ini diharapkan dapat meningkatkan efisiensi implementasi *VPN* untuk *home server* dengan memberikan panduan empiris dalam pemilihan protokol yang sesuai dengan kebutuhan spesifik. Hasil penelitian akan memberikan kontribusi praktis bagi *administrator* sistem dan peneliti di bidang keamanan jaringan dalam mengoptimalkan konfigurasi *VPN* dengan *reverse proxy*. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi untuk pengembangan solusi *home server* yang lebih efisien dan aman.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian hanya membandingkan kinerja WireGuard dan OpenVPN dalam skenario akses *Home Server* melalui *Reverse Proxy Nginx*, tidak mencakup teknologi *VPN* atau skenario lain.

2. Penelitian ini menggunakan VPS dengan kapasitas RAM 4 GB sehingga hasil pengujian dapat terpengaruh oleh keterbatasan memori
3. Pengukuran terbatas pada parameter *QoS* (*Response Time*, *Latency*, penggunaan *CPU* dan *RAM*) dengan simulasi beban terkontrol, tidak menguji kondisi jaringan riil yang dinamis.
4. Implementasi *Reverse Proxy* hanya menggunakan *Nginx* dengan konfigurasi dasar *proxy pass HTTP/HTTPS* tanpa fitur lanjutan seperti *Load Balancing* atau *Caching*.
5. Hasil pengujian bersifat spesifik pada lingkungan *hardware* dan versi *software* yang digunakan, tidak dapat digeneralisasi ke seluruh platform.

1.5 Metode Penelitian

Tahap awal adalah studi literatur, yang berfungsi sebagai fondasi teoretis penelitian. Kajian ini berfokus pada teknologi VPN (dengan penekanan khusus pada WireGuard dan OpenVPN), *reverse proxy*, dan *home server*, serta meninjau penelitian relevan sebelumnya guna mengidentifikasi konsep fundamental dan kesenjangan pengetahuan yang ada.

Tahap selanjutnya melibatkan perancangan dan implementasi. Ini mencakup desain arsitektur jaringan, pemilihan perangkat keras dan perangkat lunak yang sesuai, serta konfigurasi detail pada perangkat, *server*, dan *client* untuk membangun lingkungan pengujian yang terkontrol. Implementasi dilakukan setelah perancangan tuntas, meliputi penyiapan fisik dan logis seluruh komponen sistem, termasuk *home server*, *reverse proxy*, dan konfigurasi *VPN* WireGuard serta OpenVPN pada sisi server dan *client*.

Pembahasan dari penelitian ini terletak pada pengukuran analisis kinerja, di mana data kinerja diimplementasikan secara langsung dari lingkungan. Pengukuran ini mencakup metrik-metrik seperti *response time*, *latency*, *delay*, dan konsumsi sumber daya saat mengakses *home server* melalui *reverse proxy* menggunakan kedua protokol *VPN* tersebut. Data yang terkumpul ini kemudian menjadi basis untuk analisis.

Tahap final adalah analisis data, yang kemungkinan besar menggunakan analisis statistik. Data kinerja hasil pengukuran empiris dianalisis untuk membandingkan performa antara WireGuard dan OpenVPN. Analisis ini

bertujuan mengidentifikasi perbedaan signifikan pada metrik kinerja yang diukur dan menentukan konfigurasi *reverse proxy* yang paling optimal dalam mengakomodasi kedua protokol *VPN* ini. Dengan demikian, penelitian ini mengintegrasikan studi teoritis, perancangan, implementasi, pengukuran pengukuran analisis kinerja, dan analisis data untuk menjawab permasalahan penelitian yang telah dirumuskan.