

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era yang serba digital seperti saat ini jaringan internet merupakan hal yang wajib ada dikarenakan perkembangan teknologi yang sangat pesat kita didorong untuk melakukan segala aktivitas dan kegiatan menggunakan jaringan internet. Menurut survey Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 hingga Kuartal II tahun 2020, jumlah pengguna internet di Indonesia adalah sebanyak 196,7 juta jiwa, setara dengan 73,7% dari populasi penduduk di Indonesia [1]. Keamanan jaringan menjadi salah satu komponen yang harus diperhatikan terlebih banyak sekali ancaman dan serangan yang terjadi di luar sana menurut Lanskap Keamanan Siber Indonesia 2022 Badan Siber dan Sandi Negara (BSSN) pada tahun 2022 ada banyak serangan di internet seperti *Web Defacement*, *ransomware* hingga kebocoran data[2] yang nantinya jika hal itu terjadi akan banyak biaya yang harus dikeluarkan untuk menangani kerusakan yang ditimbulkan. Oleh karena itu, untuk mencegah kerusakan yang disebabkan oleh serangan dari peretas yang saat ini semakin bervariasi, seperti halnya jika suatu jaringan lokal sudah terhubung dengan internet maka peretas akan dengan mudah melakukan serangan pada jaringan tersebut. Untuk itu perlu upaya sejak dini yang harus dilakukan untuk mengurangi berbagai macam ancaman dan serangan yang terjadi pada jaringan internet yang bisa terjadi kapan saja.

Untuk mengurangi ancaman tersebut, ada berbagai macam cara yang dapat digunakan salah satunya adalah membangun sebuah jaringan *VPN (Virtual Private Network)* yang bisa digunakan untuk melakukan pertukaran data di internet dengan lebih aman. Namun dalam hal ini tidak hanya faktor keamanan saja yang harus kita perhatikan, faktor lain seperti performa, *QoS (Quality of Service)*, serta kecepatan akses terhadap layanan server juga perlu menjadi pertimbangan. Dapat kita ketahui bahwa saat ini sudah banyak *VPN (Virtual Private Network)* protokol seperti *PPTP*, *L2TP*, *SSTP*, *OpenVPN*, dan *WireGuard*. Pada penelitian ini akan diambil dua *VPN (Virtual Private Network)* protokol yaitu *OpenVPN* dan *WireGuard* yang merupakan *VPN (Virtual Private Network)* yang cukup populer

dan banyak digunakan serta bersifat terbuka (*Open Source*)[3]. Pengujian ini dilakukan dengan menggunakan parameter *QoS (Quality of Service)* serta menggunakan software benchmark *ab (Apache Bench)* untuk mengetahui performa dalam melakukan akses web server. Penelitian ini akan dilakukan pada sistem operasi *VyOS* dan disimulasikan menggunakan *GNS3 (General Network Simulation 3)*.

Berdasarkan permasalahan diatas, penulis melakukan penelitian dengan judul "Analisis Perbandingan Performa *OpenVPN* dan *WireGuard* sebagai *VPN site-to-site* pada Sistem Operasi *VyOS* menggunakan *GNS3*". Diharapkan pada penelitian ini didapatkan kesimpulan mengenai *VPN (Virtual Private Network)* manakah yang memiliki performa lebih baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan diselesaikan pada penelitian ini antara lain :

1. Bagaimana melakukan analisis perbandingan performa *VPN (Virtual Private Network) Site-to-site OpenVPN* dan *WireGuard* pada Sistem Operasi *VyOS* berdasarkan pengukuran parameter *QoS (Quality of Service)* dalam akses layanan server pada jaringan ?
2. *VPN (Virtual Private Network)* manakah yang memiliki performa lebih baik ?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain :

1. Penelitian ini hanya membahas mengenai *VPN (Virtual Private Network) Site-to-site OpenVPN* dan *WireGuard*.
2. Menggunakan *GNS3 (General Network Simulation 3) versi 2.2.40.1* sebagai simulator jaringan.
3. Sistem Operasi Router yang digunakan adalah *VyOS 1.3 Equuleus*. Sedangkan client & server menggunakan Sistem Operasi *Debian 10 Buster*.

4. Virtual Machine yang digunakan adalah *Oracle VM VirtualBox* versi 7.0.8.
5. Pengujian yang dilakukan pada perbandingan performa *OpenVPN* dan *WireGuard* adalah uji *Throughput, Delay, Jitter, Packet Loss* menggunakan tools *Wireshark* dan *iperf3* , pengujian performa akses layanan *Web Server*, dan pengujian performa dalam melakukan *Download & Upload file* pada *FTP (File Transfer Protocol)*.
6. Menggunakan tools *ab (Apache Bench)* versi 2.3 untuk menguji performa *VPN (Virtual Private Network)* dalam melakukan akses layanan *Web Server*.
7. Menggunakan IP Address v4.
8. Menggunakan *static routing*.
9. Dalam penelitian ini tidak membahas mengenai pengujian keamanan.

1.4 Maksud dan Tujuan Penelitian

1. Analisis perbandingan performa masing-masing *VPN (Virtual Private Network) Site-to-site OpenVPN* dan *Wireguard* pada Sistem Operasi *VyOS* berdasarkan pengukuran parameter *QoS (Quality of Service)* dalam melakukan akses layanan server pada jaringan.
2. Mencari data dari hasil analisis perbandingan performa untuk menentukan manakan *VPN (Virtual Private Network) Site-to-site* yang paling baik untuk digunakan.
3. Sebagai syarat menyelesaikan studi S1.

1.5 Manfaat Penelitian

1. Menambah wawasan dan pengetahuan mengenai Ilmu Komputer terutama pada bidang Jaringan Komputer.
2. Sebagai informasi terkait dengan *VPN (Virtual Private Network) Site-to-site*.

3. Hasil dari penelitian ini dapat menjadi sumber referensi dalam menentukan *VPN (Virtual Private Network) Site-to-site* yang terbaik dalam melakukan pengembangan jaringan.

1.6 Metode Penelitian

Metodologi yang digunakan pada penelitian ini adalah metode penelitian simulasi.

1.6.1 Perancangan

Melakukan perancangan topologi simulasi jaringan *VPN (Virtual Private Network) Site-to-site OpenVPN dan WireGuard* pada jaringan secara virtual menggunakan *GNS3*.

1.6.2 Implementasi

Pada tahap ini dilakukan instalasi semua kebutuhan dalam melakukan penelitian seperti *software* dan sistem operasi yang digunakan serta melakukan konfigurasi *VPN (Virtual Private Network) Site-to-site OpenVPN dan WireGuard*.

1.6.3 Pengujian

Melalui simulasi jaringan yang sudah diterapkan maka pada tahap ini dilakukan pengujian pada *VPN (Virtual Private Network) Site-to-site OpenVPN dan WireGuard* menggunakan parameter *QoS (Quality of Service)* seperti *Delay, Jitter, Packet Loss dan Throughput* jaringan dan *Benchmark* akses layanan *web server* menggunakan *ab (Apache Bench)* serta juga akan dilakukan pengujian performa dalam melakukan proses transfer file pada *FTP (File Transfer Protocol)*.

1.6.4 Analisis

Pada tahap ini dilakukan analisis terhadap hasil pengujian yang sudah dilakukan berupa perbandingan data yang sudah diperoleh untuk mengetahui *VPN (Virtual Private Network)* yang memiliki performa terbaik.

1.7 Sistematika Penulisan

Pada bagian ini dituliskan urutan dan sistematika penulisan penelitian yang dibagi menjadi beberapa bab, yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini memuat tentang Latar Belakang dari permasalahan yang dihadapi, Rumusan Masalah, Batasan Masalah, Maksud dan Tujuan Penelitian, Manfaat Penelitian, Metode Penelitian dan Sistematika Penelitian.

BAB II LANDASAN TEORI

Bab ini berisi tentang Tinjauan Pustaka serta Dasar Teori yang mendasari penelitian dan digunakan untuk mendukung penelitian

BAB III METODE PENELITIAN

Bab ini berisi tentang mengenai gambaran umum penelitian, alat dan bahan penelitian, serta langkah-langkah penelitian yang akan dilakukan.

BAB IV HASIL dan PEMBAHASAN

Bab ini berisis tentang hasil pengujian berupa data yang telah didokumentasikan dengan membuat tabel dan diagram serta akan dilakukan pembahasan dan perbandingan data hasil pengujian performa *OpenVPN* dan *WireGuard VPN(Virtual Private Network)*.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dari penelitian ini dan saran untuk penelitian selanjutnya serta pemaparan sumber-sumber literatur yang digunakan dalam penulisan penelitian ini.