BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Serangan *Denial of Service* (DoS) adalah salah satu bentuk serangan yang sering terjadi pada situs, jaringan, *router*, dan server, termasuk *router* mikrotik. Tujuan dari serangan DoS adalah membuat jaringan *router* menjadi tidak aktif sehingga tidak dapat melayani permintaan dari pengguna yang memiliki hak akses yang sah. Dampak dari serangan ini dapat mengganggu aktivitas operasional organisasi dan menyebabkan kerugian baik dalam bentuk material maupun nonmaterial [1].

Menjaga keamanan hak akses terhadap sumber daya merupakan hal yang sangat krusial. Oleh karena itu, perlu memberikan perhatian lebih pada investasi dalam bidang keamanan guna mencegah pencurian data dan serangan yang sering terjadi. Terutama saat komputer server terhubung dengan internet, risiko serangan menjadi semakin tinggi. Penerapan metode authentikasi perlu digabungkan dengan metode lain di jaringan agar hak akses dapat benar-benar terjamin. Oleh karena itu, diperlukan mekanisme di jaringan yang dapat secara optimal mencegah kemungkinan ancaman, dan salah satu pendekatan yang efektif adalah dengan memanfaatkan *virtual private network* (VPN) [2].

Virtual Private Network (VPN) banyak digunakan perusahaan untuk menghubungkan kantor-kantor cabang ke kantor pusat melalui media internet [3]. Koneksi VPN yang memungkinkan untuk menghubungkan dua Jaringan Area Lokal (LAN) disebut dengan VPN *site-to-site* [4]. VPN *site-to-site* merupakan bentuk jaringan VPN yang berfungsi untuk menghubungkan dua atau lebih jaringan lokal yang terpisah secara geografis, sehingga memungkinkan mereka untuk berkomunikasi dengan aman melalui internet. Beberapa protokol yang sering digunakan saat ini adalah IPsec, OpenVPN dan yang terbaru adalah WireGuard. WireGuard adalah *Virtual Private Network* (VPN) gratis dan *open source* yang bertujuan untuk menggantikan IPsec dan OpenVPN [5]. Dibandingkan dengan IPSec, WireGuard lebih sederhana dan lugas, serta tidak rentan terhadap kegagalan

dan kesalahan konfigurasi. Sedangkan jika dibandingkan dengan OpenVPN, WireGuard dirancang dengan desain yang lebih sederhana dan mengurangi kompleksitas dengan meminimalkan fitur yang tidak diperlukan [6].

Dibandingkan dengan protocol lain di atas, WireGuard memiliki kelebihan dalam menangani serangan DDoS Analisis keamanan akan mengevaluasi sejauh mana WireGuard mampu melindungi jaringan dari serangan DDoS dan bagaimana itu memenuhi standar keamanan industri. Analisis performansi akan mengukur seberapa cepat dan efisien protokol ini dalam mentransfer data antara jaringan yang terhubung. Dengan mempertimbangkan faktor-faktor seperti keamanan, kinerja, dan kemudahan penggunaan, organisasi dapat membuat keputusan yang terinformasi tentang apakah protokol WireGuard adalah pilihan terbaik untuk kebutuhan jaringan mereka dalam upaya pencegahan serangan DDoS. Atas dasar latar belakang di atas, penulis melakukan penelitian dengan judul ”**Analisis Keamanan dan Performansi Jaringan VPN *Site-to-Site* Menggunakan Protokol WireGuard dalam Menangani Serangan DDoS**”.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah :

1) Bagaimana cara mengimplementasikan VPN *site-to-site* menggunakan protokol WireGuard untuk menangani serangan DDoS?
2) Bagaimana tingkat keamanan VPN *site-to-site* menggunakan protokol WireGuard dalam menangani serangan DDoS?
3) Bagaimana performa jaringan VPN *site-to-site* menggunakan protokol WireGuard saat terkena serangan DDoS?

1.3 BATASAN MASALAH

Batasan masalah dalam penelitian dan pengembangan tugas akhir ini adalah:

1) *Tunneling protocol* yang digunakan adalah WireGuard.
2) Serangan yang digunakan untuk menguji keamanan adalah DDoS TCP syn *Flooding*.

3) Pengujian dilakukan pada *webserver* lokal.
4) Pengujian menggunakan jaringan lokal laboratorium FTTE Institut Teknologi Telkom Purwokerto
5) Performansi diukur menggunakan parameter meliputi ketersediaan, *delay, Throughput,* dan *packet loss.*
6) Aplikasi yang digunakan untuk mengukur performansi adalah Wireshark.

1.4 TUJUAN

Tujuan dari penelitian tugas akhir ini adalah:

1) Merancang implementasi VPN *site-to-site* menggunakan protokol WireGuard untuk menangani serangan DDoS.
2) Menganalisis keamanan jaringan VPN *site-to-site* menggunakan protokol WireGuard berdasarkan parameter ketersediaan.
3) Menganalisis performa jaringan VPN *site-to-site* menggunakan protokol WireGuard berdasarkan parameter *throughput*, *delay*, dan *packet loss*

1.5 MANFAAT

Penelitian ini memiliki manfaat diantara lain dalam konteks jaringan VPN site-to-site, penting untuk memahami kelebihan dan kekurangan yang terkait dengan penggunaan protokol WireGuard. Selain itu, panduan instalasi dan konfigurasi WireGuard perlu disediakan kepada pengguna agar mereka dapat melaksanakannya dengan tepat dan efisien. Selanjutnya, pertimbangan terhadap tingkat keamanan WireGuard dalam menghadapi serangan DDoS juga perlu dievaluasi untuk memastikan kehandalan sistem.

1.6 SISTEMATIKA PENULISAN

Penelitian ini memiliki beberapa bagian. Sistematika penulisan penelitian ini didasarkan pada pengelompokan pokok-pokok pikiran yang dibagi menjadi beberapa bab. Bab 1 akan mengulas latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Bab 2 akan menggambarkan landasan teori yang digunakan sebagai acuan penulis

dalam menyusun penelitian. Selain itu, diuraikan juga referensi-referensi relevan yang berkaitan dengan pembahasan masalah dalam skripsi ini. Bab 3 akan membahas alat-alat yang digunakan dalam penelitian, alur penelitian, perancangan sistem, perancangan *end device*, dan pengujian sistem yang dilakukan selama penelitian. Bab 4 akan menjelaskan hasil pengujian keamanan dan performansi implementasi VPN *site-to-site* menggunakan protokol WireGuard, serta menyajikan analisis yang mendukung hipotesis penelitian dan hasil implementasi pengujian VPN dengan protokol WireGuard. Bab 5 berisi kesimpulan dan hasil dari analisis dan implementasi VPN menggunakan protokol WireGuard, serta memberikan saran untuk pengembangan jaringan *private* antar cabang di masa depan bagi peneliti lain.