BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong penggunaan *Virtual Private Server* (VPS) secara luas untuk memenuhi berbagai kebutuhan seperti hosting aplikasi, situs web, dan penyimpanan data. VPS menjadi pilihan dominan karena keunggulannya dalam hal fleksibilitas, efisiensi biaya, dan kinerja yang dapat diakses secara remote melalui jaringan internet [1]. Namun, penggunaan VPS yang diakses melalui jaringan publik meningkatkan risiko keamanan, terutama terhadap serangan siber seperti *Distributed Denial of Service* (DDoS) yang semakin marak terjadi. Studi terbaru menunjukkan bahwa VPS yang terekspos secara publik sering menjadi target serangan otomatis yang mencoba mengeksploitasi kerentanan layanan, termasuk serangan *password guessing* dan *flooding* yang dapat menyebabkan *downtime* dan gangguan layanan [2],[3]. Oleh karena itu, diperlukan solusi keamanan yang efektif untuk mengamankan akses VPS dari ancaman tersebut.

Aksesibilitas jaringan publik pada *Virtual Private Server* (VPS), meskipun menawarkan kemudahan, membuka celah terhadap ancaman keamanan seperti penyadapan data dan eksploitasi server [3]. Ancaman-ancaman ini menjadi perhatian utama terutama bagi organisasi yang menangani informasi sensitif [2]. Sebagai solusi, *Virtual Private Network* (VPN) sering diimplementasikan, namun VPN konvensional memiliki keterbatasan seperti konfigurasi kompleks, kinerja jaringan yang suboptimal, dan kebutuhan akan perangkat keras tambahan seperti *firewall* khusus [4]. Keterbatasan ini memotivasi pencarian solusi yang lebih efisien dan terintegrasi untuk mengamankan akses VPS.

Dalam menghadapi tantangan keamanan akses VPS melalui jaringan publik, teknologi *Tailscale* yang berbasis protokol *WireGuard* menawarkan solusi inovatif dengan pendekatan *zero-trust networking*. Pendekatan ini memungkinkan pembangunan jaringan privat yang efisien tanpa memerlukan konfigurasi rumit, sehingga memudahkan pengelolaan dan pengamanan VPS. Dengan enkripsi ujung-

ke-ujung yang kuat dan autentikasi perangkat yang ketat, *Tailscale* membatasi akses hanya pada perangkat yang terverifikasi, sehingga mengurangi risiko serangan siber, termasuk serangan *Distributed Denial of Service* (DDoS). Selain itu, arsitektur *peer-to-peer* yang digunakan *Tailscale* memungkinkan koneksi langsung antar perangkat tanpa eksposur layanan ke jaringan publik, meningkatkan privasi dan keamanan secara signifikan. Menurut [5] menunjukkan bahwa *WireGuard* sebagai protokol dasar *Tailscale* memiliki performa tinggi dengan latensi rendah dan keamanan kriptografi yang kuat, menjadikannya solusi ideal untuk pengamanan jaringan modern termasuk VPS .

Keunggulan lain dari *Tailscale* terletak pada kemampuannya mendukung pengelolaan jaringan terdistribusi secara efisien, yang sangat penting dalam era cloud computing saat ini. Kebutuhan akan akses aman lintas perangkat dan platform menjadi prioritas utama bagi organisasi yang mengelola infrastruktur IT modern. *Tailscale* menyediakan dukungan *multi-platform* yang luas, mencakup sistem operasi Windows, Linux, macOS, bahkan perangkat *mobile* seperti iOS dan Android, sehingga memungkinkan integrasi yang mudah dan konsisten di berbagai lingkungan kerja. Selain itu, performa jaringan *Tailscale* unggul berkat implementasi protokol *WireGuard* yang telah terbukti memiliki latensi rendah dan *throughput* tinggi dibandingkan dengan VPN tradisional seperti *Open*VPN dan IPsec.

Penelitian ini bertujuan untuk mengeksplorasi implementasi *Tailscale* dalam mengamankan akses *Virtual Private Server* (VPS) melalui konversi jaringan publik ke *private*. Tujuan dari penelitian ini adalah mengevaluasi dampak teknologi *Tailscale* terhadap peningkatan keamanan. Proses yang dilakukan adalah dengan memblokir akses masuk yang bersifat publik dan hanya diizinkan akses masuk tertentu menggunakan VPN berdasarkan pengujian serangan dengan DDOS. Tahapan penelitian yang dilakukan meliputi proses implementasi VPS, konfigurasi VPS dan pengujian *Tailscale*. Selanjutnya, dilakukan pengujian keamanan pada server yang telah diinstal dengan *Tailscale*. Harapan dari penelitian ini dapat memberikan kontribusi signifikan dalam pengembangan solusi keamanan VPS.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah seperti di 1.1, maka rumusan masalah dari penelitian ini, yaitu :

1. Apakah implementasi *Tailscale* dapat mengamankan akses *Virtual Private Server* (VPS) melalui konversi jaringan publik ke jaringan privat?
2. Apakah peningkatan keamanan VPS dengan *Tailscale* terbukti dapat mencegah serangan *Distributed Denial of Service* (DDoS)?

1.3 Batasan Masalah

Batasan masalah penelitian ini, yaitu:

1. Lingkungan pengujian terbatas pada jaringan lokal:

   Seluruh simulasi dilakukan pada jaringan lokal menggunakan *Windows Subsystem for Linux (WSL)* dan *laptop*

2. Jumlah perangkat dibatasi:

   Penelitian hanya menggunakan 2 perangkat utama, yaitu:

   a. VPS Ubuntu 20.04 LTS (sebagai server)
   b. Laptop windows sebagai klien + WSL Ubuntu 20.04

3. Simulasi serangan DdoS dalam sekala ringan:

   Pengujian dilakukan dalam jaringan lokal yang sama dan terbatas pada penggunaan *tools* HPING3 untuk menghindari dampak buruk.

4. Fokus implementasi menggunakan *Tailscale* VPN.

1.4 Tujuan Penelitian

1. Menganalisis implementasi *Tailscale* dalam mengamankan akses *Virtual Private Server* (VPS) melalui konversi jaringan publik menjadi jaringan privat.
2. Mengevaluasi efektivitas *Tailscale* dalam meningkatkan keamanan akses VPS terhadap ancaman seperti serangan *Distributed Denial of Service* (DDoS).

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang keamanan jaringan, khususnya dalam memahami implementasi teknologi *Tailscale* untuk mengamankan akses *Virtual Private Server* (VPS) melalui pendekatan *zero-trust* networking. Penelitian ini juga akan menyediakan panduan praktis untuk meningkatkan keamanan akses VPS dari ancaman siber seperti DDoS, serta membantu organisasi dalam mengelola jaringan privat.

1.6 Sistematika Penulisan

Berikut sistematika penulisan agar pembaca lebih mudah memahami islaporan penelitian :

BAB I PENDAHULUAN

Pada Bab 1 membahas tentang isi dan rencana dalam pengerjaan skripsi terkait latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan

BAB II TINJAUAN PUSTAKA

Pada Bab 2 membahas tentang kajian tinjauan pustaka yang mencangkup studi literatur, table aslian dan dasar teori. Hal ini bersumber dari jurnal atau referensi yang berkaitan dengan penelitian ini.

BAB III METODE PENELITIAN

Pada Bab 3 membahas tentang metode penelitian yang digunakan mencangkup objek penelitian, alur penelitian, serta alat dan bahan yang akan digunakan.

BAB IV HASIL DAN PEMBAHASAN

Pada Bab 4 membahas tentang implementasi hasil dan juga pembahasan pada perancangan penelitian.

BAB V PENUTUP

Pada Bab 5 membahas tentang kesimpulan dan saran yang didapatkan dari hasil penelitian.