BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang sudah dilakukan, berikut ini merupakan kesimpulan dari hasil penelitian:

1. Implementasi *Tailscale* pada Virtual Private Server (VPS) terbukti efektif dalam mengamankan akses dengan mengubah koneksi dari jaringan publik ke jaringan privat. Sebelum implementasi, VPS memiliki banyak port terbuka dan dapat diakses secara publik, meningkatkan potensi serangan siber. Setelah Tailscale diaktifkan, seluruh koneksi dialihkan ke jaringan privat terenkripsi melalui skema IP privat milik Tailscale (misalnya 100.99.144.54), sementara akses langsung ke IP publik seperti 103.127.137.72 berhasil diblokir. Dengan demikian, hanya perangkat yang terautentikasi di dalam organisasi Tailscale yang bisa mengakses VPS, yang secara signifikan meningkatkan lapisan keamanan akses.
2. Tailscale terbukti mampu meningkatkan keamanan VPS terhadap serangan Distributed Denial of Service (DDoS). Simulasi serangan menggunakan *tools hping3* menunjukkan bahwa *kombinasi Tailscale dan firewall UFW* berhasil memblokir seluruh trafik berbahaya dari jaringan publik. Hasil pengujian juga didukung oleh log firewall, yang menunjukkan bahwa paket-paket serangan tidak berhasil mencapai layanan utama VPS. Hal ini menunjukkan bahwa integrasi Tailscale memberikan peningkatan proteksi nyata terhadap ancaman DDoS.

5.2 Saran

Adapun saran yang dapat diberikan untuk penelitian lebih lanjut adalah:

1. *Tailscale* layak diterapkan dalam lingkungan produksi sebagai solusi VPN yang ringan dan efisien, terutama bagi organisasi yang memerlukan komunikasi internal yang aman tanpa kompleksitas konfigurasi. Penggunaannya sangat relevan untuk infrastruktur *cloud* maupun *hybrid*.
2. Pengujian lanjutan disarankan mencakup jenis serangan lain di luar TCP SYN, seperti UDP *flood*, DNS *amplification*, dan serangan pada *application layer*, guna mengevaluasi ketahanan sistem secara lebih komprehensif.