BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan *Extended Access Control List* (ACL) sebagai *Policy Enforcement Point* (PEP) dalam kerangka *Zero Trust Architecture* (ZTA) terbukti efektif dalam meningkatkan keamanan internal jaringan. Implementasi ini berhasil merealisasikan prinsip utama *Zero Trust*, yaitu *Verify Explicitly* dan *Least Privilege*, melalui mekanisme inspeksi paket yang dilakukan secara eksplisit pada setiap lalu lintas antar-segmen jaringan.

Hasil pengujian menunjukkan bahwa *Extended* ACL mampu menerapkan kontrol akses secara granular, tidak hanya berdasarkan alamat IP sumber dan tujuan, tetapi juga dengan memvalidasi jenis protokol dan port layanan. Mekanisme ini terbukti efektif dalam membatasi akses tidak sah, seperti pemblokiran protokol ICMP untuk mencegah aktivitas pemindaian jaringan (*network scanning*), sekaligus tetap mengizinkan akses layanan bisnis yang sah seperti HTTP. Dengan demikian, risiko pergerakan lateral (*lateral movement*) antar VLAN dapat diminimalkan secara signifikan.

Perbandingan antara mekanisme keamanan menunjukkan bahwa *Standard* ACL memiliki keterbatasan dalam konteks *Zero Trust* karena hanya mampu melakukan pemfilteran berbasis IP sumber, sehingga tidak cukup mendukung penerapan prinsip least privilege. Sebaliknya, *Extended* ACL memberikan fleksibilitas dan presisi kebijakan yang dibutuhkan dalam arsitektur *Zero Trust*, khususnya dalam penerapan *micro-segmentation* dan isolasi trafik antar zona keamanan. Oleh karena itu, *Extended* ACL dinilai lebih relevan dan efektif untuk diterapkan sebagai mekanisme pengendalian akses pada jaringan perusahaan yang menuntut tingkat keamanan internal yang tinggi.

5.2 Saran

Penelitian ini masih memiliki beberapa keterbatasan yang dapat menjadi peluang pengembangan pada studi selanjutnya. Salah satu keterbatasan utama adalah penggunaan Cisco Packet Tracer sebagai media simulasi, yang memiliki

batasan dalam merepresentasikan kompleksitas kebijakan keamanan tingkat lanjut. Penelitian mendatang disarankan untuk menggunakan emulator jaringan yang lebih realistis seperti GNS3 atau EVE-NG, maupun perangkat jaringan fisik, agar implementasi *Zero Trust* dapat diuji pada lingkungan yang lebih mendekati kondisi nyata.

Selain itu, pengembangan mekanisme kontrol akses dapat diarahkan pada penerapan kebijakan yang lebih adaptif, seperti *Reflexive* ACL *atau Zone-Based Firewall* (ZBF), guna meningkatkan kemampuan sistem dalam menangani sesi koneksi dinamis serta trafik balik (*return traffic*). Integrasi mekanisme autentikasi dan otorisasi berbasis identitas pengguna juga dapat dipertimbangkan untuk memperkuat prinsip *Never Trust, Always Verify* dalam *Zero Trust Architecture*.

Penelitian selanjutnya juga disarankan untuk memperluas cakupan implementasi *Zero Trust* dengan membandingkan efektivitas ACL berbasis IPv4 dan IPv6, mengingat meningkatnya adopsi IPv6 pada infrastruktur jaringan modern. Studi tersebut diharapkan dapat memberikan wawasan tambahan mengenai penerapan kontrol akses granular dalam berbagai skema pengalamatan jaringan.