BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan rangkaian tahapan penelitian mulai dari analisis kebutuhan, perancangan, implementasi, hingga pengujian, dapat ditarik kesimpulan bahwa penerapan metode *Port Knocking* yang dipadukan dengan *Access Control List* (ACL) pada perangkat MikroTik hAP lite RB941-2nD mampu memberikan peningkatan signifikan terhadap keamanan dan segmentasi jaringan di lingkungan Kantor Pengadilan Agama Rantauprapat.

Metode *Port Knocking* berperan efektif sebagai lapisan autentikasi awal yang menyembunyikan *port-port* manajemen dari akses langsung pihak yang tidak berwenang. Hal ini berhasil mengurangi potensi serangan seperti *port scanning* dan *brute force* karena *port* hanya akan terbuka ketika urutan "ketukan" yang benar dilakukan.

Sementara itu, ACL menjadi lapisan verifikasi lanjutan yang membatasi akses berdasarkan parameter identitas perangkat, seperti alamat IP dan MAC *Address*. Kombinasi kedua teknik ini menciptakan sistem keamanan berlapis yang tidak hanya mencegah akses dari pihak eksternal yang tidak dikenal, tetapi juga meminimalkan risiko penyalahgunaan dari pihak internal.

Hasil pengujian menunjukkan bahwa konfigurasi yang diimplementasikan dapat berjalan sesuai rancangan, memberikan kemudahan bagi administrator dalam melakukan manajemen akses, serta meningkatkan efisiensi penggunaan sumber daya jaringan melalui segmentasi yang lebih terstruktur. Dengan demikian, sistem yang dikembangkan dapat dijadikan solusi praktis sekaligus efektif untuk pengamanan jaringan di lingkungan instansi dengan tingkat risiko keamanan yang tinggi.

5.2 Saran

Untuk mendukung keberlanjutan dan optimalisasi sistem yang telah dibangun, maka disampaikan beberapa rekomendasi :

1. Pemeliharaan dan pembaruan berkala

Perangkat MikroTik dan seluruh sistem pendukungnya perlu diperbarui secara rutin guna menutup potensi celah keamanan yang muncul akibat perkembangan ancaman siber.

2. Dokumentasi konfigurasi

   Seluruh proses dan aturan konfigurasi hendaknya terdokumentasi secara sistematis. Dokumentasi ini akan memudahkan proses *troubleshooting,* migrasi sistem, atau pelatihan bagi administrator baru.

3. Pelatihan dan peningkatan kompetensi

   Administrator jaringan disarankan untuk mengikuti pelatihan teknis secara berkala, khususnya yang berkaitan dengan penerapan *multi-layer security*, sehingga mampu melakukan penyesuaian ketika terjadi perubahan kebutuhan atau kondisi jaringan.

4. Integrasi metode keamanan tambahan

   Untuk meningkatkan ketahanan sistem terhadap serangan yang lebih kompleks, penelitian selanjutnya dapat mengintegrasikan teknik keamanan lain, seperti penggunaan *Virtual Private Network* (VPN), *Intrusion Detection System* (IDS), atau kebijakan firewall berbasis perilaku *(behavior-based filtering).*

5. Monitoring dan evaluasi berkelanjutan

   Sistem keamanan yang diterapkan perlu dipantau secara *real-time* dengan memanfaatkan fitur *logging* dan analisis lalu lintas jaringan. Evaluasi berkala akan membantu mengidentifikasi kelemahan yang mungkin tidak terdeteksi pada tahap awal penerapan.

Dengan penerapan saran-saran tersebut, diharapkan sistem keamanan berbasis *Port Knocking* dan ACL ini tidak hanya efektif pada saat implementasi awal, tetapi juga mampu beradaptasi terhadap perkembangan teknologi dan ancaman siber di masa mendatang.