

BAB V

KESIMPULAN DAN SARAN

A. KESIMPULAN

Penelitian yang dilaksanakan di PKBM Al Suroya Metro Timur dari tanggal 20 Oktober hingga 20 Desember 2023 menggunakan metode NDLC (*Network Development Life Cycle*), dengan pengujian langsung pada mikrotik yang terhubung dengan server PKBM Al Suroya Metro Timur. Penelitian ini berhasil mencapai tujuannya, yaitu mengimplementasikan sistem autentikasi dan pengamanan berbasis *captive portal* pada jaringan *wireless* di PKBM Al Suroya Metro Timur. Berdasarkan hasil pengujian *Black Box Testing* dan uji kelayakan yang dilakukan bersama admin jaringan dan pendamping instansi menunjukkan bahwa *captive portal* berhasil mengatasi masalah yang ada pada PKBM dan setiap pengguna yang terhubung dengan jaringan yang tersedia diharuskan *login* terlebih dulu dengan *username* dan *password* yang telah disediakan.

Beberapa kelebihan yang ada pada implementasi sistem autentikasi dan pengamanan berbasis *captive portal* di PKBM Al Suroya Metro Timur adalah sebagai berikut:

1. Sistem keamanan jaringan yang dibuat memberikan *page login* terlebih dahulu dan melakukan autentikasi berupa *captive portal* sebelum mengakses jaringan. Sistem ini memberikan solusi pada kendala yang sedang dihadapi yaitu masih menggunakan *password* yang sama untuk semua penggunanya, sehingga keamanan jaringan masih rentan dibobol atau diketahui oleh pihak yang tidak berwenang yang ikut mengakses jaringan.
2. Penelitian ini menghasilkan perancangan jaringan yang didalamnya terdapat manajemen *bandwidth* sehingga setiap *username* memiliki kecepatannya masing-masing, ini berguna untuk memastikan bahwa semua pengguna dapat memiliki akses internet yang stabil.

B. SARAN

Sistem yang diterapkan oleh penulis tentunya belum sempurna dan masih memiliki kekurangan. Dengan penerapan sistem autentikasi dan pengamanan berbasis *captive portal* pada jaringan *wireless* di PKBM Al Suroya Metro Timur

diharapkan dapat membantu admin jaringan dalam proses pengelolaan dan perawatan jaringan internet pada PKBM Al Suroya Metro Timur.

Penulis berharap sistem autentikasi dan pengamanan pada jaringan *wireless* berbasis *captive portal* yang telah diterapkan dapat lebih disempurnakan pada penelitian yang akan datang dengan menambahkan fitur keamanan jaringan lainnya, diantaranya sebagai berikut:

1. Penambahan filtering akses pada jaringan *wireless* sehingga jaringan hanya dapat digunakan pada kebutuhan yang memang diperlukan.
2. Penambahan fitur penggunaan *MAC Address* sebagai akses *login user* sehingga pengguna jaringan akan lebih mudah di kontrol.