

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian terapan yang telah dilakukan pada *router mikrotik* dengan pendalaman tentang pemanfaatan *firewall* dalam keamanan jaringan pada *mikrotik* dapat disimpulkan dalam poin sebagai berikut:

1. Pada penelitian jaringan *hotspot* dengan menggunakan *wifi* di Kedai Khab Khun Kafe, ditemukan beberapa tahapan instalasi dan setelah didukung dengan pengembangan dari mengelola kuota data sampai pengamanan jaringan dengan pengelolaan sistem pengaturan pada kuota dan waktu. Tahapan-tahapan pada konfigurasi harus dilakukan dengan teliti untuk mendapatkan performa dan kualitas yang kita inginkan. Dengan pengembangan model PPDIIOO sangat membantu dalam pengelolaan jaringan dalam hal kuota untuk menyeimbangkan pengeluaran dan kepuasan *user* dalam memakai fasilitas *wifi*.
2. Dengan memahami *mikrotik* dan penggunaannya dalam sistem keamanan jaringan bisa mengontrol aktivitas pengguna jaringan dengan maksimal dan juga dengan memanfaatkan *mikrotik router* bisa melihat *traffic* data yang dipakai *user* serta *statistic*. Pada fitur *firewall* yang di dalamnya ada beberapa fitur pembantu seperti *filter rule*, *NAT*, *mangle*, *connection*, *service port*, *layer 7 protocol*,

sangat membantu untuk mengatur keamanan jaringan. Dengan adanya fitur di atas serta memaksimalkan fungsinya bisa melakukan pemblokiran terhadap suatu *website* yang tidak aman untuk diakses, baik blok melalui *content*, *IP address* dengan batuan fitur dalam *firewall*.

5.2 Saran

Dari kesimpulan di atas penulis memberikan beberapa hal terkait dengan tambahan sebagai saran sebagai berikut:

1. Sebaiknya menggunakan PC dengan spesifikasi baik dan RAM yang besar serta melengkapi perangkat keras secara komplit dan menginstall semua perangkat lunak untuk peranan yang maksimal saat setup dan konfigurasi. Sebaiknya sebelum setup harus mempelajari teknik-teknik dan langkah-langkah setup dan konfigurasi dengan banyak referensi baik pustaka ataupun observasi di lapangan langsung.
2. Membeli *router* atau *accesspoint* yang kapasitasnya lebih dari 300 Mbps untuk dapat mengcover lebih dari 20 *user* dalam satu *router* ataupun *accesspoint*.
3. Melakukan pemeriksaan terhadap performa *Router* dan melakukan *restart* secara rutin dan terjadwal;
4. Selalu teliti dalam melakukan blok via *address* karena ada beberapa *website* yang mempunyai *address* lebih dari satu jadi harus diblok semuanya agar tidak lolos akses.