BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil Penelitian yang dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut :

1. Penggunaan PC routerPfsense 2.3.2 lebih mudah dalam melakukan penyetingan dan konfigurasinya serta lebih menghemat pengeluaran karena dapat diperoleh secara gratis.
2. Terbentuknya pengamanan *wireless* hotspot dengan sistem otentikasi *Captive portal* menggunakan pfsense, sehingga user diwajibkan untuk melakukan login dengan menggunakan *username* dan *password* yang telah dibuat terlebih dahulu oleh admin.
3. SSL yang dibuat di *internal certificate* manager PfSense berfungsi sebagai enkripsi pada protocol HTTPS *Captive Portal*. Dari hasil pengujian pengamanan mengguakan sartifikat SSL pada *Captive portal* dapat menahan dari ancaman *spoffing username* dan *password*.
4. Implementasi kemanan Snort IDS *Intrusion Detection System* di PfSense, rules yang dibuat dapat mendeteksi serangan DOS *(Denial Of Service)* pada *TCP flooding* dan *UDP flooding* yang hanya menghasilkan *alert* jika terjadi serangan oleh *attacker*.
5. Dengan menerapkan *Traffic Shaper* per IP metode ini dapat mengatasi pemakaian limit *bandwidth* sehingga saat *download* tidak menghabiskan *bandwidth* mengganggu user yang menggunakan hotspot.

5.2 Saran

Berdasarkan kesimpulan yang telah dibuat, ada beberapa saran untuk pengembangan sistem selanjutnya :

1. Penerapan *Captive portal* dengan local user management menjadi salah satu kesulitan tersendiri bagi seorang sistem administrator dikarenakan

seorang admin harus memasukan dan membuat *username* serta *password* satu persatu terhadap user yang ingin menggunakan fasilitas captive portal. Penggunaan radius server bisa menjadi solusi untuk menggantikan otentikasi dengan local user management karena tidak perlu mendaftarkan *username* serta *password* satu persatu.

2. Dalam penerapan ssl dan sertifikat yang dibuat di PfSense masih diperlukan pemasangan sertifikat terhadap user. Maka dari itu perlunya SSL bersifat public artinya domain dengan SSL yang telah di hosting. Kemudian penggunaan proxy salah satu alternatif untuk usermempermudah melakukan proses pemasangan sertifikat tersebut.
3. Implementasi pembatasan *bandwidth* secara keseluruhan mempengaruhi kualitas dari kecepatan internet dari ISP, dikarenakan hanya membatasi keseluruhan user secara merata. Dan tidak membatasi 1 IP ataupun mac address sehingga semua koneksi baik itu upload maupun *download* akan sama. Maka dari itu penggunaan traffic shaping dan limiter dengan queue bisa menjadi solusi untuk menyempurnakan sistem manajemen *bandwidth* untuk user pengguna hotspot.
4. Penerapan mekanisme keamanan IDS pada PfSense seharusnya bisa dikembangkan menjadi IPS karena IPS bisa memblokir aktivitas *attacker* yang ingin menyalahgunakan layanan *Captive portal* tersebut.