

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Pada bab ini akan membahas kesimpulan apa saja yang diperoleh dalam pengerjaan Tugas Akhir ini. Berikut ini hasil kesimpulan pada implementasi IDPS Suricata pada PfSense.

- a. Suricata mampu mendeteksi seluruh lalu lintas yang mengalir pada jaringan WiFi secara *real time*. Suricata mendeteksi serangan dengan cara memasukkan *alert* pada sistem Suricata.
- b. Suricata dapat berjalan dengan mode IDS maupun IDPS/ IPS pada jaringan WiFi. Jika ingin menjalankan pada mode IDPS.
- c. Suricata memiliki tingkat akurasi pendeteksian yang sangat baik. Selain itu suricata juga dapat berjalan pada seluruh cpu yang ada pada device.

5.2. Saran

Karena IDPS Suricata harus bekerja secara *real time* dan dalam waktu yang lama, maka dibutuhkan seorang administrator untuk mengawasi dan menjalankan IDPS Suricata. Saran untuk penelitian kedepannya yaitu membuat IDPS Suricata dapat digunakan untuk melakukan pengawasan dan pendeteksian secara maksimal meskipun administrator tidak berada ditempat. Cara untuk

melakukan hal tersebut yaitu dengan cara Suricata dapat diremote melalui jarak jauh dengan koneksi internet. Meskipun administrator tidak berada ditempat, tetapi administrator mampu mendeteksi serangan melalui remote jarak jauh.