BAB V
PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat diberikan peneliti sebagai berikut:

1. Dengan diterapkannya inspeksi data secara mendalam dan akses kontrol, layanan *DHCP Server* sudah lebih aman dibanding sebelumnya, terutama untuk mencegah dan mengatasi salah satu serangan *DDoS* yaitu serangan *DHCP Starvation*. Hal tersebut dibuktikan oleh berberapa hasil di bab pengujian. Pengujian tersebut meliputi kondisi saat *CPU Load*, *packet data* dan *DHCP Leases* saat sebelum diterapkan DPI dan Sesudah DPI diterapkan. DPI mampu menurunkan menurunkan *Load CPU* dari 13% ke kondisi normal nya yaitu 2% dalam waktu 16 menit, paket data yang masuk saat serangan mampu diturunkan dari kondisi maksimum yaitu 14Mbps hingga ke kondisi normal yaitu 0,5Mbps dalam waktu 10 menit dan membuang packet data *DHCP Discover* yang datang dari serangan *DHCP Starvation* yang mengakibatkan menghabiskan ketersediaan *IP Address* di *DHCP Leases*.
2. Diterapkannya berberapa model keamanan di *firewall* seperti Access Control List terhadap pengguna sah yang dapat mengakses *DHCP Server* di *Bridge Filtering* untuk keamanan *layer 2* dan Deep Packet Inspection di *firewall* untuk keamanan *layer 3*. Deep Packet Inspection dapat diterapkan di fitur *mangle* dan *filter rules*. *Mangle* berfungsi untuk merubah nilai *DSCP* dari 0 ke 56 dan menandai paket data yang masuk melalui interfaces *bridge server, bridge laboratorium* dan *bridge Wi-Fi* serta *filter rules* membuat aturan hanya user yang memiliki nilai *DSCP* 56 yang dapat mengakses layanan *DHCP Server* dengan sepuluh *packet data* dalam waktu satu jam.
3. *DHCP Server* dapat beroperasi lebih aman sesudah diterapkannya Deep Packet Inspection dan Access Control List, dikarenakan dua model keamanan tersebut sudah dapat mencegah dan mengatasi serangan *DHCP Starvation* yang menyebabkan ketersediaan *IP Address* yang disediakan *DHCP Server* dapat habis dikarenakan serangan tersebut.

5.2 Saran

Saran yang dapat diberikan peneliti sebagai berikut:

1. Menambahkan parameter *IP Address* yang akan diterapkan di Access Control List maupun Deep Packet Inspection untuk penelitian selanjutnya, agar lebih mudah dalam mendeteksi serangan *DDoS*, termasuk *DHCP Starvation*.
2. Alat untuk kebutuhan layanan *firewall* dapat diganti dengan alat *firewall* yang lain, seperti pfsense, fortinet, palo alto dan lain-lain. Agar kinerja dari *firewall* lebih optimal dan dapat mencegah dan mengatasi serangan *DDoS* yang lain.
3. Menambahkan sensor untuk deteksi serangan *DDoS* selain fitur *logging* yang ada di mikrotik, seperti contohnya *Bot Gateway*. Agar sistem deteksi yang diterapkan lebih optimal.