BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penjelasan dan pembahasan yang telah diuraikan pada bab-bab sebelumnya hingga tahap implementasi dan analisis hasil, maka peneliti dapat mengambil kesimpulan sebagai berikut :

1. Proses perancangan dengan *filter rule* maka ketika terdapat paket new yang tidak wajar akan dilakukan grouping menggunakan *address list* dengan nama "DNS *Flood*", setelah alamat IP penyerang dan alamat IP tujuan berhasil ditangkap menggunakan *address-list* maka alamat IP tersebut akan di drop oleh *firewall filter* yang kita buat di awal tadi. Dengan begitu perangkat router mikrotik dapat terhindar dari serangan UDP DNS *Flood* oleh orang yang tidak dikenal. Begitu juga dengan penyerangan *brute force* .
2. Hasil dari masing-masing metode sudah jelas. Bahwa menggunakan metode *filter firewall* berhasil dapat menangkap IP penyerang yang masuk ke *address-list* dan dapat memblokirnya. Dengan adanya metode *filter firewall* ancaman serangan *flooding* dapat diminimalisir.

5.2 Saran

Berdasarkan penelitian yang dilakukan oleh peneliti, beberapa saran yang dapat dilakukan untuk pengembangan penelitian selanjutnya adalah sebagai berikut:

1. Penelitian ini dapat dikembangkan dengan untuk mencegah serangan DDoS yang lain seperti SYN-*Flooding*, SMURF *Attack*, ICMP-*Flooding* dan juga dapat dikembangkan dengan menggunakan algoritma lain untuk mencegah serangan DDoS.