

ABSTRAK

Keamanan pada jaringan data sangatlah dibutuhkan. Suatu *server* pengguna membutuhkan keamanan pada trafik jaringannya agar *server* tersebut tidak mengalami gangguan yang dapat memberi efek negatif pada penggunanya. Pengguna dapat mengatasi permasalahan tersebut dengan menggunakan sebuah *router* yang dapat di kendalikan ataupun sebuah *router* yang dapat di perintah sesuai apa yang terjadi.

Iptables adalah suatu *tools* dalam system operasi *linux* yang berfungsi sebagai alat untuk melakukan penyaringan terhadap trafik data pada jaringan. *Iptables* dapat menjadi solusi untuk membantu *server* dalam mengatur data yang masuk melalui jaringan *server/host*. *Socket* adalah mekanisme komunikasi yang memungkinkan terjadinya pertukaran data antar program dalam satu mesin maupun antar mesin. *Socket* sendiri dapat menjadi solusi untuk mengirimkan sebuah perintah ke *router* untuk membantu *server*, jika terdapat sebuah kejanggalan dalam suatu trafik jaringan. *Router* membutuhkan sebuah program yang dapat menerima sebuah perintah dan dapat menjalankan perintah apa yang seharusnya dilakukan secara *real-time*, sehingga *server* tidak langsung terbebani dengan adanya serangan.

Tugas Akhir ini difokuskan pada pembuatan sebuah program *host-based firewall* yang diletakkan dalam sisi *server* atau pengguna dan *router* yang dapat mengirimkan data secara *one point to multiple points* dengan menggunakan *socket* sebagai metode pengirimannya dan menggunakan *iptables* sebagai pengatur lalulintas jaringan data dan eksekutor terhadap penyerang.

Kata kunci : Keamanan jaringan, *Iptables* , *Socket*, Pengiriman data *real-time*, *host-based firewall*.