

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Banyak cara agar sebuah komputer dapat lebih dimaksimalkan dalam penggunaannya. Membuat jaringan/menghubungkan antar dua komputer atau lebih merupakan salah satu contohnya. Dengan adanya jaringan tersebut informasi dapat ditangani dengan cepat dalam pengelolaannya sehingga tidak hanya dibutuhkan pihak *internal*, tetapi juga pihak-pihak *eksternal*. Semakin berkembangnya jaringan komputer ini melahirkan sebuah istilah *internet*.

*Internet* merupakan salah satu sarana dalam menyampaikan informasi yang dibutuhkan tanpa hambatan ruang dan waktu. Internet bukan lagi sesuatu yang mewah tetapi menjadi komponen dasar baik bagi perorangan maupun bisnis. Ketika melakukan koneksi komputer ke *internet* akan didapati beberapa masalah yang berhubungan keamanan. Masalah-masalah tersebut antara lain keamanan data dan keamanan komputer itu sendiri. Perpindahan data melalui koneksi *internet* tersebut dapat membuka kesempatan kepada orang lain untuk mengintip atau mengubah data melalui upaya-upaya penyusupan dan beberapa tindakan lain yang dapat merusak seperti serangan virus. Untuk saat ini saja sistem-sistem komputer tidak menjamin 100% data yang ada benar benar aman, sehingga perlu adanya usaha yang dapat meminimalkan gangguan-gangguan tersebut.

Banyak cara yang digunakan untuk melakukan pengamanan terhadap web server, database server, atau sumber informasi lain yang terhubung ke *internet* dari gangguan-gangguan tersebut. Salah satu contohnya adalah *firewall*. Sebuah *firewall* pada jaringan dapat melindungi baik user ataupun data yang terdapat pada jaringan lokal dari pengaksesan yang tidak diinginkan dari jaringan luar. Secara konstan *firewall* mengawasi seluruh aliran yang masuk dan keluar ke koneksi anda, menunggu aliran yang ada untuk dihentikan atau ditolak berdasarkan aturan yang sudah ada. *Firewall* dapat berbentuk *hardware*/fisik maupun *software*. Saat ini terdapat banyak perangkat keras atau hardware yang dapat membentengi atau sebagai *firewall* sistem seperti contoh *cisco*, *sonicwall* dan nokia yang

menyertakan perangkat lunak tertentu untuk melakukan konfigurasi *firewall*. Namun perangkat tersebut harganya cukup mahal. Begitu juga yang bersifat software yang tinggal ditambahkan pada sebuah server atau komputer lain yang dikonfigurasi menjadi *firewall* seperti checkpoint, McAfee dan Symantech.

Namun ada juga yang menyediakan aplikasi *firewall* secara gratis. *Freebsd* sebagai salah satu sistem operasi *open source* menyediakan aplikasi *firewall* yang bersifat gratis. Aplikasi yang dibutuhkan *freebsd* agar dapat bertindak sebagai *firewall*.

Persoalan mengenai maraknya pornografi ataupun penipuan online telah menjadi ancaman yang serius di dunia maya. Dan bahkan, hal tersebut mampu merambah zona aman pada internet tanpa ketahuan. Tentunya, keamanan pada jaringan komputer harus lebih ditingkatkan demi mengantisipasi hal serupa terjadi. Salah satu upaya untuk meningkatkan keamanan pada jaringan komputer yaitu memanfaatkan *firewall*.

Oleh karena itu perancangan konfigurasi sistem berbasis *firewall* sebagai upaya melakukan pencegahan akses tak senonoh itu terjadi. Karena *firewall* merupakan alat untuk mengimplementasikan kebijakan security (*security policy*). Sedangkan kebijakan *security*, dibuat berdasarkan pertimbangan antara fasilitas yang disediakan dengan implikasi *security*-nya. Semakin ketat kebijakan *security*, semakin kompleks pula konfigurasi layanan informasi dan semakin sedikit juga fasilitas yang tersedia di jaringan komputer. Salah satu sistem operasi yang ada sistem *firewall*nya adalah *FreeBSD*. *FreeBSD* adalah *UNIX-like operating system* (sistem operasi seperti UNIX), sangat banyak digunakan dalam dunia ISP (*Internet service provider*), *embedded devices*, serta bidang lain yang membutuhkan reliability tinggi.

Untuk perancangan konfigurasi ini, penulis mengambil studi penelitian di Jurusan Teknik Komputer Politeknik Negeri Sriwijaya. Dimana, pokok permasalahan yang terjadi yaitu kurangnya proteksi pada jaringan lokal, sehingga menyebabkan akses *website* tak senonoh pun bisa sewaktu waktu terjadi.

Dengan latar belakang tersebut, maka dapat diambil judul “***Rancang Bangun Konfigurasi Firewall Untuk Membatasi Akses Website Menggunakan FreeBSD***”.

### **1.2. Rumusan Masalah**

Berdasarkan latar belakang di atas maka penulis merumuskan masalah, yaitu kurangnya proteksi pada jaringan lokal sehingga memungkinkan website tak layak akses bisa masuk ke dalam sistem. Sehingga dibutuhkanlah konfigurasi sistem berbasis *firewall* untuk mengatasi masalah tersebut.

### **1.3. Tujuan**

Berdasarkan latar belakang di atas, maka tujuan yang ingin dicapai dari penulisan laporan akhir ini adalah untuk membatasi akses *website* yang tak wajar menggunakan *FreeBSD*.

### **1.4. Manfaat**

Adapun manfaat dari penulisan Laporan Akhir ini adalah:

1. *Firewall* bermanfaat sebagai filter yang digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan. Sehingga akses ke *website* yang tak layak akses dapat ditanggulangi.
2. Fungsi Aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik.