

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi yang berkembang pesat saat ini sudah merupakan suatu hal yang pokok dan menjadi keharusan bagi perusahaan-perusahaan yang maju dan berkembang. Yang paling utama dari masalah tersebut adalah persaingan dengan perusahaan lain, yang menuntut cepatnya penyampaian informasi dan pengolahan data yang cepat dan akurat. Internet merupakan sebuah teknologi informasi yang mendukung masalah tersebut, berbagai aktifitas yang bisa dilakukan dengan cepat dan mudah hanya dengan mengakses internet di suatu perusahaan maupun akses secara intranet. Web browser untuk mencari informasi, email untuk mengirim data atau informasi yang lain, ftp untuk saling bertukar data antar karyawan maupun dengan orang lain.

Dari berbagai manfaat yang bisa dilakukan, terdapat pula kendala atau masalah yang dihadapi perusahaan maupun perseorangan dalam resource sharing, penggunaan file, program dan hardware secara bersama-sama dapat dimanfaatkan oleh orang lain yang tidak berhak. Akses secara ilegal yang dilakukan dari luar maupun dari dalam perusahaan dapat menimbulkan suatu masalah yang serius apabila tidak ditangani atau setidaknya dicegah oleh administrator sistem.

Suatu mekanisme pengamanan yang bisa dilakukan untuk membatasi akses ilegal adalah membuat kebijakan atau policy yang mengatur perbedaan dan hal-hal yang bisa dilakukan oleh seseorang dalam perusahaan. Keamanan yang bersifat

intranet maupun internet menjadi suatu keharusan untuk diperhatikan, karena jaringan komputer yang bersifat publik pada dasarnya tidak aman, data yang di sharing atau akses data yang tidak menggunakan sistem keamanan memungkinkan bagi orang lain yang tidak berhak dapat membaca atau bahkan merubah isi dari data tersebut.

Adalah tugas dari seorang administrator jaringan dalam mengamankan dan melindungi jaringan yang mereka kelola, walaupun dengan teknologi yang canggih atau peralatan terkini, sebuah jaringan tidak bisa dikatakan sepenuhnya aman. Sebab sebuah serangan tidak hanya dilakukan dari luar jaringan tetapi juga dari dalam jaringan, hal inilah yang harus diperhatikan oleh seorang administrator dalam mengelola dan membuat kebijakan atau policy yang mengatur user dalam mengakses jaringan.

Internet firewall dengan segala kelebihan dan kekurangannya merupakan suatu mekanisme pengamanan yang paling banyak dipakai saat ini. Firewall merupakan sebuah tembok yang membatasi akses suatu sistem jaringan yang ada dibalikinya dari berbagai macam ancaman dan gangguan dari luar maupun dari dalam sistem jaringan intranet. Fungsinya bisa sebagai pembatas antara hak akses dan mengatur policy antara jaringan internal dan external dalam hal ini akses internet dan intranet. Hal ini sangat penting karena tidak semua orang diperbolehkan untuk bisa mengakses kedalam jaringan yang kita miliki. Konfigurasi dari sistem pengamanan firewall bergantung kepada kebijaksanaan dari organisasi yang bersangkutan.

Pada perusahaan yang besar dan kompleks, biasanya seorang administrator jaringan mengelola lebih dari satu mesin server. Ini dikarenakan setiap layanan yang ada membutuhkan sebuah mesin server yang handal dan mampu menangani tugas secara simultan. sebagai contoh untuk mail menggunakan mail server yang terpisah dengan server untuk data maupun server untuk firewall.

Faktor keterbatasan dalam administrasi server yang dilakukan seorang admin secara langsung tersebut berdampak bagi administrator dalam mengelola server. Jika seorang administrator memiliki tanggung jawab untuk mengatur beberapa server yang berada pada ruang dan lantai yang berbeda, maka akan menyulitkan bila aktifitas tersebut dilakukan secara langsung pada sistem.

Sistem firewall yang sudah dibangun pun membutuhkan monitoring maupun konfigurasi ulang tergantung dari kebijakan yang berlaku. Hal inilah yang mungkin sedikit menyulitkan administrator jaringan dalam mengelola jaringan mereka. Karena sangat penting untuk menerapkan sistem keamanan atau aturan aturan baru yang sudah ditetapkan. Penanganan secara remote memungkinkan konfigurasi secara cepat dapat dilakukan tanpa harus dilakukan secara langsung pada server tersebut. Pada aplikasi webmin yang berbasis web, konfigurasi pada beberapa server dapat dilakukan hanya menggunakan computer client yang mempunyai akses terhadap server. Walaupun berbasis web based administration, webmin tidak menggunakan port 80 (default:10000) dan juga memungkinkan penambahan beberapa modul tambahan untuk keamanan dalam mengakses dan mengkonfigurasi server firewall.

Dari latar belakang masalah yang ada maka penulis mengambil judul “**Sistem Administrasi Firewall Secara Remote Untuk Keamanan Jaringan Pada Server Berbasis Linux Menggunakan Webmin “**

1.2 Rumusan Masalah

Adapun rumusan masalah dari latar belakang yang ada adalah membangun sebuah server firewall yang handal secara remote menggunakan webmin sebagai aplikasi pendukung untuk konfigurasi dan monitoring sistem, pengamanan jaringan menggunakan firewall dapat dilakukan secara local maupun remote. Konfigurasi yang dilakukan oleh seorang administrator jaringan akan lebih mudah apabila akses ke server firewall dilakukan secara remote, karena tidak harus dilakukan secara lokal maka konfigurasi kebijakan atau policy keamanan jaringan akan lebih cepat terkontrol.

1.3 Batasan Masalah

Batasan masalah dimaksudnya untuk lebih mengarahkan penulis dalam pembahasan skripsi ini lebih jelas dan terarah. Dan lebih mengarahkan penulis dalam meneliti dan menentukan metode yang tepat dan cepat dalam menentukan tercapainya penelian yang penulis lakukan. Adapun batasan batasan yang penulis lakukan meliputi :

1. Konfigurasi IPTables sebagai aplikasi firewall
2. Konfigurasi webmin yang digunakan untuk interface konfigurasi maupun monitoring terhadap system

3. Beberapa pengujian firewall pada sistem antara lain:
 - Pengujian firewall sebagai paket filtering
 - pengujian direktori log untuk memantau aktivitas
4. Pengujian firewall yang dilakukan secara local

1.4 Maksud dan Tujuan

Adapun maksud dan tujuan diadakan penelitian ini adalah :

Tujuan secara khusus :

1. Penelitian ini dibuat sebagai syarat kelengkapan akademik untuk memperoleh gelar sarjana S1 pada STMIK AMIKOM YOGYAKARTA

Tujuan secara umum :

1. Installasi dan konfigurasi IPTables sebagai aplikasi firewall yang dilakukan pada distro fedora 7
2. Membangun sebuah sistem firewall yang handal
3. Konfigurasi dan monitoring firewall yang dilakukan secara remote menggunakan webmin
4. Pembatasan akses akses yang dilakukan user agar sesuai dengan hak akses yang dimiliki.
5. Membatasi akses antara jaringan lokal dengan jaringan internet.

1.5 Metode Penelitian

Metode yang penulis lakukan bertujuan agar hasil dari penelitian dan analisis dapat lebih terarah dan data yang diperoleh lebih akurat. Kelengkapan

data yang diperoleh dapat memberikan kontribusi pada penulis dalam menyusun skripsi ini dan memberikan waktu yang lebih singkat. Adapun beberapa metode metode yang penulis lakukan dalam pengumpulan data terdiri dari metode sebagai berikut :

1. Metode Observasi (*Observation*)

Pengamatan secara langsung mengenai objek yang akan dilakukan penelitian. Meliputi Installasi, konfigurasi, tools yang dipakai dan pengujian koneksi terhadap internet.

2. Metode Wawancara (*Interview*)

Metode ini dilakukan penulis dengan mengajukan pertanyaan pertanyaan seputar objek atau yang berkenaan dengan objek penelitian. Teknik wawancara dilakukan dengan bimbingan teknisi yang bersangkutan.

3. Metode Kepustakaan (*Library*)

Penulis mengumpulkan data data melalui buku, jurnal maupun makalah yang ada diinternet. Referensi melalui buku banyak memberikan kontribusi yang besar pada penulis dalam menyusun laporan ini.

4. Metode Kearsipan (*Documentation*)

Penyusun melakukan pengumpulan data dengan cara membaca dan mempelajari data-data arsip yang sudah ada yang berhubungan dengan permasalahan yang diteliti.

1.6 Sistematika Penulisan

Sistematika penulisan yang disusun oleh penulis akan memuat uraian secara garis besar isi dari skripsi per bab, yaitu sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini penulisan mencakup latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini penulis menguraikan tentang kajian pustaka yang mendasari penulis melakukan penelitian ini. Dan juga berisi tentang konsep dasar sistem, keamanan jaringan dan firewall.

BAB III METODOLOGI PENELITIAN

Membahas tentang point – point dari penelitian yang penulis lakukan. Mencakup subjek penelitian, alat penelitian, dan konsep rancangan sistem.

BAB IV ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini menjelaskan tentang proses analisis kebutuhan sistem dan perancangan sistem.

BAB V HASIL DAN PEMBAHASAN

Membahas tentang hasil dari perancangan sistem yang telah dilakukan dan pembahasannya. Mencakup hasil yang ditemui pada penelitian, pengujian pengujian yang

dilakukan pada konfigurasi firewall yang telah diterapkan dan dampak yang terjadi pada sistem maupun komputer client.

BAB VI PENUTUP

Menguraikan kesimpulan dari penelitian dan memberikan saran untuk penelitian selanjutnya.

1.7 Jadwal Kegiatan Penelitian

Untuk memperlancar kegiatan penelitian ini agar dapat terencana dan tepat waktu, maka penulis membuat suatu rencana atau jadwal kegiatan agar mencapai target yang ditentukan. Adapun tahapan rencana kegiatan diuraikan sebagai berikut :

Tabel 1.1 Jadwal kegiatan

| No | Rincian Tahap Kerja | Bulan | | | | | | | | | | | |
|----|--------------------------------------|-------|---|---|---|-------|---|---|---|-----|---|---|---|
| | | Maret | | | | April | | | | Mei | | | |
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Pengajuan Proposal | | | | | | | | | | | | |
| 2 | Persiapan dan Pengumpulan data | | | | | | | | | | | | |
| 3 | Analisa masalah | | | | | | | | | | | | |
| 4 | Perancangan sistem | | | | | | | | | | | | |
| 5 | Pengujian dan pengamanan firewall | | | | | | | | | | | | |
| 6 | Pembuatan Laporan | | | | | | | | | | | | |