BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam beberapa tahun belakangan ini, sistem keamanan komputer telah menjadi fokus utama dalam dunia Jaringan Komputer. Keamanan komputer merupakan salah satu kunci yang dapat mempengaruhi tingkat *Reliability* yang di dalamnya termasuk *Performance* dan *Availibility* suatu Internetwork.

Saat ini telah banyak perusahaan yang mengeluarkan banyak biaya demi mengamankan sistemnya agar terhindar dari serangan *malware* jahat, *virus*, *hacker*, dan hal yang tidak diinginkan lainnya yang dapat berdampak pada terganggunya kinerja perusahaan mereka. Hal ini diperburuk dengan masih dipergunakannya *firewall* tunggal untuk mengamankan jaringan sebesar perusahaan, padahal untuk mengamankan jaringan di era ini sudah sangat diperlukan *multi firewall* yang bekerja secara *redundant* serta ditambahkan *dengan Intrusion Prevention System (IPS).*

IPS sendiri merupakan teknologi terbaru hasil dari pengembangan dari *Intrusion Detection System* (*IDS*). *IPS* merupakan jenis metode pengamanan jaringan yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk mencegah aktivitas tersebut. Sebagai pengembangan dari teknologi *firewall,* IPS melakukan pengendali dari suatu system berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *ports* atau *IP address* seperti *firewall* umumnya.

Selain itu *IPS* dapat menghasilkan *packet loss* yang bernilai 0% walau server dalam keadaan diserang, dan ketika server *IPS down* karena diserang sejumlah *client* penyerang dengan besaran paket tertentu, dengan bantuan *redundant firewall* akan berpindah secara otomatis dari *server master* ke *server slave* agar kerusakan dapat diminimalisir dengan segera.

1.2. Rumusan Masalah

Secara garis besar pokok permasalahan yang dibahas dalam tugas akhir ini meliputi:

- Pemodelan sistem *Failover Firewall* yang digunakan pada sistem *Redundant Firewall IPS*.
- Pemodelan sistem *Security* yang digunakan untuk menyerang sistem *Redundant Firewall IPS*.
- Menganalisa hasil implementasi yang telah dilakukan dengan pengukuran parameter performansi: f*ailover time* dan parameter *security* yang diujikan terhadap sistem *Redundant Firewall* tersebut.
- Menganalisa performansi jaringan pada saat sistem dilakukan pengujian
- Bagaimana mekanisme penyerangan terhadap sistem *redundant firewall IPS* untuk menguji karakteristik sistem.
- Bagaimana mekanisme pemblokiran serangan terhadap sistem *redundant firewall IPS* untuk menguji karakteristik sistem.
- Jumlah maksimal user yang bisa dilayani oleh sebuah single *firewall* dibandingkan dengan sistem *redundant firewall IPS*.

1.3. Batasan Masalah

Pembuatan sistem clustering yang diteliti pada tugas akhir ini dibatasi oleh beberapa hal sebagai berikut:

1. Sistem *Redundant Firewall* hanya menggunakan sistem *Failover Firewall*.
2. Server yang digunakan *operating system Ubuntu.*
3. Sistem yang dibangun menggunakan IPS (*Intrusion Prevention System*) sebagai sistem pemblokiran serangan.
4. Sistem diuji kemampuannya untuk mencegah serangan *DDoS* menggunakan program *TFN* serta digunakan pula *IPS* untuk memblok paket yang tidak diinginkan.

1.4. Tujuan dan Kegunaan

Hasil yang diharapkan dari penelitian ini antara lain sebagai berikut:

1. Memahami prinsip kerja suatu sistem *redundant firewall* menggunakan metode *failover firewall* , mulai saat sistem bekerja secara normal hingga sistem mengalami *failover* disebabkan karena kelemahan sistem.
2. Mengimplementasikan sistem *redundant firewall* dengan menggunakan metode *IPS*.
3. Mengetahui karakteristik dari metode IPS.

1.5. Metode Penelitian

Untuk melakukan kajian perancangan dalam permasalahan tersebut, metodologi penelitian yang diambil meliputi :

1. Studi literatur dan kepustakaan, yaitu mempelajari teori pendukung tentang sistem *redundant firewall,* dan metode keamanan jaringan.
2. Implementasi, yaitu mengimplementasikan rancangan yang telah dibuat dengan parameter yang telah ditentukan.
3. Analisa kinerja sistem dengan mengamati dan mengevaluasi data hasil tes performansi.

1.6. Sistematika Penulisan

Adapun sistematika penulisan pada Tugas Akhir ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, batasan masalah, tujuan, metodologi penelitian serta sistematika penulisan.

BAB II Dasar Sistem *Redundant Firewall*

Bab ini berisi deskripsi teori dasar mengenai sistem *redundant firewall dan Intrusion Prevention System*.

BAB III Implementasi Sistem *Redundant Firewall*

Bab ini akan dibahas proses perancangan dan implementasi sistem *redundant firewall IPS*, serta skenario pengujian terhadap sistem *redundant firewall IPS.*

BAB IV Analisa Implementasi Sistem *Redundant Firewall*

Bab ini akan membahas analisis dan evaluasi dari kinerja sistem *redundant firewall IPS* tersebut terhadap skenario parameter pengujian yang diberikan.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan dan saran dari Tugas Akhir terhadap untuk pengembangan lebih lanjut.