

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Internet merupakan hal yang vital bagi masyarakat saat ini, terutama masyarakat yang bergelut dengan teknologi informasi. Dengan adanya internet, komunikasi baik yang jarak jauh maupun dekat dapat dilakukan hanya dengan suatu perangkat yang mendukung jaringan internet. Selain melakukan komunikasi, informasi juga mudah didapat dengan mengandalkan teknologi ini. Dengan kemudahan ini, tidak jarang beberapa pengguna menyalahgunakan teknologi internet dengan berbagai hal. Seperti mengakses situs - situs yang berbau pornografi, melakukan kejahatan di dunia maya (*cybercrime*), bahkan melakukan serangan terhadap informasi – informasi yang sudah ada seperti penyerangan *database*, *web*, dan data – data penting lainnya.

Untuk menghindari dampak negatif tersebut, diperlukan perlindungan terhadap jaringan komputer agar pengguna tidak menyalahgunakan dan merasa aman pada jaringan yang dimilikinya. *Firewall* merupakan fitur keamanan pada jaringan komputer yang dapat mengatur masuk keluarnya paket data. Pada jaringan yang sederhana, *firewall* biasanya hanya diimplementasikan pada komputer yang bersangkutan. Padahal belum tentu *firewall* pada komputer mampu memproteksi keamanan paket data yang diakses oleh penggunanya.

Oleh karena itu, sebaiknya dipersiapkan suatu *firewall* yang mampu memproteksi pengguna dari akses internal maupun eksternal. Smoothwall Express merupakan sistem operasi berbasis Linux yang memiliki fitur *firewall* yang mampu membatasi akses yang masuk maupun keluar pada suatu jaringan. Smoothwall Express memiliki fitur *web filtering* dan memiliki IDS yang terintegrasi langsung pada sistem operasinya. Dengan demikian penulis akan mengangkat judul Implementasi *Firewall* dan IDS pada Smoothwall Express. Implementasi ini rencananya akan digunakan pada jaringan yang memiliki topologi satu *firewall* dan satu DMZ, dengan pengujian

URL filter, pembatasan waktu akses dan menampilkan hasil *log* dari serangan DDoS, *sniffing*, *port scanning*.

1.2 Rumusan Masalah

Adapun rumusan masalah dari proyek akhir ini diantaranya :

1. Bagaimana konfigurasi *firewall* pada sistem operasi Smoothwall Express ?
2. Bagaimana cara mendeteksi ancaman DDoS, *sniffing* dan *port scanning* yang terjadi pada jaringan tersambung dengan sistem operasi Smoothwall Express?
3. Bagaimana cara melakukan integrasi antara sistem operasi Smoothwall Express dengan IDS ?

1.3 Tujuan

Berdasarkan rumusan masalah diatas, maka tujuan dari proyek akhir ini adalah :

1. Dapat melakukan konfigurasi *firewall* pada sistem operasi Smoothwall Express.
2. Dapat mendeteksi ancaman DDoS, *sniffing* dan *port scanning* pada jaringan yang tersambung dengan sistem operasi Smoothwall Express.
3. Dapat melakukan integrasi sistem operasi Smoothwall Express dengan IDS.

1.4 Batasan Masalah

Batasan masalah pada proyek akhir ini diantaranya :

1. Sistem operasi yang digunakan untuk implementasi *firewall* dan IDS adalah Smoothwall Express versi 3.1.

2. Konfigurasi *firewall* yang dilakukan mencakup *url filter* dan pembatasan waktu akses.
3. Deteksi ancaman menggunakan fitur Snort yang ada pada sistem operasi ini.
4. Ancaman yang diuji berupa DDOS, *Sniffing*, dan *port scanning*.
5. Jenis serangan DDOS berupa ICMP *flooding*.
6. Simulasi yang dilakukan menggunakan bantuan aplikasi VM VirtualBox.
7. Tidak membahas tentang serangan *malware* maupun *virus*.
8. Dikerjakan pada topologi satu *firewall* dan satu DMZ.
9. *Web server* yang ada hanya digunakan untuk proses pencarian *username* dan *password* untuk simulasi serangan *sniffing*.
10. Tidak membahas pencegahan serangan *sniffing*.

1.5 Definisi Operasional

Firewall [1] adalah suatu aturan yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan melakukan filterisasi, membatasi ataupun menolak suatu koneksi pada jaringan yang dilindunginya dengan jaringan luar lainnya seperti internet.

Intrusion detection system (IDS) [2] adalah suatu teknik atau metode yang digunakan untuk mendeteksi ancaman yang mencurigakan pada jaringan. IDS memiliki dua kategori dasar yaitu *signature-based* dan *anomaly detection system*.

Sistem Operasi [3] merupakan program yang mampu mengontrol eksekusi program – program aplikasi dan berfungsi sebagai *interface* antara *user* dengan *hardware*.

Smoothwall [4] merupakan suatu distro Linux yang dirancang untuk digunakan sebagai *firewall*. Smoothwall dikonfigurasi melalui GUI berbasis *web*. Sistem operasi ini fokus pada konten *web filtering*.

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan adalah studi literatur, analisis, perancangan, implementasi, pengujian dan penyusunan laporan.

1. Studi Literatur

Mempelajari teori yang berkaitan dengan proyek akhir seperti *firewall*, dan IDS.

2. Analisis Kebutuhan Sistem

Langkah ini digunakan untuk mengetahui kebutuhan perangkat baik *hardware* maupun *software* yang akan digunakan.

3. Perancangan Model

Langkah ini bertujuan untuk merancang topologi jaringan yang akan digunakan.

4. Implementasi

Implementasi memuat semua hal mengenai instalasi maupun konfigurasi yang dibutuhkan.

5. Pengujian

Pengujian dilakukan setelah sistem sudah berjalan dengan baik, yaitu berupa simulasi *web filtering*, pembatasan waktu akses situs dan pencegahan serangan (DDOS, *sniffing*, dan *port scanning*) kemudian menganalisa hasilnya.

6. Penyusunan Laporan

Pada langkah ini semua metode yang telah dilakukan dan data yang telah terkumpul dibuat dokumentasi berupa laporan proyek akhir.

1.7 Jadwal Pengerjaan

Adapun jadwal pengerjaan dari proyek akhir dilakukan dari bulan Januari sampai dengan Juni 2015 yaitu sebagai berikut :

Tabel 1-1 Jadwal pengerjaan proyek akhir

No.	Tahap pekerjaan	Jadwal Pelaksanaan																							
		Jan				Feb				Mar				April				Mei				Juni			
		4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
1	Studi Literatur	■	■																						
2	Analisis Kebutuhan Sistem			■	■	■																			
3	Perancangan Model					■	■																		
4	Implementasi							■	■	■	■	■	■	■	■	■	■	■	■	■					
5	Pengujian																			■	■	■	■	■	
6	Penyusunan Laporan	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	