

Daftar Isi

Lembar Pengesahan.....	i
Lembar Pernyataan Orisinalitas.....	ii
Abstrak.....	iii
Abstract.....	iv
Kata Pengantar.....	v
Daftar Isi.....	vii
Daftar Gambar.....	x
Daftar Tabel.....	xiii
Daftar Singkatan.....	xiv
Daftar Istilah.....	xv
Bab I Pendahuluan.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	1
1.3 Tujuan.....	2
1.4 Batasan Masalah.....	2
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	3
Bab II Dasar Teori.....	5
2.1 <i>Intrusion Prevention System</i>	5
2.1.1 Pengertian <i>Intrusion Prevention System</i>	5
2.1.2 Jenis-jenis <i>Intrusion Prevention System</i>	5
2.1.2.1 <i>Host-based Intrusion Prevention System</i>	5
2.1.2.2 <i>Network-based Intrusion Prevention System</i>	6
2.1.3 Jenis-jenis <i>Intrusion Prevention System Open Source</i>	6
2.1.3.1 <i>PortsEntry</i>	6
2.1.3.2 <i>Sshdfilter</i>	6
2.1.3.3 <i>Snort</i>	6
2.1.4 Sistem Kerja <i>Intrusion Prevention System</i>	7
2.1.4.1 <i>Signature-based Detection</i>	7
2.1.4.2 <i>Statistical Anomaly-based Detection</i>	7
2.1.4.3 <i>Stateful Protocol Analys Detection</i>	7

2.1.5	Teknik Mencegah Serangan.....	8
2.2	<i>Captive Portal</i>	8
2.2.1	Pengertian <i>Captive Portal</i>	8
2.2.2	Cara Kerja <i>Captive Portal</i>	9
2.2.3	Teknik Implementasi <i>Captive Portal</i>	9
2.2.3.1	<i>Redirection by HTTP</i>	9
2.2.3.2	<i>IP Redirect</i>	10
2.2.3.3	<i>Redirection by DNS</i>	10
2.3	<i>Load Balancing</i>	10
2.3.1	Definisi <i>Load Balancing</i>	10
2.3.2	Kegunaan <i>Load Balancing</i> dalam Dunia Telekomunikasi.....	11
Bab III Perancangan Sistem.....		12
3.1	Alur Perancangan Tugas Akhir.....	12
3.2	Perancangan dan Konfigurasi Sistem.....	13
3.3	Tahap Analisis.....	14
3.4	Komponen Spesifikasi Sistem.....	15
3.4.1	Komponen Perangkat Keras.....	15
3.4.2	Komponen Perangkat Lunak.....	16
3.5	Skenario Pengujian.....	16
3.5.1	Skenario Pengujian <i>Intrusion Prevention System</i>	17
3.5.2	Skenario Pengujian Autentikasi.....	17
3.5.3	Parameter Pengujian.....	18
3.5.3.1	Kondisi Jaringan.....	18
3.5.3.2	Jumlah Serangan.....	18
3.5.3.3	<i>Continuity Time</i>	18
Bab IV Pengujian dan Analisis.....		19
4.1	Skenario Pengujian Autentikasi.....	19
4.1.1	Pengujian dan Analisa Proses Autentikasi.....	19
4.1.2	Pengujian dengan <i>Port Scanning</i> dan <i>DoS</i>	25
4.1.2.1	Pengujian <i>Captive Portal</i> dengan <i>Port Scanning</i>	25
4.1.2.2	Pengujian <i>Captive Portal</i> dengan <i>DoS</i>	32
4.2	Skenario Pengujian <i>Intrusion Prevention System</i>	35
4.2.1	Pengujian dengan <i>Port Scanning</i>	35
4.2.2	Pengujian dengan <i>Denial of Service</i>	46
4.2.3	Pengujian dengan <i>Distributed Denial of Service</i>	49
4.2.3.1	<i>DDoS</i> dari 1 Komputer Penyerang.....	49
4.2.3.2	<i>DDoS</i> dari 2 Komputer Penyerang.....	51
4.2.3.3	<i>DDoS</i> dari 3 Komputer Penyerang.....	53

4.2.3.4 <i>DDoS</i> dari 4 Komputer Penyerang.....	53
4.3 Perhitungan <i>Throughput</i> pada Jaringan.....	56

Bab V Kesimpulan dan Saran..... 58

5.1 Kesimpulan.....	58
5.2 Saran.....	59

Daftar Pustaka..... 61

Lampiran A

Lampiran B