

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Rumusan Penelitian	3
1.3. Pertanyaan Penelitian	4
1.4. Batasan Masalah	4
1.5. Tujuan Penelitian	4
1.6. Manfaat Penelitian	5
BAB II	6
TINJAUAN PUSTAKA DAN LANDASAN TEORI	6
2.1 Tinjauan Pustaka	6
2.2 Landasan Teori	13
2.2.1 <i>Software Defined Network (SDN)</i>	13
2.2.2 <i>Intrusion Detection Prevention System (IDPS)</i>	14
2.2.3 <i>Serangan Distributed Denial of Service (DDoS)</i>	17
2.2.4 <i>Wireshark</i>	18
2.2.5 <i>OpenDayLight</i>	19
2.2.6 <i>OpenFlow</i>	20
2.2.7 <i>Suricata</i>	21
2.2.8 <i>Teknik Analisis Network</i>	22
2.2.9 <i>Parameter QoS (Quality of Service)</i>	26
BAB III	29
METODOLOGI PENELITIAN	29
3.1 Subjek dan Objek Penelitian	29
3.2 Alat dan Bahan Penelitian	29
3.3 Proses Penelitian	31
3.3.1 Identifikasi Masalah	32
3.3.2 Studi Literatur	32

3.3.3	Mendesain Topologi Jaringan	33
3.3.4	Melakukan Instalasi Kebutuhan Penelitian.....	36
3.3.5	Konfigurasi Sistem dan Implementasi SDN dan IDPS.....	36
3.3.6	Pengujian Sistem.....	38
3.3.7	Pengambilan Data dan Analisis Data	38
BAB IV		39
HASIL DAN PEMBAHASAN		39
4.1	Implementasi dan Konfigurasi Sistem	39
4.1.1	<i>Server</i>	39
4.1.2	<i>Controller</i>	41
4.1.3	<i>OPNSense</i>	43
4.1.4	Implementasi di GNS3	45
4.2	Skenario Simulasi Penyerangan	46
4.2.1	<i>DDoS ICMP Flood</i>	46
4.2.2	<i>DDoS SYN Flood</i>	48
4.3	Pengujian Sistem.....	50
4.3.1	Serangan ICMP Flood.....	50
4.3.2	Serangan SYN Flood	59
4.4	Pengukuran <i>Quality of Service (QoS)</i>	66
4.3.3	Throughput.....	66
4.3.4	Packet Loss	76
4.3.5	Delay	86
4.3.6	Jitter.....	96
BAB V		105
KESIMPULAN		105
5.1	Kesimpulan	105
5.2	Saran.....	106
DAFTAR PUSTAKA		107
LAMPIRAN.....		110