

DAFTAR GAMBAR

Gambar 1. 1 Grafik Trafik Anomali Serangan Siber di Indonesia Tahun 2023.....	1
Gambar 2. 1 Arsitektur <i>Software Defined Network</i>	13
Gambar 2. 2 Konsep IDS dan IPS	15
Gambar 2. 3 Penggunaan Wireshark	18
Gambar 3. 1 Diagram Alir Penelitian.....	32
Gambar 3. 2 Topologi Jaringan	33
Gambar 3. 3 <i>Flowchart</i> Implementasi SDN dan IDPS	36
Gambar 4. 1 Menambah <i>Repository Suricata</i>	39
Gambar 4. 2 <i>Custom Rule</i> Suricata	40
Gambar 4. 3 Instalasi dan Konfigurasi <i>OpenDayLight</i>	42
Gambar 4. 4 Menambah <i>Interface</i> sesuai Topologi	43
Gambar 4. 5 Menambah <i>Bridge</i>	44
Gambar 4. 6 Mengatur <i>Firewall NAT Outbound</i>	44
Gambar 4. 7 Mengatur <i>DHCP Gateway</i>	45
Gambar 4. 8 Implementasi di GNS3	45
Gambar 4. 9 Perintah <i>DDoS ICMP Flood</i> Dijalankan.....	47
Gambar 4. 10 Perintah <i>DDoS SYN Flood</i> Dijalankan.....	48
Gambar 4. 11 Pengujian Serangan <i>ICMP Flood</i> Tanpa Menggunakan IDPS.....	51
Gambar 4. 12 <i>Capture Wireshark</i> Serangan <i>ICMP Flood</i> Tanpa Menggunakan IDPS	52
Gambar 4. 13 Pengujian Serangan <i>ICMP Flood</i> dengan IDPS	53
Gambar 4. 14 Eksekusi <i>script RulesDrop.py</i> untuk proteksi <i>DDoS ICMP Flood</i>	54
Gambar 4. 15 Tampilan terminal saat <i>Suricata</i> aktif dan memproses paket ketika Serangan <i>ICMP Flood</i>	55
Gambar 4. 16 <i>Fastlog</i> Ketika Serangan <i>ICMP Flood</i> dengan IDPS.....	56
Gambar 4. 17 Deteksi <i>ICMP Flood</i> Dan Pengiriman <i>Flow DROP</i> ke <i>ODL</i>	57
Gambar 4. 18 <i>Capture Wireshark</i> Serangan <i>ICMP Flood</i> dengan IDPS	58
Gambar 4. 19 Pengujian Serangan <i>SYN Flood</i> Tidak Menggunakan IDPS.....	59
Gambar 4. 20 <i>Capture Wireshark</i> Serangan <i>SYN Flood</i> Tidak Menggunakan IDPS	60
Gambar 4. 21 Pengujian Serangan <i>SYN Flood</i> dengan Menggunakan IDPS	61
Gambar 4. 22 Tampilan Terminal <i>Suricata</i> Aktif dan Memproses Paket Ketika Serangan <i>SYN Flood</i>	62
Gambar 4. 23 Eksekusi <i>Script start_suricata.py</i> untuk Proteksi <i>DDoS SYN Flood</i>	63
Gambar 4. 24 Log <i>Suricata</i> Mendeteksi Dan Memblokir Serangan <i>SYN Flood</i> ..	64

Gambar 4. 25 Deteksi <i>SYN Flood</i> Dan Pengiriman <i>Flow DROP</i> ke <i>ODL</i>	64
Gambar 4. 26 <i>Capture Wireshark</i> Ketika Serangan <i>SYN Flood</i> Setelah IDPS Aktif	65
Gambar 4. 27 Grafik <i>Throughput</i> Ketika Serangan <i>ICMP</i> Tanpa IDPS	67
Gambar 4. 28 Grafik <i>Throughput</i> Ketika Serangan <i>ICMP Flood</i> dengan IDPS...	69
Gambar 4. 29 Grafik <i>Throughput</i> Ketika Serangan <i>SYN Flood</i> Tanpa IDPS	71
Gambar 4. 30 Grafik <i>Throughput</i> Ketika Serangan <i>SYN Flood</i> dengan IDPS	74
Gambar 4. 31 Perbandingan <i>Throughput</i> pada Setiap Pengujian.....	74
Gambar 4. 32 Grafik <i>Packet Loss</i> Ketika Serangan <i>ICMP Flood</i> Tidak Menggunakan IDPS	78
Gambar 4. 33 Grafik <i>Packet Loss</i> Ketika Serangan <i>ICMP Flood</i> dengan IDPS ..	80
Gambar 4. 34 Grafik <i>Packet Loss</i> Ketika Serangan <i>SYN Flood</i> Tidak Menggunakan IDPS	82
Gambar 4. 35 Grafik <i>Packet Loss</i> Ketika Serangan <i>SYN Flood</i> dengan IDPS	84
Gambar 4. 36 Perbandingan <i>Packet Loss</i> pada Setiap Pengujian	85
Gambar 4. 37 Grafik <i>Delay</i> Ketika Serangan <i>ICMP Flood</i> Tidak Menggunakan IDPS	87
Gambar 4. 38 Grafik <i>Delay</i> Ketika Serangan <i>ICMP Flood</i> dengan IDPS	90
Gambar 4. 39 Grafik <i>Delay</i> Ketika Serangan <i>SYN Flood</i> Tidak Menggunakan IDPS	92
Gambar 4. 40 Grafik <i>Delay</i> Ketika Serangan <i>SYN Flood</i> dengan IDPS.....	94
Gambar 4. 41 Perbandingan <i>Delay</i> pada Setiap Pengujian.....	94
Gambar 4. 42 Grafik <i>Jitter</i> Ketika Serangan <i>ICMP Flood</i> Tidak Menggunakan IDPS	97
Gambar 4. 43 Grafik <i>Jitter</i> Ketika Serangan <i>ICMP Flood</i> dengan IDPS	99
Gambar 4. 44 Grafik <i>Jitter</i> Ketika Serangan <i>SYN Flood</i> Tidak Menggunakan IDPS	101
Gambar 4. 45 Grafik <i>Jitter</i> Ketika Serangan <i>SYN Flood</i> dengan IDPS	103
Gambar 4. 46 Perbandingan <i>Jitter</i> pada Setiap Pengujian.....	103