

SKRIPSI

***ANALISIS INTRUSION PREVENTION SYSTEM (IPS) PADA
SOFTWARE DEFINED NETWORK (SDN) DALAM
MENCEGAH SERANGAN DISTRIBUTED DENIAL OF
SERVICE (DDOS)***

***ANALYSIS OF INTRUSION PREVENTION SYSTEM (IPS) ON
SOFTWARE DEFINED NETWORK (SDN) IN PREVENTING
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS***



Disusun oleh

**WENY IRMA SYAFRIL
2212101128**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2024

SKRIPSI

***ANALISIS INTRUSION PREVENTION SYSTEM (IPS) PADA
SOFTWARE DEFINED NETWORK (SDN) DALAM
MENCEGAH SERANGAN DISTRIBUTED DENIAL OF
SERVICE (DDOS)***

***ANALYSIS OF INTRUSION PREVENTION SYSTEM (IPS) ON
SOFTWARE DEFINED NETWORK (SDN) IN PREVENTING
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS***



Disusun oleh

**WENY IRMA SYAFRIL
2212101128**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2024

***ANALISIS INTRUSION PREVENTION SYSTEM (IPS) PADA
SOFTWARE DEFINED NETWORK (SDN) DALAM
MENCEGAH SERANGAN DISTRIBUTED DENIAL OF
SERVICE (DDOS)***

***ANALYSIS OF INTRUSION PREVENTION SYSTEM (IPS) ON
SOFTWARE DEFINED NETWORK (SDN) IN PREVENTING
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2024**

Disusun oleh

**WENY IRMA SYAFRIL
221210128**

DOSEN PEMBIMBING

**Bongga Arifwidodo, S.ST., M.T.
Dadiek Pranindito, S.T., M.T.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2024

HALAMAN PENGESAHAN

ANALISIS INTRUSION PREVENTION SYSTEM (IPS) PADA SOFTWARE DEFINED NETWORK (SDN) DALAM MENCEGAH SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS)

ANALYSIS OF INTRUSION PREVENTION SYSTEM (IPS) ON SOFTWARE DEFINED NETWORK (SDN) IN PREVENTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Disusun oleh
WENY IRMA SYAFRIL
2212101128

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 19 Juni 2024

Susunan Tim Penguji

Pembimbing Utama : Bongga Arifwidodo, S.ST., M.T.
NIDN. 0603118901

Pembimbing Pendamping : Dadiék Pranindito, S.T., M.T.
NIDN. 0626108502

Penguji 1 : Jafaruddin Gusti Amri Ginting, S.T., M.T.
NIDN. 0620108901

Penguji 2 : Fauza Khair, S.T., M.Eng.
NIDN. 0622039001

(Arifwidodo) 19/6/2024
(Dadiék Pranindito) 25/6/2024
(Jafaruddin Gusti Amri Ginting) 25/6/2024
(Fauza Khair) 24/06/2024

Mengetahui,

Ketua Program Studi D4 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetyo Yulianto, S.T., M.T.
NIDN. 0622079001

Prasetyo Yulianto

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, WENY IRMA SYAFRIL, menyatakan bahwa skripsi dengan judul “ ANALISIS INTRUSION PREVENTION SYSTEM (IPS) PADA JARINGAN SOFTWARE DEFINED NETWORK (SDN) DALAM MENCEGAH SERANGAN DISTRIBUTED DANIEL OF SERVICE (DDOS)” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 12 Juni 2024

Yang menyatakan,



(Weny Irma Syafril)

PRAKATA

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “**Analisis *Intrusion Prevention System (IPS)* Pada *Software Defined Network (SDN)* Dalam Mencegah Serangan *Distributed Denial Of Service (DDoS)*”.**

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Allah SWT yang telah memberikan segala nikmat dan karunia-Nya sehingga dapat menyelesaikan skripsi ini
2. Kedua orang tua dan keluarga tercinta yang telah memberikan motivasi serta dukungan secara moril dan materil sehingga tugas akhir ini bisa terselesaikan.
3. Bapak Bongga Arifwidodo, S.ST.,M.T selaku pembimbing I yang telah membimbing dan memberikan ilmu kepada penulis sehingga dapat menyelesaikan skripsi ini..
4. Bapak Dadiék Pranindito S.T. M.T selaku pembimbing II yang telah membimbing dan memberikan ilmu kepada penulis sehingga dapat menyelesaikan skripsi ini
5. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T selaku Rektor Institut Teknologi Telkom Purwokerto.
6. Ibu Dr. Anggun Fitriani Isnawati S.T., M.Eng selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro.
7. Bapak Prasetyo Yuliantoro S.T., M.T selaku Ketua Program Studi S1 Teknik Telekomunikasi.
8. Seluruh dosen, staff dan karyawan Program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.

9. Kepada seluruh keluarga dan juga kerabat penulis yang telah mendoakan sehingga skripsi ini bisa terselesaikan
10. Orang terdekat Penulis yaitu M. Odi, Felmi dan Novika yang selalu memberikan doa dan dukungan bagi penulis dalam menyelesaikan studi di S1 Teknik Telekomunikasi

Atas segala kekurangan laporan tugas akhir ini, penulis sangat mengharapkan masukan, kritik, dan saran yang bersifat membangun ke arah perbaikan dan penyempurnaan skripsi ini agar penyusunan selanjutnya lebih baik lagi. Penulis berharap skripsi ini dapat bermanfaat bagi seluruh pihak yang ada.

Purwokerto, 12 Juni 2024

(Weny Irma Syafri)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN.....	II
HALAMAN PERNYATAAN ORISINALITAS	II
PRAKATA.....	IV
ABSTRAK	V
ABSTRACT.....	VI
DAFTAR ISI.....	VII
DAFTAR GAMBAR.....	VIII
DAFTAR TABEL	XII
DAFTAR LAMPIRAN	XIII
BAB 1 PENDAHULUAN	1
1.1 LATAR BELAKANG	1
1.2 RUMUSAN MASALAH	3
1.3 BATASAN MASALAH.....	3
1.4 TUJUAN	4
1.5 MANFAAT	4
1.6 SISTEMATIKA PENULISAN	4
BAB 2 DASAR TEORI.....	5
2.1 KAJIAN PUSTAKA	5
2.2 DASAR TEORI.....	8
2.2.1 <i>SOFTWARE DEFINED NETWORK</i>	8
2.2.2 <i>CONTROLLER</i>	9
2.2.2.1 <i>OPEN NETWORK OPERATING SYSTEM</i>	9
2.2.2.2 <i>RYU</i>	9
2.2.2.3 <i>FLOODLIGHT</i>	9
2.2.2.4 <i>POX</i>	10
2.2.3 <i>OPENFLOW</i>	10
2.2.4 <i>TRANSMISSION CONTROL PROTOCOL(TCP)</i>	10
2.2.5 <i>USER DATAGRAM PROTOCOL(UDP)</i>	11
2.2.6 KEMAMAN JARINGAN	12
2.2.7 <i>INTRUSION PREVENTION SYSTEM(IPS)</i>	12
2.2.8 <i>INTRUSION DETECTION SYSTEM(IDS)</i>	13
2.2.9 <i>SNORT</i>	13
2.2.10 <i>DISTRUBUTED DANIEL OF SERVICE</i>	13
2.2.11 <i>QUALITY OF SERVICE(QoS)</i>	14
2.2.11.1 <i>THROUGHPUT</i>	14

2.2.12	MEMORI	15
2.2.13	<i>CENTRAL PROCESSING UNIT</i>	15
2.2.14	<i>IPERF</i>	15
2.2.11	<i>TOP</i>	16
BAB 3 METODE PENELITIAN..... ERROR! BOOKMARK NOT DEFINED.		
3.1	ALAT YANG DIGUNAKAN	17
3.1.1	PERANGKAT KERAS.....	17
3.1.2	PERANGKAT LUNAK	17
3.2	ALUR PENELITIAN	17
3.3	INSTALASI KEBUTUHAN SIMULASI.....	20
3.3.1	INSTALL <i>RYU</i> BESERTA SERVICE PENDUKUNG	20
3.3.2	INSTALL <i>MININET</i>	21
3.3.3	INSTALL <i>SNORT</i>	21
3.3.4	INSTALL <i>HPING3</i>	21
3.3.5	INSTALL <i>IPERF</i>	22
3.3.6	INSTALL <i>TOP</i>	22
3.4	RANCANGAN SYSTEM.....	22
3.4.1	PERANCANGAN SONFWARE DEFINED NETWORK.....	22
3.4.2	PERANCANGAN INSTRUSION PREVENTION SYSTEM.....	25
3.4.2.1	PERANCANGAN IDS <i>SNORT</i>	25
3.4.2.2	PERANCANGAN <i>REST FIREWALL</i>	29
3.5	PENGUJIAN SISTEM	30
3.6	PENGUJIAN SERANGAN	36
3.6.1	PENGUJIAN SERANGAN TCP SYN <i>FLOOD</i>	36
3.6.2	PENGUJIAN SERANGAN UDP <i>FLOOD</i>	39
3.7	PENGUJIAN SISTEM KEMAMAN IPS	41
3.8	SKENARIO PENGUJIAN DAN PENGAMBILAN DATA	48
3.8.1	DATA QUALITY OF SERVICE(QoS)	49
3.8.2	DATA CPU <i>USAGE</i> DAN MEMORY <i>USAGE</i>	50
BAB 4 HASIL DAN PEMBAHASAN.....		51
4.1	DATA <i>QUALITY OF SERVICE</i> (QoS)	51
4.2	DATA PENGGUNAAN CPU DAN MEMORI	64
BAB 5 PENUTUP.....		69
5.1	KESIMPULAN	69
5.2	SARAN	69
DAFTAR PUSTAKA		70
LAMPIRAN.....		72

DAFTAR GAMBAR

Gambar 2.1 Arsitektur SDN [10].....	8
Gambar 2.2 Pembentukan dan pemutusan hubungan TCP [14]	11
Gambar 3.1 Diagram Alur Penelitian	18
Gambar 3.2 Rancangan Topologi jaringan	23
Gambar 3.3 Running Ryu	31
Gambar 3.4 Running Topologi pada Mininet	31
Gambar 3.5 Hasil Pingall	32
Gambar 3.6 Perintah Allowflow.Sh.....	32
Gambar 3.7 Running AllowFlow.Sh	33
Gambar 3.8 Controller Ryu memberi izin Host.....	33
Gambar 3.9 Hasil pingall setelah ditambahkan allowFlow.sh.....	33
Gambar 3.10 Menjalankan server pada Host 1	34
Gambar 3.11 Running snort	34
Gambar 3. 12. Menampilkan Alert pada folder alerts.csv	34
Gambar 3.13 Menampilkan alert pada telegram.....	35
Gambar 3.14 Ping host pada server	35
Gambar 3.15 Menampilkan alert dari Folder Alerts.csv	35
Gambar 3.16 Alert pada telegram.....	36
Gambar 3.17 Hasil ping host 3 ke server	37
Gambar 3.18 Perintah serangan TCP Syin Flood	37
Gambar 3.19 Hasil deteksi snort melalui folder Alerts.csv.....	38
Gambar 3.20 Hasil notifikasi snort pada Telegram.....	38
Gambar 3.21 Hasil ping Host 3 ke server	39
Gambar 3.22 serangan UDP Dilancarkan	39
Gambar 3.23 Alert.csv saat serangan UDP	40
Gambar 3.24 Notifikasi serangan UDP pada Telegram	40
Gambar 3.25 Flowchart Sistem keamanan IPS	42
Gambar 3.26 Hasil Bandwidth dan Transfer server saat normal	43
Gambar 3.27 Attacker melakukan penyerangan ke server	44
Gambar 3.28 Hasil ping IP host 2 ke server saat diserang	44
Gambar 3.29 Alert pada log alerts CSV	45
Gambar 3.30 Notifikasi snort pada Telegram.....	45
Gambar 3.31 Menjalankan script block.sh untuk blokir serangan	46
Gambar 3.32 Ryu memblok IP penyerang	46
Gambar 3.33 Alert pada Log Alerts.csv.....	47
Gambar 3.34 Hasil bandwidth dan transfer setelah blokir serangan..	47
Gambar 3.35 Host 3 gagal melakukan ping ke server	48
Gambar 3.36 Topologi pengambilan data Qos Throughput.....	49
Gambar 4.1 <i>Throughput</i> kondisi normal pada protokol TCP	52
Gambar 4.2 <i>Throughput</i> kondisi normal pada protokol UDP	53
Gambar 4.3 Alert <i>Snort</i> saat kondisi normal	54

Gambar 4.4 Notifikasi <i>alert snort</i> pada Telegram	54
Gambar 4.5 Deteksi DDoS TCP SYN <i>Flood</i>	55
Gambar 4.6 Notifikasi serangan TCP SYN <i>Flood</i> pada Telegram	56
Gambar 4.7 IPS berhasil memblokir serangan SYN <i>Flood</i>	57
Gambar 4.8 Perbandingan Transfer TCP SYN <i>Flood</i>	58
Gambar 4.9 Perbandingan Bandwitdh TCP SYN <i>Flood</i>	59
Gambar 4.10 <i>Snort</i> mendeteksi ada serangan DDoS UDP <i>Flood</i>	60
Gambar 4.11 Notifikasi Alert pada Telegram.....	60
Gambar 4.12 IPS berhasil memblokir serangan UDP <i>Flood</i>	61
Gambar 4.13 Perbandingan Transfer UDP <i>Flood</i>	62
Gambar 4.14 Perbandingan Nilai Bandwitdh UDP <i>Flood</i>	63
Gambar 4.15 Kondisi Sebelum Diserang	64
Gambar 4.16 Kondisi saat serangan TCP SYN <i>Flood</i>	64
Gambar 4.17 Kondisi setelah Blokir menggunakan IPS	64
Gambar 4.18 Penggunaan CPU saat TCP SYN <i>Flood</i>	65
Gambar 4.19 Penggunaan Memori Saat TCP SYN <i>Flood</i>	65
Gambar 4.20 Kondisi saat serangan UDP <i>Flood</i>	66
Gambar 4.21 Kondisi saat blokir serangan menggunakan IPS.....	66
Gambar 4.22 Penggunaan CPU Pada UDP <i>Flood</i>	67
Gambar 4.23 Penggunaan memori saat UDP <i>Flood</i>	67

DAFTAR TABEL

Tabel 2.1 Kajian Penelitian Sebelumnya	7
Tabel 2.2 Kategori Throughput berdasarkan TIPHON [18].....	15
Tabel 3.1 Spesifikasi Perangkat Keras.....	17
Tabel 3.2 Perangkat Lunak.....	17
Tabel 3.3 Pengalamatan IP Address	24
Tabel 3.4 Penjelasan Perintah Rules	27
Tabel 4.1 Nilai Throughput Serangan TCP SYN Flood	56
Tabel 4.2 Hasil Througput serangan saat integrasi IPS.....	57
Tabel 4.3 Hasil Throughput saat serangan DDoS UDP Flood.....	61
Tabel 4.4 Hasil Throughput serangan saat intergrasi IPS	62

DAFTAR LAMPIRAN

- Lampiran A: Hasil Nilai Throughput TCP SYN *Flood* tanpa IPS**
- Lampiran B: Hasil Nilai Throughput UDP *Flood* tanpa IPS**
- Lampiran C: Hasil Nilai Throughput TCP SYN *Flood* dengan IPS**
- Lampiran D: Hasil Nilai Throughput UDP *Flood* tanpa IPS**