

**ANALISIS IMPLEMENTASI *INTRUSION PREVENTION SYSTEM (IPS)*
UNTUK MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
(DDoS) PADA JARINGAN *SOFTWARE DEFINED NETWORK (SDN)***

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Meraih Gelar Sarjana Teknik Pada
Program Studi Sistem Telekomunikasi UPI Kampus di Purwakarta



Oleh

Amalia Annisa

2001624

**PROGRAM STUDI SISTEM TELEKOMUNIKASI
KAMPUS UPI DAERAH DI PURWAKARTA
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

LEMBAR HAK CIPTA

**ANALISIS IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS)
UNTUK MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
(DDoS) PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN)**

Oleh,

Amalia Annisa (2001624)

Skripsi yang diajukan untuk Memenuhi Salah Satu Syarat Mendapat Gelar
Sarjana Teknik pada Program Studi Sistem Telekomunikasi

UPI Kampus di Purwakarta

© **Amalia Annisa** 2024

Universitas Pendidikan Indonesia

Agustus 2024

Hak cipta dilindungi undang-undang

Segala bentuk perbanyakan dari skripsi ini tidak boleh dilakukan tanpa izin dari
penulis

LEMBAR PENGESAHAN

SKRIPSI
AMALIA ANNISA
2001624

**ANALISIS IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS)
UNTUK MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
(DDoS) PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN)**

Disetujui dan Disahkan oleh Pembimbing,

Pembimbing I



Galura Muhammad Suranegara, S.Pd., M.T
NIP.920190219920111101

Pembimbing II



Endah Setyowati, S.T., M.T
NIP.199209082024062002

Ketua Program Studi Sistem Telekomunikasi



Galura Muhammad Suranegara, S.Pd., M.T
NIP.920190219920111101

KATA PENGANTAR

Puji dan Syukur penulis panjatkan ke hadirat Allah SWT yang senantiasa memberikan hidayah, Rahmat, kekuatan lahir dan batin kepada penulis. Serta tidak lupa shalawat dan salam semoga tetap terlimpah dan tumpah kepada Nabi Muhammad SAW yang telah memberikan kekuatan sehingga penulis dapat menyelesaikan skripsi dengan judul “Analisis Implementasi *Intrusion Prevention System (IPS)* untuk Mitigasi Serangan *Distributed Denial Of Service (DDoS)* pada Jaringan *Software Defined Network (SDN)*”.

Skripsi ini disusun sebagai syarat dalam memperoleh gelar Sarjana Teknik pada Jurusan Sistem Telekomunikasi Universitas Pendidikan Indonesia. Dalam penulisan Skripsi ini, penulis menyadari bahwa skripsi ini masih belum sempurna dalam kajian maupun penyajian karena adanya keterbatasan dan pengetahuan dalam pembuatannya.

Demikian, semoga hasil penelitian yang dilakukan dapat bermanfaat khususnya bagi penulis sendiri dan umumnya bagi yang membaca. *Aamiin*

Purwakarta, Agustus 2024

Amalia Annisa

UCAPAN TERIMAKASIH

Puji Syukur penulis ucapkan ke hadirat Allah SWT yang telah melimpahkan Rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penelitian dan penyusunan skripsi “Analisis Implementasi *Intrusion Prevention System (IPS)* untuk Mitigasi Serangan *Distributed Denial Of Service (DDoS)* pada Jaringan *Software Defined Network (SDN)*” dengan lancar dan baik. Penulis sadari skripsi yang disusun oleh penulis tidak akan selesai tanpa adanya doa, bimbingan dan dukungan dari pihak yang lain. Sehingga pada kesempatan kali ini, penulis ingin mengucapkan banyak terimakasih kepada:

1. Keluarga tercinta terutama Bapak dan Ibu terkasih serta kedua kakak atas segala doa, keikhlasan, dukungan dan semangat kepada penulis selama penyusunan skripsi sehingga penulis diberi kelancaran dalam menyelesaikan skripsi yang dilakukan oleh penulis.
2. Bapak Galura Muhammad Suranegara, S.Pd.,M.T, selaku Kepala Program Studi Sistem Telekomunikasi dan sekaligus Dosen Pembimbing I yang telah mencurahkan waktu, ilmu, dan tenaganya untuk memberikan bimbingan, saran, motivasi, serta perhatiannya selama penyusunan proposal skripsi dan skripsi.
3. Ibu Endah Setyowati, S.T., M.T, selaku dosen Pembimbing II yang juga telah mencurahkan waktu, ilmu, dan tenaganya untuk memberikan bimbingan, saran, motivasi, dan perhatiannya selama penyusunan skripsi.
4. Ibu Dewi Indriati Hadi Putri, S.Pd., M.T, selaku dosen wali yang telah membersamai, memberikan waktu, ilmu, arahan, motivasi dan membimbing penulis selama perkuliahan.
5. Seluruh dosen dan staf akademik Sistem Telekomunikasi yang tidak dapat penulis sebutkan satu persatu, yang telah ikhlas membantu dan memberikan waktu, ilmu, bimbingan, arahan, juga motivasinya kepada penulis.
6. Sahabat baik, Dede Rima yang telah memberikan banyak motivasi, dukungan, masukan, dan bersedia menjadi tempat berbagi cerita terbaik bagi penulis selama kurang lebih 10 tahun,
7. Teman-teman seperjuangan Diva Nuranty Yovanka, Sri Anggraeni, Cindy Liu, Najwa Zahratul Kubro, Annisa Amalia, Futuh Balad yang telah memberikan

semangat, motivasi, rasa nyaman, dan dapat menghibur penulis dalam proses penyusunan skripsi.

8. Teman-teman Sistem Telekomunikasi angkatan 2020 terimakasih atas segala cerita, kenangan, kesan, dan pesan selama perkuliahan berlangsung.
9. Semua pihak yang tidak dapat disebutkan satu persatu, terimakasih atas segala yang telah dicurahkan.

ABSTRAK

Penelitian ini mempunyai tujuan untuk mengevaluasi dampak dari implementasi *Intrusion Prevention System* pada performa jaringan *Software Defined Network* yang mengalami berbagai jenis serangan *Distributed Denial of Service*. Dengan melakukan 2 perbandingan yaitu perbandingan Pengukuran I sebelum serangan dengan Pengukuran II saat terjadi serangan dan perbandingan Pengukuran II saat terjadi serangan dengan Pengukuran III saat terjadi serangan dengan IPS aktif. Melalui analisis terhadap parameter yang mengukur performa jaringan seperti *throughput*, *delay*, *packet loss*, serta penggunaan CPU dan memori. Dari hasil penelitian menunjukkan bahwa serangan DDoS mempunyai dampak yang signifikan terhadap performa jaringan dan implementasi IPS mampu meningkatkan *throughput* dan menurunkan *packet loss* secara signifikan. Namun di samping itu, menyebabkan adanya peningkatan *delay* dan penggunaan sumber daya sistem, memperlihatkan kebutuhan akan kapasitas infrastruktur jaringan yang lebih besar untuk mendukung operasi IPS. Melihat hal tersebut, maka sekalipun IPS efektif dalam mengurangi dampak serangan, terdapat beberapa hal yang masih membutuhkan pertimbangan dalam hal jaringan dan kebutuhan sumber daya.

Kata Kunci: SDN, DDoS Attack, IPS, Mitigasi, Network Security

ABSTRACT

This study aims to evaluate the impact of Intrusion Prevention System implementation on the performance of Software Defined Network networks that experience various types of Distributed Denial of Service attacks. By doing 2 comparisons, namely comparison of Measurement I before the attack with Measurement II during the attack and comparison of Measurement II during the attack with Measurement III during the attack with an active IPS. Through analysis of parameters that measure network performance such as throughput, delay, packet loss, and CPU and memory usage. The results show that DDoS attacks have a significant impact on network performance and IPS implementation is able to increase throughput and reduce packet loss significantly. However, it caused an increase in delay and system resource usage, demonstrating the need for greater network infrastructure capacity to support IPS operations. Given this, even though IPS is effective in reducing the impact of attacks, there are some things that still require consideration in terms of network and resource requirements.

Keywords: SDN, DDoS Attack, IPS, Mitigation, Network Security

DAFTAR ISI

LEMBAR HAK CIPTA	i
LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS SKRIPSI	ii
KATA PENGANTAR	iii
UCAPAN TERIMAKASIH.....	v
ABSTRAK	vii
<i>ABSTRACT</i>	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	3
1.5.1 Manfaat Teoritis.....	3
1.5.2 Manfaat Praktis	4
1.6 Struktur Organisasi Skripsi.....	4
BAB II DASAR TEORI	5
2.1 <i>Software Defined Network Software</i>	5
2.2 <i>Distributed Denial of Service</i>	7
2.3 <i>Intrusion Prevention System</i>	8
2.4 Snort.....	10
2.5 Mininet.....	10
2.6 Performa Jaringan.....	11
2.6.1 <i>Quality of Service (QoS)</i>	11
2.6.2 <i>Resource Usage</i>	13
2.7 Performa Jaringan.....	14
BAB III METODE PENELITIAN.....	16
3.1 Desain Penelitian	16
3.2 Alur Penelitian	16
3.3 Alur Percobaan	18
3.4 Karakteristik Objek Penelitian.....	18
3.4.1 Jaringan SDN.....	19
3.4.2 Sistem IPS.....	20
3.4.3 Serangan DDoS.....	22
3.4.4 Perangkat Lunak	23
3.5 Teknik Pengumpulan Data	23
3.6 Teknik Analisis Data	25
BAB IV HASIL DAN PEMBAHASAN	28
4.1 Hasil dan Pembahasan Pertimbangan Waktu Pengujian	28
4.1.1 Pengukuran I.....	29
4.1.2 Pengukuran II.....	30
4.1.3 Pengukuran III	36
4.2 Hasil dan Pembahasan Pengujian	41

4.2.1 Hasil dan Pembahasan Pengukuran I dan II	42
4.2.2 Hasil dan Pembahasan Pengukuran II dan III.....	50
BAB V PENUTUP.....	59
5.1 Kesimpulan.....	59
5.2 Implikasi	61
5.3 Rekomendasi	62
DAFTAR PUSTAKA	63
LAMPIRAN.....	66

DAFTAR GAMBAR

Gambar 2. 1	Arsitektur SDN.....	6
Gambar 3. 1	Alur Penelitian.....	17
Gambar 3. 2	Alur Percobaan.....	18
Gambar 3. 3	Topologi Jaringan.....	20
Gambar 3. 4	Versi Snort.....	22
Gambar 3. 5	Versi Hping3	23
Gambar 3. 6	Proses Pengukuran Penelitian	24
Gambar 4. 1	Perbandingan <i>Throughput</i> pada Pengukuran I dan II.....	44
Gambar 4. 2	Perbandingan <i>Delay</i> pada Pengukuran I dan II.....	45
Gambar 4. 3	Perbandingan <i>Packet loss</i> pada Pengukuran I dan II	46
Gambar 4. 4	Perbandingan Penggunaan CPU pada Pengukuran I dan II	48
Gambar 4. 5	Perbandingan Penggunaan Memori pada Pengukuran I dan II.....	49
Gambar 4. 6	Perbandingan <i>Throughput</i> pada Pengukuran II dan III.....	52
Gambar 4. 7	Perbandingan <i>Delay</i> pada Pengukuran II dan III	53
Gambar 4. 8	Perbandingan <i>Packet loss</i> pada Pengukuran II dan III.....	54
Gambar 4. 9	Perbandingan Penggunaan CPU pada Pengukuran II dan III	56
Gambar 4. 10	Perbandingan Penggunaan Memori pada Pengukuran II dan III ...	57

DAFTAR TABEL

Tabel 2. 1 Standar <i>Throughput</i> Tiphon.....	12
Tabel 2. 2 Standar <i>Delay</i> Tiphon	12
Tabel 2. 3 Standar <i>Packet loss</i> Tiphon.....	13
Tabel 2. 4 Penelitian Terdahulu	14
Tabel 3. 1 Perangkat Lunak	23
Tabel 3. 2 Pengukuran Penelitian.....	24
Tabel 4. 1 Nilai rata-rata Rata-rata Pengukuran I	29
Tabel 4. 2 Nilai rata-rata Rata-rata Pengukuran II.....	31
Tabel 4. 3 Nilai rata-rata Rata-rata Pengukuran III.....	36
Tabel 4. 4 Nilai rata-rata Pengukuran I dan II	43
Tabel 4. 5 Nilai rata-rata Pengukuran II dan III.....	51

DAFTAR LAMPIRAN

Lampiran 1. SK Pembimbing Skripsi	66
Lampiran 2. Kartu Bimbingan Skripsi	70
Lampiran 3. Submit Jurnal	72
Lampiran 4. Topologi Jaringan	73
Lampiran 5. Perintah Serangan	75
Lampiran 6. D-ITG	77
Lampiran 7. Snort IPS	81
Lampiran 8. Menjalankan Dstat	83
Lampiran 9. Data Pengujian	84

DAFTAR PUSTAKA

- Abhilash, G., & Divyansh, G. (2018). *Intrusion Detection and Prevention in Software Defined Networking*. 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 1–4. <https://doi.org/10.1109/ANTS.2018.8710141>
- Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan *Network Intrusion Detection and Prevention System*. *JOINTECS (Journal of Information Technology and Computer Science)*, 5(1), 17. <https://doi.org/10.31328/JoinTECS.V5i1.1240>
- Ananta, W. A. D., Kurniawan, T., & Widjajarto, A. (2023). Implementasi Serangan *Distributed Denial of Service (DDoS)* Menggunakan HPING3 pada *Software Defined Network (SDN)* dengan Metode PPDIOO. *Journal Of Management & Business*, 6(1), 266–275.
- Arifwidodo, B., Setiyadi, B., & Ikhwan, S. (2022). Implementasi *Intrusion Prevention System (IPS)* Pada *Software Defined Network (SDN)* Menggunakan RYU Controller. *Information Communication & Technology*, 21(1), 113–117.
- Arman, M., & Inayatullah, I. (2019). Rancang Bangun *Owncloud* dan Melindunginya Terhadap Serangan Ddos. *Jurnal Integrasi*, 11(1), 49–58. <https://doi.org/10.30871/Ji.V11i2.770>
- Barends, J. K., Dewanta, F., & Karna, N. B. A. (2022). Perancangan dan Analisis *Intrusion Prevention System* Berbasis SNORT dan IPTABLES dengan Integrasi Honeypot Pada Arsitektur *Software Defined Network*. *MULTINETICS*, 7(2).
- Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). *Implementing An Intrusion Detection and Prevention System Using Software-Defined Networking: Defending Against Port-Scanning and Denial-of-Service Attacks*. *Journal of Network and Computer Applications*, 136, 71–85. <https://doi.org/10.1016/J.Jnca.2019.03.005>
- Boukria, S., & Guerroumi, M. (2019). *Intrusion Detection System for SDN Network Using Deep Learning Approach*. 2019 International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS), 1–6. <https://doi.org/10.1109/ICTAACS48474.2019.8988138>
- Chovanec, M., Hasin, M., Havrilla, M., & Chovancová, E. (2023). *Detection of HTTP DDoS Attacks Using Nfstream and Tensorflow*. *Applied Sciences*, 13(11), 6671. <https://doi.org/10.3390/App13116671>
- Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh Sebagai *Log Event Management* dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1), 1–7. <https://doi.org/10.30630/Jitsi.3.1.59>
- Girdler, T., & Vassilakis, V. G. (2021). *Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking: Defending Against ARP Spoofing Attacks and Blacklisted MAC Addresses*. *Computers & Electrical Engineering*, 90, 106990. <https://doi.org/10.1016/J.Compeleceng.2021.106990>
- Harshita. (2017). *Detection and Prevention of ICMP Flood DDOS Attack*. *International Journal of New Technology and Research*, 3(3), 63–69.

- Huda, I. M., & Suartana, I. M. (2021). Implementasi *Intrusion Prevention System* Untuk Mencegah Serangan DDoS pada *Software Defined Network*. (*Journal Of Informatics and Computer Science*, 03(02), 113–117.
- Islam, H. Z., Faiqurahman, M., & Sumadi, F. D. S. (2024). Analisis Dampak Serangan Dos pada *Software Defined Network*. *Jurnal Repositor*, 4(1). <https://doi.org/10.22219/Repositor.V4i1.32315>
- Lee, T.-H., Chang, L.-H., & Syu, C.-W. (2020). *Deep Learning Enabled Intrusion Detection and Prevention System Over SDN Networks*. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–6. <https://doi.org/10.1109/Iccworkshops49005.2020.9145085>
- Muntaha, M. F., Trisnawan, P. H., & Primananda, R. (2019). Implementasi *Intrusion Prevention System* (IPS) Berbasis Athena Untuk Mencegah Serangan DDoS Pada Arsitektur *Software-Defined Network* (SDN). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 3(7), 6874–6855. <http://j-ptiik.ub.ac.id>
- Nilayam, L. (2023). *Early Detection and Prevention of Distributed Denial of Service Attack Using Software-Defined Networks with Mininet Network Simulator*. *International Research Journal of Engineering and Technology*, 10(08).
- Nisa, F., & Ramadona, S. (2023). Sistem Pencegahan Serangan *Distributed Denial of Service* Pada Jaringan SDN. *Jurnal Sistim Informasi Dan Teknologi*, 5(3), 22–30. <https://jsisfotek.org/index.php>
- Nisa, I. S., Saputro, R. M., Nugroho, T. F., & Lahitani, A. R. (2024). Analisis *Quality of Service* (Qos) Menggunakan Standar Parameter Tiphon Pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya. *Teknomatika: Jurnal Informatika Dan Komputer*, 17(1), 1–9. <https://doi.org/10.30989/Teknomatika.V17i1.1307>
- Nugroho, M. A., & Suwastika, N. A. (2018). Perancangan *Intrusion Prevention System* pada Jaringan *Software Defined Networks*. *JUMANJI (Jurnal Masyarakat Informatika Unjani)*, 2(1), 1. <https://doi.org/10.26874/Jumanji.V2i1.17>
- Paramita, R. W. D., Rizal, N., & Sulistyan, R. B. (2021). *Metode Penelitian Kuantitatif* (3 Ed.). Widya Gama Press.
- Perwira, R. I., Fauziah, Y., Mahendra, I. P. R., Prasetyo, D. B., & Simanjuntak, O. S. (2019). *Anomaly-Based Intrusion Detection and Prevention Using Adaptive Boosting in Software-Defined Network*. *2019 5th International Conference on Science in Information Technology (Icsitech)*, 188–192. <https://doi.org/10.1109/Icsitech46713.2019.8987531>
- Prabowo, W. A., Fauziah, K., Nahrowi, A. S., Faiz, M. N., & Muhammad, A. W. (2023). *Strengthening Network Security: Evaluation Of Intrusion Detection and Prevention Systems Tools in Networking Systems*. *International Journal of Advanced Computer Science and Applications*, 14(9). <https://doi.org/10.14569/IJACSA.2023.0140934>
- Pratama, M. P., & Trisnawan, P. H. (2022). Sistem Pendeteksi DDoS Menggunakan Algoritma CUSUM Pada Openflow SDN. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 6(5), 2495–2506. <http://j-ptiik.ub.ac.id>

- Quingueni, A. M., & Kitsuwani, N. (2019). *Reduction of Traffic Between Switches and IDS For Prevention of Dos Attack in SDN*. 2019 19th International Symposium on Communications and Information Technologies (ISCIT), 277–281. <https://doi.org/10.1109/ISCIT.2019.8905165>
- Rahmawan, A. D., & Risqiwati, D. (2020). Analisa Performa *Controller* Pada Arsitektur Jaringan *Software Defined Network* (SDN). *Jurnal Repositor*, 2(12), 1727–1738.
- Ramdhan, M. (2021). *Metode Penelitian*.
https://scholar.google.com/citations?view_op=view_citation&hl=id&user=v9rt8tuaaaaj&citation_for_view=v9rt8tuaaaaj:wbdj-copyuoc
- Sari, I., Muh Yamin, & LM. Fid Aksara. (2019). Sistem Monitoring Serangan Jaringan Komputer Berbasis *Web Service* Menggunakan Honeypot Sebagai Intrusion Prevention System. *Semantik*, 5(1).
<https://doi.org/10.5281/ZENODO.2651714>
- Snort—Network Intrusion Detection & Prevention System*. (2023).
<https://www.snort.org/>
- Suwanto, R., Ruslianto, I., & Diponegoro, M. (2019). Implementasi *Intrusion Prevention System* (IPS) Menggunakan Snort dan Iptable Pada Monitoring Jaringan Lokal Berbasis Website. *Coding Jurnal Komputer Dan Aplikasi*, 7(01), 97–107. <https://doi.org/10.26418/coding.v7i01.32690>
- Syahputra, M. Q., Akbi, D. R., & Risqiwati, D. (2020). Deteksi dan Mitigasi Serangan DDoS Pada *Software Defined Network* Menggunakan Algoritma Decision Tree. *Jurnal Repositor*, 2(11), 1491.
<https://doi.org/10.22219/repositor.v2i11.795>
- Tanang Anugrah, F., Ikhwan, S., & Gusti A.G, J. (2022). Implementasi *Intrusion Prevention System* (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. *Techné: Jurnal Ilmiah Elektroteknika*, 21(2), 199–210.
<https://doi.org/10.31358/techne.v21i2.320>
- Thomas, T. (2005). *Network Security First-Step* (1 Ed.). Andi Offset.
- Yasin, A. (2020). Simulasi Serangan *Distributed Denial of Service* (DDoS) Di *Software-Defined Network* Di Simulasi Jaringan Mininet Dan Gns3. *Jurnal Teknologi Informasi Indonesia*, 05(01), 32–41.
<https://doi.org/10.30869/jtii.v5i1.927>
- Yudhana, A., Riadi, I., & Suharti, S. (2021). *Distributed Denial of Service* (DDoS) Analysis on Virtual Network and Real Network Traffic. *Journal Of Informatics and Telecommunication Engineering*, 5(1), 112–121.
<https://doi.org/10.31289/jite.v5i1.5344>