MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

Disusun oleh

OKTAVIANA NOVIA BARUNG

21.83.0635

Kepada

FAKULITAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

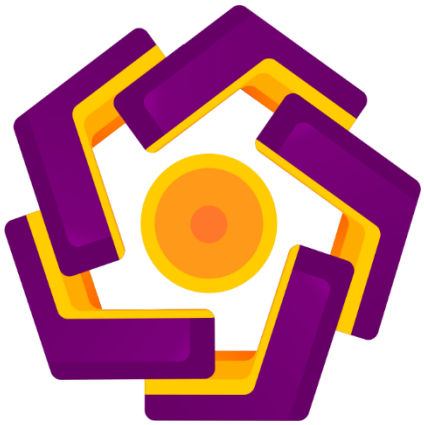
2026

MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer



disusun oleh

OKTAVIANA NOVIA BARUNG

21.83.0635

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PENGESAHAN

SKRIPSI

MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

Yang disusun dan diajukan oleh

Oktaviana Novia Barung
21.83.0635

telah disetujui oleh Wahid Miftahul Ashari, S.Kom., M.T
pada tanggal 20 April 2026

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

MITIGASI SERANGAN DDOS PADA *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

Yang disusun dan diajukan oleh

Oktaviana Novia Barung

21.83.0635

Telah dipertahankan di depan dewan penguji
pada tanggal 20 April 2026

Susunan Dewan Penguji

Nama penguji	Tanda tangan
Senie Destya, S.T., M.Kom. **NIK.190302312**	
Jeki Kuswanto, S.kom., M.Kom. **NIK. 190302456**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK.190302452**	

Skripsi ini telah diterima sebagai salah satu
persaryatan untuk memperoleh gelar Sarjana Komputer
tanggal 20 april 2025

DEKAN FAKULITAS ILMU KOMPUTER

Prof. Dr. Kursini, M.Kom.
NIK. 190302106

HALAMANA PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Oktaviana Novia Barung

NIM : 21.83.0635

Menyatakan bahwa Skripsi dengan judul berikut:

Mitigasi Serangan DDoS Pada Jaringan *Software Defined Networking* (SDN) Menggunakan IDS, Firewall, dan Load Balancing.

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 April 2026

Yang Menyatakan,

Oktaviana Novia Barung

HALAMAN PERSEBAHAN

Dengan penuh rasa syukur kehadirat Tuhan yang Maha Esa atas berkat dan rahmatnya, karya sederhana ini saya persembahkan kepada orang yang telah mendukung, membimbing, dan menyemangati dalam peroses penyelesaian skripsi ini. Oleh karena itu, dengan penuh rasa hormat dan terima kasi, laporan ini penulis persembahkan kepada:

1. Papa, Mama, dan adiku, terima kasih atas doa yang tidak pernah terputus, kasih sayang yang selalu menguatkan, serta pengorbanan yang tak terhingga. Segala pencapaian ini tidak lepas dari dukungan dan kepercayaan yang diberikan kepada saya.
2. keluarga besar, terima kasih atas perhatian, dukungan, dan motivasi yang diberikan
3. Bapak Wahid Miftahul Ashari, S.Kom., M.T. selaku dosen pembimbing saya, terima kasih telah memimbing dengan sabar, memberikan arahan, serta meluangkan waktu dan perhatian selama peroses penyusunan skripsi ini.
4. Untuk teman-teman saya, terima kasih karena selalu ada dalam setiap peroses, baik saat tertawa maupun saat Lelah. Kebersamaan, dukungan, dan kepedulian yang kalian berikan membuat perjalanan ini terasa lebih ringan.
5. Dan kepada idola saya Bangtan, terima kasih atas karya dan pesan-pesan yang disampaikan untuk selalu percaya pada peroses, menerima kekurangan diri, dan tetap melangkah meskipun tidak selaluh muda.

KATA PENGANTAR

Puji dan Syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala Rahmat dan karunianya sehingga penulis dapat menyelesaikan penelitian ini dengan baik. Penelitian yang berjudul "Mitigasi Serangan DDoS Pada Jaringan Software Defined Networking (SDN)" ini disusun sebagai salah satu syarat untuk memperolrh gelar sarjana pada program studi Teknik Komputer, Fakulitas Ilmu Komputer, Universitas Amikom Yogyakarta.

Dalam peroses penyusunan skripsi ini, penulis menyadari bahwa tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak, skripsi ini tidak akan dapat terselesaikan dengan baik. Oleh karena itu, pada kesempatan ini penulis menyampaikan terima kasih kepada:

1. Kedua orang tua tercinta atas doa, kasih sayang, pengorbanan, serta dukungan yang tiada henti.
2. Bapak Wahid Miftahul Ashari, S.Kom., M.T, selaku dosen pemimbing yang telah meluangkan waktu, memberi arahan, serta bimbingan yang diberikan dalam peroses penelitian dan penyusunan skripsi ini.
3. Seluruh dosen program studi Teknik Komputer, Fakulitas Ilmu Komputer, Universitas Amikom Yogyakarta, atas ilmu dan arahan yang telah diberikan selama masa perkuliahan.
4. Teman-teman seperjuangan yang memberikan dukungan, kerja sama, dan motivasi yang diberikan selama peroses perkuliahan dan penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari semputna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan dan penyempurnaan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta berkontribusi dalam pengembagan ilmu pengetahuan, khususnya di bidang keamanan keamanan siber.

Yogyakarta, 20 April 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

DDoS	Distributed Denial of Service
SDN	Software Defined Networking
IDS	Intrusion Detection System
QoS	Quality of Service

DAFTAR ISTILAH

- SDN (Software Defined Networking)
  Arsitektur jaringan yang memisahkan control plane dari data plane dalam perangkat keras, menjadikan terpusat dan dapat deprogram melalui perangkat lunak.
- DDoS (Distributed Denial of Service)
  Serangan siber dengan tujuan membanjiri target dengan lalu lintas berbahaya
- IDS (Intrusion Detection System)
  System keamanan yang memantau lalu lintas jaringan atau perangkat untuk mendeteksi aktivitas berbahaya, mencurigakan, atau pelangaran kebijakan.
- QoS (Quality of Service)
  Teknologi manajemen lalu lintas jaringan yang meprioritaskan data untuk menjamin kinerja yang andal

INTISARI

Serangan Distributed Denial of Service (DDoS) pada Software Defined Network (SDN) menjadi ancaman yang signifikan karena dapat mengganggu ketersediaan layanan serta menurunkan keandalan infrastruktur jaringan. Salah satu bentuk serangan yang umum terjadi adalah ICMP Flood, yaitu serangan yang membanjiri target dengan paket ICMP dalam jumlah besar sehingga sumber daya jaringan tidak mampu melayani permintaan pengguna secara normal. Pada arsitektur SDN, kondisi ini berpotensi memberikan dampak lebih besar karena controller berperan sebagai pusat pengendalian jaringan. Oleh karena itu, diperlukan mekanisme deteksi dan mitigasi yang mampu menjaga stabilitas jaringan serta meminimalkan dampak serangan terhadap kualitas layanan.

Penelitian ini mengimplementasikan mekanisme mitigasi serangan DDoS pada jaringan SDN dengan mengintegrasikan Intrusion Detection System (IDS), firewall, dan load balancing pada Ryu Controller. Simulasi dilakukan menggunakan Mininet dengan tiga skenario pengujian, yaitu kondisi normal, saat serangan ICMP Flood berlangsung, dan setelah mitigasi diaktifkan. Parameter evaluasi yang digunakan meliputi packet loss, delay, jitter, dan throughput. Hasil pengujian menunjukkan bahwa serangan menyebabkan peningkatan signifikan pada delay, jitter, throughput menurun, serta packet loss mencapai lebih dari 33.6%. Setelah mekanisme mitigasi diaktifkan, nilai delay dan jitter menurun secara signifikan, nilai throughput naik dan packet loss kembali 0%, sehingga performa jaringan kembali stabil. Dengan demikian, mekanisme mitigasi yang diterapkan terbukti efektif dalam mengurangi dampak serangan DDoS pada jaringan SDN.

Kata Kunci: DDoS, SDN, mitigasi, mininet, Icmp Flood

ABSTRACT

Distributed Denial of Service (DDoS) attacks on Software-Defined Networks (SDNs) pose a significant threat because they can disrupt service availability and reduce the reliability of network infrastructure. One common form of attack is the ICMP Flood, which floods a target with a large number of ICMP packets, rendering network resources unable to properly serve user requests. In an SDN architecture, this situation has the potential to have a greater impact because the controller acts as the central control center of the network. Therefore, detection and mitigation mechanisms are needed to maintain network stability and minimize the impact of attacks on service quality.

This study implemented a DDoS attack mitigation mechanism on an SDN network by integrating an Intrusion Detection System (IDS), firewall, and load balancing into the Ryu Controller. Simulations were conducted using Mininet with three test scenarios: normal conditions, during an ICMP Flood attack, and after mitigation was activated. Evaluation parameters used included packet loss, delay, jitter, and throughput. The test results showed that the attack caused a significant increase in delay, jitter, decreased throughput, and packet loss of over 33.6%. After the mitigation mechanism was activated, delay and jitter values decreased significantly, throughput increased, and packet loss returned to 0%, stabilizing network performance. Thus, the implemented mitigation mechanism proved effective in mitigating the impact of DDoS attacks on SDN networks.

Keyword: DDoS, SDN, mitigation, mininet, Icmp Flood