Mitigasi *Distributed Denial of Service* (DDoS) *Attack* Pada Arsitektur *Software Defined Network* (SDN)

Mitigation of Distributed Denial of Service (DDoS) Attacks on Software Defined Network (SDN) Architecture

Tamsir Ariyadi[1], Aan Restu Mukti[2], Heru Saputra[3]
Teknik Komputer, Universitas Bina Darma Palembang[1,3]
Teknik Informatika, Universitas Bina Darma Palembang[2]
Email: tamsirariyadi@binadarma.ac.id[1], aanrestu@binadarma.ac.id[2], apodiokau12@gmail.com[3]

Abstrak

Mitigasi adalah langkah-langkah sebuah usaha yang dilakukan untuk mengurangi suatu resiko. Pada era globalisasi perkembangan teknologi informasi telah semakin canggih dan berkembang sangat pesat serta keamanan jaringan komputer begitu penting untuk diterapkan dalam teknologi informasi, dimana keamanan jaringan digunakan untuk mengidentifikasi *user* ilegal dalam *computer network*. *SDN (Software Defined Networking)* adalah teknologi yang dapat membantu mengelola serta memelihara jaringan secara terprogram untuk meningkatkan kinerja dan monitoring jaringan. *Arsitekur Software Defined Networking* menerapkan desain manajemen jaringan yang memisahkan control plane dari data plane yang bertujuan untuk memprogram perangkat secara terpusat. Terlepas dari keunggulan yang dimiliki SDN ada masalah yang harus diperhatikan yaitu serangan *DDoS Attack.* Penelitian ini bertujuan untuk melakukan mitigasi terhadap serangan DDoS untuk arsitektur SDN pada Jaringan *Wireless.* Serangan yang digunakan adalah serangan *Ping of Death* dan pengujian dilakukan dengan membandingkan hasil *traffic* saat tidak menjalankan aturan mitigasi dan menjalankan aturan mitigasi. Hasil pengujian dengan tidak menjalankan aturan mitigasi, rata-rata jumlah packet yang masuk yaitu 1.021M dan ketika menjalankan aturan mitigasi rata-rata jumlah packet menurun menjadi 8.34K.

Kata kunci: Mitigasi, *DDoS Attack* dan Arsitektur SDN

Abstract

Mitigation is an effort taken to reduce a risk. In the era of globalization, the development of information technology has become increasingly sophisticated and growing very rapidly and computer network security is so important to be applied in information technology, where network security is used to identify illegal users in computer networks. SDN (Software Defined Networking) is a technology that can help manage and maintain a network programmatically to improve network performance and monitoring. The Software Defined Networking architecture implements a network management design that separates the control plane from the data plane for the purpose of centrally programming devices. Apart from the advantages that SDN has, there is a problem that must be considered, namely DDoS Attacks. This study aims to mitigate against DDoS attacks for SDN architecture on Wireless Networks. The attack used is the Ping of Death attack and the test is carried out by comparing the traffic results when not running the mitigation rules and running the mitigation rules. The test results by not running the mitigation rules, the average number of incoming packets is 1.021M and when running the mitigation rules the average number of packets decreases to 8.34K.

Keywords: Mitigation, DDoS Attack, SDN Architecture.

1. PENDAHULUAN

Mitigasi adalah langkah-langkah sebuah usaha yang dilakukan untuk mengurangi suatu resiko atau upaya untuk melakukan drop serta dampak dari akibat seerangkaian peristiwa yang terjadi. Mitigasi serangan DDoS bertujuan untuk mengukur waktu yang dibutuhkan oleh sistem dalam melakukan mitigasi atau menanggulangi berbagai jenis serangan DDoS[1].

Pada era globalisasi perkembangan teknologi informasi telah semakin canggih dan berkembang sangat pesat serta menuntut kecepatan arus informasi. Setelah menjadi kebutuhan utama, kebutuhan akan informasi telah menjadi kebutuhan penting dalam pengguna, serta Keamanan jaringan komputer begitu penting untuk diterapkan dalam teknologi informasi, dimana keamanan jaringan digunakan untuk mengidentifikasi *user* illegal akses terhadap *computer network*. *Computer Network* merupakan kebutuhan agar proses komunikasi data dapat terjadi sehingga menghasilkan adanya *sending and receiver*. *Computer network* terdapat celah keamanan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab atau biasa disebut *cyber security*, kejadian-kejadian yang tidak dapat diprediksi yang akan menyebabkan *server down*[2].

Software Defined Networking (SDN) adalah konsep yang muncul yang memelihara dan menganalisis status jaringan dengan arsitektur terpusatnya. Fasilitas ini memastikan operator jaringan untuk memantau dan mengelola elemen-elemen jaringan dengan aplikasi khusus yang berjalan pada satu atau beberapa pengontrol[3]. SDN *(Software Defined Networking*) adalah teknologi yang dapat membantu mengelola dan memelihara jaringan secara terprogram untuk meningkatkan kinerja dan monitoring jaringan. Jaringan yang dibuat oleh SDN sangat kompleks, tetapi jaringan yang diperlukan untuk mengembangkan aplikasi memerlukan kemampuan yang fleksibel dan mudah dipantau, serta tugas *forwarding* dan *routing* dipisahkan, Arsitekur *Software Defined Networking* menerapkan konsep melakukan pemisahan kontrol *plane* dan data *plane* pada *router* atau *switch* tujuan dari Arsitektur *Software Defined Networking* adalah membentuk jaringan lebih fleksibilitas dan kemudahan mengontrol jaringan jika terjadi perubahan pada *business requirement*[4].

DDoS attack adalah serangan cyber di mana lalu lintas palsu terus dikirim ke *server* atau sistem, *server* tidak dapat menangani semua lalu lintas dan *server* atau sistem menjadi *down*, serta tujuan dari serangan DDoS adalah untuk membuat sistem target tidak dapat diakses atau untuk meminta layanan. Serangan *Distributed Denial of Service* (DDoS) telah sangat mengganggu ketersediaan jaringan selama beberapa dekade dan masih belum ada mekanisme pertahanan yang efektif untuk melawannya[5].

Wireless network adalah bagian dari solusi yang paling baik terhadap perancangan *network komputer* bias diakses dimanapun dan kapanpun. Beberapa perusahaan atau organisasi menganggap *wireless* sebagai pendukung jaringan komputer yang memakai system analog, Dalam implementasinya *wireless* tersebut tetap menggunakan sistem kabel sebagai *backbone*, yang bertujuan agar pengguna layanan bisa melakukan akses *internet* dan *browsing*. Permasalahan dari pemakaian kabel ialah *backbone* ini dapat menjadi hambatan yang pada tempat-tempat yang sulit dijangkau oleh kabel. *Wireless Network* memiliki manfaat seperti mudah dan bias diakses kapanpun serta nyaman untuk digunakan. Bila dalam satu jaringan tersebut maka bisa melakukan koneksi setiap waktu yang diinginkan[6]. *Wireless network* ialah kumpulan beberapa komputer terkoneksi antar satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Pada dasarnya *wireless* dengan LAN merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainnya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika LAN masih menggunakan kabel sebagai media lintas data, sedangkan *wireless* menggunakan media gelombang radio[7].

Berdasarkan hasil yang didapat melalui observasi. Permasalahan yang ada di PT. Telkom Akses yaitu banjirnya lalu lintas *traffic* jaringan pada Gudang *Inventory*, inilah yang menyebabkan jaringan tidak bisa diakses oleh *user*, hal ini mengakibatkan aktivitas pekerjaan

dan penyimpanan data *asset* menjadi ternganggu, sehingga penggunaan *internet* menjadi *down* atau tidak bisa digunakan serta menjadi terganggu.

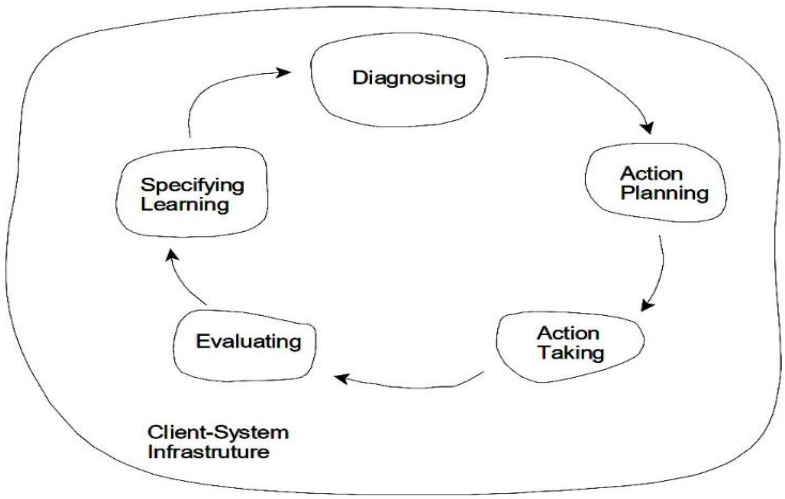
Dari permasalahan yang ada, salah satu solusi yang dapat dilakukan pada permasalahan yang terjadi pada Gudang *Inventory* Telkom Akses ialah menggunakan *firewall iptables*. Dengan adanya *firewall iptables* dapat mengamankan jaringan dengan melakukan penyaringan *traffic* pada *server*, sehingga aktivitas jaringan atau *server* di Gudang *Inventory* bisa digunakan dengan baik tanpa adanya gangguan.

Pada penelitian sebelumnya terkait serangan *Distributed Denial of Service* pada *Software Defined Network* (SDN) sebagai rujukan dari penelitian, terdapat lebih dari satu penelitian yang memiliki hubungan menurut A. Alshamrani (2017) mengemukakan bahwa ada celah yang rentan pada sistem komunikasi SDN. Kerentanan keamanan itu seperti *Misbehaviour attack* dan *NewFlow attack*. Kemudian melakukan mitigasi serangan dengan meneruskan *traffic* yang dikirim penyerang ke *honeypot* supaya serangan dapat dilakukan monitoring dan analisa. Berikutnya celah keamanan itu bisa dibuat untuk melakukan serangan terus menerus ke *traffic* pada SDN[8]. Lalu, dalam penelitian lainnya Dayal N, & Srivastava S. (2017) dilakukan penyerangan DDoS pada SDN. Serangan DDoS dilakukan agar bisa melihat dampak terhadap komponen SDN. Serangan dilakukan dengan sejumlah DDoS. *Research* ini menghasilkan parameter yang bisa dipakai agar dapat mendeteksi DDoS seperti IP *source*, address IP, dan protokol-protokol lainnya[9].

Berdasarkan uraian masalah dan penelitian terdahulu tersebut belum dibahas tentang mitigasi terhadap kepadatan lalu lintas jaringan SDN terutama fokus kepada arsitekturnya, Jaringan *Wireless* dan *Firewall Iptables* dari serangan DDoS. Kemudian penulis akan melakukan *research* ini dengan tema "*Mitigasi Distributed Denial of Service* (DDoS) *Attack* Pada Arsitektur *Software Defined Network* (SDN)" di jaringan *wireless*.

2. METODE PENELITIAN

Tahapan penelitian ini diuraikan agar pencariannya sistematis dan progresif. Agar rencana yang dijalankan dapat mencapai hasil yang baik dan mencapai keluaran agar bisa digunakan sebagai referensi untuk penelitian masa depan. Adapun tahapan-tahapan yang akan dilakukan yaitu diagnosis, pembuatan rencana tindakan, pelaksanaan tindakan, mengevaluasi dan melaksanakan pembelajaran.



Gambar 1. Tahapan Penelitian

Tahapan pertama yang akan dilakukan yaitu (*Diagnosing*) mencoba lakukan diagnosis permasalahan yang terdapat pada jaringan *wireless*. Adapun permasalahan yang ada pada jaringan *wireless* yaitu banjirnya lalu lintas *traffic* jaringan pada jaringan *wireless*. Lalu melanjutkan tahap tindakan (*Action Planning*) melakukan rencana tindakan dengan

mempersiapkan tindakan untuk melakukan mitigasi serangan DDoS yang menyebabkan banjirnya *traffic* pada jaringan *wireless.* Pada Tahapan ketiga yaitu tahap tindakan (*Action Taking*) melakukan mitigasi terhadap banjirnya *traffic* lalu lintas jaringan pada jaringan *wireless* yang disebabkan oleh serangan DDoS, Mitigasi dilakukan menggunakan *firewall iptables* yang berjalan pada *mininet*. Tahap ke empat (*Evaluating*) melakukan evaluasi terhadap tindakan yang telah dibuat, serta dilihat bagaimana hasil dari tindakan yang dilakukan yaitu mitigasi serangan DDoS *attack* untuk SDN pada jaringan *wireless*. Tahap terakhir yaitu (*Specifying Learning*) setelah mitigasi serta penerapan (Action Research) dianggap cukup maka berikutnya akan melakukan peninjauan ulang terhadap tahapan yang dilakukan.

2.1 *Mininet*

Mininet merupakan *emulator* untuk membuat prototipe cepat jaringan besar dengan sumber daya terbatas misalnya satu *computer*, laptop atau mesin *virtual*. *Mininet* dikembangkan untuk mendukung penelitian di bidang SDN dan *OpenFlow*. *Emulator mininet* memungkinkan anda untuk secara otomatis menjalankan kode ini secara interaktif di laptop atau perangkat keras *virtual* anda tanpa perubahan kode apa pun. dengan kata lain, kode simulasi persis sama dengan kode dilingkungan jaringan, *Mininet* adalah solusi yang disertakan ini dianggap yang terbaik dalam hal kegunaan, kinerja, akurasi dan skalabilitas serta dapat memberikan lingkungan (kenyamanan) yang realistis dan *Mininet* adalah jaringan sumber terbuka yang digunakan untuk penelitian SDN[10].

2.2 *Firewall Iptables*

Iptables salah satu *tools firewall* pada sistem operasi *linux*. Fungsi *iptables* mengamankan jaringan dengan melakukan penyaringan trafik pada *server*. Dengan *iptables*, anda dapat mengatur lau lintas jaringan termasuk mengizinkan atau memblokir koneksi yang masuk, keluar atau sekedar melewati *server*[11]. Pada *iptables* bisa membuat aturan pada *server* untuk mengelola jenis paket yang dapat diterima, mengatur trafik berdasarkan asal dan tujuan data, mengelola port serta lainnya, *Iptables* bekerja dengan membandingkan lau lintas jaringan dengan serangkaian aturan yang telah dibuat. Jadi, semua paket dalam lau lintas jaringan akan dicek serta dalam pengaturan paket, *iptables* memiliki beberapa tabel yang berfungsi untuk menentukan arah putaran data dan *iptables* memiliki kemampuan *firewall* yang dapat menangani beberapa jenis serangan bervolume tinggi. *Server* dengan sistem operasi *Linux* digunakan sebagai *server*[12].

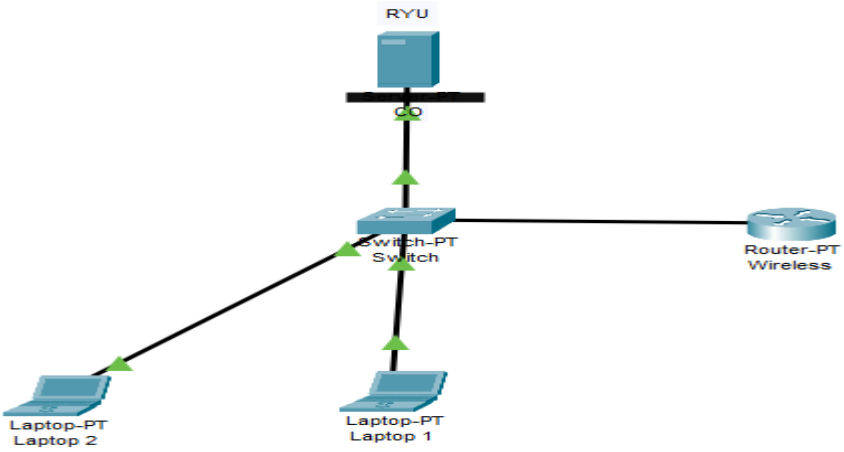
3. HASIL DAN PEMBAHASAN

Melakukan *literature review* yang berkaitan erat dengan permasalahan yang akan diteliti dari jurnal dan buku. Pada tahap ini peneliti melakukan diagnosa permasalahan yang terdapat pada jaringan *wireless* di Gudang Inventory PT. Telkom Akses Palembang. Adapun permasalahan yang ada di PT. Telkom Akses yaitu banjirnya lalu lintas *traffic* jaringan pada Gudang Inventory, inilah yang menyebabkan jaringan tidak bisa diakses oleh *user*, hal ini mengakibatkan aktivitas pekerjaan dan penyimpanan data *asset* menjadi ternganggu, sehingga penggunaan*internet* menjadi *down* atau tidak bisa digunakan serta menjadi ternganggu.

3.1 *Diagnosing* topologi jaringan *wireless*

Dari analisis yang dilakukan pada Jaringan *Wireless* Gudang Inventory PT. Telkom Akses saat ini menggunakan topologi jaringan *wireless*. Dimana jaringan ini tidak menggunakan kabel untuk bertukar informasi/ data dengan komputer lain melainkan menggunakan gelombang elektromagnetik untuk mengirimkan sinyal informasi data antar komputer satu dengan komputer lainnya.Gudang Inventory terdapat 1 *router wireless*, 2 laptop dan 1 *switch* dan pengontrol (*controller*) bertindak sebagai otak jaringan serta mengontrol perilaku seluruh jaringan. Mekanisme jaringan *wireless* pada Gudang Inventory PT. Telkom

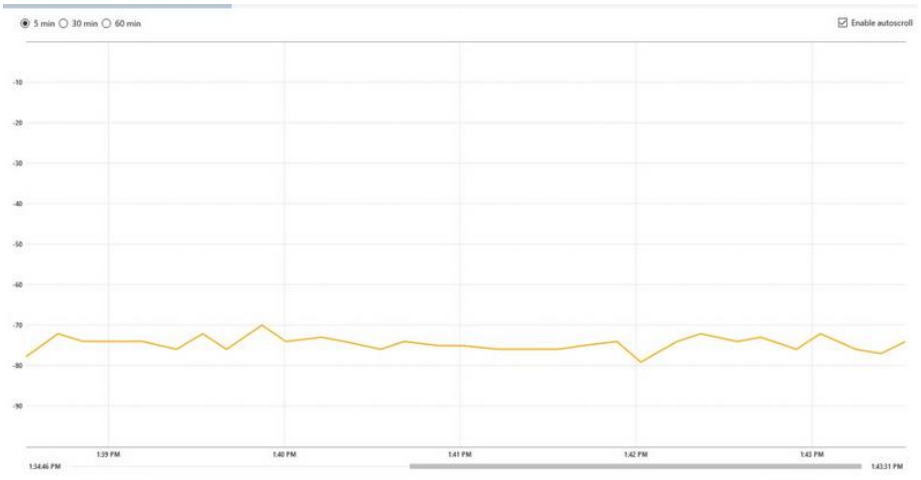
Akses adalah setiap para *staff* masing-masing menggunakan laptop yang terhubung ke jaringan *wireless*, pada umumnya situs yang sering diakses yaitu *WTMTA* dan *SAP*.



Gambar 2. Topologi Jaringan SDN

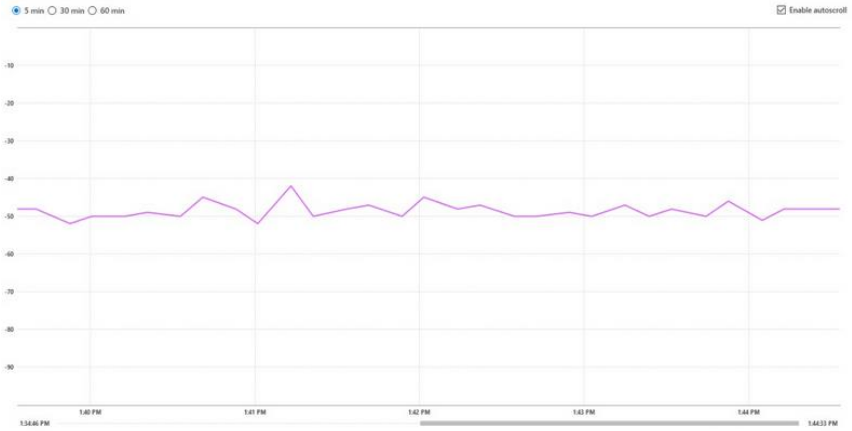
3.2 Diagnosing Traffic Jaringan *Wireless*

1. Pengecekan *traffic* di gudang *inventory* Telkom Akses, pengecekan pertama dilakukan pada jam 9 pagi dalam kurun waktu pengecekan selama 5 menit. Dari hasil pengecekan *traffic* tersebut bisa dilihat pada gambar 3 yang dimana *traffic* menunjukan bahwa *traffic* masih dalam keadaan cukup baik.



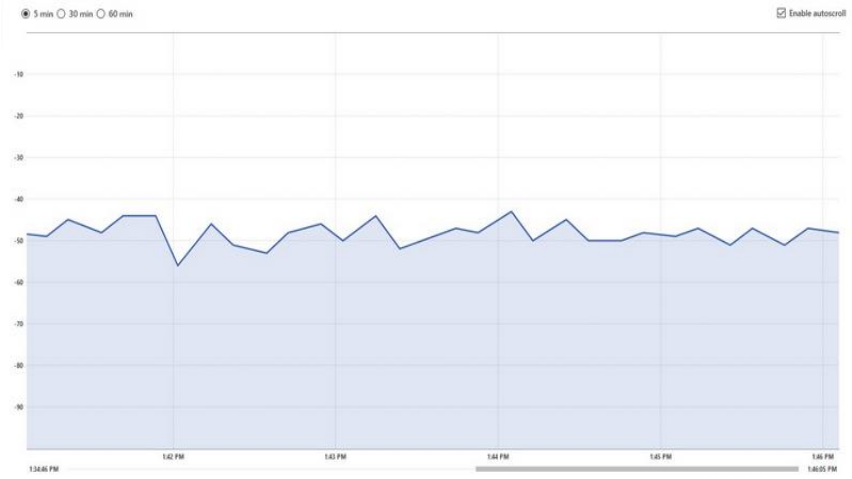
Gambar 3. *Traffic* Jaringan *Wireless*

2. Pada pengecekan *traffic* ke dua yang dilakukan pada waktu 12:30 sampai 12:35, pengecekan juga dilakukan dalam waktu 5 menit sama halnya yang dilakuan pada pengecekan pertama. Dari hasil pengecekan *traffic* kedua bisa dilihat pada gambar 4 yang dimana menunjukan bahwa *traffic* mengalami peningkatan dari *traffic* sebelumnya.



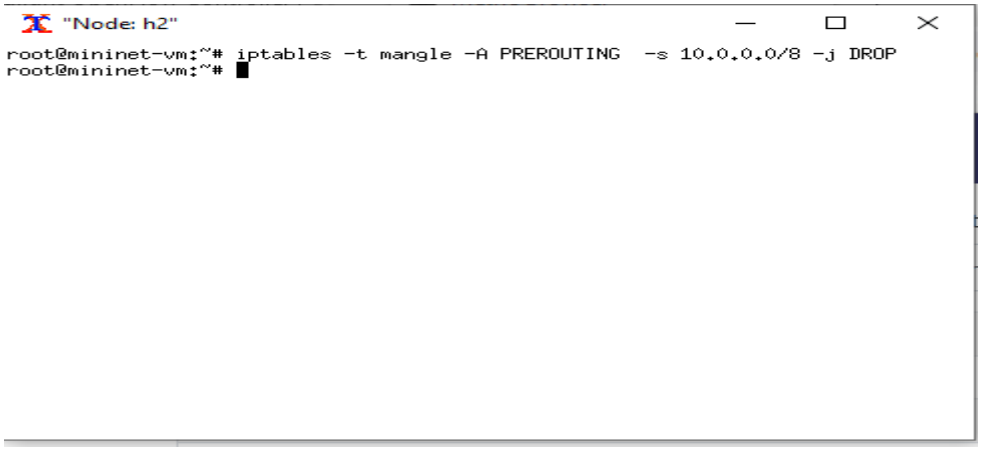
Gambar 4. *Traffic* Jaringan *Wireless*

3. Pada pengecekan *traffic* ke tiga yang dilakukan pada waktu 16:30 sampai 16:35, pengecekan juga dilakukan dalam waktu 5 menit sama halnya yang dilakuan pada pengecekan pertama dan kedua. Dari hasil pengecekan *traffic* ke tiga bisa dilihat pada gambar 5 yang dimana menunjukan bahwa *traffic* mengalami peningkatan dari *traffic* sebelumnya dan *traffic* lalu lintas mengalami kebanjiran.



Gambar 5. *Traffic* Jaringan *Wireless*

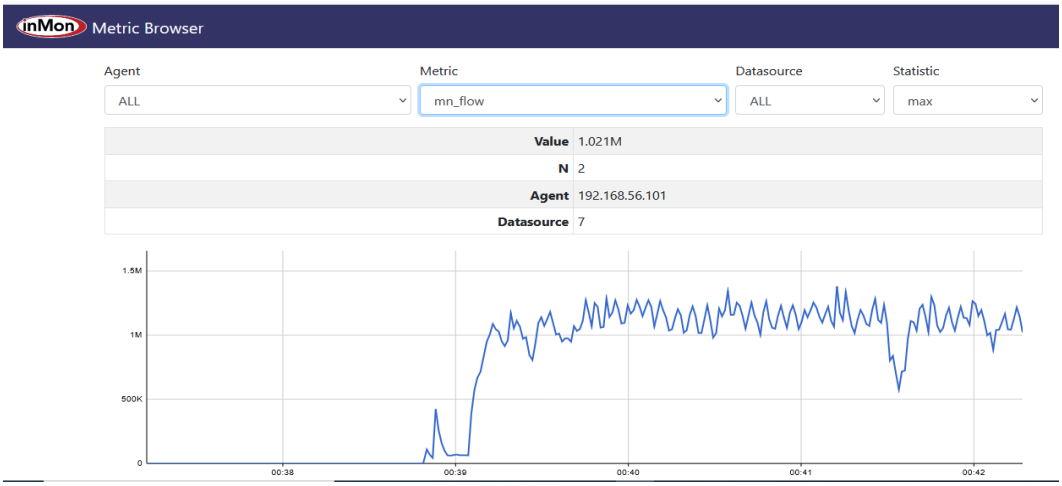
Setelah *mendiagnosis* pemulis melakukan rencana tindakan (*Action Planning*) dalam melakukan tahap tindakan penulis menggunakan *firewall iptables* untuk melakukan mitigasi serangan DDoS untuk arsitektur SDN. Dalam *firewall iptables* bisa mengidentifikasi, mengelola dan mitigasi. Hitung dan identifikasi jumlah paket masuk yang masuk ke pengontrol per detik, kelola *port*, dan terakhir mitigasi *port* dengan menetapkan aturan aliran prioritas pada pengontrol untuk memblokir *port* penyerang



Gambar 6. *Firewall Iptables*

Pada tahapan ketiga tahap tindakan (*Action Planning*) ini penulis melakukan tindakan terhadap banjirnya *traffic* lau lintas jaringan yang mengakibatkan para staf di gudang inventory Telkom Akses Palembang tidak bisa membuka *server* ataupun *system*. Terdapat dua Tindakan yang akan dilakukan yaitu setelah dimitigasi dan sebelum mitigasi serta mengukur jumlah paket yang masuk ke *controller* dan serangan yang digunakan yaitu ping of death. Serangan ping of death yang dilakukan menggunakan mininet yang berjalan di *VirtualBox*, dalam kurun waktu per 3 detik.

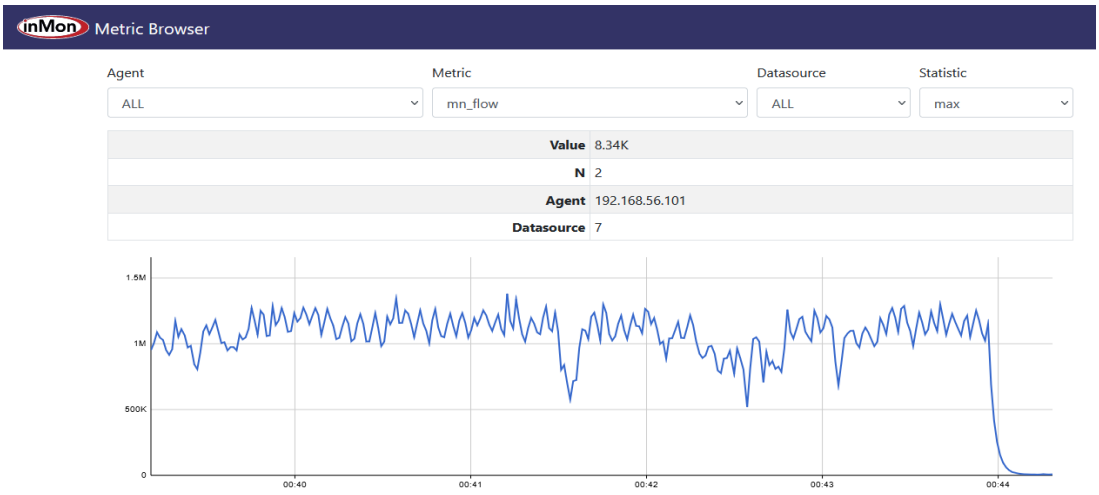
Pada tahap tindakan yang dilakukan penulis mendapatkan traffic pada *mn_flow* mengalami kebanjiran lalu lintas jaringan, dimana dari garis *traffic* lalu lintas jaringan tersebut terlihat melewati satu M (1M). *Traffic* mengalami penaikan serta penurunan jumlah paket per 3 detik mengalami perubahan serta bisa kita lihat pada gambar dibawah menyatakan nilai (*value)* 1.021, N 2, data *source* 7 serta dengan alamat ip 192.168.56.101.



Gambar 7. *Traffic* Sebelum Mitgasi

Pada gambar 8 merupakan gambar grafik untuk pengujian jumlah paket perdetik yang masuk ke controller. Dengan melakukan perbandingan antara sebelum dimitigasi dan setelah dimitigasi. Sebelum mitigasi dijalankan jumlah paket nilai (*value*) menyentuh 1.021M dan setelah dimitigasi jumlah nilai (*value*) mengalami penuruan tajam yaitu sebesar 8.34K, N 2, datasoource 7 serta dengan alamat ip 192.168.56.101. Pengunaan *firewall iptables* untuk

mitigasi serangan DDoS *Attack* untuk Arsitektur SDN sangat membantu dalam penurunan banjirnya *traffic* lalu lintas jaringan.



Gambar 8. *Traffic* Setelah Mitigasi

Hasil dari mitigasi DDoS attack untuk arsitektur SDN pada jaringan *wireless* yang dilakukan dengan menggunakan *mininet* yang berjalan di *VirtualBox, traffic* lalu lintas jaringan mengalami penurunan serta kenaikan per 3 detik. Ketika di mitigasi traffic mengalami penurunan yang signifikan. Sebelum dimitigasi jumlah paket serangan mencapai 1.021M dan setelah dimitigasi jumlah paket berkurang menjadi 8,34K. Pengunaan *Firewall Iptables* sangat membantu dalam penurunan *traffic* lalu lintas jaringan pada tampilan *mn_flow*, sehingga membuat informasi serta komunikasi menjadi lancar dan pengunaan jaringan *wireless* menjadi lancar tanpa adanya kendala.

Tabel 1 Jumlah Paket serangan DDoS

	Jumlah paket serangan DDoS
Firewall Iptables Tidak Dijalankan	1.021 M
Firewall Iptables Dijalankan	8. 34K

Tes fungsi sistem dilakukan untuk menentukan apakah persyaratan fungsi sistem terpenuhi dan dilakukan sesuai dengan spesifikasi fase tindakan yang dilakukan.

Tabel 2 Pengujian Fungsi Sistem

Pengujian	Hasil
Menambah *flow rule* di *switch*	Berhasil
Pengambilan data di *flow entries*	Berhasil
Pengunaan *Firewall Iptables*	Berhasil

4. KESIMPULAN DAN SARAN

Penelitian mitigasi serangan DDoS *Attack* untuk Arsitektur SDN dengan mengunakan firewall iptables dapat mengatur lau lintas jaringan termasuk mengizinkan atau memblokir koneksi yang masuk, keluar atau sekedar melewati server dan dari hasil pengujian yang dilakukan, didapatkan jumlah nilai (*value*) 1.021M sebelum mitigasi dan hasil nilai (value) setelah dimitigasi menjadi 8.34K. Saran untuk penelitian berikutnya dapat menggembangkan

lagi dalam hal mitigasi agar hasil lebih efektif serta dalam hal pengujian bisa menggunakan serangan yang lain tidak hanya serangan *ping of death*.

UCAPAN TERIMA KASIH

Kepada Semua pihak yang telah membantu dalam proses penelitian ini meliputi Dosen dan Mahasiswa program studi Teknik Komputer dan Teknik Informatika serta Terima kasih disampaikan kepada Tim TechnoCOM.

DAFTAR PUSTAKA

[1] J. Chris, J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software- Defined Network (SDN)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, 2019.

[2] T. Ariyadi, "Mitigasi Keamanan Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN)," *INOVTEK Polbeng - Seri Inform.*, vol. 3, no. 2, p. 147, 2018, doi: 10.35314/isi.v3i2.455.

[3] C. Toprak, C. Turker, and A. T. Erman, "Deteksi Serangan Kelaparan DHCP di Jaringan yang Ditentukan Perangkat Lunak," *UBMK 2018 - Konf. Int. ke-3 tentang Ilmu dan Tek. Komput.*, 2018.

[4] F. Ramadhan, R. Primananda, and W. Yahya, "Implementasi Routing Berbasis Algoritme Dijkstra Pada Software Defined Networking Menggunakan Kontroler Open Network Operating System," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer; Vol 2 No 7*, vol. 2, no. 7, 2018.

[5] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2019.2963077.

[6] nesabamedia.com, "Pengertian, Manfaat dan Macam-Macam Jaringan Komputer (Lengkap)," *Http://Www.Nesabamedia.Com/Pengertian-Manfaat-Dan-Macam-Macam-Jaringan-Komputer/*. 2017.

[7] M. Rusdan and M. Sabar, "Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication," *Jt. (Journal Inf. Technol.*, vol. 2, no. 1, 2020.

[8] A. Alshamrani, A. Chowdhary, S. Pisharody, D. Lu, and D. Huang, "A defense system for defeating DDoS attacks in SDN based networks," in *MobiWac 2017 - Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, Co-located with MSWiM 2017*, 2017. doi: 10.1145/3132062.3132074.

[9] N. Dayal and S. Srivastava, "An RBF-PSO based approach for early detection of DDoS attacks in SDN," in *2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018*, 2018, vol. 2018-January. doi: 10.1109/COMSNETS.2018.8328175.

[10] N. A. Faruqi, L. Nurwadi, N. Ismail, and D. Maryanto, "Simulasi Kinerja Berbagai Topologi Jaringan Berbasis Software-Defined Network (SDN)," *Senter*, vol. 3, 2017.

[11] T. Ariyadi and M. A. Prabowo, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," *INOVTEK Polbeng - Seri Inform.*, vol. 6, no. 1, p. 80, 2021, doi: 10.35314/isi.v6i1.1698.

[12] M. S. Hawari, "Penerapan Iptables Firewall Pada Linux Dengan Menggunakan Fedora," *J. Manaj. Inform.*, vol. 6, 2017.