Jurnal Jaringan Komputer dan Keamanan
JJKK, Vol. 02, No. 03, Oktober 2021: 55-59
Received: 5 Agustus 2021; Revised: 29 Sep 2021; Accepted: 30 Okt 2021

Mitigasi Serangan Distributed Denial of Service (DDoS) pada Arsitektur Software Defined Networking (SDN) Menggunakan Firewall Iptables

Heru Saputra

Program Studi Teknik Informatika
Universitas Bina Darma
email : herusaputra@gmail.com
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

Distributed Denial of Service (DDoS) attacks are one of the main threats to the availability of network services in the era of information technology globalization. Software Defined Networking (SDN) architecture offers the convenience of centralized network management, but on the other hand, it also has potential vulnerabilities to cyber attacks, especially DDoS. This study aims to mitigate DDoS attacks on SDN architecture in wireless networks using iptables firewall. The research method used is action research which includes the stages of diagnosis, action planning, action implementation, evaluation, and learning. The simulated attack is Ping of Death using mininet on a virtual machine. The test results show that before mitigation the number of attack packets reached 1,021 M packets per second, while after mitigation using iptables the number of packets decreased significantly to 8.34 K packets per second. Thus, the implementation of iptables firewall is proven effective in suppressing DDoS attack traffic on SDN architecture in wireless networks.

Kata kunci: *Mitigation; DDoS; Software Defined Networking; iptables; wireless networks.*

Abstrak

Serangan Distributed Denial of Service (DDoS) merupakan salah satu ancaman utama terhadap ketersediaan layanan jaringan pada era globalisasi teknologi informasi. Arsitektur Software Defined Networking (SDN) menawarkan kemudahan pengelolaan jaringan secara terpusat, namun di sisi lain juga memiliki potensi kerentanan terhadap serangan siber, khususnya DDoS. Penelitian ini bertujuan untuk melakukan mitigasi serangan DDoS pada arsitektur SDN di jaringan nirkabel menggunakan firewall iptables. Metode penelitian yang digunakan adalah action research yang meliputi tahapan diagnosis, perencanaan tindakan, pelaksanaan tindakan, evaluasi, dan pembelajaran. Serangan yang disimulasikan adalah Ping of Death menggunakan mininet pada mesin virtual. Hasil pengujian menunjukkan bahwa sebelum mitigasi jumlah paket serangan mencapai 1.021 M paket per detik, sedangkan setelah mitigasi menggunakan iptables jumlah paket menurun secara signifikan menjadi 8,34 K paket per detik. Dengan demikian, penerapan firewall iptables terbukti efektif dalam menekan lalu lintas serangan DDoS pada arsitektur SDN di jaringan nirkabel.

Kata kunci: *Mitigasi; DDoS; Software Defined Networking; iptables; jaringan nirkabel.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong hampir seluruh aktivitas organisasi bergantung pada jaringan komputer dan internet. Kemudahan akses, kecepatan pertukaran data, serta integrasi sistem informasi berbasis jaringan memberikan berbagai keuntungan bagi institusi dan perusahaan. Namun, di sisi lain, ketergantungan yang tinggi terhadap jaringan juga meningkatkan risiko keamanan siber secara signifikan (Stallings, 2018; Irianto & Negara, 2021). Jaringan komputer yang terhubung ke internet sangat rentan terhadap berbagai jenis serangan, baik yang bersifat pasif maupun aktif, yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan layanan.

Salah satu serangan siber yang paling berbahaya dan sering terjadi adalah Distributed Denial of Service (DDoS). Serangan ini bertujuan untuk melumpuhkan layanan jaringan dengan cara membanjiri server dengan lalu lintas palsu dalam jumlah sangat besar sehingga sumber daya sistem menjadi habis dan tidak mampu melayani pengguna yang sah (Mirkovic & Reiher, 2014; Behl & Behl, 2017). Dampak serangan DDoS tidak hanya berupa gangguan layanan, tetapi juga kerugian finansial, penurunan kepercayaan pengguna, serta terganggunya proses bisnis perusahaan (Kurniawan & Negara, 2020).

PT Telkom Akses Palembang, khususnya pada bagian gudang inventori, memanfaatkan jaringan nirkabel (wireless network) untuk mendukung aktivitas pertukaran informasi antara staf administrasi dan teknisi lapangan. Jaringan ini digunakan untuk akses sistem inventori, pelaporan pekerjaan, serta komunikasi internal. Namun, pada kondisi tertentu seperti saat terjadi peningkatan jumlah pengguna atau lalu lintas tidak wajar, jaringan mengalami lonjakan trafik yang mengakibatkan sistem menjadi tidak stabil, koneksi melambat, bahkan terhenti sama sekali. Kondisi ini mengindikasikan adanya potensi serangan DDoS yang dapat menghambat operasional gudang inventori.

Arsitektur Software Defined Networking (SDN) hadir sebagai paradigma baru dalam pengelolaan jaringan yang memisahkan control plane dan data plane, sehingga seluruh pengaturan jaringan dapat dikendalikan secara terpusat melalui controller (Kreutz et al., 2015). SDN menawarkan fleksibilitas, kemudahan konfigurasi, efisiensi pengelolaan, serta kemampuan otomasi yang lebih baik dibandingkan jaringan konvensional. Namun demikian, beberapa penelitian menunjukkan bahwa arsitektur SDN juga memiliki celah keamanan, terutama terhadap serangan DDoS yang dapat menargetkan controller maupun data plane (Scott-Hayward et al., 2016; Negara et al., 2022).

Masalah utama yang dihadapi pada jaringan gudang inventori PT Telkom Akses adalah terjadinya banjir lalu lintas akibat serangan DDoS yang mengganggu akses server dan sistem informasi. Serangan ini menyebabkan penurunan kualitas layanan (quality of service), meningkatnya packet loss, serta bertambahnya waktu tunda (delay) jaringan. Oleh karena itu, dibutuhkan suatu mekanisme mitigasi yang andal, efektif, dan mudah diterapkan untuk meminimalkan dampak serangan DDoS pada infrastruktur jaringan berbasis SDN.

Salah satu metode mitigasi yang banyak digunakan dalam pengamanan jaringan adalah pemanfaatan firewall iptables. Iptables merupakan sistem packet filtering pada sistem operasi Linux yang mampu mengendalikan lalu lintas jaringan berdasarkan alamat IP, port, protokol, dan pola tertentu (Alamsyah & Negara, 2021; Barik et al., 2019). Dengan konfigurasi yang tepat, iptables mampu memblokir trafik mencurigakan sebelum mencapai sumber daya utama. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengimplementasikan teknik mitigasi serangan DDoS pada arsitektur SDN menggunakan firewall iptables guna meningkatkan keamanan dan kestabilan jaringan pada gudang inventori PT Telkom Akses Palembang.

2. METODOLOGI PENELITAN

Penelitian ini menggunakan pendekatan action research yang terdiri atas lima tahap utama, yaitu diagnosis, perencanaan tindakan (action planning), pelaksanaan tindakan (action taking), evaluasi (evaluating), dan pembelajaran (learning).

2.1 Diagnosis

Tahap diagnosis dilakukan dengan mengidentifikasi kondisi jaringan nirkabel di gudang inventori PT Telkom Akses. Hasil diagnosis menunjukkan bahwa jaringan mengalami lonjakan lalu lintas secara tidak wajar yang menyebabkan akses pengguna terhambat. Topologi jaringan menggunakan satu wireless router, dua unit laptop client, satu switch, dan satu controller yang berfungsi sebagai pengendali jaringan SDN.

2.2 Perencanaan Tindakan (Action Planning)

Pada tahap ini dirancang mekanisme mitigasi menggunakan firewall iptables. Proses mitigasi mencakup identifikasi jumlah paket yang masuk ke controller, pengelolaan port jaringan, dan pemblokiran lalu lintas berbahaya melalui aturan (rule) pada iptables.

2.3 Pelaksanaan Tindakan (Action Taking)

Simulasi serangan dilakukan menggunakan mininet yang dijalankan pada VirtualBox. Jenis serangan yang digunakan adalah Ping of Death dengan interval serangan setiap tiga detik. Pengujian dilakukan dengan dua kondisi, yaitu sebelum dan sesudah penerapan mitigasi menggunakan iptables.

2.4 Evaluasi

Evaluasi dilakukan dengan membandingkan jumlah paket yang masuk ke controller sebelum dan sesudah mitigasi. Data hasil pengujian dianalisis untuk mengetahui efektivitas firewall dalam menekan lalu lintas serangan.

2.5 Pembelajaran (Learning)

Tahap pembelajaran dilakukan untuk mengevaluasi keberhasilan penerapan mitigasi serta sebagai bahan perbaikan untuk penelitian selanjutnya.

3. HASIL DAN PEMBAHASAN

Hasil Monitoring Lalu Lintas Jaringan

Monitoring lalu lintas jaringan dilakukan pada tiga waktu yang berbeda. Hasil pemantauan menunjukkan peningkatan lalu lintas yang signifikan menjelang sore hari hingga terjadi kondisi banjir lalu lintas (traffic flooding).

Hasil Uji Serangan Sebelum Mitigasi

Pada kondisi sebelum mitigasi, jumlah paket serangan yang masuk ke controller mencapai nilai puncak sebesar 1.021 M paket per detik, yang menyebabkan layanan jaringan menjadi tidak stabil dan akses pengguna terganggu.

Hasil Uji Serangan Setelah Mitigasi

Setelah firewall iptables diaktifkan, jumlah paket serangan berhasil ditekan secara signifikan menjadi 8,34 K paket per detik, sehingga kinerja jaringan kembali stabil.

Hasil Pengujian Fungsi Sistem

Komponen yang Diuji	Hasil
Penambahan *flow rule* di *switch*	Berhasil
Pengambilan data *flow entries*	Berhasil
Penerapan firewall *iptables*	Berhasil

Pembahasan

Hasil penelitian membuktikan bahwa serangan DDoS memberikan dampak yang sangat signifikan terhadap kinerja jaringan, khususnya pada arsitektur SDN yang terpusat pada controller. Lonjakan paket hingga mencapai lebih dari satu miliar paket per detik berpotensi melumpuhkan seluruh layanan jaringan.

Penerapan firewall iptables sebagai mekanisme mitigasi terbukti mampu menurunkan jumlah paket serangan secara drastis. Penurunan dari 1.021 M menjadi 8,34 K paket per detik menunjukkan tingkat efektivitas yang sangat tinggi. Hal ini membuktikan bahwa iptables mampu melakukan pemfilteran lalu lintas secara efisien dan memblokir sumber serangan berdasarkan aturan yang ditentukan.

Selain itu, hasil pengujian fungsional menunjukkan bahwa seluruh komponen sistem berjalan sesuai spesifikasi. Dengan demikian, metode mitigasi ini layak diterapkan sebagai solusi pengamanan jaringan SDN terhadap serangan DDoS.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa: Serangan DDoS pada arsitektur SDN dapat menyebabkan lonjakan lalu lintas jaringan yang sangat besar dan mengganggu ketersediaan layanan.Firewall iptables mampu melakukan mitigasi serangan secara efektif dengan menurunkan jumlah paket serangan dari 1.021 M menjadi 8,34 K paket per detik.Implementasi iptables pada lingkungan SDN berbasis jaringan nirkabel terbukti meningkatkan stabilitas dan keamanan jaringan.Metode ini layak digunakan sebagai solusi mitigasi DDoS pada infrastruktur jaringan berbasis SDN.

Referensi

Alamsyah, R., & Negara, E. S. (2021). Analisis Implementasi Firewall Iptables untuk Keamanan Jaringan. Jurnal Teknologi Informasi dan Komunikasi.

Behl, A., & Behl, K. (2017). Cyberwar: The Next Threat to National Security and What to Do About It. Oxford University Press.

Barik, R. K., Dubey, H., & Mankodiya, K. (2019). Security in SDN Using Iptables-Based Firewall. International Journal of Network Security.

Irianto, D., & Negara, E. S. (2021). Manajemen Keamanan Jaringan pada Infrastruktur Enterprise. Jurnal Sistem Informasi.

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14–76.

Kurniawan, R., & Negara, E. S. (2020). Analisis Serangan Distributed Denial of Service pada Jaringan Komputer. Jurnal Keamanan Siber Indonesia.

Mirkovic, J., & Reiher, P. (2014). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review.
Negara, E. S., Surya, R., & Hidayat, M. (2022). Security Threats and Mitigation Techniques in Software Defined Networking. International Journal of Computer Networks.
Scott-Hayward, C., O'Callaghan, G., & Sezer, S. (2016). SDN Security: A Survey. IEEE SDN for Future Networks and Services.
Stallings, W. (2018). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education.