Pengujian Serangan *UDP Flood* di Jaringan *Software-Defined* pada *GNS3*

Alimuddin Yasin¹
Program Studi Teknik Informatika
Politeknik Gorontalo
alimuddiny@poligon.ac.id

Salman Suleman²
Program Studi Teknik Informatika
Politeknik Gorontalo
salman@poligon.ac.id

Abstract— *Software Defined Network (SDN) adalah teknologi baru dalam jaringan komputer. Dimana dalam arsitektur ini control plane terpisah dengan data plane. Controller sebagai control plane dan switch sebagai data plane yang dihubungkan oleh protokol openflow. Teknologi ini masih dalam tahap pengembangan sehingga isu keamanan masih terbuka lebar untuk diteliti terlebih serangan dampak Distributed Denial of Service (DDoS) pada switch openflow. Untuk mensimulasikan serangan DDoS di jaringan SDN dipilih software simulator GNS3 untuk mensimulasikan arsitektur jaringan SDN untuk menguji dampak serangan DDoS terhadap kualitas jaringan saat serangan DDoS terjadi. Serangan DDoS dapat mempengaruhi kualitas jaringan di Arsitektur jaringan SDN di GNS3 sehingga mengakibatkan switch openflow tidak dapat berfungsi sementara waktu.*

Kata kunci : DDoS, SDN, GNS3, Openflow

I. PENDAHULUAN

Pada masa sekarang ini arus informasi komputer yang berkembang dimasyarakat berkembang semakin cepat dan hampir menjadi kebutuhan yang sangat penting dalam kehidupan serta berjalan dengan sebuah kebutuhan manusia, sisi efisiensi, praktis serta murah dan sangat membantu untuk menyelesaikan pekerjaan. Begitu pula dengan perkembangan infrastruktur jaringan.

Saat ini infrastruktur jaringan komputer mengalami perkembangan. Arsitektur jaringan yang baru berbeda dengan arsitektur jaringan yang sebelumnya. Dimana dalam arsitektur jaringan sebelumnya Control plane dan data plane berada dalam satu perangkat yang sama. Sedangkan dalam Arsitektur jaringan yang baru *Control Plane* dan *Data Plane* tidak lagi berada dalam satu perangkat. Arsitektur ini disebut arsitektur *Software Defined Network (SDN)*. Dalam Arsitektur *SDN* yang bertugas sebagai *Control Plane* adalah *SDN Controller* yang secara terpusat dapat mengendalikan *data plan* yang berada di *Switch Openflow* dengan perantara protokol *openflow*. *Openflow* adalah protokol dari *SDN* yang digunakan dalam mengakses jaringan dengan *Software* khusus yang menyediakan *Application Programming Interface (API)* terhadap tabel *forwarding* dari *switch* yang berasal dari vendor yang berbeda [1].

Isu keamanan jaringan pada jaringan *SDN* masih terbuka lebar untuk diteliti. Salah satunya adalah Dampak

serangan *Distributed denial-of-service (DDoS)* di dalam jaringan *SDN*. *DDoS* adalah serangan untuk membanjiri jaringan dengan data (*flooding*) sehingga *host* atau *service* menjadi tak dapat diakses oleh *user* yang berhak [2].

Dalam *paper* [3] mengemukakan *DDoS* dapat menyebabkan *controller* tidak dapat diakses oleh perangkat jaringan *SDN* dikarenakan tingginya trafik data yang menuju *controller* sehingga mengakibatkan jaringan *SDN* tidak dapat berfungsi.

Berdasarkan hasil penelitian tersebut dapat disimpulkan bahwa *controller* lebih rentan terhadap serangan *DDoS*. Tetapi muncul pertanyaan bagaimana dampak serangan *DDoS* dengan menggunakan Protokol *UDP (UDP Flood)* terhadap *Switch Openflow* di jaringan *SDN*?. Oleh karena itu penelitian ini akan meneliti dampak serangan *UDP Flood* Terhadap Kualitas Jaringan (*Delay* dan *Packet Lost*) pada *Switch Openflow* di jaringan *SDN* pada simulator *GNS3*.

UDP flood merupakan serangan yang bersifat *connectionless*, yaitu tidak memperhatikan apakah paket yang dikirim diterima atau tidak. *flood attack* akan menempel pada *servis UDP chargen* di salah satu mesin, yang untuk keperluan “percobaan” akan mengirimkan sekelompok karakter ke mesin lain, yang di program untuk menuliskan setiap kiriman karakter yang di terima melalui *servis chargen*. Karena paket *UDP* tersebut di *spoofing* antara ke dua mesin tersebut, maka yang terjadi adalah banjir tanpa henti kiriman karakter yang tidak berguna antara ke dua mesin tersebut. [4]

Salah satu *Network simulator* yang tersedia dan bebas digunakan adalah *GNS3 (graphical network simulator)* yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan *simulator* lainnya. [5] Aplikasi ini dapat di instal di berbagai sistem operasi yaitu *windows, linux* maupun *MacOS*.

Baik tidaknya layanan jaringan dapat diukur dengan metode Kualitas layanan jaringan atau *Quality of Service (QoS)* dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan jaringan [6].

Dalam mengirimkan data paket dengan besar 3 Mbyte di saat jaringan sepi waktu pengiriman adalah 5 menit tetapi pada saat jaringan sibuk sampai 15 menit, hal ini disebut *latency*. *Latency* pada saat jaringan sibuk berkisar 50 – 70 msec [7]. *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)* mengelompokkan *Delay/latency* menjadi empat kategori penurunan kinerja jaringan berdasarkan nilai *Delay* seperti terlihat pada Tabel 1. Berikut

kontroller dan server monitoring dengan perantara hub serta masing-masing switch memiliki dua buah host (Gambar 1)

Tabel 1. Performansi jaringan IP berdasarkan Latensi/Delay

Kategori Latensi	Besar Delay
Sangat Bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	> 450 ms

Jumlah paket yang hilang saat pengiriman paket data ke tujuan, kualitas terbaik pada saat LAN/WAN jika jumlah *losses* paling kecil [8] . Di dalam implementasi jaringan IP, nilai packet loss ini diharapkan minimum. Empat kategori penurunan performansi jaringan dengan versi TIPHON-Telecommunications and internet protocol harmonization over networks, terdapat pada Tabel 2 berikut.

Tabel 2. Performansi jaringan IP berdasarkan packet loss

Kategori Degradasi	Paket Loss
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Jelek	25%

II. METODOLOGI

- 1) Studi Literatur, Konfigurasi Dan Konsep
- 2) Rancangan Topologi Dan Skenario Serangan DDoS.
- 3) Instalasi dan Konfigurasi Kontroller,
- 4) Implementasi GNS3

Berikut langkah langkah dalam mengimplementasikan Software simulasi GNS3:

- a. Instalasi dan Konfigurasi *GNS3*
- b. Konfigurasi *OpenWRT*
- c. Implementasi Topologi
- d. Konfigurasi *Switch Openflow*
- e. Konfigurasi Host

- 5) Simulasi dan Pengujian Serangan UDP Flooding di Jaringan SDN
- 6) Pengujian Hasil Simulasi DDoS di GNS3
- 7) Mendokumentasikan Hasil

III. HASIL DAN PEMBAHASAN

- 1) Rancangan Topologi

Rancangan topologi yang digunakan yaitu topologi linear dimana terdapat dua buah *switch* yang saling terhubung satu sama lain. Dan masing masing switch terhubung ke

Gambar 1. Rancangan Topologi

Kontroller	= Melakukan kontrol terhadap kedua <i>switch</i> serta yang mengatur jaringan SDN
Monitoring Server	= Melakukan Monitorig jaringan yang berisi Software Monitoring Sflow
Openflow Switch	= Kedua Switch Openflow Terhubung terhubung satu sama lain dan memiliki masing masing 2 Host serta terhubung ke kontroller
Host	= Host yang terhubung pada Switch OpenFlow
	= Koneksi antar perangkat pada jaringan SDN
	= Koneksi dari kontroller ke switch dan ke monitoring server
	= Arah Serangan DDoS. Serangan dilakukan oleh host-1 pada Switch Openflow-1 ke Host-2 pada Switch Openflow-2

- 2) Pengujian *Delay* dan Packet Lost UDP Flood Attack di *GNS3*

Hasil pengujian simulasi serangan *UDPFlood* di Jaringan SDN pada jaringan SDN di GNS3 ditampilkan Tabel 3 dan Tabel 4.

Hasil pengukuran delay yang di presentasikan oleh Tabel 3 menunjukan UDP Flood yang dikirim sebanyak 80000 paket di *GNS3* menghasilkan *delay* rata-rata sebesar 729,263 ms. Besar *delay* tersebut masuk dalam kategori jelek jika melihat tabel performansi jaringan berdasarkan *delay* oleh *TIPHON*.

Packet lost (Tabel 4) yang diakibatkan oleh serangan UDP di GNS3 menghasilkan packet lost tertinggi sebesar 41% dengan sequence error 25 paket ICMP dari jumlah total paket ICMP 60 paket yang dihasilkan oleh Ping. Packet lost terjadi mulai ketika melakukan serangan UDP sebanyak 40000 paket dengan presentasi packet lost rata-rata sebesar 15 % dengan jumlah rata-rata sequens error 5 paket ICMP yang dihasilkan oleh Ping.

Tabel 3. Pengukuran Delay UDP Flood Attack di GNS3

Jumlah Paket	Delay	Percobaan Ke-			Total	Rata-Rata
		1	2	3		
Normal	Min	1,551	1,698	1,815	5,064	1,688
	Average	2,367	2,698	2,964	8,029	2,676
	Max	3,651	10,103	10,480	24,234	8,078
5000,000	Min	1,606	1,720	1,682	5,008	1,669
	Average	3,061	2,725	3,284	9,070	3,023
	Max	14,284	11,918	34,973	61,175	20,392
20000,000	Min	1,532	1,546	1,573	4,651	1,550
	Average	8,587	12,019	26,229	46,835	15,612
	Max	163,274	368,425	879,746	1411,445	470,482
40000,000	Min	1,710	1,496	1,867	5,073	1,691
	Average	230,767	406,345	74,822	711,934	237,311
	Max	3924,810	5943,296	2037,709	11905,815	3968,605
60000,000	Min	1,830	2,331	1,550	5,711	1,904
	Average	459,901	13,299	300,574	773,774	257,925
	Max	5151,032	216,657	4203,440	9571,129	3190,376
80000,000	Min	1,864	1,607	1,615	5,086	1,695
	Average	507,949	1672,061	7,780	2187,790	729,263
	Max	6616,038	13233,591	115,720	19965,349	6655,116
100000,000	Min	1,809	1,548	1,610	4,967	1,656
	Average	82,565	284,932	1350,499	1717,996	572,665
	Max	2171,915	4916,076	11835,629	18923,620	6307,873

Tabel 4. Pengukuran Packet Lost UDP Flood Attack di GNS3

Jumlah Serangan		Percobaan Ke-			Rata Rata
		1	2	3	
Normal	Seq Received	60	60	60	60
	Seq Error	0	0	0	0
	Packet Lost %	0	0	0	0
5000	Seq Received	60	60	60	60
	Seq Error	0	0	0	0
	Packet Lost %	0	0	0	0
20000	Seq Received	60	60	60	60
	Seq Error	0	0	4	0
	Packet Lost %	0	0	6	0
40000	Seq Received	50	52	55	51
	Seq Error	10	8	5	9
	Packet Lost %	16	13	8	15
60000	Seq Received	35	41	53	38
	Seq Error	25	19	7	22
	Packet Lost %	41	31	11	36
80000	Seq Received	51	57	51	54
	Seq Error	9	3	9	6
	Packet Lost %	15	5	15	10
100000	Seq Received	46	52	57	49
	Seq Error	14	8	3	11
	Packet Lost %	23	13	5	18

IV. KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan penelitian ini adalah :Serangan UDP Flood dapat mempengaruhi kualitas jaringan di Arsitektur jaringan SDN di GNS3 dimana pada saat pengiriman paket UDP Flood dengan jumlah paket yang dikirim sebanyak 6000 paket mengakibatkan kualitas jaringan menjadi jelek berdsarkan nilai delay pada TIPHON.

V. SARAN

Dalam penelitian selanjutnya disarankan untuk melakukan pengujian yang sama dengan menggunakan kontroller dan switch selain kontroller floodlight dan software switch OpenVSwitch, hasil yang berbeda bisa saja terjadi dibandingkan pada penelitian ini.

VI. DAFTAR PUSTAKA

- [1] Kartadie, Rikie, Ema Utami, and Eko Pramono, 2014, "Prototipe Infrastruktur Software-Defined Network Dengan Protokol Openflow Menggunakan Ubuntu Sebagai Kontroler," Jurnal Dasi, vol. Vol. 15 No. 1, Mar. 2014.
- [2] Yudha Purwanto, Kuspriyanto, Hendrawan, dan Budi Rahardjo, 2014, "Traffic Anomaly Detection in DDoS Flooding Attack," The 8th International Conference On Telecommunication System, Services, And Application
- [3] Dharma, N. I., et al., 2015, "Time-based DDoS detection and mitigation for SDN controller." Network Operations and Management Symposium (APNOMS), 2015 17th Asia-Pacific. IEEE, .
- [4] M. Masikos, O. Zouraraki C. Patrikakis. diakses tanggal 20/3/2016, Distributed Denial of Service Attacks -The Internet Protocol Journal- http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html
- [5] RedNectar Chris Welsh, 2013, GNS3 Network Simulation Guide. PACKT
- [6] Ferguson, P. & Huston, G. 1998. Quality of Service. John Wiley & Sons Inc
- [7] Santosa, B. 2004. Manajemen Bandwidth Internet dan Intranet.
- [8] ETSI, diakses tanggal 20 april 2016, TR 101 329 V2.1.1. 1999. Telecommunications and Internet Protocol harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS). <http://www.etsi.org>
- [9] Slickkitten. Diakses tanggal 30/12/2015. About OpenWRT. <http://wiki.openwrt.org/about/start>.