PENGUJIAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) DI JARINGAN SOFTWARE-DEFINED PADA GNS3

Alimuddin Yasin*[1], Ema Utami[2], Eko Pramono[3]
[1,2,3]Magister Teknik Informatika STMIK AMIKOM Yogyakarta
[51]Teknik Informatika Politeknik Gorontalo
E-mail: *[1]alimuddiny@poligon.ac.id, [2]ema.u@amikom.ac.id, [3]eko.p@amikom.ac.id

ABSTRAK

Software *Defined Network (SDN)* adalah teknologi baru dalam jaringan komputer. Dimana dalam arsitektur ini c*ontrol 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 *Distrubuted 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 serta penggunaan CPU dan RAM saat serangan DDoS terjadi. Serangan DDoS dapat mempengaruhi kualitas jaringan di Arsitektur jaringan SDN di GNS3 serta penggunaan *CPU* dan *RAM* pada switch openflow meningkat sehingga mengakitbatkan *switch openflow* tidak dapat berfungsi sementara waktu.

Kata Kunci: DDoS, SDN, GNS3, Openflow

A. PENDAHULUAN

Software *Defined Network (SDN)* arsitektur merupakan teknologi baru dalam jaringan komputer. Dengan *SDN* arsitektur, *control plane* terpisah dari *data plane* dimana *SDN Controler* bertindak sebagai *control plane* dan *switch* berfungsi menjalankan *data plane* yang berkomunikasi menggunakan protokol *Openflow* sehingga dalam melakukan manajemen jaringan secara terpusat. *Openflow* merupakan protokol dari *SDN* yang ditujukan untuk mengontrol akses jaringan dengan *software* khusus yang menyediakan *Application Programming Interface (API)* terhadap tabel *forwarding* dari *switch* yang berasal dari vendor yang berbeda [1].

Teknologi *SDN dan* protokol *Openflow* sampai saat ini masih dalam tahap pengembangan. Sehingga isu keamanan jaringan pada jaringan *openflow* masih terbuka lebar untuk diteliti. Salah satunya adalah dampak serangan *Distributed denial-of-service (DDoS)* terhadap jaringan *SDN*. *DDoS* merupakan bentuk serangan untuk membanjiri jaringan dengan data (*flooding)* yang membuat suatu *host* atau *service* menjadi tak dapat diakses oleh *user* yang berhak [2].

Dalam *paper* [3] mengemukakan bahwa tingginya paket berbahaya yang dihasilkan oleh *DDoS* dapat membanjiri *controller* sehingga membuat *controler* tidak dapat dijangkau oleh jaringan yang sah yang mengakibatkan jaringan *SDN* tidak dapat berfungsi. Peryataan yang sama juga di kemukakan dalam penelitian [4] yaitu salah satu kelemahan dari Arsitektur jaringan *SDN* dengan protokol *openflow* apabila *controler* tidak dapat diakses oleh perangkat jaringan melalui protokol *openflow* maka jaringan gagal bekerja. Salah satu penyebabnya kontroller

openflow tidak bisa beroperasi adalah serangan *DDoS* yang di tujukan ke Kontroler *SDN.*

Berdasarkan hasil dari dua penelitan tersebut dapat disimpulkan bahwa *controller* lebih rentan terhadap serangan *DDoS.* Tetapi muncul pertanyaan bagaimana dampak serangan *DDoS (TCP Syn Flood)* terhadap *Switch Openflow* di jaringan *SDN*?. Oleh karena itu penelitian ini akan meneliti dampak serangan *TCP Syn Flood* Terhadap Kualitas Jaringan (Delay dan Packet Lost) serta penggunaan CPU dan RAM dari Switch *Openflow* di jaringan *SDN* pada simulator GNS3.

SYN flooding attack adalah jenis serangan *Denial-of-service* yang menggunakan paket-paket *SYN*. Serangan ini melumpuhkan koneksi ke sebuah Server karena banyaknya paket yang masuk. Paket-paket *SYN* adalah salah satu jenis paket dalam protokol *Transmission Control Protocol (TCP/IP)* yang dapat digunakan untuk membuat koneksi antara dua host dan dikirimkan oleh *host* yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "*TCP Three-way Handshake*" [5]

GNS3 adalah sebuah program *graphical network simulator* yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan *simulator* lainnya. Program ini dapat dijalankan di berbagai sistem operasi, seperti Windows, Linux, atau Mac OS X. Untuk memungkinkan simulasi lengkap, GNS3 memiliki beberapa komponen [6] yaitu: *Dinamips*, Qemu, *VPCS.*

Kualitas layanan jaringan atau *Quality of Service (QoS)* merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu servis [7].

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 [8]. 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

Tabel 1. Performansi jaringan IP berdasarkan Latensi/Delay [9]

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. Secara umum terdapat empat kategori penurunan performansi jaringan dengan versi TIPHON-Telecomunications and internet protocol harmonization over networks, terdapat pada Tabel 2 berikut.

Tabel 2. Performansi jaringan IP berdasarkan packet loss [9]

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

B. METODE PENELITIAN

1) Studi Literatur, Konfigurasi Dan Konsep

Mengumpulkan bahan atau materi dari journal atau buku yang relevan yang dijadikan referensi dan melakukan studi konfigurasi terhadap *mininet, GNS3, switch openflow,*dan semua *software* yang dibutuhkan dalam melakukan penelitian serta melakukan studi konsep serangan *DDoS.*

2) Rancangan Topologi Dan Skenario Serangan DDoS.

Membuat rancangan topologi yang akan di simulasikan serta merancang skenario serangan *DDoS* di lingkungan *SDN.*

3) Instalasi dan Konfigurasi Kontroller,

Tahap ini melakukan instalalsi dan konfigurasi kontroller,

4) Implementasi GNS3

Berikut langkah langkah dalam mengimplementasikan Software simulasi GNS3:

a. Instalasi dan Konfigurasi *GNS3*

Tahap ini akan melakukan instalasi *GNS3* dan paket pendukungnya yaitu *Qemu VM* pada komputer atau laptop

b. Konfigurasi *OpenWRT*

Disini *OpenWRT* akan dijalankan pada *Qemu VM* dan selanjutnya *OpenWRT* akan di install software *switch Open V Switch* sehingga *OpenWRT* dapat berfungsi sebagai *Switch Openflow*. *OpenWRT* adalah distribusi *GNU* / *Linux* sangat luas untuk perangkat *embedded*. Tidak seperti distribusi lain, *OpenWRT* dibangun dari dasar sampai berfitur lengkap, mudah dimodifikasi untuk sistem operasi *router* [10].

c. Implementasi Topologi

Tahap ini akan mengimplementasikan topologi yang sudah dirancang sebelumnya.

d. Konfigurasi *Switch Openflow*

Software *switch openflow* yaitu *OpenVSwitch* akan dikonfigurasi agar *switch* bisa dikontrol oleh kontroller

e. Konfigurasi Host

Masing masing *host* pada GNS3 dapat melakukan serangan *DDoS* dan pengujian kualitas jaringan maka instalasi *DDoS tool* diperlukan untuk melakukan simulasi serangan. Sedangkan untuk pengukuran kualitas jaringan menggunakan software ping bawaan sistem.

5) Simulasi dan Pengujian Serangan

Dalam tahap ini akan dilakukan Simulasi Serangan *DDoS* berdasarkan tahapan rancangan skenario topologi Dan serangan DDoS sebelumnya. Simulasi serangan *DDoS* di artsitektur jaringan *SDN* akan di simulasikan pada simulator *GNS3*. Dimana, *type* serangan yang akan digunakan dalam pengujian ini yaitu *TCP Syn Flood Attack.*

6) Pengujian Hasil Simulasi DDoS di Mininet dan GNS3

Saat melakukan simulasi serangan *DDoS* pada mininet dan *GNS3* disamping itu juga pengukuran kualitas jaringan dengan menggunakan protokol *icmp* dengan perintah *ping* untuk mengukur *delay* dan *packet loss* serta melakukan monitoring laulintas jaringan dan capture data secara realtime pada Jaringan *SDN* untuk mendeteksi serangan *DDoS* dan mengumpulkan informasi *statistic* keadaan jaringan saat terjadi serangan.

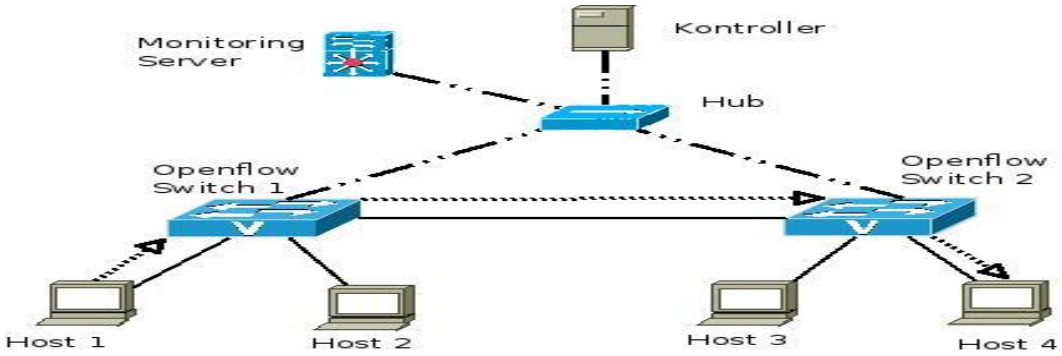
7) Mendokumentasikan Hasil

Data dari pengujian yang akan di dokuentasikan berdasarkan hasil pengamatan Simulasi *DDoS* dilingkungan *SDN* pada *software simulator GNS3*

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



Gambar 1. Rancangan Topologi

Kontroller	e=	Melakukan kontrol terhadap kedua switch switc serta yang mengatur jaringan SDN
Monitoring Server	=	Melakukan Monitorig jaringan yang berisi Sofware Monitoring Sflow Trend dan Netflow Analizer
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 perankat 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 Syn Flood Attack di *GNS3*

Hasil pengujian simulasi serangan *TCP Syn Flood* di Jaringan SDN pada jaringan SDN di GNS3 sebagai berikut (Tabel 3 dan Tabel 4).

Tabel 3. Pengukuran Delay Syn FLood Attack di GNS3

Jumlah Serangan	Delay (ms)	Percobaan Ke-			Total (ms)	Rata-Rata (ms)
		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	Min	1.488	1.650	1.680	4.818	1.606
	Average	3.632	8.978	7.307	19.917	6.639
	Max	62.375	329.233	118.271	509.879	169.960
20000	Min	1.762	1.573	1.667	5.002	1.667
	Average	203.309	102.051	245.587	550.947	183.649
	Max	4224.090	2499.749	4558.089	11281.928	3760.643
40000	Min	2.232	2.077	1.676	5.985	1.995
	Average	131.090	9.421	585.867	726.378	242.126
	Max	2356.563	115.956	6382.865	8855.384	2951.795
60000	Min	1.831	1.606	1.555	4.992	1.664
	Average	26.527	546.810	1856.297	2429.634	809.878
	Max	1014.263	6782.587	13775.537	21572.387	7190.796
80000	Min	3.775	1.613	1.835	7.223	2.408
	Average	9.276	1501.325	4.639	1515.240	505.080
	Max	71.433	11296.439	92.983	11460.855	3820.285
100000	Min	3.085	1.450	3.270	7.805	2.602
	Average	5610.84	2013.318	24.688	7648.846	2549.615
	Max	20736.245	14185.910	164.657	35086.812	11695.604

Hasil pengukuran delay yang di presentasikan oleh Tabel 3 menunjukan *TCP Syn* yang dikirim sebanyak 60000 paket di *GNS3* menghasilkan *delay* rata-rata sebesar 809.878 ms. Besar *delay* tersebut masuk dalam kategori jelek jika melihat tabel performasi jaringan berdasarkan *delay* oleh TIPHON. Packet lost (Tabel 4) yang diakibatakan oleh serangan *TCP Syn* di GNS3 menghasilkan paket lost tertinggi sebesar 65% dengan sequence error 38 paket ICMP dari jumlah total paket ICMP 60 paket yang dihasilkan oleh Ping. Packet lost terjadi mulai ketika melakukan serangan TCP Syn sebanyak 20000 paket dengan presentasi packet lost rata-rata sebesar 8 % dengan jumlah rata-rata sequens error 5 paket ICMP yang dihasilkan oleh Ping.

Tabel 4. Pengukuran Packet Lost Syn 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	57	54	55	55
	Seq Error	3	6	5	5
	Packet Lost %	5	10	8	8
40000	Seq Received	43	45	52	47
	Seq Error	17	15	8	13
	Packet Lost %	28	25	13	22
60000	Seq Received	53	51	57	54
	Seq Error	7	9	3	6
	Packet Lost %	11	15	5	10
80000	Seq Received	57	41	48	49
	Seq Error	3	19	12	11

	Packet Lost %	5	31	20	19
100000	Seq Received	38	57	22	39
	Seq Error	22	3	38	21
	Packet Lost %	36	5	63	35

3) Penggunaan RAM dan CPU pada switch openflow GNS3

Hasil pengamatan penggunaan RAM dan CPU pada switch openflow di GNS3 dan pada laptop/pc saat terjadi serangan sebagai berikut,

Tabel 5. Penggunaan RAM dan CPU pada Switch GNS3 dan Laptop

Jenis Serangan	Jumlah Serangan	Switch 1 GNS3		Switch 2 GNS3		Laptop GNS3	
		CPU	RAM (71MB)	CPU	RAM (71MB)	CPU	RAM (5.6GB)
Normal	0	2%	18 M	3%	18 M	22%	3 G
TCP Syn Flood Attack	5000	80%	37 M	96%	46 M	78%	3.3 G
	20000	98%	54 M	90%	57 M	81%	3.4 G
	40000	97%	60 M	99%	65 M	83%	3.4 G
	60000	98%	71 M	95%	61 M	98%	3.5 G
Rata-Rata		93%	55.5 M	95%	57.25M	85%	3.4G

Tabel 5 menunjukan bahwa serangan *DDoS* yang dilakukan di jaringan SDN di *GNS3* dapat mempengaruhi sumber daya *RAM* dan *CPU* pada Mesin *Virtual Switch OpenFlow* dengan rata-rata penggunaan 93% CPU dan 55.5Mb RAM pada *switch-1* dan 95% CPU dan 57.25M RAM pada *switch-2* sehingga mempengaruhi kinerja dari switch.

Saat serangan TCP Syn Flood attack dengan jumlah beban 60000 paket, software OpenVSwitch pada switch-1 dihentikan oleh sistem dengan mengeluarkan peringatan "Killed process 1158 (ovs-vswitchd)" sehingga menyebabkan switch gagal berfungsi sebagai switch openflow sementara waktu ssampai service OpenVSwitch di jalankan kembali oleh sistem secara otomatis.

Saat serangan berlangsung di GNS3 sumberdaya RAM dan CPU yang berada pada Laptop/PC ikut terpengaruh. Rata-rata penggunaan resource pada laptop saat dilakukan serangan yaitu 85% CPU dan 3.4 GB Ram.

KESIMPULAN DAN SARAN

Kesimpulan

Kesimpulan yang dapat diambil berdasarkan penelitian ini adalah :

1. Serangan DDoS dapat mempengaruhi kualitas jaringan di Arsitektur jaringan SDN di GNS3 dimana pada saat pengiriman paket dengan jumlah paket yang dikirim sebanyak 6000 paket mengakibatkan kualitas jaringan menjadi jelek berdsarkan nilai delay pada TIPHON
2. Dari hasil pemantauan Serangan DDoS di GNS3 bahwa serangan DDoS berdampak juga pada sumber daya pada switch openflow baik dari penggunaan CPU maupun penggunaan RAM sehingga menyebabkan software OpenVSwitch direstart oleh sistem dan mengakibatkan Switch Openflow gagal beroperasi sementara waktu sampai OpenVSwitch berjalan dengan baik.

Saran

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

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 ManagementSymposium (APNOMS), 2015 17th Asia-Pacific. IEEE, .

[4] Mousavi, Seyed Mohammad, and Marc St-Hilaire., 2015, "*Early detection of DDoS attacks against SDN controllers*." Computing, Networking and Communications (ICNC), 2015 International Conference on. IEEE, 2015.

[5] 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

[6] RedNectar Chris Welsh, 2013, GNS3 Network Simulation Guide. PACKT

[7] Ferguson, P. & Huston, G. 1998. Quality of Service. John Wiley & Sons Inc

[8] Santosa, B. 2004. Manajemen Bandwidth Internet dan Intranet.

[9] 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

[10] Slickkitten. Diakses tanggal 30/12/2015. About OpenWRT. http://wiki.openwrt.org/about/start.