Perancangan Dan Implementasi *Cloud Base Microsegmentation Firewall* Menggunakan Metode Ppdioo

1st Muhammd Rizki Septiawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rizkiseptiawan@student.telkomuniversity.ac.id

2nd M. Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

3rd M. Fathinuddin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
muhammadfathinuddin@telkomuniversity.ac.id

Abstrak* — seiring dengan kemajuan ini, timbul kekhawatiran seputar keamanan data pengguna. Baru-baru ini, kita menyaksikan peningkatan jumlah serangan keamanan siber, terutama dalam bentuk serangan ddos salah satu pendekatan yang diambil untuk mengatasi tantangan ini adalah penerapan konsep mikrosegmentasi dalam jaringan *cloud*. Topologi ini akan diimplementasikan dalam simulasi jaringan menggunakan gns3, yang akan diukur meliputi aspek fungsionalitas, statistik keamanan, kualitas layanan (*quality of service*), pengujian akan dilakukan dalam dua skenario berbeda yaitu kondisi normal dan serangan ddos dari zona external. Serangan dilakukan dengan metode icmp *flood* dan syn *flood.

Kata kunci*— fortigate, *firewall*, ddos, *quality of service.

I. PENDAHULUAN

Peningkatan penggunaan teknologi cloud di kalangan perusahaan telah menjadi suatu tren yang semakin menonjol. Konsep komputasi awan (*cloud computing*) memberikan perusahaan akses ke sumber daya TI dengan fleksibilitas dan efisiensi yang tinggi, tanpa perlu membeli, mengelola, atau merawat infrastruktur perangkat lunak secara mandiri. Namun, walaupun memberikan berbagai keuntungan tersebut, penggunaan teknologi cloud juga membawa potensi risiko yang serius terkait dengan aspek keamanan. Dengan meningkatnya penggunaan teknologi cloud dan risiko keamanan yang semakin kompleks, cloud microsegmentation firewall menjadi solusi keamanan yang penting dan efektif untuk melindungi jaringan cloud perusahaan.

II. KAJIAN TEORI

Cloud server merupakan jenis infrastruktur yang terdiri dari sejumlah server fisik yang terhubung dan berfungsi secara bersama di pusat data. Prinsip ini mengizinkan pengguna untuk meraih akses kepada sumber daya ini secara jauh menggunakan internet. Pada umumnya, cloud computing bersifat public, private, community dan hybrid cloud[1].

Microsegmentation memungkinkan secara logis membagi data center menjadi segmen keamanan yang berbeda dan tingkat beban secara individual yang kemudian menentukan kontrol keamanan dan layanan secara unik pada setiap segmennya [2].

Virtualisasi adalah teknologi yang memainkan peran sentral dalam perkembangan Network Function Virtualization (NFV). Dalam konsep ini, teknologi virtualisasi memungkinkan perangkat keras seperti server dan komputer untuk menjalankan berbagai sistem operasi dalam bentuk sumber daya virtual.

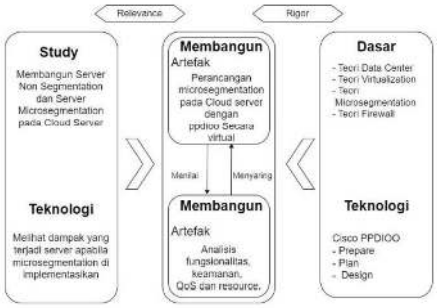
Firewall adalah sebuah sistem aplikasi yang ada dalam komputer, berfungsi untuk melindungi komputer yang terhubung dalam jaringan komputer dari berbagai ancaman atau gangguan yang berasal dari pengguna yang tidak sah. Penggunaan firewall merupakan metode untuk memastikan bahwa informasi yang bersifat pribadi atau data yang terhubung dengan internet tidak dapat diakses oleh pihak yang tidak memiliki otoritas.

Serangan DDoS (Distributed Denial of Service) bertujuan untuk menargetkan sumber daya sistem dan bandwidth jaringan dengan maksud mengganggu aliran lalu lintas normal antara klien dan server.

III. METODE

A. Pengembangan Model Konseptual

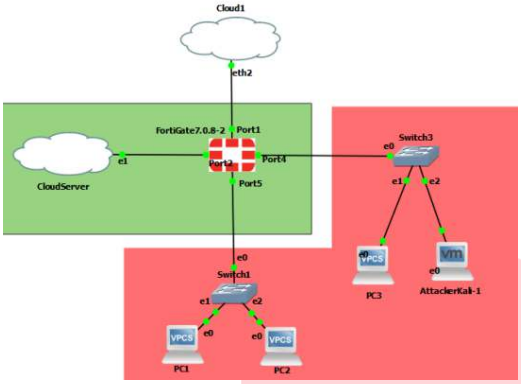
Conceptual Model Development merupakan proses merancang dan membangun representasi abstrak yang menggambarkan hubungan dan konsep-konsep yang penting dalam suatu system. Model konseptual bertujuan untuk memberikan pemahaman yang lebih jelas dan terstruktur tentang suatu masalah yang sedang diteliti.



IV. PEMBAHASAN PENELITIAN

A. Topologi

zone yang akan di gunakan melibatkan penggunaan cloud debian yang dilindungi oleh perlindungan keamanan dari perangkat FortiGate, yang telah dibagi menjadi dua zona yaitu zone cloud dan zone external.



GAMBAR IV-1
Topologi'

B. *Konfigurasi* alamat IP

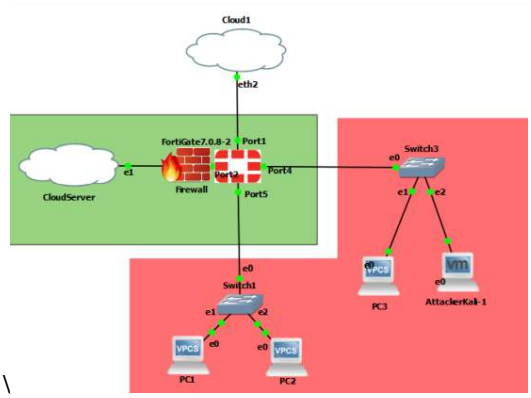
Dalam mendukung penelitian ini, diperlukan alamat IP yang akan digunakan dalam pengaturan konfigurasi topologi jaringan. Pengaturan alamat IP ini akan diterapkan baik pada topologi microsegmentation maupun non microsegmentation.

TABLE IV-1
Alamat IP

Perangkat	Alamat IP	Netmask
Cloud Server	20.1.2.1	255.255.255.0
PC 1	10.1.1.2	255.255.255.0
PC 2	10.1.1.3	255.255.255.0
PC 3	30.1.1.3	255.255.255.0
ATTACKER	30.1.1.2	255.255.255.0

C. Skenario pengujian pertama

Skenario pengujian pertama akan mendapatkan hasil simulasi dari penyerangan DDoS melalui metode ICMP flood attack dan SYN flood attack. Serangan ini akan diluncurkan oleh pihak penyerang yang berada di zone external dan ditargetkan menuju jaringan cloud server yang diamankan oleh firewall FortiGate.

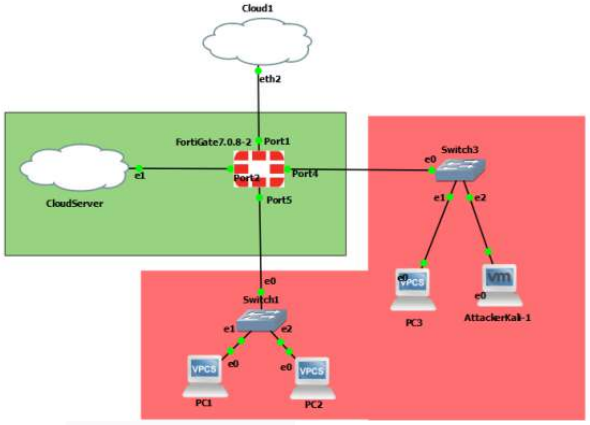


\

GAMBAR IV-2
Firewall zone

D. Skema Pengujian kedua

Pada skenario pengujian kedua, simulasi akan dijalankan untuk mendapatkan hasil dari serangan DDoS menggunakan metode ICMP flood attack dan SYN flood attack. Serangan tersebut akan diinisiasi oleh penyerang yang berada di zone external dan diarahkan ke jaringan cloud server tanpa ada perlindungan dari firewall FortiGate.



GAMBAR IV-3
Non *Firewall zone*

E. Pengujian Fungsional Sistem

Pengujian fungsi dijalankan dengan menggunakan metode PING pada setiap host yang terdapat dalam susunan jaringan. Namun perlu diingat bahwa tidak semua host akan diuji. Proses pengujian fungsi ini dilaksanakan pada kedua tipe topologi yang ada.

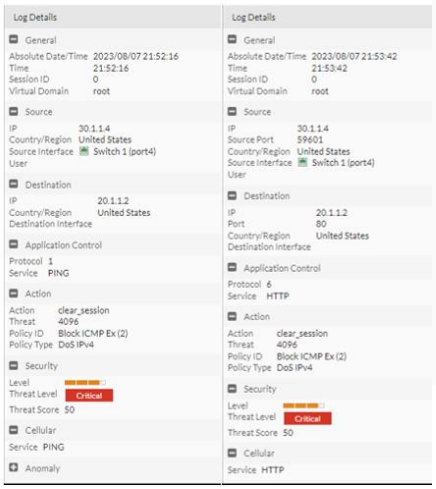
TABLE IV-2
test konektifitas

No	Host asal	Host tujuan	Status	Keterangan
1	PC 1	PC 2	Sukses	Sukses
		PC 3	Gagal	*Network Timeout*
		Attacker	Gagal	*Network Timeout*
		Cloud	Sukses	Karena terdapat access list *Firewall Policy*
2	Attacker	PC 1	Gagal	*Network Timeout*
		PC 2	Gagal	*Network Timeout*
		PC 3	sukses	Sukses
		Cloud	Sukses	Karena terdapat access list *Firewall Policy*
3	*Cloud*	PC 1	Sukses	Karena terdapat access list *Firewall Policy*
		PC 2	Sukses	Karena terdapat access list *Firewall Policy*
		PC 3	Sukses	Karena terdapat access list *Firewall Policy*
		Attacker	Sukses	Karena terdapat access list *Firewall Policy*

F. Pengujian kemanan

Pengunjian keamanan pada penelitian ini menggunakan serangan dari DDOS menggunakan metode ICMP *Flood attack* dan SYN *Flood attack*. Serangan berasal dari *external zone* menuju *cloud zone*. Agar serangan bisa di lancarkan maka dibutuhkan *tools* Hping3 yang telah terpasang pada kali linux.

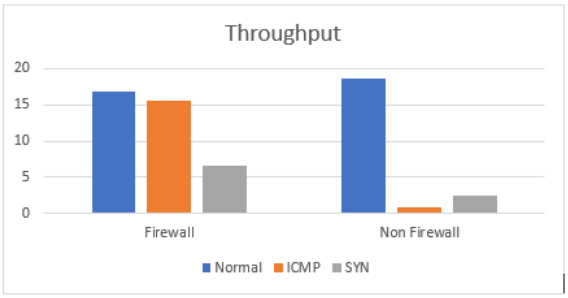
ICMP : # hping3 -S -p 80 –-flood [IP Target]
SYN : # hping3 -c 1500 -d 120 -S -w 64 -p 80 –flood –rand-source [IP Target]



GAMBAR IV-4
Detail serangan

G. Quality Of Service

Pada bagian ini akan membahas mengenai perbandingan Throughput yang telah di uji pada bagian sebelumnya.

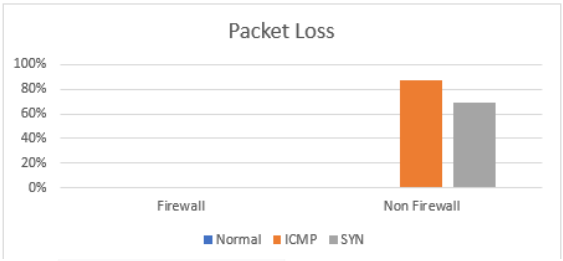


GAMBAR IV-5
Throuhput

TABLE IV-3
detail Throuhput

	Normal	ICMP	SYN
Firewall	16.9	15.5	6.65
Non *Firewall*	18.7	0.807	2.4

Terlihat bahwa *throughput* dari skema non *firewall* terjadi penurunan yang sangat signifikan dibandingkan dengan skema yang menggunakan *firewall,l* pada bagian skema yang menggunakan *firewall* terjadi juga penurunan namun tidak terlalu jauh.

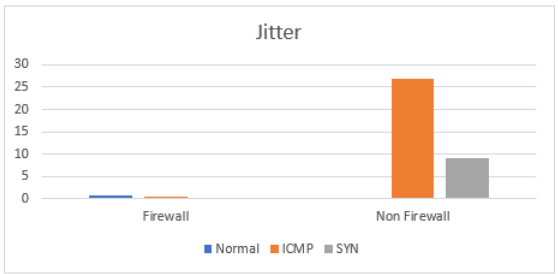


GAMBAR IV-6
Packet Loss

TABLE IV-4
Detail Packet Loss

	Normal	ICMP	SYN
Firewall	0%	0%	0%
Non *Firewall*	0%	87%	69%

Memperlihatkan besarnya paket yang telah hilang dari skema non *firewall* berada pada 87% untuk penyerangan menggunakan ICMP sedangkan penyerangan menggunakan SYN berada pada 69%.



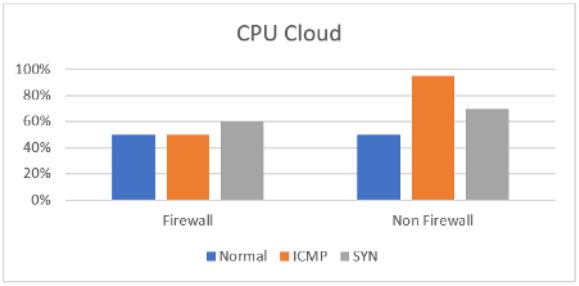
GAMBAR IV-7
Jitter

TABLE IV-5
Detail Jitter

	Normal	ICMP	SYN
Firewall	0.615	0.378	0.184
Non *Firewall*	0.232	27	9

Memperlihakan bahwa *jitter* yang di ukur dari non *firewall* saat di serang ICMP dan SYN memiliki angka yang sangat tinggi yaitu berada pada 27 untuk penyerangan menggunakan ICMP, sedangkan untuk SYN berada pada 9.

H. Analisis Pengujian Resource Utilization

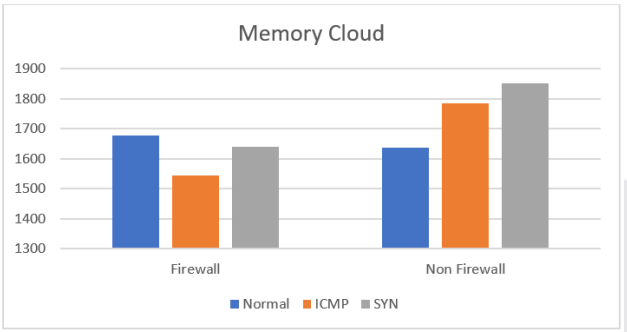


GAMBAR IV-8
Analisis CPU *Cloud Resource*

TABLE IV-6
Detail Analisis CPU *Cloud Resource*

	Normal	ICMP	SYN
Firewall	50%	50%	60%
Non Firewall	50%	95%	70%

Terlihat penggunaan CPU *cloud* data menunjukan dari sisi *firewall* tadi perubahan sedkit namun tidak mempengaruhi kinerja dari *cloud* tersebut, sedangkan dari skema non *firewall* terjadi peningkatan CPU yang cukup signifikan berada pada 90% saat di serang dengan ICMP, sedangkan untuk yang SYN memang terjadi peningkatan juga berada pada 70% hal tersebut terjadi karena saat penyerangan SYN terjadi FortiGate lebih Cepat *crash* saat di serang dengan SYN menyebabkan serangan yang dilancarkan menjadi terputus.

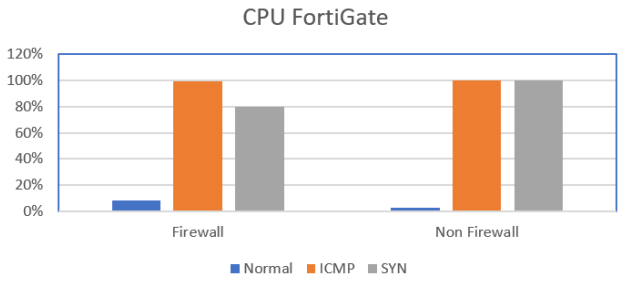


GAMBAR IV-9
Analisis Memory Cloud Resource

TABLE IV-7
Analisis Memory Cloud Resource

	Normal	ICMP	SYN
Firewall	1677	1545	1641
Non *Firewall*	1636	1785	1852

Perlihatkan statistik dari *memory* pada *cloud* yang dimana saat *cloud* dilindungi oleh FortiGate dengan *firewall* tidak terjadinya banyak perubahan pada *cloud* hal itu terjadi dikarenakan FortiGate telah melakukan *blocking* serangan yang berlangsung. Sedangkan pada FortiGate yang tidak di pasang *firewall* terjadi peningkatan *mermory* pada saat di serang.

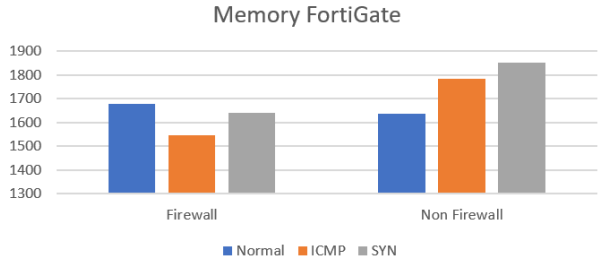


GAMBAR IV-10
Analisis FortiGate CPU Resource

TABLE IV-8
Detail Analisis FortiGate CPU Resource

	Normal	ICMP	SYN
Firewall	8%	99%	80%
Non *Firewall*	3%	100%	100%

Terdapat statistik CPU FortiGate saat penyerangan berlangsung, kedua skema terjadi peningkatan, yang di mana FortiGate dengan *firewall* mencapai 99% namun kondisi ini berlangsung tidak lama, sedangkan untuk CPU non *firewall* terjadinya peningkatan CPU yang berada pada 100% hal tersebut membuat FortiGate menjadi *crash* semua konektifitas menjadi terputus dan harus di lakukan *restarting system.*



GAMBAR IV-11
Analisis FortiGate Memory Resource

TABLE IV-9
Detail Analisis FortiGate CPU Resource

	Normal	ICMP	SYN
Firewall	1677	1545	1641
Non *Firewall*	1636	1785	1852

FortiGate yang tidak di pasang *firewall* lebih unggul dalam kondisi normal dibandingkan dengan ForitGate yang di pasang *firewall* hal tersebut dapat terjadi karena FortiGate mempunyai beban *firewall* telah di terapkan. Namun saat terjadinya penyerangan justruk bahwa FortiGate dengan *firewall* menunjukan penggunaan *memory* lebih rendah di banding dengan non *firewall*.

V. KESIMPULAN

Kesimpulan dari penelitian ini didasarkan pada hasil pengujian dan analisis yang dilakukan dalam merancang *Cloud Microsegmentation* dengan metode *Firewall zone* di GNS3.

1. Berdasarkan hasil pengujian dan Analisa fungsional skenario pertama dan skenario kedua yaitu *Microsegmentation* yang menerapkan *firewall* dan yang

tidak menerapkan *firewall* mampu berkomunikasi sesuai dengan rule yang telah di buat pada ForiGate.

2. Berdasarlam hasil pengujian dan Analisa keamanan pada sekenario pertama yang menggunakan FortiGate *firewall Policy* mampu memitigasi serangan yang di lancarkan dari zona *external* sedangkan tanpa menggunakan *firewall Policy* pada FortiGate tidak mampu menahan serangan yang telah di lancarkan yang mengakibatkan koneksi menjadi terpus dari seluruh host hal tersebut terjadi dikarenakan adanya serangan yang membuat FortiGate kewalahan dan menjadi crash.
3. Berdasarlam hasil pengujian *Quality of Service microsegmentation* dengan *firewall* dapat mempertahankan QoS ketika di serang hanya sedikit terdapat sedikit pengurangan qualitas, sedangkan pada *microsegmentation* non *firewall* hal tersebut cendrung menunjukan hasil yang sangat buruk.
4. Berdasarlam hasil pengujian *Resource Utilization microsegmentation* FortiGate *firewall* makan resource yang lebih besar saat kondisi normal sedangkan pada saat serangan terjadi hasil yang di dapat menunjukan bahwa Microsegmentation *firewall* dapat bertahan dan melakukan *blocking* serangan tersebut, sedangkan untuk Fortigate non *firewall* akan terjadi *crash* yang akan memutuskan konesi dari *zone* luar sehingga *cloud* tidak dapat di akses atau berkomunikasi sama sekali.

REFERENSI

[1] Ashari, A., Setiawan, H., Ilmu, J., Mipa, F., & Mada, U. G. (2011). Cloud Computing : Solusi ICT ? 3(2), 336–345

[2] Vincentis, M. D. (2017). Micro-segmentation For Dummies, 2nd VMware Special Edition. John Wiley & Sons, Inc.