Implementasi dan Analisis Profil Sistem Pada Virtualisasi Fortigate Firewall Berdasarkan Metrik Sumber Daya Komputasi

Implementation and Analysis of System Profile on Fortigate Firewall Virtualization Based on Computing Resource Metrics

1st Maulana Malik Ibrahim
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
maulanamalikibra@student.telkomuniverity.ac.id

2nd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd M. Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

Abstrak— Perbuatan melawan hukum yang dilakukan dengan berbasis internet disebut *Cybercrime*. *Cybercrime* dapat dicegah dan ditanggulangi dengan berdasarkan aspek keamanan jaringan. Ancaman terhadap jaringan komputer lainnya yaitu *Distributed Denial of Service* (DDoS). Salah satu melindungi sistem dari serangan DDoS yaitu dengan memproteksi menggunakan *firewall*. *Firewall* adalah sebuah sistem atau perangkat yang bisa memberikan izin keluar masuknya data atau informasi pada lalu lintas jaringan. Salah satu fungsi *firewall* adalah melindungi layanan IT. Pada penelitian ini menggunakan *virtualized* Fortigate *firewall* versi 7.2.0 dengan implementasi fungsi *firewall* pada *load testing* pada spesifikasi *firewall* 1,5 GB *memory* dan 2 GB *memory*. Penelitian ini berusaha mendapatkan karakter *firewall* berdasarkan sumber daya komputasi dan menggunakan dua skenario pengujian yaitu *service* HTTP *allow* dan *service* HTTP *block*. Pengujian yang dilakukan adalah DDoS SYN flood dari Kali Linux yang mengarah ke *web server* di Ubuntu *server*. Platform percobaan dilakukan dengan *virtualized firewall* Fortigate pada skala laboratorium. Percobaan yang dilakukan adalah sebelum serangan, saat serangan, setelah serangan. Hasil yang diperoleh adalah konsumsi sumber daya komputasi CPU 97,1%, *memory* 83,7%, dan *session* 148883. Untuk kelanjutan penelitian dapat berupa profil yang menggambarkan relasi antara serangan, *firewall*, dan *server*.

Kata kunci— *virtualized*, fortigate, *profiling*, *testing*, sumber daya komputasi

I. PENDAHULUAN

Keamanan suatu jaringan komputer merupakan salah satu bagian sistem yang harus dilindungi untuk mengamankan data-data yang ada dan menghindari ancaman informasi pada server komputer. Keamanan informasi merupakan cara untuk melindungi informasi dari segala kemungkinan ancaman yang terjadi dan mendeteksi adanya suatu pencurian data atau informasi, seperti penyerangan Denial of Service (DOS). Jika perangkat komputer terkena serangan tersebut akan mengakibatkan server down dan bisa juga secara otomatis server tidak dapat beroperasi lagi. Dari berbagai serangan yang dialami sebuah server, dapat dilakukan tindakan pencegahan dengan melakukan identifikasi celah keamanan yang maksimal pada perangkat komputer, salah satunya dengan menggunakan firewall.

Firewall merupakan suatu sistem yang dapat menerapkan access control policy pada lalu lintas jaringan, yang dapat membantu melindungi dari serangan lalu lintas jaringan dan serangan lainnya serta dapat memfilter lalu lintas jaringan yang masuk pada jaringan. Implementasi firewall sangat penting diterapkan pada perangkat komputer untuk menghindari dari pencurian data-data yang ada di dalam perangkat yang sifatnya rahasia.

Implementasi firewall penting untuk diterapkan pada jaringan untuk menjaga dari ancaman serangan. Dasar kinerja yang dimiliki firewall, yaitu dapat mendeteksi traffic jaringan yang sah. Seingga dapat diberikan akses ke dalam sistem dengan melewati firewall untuk dibatasi. Pembatasan akses yang masuk ke dalam jaringan lokal, kemudian melakukan pencegahan jaringan yang tidak terdaftar pada sistem. Pembatasan dilakukan dengan diaturnya rules atau policy pada konfigurasi firewall. Salah satu jenis firewall yang sering dibicarakan adalah Next Generation Firewall (NGFW). Next Generation Firewall merupakan firewall yang memiliki kemampuan dalam mendeteksi dan memblokir suatu serangan yang berbahaya. Kemampuan NGFW dengan memberikan proteksi dan perlindungan yang tinggi, serta dapat menerapkan keamanan yang terdapat pada tingkat protocol, port, dan aplikasi.

Ketersediaan sumber daya komputasi firewall seperti penggunaan CPU, memory, bandwidth dan session berdasarkan peningkatan kinerja suatu firewall dengan melakukan proses pemantauan pada sistem jaringan. Pada saat melakukan konfigurasi perlu dilakukannya pengujian keamanan pada suatu jaringan dengan menetapkan kebijakan

yang dibutuhkan untuk melindungi sistem dari ancaman serangan.

Pada tugas akhir ini, melakukan implementasi peran firewall dan melakukan profiling sistem pada firewall berdasarkan sumber daya komputasi terhadap availability suatu jaringan dengan melakukan pendeteksian, pencegahan dan pemulihan. Pada proses analisis ini dilakukan pendeteksian dengan akses traffic IP Address yang di ijinkan masuk ke dalam sistem, kemudian pada proses pencegahan melakukan setting rules pada firewall, selanjutnya pada proses pemulihan dilakukan pemantauan berdasarkan karakteristik sumber daya komputasi firewall. Hasil analisis yang di dapat bertujuan untuk melihat adanya ketersediaan layanan berdasarkan sumber daya komputasi.

II. DASAR TEORI

A. Keamanan Informasi

Keamanan jaringan merupakan cara untuk memberikan perlindungan terhadap suatu jaringan agar terhindar dari ancaman atau serangan. Ancaman atau serangan yang berasal dari luar jaringan yang bertujuan merusak atau meretas data. Perancangan keamanan informasi dapat dilakukan dengan menggunakan sistem keamanan seperti *firewall*.[1].

B. *Firewall*

Firewall adalah adalah sistem keamanan komputer yang mampu melindungi dari serangan atau ancaman dari luar. firewall merupakan perangkat lunak untuk mencegah akses yang dianggap ilegal atau tidak sah dari jaringan pribadi [2].

C. Fortigate

Fortigate merupakan sistem keamanan yang dikeluarkan oleh Fortinet. Fortinet adalah perusahaan penyediaan layanan, dan badan pemerintahan di seluruh dunia termasuk mayoritas dari perusahaan *Fortune* Global 100 tahun 2009. *Fortinet* merupakan pemimpin pasar untuk *unified threat management* (UTM). Fasilitas utama dari fortigate adalah mencegah serangan *Distributed Denial of Service Attacks* yang dilakukan penyerang untuk menembus sistem keamanan dan mencuri data pada sistem.

D. *Denial of Service* (DoS)

Distributed Denial of service (DDoS) adalah serangan yang menyebabkan kerusakan pada target. Serangan DDoS melakukannya dengan membanjiri target dengan lalu lintas, atau mengirimkan informasi yang memicu kerusakan pada target. Serangan DoS membuat target atau korban kehilangan layanan atau sumber daya yang mereka punya [3].

E. Hping3

Hping3 merupakan sebuah TCP/IP *assembler* dan juga merupakan *command-line* yang berjalan pada pemrosesan paket TCP/IP. Hping dapat digunakan untuk membuat paket IP yang berisi TCP, UDP atau ICMP *payloads*. *Hping3* merupakan versi terbaru dari Hping dan Hping2, Hping3 merupakan aplikasi *stand alone*, sedangkan Hping2 masih memerlukan aplikasi dari pihak ketiga seperti *scapy* dan *ids wakeup*. [4].

F. Sumber Daya Komputasi

Sumber daya komputasi merupakan teknologi yang digunakan dalam bentuk perangkat komputer yang terdiri dari perangkat keras dan perangkat lunak (Hardware dan Software). Sumber daya komputasi ini digunakan untuk membantu fungsi tugas manusia. [5].

G. *Load Testing*

Load testing adalah teknik *performance testing* yang merespon sistem diukur dengan berbagai load condition. Pengujian menggunakan *Load Testing* membantu menentukan bagaimana *software* merespon ketika ada akses *software* secara bersamaan [6].

III. METODE

A. Model Konseptual Penelitian

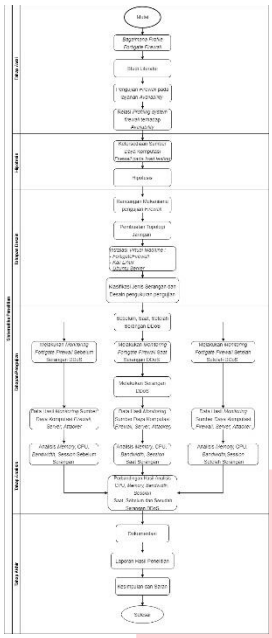
Model konseptual ini bertujuan untuk memudahkan dalam melakukan identifikasi permasalahan yang ditemukan pada penelitian ono yaitu, sebagai berikut:

GAMBAR 1
MODEL KONSEPTUAL PENELITIAN

Dapat diketahui pada Gambar 1 bahwa terdapat tiga ruang lingkup yaitu lingkungan, penelitian dan dasar ilmu. Pada aspek lingkungan berupa *problems* yang terjadi dan *technology* yang terdapat pada penelitian ini. Pada penelitian Terdapat "Membangun" yaitu melakukan *profiling firewall* berdasarkan analisis sumber daya komputasi terhadap pertahanan layanan *availability* pada Fortigate *firewall*. Pada "Evaluasi" berfokus pada *profiling firewall* dan pertahanan layanan *availability* dan menjalankan skenario pengujian serangan DDoS dalam konsumsi pola pemantauan dan pengukuran sumber daya komputasi pada *firewall, server* dan *attacker*. Dasar ilmu merupakan bahan dasar dalam melakukan penelitian ini yang mencakup pada teori keamanan jaringan, aspek-aspek keamanan informasi yaitu *availability*, teori *firewall*, dan teori sumber daya komputasi.

B. Sistematika Penelitian

Sistematika penelitian digunakan untuk penyelesaian masalah dalam menggambarkan alur penelitian yang akan dikerjakan sebagai gambaran dalam mecahkan masalah berikut:



GAMBAR 2
SISTEMATIKA PENELITIAN

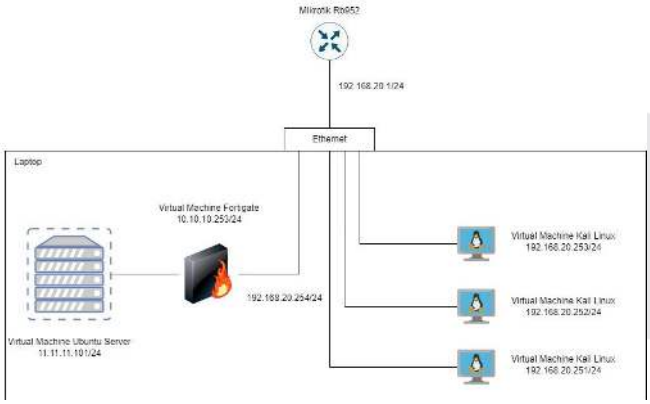
IV. HASIL DAN PEMBAHASAN

A. Rancangan Sistem

Dalam melakukan *profiling* fortigate *firewall* serta melakukan analisis dan pengukuran pada penggunaan sumber daya komputasi (CPU, *memory, bandwidth, session*) pada *firewall, server,* dan *attacker,* dibutuhkan perancangan mekanisme sistem untuk melakukan pengujian.

1. Topologi Jaringan

Topologi jaringan digunakan untuk menggambarkan kegiatan yang akan dilakukan dalam pengujian ini, sebagai langkah untuk mendapatkan hasil percobaan dalam melakukan serangan yaitu pada sebelum, saat dan sesudah serangan DDoS.



GAMBAR 3
TOPOLOGI JARINGAN PENGUJIAN

2. Daftar IP Address

IP *Address* yang digunakan pada penelitian ini, dilampirkan pada Tabel 1 Daftar IP address:

TABEL 1
DAFTAR IP ADDRESS**:**

Nama	Host	Default Gateway	IP Address
Router	Mikrotik Rb952		192.168.20.1/24
VM1	Fortigate *Firewall*	192.168.20.1/24	IP WAN: 192.168.20.99/24 IP LAN: 10.11.11.10/24
VM3	Kali Linux *Attacker* 1		192.168.20.252/24
VM4	Kali Linux *Attacker* 2		192.168.20.253/24
VM5	Kali Linux *Attacker* 3		192.168.20.254/24
VM2	Ubuntu Server	11.11.11.253/24	IP WAN: 192.168.20.100 IP Static: 11.11.11.101

B. Skenario Pengujian

Dalam melakukan pengujian, diperlukan skenario pengujian yang menggambarkan mekanisme pengukuran sumber daya komputasi pada fortigate *firewall*, *attacker*, dan *server.* Terdapat dua skenario pengujian yang dilakukan yaitu, skenario pertama dengan *service* HTTP *allow* dan skenario kedua dengan *service* HTTP di *block*. Pada kedua skenario tersebut bertujuan untuk melihat perbandingan pada pengukuran sumber daya komputasi, serta melakukan pemantauan dan analisis pada sebelum serangan, saat serangan dan sesudah serangan DDoS. Dalam penelitian ini terdapat dua skenario pengujian yang dilakukan, yaitu:

1. Skenario pengujian *service* HTTP *allow*.

GAMBAR 4
RULES SERVICE HTTP *ALLOW*

2. Skenario pengujian *service* HTTP *block.*

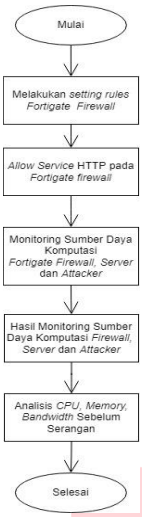
GAMBAR 5
RULES SERVICE HTTP *BLOCK*

1. Skenario 1: *Service* HTTP *Allow*

Pada skenario 1 dilakukan pengujian dengan memberikan izin *web server* pada *service* HTTP di Fortigate *firewall*, pada skenario ini terdiri dari tiga pengujian yaitu pengujian sebelum serangan, saat serangan dan sesudah serangan

a. Pengujian Sebelum Serangan

Tahap pertama dalam skenario ini yaitu, pengujian sebelum melakukan serangan DDoS dengan *service* HTTP *allow*



GAMBAR 6
PENGUJIAN SEBELUM SERANGAN *SERVICE* HTTP *ALLOW*

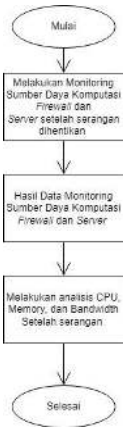
b. Pengujian Saat Serangan

Tahap ke dua dalam skenario ini yaitu, pengujian saat melakukan serangan DDoS dengan *service* HTTP *allow*

GAMBAR 7
PENGUJIAN SAAT SERANGAN SERVICE HTTP ALLOW

c. Pengujian Sesudah Serangan

Tahap ke tiga dalam skenario ini yaitu, pengujian sesudah melakukan serangan DDoS dengan *service* HTTP *allow*



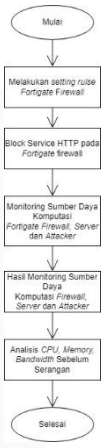
GAMBAR 8
PENGUJIAN SETELAH SERANGAN *SERVICE* HTTP *ALLOW*

2. Skenario 2: *Service* HTTP *Block*

Pada skenario 2 dilakukan pengujian dengan memblokir akses *web server* pada *service* HTTP. Pada skenario ini terdiri dari tiga pengujian yaitu, pengujian sebelum serangan, saat serangan dan sesudah pengujian.

a. Pengujian Sebelum Serangan

Tahap pertama dalam skenario ini yaitu, pengujian sebelum melakukan serangan DDoS dengan *service* HTTP *block*.



GAMBAR 9
PENGUJIAN SEBELUM SERANGAN *SERVICE* HTTP *BLOCK*

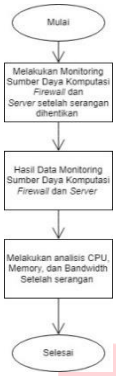
b. Pengujian Saat Serangan

Tahap ke dua dalam skenario ini yaitu, pengujian saat melakukan serangan DDoS dengan *service* HTTP *block*

GAMBAR 10
PENGUJIAN SAAT SERANGAN *SERVICE* HTTP *BLOCK*

c. Pengujian Sesudah Serangan

Tahap ke tiga dalam skenario ini yaitu, pengujian sesudah melakukan serangan DDoS dengan *service* HTTP *block*



GAMBAR 11
PENGUJIAN SESUDAH SERANGAN *SERVICE* HTTP *BLOCK*

C. Implementasi dan Analisis Hasil Pembahasan

Pada bab ini dilakukan analisis hasil pengujian dari bab sebelumnya, bertujuan untuk mengetahui perbandingan antara pengujian sebelum, saat dan sesudah dilakukan serangan pada setiap hasil sumber daya komputasi CPU, memory dan session. Pada perbandingan analisis ini dibedakan berdasarkan dua skenario yaitu skenario 1 analisis pengujian pada service HTTP allow dan skenario 2 analisis pengujian pada service HTTP block.

1. Perbandingan Hasil Analisis Pengujian *Service* HTTP *Allow* dengan *Service* HTTP *Block*

Dalam melakukan analisis hasil perbandingan dari sebelum serangan, saat serangan, setelah serangan pada pengujian *service* HTTP *allow* dan *service* HTTP *block* berdasarkan perbedaan pada spesifikasi *memory* pada *firewall* yaitu:

1. 1,5 GB *memory.*
2. 2 GB *memory.*

Serta perbedaan dari jumlah paket yang dilakukan pada saat pemantauan sumber daya komputasi. Berikut penjelasan perbandingan hasil persentase penggunaan sumber daya komputasi.

a. Sebelum Serangan

Perbandingan hasil analisis sebelum serangan dengan *service* HTTP *allow* dan *service* HTTP *block* didapatkan nilai hasil yang sama pada setiap pengukuran penggunaan sumber daya komputasi pada *firewall, attacker* dan *server* dikarenakan tidak adanya aktivitas atau serangan yang membanjiri *traffic firewall* sehingga tidak terjadinya peningkatan pada sumber daya komputasi. Hasil yang didapatkan pada spesifikasi 1,5 GB *memory* pada penggunaan CPU *firewall*, *attacker,* dan *server* sebagai berikut:

1. Pada *firewall* penggunaan CPU berada pada range 0-2%.
2. Pada *attacker* penggunaan CPU berada pada range 1-2%.
3. Pada *server* penggunaan CPU berada pada range 0-0,3.

Sedangkan pada spesifikasi 2 GB *memory* pada penggunaan CPU *firewall*, *attacker*, dan *server* sebagai berikut:

1. Pada *firewall* penggunaan CPU berada pada range 0-1%.
2. Pada *attacker* penggunaan CPU berada pada range 1-2%.
3. Pada *server* penggunaan CPU berada pada range 0-0,3.

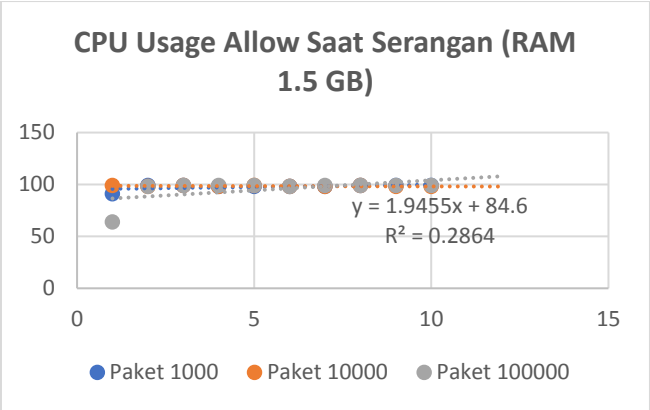
b. Saat Serangan

Perbandingan hasil analisis saat serangan berdasarkan penggunaan sumber daya komputasi CPU, *memory* pada *firewall* dengan *service* HTTP *allow* dan *service* HTTP *block* berdasarkan spesifikasi fortigate 1,5 GB memory dan 2 GB *memory*, diperoleh hasil peningkatan yang sama pada penggunaan sumber daya komputasi *firewall*. Hal tersebut dikarenakan pengaruh pada *firewall* yang dapat melindungi *server* dari serangan DDoS yang melintas pada fortigate *firewall.* Penggunaan CPU *firewall* saat serangan mengalami peningkatan mencapai range 98-100%. Peningkatan penggunaan CPU terjadi pada menit-menit pertama saat dilakukannya serangan. Sedangkan pada penggunaan *memory* diperoleh perbedaan hasil pada spesifikasi yang berbeda, dikarenakan perbedaan ini dipengaruhi oleh perubahan *memory* pada spesifikasi *firewall.* Diperoleh perbedaan hasil penggunaan pada *memory* sebagai berikut:

1. Nilai penggunaan *memory* pada spesifikasi 1,5 GB *memory* dengan *service* HTTP *allow* cenderung lebih besar yaitu 83,7%, sedangkan pada *service* HTTP *block* diperoleh nilai yang lebih rendah yaitu 73,7%.
2. Nilai penggunaan *memory* pada spesifikasi 2 GB *memory* dengan *service* HTTP *allow* cenderung lebih besar yaitu 66,2%, sedangkan pada *service* HTTP *block* diperoleh nilai yang lebih rendah yaitu 58,2%.

1. Penggunaan CPU *Firewall*

Konsumsi penggunaan sumber daya komptasi tertinggi pertama yaitu CPU *firewall*. Penggunaan sumber daya komputasi CPU mengalami kenaikan pada setiap jumlah paket yang dikirimkan saat dilakukan serangan pada *service* HTTP *allow* dan *service* HTTP *block.* Berikut hasil persentase penggunaan CPU *service* HTTP *allow* dan *service* HTTP *block* pada spesifikasi 1,5 GB *memory* dan *2* GB *memory*.

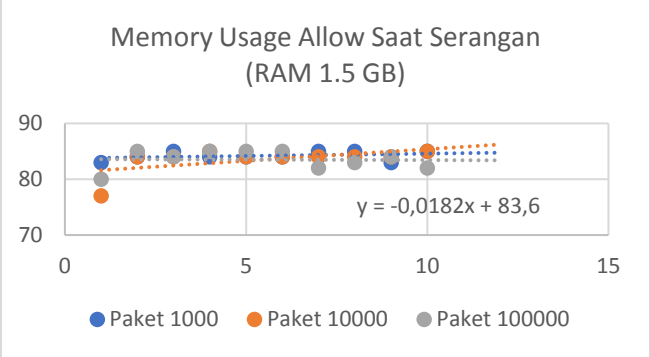


GAMBAR 12
GRAFIK HASIL PERSENTASE PENGGUNAAN CPU *SERVICE* HTTP *ALLOW* 1,5 GB *MEMORY*

Berdasarkan Gambar 10, hasil persentase penggunaan CPU *firewall* pada *service* HTTP *allow* dengan spesifikasi 1,5 GB *memory*, diperoleh hasil persentase rata-rata sebesar 97,1%. Rumus gradien linear menunjukkan hasil persentase penggunaan CPU *firewall* pada *service* HTTP *allow* mengalami kenaikan secara linear. Rumus yang digunakan untuk gradien linear adalah "y=mx+c", dengan persamaan linear pada penggunaan CPU pada *service* HTTP *allow* 1,5 GB *memory* yaitu "y=1,9455x+84,6".

2. Penggunaan *memory Firewall*

Konsumsi penggunaan sumber daya komptasi kedua yaitu *memory firewall*. Penggunaan sumber daya komputasi *memory* mengalami kenaikan pada setiap jumlah paket yang dikirimkan saat dilakukan serangan pada *service* HTTP *allow* dan *service* HTTP *block.* Berikut hasil persentase penggunaan *memory service* HTTP *allow* dan *service* HTTP *block* pada spesifikasi 1,5 GB *memory* dan *2* GB *memory.*



GAMBAR 13
GRAFIK HASIL PERSENTASE PENGGUNAAN *MEMORY SERVICE* HTTP *ALLOW* 1,5 GB *MEMORY*

Berdasarkan Gambar 13, hasil persentase penggunaan *memory firewall* pada *service* HTTP *allow* dengan spesifikasi 1,5 GB *memory*, diperoleh hasil persentase rata-rata sebesar 83,7%. Rumus gradien linear menunjukkan hasil persentase penggunaan *memory firewall* pada *service* HTTP *allow* mengalami kenaikan secara linear. Rumus yang digunakan untuk gradien linear adalah "y=mx+c", dengan persamaan linear pada penggunaan *memory* pada *service* HTTP *allow* 1,5 GB *memory* yaitu "y=-0,0182x+83,6".

Berdasarkan hasil persentase pada grafik penggunaan sumber daya komputasi pada *firewall* yaitu CPU dan *memory* dengan *service* HTTP *allow* dan *service* HTTP *block*. Menunjukkan bahwa peningkatan sumber daya komputasi tertinggi diperoleh pada sumber daya komputasi CPU yaitu sebesar 97,1%. Selanjutnya peningkatan kedua diperoleh pada sumber daya komputasi *memory* yaitu sebesar 83,7%. Penggunaan CPU dan *memory* menunjukkan bahwa penggunaan sumber daya komputasi telah mencapai nilai *threshold* diatas 70%-80%, maka dapat dikatakan bahwa penggunaan sumber daya komputasi CPU dan *memory* pada *firewall* saat serangan DDoS dijalankan dalam kondisi yang aman.

c. Setelah Serangan

Berdasarkan perbandingan hasil analisis setelah serangan pada pengujian *service* HTTP *allow* dan *service* HTTP *block* berdasarkan penggunaan sumber daya komputasi CPU dan *memory* pada *firewall* dengan spesifikasi yang berbeda yaitu:

1. Spesifikasi 1,5 GB *memory*, 1 *core* CPU.
2. Spesifikasi 1,5 GB *memory*, 1 *core* CPU.

Terjadi penurunan persentase dari CPU dan *memory* selama 10 menit pengujian. Hal tersebut dipengaruhi karena tidak adanya *traffic* yang membanjiri *firewall* karena serangan sudah diberhentikan.

V. KESIMPULAN

A. Kesimpulan

Penelitian ini menghasilkan kesimpulan sebagai berikut:

1. Untuk melakukan implementasi fungsi *firewall* untuk melindungi aset IT, dibutuhkan sumber daya komputasi CPU dan *memory* yang lebih besar dari penelitian ini. Sumber daya komputasi yang sesuai dapat melindungi aset IT dengan optimal.
2. Untuk mengetahui profil *firewall*, dilakukan *profiling* sistem pada *virtualized* Fortigate *firewall* dengan dibedakan *rules firewall* yang diimplementasi pada *virtualized* Fortigate *firewall*, yaitu *service* HTTP *allow* dan *service* HTTP *block*. *Rules firewall* digunakan untuk membandingkan profil sistem *virtualized* Fortigate *firewall* berdasarkan konsumsi sumber daya komputasi pada *firewall*.

B. Saran

Berdasarkan hasil analisis dan pengujian yang telah dilakukan, berikut berupa saran yang dapat disampaikan:

1. Adanya kekurangan pada spesifikasi *appliance* dikarenakan pada eksperimen virtualisasi fortigate firewall ini maksimum spesifikasi *memory* dan CPU yang dapat diimplementasi sebesar 2 GB *memory* dan 1 *core* CPU saja. Disarankan untuk menggunakan Fortigate *firewall* dengan spesifikasi lebih tinggi yang berupa *appliances*.

2. Melakukan serangan DDoS dengan jenis yang lain untuk mendapatkan gambaran profil yang menyeluruh.

3. Melakukan profiling pada *attacker* & *server* layanan agar mendapatkan relasi yang luas.

REFERENSI

[1] I. A. Paramitha, "Tinjauan Pustaka Tinjauan Pustaka," *Conv. Cent. Di Kota Tegal*, pp. 6–37, 2017.

[2] E. D. Zwicky, S. Copper, and D. B. Chapman, "Building Internet Firewall," p. 78, 2020.

[3] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) Menggunakan Metode Data Mining Naïve Bayes memperoleh gelar Sarjana Komputer Disusun oleh :," *Univ. Brawijaya*, vol. 6, no. 1, p. 63, 2021.

[4] Y. Zamrodah, "Penggunaan NMAP dan Hping3 Dalam Menganalisa Keamanan Jaringan pada B2P2TO2T" vol. 15, no. 2, pp. 1–23, 2016.

[5] S. N. Khasanah and S. J. Kuryanti, "Rancangan Virtualisasi Server Menggunakan VMWare Vsphare," *EVOLUSI - J. Sains dan Manaj.*, vol. 7, no. 1, pp. 42–46, 2019, doi: 10.31294/evolusi.v7i1.5091.

[6] D. I. Permatasari, "Pengujian Aplikasi menggunakan metode Load Testing dengan Apache JMeter pada Sistem Informasi Pertanian," *J. Sist. dan Teknol. Inf.*, vol. 8, no. 1, p. 135, 2020, doi: 10.26418/justin.v8i1.34452.