Implementasi Dan Analisis Profil Sistem Pada Virtualisasi Sophos *Firewall* Berdasarkan Metrik Sumber Daya Komputasi

Implementation And Analysis Of System Profile On Sophos Firewall Virtualization Based On Computing Resource Metrics

1st Lathifa Artaminati
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
lathifaartaminati@student.telkomuniversity.ac.id

2nd Adityas Widjajarto[2]
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— *Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melalauinya dan mencegah lalu lintas jaringan yang tidak aman. *Firewall* dapat digunakan untuk mencegah serangan pada layanan IT. Pada penelitian ini melakukan implementasi *firewall* pada *load testing*. Penelitian ini menggunakan studi literatur dan analisa monitoring pengukuran penggunaan sumber daya komputasi sebagai metode untuk melakukan pengujian. Pengujian dilakukan meggunakan dua skenario pengujian serangan yaitu *service* HTTP *allow* dan *service* HTTP *block* dengan melakukan monitoring pada tiga jenis klasifikasi serangan yaitu sebellum , saat, dan setelah serangan. Pada penelitian ini menggunakan *virtualized* Sophos *firewall* versi 16.3.2 dengan RAM 3,5 GB dan 4 GB untuk melakukan pengujian atau Ekperimen. Eksperimen pada skala laboratorium berupa *virtualized* Sophos *firewall* dengan *rules firewall* untuk menangani serangan DDoS SYN *flood* dari Kali Linux yang mengarah ke *web server* di Ubuntu *server*. Hasil eksperimen pada *firewall* berupa konsumsi sumber daya komputasi tertinggi yaitu CPU 98,7%, *memory* 72% dan *session* 243837,53. Untuk kelanjutan penelitian dapat berupa profil yang menggambarkan relasi antara serangan, *firewall,* dan *server*.

Kata kunci— *virtualized* sophos, *firewall, profiling, monitoring,* sumber daya komputasi

I. PENDAHULUAN

Aspek keamanan jaringan biasanya dinyatakan dalam (*confidentiality*) data dan informasi hanya dapat diakses oleh siapapun yang berwenang, menjamin integritas (*integrity*) data dan informasi hanya dapat dimodifikasi oleh pihak yang berwenang, serta ketersediaan *(availability)* informasi yang dapat diakses dengan mudah ketika dibutuhkan. Berdasarkan dari aspek keamanan jaringan, khususnya pada layanan *availability,* ancaman terhadap jaringan komputer seperti *Distributed Denial of Service* (DDoS) harus dicegah dan ditanggulangi agar tidak merugikan banyak pihak. Cara kerja *Distributed Denial of Service* (DDoS) yaitu dengan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan. Salah satu cara mencegah dan menanggulanginya yaitu dengan mengamankan sistem menggunakan *firewall. Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. *Firewall* berfungsi untuk mencegah akses dari pihak luar ke sistem internal. Dengan demikian, data – data yang berada dalam jaringan komputer tidak dapat diakses oleh pihak luar. Pada penelitian ini, *Next-Generation Firewall* berfungsi untuk melakukan pemblokiran terhadap serangan *cyber* yang dianggap berbahaya, melakukan perlindungan terhadap target (*server),* dan melakukan pemblokiran lalu lintas jaringan menggunakan *rules firewall* yang telah ditentukan untuk melindungi *server* dari ancaman DDoS. Pada tugas akhir ini, penelitian menjalankan implementasi *firewall* dan melakukan *profiling* sistem *virtualized* Sophos *firewall* guna mengetahui sumber daya komputasi pada fungsi deteksi, pencegahan, dan pemulihan terhadap pertahanan pada layanan *availability* yang ada pada *firewall*. Pada *Profiling* sistem *virtualized* Sophos *firewall* terdapat dua skenario pengujian yaitu *service* HTTP *allow* dan *service* HTTP *block* denga RAM Sophos 3,5 GB dan 4 GB terhadap *load testing* berdasarkan penggunaan sumber daya komputasi pada saat sebelum, saat, dan setelah serangan. Selanjutnya pada analisis, dilakukan perbandingan data hasil pengujian pada konsumsi penggunaan sumber daya komputasi pada *firewall* sebelum, saat, dan setelah serangan terhadap *load testing.*

II. KAJIAN TEORI

A. Keamanan Jaringan

Keamanan jaringan merupakan suatu cara yang difungsikan untuk memberikan perlindungan terhadap suatu jaringan agar terhindar dari berbagai ancaman yang berasal dari jaringan luar dengan tujuan merusak atau mencuri data [1].

B. *Firewall*

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman [3].

C. Sophos

Sophos *Firewall Operating System* adalah sistem operasi yang dibuat khusus untuk menjadi fondasi dari perangkat lunak *firewall* Sophos XG. Sophos *Firewall* dapat melindungi jaringan dari ancaman terbaru seperti *ransomware, cryptomining, bot, worm,* retas, serangan DDoS, pelanggaran dan APT.

D. *Distributed Denial of Service* (DDoS)

Distibute Denial of Service (DDoS) adalah jenis serangan *cyber* yang diakibatkan oleh banjirnya jaringan internet oleh *fake traffic* (lalu lintas intrnet) pada sistem, *server*, atau jaringan.

E. Hping3

Hping3 adalah sebuah TCP/IP assembler dan juga merupakan *command-line* yang berorientasi pada pemrosesan paket TCP/IP. Kelebihan Hping3, yaitu untuk pengecekan kondisi komputer dan *port – port*nya, paket yang dikirimkan dapat berupa TCP, UDP atau ICMP, dan aplikasi ini berukuran kecil sehingga ringan dijalankan [4].

F. Sumber Daya Komputasi

Sumber Daya Komputasi merupakan seperangkat teknologi yang digunakan dalam bentuk perangkat komputer, terdiri dari perangkat keras dan perangkat lunak dan digunakan untuk membantu fungsi tugas manusia [5].

G. CPU

CPU berfungsi untuk memproses berbagai macam data dan instruksi, *processor* ini sangat penting peranannya dalam menentukan kerja PC [6].

H. *Memory*

Memory berfungsi untuk melakukan penyimpanan baik permanen atau sementara [7].

I. *Load Testing*

Load testing adalah salah satu jenis pengujian performansi sebuah sistem yang dapat disimulasikan untuk menangani beban yang sesuai dengan beban sesungguhnya di lingkungan pengguna [8].

III. METODE

A. Model Konseptual Penelitian

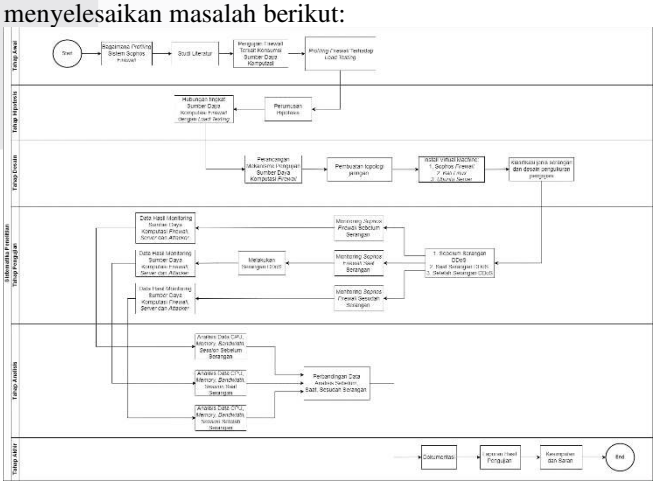
Model konseptual ini bertujuan untuk memudahkan dalam melakukan identifikasi permasalahan yang ditemukan pada penelitian ini yaitu, sebagai berikut:

GAMBAR 1
MODEL KONSEPTUAL PENELITIAN

Pada Gambar 1 menggambarkan mengenai konsep penelitian yang terdiri dari tiga bagian yaitu lingkungan, penelitian dan dasar ilmu. Pada bagian lingkungan terdapat *problems* dan *technology* pada penelitian ini. Selanjutnya, pada bagian penelitian terdapat "Membangun" yaitu melakukan *profiling firewall* berdasarkan analisis sumber daya komputasi terhadap *availability* dari Sophos *firewall.* Kemudian pada "Evaluasi" menggambarkan kegiatan atau aktivitas yang akan dilakukan pada penelitian ini, yaitu *profiling* sistem Sophos *firewall,* pola konsumsi pengujian DDoS, pengujian *firewall* terhadap layanan *availability,* dan melakukan *monitoring* sumber daya komputasi *firewall.* Dasar ilmu yang menjadi landasan dasar teori yang digunakan pada penelitian ini mencakup teori keamanan informasi, keamanan jaringan, *firewall,* sumber daya komputasi, dan jenis serangan dan didukung dengan menggunakan metode yaitu studi literatur dan analisis *monitoring* dan pengukuran sumber daya komputasi.

B. Sistematika Penelitian

Sistematika penelitian digunakan sebagai gambaran dalam menyelesaikan masalah berikut:



GAMBAR 2
SISTEMATIKA PENELITIAN

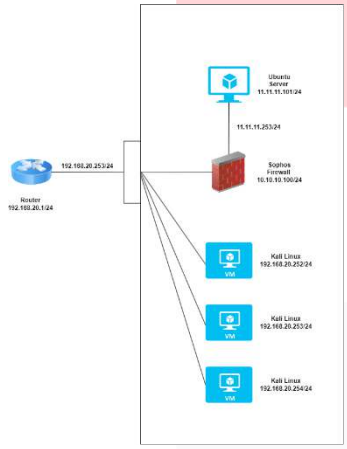
IV. HASIL DAN PEMBAHASAN

A. Rancangan Sistem

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

1. Topologi Jaringan

Topologi jaringan digunakan untuk menggambarkan pengujian 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* yaitu sebagai berikut**:**

TABEL 1
DAFTAR IP ADDRESS

Nama	Host	Default Gateway	IP Address
Router	Mikrotik Rb952	192.168.20.1/24	192.168.20.1/24
VM1	Sophos *Firewall*		IP WAN: 192.168.20.253/24 IP LAN: 10.10.10.100/24
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 NAT: 192.168.20.100 IP Static: 11.11.11.101

B. Skenario Pengujian

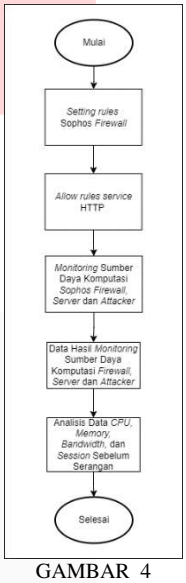
Pada penelitian ini, terdapat dua skenario pengujian yang dilakukan yaitu, skenario pertama dengan *service* HTTP *allow* dan skenario kedua dengan *service* HTTP di *block*. Masing – masing skenario memiliki tiga jenis klasifikasi pengujian yaitu, sebelum serangan, saat serangan, dan setelah serangan.

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

Pada skenario *service* HTTP *allow,* melakukan pengujian dengan cara memberikan hak akses pada *web server* atau target untuk dapat mengakses *service* HTTP.

a) Pengujian Sebelum Serangan

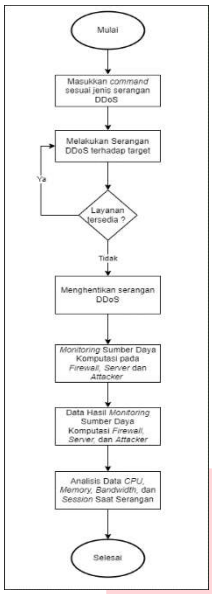
Tahap pertama dalam skenario ini yaitu, pengujian sebelum melakukan serangan DDoS dengan *service* HTTP *allow*



GAMBAR 4
PENGUJIAN SEBELUM SERANGAN *SERVICE* HTTP *ALLOW*

b) Pengujian Saat Serangan

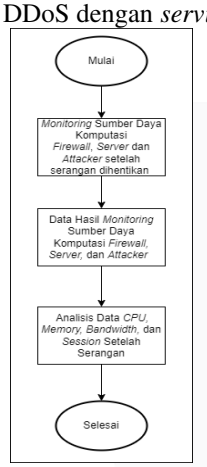
Tahap pertama dalam skenario ini yaitu, pengujian saat melakukan serangan DDoS dengan *service* HTTP *allow*



GAMBAR 5
PENGUJIAN SAAT SERANGAN *SERVICE* HTTP *ALLOW*

c) Pengujian Sesudah Serangan

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



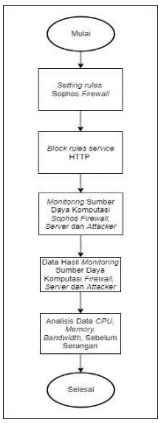
GAMBAR 6
PENGUJIAN SESUDAH SERANGAN *SERVICE* HTTP *ALLOW*

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

Pada skenario *service* HTTP *block,* melakukan pengujian dengan cara memblokir hak akses *web server* atau target agar tidak dapat mengakses *service* HTTP.

a) Pengujian Sebelum Serangan

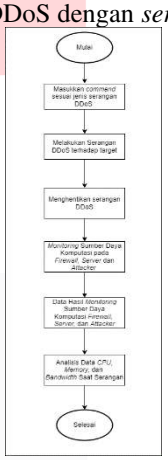
Tahap pertama dalam skenario ini yaitu, pengujian sebelum melakukan serangan DDoS dengan *service* HTTP *block*.



GAMBAR 7
PENGUJIAN SEBELUM SERANGAN *SERVICE* HTTP *BLOCK*

b) Pengujian Saat Serangan

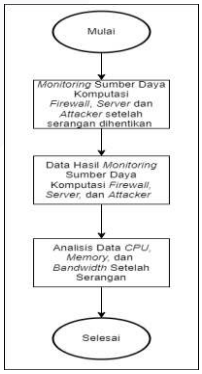
Tahap pertama dalam skenario ini yaitu, pengujian saat melakukan serangan DDoS dengan *service* HTTP *block*



GAMBAR 8
PENGUJIAN SAAT SERANGAN *SERVICE* HTTP *BLOCK*

C. Pengujian Sesudah Serangan

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



GAMBAR 9
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 hasil analisis dibedakan berdasarkan dua skenario pengujian yaitu skenario pengujian

pada *service* HTTP *allow* dan skenario pengujian pada *service* HTTP *block*.

1. Perbandingan Hasil Persentase Sumber Daya Komputasi

Dalam melakukan analisis hasil perbandingan sebelum serangan, saat serangan, dan setelah serangan pada pengujian *service* HTTP *allow* dan *service* HTTP *block* pada setiap jumlah paket berdasarkan *memory* RAM Sophos *firewall* yaitu RAM 3,5 GB dan 4 GB. Diperoleh hasil persentase pada CPU dan *memory firewall.*

a. Sebelum Serangan

Berdasarkan perbandingan hasil analisis sebelum serangan pada skenario pengujian *service* HTTP *allow* dan *service* HTTP *block*, diperoleh nilai rata-rata yang sama pada setiap jumlah paket penggunaan sumber daya komputasi pada *firewall, attacker* dan *server.* Hal tersebut dipengaruhi oleh tidak adanya aktivitas atau proses, dan serangan yang berjalan sehingga tidak terjadi peningkatan pada nilai penggunaan sumber daya komputasi. Hasil yng diperoleh pada *memory* RAM 3,5 GB penggunaan CPU *firewall* berada pada *range* 1-3%, sedangkan pada *memory* RAM 4 GB berada pada *range* 1-4%.

b. Saat Serangan

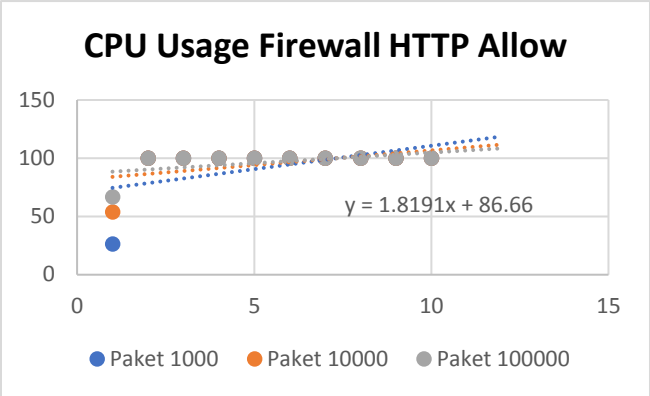
Perbandingan hasil analisis saat serangan pada skenario pengujian *service* HTTP *allow* dan *service* HTTP *block* diperoleh hasil yang hampir sama dan terjadi peningkatan pada penggunaan sumber daya komputasi *firewall* dengan *memory* RAM Sophos yaitu RAM 3,5 GB dan RAM 4 GB. Hal tersebut dipengaruhi oleh fungsi *firewall* yang dapat melindungi target *server* dari serangan DDoS yang melintas pada Sophos *firewall.* Penggunaan CPU *firewall* saat serangan mengalami peningkatan mencapai 100%. Peningkatan penggunaan CPU *firewall* rata-rata terjadi pada menit pertama saat melakukan serangan. Lain hal dengan penggunaan *memory* pada *firewall,* diperoleh perbedaan hasil penggunaan pada *memory* RAM 3,5 GB dan 4 GB, sebagai berikut:

a) Nilai penggunaan *memory* pada *memory* RAM 3,5 GB dengan *service* HTTP *allow* cenderung lebih rendah yaitu sebesar 69,2%, sedangkan pada *service* HTTP *block* diperoleh nilai yang lebih tinggi sebesar 72%.

b) Nilai penggunaan *memory* pada *memory* RAM 4 GB dengan *service* HTTP *allow* cenderung lebih tinggi yaitu sebesar 62,6%, sedangkan pada *service* HTTP *block* diperoleh nilai yang lebih rendah sebesar 58,35%.

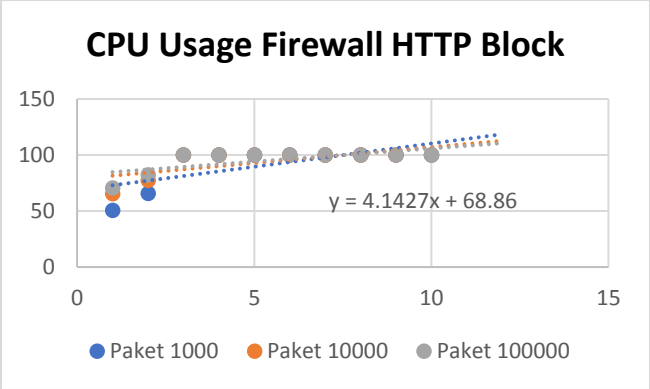
c) Penggunaan CPU *Firewall*

Konsumsi penggunaan sumber daya komputasi tertinggi kedua pada karakteristik Sophos *firewall* yaitu pada penggunaan sumber daya *memory*. Penggunaan sumber daya *memory* mengalami kenaikan pada setiap jumlah paket yang dikirimkan saat serangan pada *service* HTTP *allow* dan *service* HTTP *block.*



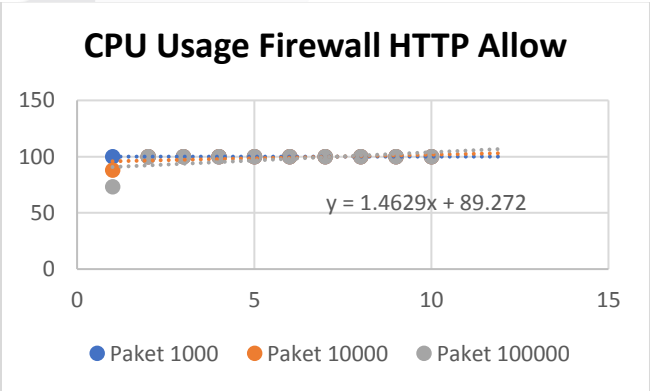
GAMBAR 10
GRAFIK PERSENTASE PENGGUNAAN CPU *ALLOW*
(RAM 3,5 GB)

Berdasarkan Gambar 10, hasil persentase penggunaan CPU *firewall* pada *service* dengan *memory* RAM 3,5 GB, diperoleh hasil persentase sebesar 94,8%.



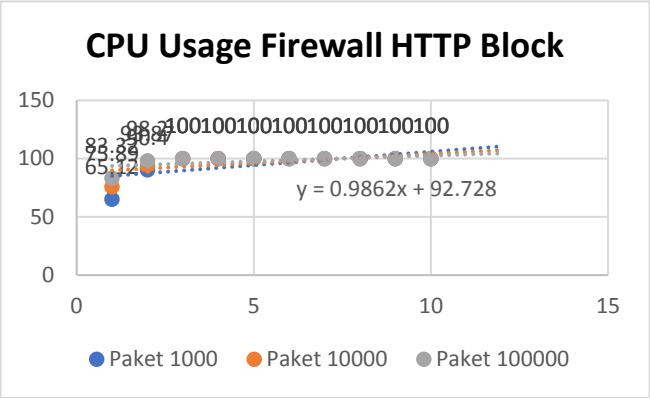
GAMBAR 11
GRAFIK PERSENTASE PENGGUNAAN CPU *BLOCK*
(RAM 3,5 GB)

Berdasarkan Gambar 11, hasil persentse penggunaan CPU *firewall* pada *service* HTTP *block* dengan *memory* RAM 3,5 GB, diperoleh hasil persentase sebesar 93,7%.



GAMBAR 12
GRAFIK PERSENTASE PENGGUNAAN CPU *ALLOW*
(RAM 4 GB)

Berdasarkan Gambar 12, hasil persentse penggunaan CPU *firewall* pada *service* HTTP *block* dengan *memory* RAM 4 GB, diperoleh hasil persentase sebesar 98,7%.

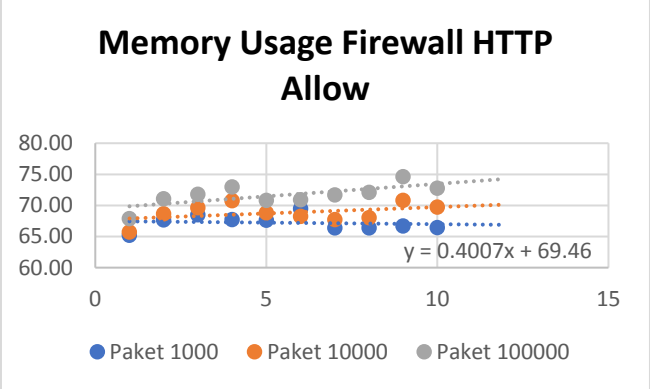


GAMBAR 13
GRAFIK HASIL PERSENTASE PENGGUNAAN CPU *BLOCK* (RAM 4 GB)

Berdasarkan Gambar 13, hasil persentase penggunaan CPU *firewall* pada *service* dengan *memory* RAM 4 GB, diperoleh hasil persentase sebesar 96,8%.

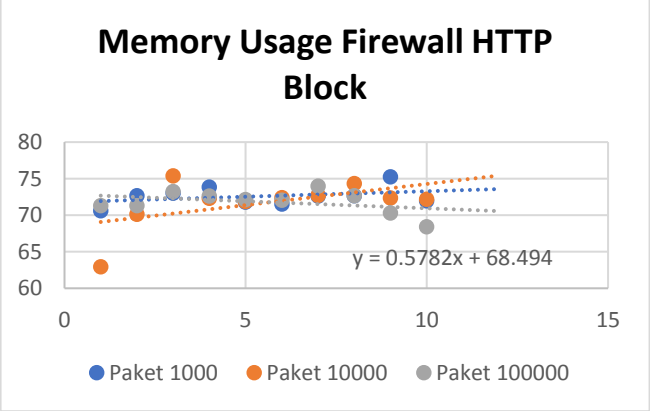
2. Penggunaan *Memory Firewall*

Konsumsi penggunaan sumber daya komputasi tertinggi kedua pada karakteristik Sophos *firewall* yaitu pada penggunaan sumber daya *memory*. Penggunaan sumber daya *memory* mengalami kenaikan pada setiap jumlah paket yang dikirimkan saat serangan pada *service* HTTP *allow* dan *service* HTTP *block.*



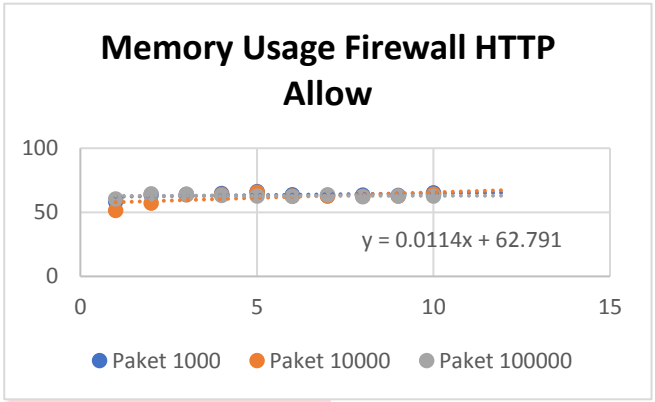
GAMBAR 14
GRAFIK HASIL PERSENTASE PENGGUNAAN *MEMORY ALLOW* (RAM 3,5 GB)

Berdasarkan Gambar 14, hasil persentse penggunaan *memory firewall* pada *service* HTTP *allow* dengan *memory* RAM 3,5 GB, diperoleh hasil persentase sebesar 69,2%.



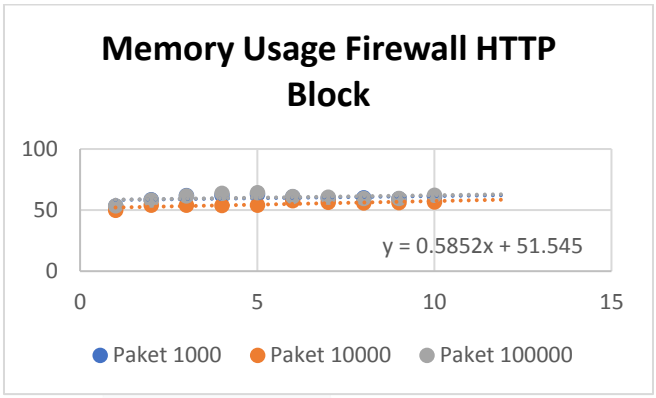
GAMBAR 15
GRAFIK HASIL PERSENTASE PENGGUNAAN *MEMORY BLOCK* (RAM 3,5 GB)

Berdasarkan Gambar 15, hasil persentse penggunaan *memory firewall* pada *service* HTTP *block* dengan *memory* RAM 3,5 GB, diperoleh hasil persentase sebesar 72%.



GAMBAR 16
GRAFIK HASIL PERSENTASE PENGGUNAAN *MEMORY ALLOW* (RAM 4 GB)

Berdasarkan Gambar 16, hasil persentse penggunaan *memory firewall* pada *service* HTTP *allow* dengan *memory* RAM 4 GB, diperoleh hasil persentase sebesar 62%.



GAMBAR 17
GRAFIK HASIL PERSENTASE PENGGUNAAN *MEMORY BLOCK* (RAM 4 GB)

Berdasarkan Gambar V- 96, hasil persentse penggunaan *memory firewall* pada *service* HTTP *block* dengan *memory* RAM 4 GB, diperoleh hasil persentase sebesar 58,3%.

c) Setelah Serangan

Berdasarkan perbandingan hasil analisis setelah serangan pada skenario pengujian *service* HTTP *allow* dan *service* HTTP *block* berdasarkan penggunaan sumber daya komputasi CPU dan *memory* pada *firewall, attacker,* dan *server* dengan *memory* RAM 3.5 GB dan 4 GB, terjadi penurunan selama 10 menit pada penggunaan sumber daya komputasi CPU dan *memory.* Hal tersebut dipengaruhi oleh tidak ada *traffic* yang membanjiri *firewall* karena serangan telah dihentikan.

V. KESIMPULAN

A. Kesimpulan

Berdasarkan hasil analisis dan pengujian dari penggunaan sumber daya komputasi yang dilakukan pada pengujian profil sistem Sophos *firewall,* dapat diambil kesimpulan,yaitu:

1. *Profiling* sistem *virtualized* Sophos *firewall* memberikan minimal *memory* 3.5 GB untuk fungsi *booting*. Dengan *memory* 4 GB Sophos dapat bekerja secara terbatas untuk fungsi proteksi DDoS SYN *flood* menggunakan Hping3.
2. *Profiling* sistem *virtualized* Sophos *firewall* dibedakan berdasarkan *rules* Sophos *firewall,* yaitu *service* HTTP *allow* dan *service* HTTP *block,* dan konsumsi penggunaan sumber daya komputasi tertinggi terjadi pada sumber daya CPU 98,7%.
3. Untuk sumber daya *memory,* mengalami peningkatan konsumsi penggunaan sumber daya tertinggi terjadi saat serangan sebesar 72%. Selanjutnya, konsumsi peningkatan pada pada *bandwidth* saat serangan sebesar 247,675Mbps. Kemudian, peningkatan pada *session* terjadi saat serangan pada *service* HTTP *allow* sebesar 243837,53.

B. Saran

Berdasarkan analisis dan pengujian pada penggunaan sumber daya komputasi yang dilakukan, berikut beberapa saran:

1. Pengujian lanjut dapat dilakukan dengan menggunakan *memory* yang lebih besar dari hasil penelitian ini untuk mendapatkan profil virtualisasi Sophos *firewall* yang lebih lengkap dan luas.
2. Menggunakan *virtualized* Sophos *Firewall* yang berupa *appliance* dengan spesifikasi yang lebih tinggi untuk mendapatkan profil Sophos.

REFERENSI

[1] O. A. M. A. H Kara, “済無No Title No Title No Title,” *Pap. Knowl. . Towar. a Media Hist. Doc.*, vol. 7, no. 2, pp. 107–15, 2014.

[3] A. Hikmaturokhman, A. Purwanto, and R. Munadi, “Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router,” *Semin. Nas. Inform.*, vol. 1, no. 3, pp. 1–8, 2015.

[4] Y. Zamrodah, “済無No Title No Title No Title,” vol. 15, no. 2, pp. 1–23, 2016.

[5] D. Tarigan and U. M. Buana, “Sistem Informasi Manajemen Keamanan Informasi dalam Pemanfaatan Teknologi Informasi Desi Ramadani Br Tarigan,” no. July, pp. 0–17, 2020.

[6] N. Annisa, “Mini Tinjauan Perangkat Keras Komputer,” *J. Komput.*, pp. 1–20, 2021.

[7] RI No. 43 20Permenkes19, *No Title*□, no. 2. 2019.

[8] K. Pustaka, “1. kajian pustaka 2.1,” pp. 1–17.