Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

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

Ni Made Meliana Listyawati*, Adityas Widjajarto, M Teguh Kurniawan

Fakultas Rekayasa Industri, Sistem Informasi, Universitas Telkom, Bandung, Indonesia
Email: [1*]nimademeliana@student.telkomuniversity.co.id, [2]adwjrt@telkomuniversity.co.id,
[3]teguhkurniawan@telkomuniversity.ac.id
Email Penulis Korespondensi: nimademeliana@student.telkomuniversity.co.id
Submitted: **02/09/2022**; Accepted: **26/09/2022**; Published: **30/09/2022**

Abstrak–Pada aspek keamanan, perlu diketahui seberapa efektif *firewall* dapat melindungi perangkat jaringan dari serangan DDoS. Karakteristik pada suatu *firewall* memiliki fungsi yang berbeda-beda dalam melindungi sistem dari berbagai serangan luar yang dapat menyerang dan mengambil suatu data. Pada penelitian ini melakukan implementasi virtualisasi Paloalto *firewall* yang bertujuan untuk mendapatkan fungsi profil sistem pada *firewall* berdasarkan penggunana sumber daya komputasi. *Profiling* sistem *firewall* yang diteliti berdasarkan konsumsi sumber daya komputasi pada *load testing*. Pada eksperimen ini menggunakan serangan DDoS SYN *flood* pada Kali Linux sebagai *attacker*, virtualisasi Paloalto *firewall* yang melindungi *web server* pada Ubuntu Server sebagai target serangan. Pada penelitian ini dibedakan berdasarkan dua skenario pengujian yaitu berdasarkan pengujian *service* HTTP *allow* dengan pengujian *service* HTTP *block* dengan spesifikasi *memory* Paloalto pada RAM 5.5 GB dan spesifikasi RAM 8 GB. Dilakukan pengukuran berdasarkan sumber daya komputasi pada CPU, *memory* dan *session* yang berfokus pada sebelum, saat dan sesudah serangan DDoS SYN *flood*. Pola Penggunaan sumber daya komputasi cenderung linear saat terjadinya serangan DDoS SYN *flood*. Hasil eksperimen yang didapatkan pada penggunaan sumber daya komputasi tertinggi saat serangan adalah penggunaan CPU dengan rata-rata persentase sebesar 95.8%, selanjutnya peningkatan ke dua yaitu pada penggunaan memory dengan rata-rata persentase sebesar 44%, dan urutan terakhir pada session sebesar 138682. Untuk penelitian selanjutnya dapat menggunakan variasi serangan DDoS untuk mendapatkan profil yang lebih luas.

Kata Kunci: Paloalto; Profiling; Sumber Daya Komputasi; Testing; Virtualisasi.

Abstract–On the security aspect, it is necessary to know how effectively a firewall can protect network devices from DDoS attacks. The characteristics of a firewall have different functions in protecting the system from various external attacks that can attack and retrieve data. In this research, the implementation of Paloalto firewall virtualization aims to obtain the system profile function on the firewall based on the use of computing resources. Profiling of the firewall system of this experiment based on the consumption of computing resources in load testing. This experiment used a DDoS SYN flood attack on Kali Linux as an attacker and a virtualization Paloalto firewall that protects a web server on Ubuntu Server as an attack target. This research distinguished based on two test scenarios, namely based on testing the service HTTP allow and service HTTP block with Paloalto memory specifications at RAM 5.5 GB and RAM 8 GB specifications. Measurements were made based on computing resources on CPU, memory, and a session focused on before, during, and after DDoS SYN flood attacks. The pattern of usage of computing resources tends to be linear when a DDoS SYN flood attack occurs. The experimental results obtained on the highest use of computing resources during the attack were CPU usage with an average percentage of 95.8% and the second increase was in memory usage with an average percentage of 44%, and the session usage was 138682. For further research, it can use variations of DDoS attacks to get a wider profile.

Keywords: Computing Resources; Paloalto; Profiling; Testing; Virtualization.

1. PENDAHULUAN

Keamanan suatu jaringan menjadi hal yang sangat mutlak untuk diterapkan dengan memproteksi adanya ancaman serangan. Saat ini dengan berkembangnya sistem jaringan yang semakin pesat, perlu diketahui bahwa tidak ada sistem jaringan yang benar-benar aman untuk dapat mengamankan suatu sistem maupun data dari sebuah ancaman. Berdasarkan aspek keamanan informasi, suatu kerahasiaan data bahwa informasi di dalamnya tetap aman yang hanya dapat diakses oleh pihak tertentu saja, selain itu dapat menjamin integritas sumber daya yang dapat digunakan atau dimodifikasi oleh pihak tertentu, dan adanya ketersediaan informasi atau data yang dapat memudahkan pihak berwajib untuk dapat mengakses informasi tertentu pada saat dibutuhkan [1].

Salah satu serangan yaitu *Distributed Denial of Service* (DDoS) yang dapat mengakibatkan *server down*, *crash* hingga mati secara otomatis dan tidak dapat melayani permintaan dari pengguna. Ketersediaan layanan jaringan dengan pengamanan yang sangat ketat dan lambatnya dalam mengakses suatu informasi atau data, maka akan menyulitkan pihak yang berwenang dalam mengakses data atau informasi tersebut. Terdapat beberapa tipe serangan DDoS yaitu *volume*, aplikasi, *protocol* [2]. Sehingga dari berbagai jenis serangan dapat dilakukan suatu tindakan dengan mengamankan jaringan dengan menggunakan *firewall*.

Firewall merupakan bagian terpenting dalam keamanan jaringan yang berfungsi untuk memeriksa setiap paket yang masuk atau keluar dan memilah paket tersebut apakah dapat masuk ke dalam suatu jaringan . Penggunaan *firewall* tidak dapat menjamin sepenuhnya dalam mengamankan suatu perangkat, dikarenakan beberapa *firewall* terdapat fitur yang tidak selalu sama sesuai dengan tingkat efektifitasnya masing-masing. Karakteristik *firewall* dapat menentukan jika terjadinya serangan DDoS pada suatu sistem. Pada akhir tahun 2014, bahwa serangan DDoS merupakan teknik serangan yang paling populer banyak dilakukan oleh para *attacker* [3]. Salah satu jenis *firewall* yang banyak digunakan yaitu *next generation firewall* (NGFW) merupakan *firewall* yang

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

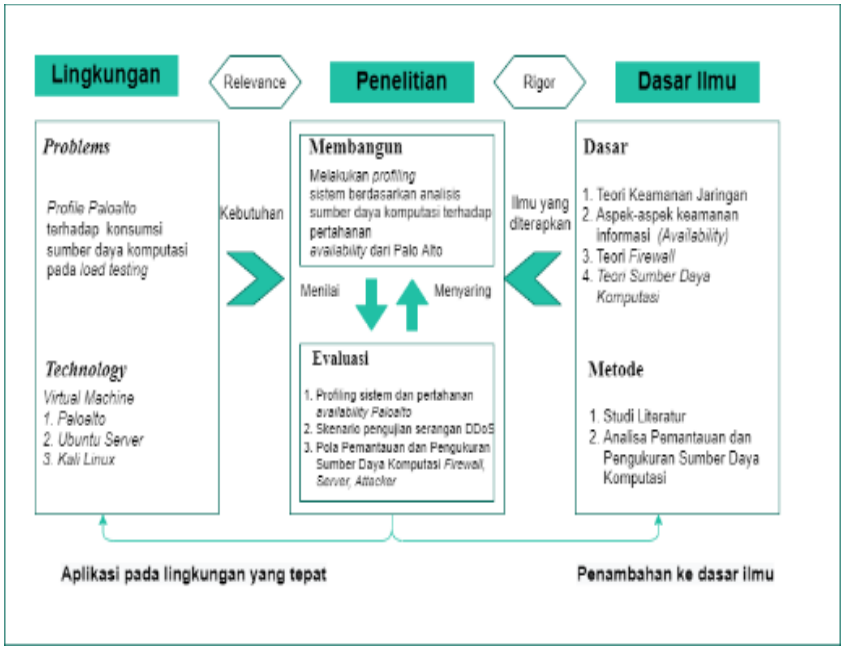
memiliki kemampuan dalam mendeteksi dan memblokir terjadinya layanan IT yang terhenti, dengan memberikan proteksi perlindungan yang dapat menerapkan keamanan [4]. Pada saat melakukan konfigurasi *firewall* perlu dilakukannya pengujian keamanan dengan menetapkan kebijakan dan prosedur, yang dibutuhkan untuk melindungi sistem dari ancaman serangan. Dilakukan berdasarkan konsumsi sumber daya komputasi yaitu salah satunya pada CPU dan *memory* [5]. Pada permasalahan yang terjadi bagaimana implementasi fungsi *firewall* untuk memproteksi atau melindungi *asset* IT [6].

Paloalto *firewall* merupakan salah satu NGFW yang dirancang untuk memberikan perlindungan keamanan yang terintegrasi dan konsisten ke seluruh jaringan pengguna. Virtualisasi Paloalto *firewall* dapat mengetahui atau mendeteksi adanya suatu serangan yang masuk ke dalam sistem penggunaan. Virtualisasi Paloalto *firewall* dapat mewujudkan salah satu aspek keamanan berdasarkan identifikasi suatu jaringan yang masuk ke dalam sistem dengan menentukan profil keamanan untuk melindungi terjadinya ancaman serangan [7]. Maka dari itu, pada penelitian ini dilakukan *profiling* sistem dengan virtualisasi Paloalto *firewall* pada pendeteksian, pencegahan dan pemulihan berdasarkan pengukuran sumber daya komputasi. Terdiri dari dua skenario pengujian yaitu berdasarkan pengujian *service* HTTP *allow* dan berdasarkan pengujian *service* HTTP *block* dengan spesifikasi *memory* Paloalto pada RAM 5.5 GB dan spesifikasi RAM 8 GB. Pada saat melakukan serangan menggunakan Hping3 yang merupakan salah satu jenis serangan DDoS, yang dapat menganalisis paket TCP/IP [8]. Dilakukan pengukuran sumber daya komputasi, mencakup penggunaan CPU, *memory*, dan *session* yang berfokus pada sebelum, saat, dan sesudah dilakukan serangan DDoS SYN *flood*.

2. METODOLOGI PENELITIAN

2.1 Model Konseptual Penelitian

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



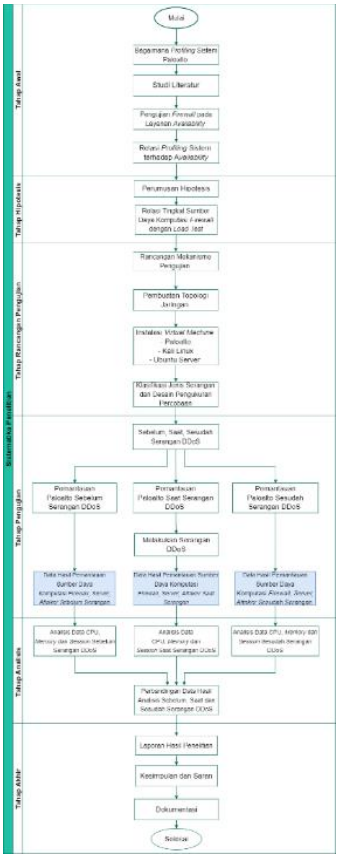
Gambar 1. Model Konseptual Penelitian

Dapat diketahui pada Gambar 1 bahwa terdapat tiga ruang lingkup yaitu lingkungan, penelitian dan dasar ilmu. Pada aspek lingkungan berupa *probles* yang terjadi dan *technology* yang terdapat pada penelitian ini. Pada penelitian Terdapat "Membangun" melakukan *profiling firewall* berdasarkan analisis sumber daya komputasi terhadap pertahanan layanan *availability* pada Paloalto *firewall*. Pada "Evaluasi" *profiling* 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.

2.2 Sistematika Penelitian

Sistematika penelitian digunakan sebagai gambaran dalam menyelesaikan suatu permasalahan dimulai dari tahap awal, tahap hipotesis, tahap rancangan pengujian, tahap pengujian, tahap analisis dan tahap akhir. Sistematika ini terdiri dari beberapa langkah yaitu:

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780



Gambar 2. Sistematika Penelitian

a. Tahap Awal

Pada tahap awal penelitian dimulai dengan mengenali *profile* sistem virtualisasi Paloalto *firewall* berdasarkan studi literatur yang terkait untuk menghasilkan latar belakang masalah pada penelitian ini dan mendapatkan informasi yang terperinci. *Profiling* sistem dapat dirumuskan sesuai batasan masalah dengan melakukan pengujian *firewall* berdasarkan penggunaan sumber daya komputasi.

b. Tahap Hipotesis

Pada tahap ke-2 yaitu tahap hipotesis, dengan melakukan pembuatan hipotesis atau praduga sementara pada penelitian ini yaitu mengenai ketersediaan sumber daya komputasi pada *asset* IT yaitu virtualisasi Paloalto *firewall*, *server* dan *attacker*. Dengan mencari relasi tingkat sumber daya komputasi pada *firewall* saat *load testing*.

c. Tahap Rancangan Pengujian

Pada tahap ke-3 yaitu tahap rancangan pengujian, perancangan pengujian dimulai dari pembuatan topologi jaringan beserta IP *address* yang telah ditentukan. Selanjutnya, melakukan instalasi *virtual machine* yang terdiri dari, VM Paloalto *firewall* sebagai objek yang digunakan pada penelitian, VM Kali Linux yang digunakan untuk melakukan *attacker* atau penyerang, dan Ubuntu Server digunakan sebagai target dalam melakukan serangan DDoS. Selanjutnya melakukan klasifikasi jenis serangan dan melakukan desain pengukuran pada percobaan.

d. Tahap Pengujian

Pada tahap ke-4 yaitu tahap pengujian, pada tahap ini terdiri dari tiga proses pengujian yang akan dibahas dalam melakukan serangan yaitu sebelum serangan, saat serangan dan sesudah serangan DDoS. Setelah menentukan proses pengujian serangan, selanjutnya melakukan pemantauan dan mengukur data hasil pada virtualisasi Paloalto *firewall* yaitu sebelum, saat dan sesudah melakukan serangan DDoS. Sehingga, didapatkan data hasil pemantuan sumber daya komputasi pada *firewall*, *server* dan *attacker* sebelum serangan, saat serangan dan sesudah serangan DDoS. Kemudian, hasil dari pemantauan tersebut akan dilakukan analisis untuk mendukung penelitian ini.

e. Tahap Analisis

Tahap ke-5 yaitu tahap analisis, dimulai dari melakukan analisis sumber daya komputer (CPU, *memory* dan *session*) pada *firewall* sebelum, saat dan sesudah serangan DDoS dilakukan pada proses pemantauan sebelumnya. Selanjutnya, hasil analisis yang didapatkan akan dijadikan perbandingan sebagai faktor utama sumber daya komputasi pada *firewall*. Berdasarkan hubungan pada pengukuran berbagai serangan.

f. Tahap Akhir

Pada tahap akhir ini, berupa penyusunan kesimpulan berdasarkan pola konsumsi tertinggi pada metrik penggunaan sumber daya komputasi dan saran yang diperoleh pada penelitian ini. Serta melampirkan dokumentasi pada hasil penelitian ini.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

2.3 *Firewall*

Firewall merupakan salah satu cara dalam melakukan keamanan pada perangkat komputer yang mampu melindungi, mengontrol, membatasi atau menolak suatu koneksi pada jaringan yang dilindungi dari serangan atau ancaman luar. *Firewall* digunakan untuk mengimplementasi kebijakan keamanan untuk mengendalikan atau filterisasi lalu lintas jaringan yang keluar masuk, bahkan melakukan pencegahan dengan memberikan pemberitahuan ketika terjadinya hal yang tidak normal pada jaringan [9].

2.4 Virtualisasi Paloalto *Firewall*

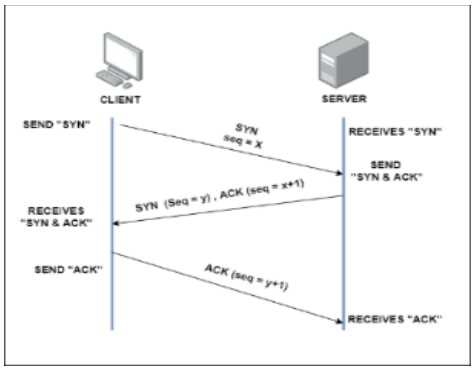
Paloalto merupakan salah satu *next generation firewall* yang dirancang untuk memberikan perlindungan keamanan yang terintegrasi dan konsisten ke seluruh jaringan pengguna. Paloalto *firewall* dapat menentukan kebijakan keamanan berdasarkan identifikasi suatu jaringan yang masuk ke dalam sistem dengan menentukan profil keamanan untuk melindungi terjadinya ancaman serangan [10].

2.5 *Distributed Denial of Service* (DDoS)

Serangan DDoS terdiri dari beberapa jenis tipe yaitu pada *volume*, aplikasi, *protocol*. Pada jenis *volume* yaitu mengirim serangan dengan menghabiskan sumber daya *bandwidth* dari pengguna, sedangkan pada aplikasi dengan menargetkan halaman *website* sehingga mengakibatkan lalu lintas *website* tidak dapat bekerja secara normal, dan *protocol attack* yang bertujuan untuk mengeksploitasi TCP contohnya seperti SYN *flood* [11]. Salah satunya pada aplikasi yang berbasis *web* dapat menggunakan *web application firewall* dengan mengurangi serangan yang terjadi [12].

2.6 TCP Three-Way Handshake

TCP *Three-Way Handshake* merupakan salah satu bagian terpenting dalam melakukan proses pembentukan koneksi antara *client* dan *server* [13].



Gambar 3. TCP *Three-Way Handshake*

Pada pembentukan koneksi TCP antara *client* dan *server*. dapat diilustrasikan pada Gambar II. 2 dengan penjelasan sebagai berikut:

a. Dimulai, dari *client* mengirimkan paket permintaan koneksi SYN ke *server* dengan nomor urut awal yang acak.
b. Setelah itu, server akan merespon dengan paket SYN memiliki nomor urut acak "y" dan paket ACK memiliki nomor urut "x+1" untuk mengakui nomor urut awal "x" yang dikirimkan oleh *client.*
c. Pada tahap ke-3, *client* akan mengirimkan paket ACK dengan nomor urut "y+1" kepada *server* untuk mengakui paket "SYN" yang telah dikirimkan oleh *server*.
d. Pada tahap ke-4, kedua ujung jika telah tersinkronkan dapat mengirim dan menerima data secara mandiri.

2.7 Hping3

Hping3 merupakan salah satu *software* serangan yang dapat mengirimkan paket khusus kepada target. Hping3 memiliki fitur utama yaitu, dapat menemukan host di jaringan yang sedang aktif, dan melakukan serangan DDoS atau *Distributed Denial of Service* dengan menggunakan SYN *flood*. [14].

2.8 *Load Testing*

Load testing merupakan salah satu pengujian performansi yang mengevaluasi kinerja sistem yang sedang diuji tanpa mencapai beban maksimum, dengan menguji layanan pada lalu lintas yang tinggi sesuai dengan beban yang dilakukan [15].

2.9 Sumber Daya Komputasi

Sumber daya komputasi merupakan representasi kemampuan komputasi dari perangkat komputer yang terdiri dari perangkat keras dan perangkat lunak untuk dapat memudahkan pengguna dalam penyelesaian masalah komputasi sesuai dengan kebutuhan. Sumber daya komputer misalnya seperti, *Central Processing Unit* (CPU) dan *memory*.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

2.9.1 CPU

CPU merupakan kompunen utama pada komputer yang berfungsi untuk menerima dan menjalankan program yang telah disimpan dengan mengambil data dari memori utama untuk diproses [16].

2.9.2 *Memory*

Memory merupakan tempat penyimpanan data yang dapat menemukan data tertentu dengan sangat cepat ketika saat dibutuhkan. *Memory* digunakan sebagai tempat informasi data yang dapat memproses data dan menyimpan hasilnya, dengan kapasitas yang cukup untuk menampung semua data yang masuk.

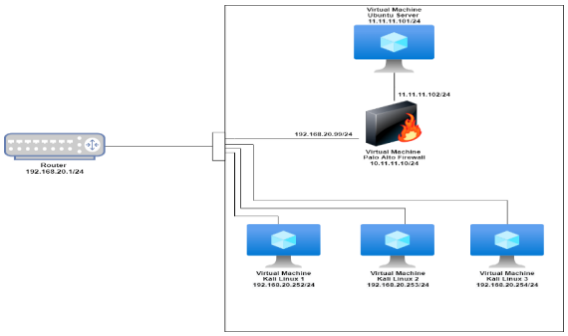
3. HASIL DAN PEMBAHASAN

3.1 Rancangan Sistem

Dalam melakukan *profiling sistem* dengan melakukan pemantauan sumber daya komputasi pada *asset* IT (Paloalto *firewall*, *attacker*, dan *server*), maka dibutuhkan suatu perancangan sistem untuk melakukan pengujian dengan membutuhkan suatu perangkat.

3.1.1 Topologi Penelitian

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 4. Topologi Jaringan Pengujian

Pada Gambar 4 topologi jaringan pada penelitian ini terdiri dari *router*, VM Paloalto *firewall*, Ubuntu Server dan Kali Linux. Router, yang digunakan sebagai penghubung antar koneksi *internet*, VM Paloalto *firewall*, sebagai *access* kontrol pada Ubuntu Server dan Kali Linux yang memiliki tiga *interface* yaitu *interface static* untuk terhubung pada GUI Paloalto dengan IP, VM Ubuntu Server, sebagai target yang terhubung dengan *firewall* dan VM Kali Linux, yang berperan sebagai *attacker* atau penyerang untuk melakukan serangan DDoS dengan tiga VM yang digunakan.

3.1.2 Daftar IP *Address*

IP *Address* yang digunakan pada penelitian ini, dilampirkan pada Tabel IV.3 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
VM1	Paloalto *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 NAT: 192.168.20.100 IP Static: 11.11.11.101

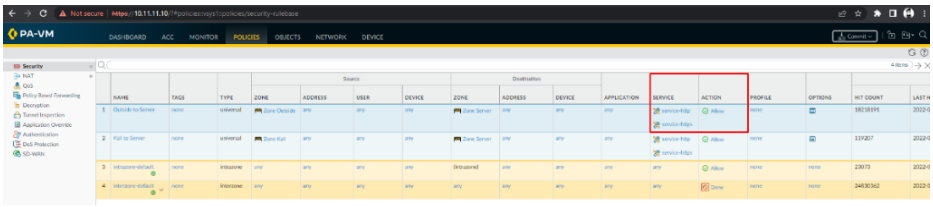
3.2 Skenario Pengujian

Pada penelitian ini, terdapat dua skenario pengujian yang dilakukan yaitu, skenario pertama dengan *service* HTTP *allow* dan skenario kedua dengan *service* HTTP di *block*. Pada kedua skenario tersebut bertujuan untuk melihat

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

perbandingan pada pengukuran sumber daya komputasi, serta melakukan pemantauan dan analisis pada saat, sebelum dan sesudah serangan DDoS.

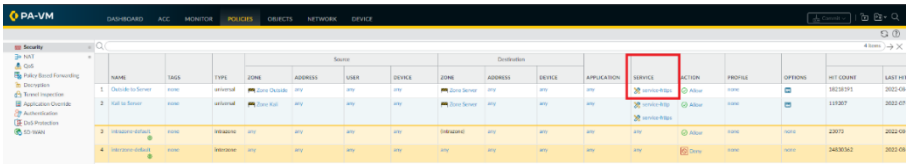
a. Skenario pengujian *service* HTTP *allow*



Gambar 5. *Rules Service* HTTP *Allow*

Pada Gambar 5 merupakan menu *rules* virtualisasi Paloalto *firewall* dengan *service* HTTP *allow*. *Rules* ini digunakan untuk memberikan hak akses *web server* atau target untuk dapat mengakses layanan HTTP.

b. *Service* HTTP *block*



Gambar 6. *Rules Service HTTP Block*

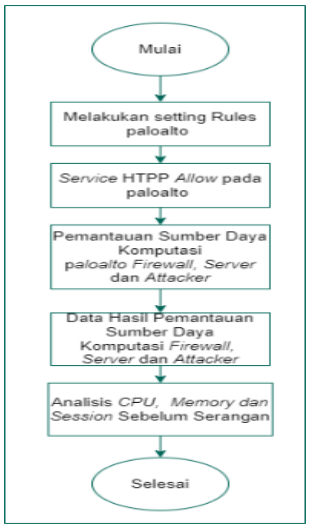
Pada Gambar 6 merupakan menu *rules* virtualisasi Paloalto *firewall* dengan *service* HTTP *block*. *Rules* ini digunakan untuk tidak memberikan hak akses *web server* atau target untuk dapat mengakses layanan HTTP. Pada ke dua skenario tersebut bertujuan untuk melihat perbandingan pada pengukuran sumber daya komputasi, serta melakukan pemantauan dan analisis pada saat, sebelum dan sesudah serangan DDoS, yang telah dilakukan sesuai dengan klasifikasi jenis serangan dan jumlah paket yang dikirimkan pada saat melakukan serangan DDoS. Jenis Serangan DDoS yang digunakan yaitu Hping3 dengan *command* yang digunakan sebagai berikut:

Tabel 2. *Command* Serangan DDoS

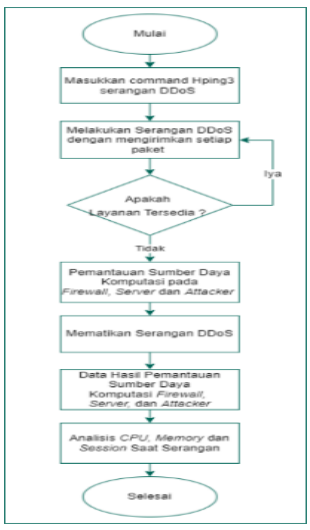
***Command* Serangan DDoS**	**Jumlah Paket Serangan (-c)**
hping3 -c 100 -d 15000 -S -w 64 -p 80 --flood --rand-source 192.168.20.100	1000 10000 100000

3.2.1 Skenario 1 : *Service* HTTP *Allow*

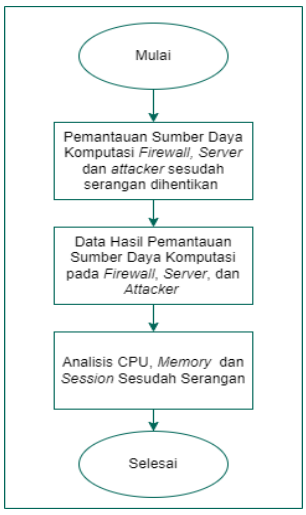
Pada skenario 1 dilakukan pengujian dengan memberikan izin *web server* pada *service* HTTP di Paloalto *firewall*, pada skenario ini terdiri dari tiga pengujian yaitu pengujian sebelum serangan, saat serangan dan sesudah serangan. Pada masing-masing pengujian memiliki proses alur yang berbeda dengan fungsi yang sama yaitu melakukan pemantauan sumber daya komputasi (CPU, *memory* dan *session*) pada virtualisasi Paloalto *firewall*, *attacker* dan *server*.



Gambar 7. Sebelum Serangan



Gambar 8. Saat Serangan



Gambar 9. Sesudah Serangan

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

a. Sebelum Serangan DDoS pada *service* HTTP *allow*

Dimulai dari *setting rules* pada *firewall*, kemudian memberikan akses layanan HTTP pada virtualisasi Paloalto *firewall*. Kemudian melakukan pemantauan sumber daya komputasi pada *firewall*, *attacker* dan *server* setelah itu menganalisis data hasil yang didapatkan pada proses pemantauan.

b. Saat Serangan DDoS pada *service* HTTP *allow*

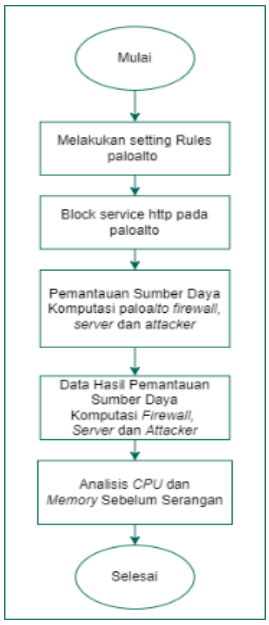
Pada saat melakukan serangan DDOS menggunakan SYN *flooding*. SYN *flooding* ini jenis serangan yang menyerang pada sisi protokol. Dimulai dengan memasukan *command* Hping3, kemudian melakukan serangan DDos, serta mengecek layanan HTTP. Jika layanan masih tersedia melakukan serangan ulang dengan mengirimkan paket. Apabila layanan tidak tersedia, selanjutnya mematikan atau menghentikan serangan. Kemudian, memantau sumber daya komputasi pada *firewall*, *attacker* dan *server*. Berikutnya mencatat data hasil pemantauan sumber daya komputasi pada *firewall*, *attacker* dan *server*. Terakhir melakukan analisis pada CPU, *memory*, dan *session* saat serangan.

c. Sesudah Serangan DDoS pada *service* HTTP *allow*

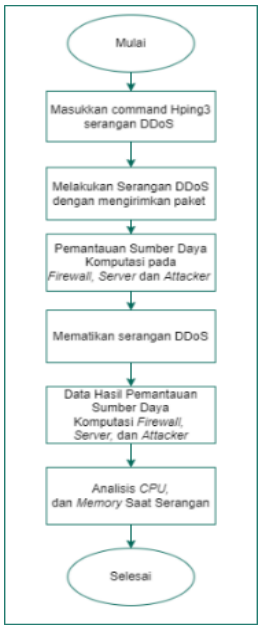
Pada pengujian sesudah serangan dimulai dengan melakukan pemantauan sumber daya komputasi pada *firewall*, *attacker*, dan *server*. Setelah itu, mencatat data hasil pemantauan sumber daya komputasi, dan terakhir melakukan analisis CPU, *memory*, dan *session*.

3.2.2 Skenario 2 : *Service* HTTP *Block*

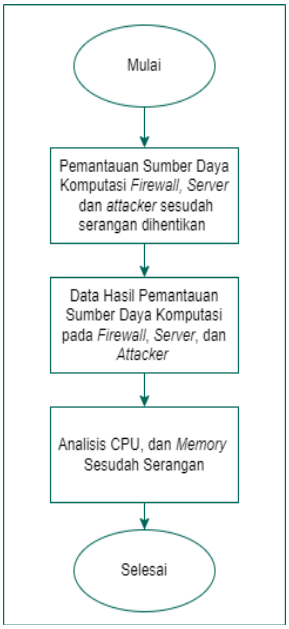
Pada skenario 2, melakukan pengujian dengan memblokir akses *web server* pada *service* HTTP. Pada skenario ini terdiri dari tiga pengujian yaitu, pengujian sebelum serangan, saat serangan dan sesudah pengujian. Pada masing-masing pengujian memiliki aktivitas yang berbeda dengan fungsi yang sama yaitu, melakukan pemantauan pada sumber daya komputassi (CPU dan *memory*) pada virtualisasi Paloalto *firewall*, *attacker* dan *server*.



Gambar 10. Sebelum Serangan



Gambar 11. Saat Serangan



Gambar 12. Sesudah Serangan

a. Sebelum Serangan DDoS pada *service* HTTP *block*

Dimulai dari *setting rules* pada *firewall*, kemudian memblokir layanan HTTP pada virtualisasi Paloalto *firewall*. Kemudian melakukan pemantauan sumber daya komputasi pada *firewall*, *attacker* dan *server* setelah itu menganalisis data hasil yang didapatkan pada proses pemantauan.

b. Saat Serangan DDoS pada *service* HTTP *block*

Pada skenario pengujian dengan service HTTP *block*, dimulai dengan memasukan command Hping3, kemudian mengirimkan serangan DDos berdasarkan ukuran paket serangan, selanjutnya melakukan pemantauan sumber daya komputasi pada *firewall*, *attacker*, dan *server*. Selanjutnya mematikan atau menghentikan serangan. Kemudian, memantau sumber daya komputasi pada *firewall*, *attacker* dan *server*. Berikutnya mencatat data hasil pemantauan sumber daya komputasi pada *firewall*, *attacker* dan *server*. Terakhir melakukan analisis pada CPU, *memory*, saat serangan.

c. Sesudah Serangan DDoS pada *service* HTTP *block*

Pada pengujian sesudah serangan dimulai dengan melakukan pemantauan sumber daya komputasi pada *firewall*, *attacker*, dan *server*. Setelah itu, mencatat data hasil pemantauan sumber daya komputasi, dan terakhir melakukan analisis CPU, dan *memory*.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

3.3 Analisis Hasil Pengujian

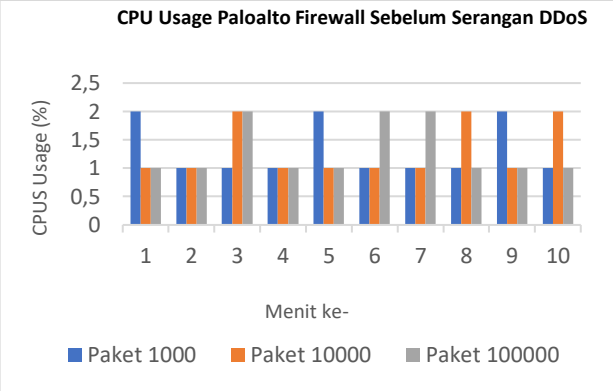
Pada bab ini dilakukan analisis hasil pengujian dari bab sebelumnya, bertujuan untuk mengetahui perbandingan antara pengujian sebelum, saat dan sesudah dilakukan serangan pada setiap hasil sumber daya komputasi CPU, memory dan session.

3.3.1 Perbandingan Hasil Persentase Penggunaan Sumber Daya Komputasi

Dalam menganalisis perbandingan yang didapatkan pada sebelum, saat dan sesudah serangan pada *service* HTTP *allow* dengan *service* HTTP block pada pengukuran paket (1000, 10000, dan 100000) terhadap penggunaan sumber daya komputasi CPU dan *memory*. Didapatkan hasil persentase pada CPU dan *memory firewall*.

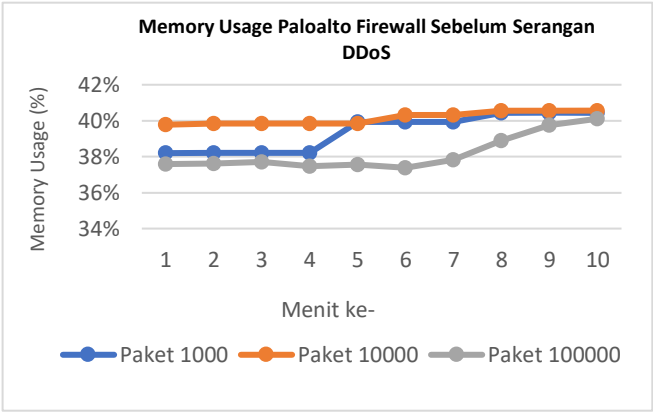
a. Sebelum Serangan

Perbandingan hasil analisis sebelum serangan dengan *service* HTTP *allow* dan *service* HTTP *block* didapatkan rata-rata hasil yang sama pada setiap ukuran paketnya, dikarenakan tidak adanya aktivitas atau serangan sehingga tidak terjadinya peningkatan pada sumber daya komputasi (CPU, dan *memory*) pada setiap ukuran paket (1000, 10000 dan 100000) yang digunakan dan spesifikasi paloalto pada RAM 5.5 GB dan RAM 8 GB. Hasil yang didapatkan pada spesifikasi RAM 5.5 GB dan RAM 8 GB penggunaan CPU *firewall* berada pada range sekitar 1-3%.



Gambar 13. CPU *Usage* Paloalto *Firewall* Sebelum Serangan DDoS

Data pertama yaitu Data hasil penggunaan CPU, pada Gambar 13 terdapat hasil rata-rata persentase tertinggi sebelum serangan yaitu Paloalto *firewall*. Hasil rata-rata persentase penggunaan CPU paloalto *firewall*, sebelum serangan sebesar 1,3%.



Gambar 14. *Memory Usage* Paloalto *Firewall* Sebelum Serangan DDoS

Data kedua yaitu data hasil penggunaan *memory*, pada Gambar 14 terdapat hasil rata-rata persentase tertinggi sebelum serangan yaitu Paloalto *firewall*. Hasil rata-rata persentase kedua yaitu penggunaan *memory* paloalto *firewall*, sebelum serangan sebesar 39%.

b. Saat Serangan

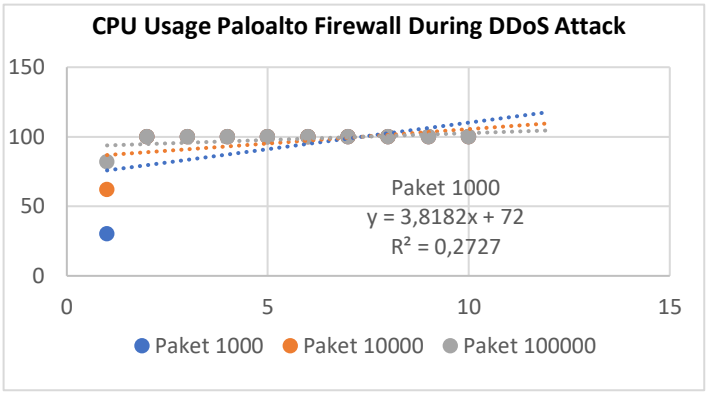
Perbandingan hasil analisis saat serangan dengan *service* HTTP *allow* dan *service* HTTP *block* didapatkan hasil yang tidak jauh berbeda yaitu, terjadinya peningkatan dalam penggunaan sumber daya komputasi pada *firewall* dengan spesifikasi Paloalto pada RAM 5.5 GB dan RAM 8 GB. Hal tersebut dikarenakan pada fungsi *firewall* dapat memproteksi adanya aktivitas atau serangan yang masuk dan melintas pada pada Paloalto *firewall*. Pada penggunaan CPU *firewall* terjadi peningkatan hingga 100% dan peningkatan rata-rata terjadi secara langsung pada menit pertama. Persentase kenaikan sumber daya komputasi tertinggi didapatkan pada penggunaan CPU dan

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

memory, berdasarkan pengukuran paket (1000, 10000, dan 100000) yang dikirimkan saat serangan. Hasil persentase didapatkan berdasarkan nilai rata-rata keseluruhan pada pengukuran paket. Adapun kenaikaan hasil persentase yang didapatkan pola dalam bentuk grafik linear, sebagai berikut:

1. Penggunaan CPU *Firewall*

Nilai konsumsi pertama penggunaan sumber daya komputasi, tertinggi pada penggunaan CPU *firewall* yang mengalami kenaikan pada setiap ukuran paket yang dikirimkan saat serangan pada *service* HTTP *allow* dan *service* HTTP *block*.

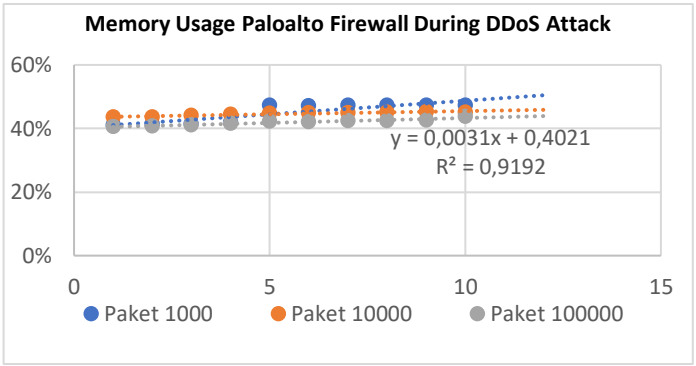


Gambar 15. Penggunaan CPU *Firewall* Saat Serangan DDoS

Pada Gambar 15 hasil persentase pada penggunaan CPU saat serangan DDoS, diperoleh hasil persentase penggunaan CPU *usage service* HTTP *block firewall* pada spesifikasi RAM 8 GB sebesar 95,8%. Pola yang digunakan yaitu gradien linear dengan rumus "y=mx+c" dengan rumus persamaan yang didapatkan yaitu y=3,8182x+72. Menunjukkan bahwa hasil persentase mengalami peningkatan secara linear, berupa garis lurus yang tertinggi pada paket 1000. Bahwa serangan DDoS cenderung memakan penggunaan CPU daripada penggunaan memori.

2. Penggunaan *Memory Firewall*

Nilai konsumsi kedua penggunaan sumber daya komputasi tertinggi pada penggunaan *memory firewall* yang mengalami kenaikan pada setiap ukuran paket yang dikirimkan saat serangan pada *service* HTTP *allow* dan *service* HTTP *block*.



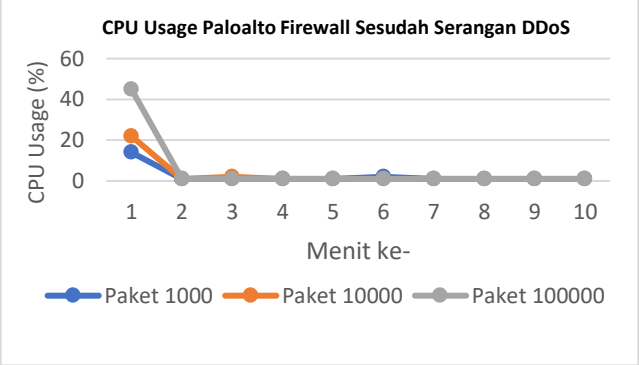
Gambar 16. Penggunaan *Memory Firewall* Saat Serangan DDoS

Pada Gambar 16 hasil persentase pada penggunaan *memory firewall* saat serangan DDoS. Berdasarkan penggunaan pada setiap ukuran paket serangan dikirimkan. Diperoleh hasil persentase penggunaan *memory usage* dengan *service* HTTP *allow firewall* pada spesifikasi RAM 5.5 GB sebesar 44%. Pola persamaan yang didapatkan yaitu y=47443x+2E+06. Menunjukkan bahwa hasil persentase mengalami peningkatan secara linear, berupa garis lurus yang tertinggi pada paket 1000. Pada paloalto firewall penggunaan *memory* berada pada *underutilization* normal yaitu dibawah 70%.

c. Sesudah Serangan

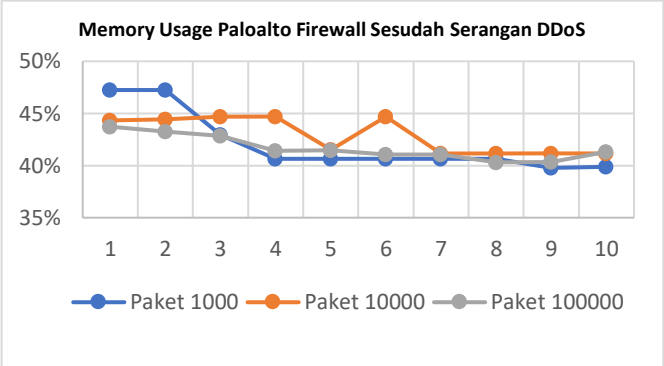
Perbandingan hasil analisis sesudah serangan dengan *service* HTTP *allow* dan *service* HTTP *block* terjadinya proses transisi penurunan yang tidak terlalu jauh berbeda pada setiap sumber daya komputasi (CPU, dan *memory*) setiap paket dan spesifikasi Paloalto yang digunakan. Dilakukan proses pemantauan selama 10 menit pada *firewall*, mengalami transisi penurunan dengan sangat cepat yaitu rata-rata kembali dalam keadaan yang normal pada menit kedua. Sedangkan penggunaan *memory firewall* mengalami transisi penurunan secara bertahap pada proses pemulihan. Hal tersebut dikarenakan fungsi sistem *firewall* dapat melakukan proses pemulihan penggunaan sumber daya komputasi kembali dalam keadaan yang normal dan stabil.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780



Gambar 17. Penggunaan CPU Firewall Sesudah Serangan DDoS

Data pertama yaitu data hasil penggunaan CPU, pada gambar terdapat hasil rata-rata persentase terjadinya penurunan sesudah serangan yaitu Paloalto *firewall*. Hasil rata-rata persentase penggunaan CPU paloalto *firewall*, sesudah serangan sebesar terjadinya penurunan sebesar 4,4%.



Gambar 18. Penggunaan Memory Firewall Sesudah Serangan DDoS

Data kedua yaitu Data hasil penggunaan *memory*, pada gambar terdapat hasil rata-rata persentase penurunan sesudah serangan yaitu Paloalto *firewall*. Hasil rata-rata persentase penggunaan *memory* paloalto *firewall*, sesudah serangan sebesar terjadinya penurunan sebesar 42%.

4. KESIMPULAN

Berdasarkan hasil analisis dari penggunaan sumber daya komputasi, dapat disimpulkan bahwa karakteristik virtualisasi Paloalto *firewall* cenderung linear, pola linear pada saat serangan naik sangat tinggi pada penggunaan CPU dengan berbagai jumlah paket serangan. Dominan hasil *profiling* sistem *firewall* Paloalto berdasarkan *service* HTTP *allow* dan *service* HTTP *block*, terjadinya peningkatan sumber daya komputasi yang tertinggi pada penggunaan CPU sebesar 95,8%. Urutan peningkatan ke dua yaitu pada penggunaan sumber daya komputasi pada faktor *memory* tertinggi sebesar 44% dan rata-rata penggunaan *session* tertinggi sejumlah 138682.

REFERENCES

[1] M. R. Kamal and M. A. Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," *Automata*, no. 4, 2021.
[2] C. Sheth and R. Thakker, "Performance Evaluation and Comparison of Network Firewalls under DDoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 12, pp. 60–67, 2013, doi: 10.5815/ijcnis.2013.12.08.
[3] N. Beigi-Mohammadi, C. Barna, M. Shtern, H. Khazaei, and M. Litoiu, "CAAMP: Completely automated DDoS attack mitigation platform in hybrid clouds," *2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016*, pp. 136–143, 2017, doi: 10.1109/CNSM.2016.7818409.
[4] K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security : A Survey," *SoutheastCon 2018*, pp. 1–6.
[5] R. E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," *IEEE Trans. Commun.*, vol. 25, no. 1, pp. 169–178, 1977, doi: 10.1109/TCOM.1977.1093714.
[6] A. A. ASTARI, "ImplemenTasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik," *Simki-Techsain Vol. 02 No. 01 Tahun 2018 ISSN 2599-3011*, vol. 02, no. 01, 2018.
[7] S. Gold, "The future of the firewall," *Netw. Secur.*, vol. 2011, no. 2, pp. 13–15, 2011, doi: 10.1016/S1353-4858(11)70015-0.
[8] A. H. Dar, B. Habib, F. Khurshid, and M. T. Banday, "Experimental analysis of DDoS attack and it's detection in

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 1, September 2022
e-ISSN 2685-998X
DOI 10.30865/json.v4i1.4780

Eucalyptus private cloud platform," *2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016*, pp. 1718–1724, 2016, doi: 10.1109/ICACCI.2016.7732295.
[9] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. - Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018.
[10] C. Confidential, "Palo Alto Networks Administrator ' ' s Guide," in *Networks*, 2015, pp. 1–338.
[11] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.
[12] K. Dhiatama Ayunda *et al.*, "Implementation and Analysis ModSecurity on Web-Based Application with OWASP Standards," *Jurnal.Mdp.Ac.Id*, vol. 8, no. 3, pp. 1638–1650, 2021, [Online]. Available: https://jurnal.mdp.ac.id/index.php/jatisi/article/view/1223.
[13] F. H. Hsu, Y. L. Hwang, C. Y. Tsai, W. T. Cai, C. H. Lee, and K. W. Chang, "TRAP: A Three-way handshake server for TCP connection establishment," *Appl. Sci.*, vol. 6, no. 11, 2016, doi: 10.3390/app6110358.
[14] Fahmi Bagaskara Perdana, M. . Dr. Ir. Rendy Munadi, and M. . Arif Indra Irawan, S.T., "Implementasi Sistem Keamanan Jaringan Menggunakan Suricata Dan Ntopng," *e-Proceeding Eng.*, vol. 6, no. 2, p. 4080, 2019.
[15] D. Makrushin, "Ampli cation Techniques of Stress Testing using Third Party Services Load and stress testing," no. January, 2021.
[16] M. K. Sriani, "Arsitektur Dan Organisasi Komputer," *Arsit. Dan Organ. Komput.*, pp. 19–22, 2020.