BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Pengguna internet khususnya di Indonesia mengalami peningkatan selama kurun waktu 2017 – 2021 yang ditunjukkan dengan meningkatnya persentase penduduk yang mengakses internet pada tahun 2017 sekitar 32,34 % menjadi 62,10 % pada tahun 2021 [1]. Namun meningkatnya akses internet juga diikuti dengan meningkatnya *cyber attacks*, khususnya terhadap *web server*. Berdasarkan statistik *vurnerability* yang dipublikasi oleh *Common Vulnerabilities and Exposures (CVE)* [2], terdapat 250 jenis kerentanan terhadap Apache HTTP *web server* dari tahun 1999 sampai tahun 2022. Pada statistik tersebut kerentanan tertinggi terdapat pada jenis serangan *denial of service* (DOS) yang mencapai 79 jenis kerentanan. Hasil *report* dari *cloudfire* [3] menunjukkan jenis serangan DOS tertinggi yaitu TCP-SYN *floods* yang mencapai 47%. Berdasarkan data kerentanan tersebut maka dibutuhkan sistem keamanan untuk menjaga kinerja layanan *web server* dari serangan TCP-SYN *floods*. Salah satu metode untuk mengatasi TCP-SYN *floods* yaitu dengan menerapkan *instrusion prevention system* (IPS).

IPS merupakan pengembangan dari *intrusion detection system* (IDS) sehingga sistem ini dapat mengidentifikasi aktivitas yang mencurigakan pada lalu lintas jaringan sekaligus melakukan tindakan atau *action* yaitu memblokir ancaman tersebut [4]. Terdapat beberapa *software* yang dapat menerapkan metode IPS, diantaranya yaitu Snort dan Suricata yang dijalankan sebagai sebuah *service* pada *tools* pfSense. Pada tahun 2020, Firdaus dan Suartana [4] yang berjudul " Implementasi Keamanan Jaringan *Intrusion Detection/Prevention System* Menggunakan PfSense " menggunakan *service* IPS Suricata pada *tools* pfSense untuk menganalisis *alert detection* dan *alert prevention* ketika mengatasi serangan *data flooding*. Namun dibutuhkan analisis mengenai parameter QoS untuk mengetahui dampak serangan *data flooding* terhadap layanan *web server* dan waktu yang dibutuhkan untuk melakukan pemblokiran serangan. Maka pada penelitian ini melakukan analisis mengenai QoS dari layanan *web server* yang menggunakan IPS Snort dan Suricata untuk mendeteksi dan mengatasi serangan *data flooding.*

Berdasarkan permasalahan yang sudah dijelaskan, maka pada penelitian ini diangkat judul "Analisis Performansi QoS IPS Snort dan Suricata Terhadap Serangan *Data flooding* Pada *Web server*". Pada penelitian ini diterapkan IPS Snort dan Suricata pada *tools* pfSense secara bergantian sebagai sistem keamanan jaringan untuk mengatasi serangan *data flooding*, kemudian dianalisis mengenai parameter QoS meliputi *throughput*, *delay*, *packet loss*, dan *Round Trip Time* dari *web server* yang menggunakan IPS Snort dan Suricata.

1.2 RUMUSAN MASALAH

Rumusan masalah pada penelitian ini yaitu:

1. Bagaimana dampak serangan *data flooding* terhadap QoS layanan *web server*?
2. Bagaimana konfigurasi IPS Snort dan Suricata untuk mengatasi serangan *data flooding* pada layanan *web server* ?
3. Bagaimana perbandingan QoS *web server* yang menerapkan IPS Suricata dan Snort untuk menghadapi serangan *data flooding* ?

1.3 BATASAN MASALAH

Batasan masalah pada penelitian ini adalah :

1. Menggunakan *open source firewall* dan *router* berbasis *Freebsd* bernama pfSense
2. Perangkat pfSense dan *server* dijalankan secara virtual menggunakan virtualbox
3. Perangkat pfSense menggunakan Snort dan Suricata sebagai *intrusion prevention system* secara bergantian
4. Snort dan Suricata menerapkan *costum rule* yang sama.
5. Jenis serangan yang digunakan yaitu *TCP SYN flood*
6. Analisis terhadap performa *web server* melalui parameter *delay*, *packet loss*, *throughput*, dan *Round Trip Time*
7. Menggunakan *Wireshark* untuk melihat lalu lintas jaringan dari sisi *client*
8. Menggunakan Nping sebagai penguji pada sistem IPS (*attacker*)

1.4 TUJUAN PENELITIAN

Tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut :

1. Mengetahui dampak serangan *data flooding* terhadap QoS layanan *web server*.
2. Memperoleh konfigurasi yang tepat pada IPS Snort dan IPS Suricata untuk mengatasi serangan *data flooding*.
3. Mendapatkan nilai QoS layanan *web server* berdasarkan performansi IPS Snort dan Suricata ketika mengatasi serangan *data flooding.*

1.5 MANFAAT PENELITIAN

Penelitian ini diharapkan dapat memberikan pemahaman bagi pembaca terutama administrator jaringan tentang dampak serangan *data flooding* terhadap QoS layanan *web server*. Administrator jaringan dapat memanfaatkan sistem keamanan jaringan berbasis *intrusion prevention system* untuk mengatasi *data flooding* dan menjadi Gambaran bagi administrator jaringan mengenai performa *web server* (QoS) yang menggunakan IPS Snort atau IPS Suricata pada *tools* pfSense ketika mengatasi serangan *data flooding.*

1.6 SISTEMATIKA PENULISAN

Penelitian ini terdiri atas 5 bab yaitu bab 1, bab 2, bab 3, bab 4, dan bab 5. Pada Bab 1 menjelaskan mengenai latar belakang, rumusan masalah, manfaat penelitian, tujuan penelitian, batasan masalah dan sistematika penulisan. Bab 2 menjelaskan tentang teori- teori yang menjadi referensi penulis pada penulisan dan implementasi penelitian. Bab 3 pada penelitian ini menjelaskan tentang implemetasi penelitian seperti alat yang digunakan, topologi, spesifikasi perangkat, dan alur penelitian. Bab 4 menjelaskan tentang hasil dari implementasi penelitian dan analisis yang didapatkan dari hasil penelitian tersebut. Sedangkan pada bab 5 menjelaskan tentang kesimpulan dari penelitian yang sudah dilakukan dan beberapa saran untuk mengembangkan penelitian.