1. Pendahuluan

Teknologi informasi pada saat ini sudah berkembang pesat terutama dalam layanan internet. Menurut (Saini, Behal, & Bhatia, 2020), Internet tidak hanya digunakan dalam lingkup individu untuk bertukar informasi, tetapi sudah digunakan untuk keperluan komersial perusahaan dalam menyediakan layanan untuk pelanggannya. Dengan meningkatnya permintaan layanan melalui jaringan internet, hal ini yang dimanfaatkan oleh *cyberattacker* untuk menyusup ke dalam jaringan tersebut dan mengirimkan serangan untuk menghabiskan sumber daya *server* yang dituju. Hal ini menyebabkan penurunan kualitas layanan internet perusahaan yang dialami oleh pelanggannya. Serangan ini disebut dengan serangan *Distributed Denial of Service* (DDoS).

Diambil dari penelitian (Pei et al., 2019), serangan DDoS merupakan sebuah teknologi yang dapat menggabungkan beberapa komputer yang sudah terinfeksi virus sehingga dapat dikendalikan jarak jauh, untuk menyerang sebuah *server* secara bersamaan untuk menaikkan jumlah lalu lintas jaringan *server* tersebut. DDoS terdiri dari beberapa jenis serangan yang berbeda menurut protokolnya, seperti *TCP Flood, UDP Flood, dan ICMP Flood*.

Intrusion Prevention System (IPS) adalah sebuah sistem yang dapat mengenali aktifitas mencurigakan dalam sebuah jaringan (Wahyudi & Utomo, 2021). IPS dapat menganalisis tiap permintaan yang masuk dan mengenali permintaan yang anomali atau sah. IPS memiliki *database signature* yang membantu proses identifikasi jaringan. Jika terdapat lalu lintas jaringan yang ditandai sebagai anomali, maka IPS akan memberikan peringatan serta langsung memitigasinya. Hasil mitigasi ini kemudian akan ditampilkan dalam *log*.

PT Datacomm Diangraha merupakan salah satu penyedia layanan teknologi informasi terkemuka di Indonesia (About - Datacomm Diangraha, 2023). Salah satu layanan yang disediakan oleh PT Datacomm Diangraha adalah pada bidang *IT Security* yang menyediakan jasa pengamanan jaringan pada perusahaan. Implementasi IPS sebagai Anti-DDoS ini dilakukan PT Datacomm Diangraha untuk memenuhi kebutuhan Perusahaan X dalam menangani serangan DDoS. PT Datacomm Diangraha memberikan solusi untuk memasang perangkat keamanan sesuai dengan spesifikasi perangkat permintaan pelanggannya.

Beberapa penelitian yang sudah dilakukan sebelumnya seperti yang dilakukan oleh (Firmansyah, Negara, & Sanjoyo, 2019), IPS diimplementasikan dalam jaringan *Software Defined Network* (SDN) untuk menjadi pengaman jaringan tersebut. SDN memiliki kelebihan dalam meningkatkan efisiensi dalam mengelola sebuah jaringan komputer, yang dapat memisahkan antara *control plane* dan *data plane*. IPS diterapkan berbasis *software* yaitu dengan mengintegrasikan fungsi *Intrusion Detection System* (IDS) pada *Snort*. Setelah sistem ini diterapkan, akan dilakukan penyerangan seperti *ICMP Flood* dan *Ping of Death*. Makalah ini akan menerapkan IPS berbasis perangkat pada jaringan perusahaan untuk melakukan pencegahan *TCP Flood, UDP Flood, ICMP Flood*, serta *malware* XSS.

Penelitian lain yang dilakukan oleh Aditya (Aditya, 2020), menampilkan cara mencegah serangan DoS dan DDoS menggunakan *Host Intrusion Prevention System* (HIPS) *Snort*. HIPS Snort akan diterapkan pada *router* untuk menjadi sistem pengaman yang mengamankan data atau *file* yang tersimpan dalam *router*. HIPS Snort akan mendeteksi aktifitas yang tidak normal akibat serangan DoS dan DDoS kemudian memitigasinya. Makalah ini mengimplementasikan perangkat IPS untuk mencegah serangan DDoS. Hasilnya serangan DDoS dapat dicegah dengan menganalisis nilai lalu lintas jaringan serta *throughput server*.

Selanjutnya penelitian dari Wahyudin (Wahyudin, 2023), IPS Suricata diintegrasikan dengan *Blockchain* untuk mendistribusikan IP yang dianggap anomali kepada semua IPS yang terdapat dalam jaringan. IP anomali tersebut merupakan IP dari penyerang yang akan dicegah selanjutnya. Terdapat tiga buah IPS Suricata yang digunakan untuk mengamankan jaringan. IPS tersebut akan memblokir serangan *SYN Flood* yang dilakukan dalam beberapa metode. Hasil yang didapatkan merupakan perbandingan jumlah paket yang diterima dan dikirimkan berbeda pada tiap metode. Makalah ini mengimplementasikan sebuah perangkat IPS pada jaringan perusahaan. Pada pengujian akan membandingkan lalu lintas jaringan normal

dengan kata lain ketika tidak terdapat serangan dan ketika terjadi serangan saat dilindungi IPS. Hasil yang didapatkan adalah lalu lintas jaringan saat terjadi serangan ketika dilindungi IPS menunjukkan kesamaan dengan lalu lintas jaringan normal dilihat dari jumlah paket yang diterima dan paket yang dikirim.

Berikutnya penelitian dari Nugraha (Nugraha, 2023), pencegahan DDoS menggunakan *Self Organizing Map* (SOM) diterapkan pada SDN. SOM berguna untuk mengklasifikasikan lalu lintas jaringan normal dan lalu lintas jaringan saat terjadi serangan DDoS berdasarkan dari dataset. Hasilnya SOM dapat memitigasi serangan DDoS dengan akurasi terbaik mencapai 76,3%. Makalah ini menggunakan perangkat IPS untuk memitigasi DDoS sehingga didapatkan tingkat keberhasilan mitigasi mencapai 100% berdasarkan perbandingan dari lalu lintas jaringan normal dan lalu lintas jaringan saat terjadi serangan DDoS dengan perlindungan IPS. Perangkat yang digunakan pada makalah ini memiliki spesifikasi yang lebih mumpuni daripada (McAfee & LLC, 2019). *Trellix NS9500* memiliki kemampuan *IPS throughput* mencapai 30 Gbps. Makalah ini menggunakan perangkat sesuai dengan yang dibutuhkan perusahaan. *IPS throughput* yang dibutuhkan perusahaan sebesar 40 Gbps, sehingga perangkat yang digunakan pada makalah ini adalah perangkat yang memiliki *IPS throughput* sebesar kebutuhan tersebut.

Berdasarkan permasalahan serta penelitian yang telah dilakukan sebelumnya, maka penelitian ini mengajukan solusi mengatasi serangan DDoS menggunakan perangkat IPS. Perangkat IPS yang digunakan ditentukan sesuai dengan spesifikasi yang dibutuhkan oleh Perusahaan X. Hasil dari penelitian ini, perangkat IPS dapat menangani serangan DDoS dengan akurasi 100% dan sebagai tambahan dapat menangani serangan *malware* XSS.