1. Pendahuluan

Pada saat ini Layanan Internet sudah menjadi suatu kebutuhan bukan lagi untuk menyediakan layanan informasi, melainkan sudah menjadi hal penting maka banyak terjadi beberapa kasus website diretas oleh attacker, untuk itu keamanan jaringan sudah sangat penting untuk menghidari pencurian data penting (Perdana, 2022).

Aspek keamanan dalam konteks aplikasi web memiliki pengaruh signifikansi. Dalam artian untuk memitigasi potensi ancaman, penerapan firewall yang terintegrasi secara langsung dengan infrastruktur server menjadi solusi yang alternatif. Dalam aplikasi web, perlindungan keamanan dapat menggunakan Web Application Firewall (WAF) yang terpasang pada lapisan server menurut (Riska & Alamsyah, 2021).

Firewall yang diadopsi dalam lingkup aplikasi web berperan sebagai barikade proaktif untuk mencegah penetrasi oleh pihak yang tidak berwenang. Web Application Firewall berperan dalam melakukan konfigurasi serta pengembangan aplikasi web, sehingga potensi celah keamanan dapat ditekan seoptimal mungkin. Firewall juga dapat menyaring data yang masuk maupun keluar sehingga dapat menghentikan suatu ancaman pada server (Muharromin, 2023).

Bahkan keamanan suatu yang berbasis web memiliki kriminal lebih tinggi sehingga jaringan keamanan tidak bisa menjamin.Karena bukti kejahatan seorang peretas jaringan sulit ditemukan dan dilacak keberadaan nya (Munawar et al., 2020).

Agar Dapat mengatasi suatu permasalahan keamanan jaringan pada Aplikasi Web dan mengurangi suatu Tindakan penyerangan yang ditimbulkan akibat dari serangan yang mengancam suatu web aplikasi maka diperlukan firewall. Firewall yang dimaksud adalah mekanisme keamanan jaringan yang digunakan untuk mengamankan baik bersifat hardware maupun software (Sahren, 2021).

Web Application Firewall memiliki keunggulan yang jelas dibandingkan dengan firewall tradisional karena memberikan informasi baru ke aplikasi web yang berkomunikasi menggunakan lapisan aplikasi. Selain itu, dapat mendeteksi malware yang mengganggu aplikasi web atau Layer 7. (Aryapranata, 2020).

Menurut Imperva untuk kuartal pertama 2018, jumlah serangan web yang disebabkan oleh suntikan SQL telah meningkat sekitar 19%, atau sekitar 3.294 kasus di seluruh dunia. Ini adalah peningkatan signifikan dari tahun sebelumnya, ketika hanya ada sekitar 896 kasus yang dilaporkan. (Wiguna, 2020)

Cross site scripting dan *SQL injection* adalah dua jenis kelemahan keamanan yang dapat digunakan untuk memanfaatkan kerentanan keamanan dalam database aplikasi, Ada potensi bagi kedua model serangan ini untuk memungkinkan aplikasi web untuk menggunanaan penyerangan dengan niat jahat untuk penyimpanan data berbasis server. menciptakan dampak yang merugikan seperti Kebocoran data, pencurian informasi sensitif, serta ketidaksesuaian integritas data. Biasanya, administrator menggunakan database sekunder untuk menyimpan data atau informasi dari database utama. Dalam kasus darurat administrator akan memulihkan database dengan menggunakan cadangan namun jenis rancangan ini tidak dapat mencegah hilangnya data atau informasi. Salah satu contoh rancangan informasi adalah Ketika pengguna mendapatkan nama pengguna dan kata sandi dari database dan akan menngunakanya untuk masuk sebagai administrator situs web. (Robinson, 2018).

Web server berperan sebagai elemen penting dalam konteks pengelolaan jaringan yang menitikberatkan pada aspek keamanan. Dalam struktur ini, web server berfungsi menggabungkan data yang berasal dari berbagai klien dalam suatu rangkaian jaringan induk.

Proses ini memungkinkan klien untuk mengirim permintaan (request) guna memperoleh informasi yang diakses melalui konektivitas web server. Penting untuk dicatat bahwa penggunaan sistem perantara dalam lingkungan ini memungkinkan akuisisi informasi, termasuk data yang bersifat pribadi dan sangat rahasia. Pengaturan ini tidak hanya memastikan akses terhadap data yang terlindungi, tetapi juga mengamankan infrastruktur dari potensi serangan malware padatahap awal (Firmansyah, 2021).

Bedasarkan kasus tersebut maka perlu meningkatkan kualitas pengamanan pada aplikasi web dengan metode yang diterapkan yaitu menggunakan web application firewall (dapat berupa perangkat keras maupun lunak) perangkat yang diujikan adalah FORTIWEB. Tidak seperti beberapa studi sebelumnya, penelitian saat ini menggunakan perangkat keras untuk membangun web application firewall.