BAB 1. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan salah satu aspek penting dalam pengelolaan infrastruktur jaringan, terutama bagi suatu organisasi ataupun instansi yang mengandalkan server web dalam menyediakan layanan dan menyimpan data. Dalam era digital yang sangat kompleks ini, ancaman siber terus berkembang, menuntut setiap organisasi maupun instansi untuk mengambil langkah proaktif dalam melindungi sistem mereka. Salah satu solusi yang efektif untuk meningkatkan keamanan jaringan dari hal tersebut yaitu dengan mengimplementasikan firewall yang handal.

OPNsense, sebagai sistem operasi firewall yang berbasis FreeBSD, memiliki berbagai fitur yang mana dirancang untuk melindungi jaringan dari akses tidak sah dan serangan siber. Dengan antarmuka pengguna yang intuitif dan mudah digunakan, OPNsense memungkinkan administrator jaringan untuk mengelola dan menggabungkan lalu lintas jaringan dengan lebih efisien. OPNsense dapat digunakan sebagai keperluan firewall dan routing dalam jaringan komputer, selain itu juga dapat berfungsi sebagai pendeteksi atau pencegahan intrusi dalam jaringan komputer. (Haeruddin, 2025)

Untuk meningkatkan fungsionalitas OPNsense, Zenarmor digunakan sebagai plugin tambahan yang memiliki fitur *next-gen* dalam keamanan jaringan. Zenarmor tidak hanya menyediakan kontrol aplikasi yang canggih tetapi juga analitik jaringan yang lebih mendalam. Dengan kemampuan pemfilteran web dan inspeksi TLS (Transport Layer Security), Zenarmor mampu mencegah ancaman yang mungkin ada pada lalu lintas jaringan terenkripsi, memberikan lapisan perlindungan bagi server web.

Implementasi OPNsense dan Zenarmor pada web server diharapkan dapat meningkatkan visibilitas dan kontrol atas lalu lintas jaringan, serta mengurangi resiko serangan siber melalui pemfilteran yang lebih baik. Selain itu, kombinasi kedua software ini memungkinkan pengelolaan kebijakan

keamanan yang lebih fleksibel dan meningkatkan kinerja jaringan dengan pengaturan prioritas lalu lintas yang tepat.

Dengan latar belakang tersebut, proposal ini bertujuan untuk menjelaskan rencana penerapan firewall menggunakan OPNsense dan Zenarmor pada web server, serta manfaat yang dapat diperoleh dari penerapan solusi keamanan ini. Melalui langkah ini, diharapkan organisasi atau instansi dapat menjaga integritas sistem serta melindungi data sensitif dari ancaman yang semakin kompleks.

1.2 Rumusan Masalah

1. Bagaimana cara mengimplementasikan firewall dengan menggunakan OPNsense dan Zenarmor untuk meningkatkan keamanan pada web server?
2. Sejauh mana OPNsense dan Zenarmor efektif dalam mencegah serangan dan ancaman terhadap web server?
3. Bagaimana cara melakukan monitoring dan analisis lalu lintas jaringan web server dengan menggunakan fitur-fitur yang ada pada OPNsense dan Zenarmor?

1.3 Tujuan

Penelitian ini bertujuan untuk:

1. Mengimplementasikan firewall menggunakan OPNsense dan Zenarmor untuk meningkatkan keamanan web server.
2. Menganalisis efektivitas OPNsense dan Zenarmor dalam mencegah serangan dan ancaman terhadap web server.
3. Melakukan monitoring dan analisis lalu lintas jaringan web server, serta mendeteksi potensi ancaman *DDoS, SQL injection*, ataupun lainnya. menggunakan fitur-fitur OPNsense dan Zenarmor.

1.4 Manfaat

1. Memiliki fitur pemantauan canggih, Zenarmor dapat memungkinkan deteksi dan pemblokiran terhadap ancaman berdasarkan analisis paket data.
2. Menampilkan analitik jaringan dengan real time dan laporan aktivitas serta pola trafik.