



ABSTRAK

Dalam perusahaan besar, *internet* merupakan sebuah media yang sangat penting bagi sebuah perusahaan. Untuk melancarkan proses bisnis mereka, dibutuhkan *server* yang dapat melayani pelanggan atau pengguna dalam waktu yang tidak terbatas menggunakan akses *internet*. Namun, serangan dari pengguna *internet* terhadap *server* tidak lah sedikit. Salah satu serangan yang sering di temui adalah *Denial of Service*. Oleh sebab itu diperlukan sebuah perangkat yang dapat mengamankan dari sejumlah serangan *Denial of Service*. Tidak hanya diamankan, sebuah serangan juga harus dapat terdeteksi agar dapat dilakukan penanganan lebih lanjut.

Salah satu metode yang sering dipakai dalam dunia jaringan komputer untuk mengamankan sebuah *server* adalah *Demilitarized Zone*. *Demilitarized Zone* merupakan sebuah topologi dimana jaringan pada *server* dipisahkan dengan jaringan lokal dan diamankan oleh sebuah *firewall*. Sebuah *firewall* juga dapat disandingkan dengan *Intrusion Detection System* atau yang biasa disebut IDS. IDS merupakan perangkat *monitoring* jaringan yang dapat berguna sebagai pendeteksi serangan. Dengan begitu, *firewall* akan memberikan *rule policy* pada setiap jaringan dan IDS akan memonitor trafik agar jaringan menjadi lebih aman.

Kata Kunci: *Denial of Service, Demilitarized Zone, Firewall, IDS*



ABSTRACT

In larger companies, the Internet is a medium that is essential for a company. To launch their business processes, it takes a server that can serve the customers or users from internet. However, attacks from the internet to the server was not a bit. One of the popular attacks is Denial of Service. Therefore, needed a device that can be secured from Denial of Service attack. Not only secured, an attack can also be detected in order to do further treatment.

One method that used in the world of computer networks to secure a server is the Demilitarized Zone. Demilitarized Zone is a network topology where the servers segregated and secured by a firewall. A firewall can also be paired with Intrusion Detection System or commonly known as IDS. IDS is a network monitoring device that can be useful for detecting attacks. That way, the firewall will provide policy rule on any network and IDS will monitor network traffic to be more secure.

Keywords: Denial of Service, Demilitarized Zone, Firewall, IDS