ABSTRACT

Inline with the needed of corporation to provide their service to colleague *(B2B)* or to customers *(B2C)* in the Internet therefore there is need to find a way or concept to secure their internal private network .

DMZ *(Demiliterized Zone)* is one of the concept that can be use to accommodate that need . DMZ act like a buffer zone that create it own zone between external network and internal network .

In general DMZ built based on three concept , which are ; NAT (*Network Address Translation*), PAT (*Port Addressable Translation*), and *Access List* . Role of NAT is to show back incoming packets from "real ip address" to internal network address . For Example : if we have "real ip address" 203.8.90.100 we can create a NAT automatically for incoming data to 192.168.100.1 (an internal ip address) .PAT is to show incoming data to the particular port or range of a port and protocol (TCP/UDP or else) from external ip address to a particular port or range a port within internal ip address . While access list's role is to control precisely what came in and what came out in the network , for example : we can deny or accept all incoming ICMP to whole ip address unless for specific ICMP that we don't want .

Keywords : DMZ , Network Security .

ABSTRAK

Seiring dengan kebutuhan para perusahaan yang perlu menyediakan layanan bisnis mereka ke relasi *(B2B)* ataupun ke konsumen *(B2C)* dalam Internet maka diperlukan juga suatu cara atau konsep untuk mengamankan jaringan internal mereka sendiri .

DMZ *(Demiliterized Zone)* adalah salah satu konsep yang bisa mengakomodir keperluan tersebut . DMZ berfungsi seperti zona penyangga atau *buffer zone* yang menciptakan zona tersendiri antara jaringan komputer luar (baca: Internet) dan jaringan komputer dalam

Secara umum DMZ dibangun berdasarkan tiga buah konsep, yaitu : NAT (*Network Address Translation*), PAT (*Port Addressable Translation*), dan *Access List.* NAT berfungsi untuk menunjukkan kembali paket-paket yang datang dari "alamat ip sesungguhnya" ke alamat internal. Misal : jika kita memiliki "alamat ip sesungguhnya" 203.8.90.100, kita dapat membentuk suatu NAT langsung secara otomatis pada data-data yang datang ke 192.168.100.1 (sebuah alamat jaringan internal). Kemudian PAT berfungsi untuk menunjukan data yang datang pada *particular port* atau *range* sebuah *port* dan *protocol* (TCP/UDP atau lainnya) dari alamat IP luar ke sebuah *particular port* atau *range* sebuah *port* dalam alamat IP internal . Sedangkan *access list* berfungsi untuk mengontrol secara tepat apa yang datang dan keluar dari jaringan , misal : kita dapat menolak atau memperbolehkan semua ICMP yang datang ke seluruh alamat IP kecuali untuk sebuah ICMP yang tidak diinginkan.

Kata Kunci : DMZ , Keamanan Jaringan