ABSTRAK

Semakin maraknya penggunaan teknologi nirkabel pada tempat-tempat umum (seperti cafe, restaurant, hotel dan perkantoran) membuat mayoritas pengusaha berlomba-lomba menyediakan akses internet gratis berbasis nirkabel di tempat usahanya. Namun tidak sedikit administrator jaringan tersebut tidak memperhatikan masalah keamanan, sehingga dapat menjadi sebuah celah dan dimanfaatkan oleh seorang "hacker" untuk merusak atau mengganggu layanan dari server setempat. Tentunya akan merugikan perusahaan tersebut karena pelanggan yang menggunakan fasilitas internet di tempat tersebut merasa terganggu atau bahkan merasa dirugikan. Oleh karena itu tugas akhir ini mencoba untuk menginovasikan sebuah sistem keamanan untuk melindungi server di tempat-tempat umum yang memiliki akses nirkabel untuk menggunakan layanannya. Sistem keamanan utama dari tugas akhir ini merupakan sistem firewall IPS (Intrusion Prevention System) yang dibantu oleh teknologi Captive Portal yang dirancang secara redundansi.

Alat authentikasi yang biasa dipakai di jaringan nirkabel adalah captive portal. Captive portal memakai standar web browser untuk memberi seorang user nirkabel kesempatan untuk mengauthentikasi dirinya, biasanya berupa username & password. Captive portal biasanya dipakai di jaringan terbuka yang tak punya metode authentikasi lain (seperti WEP atau MAC filter). Di jaringan publik atau semi-publik, teknik enkripsi seperti WEP dan WPA tidak berguna. Tidak ada cara untuk menyebarkan publik atau kunci yang dipakai bersama kepada masyarakat tanpa membahayakan keamanan dari kunci tersebut. Sistem autentikasi yang disediakan oleh Captive Portal memungkinkan untuk dirusak sehingga seorang "Hacker" mampu melakukan penyerangan terhadap server yang memang dituju olehnya. Oleh karena itu digunakanlah teknologi keamanan *Intrusion Prevention System* yang mampu melakukan blocking terhadap trafik yang dicurigai sebagai serangan dan mampu merusak atau mengganggu layanan *server* setempat.

Pada implementasi sistem ini, sudah diujicobakan pada berbagai macam serangan, seperti *Port Scanning*, DoS, dan DDoS yang merupakan salah satu tipe serangan yang mengeksploitasi sistem dimana akan dikirimkan request dalam jumlah besar, sistem yang tidak mampu menangani banyak request tersebut akan habis sumber daya sistemnya sehingga kinerja sistem secara utuh akan terganggu. Oleh karena itu, digunakanlah *Captive Portal* untuk mencegah masuknya pengguna ilegal dan redundansi *firewall* IPS yang membuat jaringan lebih tahan terhadap serangan pembanjiran trafik.

Kata Kunci : ***Captive Portal, Intrusion Prevention System, Wireless, Redundant, DDoS***