ABSTRACT

Increasingly the use of wireless technology in public places (such as cafes, restaurants, hotels and offices) make the majority of entrepreneurs are competing to provide wireless internet access based on his place of business. But not a few of the network administrator does not aware about security issues, so it may be a gap which can be exploited by a "hacker" to damage or disrupt the service of the local server. Surely it would be harm for the company because the customers who use the internet facilities at the site was disturbed or even feel aggrieved. Therefore, this thesis tries to innovate a security system to protect the server in public places that have wireless access to use their services. The main security system of this thesis is a system firewall IPS (Intrusion Prevention System) assisted by Captive Portal technology which is designed of redundancy.

Authentication tool which commonly used in wireless networks is a captive portal. Captive portal using a standard web browser to give a user access a chance to authenticate themselves, usually in the form username and password. Captive portals are usually used in open network with no other authentication methods (such as WEP or MAC filters). In the public network or a semi-public, techniques such as WEP and WPA encryption is not useful. There is no way to deploy a public or shared key to the public without jeopardizing the security of the key. Authentication system provided by the Captive Portal is possible to destroyed so that a "Hacker" are able to attack the server that is intended by it. Therefore, the security technology in this thesis is used Intrusion Prevention System which capable of doing some blocking for the traffic suspected of attacks and could damage or interfere with the local server services.

In the implementation of this system has been tested on a variety of attacks, such as port scanning, DoS and DDoS, which is one type of attacks that exploit the system where the request is sent in large quantities, the system is not able to handle the many requests the system will run out of resources so the performance of the system as a whole will suffer. Therefore, the Captive Portal is used to to prevent the entry of unauthorized users and IPS firewall redundancy that makes the network more resistance to flooding attack traffic.

Keywords : ***Captive Portal, Intrusion Prevention System, Wireless, Redundant, DDoS***