ABSTRACT

IPv6 to IPv4 transitions mode is a solution to change from IPv4 to IPv6, one of "IPv6 to IPv4" transitions is 6to4. But, there are security considerations to use 6to4 that the routers must accept and forward IPv4 packets from any other router. Thus, IPv6 to IPv4 transition mode on the public network may have some vulnerability, because of no threat detection like sniffing, and spoofing.

On network security there are various algorithm for message encryptions and decrytions, one of them is RSA (Rivest Shamir Adleman) algorithm. RSA algorithm is asymmetryc crypthographic algorithm with different key on encryption and decryption. RSA still used on electronic commerce protocol and securing with a long key, demanding a long time to crack the key. On this research, implementation of RSA algorithm for securing data and communicating between client and server on 6to4 will be analyzed.

Results from the research are, when SSH server send 10 MB data the server need 64.1172 ms on delay while FTP server need 39.6879 ms. But, the SSH server more secure than FTP server. Because, when logging in to SSH server the password, username, and data contains are encrypted while logging in to FTP server the password, username, and data contains can be sniffing by attacker. On CPU-uttility analisys, transfer using SSH causing the average CPU usage is 15.19355 %, while it's 1.333333% on FTP server (without encryption).

keywords : spoofing, sniffing, RSA, delay .