Abstract

File Transfer Protocol or FTP is a protocol used to exchange files, either file upload or file download. Unfortunately, FTP still leaves a security hole where the transmitted data over that two channels can still be read clearly. In addition, the absence of a server authentication mechanism, make the client can access the FTP server at risk for false.

This study tested the Secure FTP and FTPS, both methods which are applied to the FTP security to address the security gaps left by FTP. Security aspects tested include confidentiality (data confidentiality) and authentication (authentication). In addition, this study also tested both methods in terms of performance. Performance aspects tested include delay, throughput, and utilities of CPU and memory on a single file transfers and multiple transfers, and also to the complexity of the use of both methods.

From the test results, obtained a conclusion that the FTPS has a higher security level than the Secure FTP. In addition,on the performance, though superior to the Secure FTP in single file transfers but on the other tests, FTPS have better results than the Secure FTP. From these two aspects of testing, we can conclude that the FTPS have better abilities than Secure FTP in terms of both security and performance.

Keywords*: security, performance, FTP, Secure FTP, FTPS*