

SFTP vs. FTPS : Which One To Use?

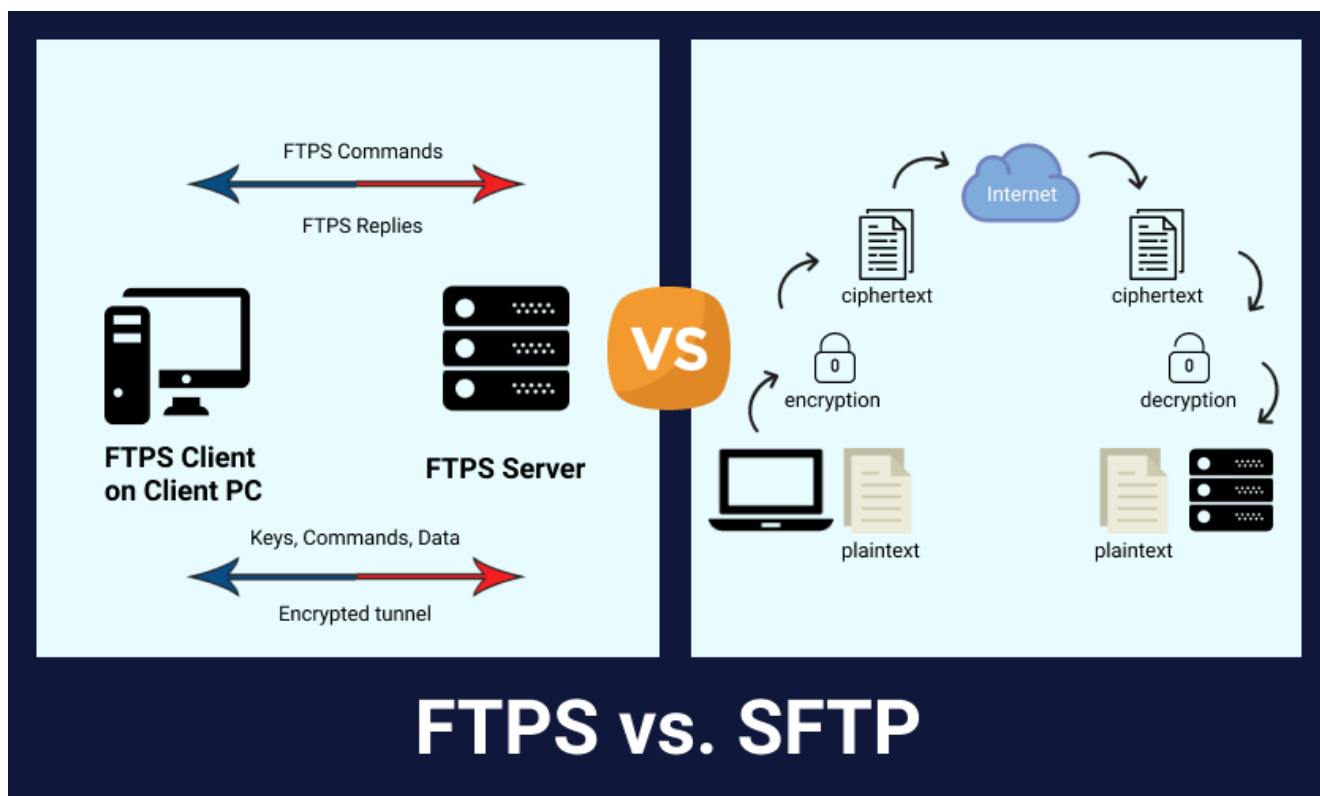
SFTP Overview

SFTP (SSH File Transfer Protocol) is referred to as the extension of the SSH protocol which permits the transfer of files through a network.

FTPS Overview

FTPS is a protocol that utilizes a Secure Sockets Layer (SSL) certificate to provide security. The authentication of a protected FTP connection is conducted through the use of the following elements: SSL certificate, user ID, and password. Upon creation of an FTPS connection, the destination FTP server is reviewed through the FTP client software to verify the trust-ability of a server's certificate.

Difference between SFTP and FTPS



SFTP vs. FTPS : Which One To Use?

Each user has unique requirements when it comes to selecting the most appropriate transfer protocol. However, using FTPS is recommended if a server requires accessibility from portable devices, such as PDAs and smartphones or operating systems which do not have SFTP/SSH clients and yet provide FTP support. Accordingly, SFTP is the way to go if you are seeking to develop a custom security solution.

As for the client side, the requirements are already determined by the server(s) with which they intend to connect. SFTP is the more favored choice when establishing a connection with internet servers due to the by-default support that it enjoys from UNIX and Linux servers.

On the other hand, you have free rein to choose both FTPS and SFTP in case of private host-to-host transfers. However, you would have to hunt for a free FTPS client and server software to use FTPS or buy a license for commercial usage.