**SFTP**

SFTP (SSH File Transfer Protocol, also known as Secure FTP) is a popular method for securely transferring files over remote systems. SFTP was designed as an extension of the Secure Shell protocol (SSH) version 2.0 to enhance [secure file transfer](https://www.serv-u.com/features/secure-file-sharing) capabilities. SFTP supports [file access](https://www.serv-u.com/features/file-access), file transfer, and file management functionalities without command or data channels. Instead, both data and commands are encrypted and transferred in specially formatted binary packets via a single, secured connection using SSH.

They require dedicated SFTP clients, that use SSH to access, manage, and transfer files. The Command-Line Interface (CLI) in UNIX® and Mac OS® X hosts can be used as SFTP clients. There are also many graphical FTP clients, such as the [free FTP client for Windows®, FTP Voyager®](https://www.serv-u.com/free-tools/ftp-voyager-ftp-client-for-windows), which supports file transfer via SFTP.

**Benefits of SFTP over FTP & FTPS**

* File transfer is much faster as SFTP transmits data in binary format; therefore, less data crosses the wire compared to FTPS.
* SFTP uses only one connection, and there’s no need for a dedicated data channel.
* The SFTP connection is always secured with SSH.
* The SFTP directory listing is uniform and machine-readable.
* In addition to file transfer, SFTP also includes operations for permission and attribute manipulation, file locking, etc.

**An SFTP connection can be authenticated in two ways:**

* Basic authentication requires a user ID and password from the SFTP client user to connect to the SFTP server.
* SSH authentication uses SSH keys to authenticate SFTP connections instead of, or in combination with, a user ID and password. An SSH public key and private key pair are required in this case.
* Generate a key pair on your computer (SFTP client), and copy the public key to the SFTP server.
* When the server authenticates your connection to it, PuTTY generates a signature using your private key.
* The server, which has the matching public key, can verify this signature and authenticate your connection.

Even if the SFTP server is hacked or spoofed, the attacker gains only one signature, not your private key or password. Because signatures cannot be re-used, he has actually gained nothing.

.