What's the best protocol for secure FTP?

SFTP vs. FTPS

Moving away from standard file transfer protocol (FTP)? Learn about the secure FTP protocol options available for transferring data and the differences between them.

Features	SFTP Also known as: FTP over SSH (Secure Shell)	FTPS Also known as: FTP over SSL (Secure Socket Layer)
Implements strong encryption algorithms	✔ Algorithms such as AES and Triple DES are used to encrypt transferred data.	✔ Algorithms such as AES and Triple DES are used to encrypt transferred data.
Encrypts usernames and passwords	✔ User IDs and passwords over the SFTP connection are encrypted.	✔ User IDs and passwords over the FTPS connection are encrypted.
Supports key-based authentication	✔ SSH keys can be used to authenticate SFTP connections in addition to (or instead of) passwords.	✘ Key-based authentication is not supported.
Supports certificates	✘ Certificates are not supported.	✔ Connections are authenticated using a user ID, password, and certificate(s).
Firewall-friendly	✔ Only needs a single port number (default of 22) to be opened through the firewall	✘ Can be very difficult to patch through a tightly secured firewall since FTPS uses multiple port numbers

Automate Secure File Transfers with SFTP and FTPS

Whether you're using SFTP, FTPS, or other protocols, GoAnywhere MFT automates the transfer of files between systems, employees, customers, and trading partners—no programming required.

DOWNLOAD TRIAL