¿Cuál es el mejor protocolo para asegurar su FTP?

SFTP vs. FTPS

¿Desea cambiar su protocolo de transferencia de archivos (FTP)? Conozca estas dos opciones de FTP seguro para transferir información, y las diferencias entre ellas.

CARACTERÍSTICAS	SFTP También conocido como FTP sobre SSH (Secure Shell)	FTPS También conocido como FTP sobre SSL (Secure Socket Layer)
Emplea potentes algoritmos de encriptación	✔ Usa algoritmos como AES y Triple DES para encriptar la información transferida	✔ Usa algoritmos como AES y Triple DES para encriptar la información transferida
Encripta usuarios y contraseñas	✔ Los ID y contraseña de usuario son encriptados	✔ Los ID y contraseña de usuario son encriptados
Soporta autenticación basada en claves	✔ Pueden usarse claves SSH para autenticar conexiones SFTP adicionalmente o en lugar de las contraseñas	✘ No soporta autenticación basada en claves
Soporta certificados	✘ No soporta certificados	✔ Las conexiones son autenticadas usando un ID de usuario, contraseña y certificados
Compatible con Firewalls	✔ Necesita un solo número de puerto (por defecto el 22) para conectarse a través del firewall	✘ Puede resultar difícil hacer un parche a través firewall debido a que el FTPS usa múltiples números de puertos

Asegure y automatice las transferencias de archivos con SFTP y FTPS

Ya sea que usted use SFTP, FTPS, u otros protocolos, GoAnywhere MFT le permite automatizar la transferencia de archivos entre sistemas, empleados, clientes y socios comerciales sin necesidad programación.

Descargue su prueba gratuita