

Secure FTP Comparison

Protocol	Description	Ports	Security	Notes
FTP	File Transfer Protocol	21/20 (TCP) control/ data	No security, public file retrieval only. Clear-text password sent over the network. May require authentication with a username and password or just "anonymous"	FTP client/server control port usually on tcp port 21. Data transfer modes (active - PORT or passive - dynamic port via PASV command). Defined by RFC 959, 1123
SFTP	Uses SSH2	22 (TCP)	Key based (Must install keys on server) Assumes both ends of the connection have been authenticated, security issues are left to the underlying transport protocol	Remote logon protocol, data is not encrypted. All communications take place through an encrypted pipe or tunnel. Derived from SCP, not FTP Note - WinSCP client defaults to SFTP protocol (Server software - CrushFTP4)
FTPS	FTP over an SSL connection (Explicit - port 21, or Implicit - port 990, encrypted)	21/20 or 990/989 (TCP)	Certificate based (CA's), requires private key generation	Setup in most servers, uses FTP ports Password and data is encrypted Defined by RFC 959, 1123, 4217 and 2228
SCP	Secure Copy	22 (TCP)	run over SSH session (source mode -f (from), sink mode -t (to))	Not used any more Data is encrypted during transfer No authentication Used mostly as a command line program - scp scp [options] [user@]host1:]file1 [...] [user@]host2:]file2
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	443 (TCP)	HTTP over an encrypted SSL or TLS connection	Administrator must create a public key certificate for the web-server Certificate must be signed by a certificate authority RFC 2818 (HTTP Over TLS)
AS2	Applicability Statement 2 (specification on secure transport)	443 (TCP)	Certificate based (CA's) S/MIME - non-repudiation, confidentiality (encryption)	Based on HTTP and SMIME - for Internet transport Files are sent as "attachments" in a specially coded SMIME message RFC 4130

Because FTP is a **port-hopping protocol** (i.e. data channels use a random port chosen during the communication), many firewalls are designed to understand FTP protocol messages to determine what secondary data connections they need to allow. However, if the control connection is encrypted using TLS/SSL (or any other method for that matter), the firewall is not able to get the port numbers of the data connections from the control connection (since it is encrypted and the firewall cannot decrypt it). Therefore, in many firewalled networks, clear FTP connections will work while FTPS connections will either completely fail or require the use of **passive mode** (assuming all ports ≥ 1024 to the server are unfiltered).

SSH - a tool used to connect to any machine from a remote location. It is strongly advised not to give **remote access** to user **root**, rather create another user with less privileges and give access to ssh.