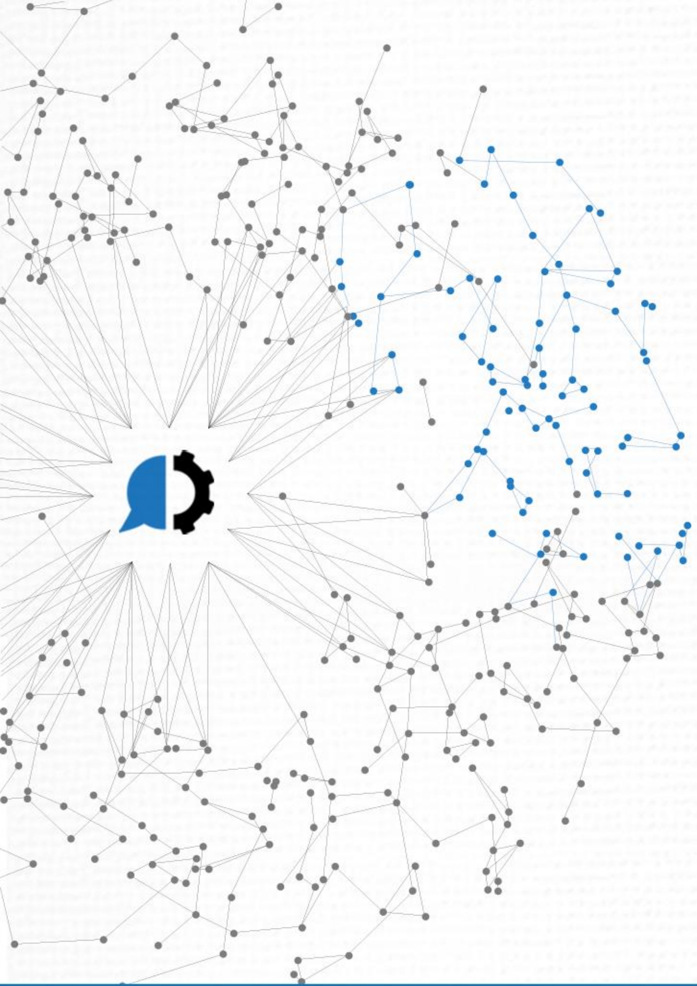


GO ANYWHERE®
Managed File Transfer

FTP, FTPS, & SFTP: Which Protocol Should You Use and When?

www.goanywhere.com

Today’s Presenters

GO ANYWHERE® Managed File Transfer

Chris Spargen

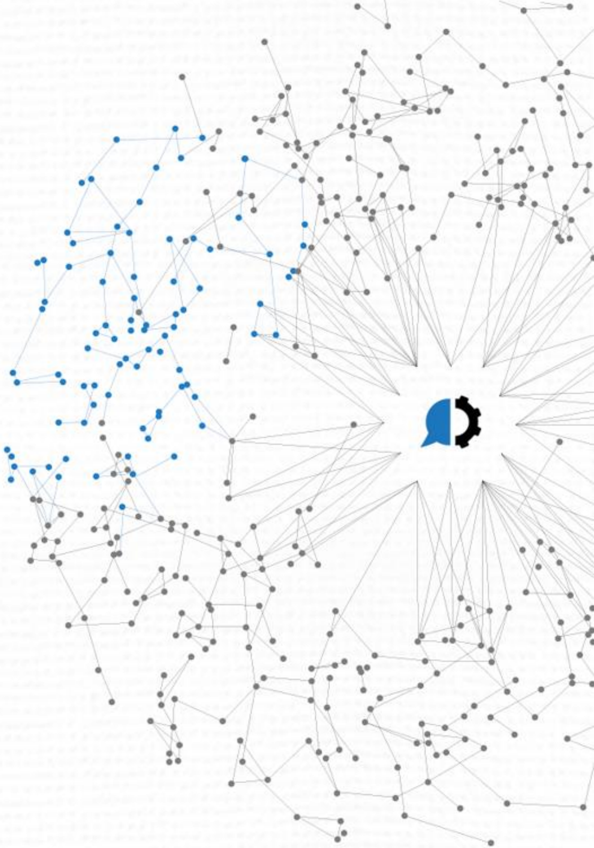
Manager of Support and Services

HelpSystems

helpsystems

Agenda

1. What is FTP?
2. What is FTPS?
3. What is SFTP?
4. The Key Similarities and Differences
5. FTPS vs. SFTP Architecture
6. Which Protocol is Best
7. Q&A



UP NEXT

What is FTP?

GO ANYWHERE® Managed File Transfer

- FTP is a popular file transfer method that has been around longer than the World Wide Web.
- It was created without the assumption that internet activity could be malicious – therefore, it wasn’t constructed to handle the kind of cybersecurity threats that exist today.
- FTP exchanges data using two separate channels known as the command channel and data channel. With plain FTP, both channels are unencrypted, leaving any data sent over these channels vulnerable to being intercepted and read.

What is FTPS?

- There are 2 distinct references to FTPS:
  - FTPES – Explicit SSL, typically uses port 21
    - Unencrypted command channel, the encryption occurs on the data channel only. The SSL handshake occurs after user authentication on the command channel.
  - FTPS – Implicit SSL, typically uses port 990
    - SSL handshake occurs when a client connects to the command channel.
- FTPS (FTP over SSL – Secure Sockets Layer) is a secure FTP protocol that allows you to protect and exchange files with trading partners, employees, and clients.
- FTPS implements strong algorithms like AES and Triple DES to encrypt sensitive file transfers.
- For authentication, FTPS uses a combination of user IDs, passwords, and/or certificates to verify a user's authenticity.

What is SFTP?

GO ANYWHERE®
Managed File Transfer

- SFTP (SSH/Secure Shell File Transfer Protocol) is a secure FTP protocol that sends files over SSH providing a high level of protection for file transfers.
- SFTP implements AES, Triple DES, and other algorithms to encrypt data that flows between systems.
- It offers several ways to authenticate a user session—with a user ID and password, SSH key, or a combination of a password and SSH key—for organizations that require stronger authentication.

The Key Similarities and Differences

- Plain FTP isn’t encrypted, unless you leverage explicit SSL.
- The design of the FTP protocol uses one channel (port 21) for sending authentication commands and receiving acknowledgements. However, it must open another port dynamically in order to transfer data. This is called the data channel.
- FTPS was designed to be more speed-friendly, with the control and data channel running asynchronously in two distinct connections in order to achieve the highest possible data transfer speed. It also layered in security by leveraging SSL.
- When it comes to ease of implementing SFTP or FTPS, SFTP is often considered the easiest secure FTP protocol to implement due to the single port.

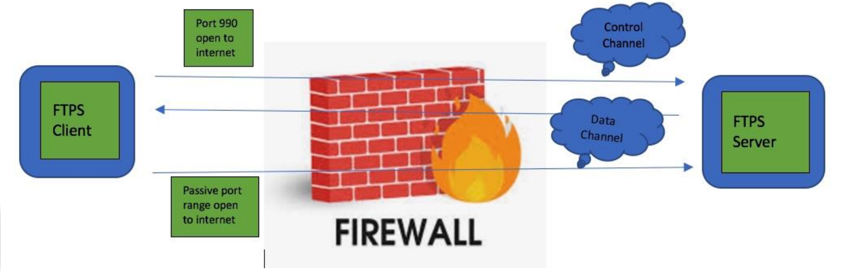
FTPS vs. SFTP

- FTPS can be difficult to connect through firewalls with high levels of security. FTPS uses multiple port numbers for the command and data channels, with a larger volume of available ports being required for the data channel.
  - SSL certificates can be signed by certificate authorities (CA's) to validate both client and server.
- SFTP is more friendly to today's client-side firewalls since it only requires a single port to be open through the firewall. This single SFTP port will be used for all communications, including the initial authentication, any commands issued, and any data transferred.
  - SSH keys can be shared among trading partners but there are no CA's or 3rd parties to verify an SSH key.

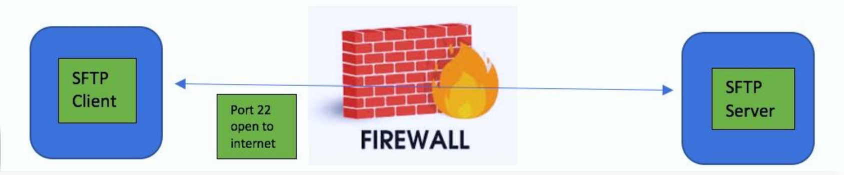
FTPS vs. SFTP Architecture

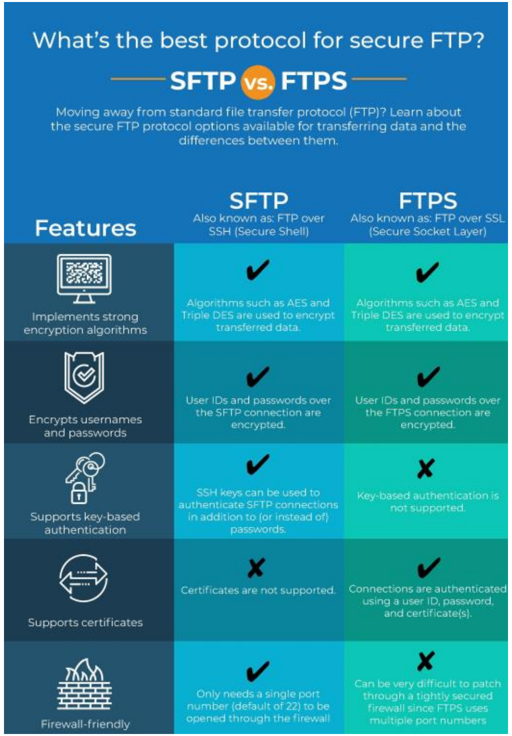
GOANYWHERE® Managed File Transfer

- FTPS


Port 990 open to internet
Control Channel
FTPS Client
Data Channel
FTPS Server
Passive port range open to internet
FIREWALL

- SFTP





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

Which Protocol is Best?

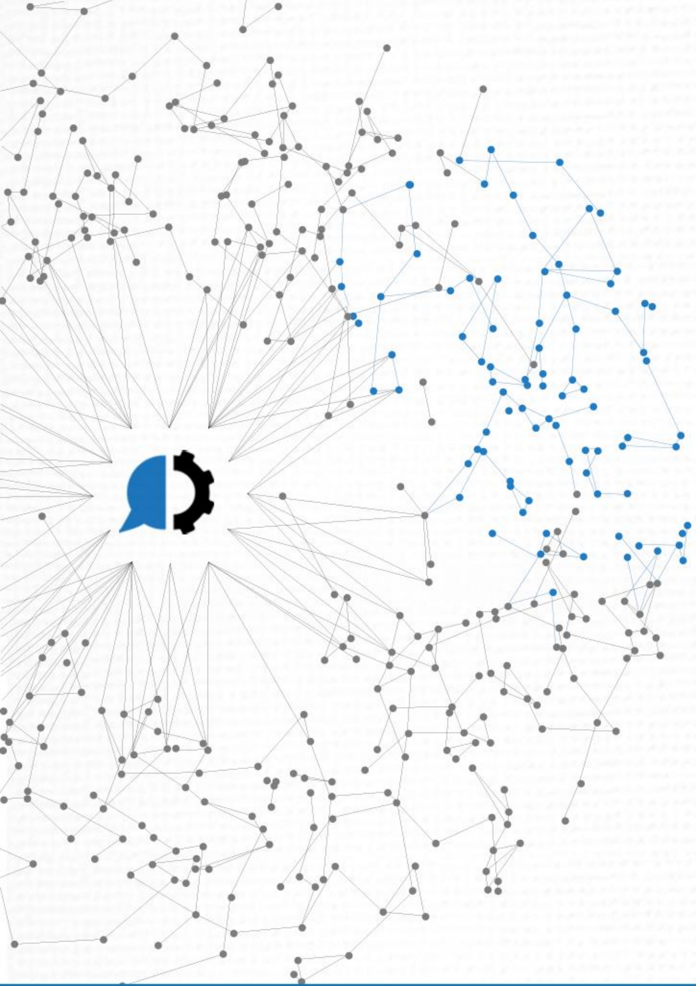
- Arguments can be made for both
- When looking at both protocols from a security perspective:
  - SFTP has historically had less vulnerabilities than FTPS (SSL)
  - SFTP uses a default port of 22 which is the default SSH port on most linux/unix operating systems.
- Examples where FTPS is the best choice:
  - Your trading partner requires 3rd-party verified SSL certificates to establish trust. SSL certificates have CA's, whereas SSH keys do not
  - You have a requirement for EBCDIC or ASCII data transfers
- An example of a situation where SFTP is the best choice:
  - Your trading partner requires SSH Public Key authentication
  - Your trading partner or firewall teams prefer a single port to be leveraged

Thank you for joining us!

GOANYWHERE®
Managed File Transfer

- Questions about new GoAnywhere features? We're happy to help.
  - goanywhere.support@helpsystems.com
  - www.goanywhere.com
- Request a walkthrough of new features at www.goanywhere/demo or reach out to your sales representative.

A survey will display after this webinar ends.
Please let us know how we did. Thanks for your feedback!



Any Questions