Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-inet-ftp

INTERNET

FTP, FTPS and SFTP: three ways to transport parcels

At Three Letters and a Warehouse Transport Company, Greg decided to send a single file. Three signs hung above the gates: FTP, FTPS and SFTP. All three promised to deliver his parcel, but every driver had different keys, different trucks and a different idea of security. Greg looked at a file called “final_version_REALLY_7.zip”. “People, I JUST WANT TO SEND ONE FILE!” 📦🤣

Two gates for one warehouse

— Good morning, I'm FTP — said the manager of the first warehouse.

— File Transfer Protocol? — asked Greg.

— Exactly. I've been moving files between clients and servers for a long time.

— Then why do you have two gates?

— One for talking, another for carrying parcels.

In classic **FTP**, the client creates a **control connection**, usually to TCP port `21`. Through it the client logs in, sends commands, changes directories and requests file lists. File contents and directory listings use a separate **data connection**.

— So I shout “bring me the parcel” at the first gate, and a truck uses the second?

— Precisely.

— Why not just one gate?

— That's how the protocol was designed. Please don't rebuild the warehouse on your first day.

Active mode: the courier calls Greg

— Let's try active mode — said the manager.

— I'm very active! I can run! — Greg cheered.

— This is about who initiates the data connection.

In **active FTP**, the client tells the server the address and port where it will accept a data connection. The server then tries to connect back to the client. Historically, the server often used source TCP port `20`, although implementations and modes differ.

The courier stood outside Greg's apartment and pressed the intercom.

— Parcel delivery!

— WHO INVITED YOU?! — shouted the NAT router.

— Greg ordered something!

— That's lovely, but I don't allow uninvited incoming Internet connections!

A client behind **NAT or a firewall** can have trouble with active FTP because the server must establish a fresh incoming connection to it.

— It worked until we locked the front door?

— Yes. And throwing every door wide open isn't a great cure.

Passive mode: Greg goes to collect the parcel

— Let's try passive mode — suggested Agnieszka.

— So we do nothing?

— No, Greg. The client initiates the data connection this time.

In **passive FTP**, the server tells the client an address and port on which it is waiting. The client opens the data connection toward the server. Commands such as `PASV` and `EPSV` are used. The server often uses a configured passive port range, which the firewall must allow.

— I leave my apartment and travel to the warehouse?

— Exactly. Your router generally finds an outbound connection easier to handle.

— What if the server gives me an unreachable private address?

— Poor NAT setup or a bad server response can still break things. EPSV helps avoid some address-related problems.

— So passive mode always works by magic?

— The Marketing Department handles magic.

A password on a postcard

At the FTP gate, Greg provided his login and password.

— Write them here — said the guard, handing him a transparent envelope.

— EVERYONE CAN SEE THIS!

— You've found the classic FTP problem.

Ordinary **FTP doesn't encrypt** login commands or file contents by default. Someone able to monitor the relevant network path may read sensitive information. FTP has a long history, but sending credentials and data in clear text across untrusted networks is a poor choice today.

— What if I name the file TOP SECRET with eight exclamation marks?

— Still not encryption.

— What if my password is really long?

— Length doesn't help if someone can observe it in transit.

Greg put down the transparent envelope.

— I'd prefer a truck with locked doors.

FTPS: the old warehouse gets TLS seals

A truck marked **FTPS** pulled up.

— I'm still FTP, but TLS protects my transport — announced its driver.

— You just added the letter S?

— The name suggests that, but technically I'm FTP secured with TLS, still using separate control and data connections.

With **explicit FTPS**, a client commonly connects to port `21` and requests TLS negotiation using `AUTH TLS`. There's also a historic **implicit FTPS** variation, traditionally on port `990`, where TLS starts immediately. Protecting the data connection also requires the right settings, such as `PROT P`.

— Does the firewall now know which gate to open for the second truck?

— Not necessarily. If control traffic is encrypted, a network device can't simply inspect FTP commands to predict the required data ports.

— A safer truck, but a more confused doorman?

— Exactly. Configure port ranges, address handling and firewall rules properly.

— Couldn't somebody have designed this more simply?

— Ask the historians.

SFTP is not FTP wearing a different hat

At the third gate stood a driver with an SSH identity badge.

— SFTP. Welcome.

— Are you FTPS with the letters rearranged? — asked Greg.

— ABSOLUTELY NOT!

SFTP is a distinct file transfer protocol operating over **SSH**. It is not the same as FTP or FTPS. It usually uses a single connection to an SSH server on TCP port `22`, unless the administrator chose another port. It doesn't use FTP's separate control and data sessions.

— One gate?

— Yes. Authentication and transport rely on SSH mechanisms.

— Password or public-key authentication?

— Depending on configuration. Public-key login uses a pair of SSH keys, with the server verifying the client's authorization.

— And the server has an identity?

— It has an SSH host key. Check its fingerprint when establishing trust, and don't casually dismiss warnings about unexpected changes.

— So you aren't ordinary FTP with a padlock?

— No. One more question like that and I'll charge tuition.

Delete is not a request for time off

Greg finally connected to the warehouse.

— I can see a directory! Can I upload, download, rename or delete?

— If your account and the server permissions allow it — replied Agnieszka.

Programs such as FileZilla and WinSCP provide convenient interfaces for working with files, but the underlying protocol still matters. Appropriate permissions, dedicated accounts and limited directories can reduce the damage from mistakes. Encrypted transport doesn't protect a file from deliberate deletion by a user authorized to delete it.

— If I erase everything, SSH won't save me?

— No. Encryption protects transmission, not bad decisions.

— And backups?

— Essential. A separate copy, not another button in your FTP client.

— Perhaps I'll start by sending one file after all.

— That's how this whole day began, Greg.

— Don't remind me.

A large file and a broken connection

The courier left with a file weighing several gigabytes. Halfway there, the Internet connection vanished.

— THE PARCEL IS LOST! — Greg shouted.

— Let's check how much actually arrived.

Many clients and servers support **resuming interrupted transfers**, but the possibilities depend on the protocol, program, server and how the file is handled. Classic FTP has commands such as REST, while SFTP supports reads and writes at specified offsets. When integrity really matters, verify the result, for example by

comparing checksums.

— If the file looks complete, is it definitely complete?

— Don't assume that. Matching size helps, but doesn't always prove identical contents.

— What if I sent an old file with the right name?

— Even a perfect protocol can't know you picked the wrong parcel.

Greg went looking for “final_version_REALLY_8.zip”.

The warehouse report

At the end of the day, the manager lined up three trucks.

— FTP?

— Traditional transport with separate control and data connections, unencrypted in its ordinary form.

— FTPS?

— FTP secured with TLS, still using separate roles for the connections.

— SFTP?

— A different file transfer protocol using SSH.

Choose based on compatibility, security requirements and access management. For new services moving data over untrusted networks, a securely configured SFTP or FTPS setup is preferable to sending passwords through plain FTP. Permissions, integrity checks and backups require separate attention.

— Can I finally send my file?

— Yes.

— Where is it?

— In the Recycle Bin on my desktop.

There was silence in the warehouse.

— PLEASE DON'T LOOK IN THERE! — Greg yelled.

Management of Three Letters and a Warehouse reports: FTP's control gate is operational, passive ports have been organized, FTPS trucks have received their TLS seals, and SFTP refuses another order labeled “the same, only with more S”. Greg finally uploaded his file. Unfortunately, it was a shortcut pointing to the file. The delivery was a technical success and an organizational disaster. 🧀🚚🤣❤️