What is SFTP

**SFTP** stand for ***SSH File Transfer Protocol***.

First, let’s review **FTP** or **file transfer protocol**.

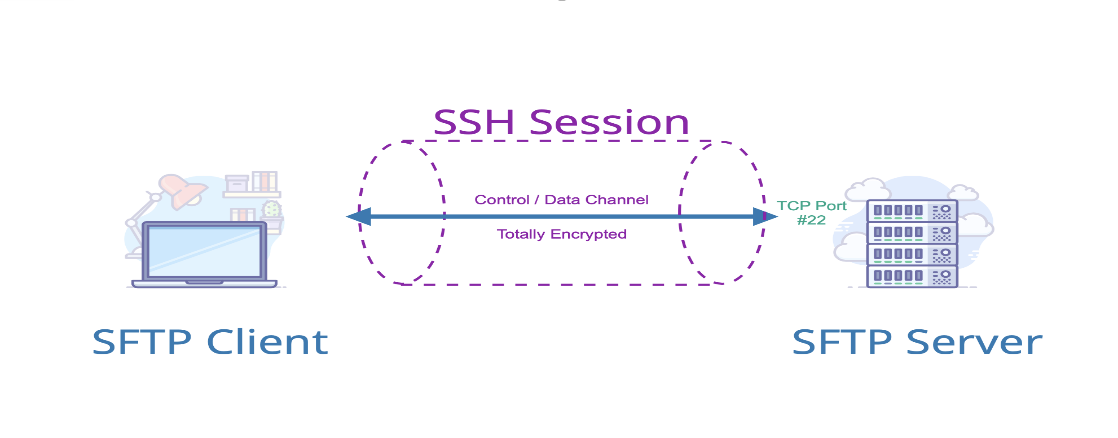
FTP is a protocol for transferring data between a computer and remote computer or server over an Internet connection. Simply FTP facilitates data transfer through a client server relationship, allowing you to manage and transfer files from one system to another.

Now let’s take a look at SFTP and find out how it can help your business with critical file transfers.

SFTP stands for SSH file transfer protocol. While SFTP is a secure protocol for transferring files, the **s** stands for **ssh** or **secure shell**.

**SFTP is a Separate Protocol**

SFTP still uses a client and server connection to facilitate file transfer, but SFTP is a separate protocol. Unlike FTP, ***SFTP file transfers*** are ***done over*** the ***control channel***. There is no need to open a separate data channel to complete you file transfer.



**SFTP** requires **authentication** by the **server** you’re **connecting** to and **runs** ***over an SSH session*** on **TCP port 22**. **SSH** or the **secure shell** acts as a ***privacy layer*** for your **connection**, establishing a secure channel between your local computer and a remote computer or server. This helps ensure that important information like **usernames, passwords**, and **personal data** aren’t sniffed by someone maliciously. Additionally, ***encryption*** helps ensure your **data isn’t visible in plain text** as it **transfers over the Internet**. With **SFTP both commands** and **data** are **encrypted**.

**SFTP in the Real World**

**SFTP** is pretty much the standard for the purpose of **secure data transfer**. Like FTP there are a lot of uses for SFTP, which makes sense since SFTP can be used by any industry for any file type. Businesses that need to protect sensitive information, love SFTP. So much so that many companies submit their payroll to ADP using SFTP.

Be it customer data, accounting and financial information, files that reveal internal operations, or agreements with contractors and government agencies. SFTP ensures secure and efficient file transmission, all without sacrificing security or compliance.

A likely candidate for SFTP is a legal firm the needs to keep tight control on its record and access to copies of files for courts, local governments, the federal government, and of course the IRS. IT professionals love SFTP because it helps keep restricted access to their overall systems and reduces risk. And movie production companies use SFTP to securely distribute digital movies to theaters, thus enabling moviegoers like yourself to enjoy the latest blockbuster on the big screen.

**Traditional SFTP on Cloud:**

In today’s world of technology, cloud computing is everywhere. Vendors such as Google and Microsoft are releasing products that have features & capabilities to enable businesses to become more lean, efficient & flexible. With these benefits on offer, almost every business out there is aiming to move to the cloud, to be more competitive.

However, migration from traditional tech stacks to the cloud comes with its own baggage, which we need to let go of. This white paper scrutinizes one such traditional technology — the File Transfer Protocol (FTP) and the Secured File Transfer Protocol (SFTP).

**FTP & SFTP**

The FTP, with its roots from the early ’70s, is a standard network protocol used to transfer files from client machines to the server and vice-versa. This was later secured by SSL thereby creating SFTP. For the remainder of this paper, reference shall be made only to SFTP as FTP fails to be an option considering security aspects.

Architecturally, **SFTP requires** that a **server be always available**, **storage space be pre-allocated** & **a stateful connection be maintained during a session**. It also has limited capabilities for DR situations and back-ups. When it comes to cloud computing, these fundamentals themselves are a misfit.

**THE CLOUD:**

**Resilience**

It is known that systems are bound to fail due to technical glitches, physical interruptions or natural calamities. Cloud computing provides us various levels of fault tolerance — regions, availability zones, availability sets etc depending on the provider.

Having a traditional SFTP on the cloud machine forces one to be on a single virtual machine only, thus, extricating the possibilities for disaster recovery. With data being valued even more than money, a data loss could be catastrophic for a business.

**Serverless Computing**

Cloud computing provides us with the facility of ‘pay per execution’. This refers to a payment model, where a customer is charged only when a piece of code (or function) executes. This is done, by provisioning the necessary computes and resources at run time, post which the resources are returned back to the pool.

An analysis of the resource usage graph of a traditional SFTP server will show that resources are used sporadically (during file transfers), lying idle for the rest of the duration, thus theoretically fitting the serverless concept, but not practically. This is because, an SFTP server (as mentioned earlier), by design, needs an always-up state. Thus, raising the operational costs.

**Elasticity**

Elasticity is a key feature when it comes to handling increased loads on a cloud environment especially for specific and (usually) short periods of time. This allows applications to perform with reasonable health even when there is a spike in the load.

With traditional SFTP servers on the cloud, such an elastic expansion is not possible. Though not a common scenario, when there is a peak in load, the performance of the server would purely depend on available resources only.

**Cost**

Cost is one of the biggest drivers for businesses to adopt cloud computing and storage space is a direct contributor to cost. For a traditional SFTP, dedicated storage space is needed. The approximate cost of minimal storage space is 150$/month (approx) as compared to a blob storage cost of around 22$/month (approx), thus, approximately 10 times more. [Costs from <https://azure.microsoft.com/en-in/pricing/calculator/>]

In addition, a back-up logic will need to be incorporated by the application team along with back-up storage. This will further shoot cost much higher compared to various back-up options provided by Azure storage at a nominal cost.

Thus it is evident that usage of a storage account is much more economical as compared to traditional disk storage when it comes to the cloud for file storage and access. This is in spite, charges being applied every time file storage is accessed.

**Maintenance**

One of the key benefits that cloud computing gives businesses, is that their application teams can focus on the core logic and not on the infrastructure, runtime etc. These ‘managed’ offerings improve not only TTM but also abstracts risks.

A traditional SFTP on cloud machine would force us to dive right back into the maintenance of the SFTP server, SSH keys, connections etc. It will also be among the application teams' responsibilities to maintain access controls, troubleshoot issues etc.

**Conclusion**

The sections so far highlight that a traditional SFTP is not an ideal fit for the cloud. In fact, most of the benefits and value add provided by the cloud computing environment are nullified with a traditional SFTP.

As there still exist requirements where files are needed to be transferred in a client-server environment, cloud vendors have launched managed offerings such as Azure SFTP Gateway. These offerings capture the essence of FTP while taking advantage of the benefits cloud computing offers.

As highlighted earlier, file transfer only requires sporadic use of resources. It thus becomes a prime use case for container-based SFTP servers (ACI based solution) that can be commissioned and destroyed on demand.

As of the date of publishing of this paper, Strati does not support any SFTP options on cloud and recommends to redesign applications to be cloud-native. In the long run, the economic and operational benefits and mitigated risks will outweigh the costs involved for revamping legacy solutions.