HTTPS vs. SFTP: What’s the Technical Difference?

During the data transmission process on the Internet, what matters the most is the application of secure file transfer methods, as they might involve the transmission of confidential and sensitive data.

Nobody wants their data to be tampered with during the transfer process. This is where secure file transfer comes in! It is the process of transferring files over a network in a secure manner, typically using encryption to protect the data being transferred.

There are several versions of secure file transfer, including

FTP (File Transfer Protocol)

FTP Secure (FTPS)

Secure FTP (SFTP)

HTTPS ((Hypertext Transfer Protocol Secure)

FTP (File Transfer Protocol) is the original file transfer protocol widely used to transfer files between computers. FTP uses separate control and data connections and can operate in active or passive mode.

FTPS (FTP Secure) is a secure version of FTP that uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt the data being transferred. FTPS uses separate control and data connections and can operate in active or passive mode.

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol used to transfer data on the Internet. HTTPS uses SSL or TLS to encrypt the transferred data, making it secure against eavesdropping and tampering.

SFTP (SSH File Transfer Protocol) is a secure version of FTP that uses the Secure Shell (SSH) protocol to transfer files. SFTP uses a single connection for control and data transfer, making it more secure and efficient than FTP.

However, we will talk about HTTPS vs. SFTP here. Though there are two methods of secure file transfer, certain technicalities are involved that separate them. But before we decode the difference, let us understand both individually.

What Is HTTPS?

Hypertext Transfer Protocol Secure (HTTPS) is a secure version of the HTTP protocol used to transfer data on the Internet. HTTPS protects the privacy and integrity of the data transferred between a web server and a client, such as a web browser.

When you visit a website using HTTPS, your web browser establishes a secure connection to the web server using a combination of the SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocol and a digital certificate.

Also Read: Differences Between HTTP and HTTPS

SSL and TLS are cryptographic protocols that provide secure communication over a computer network. The digital certificate, issued by a trusted certificate authority (CA), verifies the web server's identity and ensures the connection is secure.

Once the secure connection is established, all data transferred between the web server and the client is encrypted, making it more difficult for anyone to intercept or tamper with the data. This is especially important for websites that handle sensitive information, such as online banking or shopping sites, where the security of the data being transferred is critical.

To identify a website using HTTPS, the URL of the website typically begins with 'https://' instead of 'http://.' Additionally, most web browsers display a padlock icon in the address bar to indicate that the connection is secure.

It's important to use HTTPS when transferring sensitive or confidential data over the Internet to protect it from being intercepted or tampered with.

Benefits of HTTPS:

Encryption Layer enabled

Data Protection

Ranking Boost with Google

Protection against Phishing

Leveraged to gain Customer Trust

Payment Card Industry Compliance

Understood HTTPS? Let us try understanding SFTP now.

What is SFTP?

Secure File Transfer Protocol (SFTP) is a secure version of the File Transfer Protocol (FTP) used to transfer files over a network. SFTP is based on the Secure Shell (SSH) protocol, which provides a secure way to transfer data between two computers.

SFTP uses a single connection for control and data transfer, making it more efficient and secure than FTP, which uses separate connections for control and data transfer. In addition, it uses encryption to secure the transferred data, making it more difficult for anyone to intercept or tamper with it.

To use SFTP, you need an SFTP client program, such as FileZilla or WinSCP, and access to an SFTP server. The SFTP client establishes a secure connection to the SFTP server using a combination of the SSH protocol and authentication methods, such as password authentication or public key authentication.

Once the connection is established, you can use the SFTP client to transfer files between your computer and the SFTP server or between two SFTP servers.

Benefits of SFTP:

Accessibility

Data Security

Convenient File Management

Scalability

Disaster Recovery and Compliance

Now that we have a fair idea of HTTPS and SFTP, let us compare them and understand their technical differences.

What is the Difference Between HTTPS and SFTP?

Both HTTPS and SFTP are secure protocols that are used to transmit sensitive data over the Internet. However, there are a few differences between them.

HTTPS vs. SFTP Security

These are some of the key differences between the two protocols in terms of security:

Encryption Methods: HTTPS uses a Secure Socket Layer (SSL) or Transport Layer Security (TLS) to encrypt the transmitted data. SFTP uses public and symmetric encryption to secure the transmitted data.

Key Exchange: In HTTPS, the client and the server use a shared key to encrypt and decrypt the transmitted data.

However, in SFTP, the server and client exchange keys with the help of public key encryption. This means the client's public key is used to encrypt the data, and the server's private key is used to decrypt it.

Certificate validation: HTTPS uses digital certificates to verify the server's identity. So the client checks the certificate to ensure it is legit and issued by a repeated Certificate Authority.

Contrary to HTTPS, SFTP does not use certificates for authentication. It, however, depends on the server's host key, a unique identifier stored on the client's machine.

Overall, both HTTPS and SFTP are security protocols that can transmit sensitive data over the Internet. However, SFTP is generally considered more secure due to public and symmetric key encryption and unique host keys for authentication.

HTTPS vs. SFTP Ease of Use

When it comes to the convenience of application, these are some key differences between HTTPS and SFTP:

Protocol: HTTPS is a protocol for transmitting data over the Internet, whereas SFTP is a protocol for transferring files over a secure SSH connection. This means HTTPS usually transmits data via a web browser, while SFTP transfers files.

Accessibility: HTTPS is widely supported by web browsers and servers, so it is relatively easy to use.

SFTP requires using a separate client program, such as an SFTP client or a terminal with an SFTP command-line utility. This makes it more challenging for users who are not familiar with command-line tools to use.

Configuration: HTTPS typically requires minimal configuration. Web servers are usually configured to support HTTPS by default, and web browsers will automatically use HTTPS if available.

On the other hand, SFTP requires installing and configuring an SFTP client or server. This can be more time-consuming and may require some technical knowledge..

Overall, HTTPS is generally easier to use than SFTP, as it is widely supported and requires minimal configuration. However, SFTP is a powerful tool for securely transferring files; with the right client software, it can be relatively easy to use.

SFTP vs. HTTPS File Transfer Speed

The speed of file transfer using SFTP and HTTPS depends on various factors like the size of the file being transferred, the performance of the server and client machines, and the bandwidth of the Internet connection.

Typically, SFTP is faster than HTTPS for transferring larger files as it is typically designed for transferring files and can make more efficient use of bandwidth.

However, HTTPS can also be fast, especially using a modern version of TLS with efficient cipher suites. In addition, factors like network congestion and the distance between the client and server can also affect the speed of file transfer using HTTPS or SFTP.

Overall, the speed of file transfer using SFTP and HTTPS will vary based on various factors. For example, though SFTP may be faster for transferring files, HTTPS can also be faster, given the modern encryption methods.

These are a few parameters based on which HTTPS vs. SFTP can be compared. For a better understanding, we have made a table for you.

Difference: HTTPS and SFTP

Parameters HTTPS (Hypertext Transfer Protocol Secure) SFTP (Secure File Transfer Protocol)

Encryption Methods SFTP is a protocol used to transfer files over a secure SSH connection. HTTPS encrypt the transmitted data using a Secure Socket Layer (SSL) or Transport Layer Security (TLS).

Key Exchange The client and the server use a shared key to encrypt and decrypt the transmitted data. The server and client exchange keys with the help of public key encryption.

Certificate Validation HTTPS uses digital certificates to verify the server's identity SFTP depends on the server's host key, a unique identifier stored on the client's machine.

Protocol HTTPS is a protocol for transmitting data over the Internet. Web browsers and servers widely support HTTPS, so it is relatively easy to use.

Accessibility HTTPS is widely supported by web browsers and servers, so it is relatively easy to use. SFTP requires using a separate client program, such as an SFTP client or a terminal with an SFTP command-line utility, so it can be a bit tough to use.

Configuration Web servers are usually configured to support HTTPS by default, and web browsers will automatically use HTTPS if available. SFTP requires installing and configuring an SFTP client or server. This can be more time-consuming and may require some technical knowledge.

Achieve the Best End-to-End File Transfer Security!

Using secure file transfer protocols like HTTPS and SFTP is important in protecting the confidentiality of data being transferred. Still, it is not sufficient on its own to ensure the security of the data. You have to implement encryption, multi-factor authentication, and other measures.