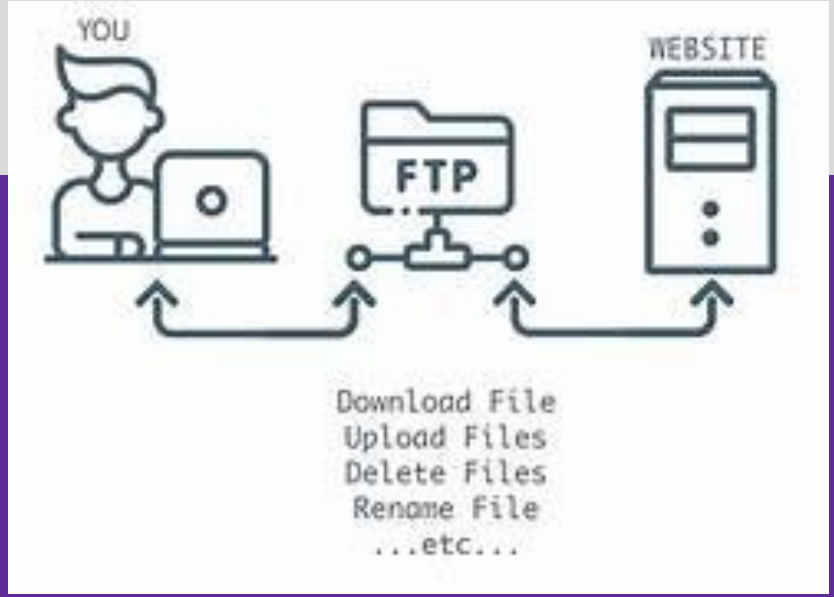
FTP

File Transfer Protocol

Protocolo de transferencia de archivos

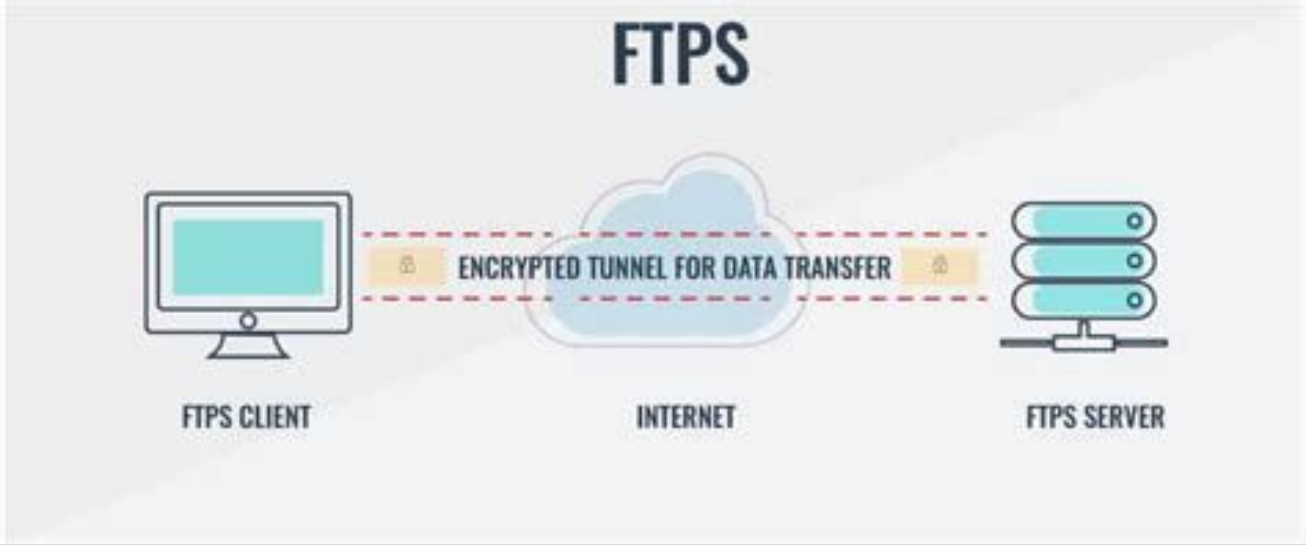


Tipos de transferencia de archivos.

1. Transferencia de archivos (sin seguridad):
    - ❑ Protocolo FTP
    - ❑ Protocolo TFTP
2. **Transferencia de archivos segura:**
    - ❑ **Protocolo FTPS**
    - ❑ **Protocolo SFTP**

2. Transferencia de archivos segura

2. Transferencia de archivos segura.
Protocolo FTPS (FTP TLS/SSL)



2. Transferencia de archivos segura.

Diferencias entre FTPS (FTP TLS/SSL) y FTP

➢ El mayor problema que tiene la transmisión de archivos a través de FTP es que este protocolo está creado pensando en la rapidez y no en la seguridad. El intercambio de información se realiza sin ningún tipo de cifrado, con lo que las transferencias no son seguras y un posible atacante puede acceder al servidor y apropiarse de los archivos transferidos.

➢ Este problema se puede evitar utilizando FTPS , que está basado en el protocolo FTP estándar, pero sobre SSL (protocolo TLS), de esta manera la información ya va cifrada.

➢ FTPS usa dos conexiones, un canal de comando y un canal de datos. Se pueden encriptar ambos, o solo el canal de datos.

2. Transferencia de archivos segura.

Diferencias entre FTPS (FTP TLS/SSL) y FTP

2. Transferencia de archivos segura.

Protocolo FTPS (FTP TLS/SSL)

➢ El protocolo FTPS (FTP sobre TLS o SSL), agrega la capa de encriptación justo debajo de la capa de aplicación. Se construye un canal encriptado tanto para la conexión de control como de datos. Se rige por el RFC 4217.

➢ SSL: Secure Sockets Layer y TLS: Transport Layer Security son protocolos de cifrado para dar seguridad y privacidad a las comunicaciones por Internet (correo electrónico, navegación web y FTP entre otras).

➢ Se utiliza cuando se necesite una transferencia segura de datos confidenciales o de carácter crítico entre un cliente y un servidor configurado para usar SSL (certificados SSL).

2. Transferencia de archivos segura.

Protocolo FTPS (FTP TLS/SSL)

➢ ¿Cómo funciona?

1.- Autenticación del servidor ante el cliente.

2.- Cliente y servidor seleccionan los códigos de cifrado compatibles.

3.- Autenticación del servidor ante el cliente (opcional).

4.- Utilización de cifrado de clave pública para compartir información de forma secreta

➢ Con el programa cliente FTP Filezilla puedes establecer conexiones FTPS si el servidor te lo permite.

2. Transferencia de archivos segura.

Protocolo FTPS (FTP TLS/SSL)

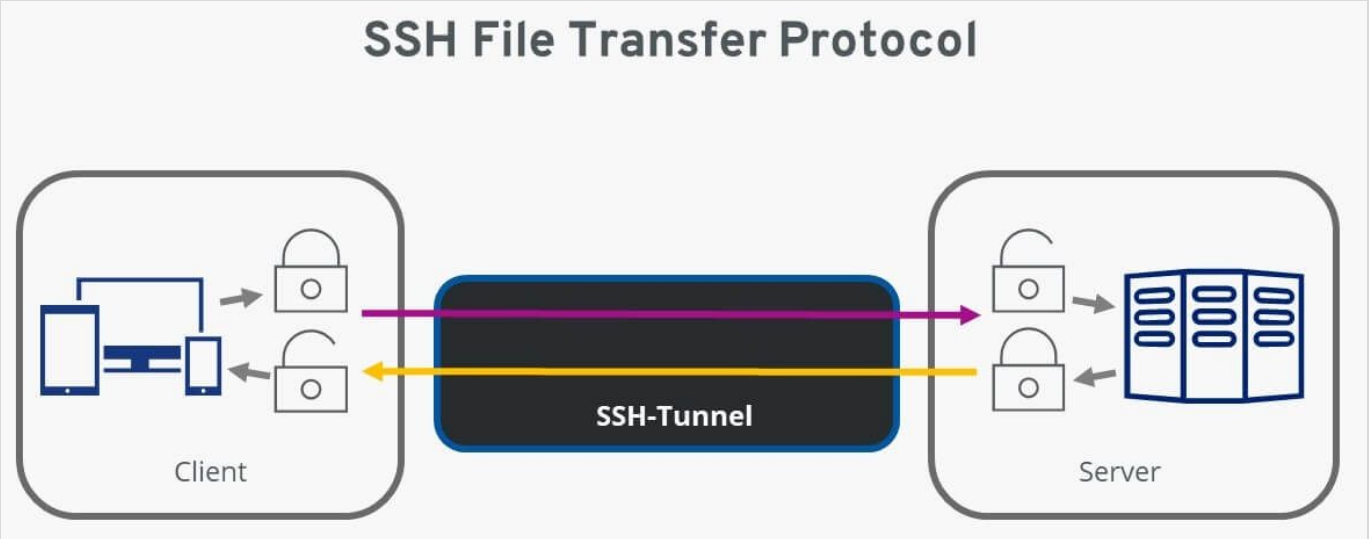
Existen dos diferentes métodos para realizar una conexión **SSL/TLS** a través de **FTP**:

1. La primera y más antigua es a través de **FTPS Implícito** (*Implicit FTPS*), que consiste en cifrar la sesión completa a través de los puertos 990 (FTPS) y 998 (FTPS Data), sin permitir negociación con el cliente, el cual está obligado a conectarse directamente al servidor FTPS con el inicio de sesión **SSL/TLS**.

2. El segundo método, que es el recomendado por el RFC 4217 y el utilizado por **vsftpd**, es **FTPS Explícito** (*Explicit FTPS* o **FTPES**), donde el cliente realiza la conexión normal a través del puerto 21 y permitiendo negociar, de manera opcional, una conexión **TLS**.

2. Transferencia de archivos segura

2. Transferencia de archivos segura.
Protocolo SFTP



2. Transferencia de archivos segura.

Protocolo SFTP

El protocolo SFTP (FTP sobre SSH). Primero se establece una conexión SSH entre el cliente y el servidor, luego se realiza el intercambio de información por FTP. También construye un canal encriptado. Utiliza el puerto 22.

- ➢ SSH File Transfer Protocol, también conocido como transferencia de ficheros SSH. SFTP está basado en SSH por completo.

- ➢SFTP es un protocolo para la transferencia segura de archivos entre cliente y servidor basado en el protocolo SSH. Este protocolo nos permite autenticarnos y realizar la transmisión de datos entre equipos utilizando criptografía del protocolo SSH.

2. Transferencia de archivos segura.

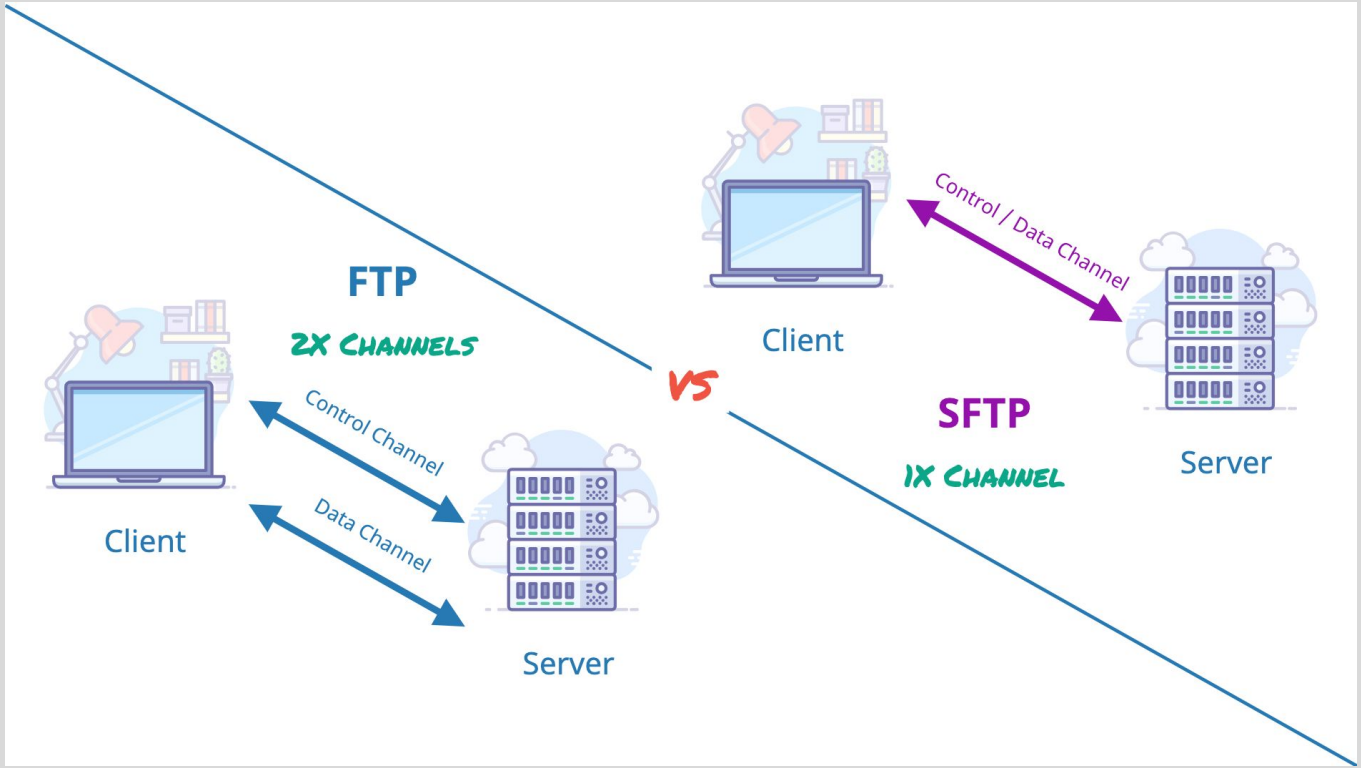
Protocolo SFTP

➢¿Cómo funciona?

SFTP proporciona dos métodos para autenticar conexiones.

1. Se puede utilizar simplemente un ID de usuario o contraseña como en FTP, con la ventaja de que en SFTP estas credenciales están encriptadas.
2. El otro método es el uso de claves SSH, una clave privada, una clave pública y el correspondiente intercambio de claves.

2. Transferencia de archivos segura.
Protocolo SFTP



2. Transferencia de archivos segura.

Diferencias entre FTPS y SFTP

FTP

FTP classic

- Plain FTP
- Clear-text password sent over the network
- Typically runs over TCP port 21
- Defined by RFC 959 and 1123

FTP/SSL

FTP over TLS/SSL

- Often called 'FTPS'
- Often called 'Secure FTP'
- Plain FTP over TLS/SSL channel
- Password is encrypted
- Transfer is encrypted
- Typically runs over TCP port 21 or 990
- Defined by RFC 959, 1123, 4217 and 2228

SFTP

SSH File Transfer Protocol

- SSH File Transfer Protocol
- Has nothing common with original FTP
- Often called 'Secure FTP'
- Password is encrypted
- Transfer is encrypted
- Typically runs over TCP port 22
- RFC not yet finished

2. Transferencia de archivos segura.

Diferencias entre FTPS y SFTP

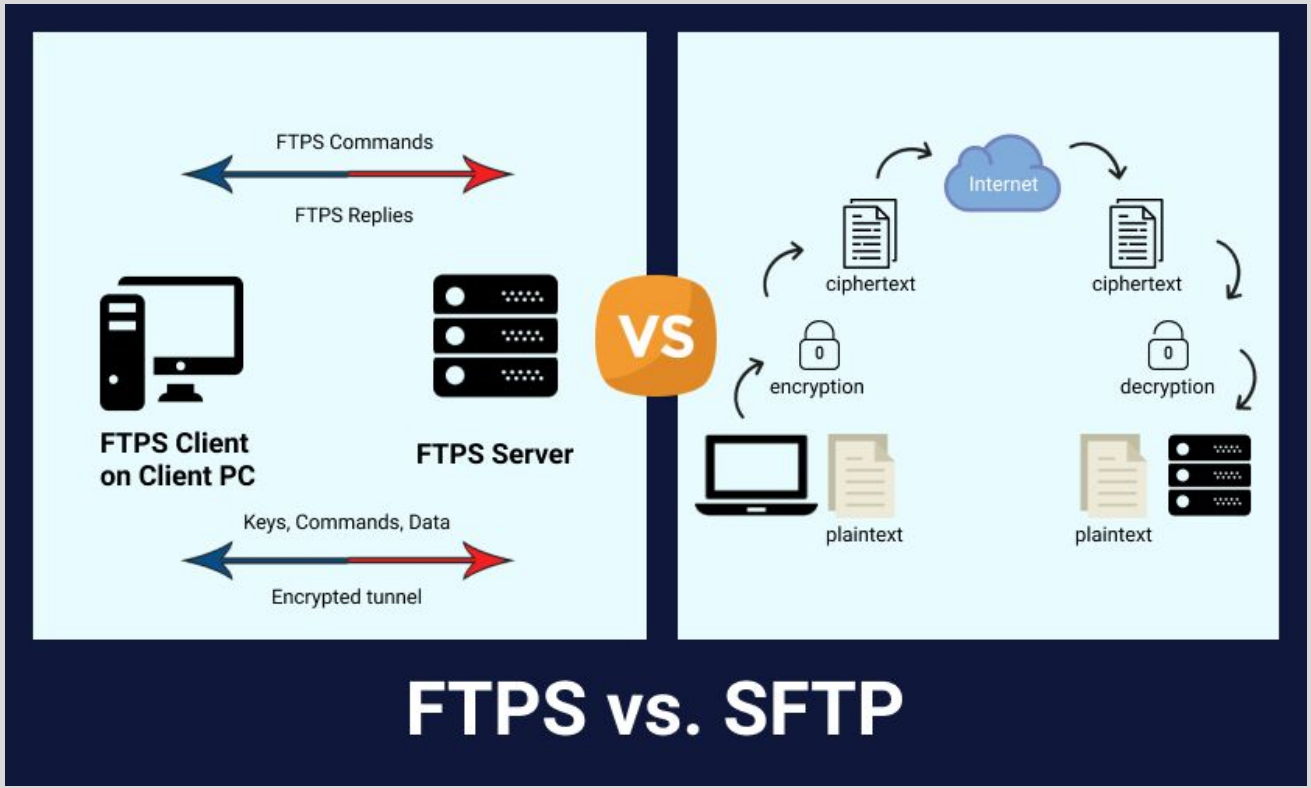
➢ FTPS está basado en FTP y podríamos considerar FTPS como la versión segura de FTP ya que permite el cifrado.

➢ SFTP está basado en SSH por completo y utiliza la criptografía del protocolo SSH.

➢ Tanto FTPS como SFTP ofrecen una fuerte protección a través de opciones de autenticación que FTP no puede proporcionar.

2. Transferencia de archivos segura.

Diferencias entre FTPS y SFTP



2. Transferencia de archivos segura.

Diferencias entre FTPS y SFTP

Entonces, ¿por qué elegir una sobre la otra?

- FTPS utiliza múltiples números de puerto. El primer puerto se usa para la autenticación y comandos de paso. Pero cada vez que se realiza una solicitud de transferencia de archivo o de listado de directorio, se necesita abrir otro número de puerto para el canal de datos.
- SFTP necesita un único número de puerto para todas las comunicaciones SFTP y cuantos menos puertos tenga abiertos nuestro firewall, menos peligro por lo que usar SFTP para el intercambio de datos puede ser una buena idea.

2. Transferencia de archivos segura.

Diferencias entre FTPS y SFTP