

FTPS, subir archivos de forma segura



Todo el mundo que tenga una **página web** de su propiedad, habrá escuchado hablar alguna vez del protocolo FTP. Se trata del mecanismo utilizado para subir los archivos de la web hasta el **servidor** donde tengamos alojado nuestro portal. Aunque es el mecanismo más utilizado a la hora de publicar un sitio, si no tomamos medidas de seguridad suficientes, puede convertirse en un método inseguro, siendo el blanco de ataques por medio de hackers, que buscan esas claves para insertar su código malicioso en los portales, desde donde llevar a cabo sus fechorías.

Para que la transmisión de los archivos que forman parte de un portal se hagan de forma más segura, se puede utilizar una variante del protocolo FTP conocido con el nombre de FTPS, que será el tema que abordaremos a lo largo de este White Paper.

¿Por qué el protocolo FTP es inseguro?

El protocolo de transferencia de archivos (FTP) es uno de los más viejos y populares que nos podemos encontrar hoy en día relacionados con el mundo de Internet. Como hemos explicado, su principal objetivo es el permitir la transferencia de archivos entre máquinas sin que el usuario tenga que iniciar una sesión en el host remoto, permitiendo la gestión de los archivos localizados en esa máquina remota mediante el uso de comandos muy simples.

Para conseguir esta transferencia de archivos el protocolo FTP hace uso del protocolo de red TCP para ello. Debido a que se trata de uno de los protocolos más antiguos tiene la desventaja de que no utiliza una autenticación de usuario y contraseña cifrada. Debido a esto, es considerado un protocolo inseguro. De ahí que sea muy recomendable cambiar tanto usuario como contraseña de forma habitual, para evitar que sea captada por personas ajenas a nuestro sitio y las puedan utilizar para llevar a cabo acciones ilícitas.

¿Qué es el protocolo FTPS?

El protocolo FTPS se podría definir como una extensión del protocolo FTP pero con la diferencia de que utiliza un **certificado SSL** para asegurar los comandos y los datos transferidos entre el cliente y el servidor. Para mejorar la seguridad, FTPS hace uso de capa SSL/TLS, protocolos de cifrado que proveen seguridad para las comunicaciones por la red.



Es similar al uso de certificados de seguridad SSL para los sitios web, que hacen que la información que circula por el portal vaya cifrada, y que en caso de que sea interceptada por algún atacante, no pueda acceder a ella a no ser que conozca la clave de descifrado.

Además del protocolo FTPS, también nos podemos encontrar otra opción a la hora de intercambiar archivos, que se conoce con el nombre de SFTP pero que son totalmente diferentes. La principal diferencia radica en que este último caso, utiliza el **protocolo SSH** para realizar la transferencia de archivos de forma segura. SSH es un protocolo muy seguro que es el utilizado para conectarse a servidores de forma remota para trabajar en ellos como si estuviéramos delante

Ventajas y desventajas del protocolo FTPS

Ya hemos dicho que su principal ventaja es la de ofrecer una conexión segura entre un equipo y una **máquina remota**. Pero además de esto nos podemos encontrar otra serie de ventajas:

- Se trata de un método muy utilizado y conocido por la gran mayoría de usuarios que trabajan con Internet de forma habitual.
- Al ser una variante de FTP, los comandos utilizados son los mismos que en este caso.
- Permite el intercambio de archivos entre servidor – servidor sin la necesidad de utilizar un cliente para ello.
- SSL y TLS ofrecen algoritmos de autenticación seguros.

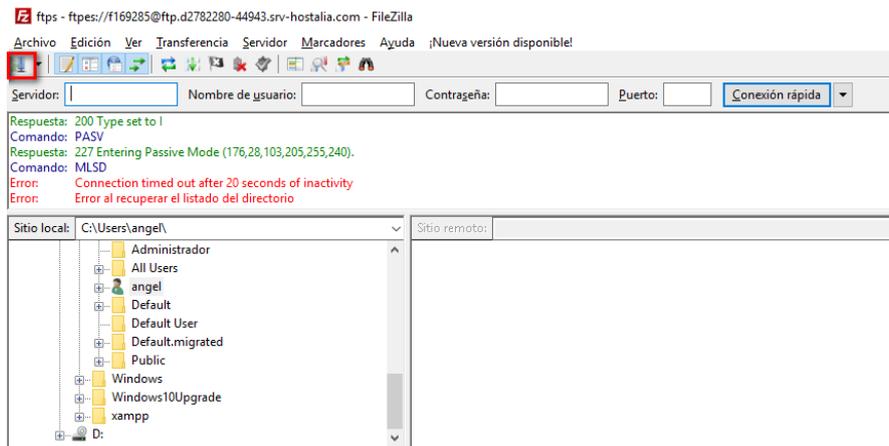
Pero no todo son ventajas, sino que el protocolo FTPS también ofrece algunas desventajas que es interesante que conozcamos:

- Podemos encontrarnos algunos problemas a la hora de listar los directorios que hay en el sitio remoto, aunque no suele ser muy habitual.
- Requiere de un canal secundario de comunicación, lo que puede causar problemas con los cortafuegos.
- No dispone de estándares de codificación de caracteres.
- No todas las conexiones SSL son compatibles con FTP y TLS.

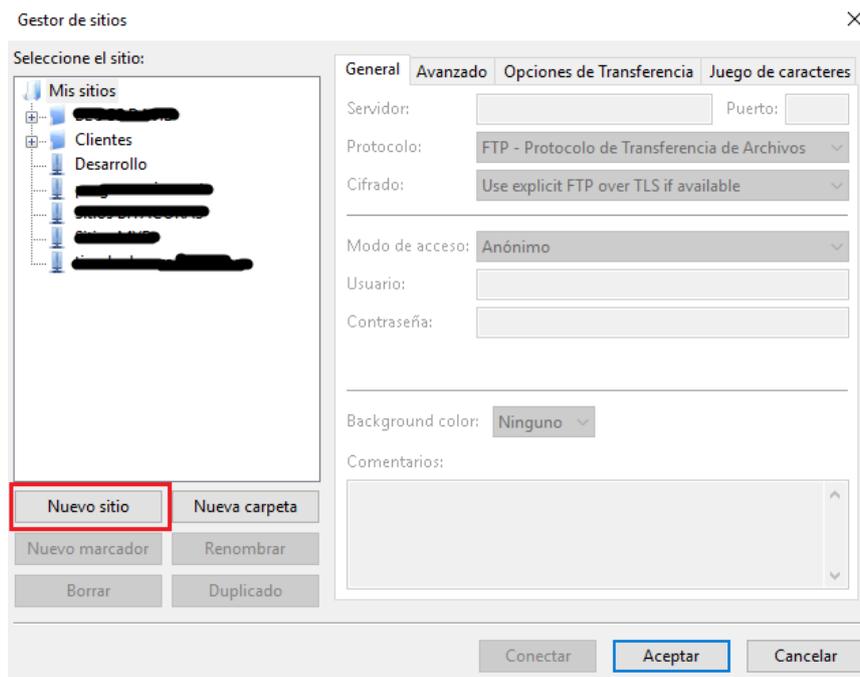
Conectarse mediante FTPS utilizando Filezilla

Una vez que conocemos de qué se trata el protocolo FTPS, es hora de conocer cómo podemos hacer uso de este protocolo utilizando para ello el programa Filezilla.

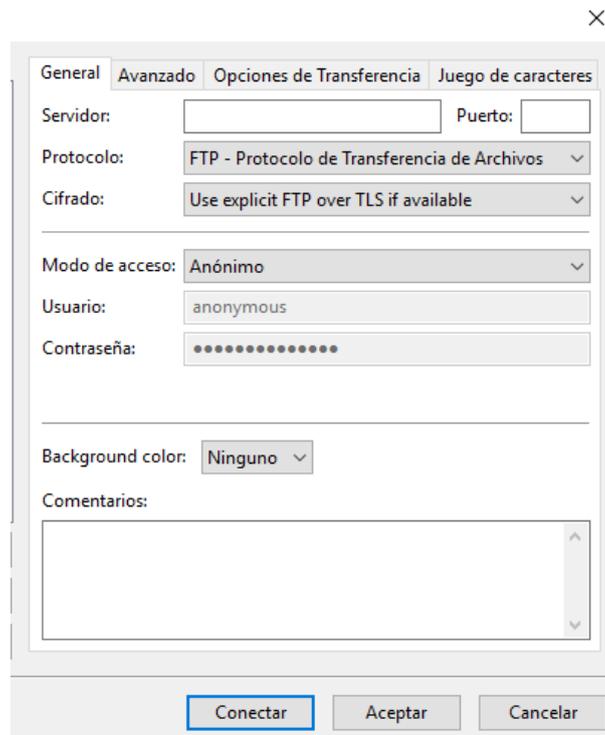
Lo primero que deberemos hacer es instalar este programa y arrancarlo. Cuando lo hayamos hecho, deberemos pulsar sobre el icono de gestión de sitio que se encuentra en la esquina superior izquierda.



En la ventana que se nos abrirá, pulsaremos sobre el botón de “Nuevo sitio”.



Cuando pulsemos ese botón, se nos ofrecerá la oportunidad de realizar una nueva conexión, cumplimentando los siguientes datos que aparecen en la imagen siguiente.



The image shows a screenshot of a software dialog box with a close button (X) in the top right corner. The dialog has four tabs: 'General', 'Avanzado', 'Opciones de Transferencia', and 'Juego de caracteres'. The 'Avanzado' tab is selected. It contains the following fields and controls:

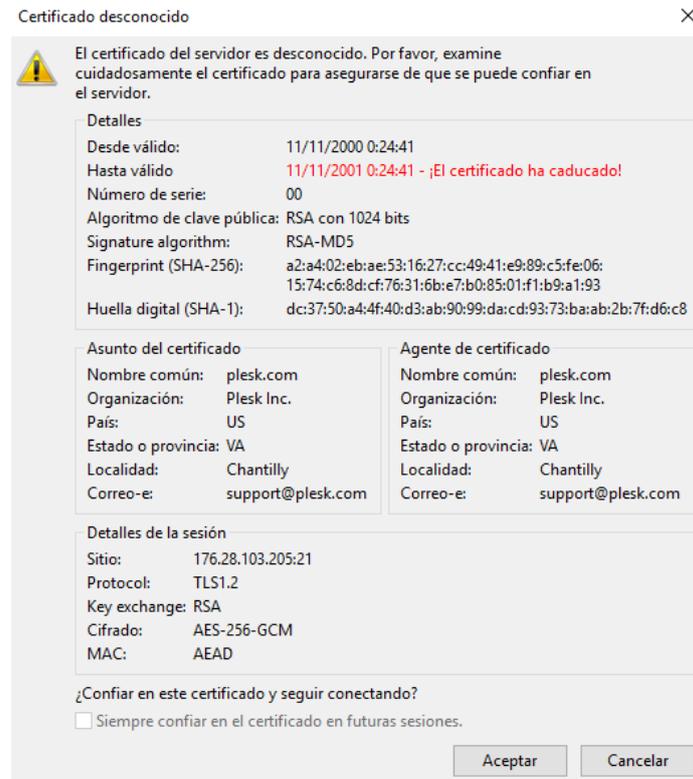
- Servidor:** A text input field.
- Puerto:** A text input field.
- Protocolo:** A dropdown menu with 'FTP - Protocolo de Transferencia de Archivos' selected.
- Cifrado:** A dropdown menu with 'Use explicit FTP over TLS if available' selected.
- Modo de acceso:** A dropdown menu with 'Anónimo' selected.
- Usuario:** A text input field containing 'anonymous'.
- Contraseña:** A password input field with 10 dots.
- Background color:** A dropdown menu with 'Ninguno' selected.
- Comentarios:** A large text area with a vertical scrollbar.

At the bottom of the dialog are three buttons: 'Conectar' (highlighted with a blue border), 'Aceptar', and 'Cancelar'.

Los datos que debemos rellenar son los siguientes:

- **Servidor:** En este campo indicaremos la **dirección IP** o nombre del servidor al que nos queremos conectar.
- **Puerto:** Valor del puerto al que nos conectaremos. Si no se ha cambiado, el puerto será el de por defecto, es decir, el puerto 21.
- **Tipo de servidor:** En este menú desplegable, deberemos seleccionar la opción **“Requiere FTP explícito sobre TSL”**.
- **Modo de acceso:** Otro menú desplegable en el que elegiremos la opción **“Normal”**. De esta forma tendremos que indicar un nombre de usuario y contraseña para llevar a cabo la conexión.
- **Usuario:** Consiste en el usuario asignado a tu plan de alojamiento.
- **Contraseña:** La contraseña que lleva asociada el usuario de nuestra cuenta.

Una vez que hemos rellenado correctamente todo los datos, pulsaremos el botón conectar. En ese momento nos aparecerá en pantalla información sobre el certificado de seguridad que deberás aceptar para que se complete la conexión.



Una vez completado este paso, ya estaremos conectados mediante el protocolo FTPS y podremos intercambiar archivos de forma más segura.

Aunque hayamos comentado que el protocolo FTP es considerado un protocolo poco seguro, eso no significa que no se pueda utilizar con total garantía. Lo único que debemos hacer es que en caso de tener sospechas de que nuestras claves hayan podido caer en manos de terceras personas, entrar en nuestro panel de control de nuestro alojamiento web y cambiarlas por otras nuevas.