Protocolo seguro de transferencia de archivos

El protocolo FTP de transferencia de archivos original, evolucionó en 1997 al protocolo FTPS para introducir seguridad en el envío.

El protocolo FTPS hace uso de SSL, TLS y es una combinación de algoritmos de cifrado asimétricos (RSA, DSA), algoritmos simétricos (DES/3DES, AES etc.) y un algoritmo de intercambio de claves con autenticación de certificados X.509.

Hay dos modos de trabajo con FTPS:

- El modo FTPS implícito SSL.

  Se requiere una sesión SSL entre el cliente y el servidor antes de que se intercambie cualquier dato. Como el nombre dice, el uso de SSL es implícito y cualquier intento de conexión de los clientes sin hacer uso de SSL es rechazado por el servidor. Los puertos de trabajo del FTPS implícito son el 990 y 989.

  Actualmente se utiliza muy poco FPS implícito a favor de hacer uso del segundo método FTPS explícito SSL.

- El modo FTPS explícito SSL.

  El cliente y el servidor negocian el nivel de protección que se utilizará. Esta situación es útil para poder trabajar con el mismo puerto con sesiones encriptadas o no encriptadas.

  En el modo explícito SSL el cliente inicia una conexión sin encriptar con el servidor FTP. El cliente pide una petición al servidor FTP para iniciar una orden sobre SSL, enviando las órdenes AUTH TLS o AUTH SSL.

  Una vez iniciado el canal SSL el cliente envía las credenciales al servidor FTP. Todas las credenciales son encriptadas y enviadas por el canal SSL. El canal de datos sigue el mismo procedimiento de protección que el canal de control. Los puertos que usa son el 20 y el 21, donde se efectúa el cifrado.

Hay otro tipo de servicio seguro con FTP llamado SFTP. SFTP está basado en SSH (secure shell), protocolo conocido para proveer seguridad a los terminales remotos. No hace uso de canales de órdenes y de datos. Los dos canales que usamos en FTPS se envían en paquetes con formato dentro de un mismo canal, es decir, el canal de datos y de órdenes es único.

Configuración del servidor proFTPd.

Se va a configurar el servidor proFTPd en modo seguro con certificado.

En primer lugar, editamos el fichero *proftpd.conf*

sudo nano /etc/proftpd/proftpd.conf

y, para poder usar conexiones FTPS, quitamos el comentario de la línea siguiente:

include /etc/proftpd/tls.conf

Ahora editamos el fichero *tls.conf*

sudo nano /etc/proftpd/tls.conf

y, para poder comprobar que funciona la seguridad en la conexión con el servidor FTP, quitamos el comentario de las líneas siguientes situadas dentro del bloque *<IfModule mod_tls.c>*

```
# Para utilizar el servicio FTPS
TLSEngine                   on
# Archivo de log
TLSLog                      /var/log/proftpd/tls.log
# Protocolo utilizado
TLSProtocol                 SSLv23

# Path de acceso a certificado y clave
TLSRSACertificateFile       /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile    /etc/ssl/private/proftpd.key


TLSOptions                  AllowClientRenegotiations
# No pedimos un certificado al cliente
TLSVerifyClient             off
# Obliga al cliente a realizar una conexión TLS
TLSRequired                 on
```

En el mismo fichero *tls.conf* añadimos

```
TLSOptions                  NoSessionReuseRequired
```

A continuación, generamos el certificado mediante el comando

sudo proftpd-gencert

Nos pedirá que introduzcamos la información que se utilizará en el certificado.

Una vez realizada la tarea anterior, fijamos los permisos correspondientes a los archivos de los certificados.

sudo chmod 600 /etc/ssl/private/proftpd.key

sudo chmod 644 /etc/ssl/certs/proftpd.crt

Reiniciamos el servidor para que surtan efecto los cambios

service proftpd restart

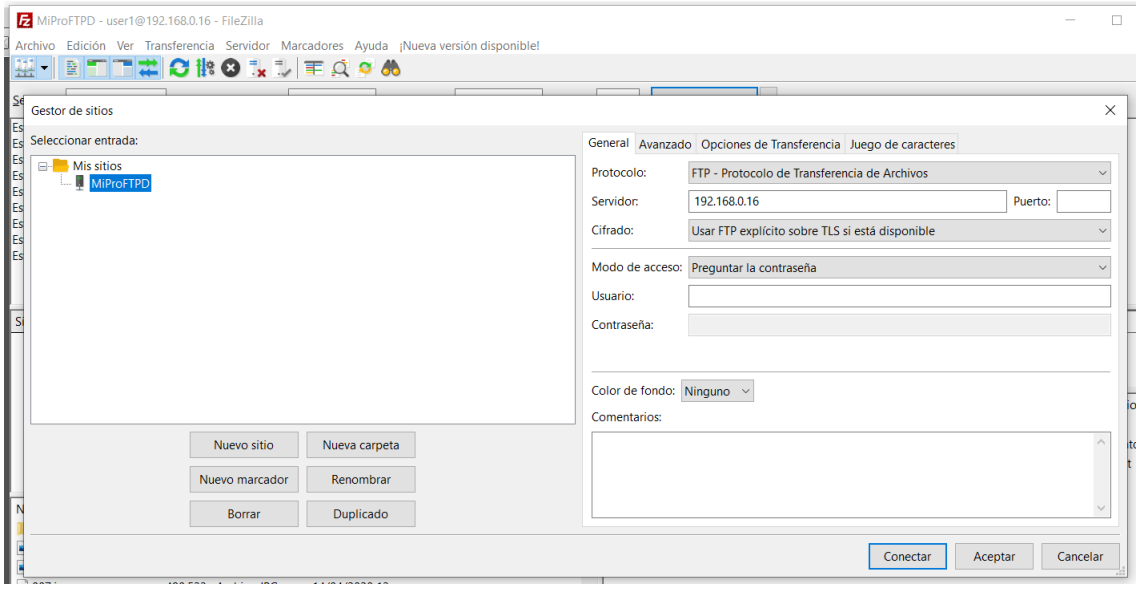
Conexión segura utilizando Filezilla

Vamos a configurar Filezilla para disponer de una conexión a nuestro servidor FTP, indicando además las características que deseamos utilizar en la conexión.

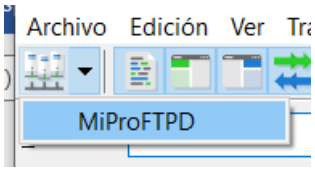
Pulsamos en el icono siguiente, situado bajo la opción de menú *Archivo*.

A continuación, aparecerá una ventana en la que definiremos las características de la conexión, de modo que podamos reutilizarla posteriormente:

Rellenamos las opciones según se indica a continuación. En la dirección del servidor debemos colocar la dirección IP a utilizar, o bien el nombre del servidor. En caso de que introduzcamos una dirección IP, hay que tener en cuenta, en posteriores accesos, si se trata de una IP estática o no.



Una vez configurada la conexión, pulsando en la flecha situada junto al icono utilizado anteriormente, aparece un desplegable con las conexiones que hemos definido.



Para establecer la conexión, nos pregunta si deseamos confiar en el certificado del servidor, aceptamos y finalmente se establecerá la conexión.

Conexión utilizando el explorador de archivos

Si queremos ser capaces de establecer la conexión mediante el explorador de archivos, hay que modificar el archivo *tls.conf* para que permita conexiones no seguras.

Para ello comentamos las líneas

TLSOptions NoSessionReuseRequired

TLSRequired on

y quitamos el comentario de la línea siguiente

TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired

Tras reiniciar el servidor de transferencia de archivos, podremos acceder al servidor utilizando tanto conexiones sin seguridad, como conexiones seguras.