UNIDAD I

Servicio de transferencia de archivos (DNS)

Servicios de red e internet

2º ASIR

CONTENIDOS

OBJETIVOS

Introducción

Funcionalidad del servicio FTP.

En un servicio de transferencia de archivos, el principal objetivo es transmitir archivos entre el equipo servidor y los equipos clientes. El servidor dispone de uno o varios directorios o carpetas donde los clientes pueden realizar (si tienen los permisos para ello) cualquiera acción básica sobre archivos y subdirectorios o subcarpetas. Entre esas acciones, un usuario podrá subir o cargar archivos desde su ordenador cliente al ordenador servidor y podrá bajar o descargar archivos desde el ordenador servidor al ordenador cliente.

El servicio de transferencia de archivos permitirá con total transparencia que en el cliente se pueda utilizar un sistema de archivos distinto al que se use en el servidor. Por ejemplo, el servidor podrá usar el sistema de archivos ext3 de Linux y el cliente el sistema NTFS de Windows y ello no tendrá ninguna influencia en la transferencia ni en como se tenga que trabajar en el cliente.

El protocolo estándar para el servicio de transferencia de archivos es FTP (File Transfer Protocol, traducido como Protocolo de Transferencia de Archivos). Las primeras pruebas del servicio FTP fueron llevadas a cabo en 1971 por el Instituto Tecnológico de Massachusetts. Sobre el protocolo se han ido sucesivas actualizaciones para mejorar su funcionalidad.

Por ejemplo, puede ser interesante instalar el servicio FTP sobre un equipo servidor web para que el administrador del sitio web pueda subir archivos al sitio web desde cualquier ordenador con posibilidad de conectarse a través de la red con el servidor.

Protocolo FTP.

El protocolo FTP es una de los primeros protocolos desarrollados para la arquitectura TCP/IP. Su primera versión, con un funcionamiento muy básico, se describe en el RFC 141. Desde esa primera implementación se han ido desarrollando sucesivas mejoras que se han ido recogiendo en sucesivos documentos RFC. La versión actual del protocolo se recoge en el RFC 959 de octubre de 1985.

FTP es un protocolo del nivel de aplicación. Permite establecer una conexión cliente/servidor para transferir archivos del servidor al cliente (descarga) o del cliente al servidor (subida). Las conexiones FTP se establecen sobre conexiones TCP de nivel de transporte.

Los objetivos principales del protocolo FTP se describen en la introducción del RFC 959 y son:

- Promover la compartición de archivos entre equipos.
- Animar al uso indirecto o implícito (a través de programas) de servidores remotos.
- Establecer transferencias de archivos que tengan total independencia de los sistemas de archivos usados en cliente y servidor.
- Transferir archivos de forma eficaz y fiable.

Protocolo FTP.

FTP permite varias operaciones sobre archivos remotos (ubicados en un servidor) subir archivos, bajar archivos, borrar archivos, crear carpetas. FTP permite que un usuario gestione o administre directamente las transferencias de archivos desde una terminal y mediante un conjunto de comandos FTP disponibles o que lo haga mediante cualquier otro programa (de interfaz gráfica o de texto) que implemente el protocolo.

El protocolo FTP no es un protocolo seguro ya que transmite la información en texto plano, tal como es codificada en origen. Aunque al realizar la conexión FTP, hay una autenticación de usuario, se transmiten el nombre y la contraseña sin encriptar. Una solución para tener conexiones FTP seguras es tunelizar las conexiones FTP sobre conexiones seguras bajo el protocolo SSH.

Una alternativa para transferencias de archivos seguras es el protocolo SFTP. Este protocolo, al igual que FTP permite realizar una serie de operaciones sobre archivos remotos.

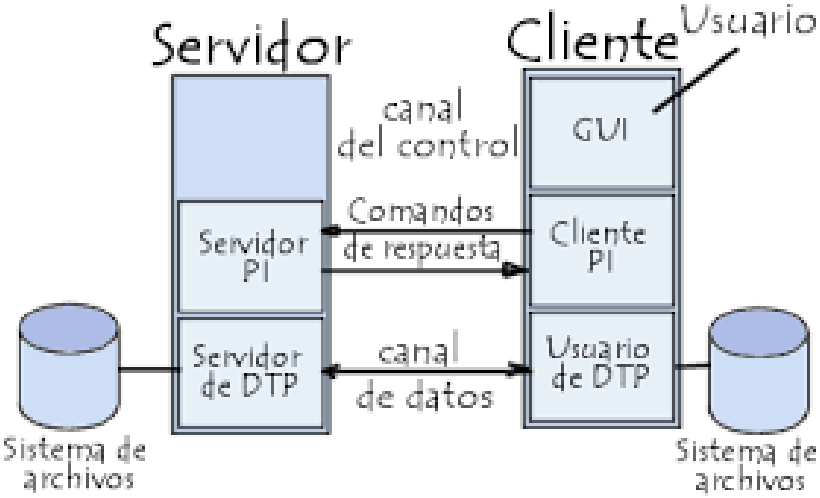
Funcionamiento.

FTP se basa en el modelo de conexión cliente/servidor. El servidor pone a disposición de los clientes uno o varios directorios en los que los usuarios pueden realizar acciones sobre sus archivos. Cuando un usuario inicia una conexión con un servidor FTP desde un cliente, es autenticado (se pide su nombre y contraseña). Cada usuario podrá acceder a los directorios en los que tenga permisos de acceso y podrá realizar en ellos las acciones para las que esté autorizado.

En las conexiones FTP, a los directorios que el servidor FTP pone a disposición de los clientes se les llama directorios remotos y a los archivos que hay dentro de ellos archivos remotos. A los directorios y archivos de equipos clientes usados en las transferencias los llamaremos directorios locales y archivos locales.

Una conexión FTP se desarrolla de la siguiente forma:

- Un usuario inicia un cliente FTP y solicita una conexión con un servidor identificándose.
- Si se establece conexión el cliente, a petición del usuario, va a enviar comandos u órdenes FTP al servidor solicitando realizar acciones.
- El servidor procesa los comandos, realiza las acciones solicitadas y envía respuestas FTP al cliente.



Funcionamiento.

Si la acción solicitada es una transferencia de un archivo, se inicia un proceso de transferencia de datos. No debes confundir una respuesta con una transferencia de datos. Por ejemplo, al solicitar la descarga de un archivo, la respuesta puede ser que el archivo se ha encontrado y enviado con éxito, mientras que la transferencia de datos es el proceso de transmisión del contenido del archivo.

Los comandos FTP son cadenas de caracteres formadas por el nombre del comando y uno o varios parámetros separados con espacios. Los comandos FTP son de tres tipos:

- Comandos de control de acceso: Por ejemplo, para autenticar al usuario (USER y PASS).
- Comandos de parámetros de transferencia: Para especificar puerto de conexión, modos de conexión y tipos de transferencia.
- Comandos de servicio FTP: Para realizar acciones sobre los directorios y archivos remotos como subir y bajar archivos, crear directorios y borrar archivos.

Funcionamiento.

En las respuestas FTP el servidor envía un código numérico de 3 dígitos con el que indica como ha sido procesado el comando al que corresponde la respuesta. El primero de los dígitos indica si el comando ha sido o no procesado con éxito. El segundo dígito indica a que se refiere la respuesta, el tercer dígito ofrece información más específica relacionada con el segundo.

Código	Descripción
1xy	La acción no se ha terminado. Debe obtenerse otra nueva respuesta para poder enviar otro comando
2xy	La acción se realizó con éxito. Puede enviarse otro comando.
3xy	Se está esperando que el cliente envíe información adicional para poder completar la acción.
4xy	Se indica que la acción solicitada no se ha podido realizar ahora pero podría realizarse más tarde
5xy	Se indica que la acción solicitada no se puede realizar.

Tipos de acceso.

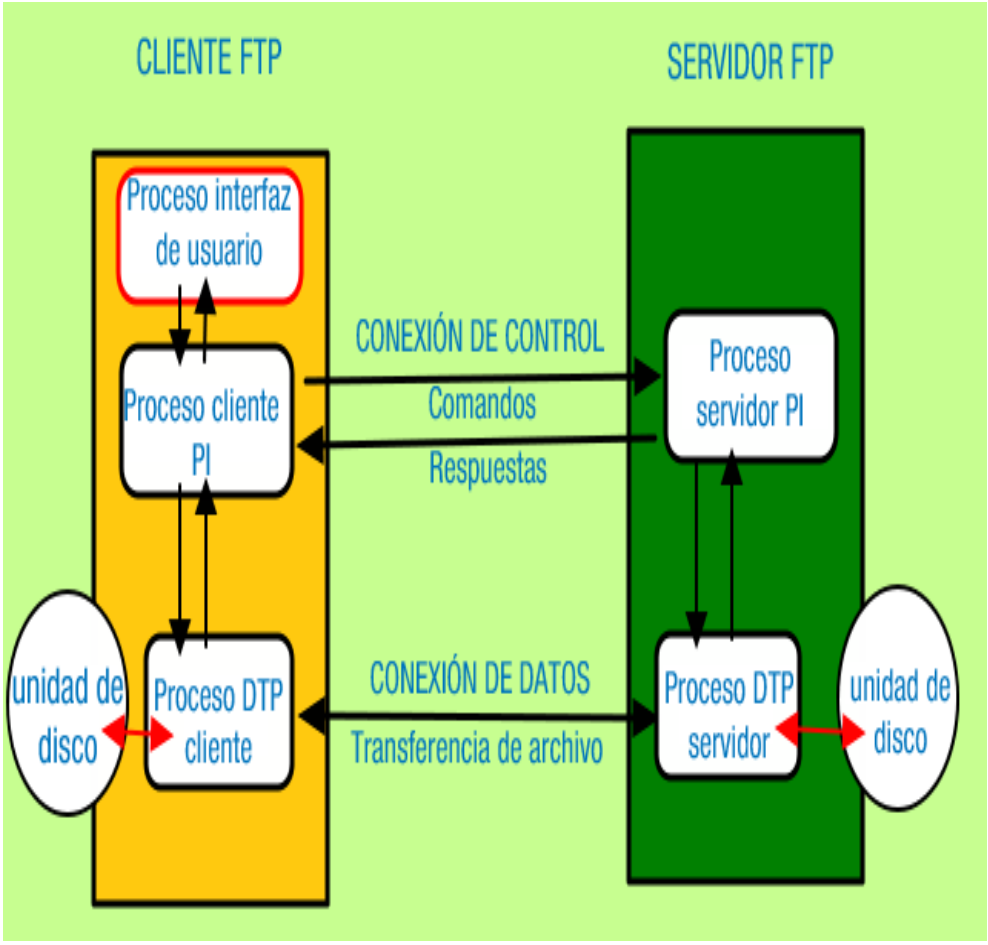
Los servidores FTP permiten dos tipos de acceso:

- Acceso anónimo:
  - El cliente FTP se conecta al servidor con un usuario especial anónimo. Se utilizan los nombres “anonymous” y/o “ftp”
  - De manera habitual (dependiendo de configuración) el usuario anónimo solo puede descargar archivos y su acceso se limita a un directorio del servidor.
- Acceso autorizado:
  - El cliente FTP se conecta mediante un usuario existente en el servidor, puede ser:
    - Usuarios locales de la máquina donde está instalado el servidor FTP.
    - Usuarios virtuales, creado para el acceso FTP.
- Una vez autenticado, un usuario accede al un directorio del servidor en el que puede estar o no confinado.
- En el servidor se configuran los privilegios que tiene cada usuario.

Conexiones de control y de datos.

Una conexión FTP entre un cliente y un servidor se desarrolla sobre dos conexiones TCP de nivel de transporte:

- Conexión de control. El cliente envía los comandos y recibe del servidor las respuestas a los comandos tras haber sido procesados por éste. Los servidores pueden atender múltiples conexiones de control simultáneas, según se configuren en el servidor para evitar sobrecargas.
- Conexión de datos. Es usada para la transferencia de archivos entre cliente y servidor cuando ha sido solicitada esta transferencia por un comando. Asociada a una conexión de control puede haber múltiples conexiones de datos simultáneas (configurables en el servidor).



Conexiones de control y de datos.

Las conexiones de datos se cierran cada vez que se termina una transferencia de archivos y se inician cada vez que se va a iniciar una nueva transferencia de archivos. La conexión de control se inicia cuando el cliente solicita la conexión con el servidor y se cierra cuando el cliente decide terminar la conexión o también puede cerrarla el servidor cuando ha transcurrido un determinado tiempo sin actividad en la conexión (timeout).

Cuando se ha establecido una conexión cliente-servidor FTP se inician en cliente y servidor los procesos usuario PI y servidor PI respectivamente. Estos procesos se comunican a través de la conexión de control. El proceso usuario PI se encarga de transmitir a través de la conexión de control los comandos FTP solicitados por el usuario de la máquina desde su interfaz de trabajo y de obtener las respuestas del servidor y entregársela a la interfaz de trabajo del usuario. El proceso servidor PI se encarga de procesar los comandos recibidos, enviar las respuestas y, si procede, iniciar un proceso de transferencia de archivos.

Cuando se va a iniciar una conexión de datos entre cliente y servidor FTP se inician en cada máquina un proceso DTP. Los procesos DTP cliente y servidor se comunican para desarrollar la transferencia de un archivo. Cuando termina la transferencia, se cierra la conexión de datos y también se cierran los procesos DTP.

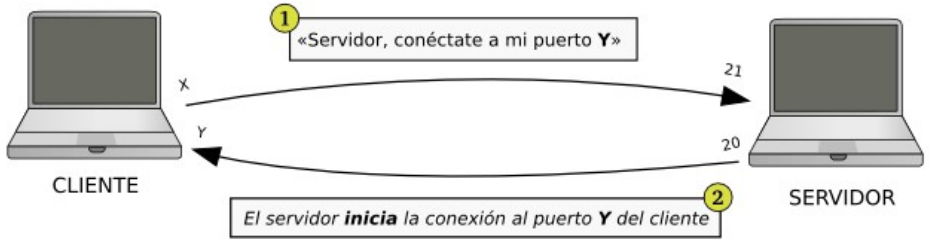
Modos de conexión del cliente.

Los servidores FTP usan el puerto TCP 21 para atender las conexiones de control FTP, es decir, recibe los comandos en el puerto 21 y envía las respuestas por su puerto 21. Si tiene varias conexiones abiertas, usa para todas ellas el puerto 21 como puerto de escucha de la conexión de control. El cliente abre un puerto superior a 1024 para cada conexión de control que establece con un servidor FTP. Si un cliente FTP tiene iniciadas varias conexiones FTP, tiene un puerto abierto por cada una de las conexiones iniciadas incluso si fueran dos simultáneas con el mismo servidor.

Hay dos modos de establecer las conexiones de datos entre cliente y servidor. A estos modos se les llama modos de conexión del cliente y se llaman:

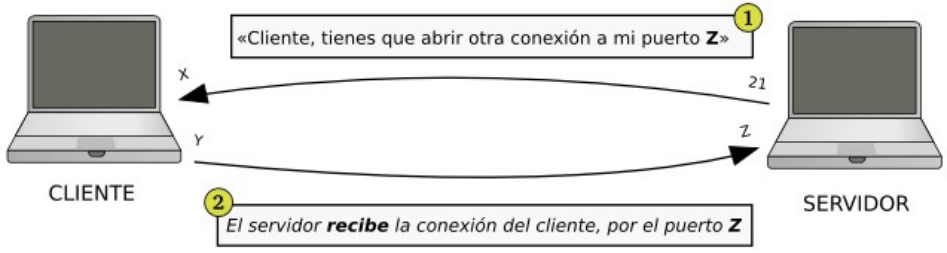
- Modo activo.
- Modo pasivo.

FTP activo:



FTP pasivo:

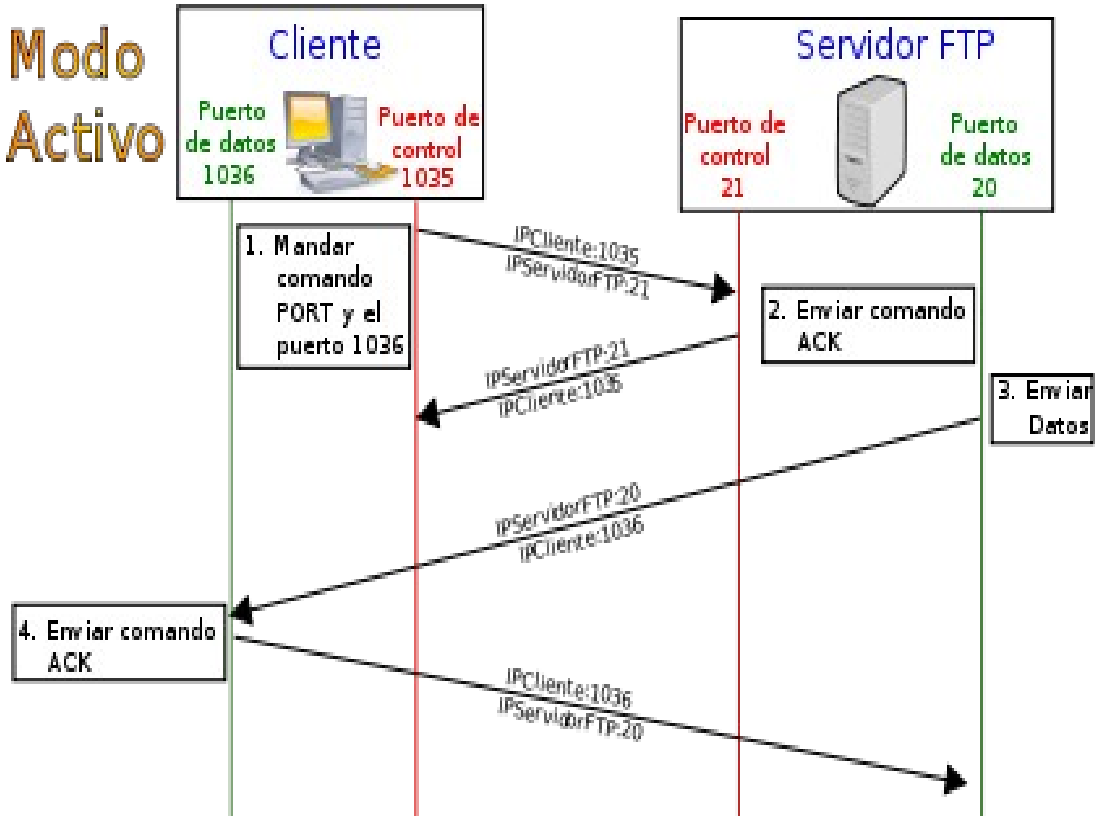
Para activarlo, el cliente se conecta al servidor y le envía la orden PASV. Después pasa esto:



Modos de conexión del cliente.

En el modo activo, una vez que se ha establecido la conexión de control, para iniciar una conexión de datos se hace lo siguiente:

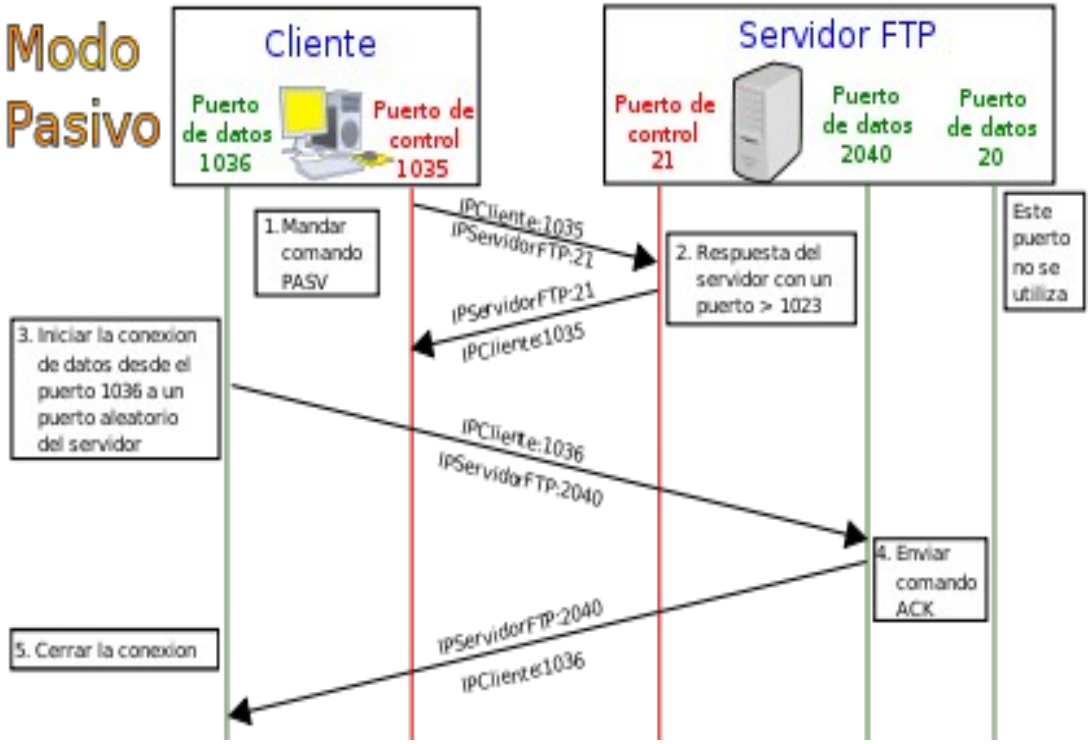
- El cliente envía al servidor un comando PORT a través de la conexión de control indicando un número de puerto TCP superior a 1024 que pretende abrir para la conexión de datos.
- El servidor inicia la conexión de datos (no la transferencia) entre su puerto TCP 20 y el puerto que le ha indicado el cliente. Esto se puede entender por un cortafuegos en el cliente como una amenaza ya que desde el exterior se inicia una conexión solicitando que el cliente abra un puerto.
- La conexión de datos se usa para la transferencia de archivos.



Modos de conexión del cliente.

En el modo pasivo, una vez que se ha establecido la conexión de control, para iniciar una conexión de datos se hace lo siguiente:

- El cliente envía al servidor un comando PASV indicando que va a establecer conexión en modo pasivo.
- El servidor responde con un número de puerto TCP superior a 1024 (aquí no es el puerto 20) que pretende abrir para la conexión de datos. El servidor usa un puerto para cada conexión de datos que tenga iniciada.
- El cliente inicia la conexión de datos abriendo un puerto TCP disponible y mayor que 1024 y conectándose con el puerto que le indicó servidor. Cuando llega la solicitud de conexión al servidor, éste abre el puerto que pretendía usar para la conexión. Se transmiten archivos por la conexión de datos.



Tipos de transferencia.

Para transmitir archivos entre clientes y servidores FTP pueden utilizarse dos tipos de transferencia de datos diferentes:

Transferencia ASCII. Se transmite byte a byte. Una transferencia ASCII es adecuada para transmitir archivos de texto codificados en ASCII (txt, html). Pero no es adecuada para transmitir otros tipos de archivos ya que en la mayoría de los casos no se completaría la recepción de esos archivos. Los archivos ASCII terminan con un carácter de control EOF. Al usar una transferencia ASCII, en el momento que se recibe un byte que corresponde a EOF se da por terminada la transmisión. Esto para los archivos ASCII es lo que se debe producir, pero no para otros archivos ya que un byte de un fichero no ASCII puede contener el código correspondiente a EOF en cualquier parte del archivo.

- Transferencia binaria. La transferencia se realiza bit a bit. Se usa en ficheros que no son de texto.

Para cambiar de un tipo de transferencia a otro, el cliente debe enviar al servidor el comando FTP TYPE e indicando el tipo de transferencia. Los programas clientes de usuario permiten que el usuario pueda solicitar el cambio del tipo de transferencia.

En Linux el programa cliente ftp permite cambiar de un tipo de transferencia a otro mediante los comandos: ascii, binary.

Seguridad.

FTP no es un protocolo seguro. Fue diseñado para ofrecer velocidad pero no seguridad. Se utilizan mecanismos de autenticación de usuarios para determinar los privilegios de acceso y transferencia en el servidor, pero:

- No se usan mecanismos para garantizar que los equipos involucrados en la transferencia son quienes dicen ser. Es vulnerable a ataques de suplantación de identidad (spoofing).
- Todo intercambio de información, incluyendo el usuario y password y la transferencia de cualquier archivo, se realiza en “texto plano” sin ningún tipo de cifrado. Es vulnerable a ataques de análisis de tráfico de red (sniffing).

Los clientes y servidores FTP pueden tener vulnerabilidades y ser aprovechadas por potenciales atacantes para comprometer los datos y los equipos donde se ejecutan.

La mayoría de los protocoles TCP/IP (FTP, HTTP, SMTP, Telnet,POP, IMAP, DNS,..) no son seguros porque en su diseño inicial no se pensó en la seguridad.

FTPS (FTP/SSL)

Conjunto de especificaciones que determinan el encapsulamiento de FTP en SSL (Secure Sockets Layer) o en TLS (Transport Layer Security) para ofrecer comunicaciones seguras. Gracias a la utilización de algoritmos criptográficos y certificados digitales se puede garantizar la confidencialidad y la integridad de la información transmitida, así como la autenticidad de los servidores.

Existen dos métodos para implementar FTPS:

- FTPS Implícito:
  - El cliente establece una conexión de control y se establece la conexión SSL/TSL.
  - Si el servidor no soporta FTPS se cierra la conexión.
  - Todas las comunicaciones, conexión de control y conexiones de datos, son cifradas. El cliente y el servidor no negocian.
  - Para mantener la compatibilidad con los clientes FTP que no soportan SSL/TSL se utilizan otros puertos para atender peticiones FTPS (990/TCP para control y 989/TCP para datos de forma estándar) .

FTPS (FTP/SSL)

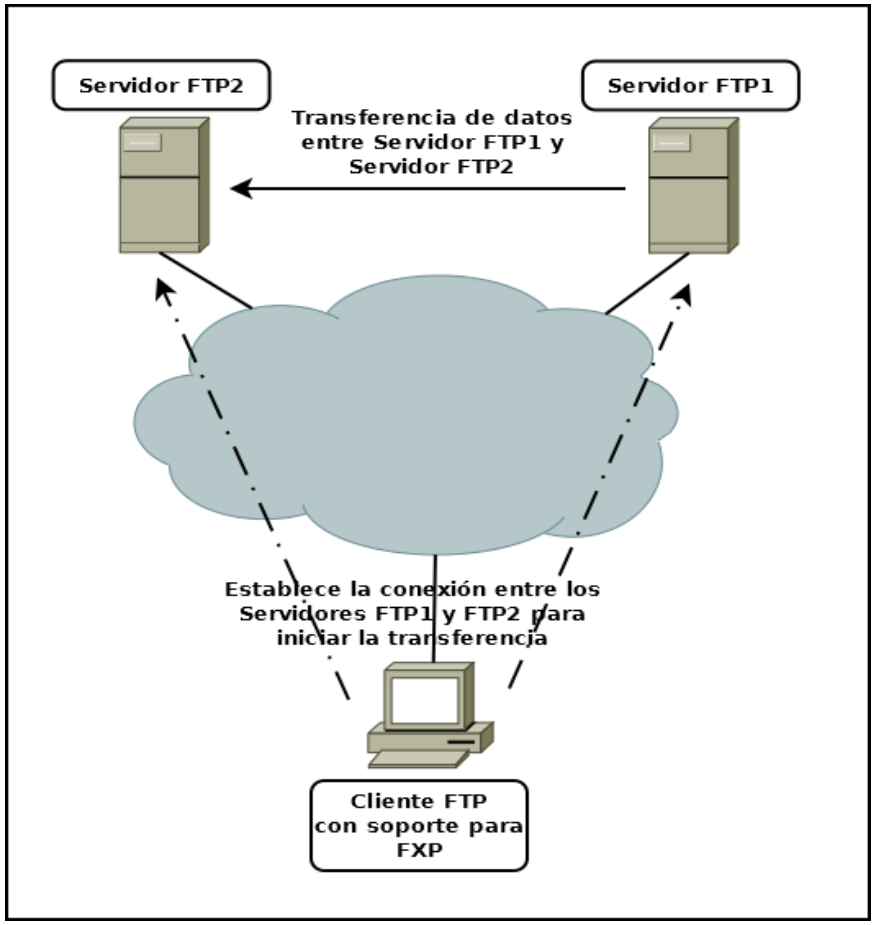
- FTPS Explicito (FTPES):
  - El cliente establece una conexión de control al puerto 21, solicita explícitamente que la comunicación sea segura enviando el comando AUTH SSL o AUTH TTL, y si el servidor lo soporta se establece una conexión SSL/TSL basándose en algoritmos criptográficos y certificados digitales.
  - Si el servidor no soporta FTPS le ofrece al cliente la posibilidad de usar FTP “normal” no seguro.
  - El cliente y el servidor pueden negociar que parte de las comunicaciones, conexión de control y/o conexiones de datos serán cifradas.
  - Es el método recomendado porque permite mayor control sobre la comunicación.

No se debe confundir FTPS con SFTP (SSH FTP), ni con enviar el protocolo FTP a través de una conexión SSH (túnel FTP sobre SSH) conocido como secure FTP. Por tanto SFTP, FTPS y secure FTP son distintos.

Protocolo FXP

FXP (File eXchange Protocol) es un protocolo de transferencia de datos directa entre servidores FTP, utilizando un cliente solo para conectarlos inicialmente. Esto significa que el ancho de banda del cliente es solo para conexión inicial y no para la transferencia de ficheros que se hace directamente de un servidor a otro. Para que sea posible los servidores tienen que permitirlo.

FPX se puede utilizar si quieres migrar ficheros de un servidor FTP a otro ahorrando la descarga desde un servidor al cliente y posteriormente la subida del cliente al otro servidor (se consigue mayor rapidez y menos sobrecarga de la red.



Servicio TFTP

TFTP (Trivial FTP) es un protocolo de capa de aplicación diseñado para ofrecer un servicio de transferencia de ficheros simple y rápido basado en el modelo cliente/servidor.

Al igual que en FTP existen clientes TFTP y servidores TFTP.

Sus características principales son:

- TFTP utiliza UDP como protocolo de nivel de transporte. Los servidores TFTP usan el puerto 69/UPD como puerto estándar.
- No existen mecanismos de autenticación o cifrado.

Al utilizar el protocolo UDP la capa de transporte no garantiza la integridad de la información transmitida pero la velocidad de transferencia es mayor que en FTP.

Se utiliza principalmente en estaciones o dispositivos de red para cargar y hacer copias de seguridad del sistema operativo, archivos de configuración, aplicaciones, etc.

Cisco, usa TFTP para realizar copias de seguridad de archivos de configuración y cargar nuevas versiones del sistema operativo en sus dispositivos

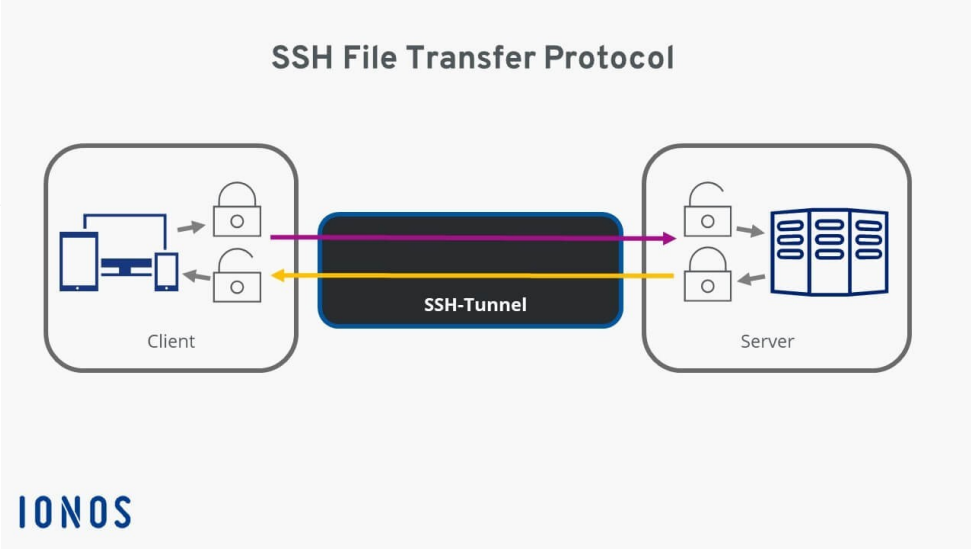
Servicio SFTP/SCP

El protocolo de transferencia SSH (Secure Shell), se desarrolló, entre otras finalidades, para mejorar la protección de la transferencia de datos por FTP. Este protocolo es responsable de la autenticación segura de los puntos de comunicación. En cuanto un cliente inicia una sesión, el servidor comprueba a través de SSH y con su ayuda la identidad del cliente. La autenticación mutua se realiza por certificados y mediante el método de clave pública y privada, también llamado cifrado asimétrico.

Los servidores SSH usan el puerto 22/TCP como puerto estándar.

SSH se implementa como SFTP o SCP:

- SFTP: permite transferencia de ficheros entre sistemas remotos, listar ficheros y directorios del servidor, realizar funciones como renombrar, borrar, crear archivos y carpetas, cambiar permisos…
- SPC: permite la copia de ficheros entre sistemas remotos. Hay clientes SPC gráficos que integran otras funciones, pero no son cliente SPC “puros”.



Servidores FTP

Existen una gran cantidad de servidores FTP. A la hora de elegir un servidor FTP habrá que evaluar varias de sus características. Algunas de estas características son: Facilidad de instalación y configuración, seguridad del servicio, opciones disponibles de configuración, gestión de cuentas de usuario y permisos de acceso a recursos, limitación del ancho de banda para las transferencias de archivos, número máximo de conexiones simultáneas etc. A continuación se describen algunos de los servidores FTP más destacados.

- vsftpd. Sóoo para Linux. Es un servidor muy seguro, fácil de instalar y configurar. Los usuarios del sistema Linux en el que se instale el servidor son usuarios para el servicio. La configuración es muy sencilla y se centra fundamentalmente en la seguridad y la eficiencia.
- Filezilla Server. Muy fácil de usar. Su mejor característica es la relativa a la configuración de cuentas de usuario y grupos de usuarios y el establecimiento de permisos de acceso, restricciones sobre acciones, cuotas y otras limitaciones. Licencia GPL.

Servidores FTP

- FTP Serv-U. Para Windows y Linux. Muy fácil de usar y muy completo. Es muy potente en lo relativo a opciones de seguridad y establecimiento de restricciones sobre cuotas de disco y velocidades de subida y bajada para usuarios. Licencia de prueba por 30 días. Después sigue funcionando pero en un modo llamado personal con menos funcionalidades. Dispone de otras licencias de pago de los tipos Bronze, Silver y Gold.
- Microsoft FTP Server. Sólo para Windows. Está integrado dentro de los sistemas Windows formando parte de Microsoft IIS.
- Pure-FTPd. Solo para Linux. Muy fácil de instalar y configurar. Sus características más destacadas son la seguridad, la regulación del ancho de banda para las transferencias de archivos y la gran cantidad de opciones de configuración. Licencia GPL