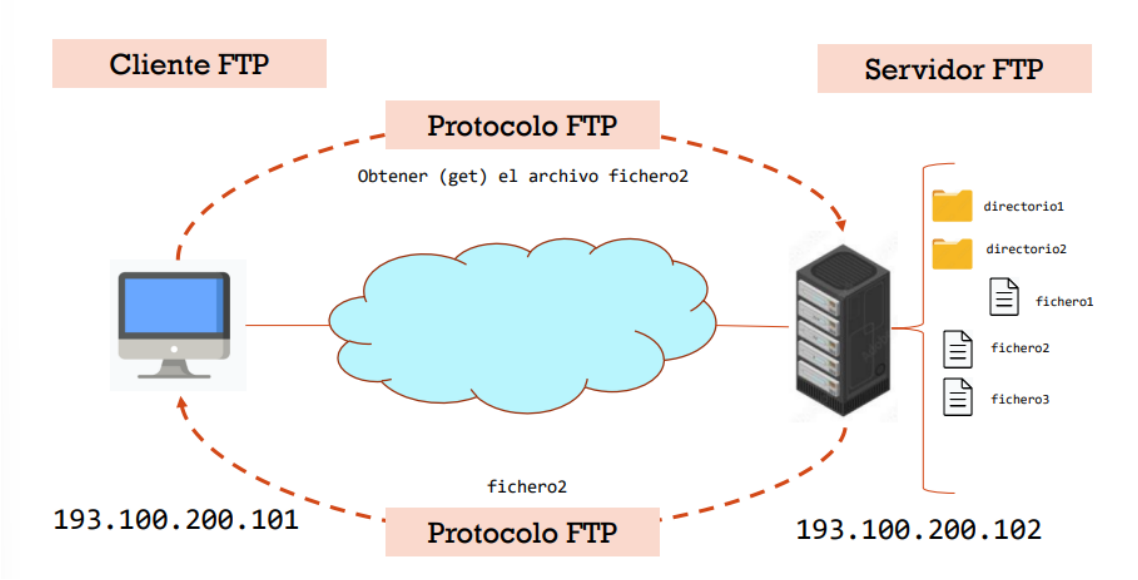
El protocolo FTP (file Transfer Protocol) es un protocolo de capa de aplicación diseñado para ofrecer un servicio estándar de transferencia de ficheros entre sistemas conectados a redes TCP/IP

Se basa en el modelo cliente servidor

Esta formado por:

- Clientes FTP: acceden al sistema de ficheros donde están instalados y establecen conexiones con los servidores FTP para subir o descargar archivos.
- Servidores FTP: acceden al sistema de ficheros del equipo donde están instalados, manejan las conexiones de los clientes y en función de los privilegios definidos permiten la descarga y/o subida de ficheros.
- Protocolo FTP: conjunto de normas y reglas en base a las cuales dialogan los clientes y servidores FTP. Utiliza TCP.



Clientes FTP

Programas que acceden al sistema de ficheros del equipo donde están instalados y establecen conexiones con los servidores FTP para subir o descargar programas

Existen múltiples clientes FTP, tanto libres como propietarios

Protocolo FTP

Determina el conjunto de normas y reglas en función de las cuales los clientes y servidores de FTP se comunican

La comunicación se basa en el envío de mensajes de texto que contienen comandos y respuestas

Utiliza TCP como protocolo de transporte

Los comandos FTP son cadenas de caracteres que finalizan con el código de final de línea

Las respuestas FTP son enviadas por el servidor como consecuencia de la acción ejecutada al recibir un comando. Están formadas por un código de 3 dígitos y un mensaje de texto descriptivo

- El primer digito indica si la acción solicitada por el comando fue exitosa o fallida
- El segundo digito indica a que se refiere la respuesta
- El tercer digito ofrece información más específica relacionada con el segundo digito

Tipos de acceso

Los servidores FTP permiten, dependiendo de como se configuren, dos tipos de acceso desde los clientes

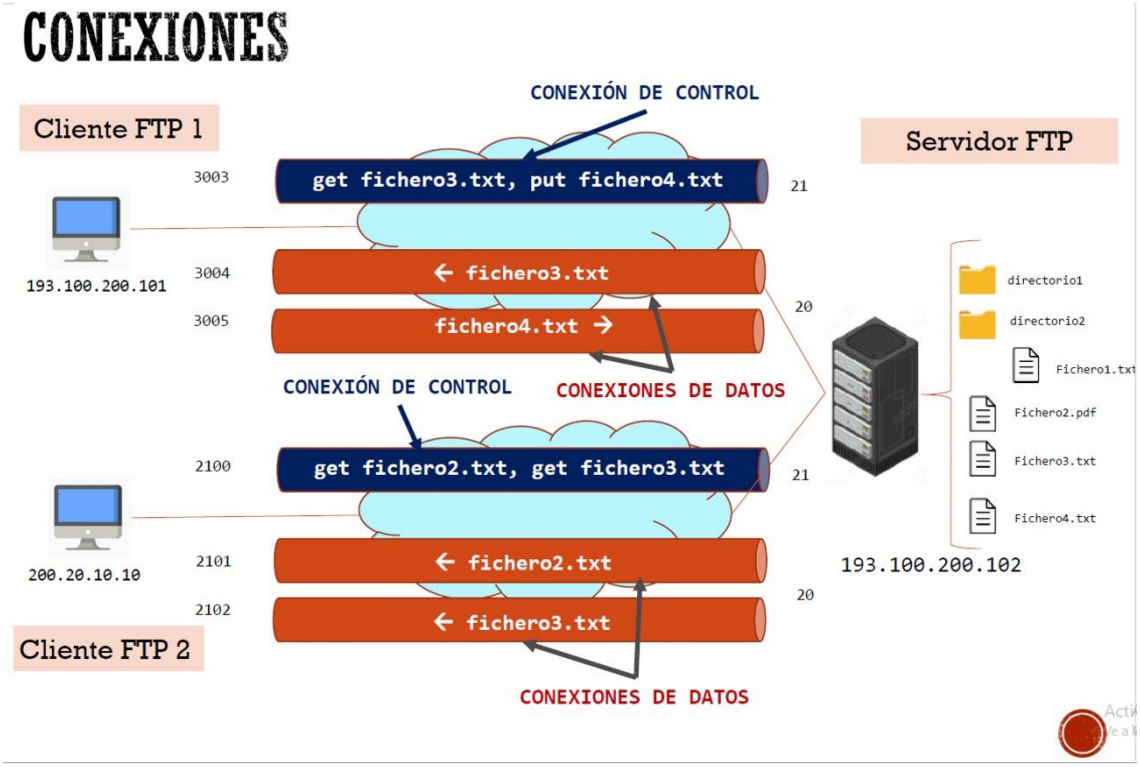
- Acceso anonimo
    - El cliente se conecta al servidor con un usuario especial (Anonymous) que no tiene contraseña. Normalmente solo se puede descargar archivos.
- Acceso autorizado
    - El cliente se conecta con un usuario (y con contraseña normalmente) que debe existir en el servidor. Según el servidor, puede ser:
        - Usuario local del sistema operativo
        - Usuarios propios del servidor FTP
    - Cada usuario accede a un directorio del servidor del que puede no tener acceso para subir a niveles superiores
    - En el servidor se configuran los permisos y privilegios que el usuario tiene.

Conexiones

FTP es un servicio basado exclusivamente en TCP que utiliza varias conexiones y puertos

- Conexión de control
    - Sirve para establecer la conexión y el envío de comandos
        - No se envían datos por esta conexión
        - Esta activa hasta el cierre de sesión o hasta que se sobrepasa el tiempo de espera sin recibir comandos, y la cierra el servidor
        - Pueden existir varias conexiones simultáneamente, aunque se puede limitar (configurar) el numero de conexiones (tanto total como por usuario)

        - Utiliza el puerto TCP 21
- Conexión de datos
    - Se crea una nueva conexión cuando el cliente solicita una transferencia de información
        - Se cierra cuando termina la transmisión
        - Cada conexión de control puede tener varias conexiones de datos (se puede configurar) simultáneamente
        - En modo activo, se utiliza el puerto TCP 20, pero en modo pasivo utiliza otro (>1023).



Por las conexiones de control nunca se envían datos

Por las conexiones de datos nunca se envían comandos de control

Inicialmente, los servidores FTP usaban el puerto:

- 21/TCP para atender conexiones de control
- 20/TCP para las conexiones de datos
- Actualmente no se usan siempre el puerto 20 para las conexiones de datos, sino se usan puertos mayores a 1023 (más adelante se expondrán los m

Un cliente FTP puede iniciar una conexión a un servidor de dos formas:

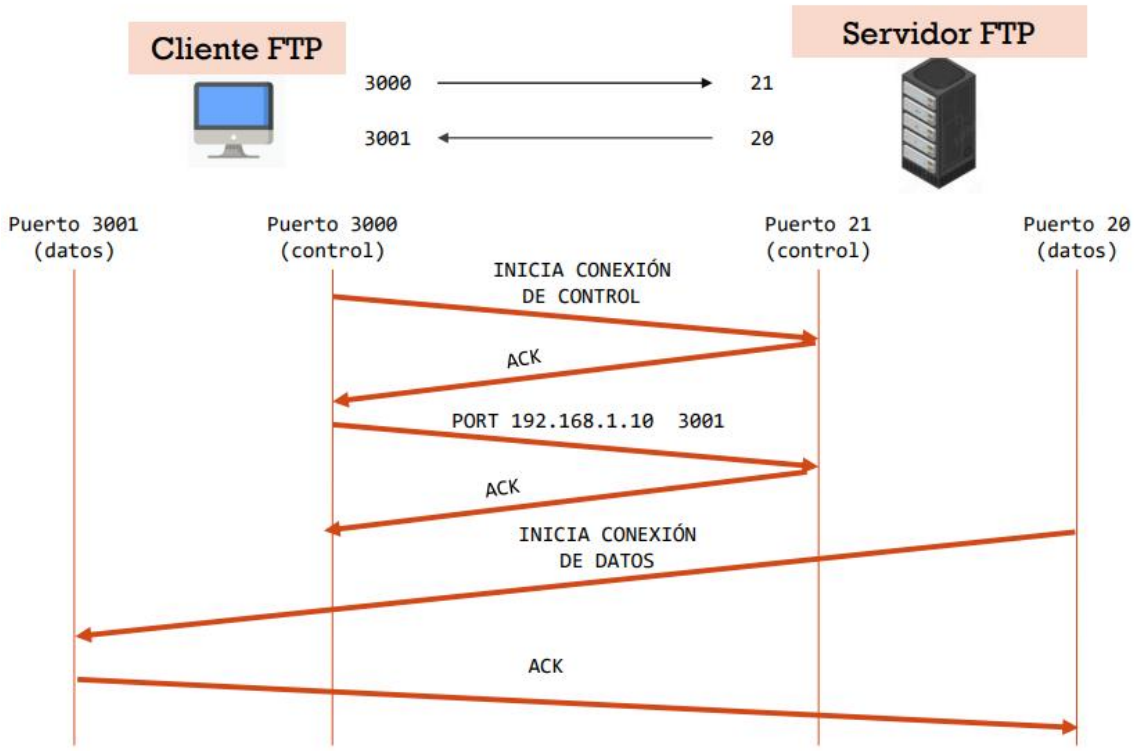
- Modo activo
- Modo pasivo

Modo activo

Es el modo nativo del servidor FTP

Funcionamiento

- El cliente establece una conexión de control al puerto 21 del servidor en un puerto suyo local > 1023 (en el siguiente ejemplo el puerto 3000)
- Cuando se solicita una transferencia de ficheros
    - El cliente envia el comando PORT al servidor, indicando su IP y el puerto se abrirá para la conexión de datos
    - El servidor indica una conexión TCP desde su puerto 20 hacia el puerto indicado por el cliente en el siguiente ejemplo el puerto 3001
- Es el servidor el que inicia las conexiones de datos y el cliente tiene que abrir puertos para atender dichas conexiones
- La maquina que ejecuta el cliente FTP tiene que aceptar conexiones a puertos, usados en las transferencias de datos, superiores a 1023



Es el servidor el que inicia las conexiones de datos y el cliente tiene que abrir puertos para atender dichas conexiones

La maquina que ejecuta el cliente FTP tiene que aceptar conexiones a puertos, usados en las transferencias de datos, superiores a 1023

Esto puede comprometer la seguridad del equipo:

- Los cortafuegos instalados en el equipo donde se encuentra el cliente FTP o en la red a la que pertenece evitarán estas conexiones aleatorias para prevenir ataques
- Si el equipo donde esta el cliente esta detrás de un Router NATP, este descartará las conexiones iniciadas desde el exterior por el servidor FTP a los puertos que abre el

cliente. Es muy habitual que los equipos de una red privada que se conecta a internet lo haga a través de un encaminador o Router que implementa NATP

- Para solventar estos problemas, consecuencia de que sea el servidor el que inicia las conexiones de datos, se desarrolló el modo pasivo.

NOTA: los cortafuegos actuales y versiones modernas de NATP implementan FTP ALG (Application Level Gateway), en este caso los clientes de la red interna si podrán iniciar conexiones FTP utilizando el modo activo

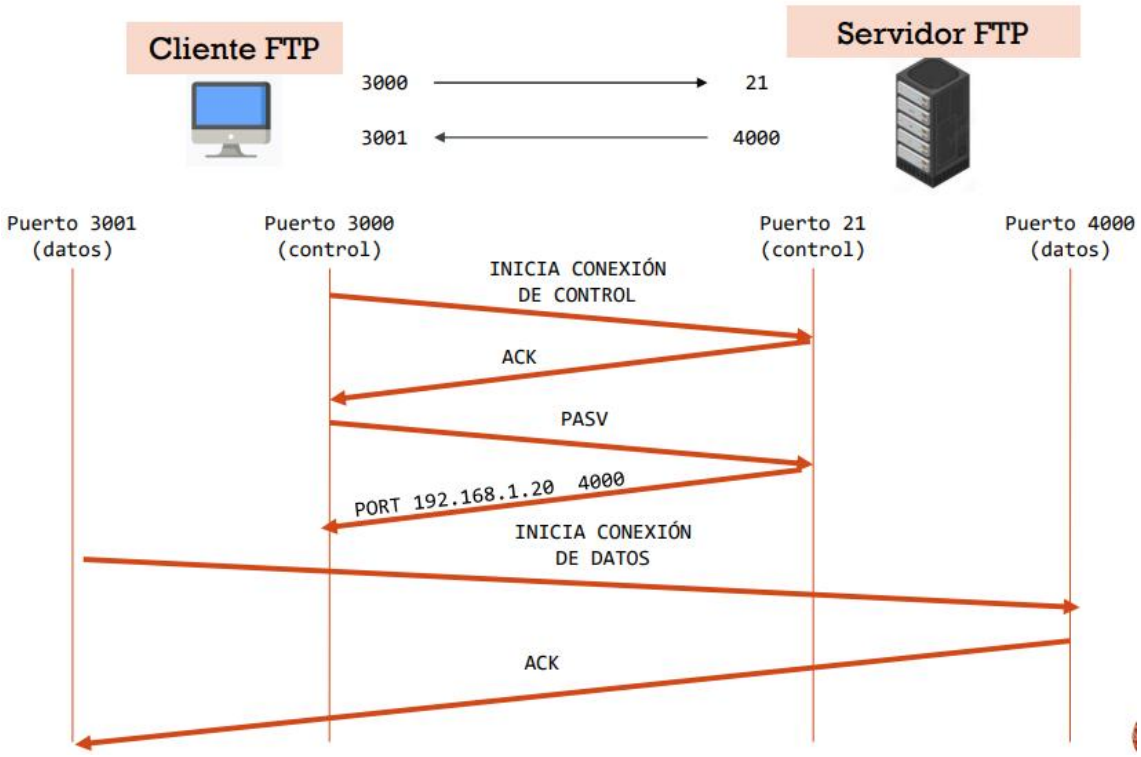
Modo pasivo

Es siempre el cliente el que inicia las conexiones con el servidor

El puerto 20 del servidor no se utiliza

Funcionamiento

- El cliente establece una conexión de control al puerto 21 del servidor suyo local > 1023 (en el siguiente ejemplo el puerto 3000). La conexión de control funciona igual que en el modo activo
- Cuando se solicita una transferencia de ficheros:
    - El cliente envía el comando PASV para activar el modo pasivo. Como respuesta a este comando el servidor retorna un nº de puerto que tenga disponible (en el siguiente ejemplo el 4000)
    - El cliente inicia una conexión TCP, abre un puerto local superior a 1023 (en el siguiente ejemplo 3001) hacia el puerto que le envió el servidor (en el ejemplo 4000)



En el modo pasivo resuelve el problema de que el cliente tenga que aceptar conexiones en puertos mayores a 1023 pero lo traslada al servidor.

- la maquina donde se ejecuta el servidor FTP tiene que aceptar conexiones en múltiples puertos y esto es una amenaza para la seguridad del equipo
- los cortafuegos actuales permiten realizar un seguimiento de las conexiones pasivas de datos, comprobando que el cliente que solicita la conexión al puerto especificado por el servidor que corresponde con el cliente al que se le indico ese puerto y que, por tanto, la conexión se establece para el envió o recepción de datos
- si el servidor está detrás de un NATP hay que:
    - configurar en el servidor la IP externa que usa el NATP y un rango de puertos para aceptar las conexiones de datos
    - redirigir el rango de puertos del encaminador que hace NATP al equipo donde está el servidor FTP

cortafuegos y encaminadores/NATP

uso de servidores y clientes FTP y los modos activo y pasivo implican una configuración adecuada de los cortafuegos y de los encaminadores/NATP que existan en los equipos y redes donde se utilizan.

Veremos a continuación algunas situaciones comunes

Resumen y comparativa de modos

MODO ACTIVO Facilita la configuración y administración del servidor FTP, pero presenta problemas de seguridad a los clientes y problemas de acceso si están detrás de cortafuegos y/o routers/NATP	Conexión control: cliente (>1023) => servidor (21) Conexión datos: Cliente (>1023) <= Servidor (20)
MODO PASIVO Favorece al cliente pero implica una configuración mas compleja en el servidor	Conexión control: cliente (>1023) => servidor (21) Conexión datos: Cliente (>1023) => Servidor (>1023)

FTPS (FTP/SSL)

Especificaciones que determinan como encapsular FTP en SSL (Secure Sockets Layer) o en TLS (Transport Layer Security) para ofrecer conexiones seguras gracias a la utilización de algoritmos criptográficos y certificados digitales.

Existen dos métodos para implementar FTPS:

- FTPS Implicito
  - El cliente establece una conexión de control y se establece la conexión SSL/TLS
  - Si el servidor no soporta FTPS se cierra la conexión
  - Todas las comunicaciones conexión de control y conexiones de datos son cifradas
  - Para mantener la compatibilidad con los clientes FTP que no soporten SSL/TLS se utilizan otros puertos para atender peticiones FTPS. Se utilizan otros puertos para atender peticiones FTPS. Se utilizan los puertos 990/TCP para control y 989/TCP para datos.
- FTPS Explicito (FTPES)
  - El cliente se conecta al puerto 21, y se solicita explícitamente que la comunicación sea segura mediante el comando AUTH SSL o AUTH TTL. Si el servidor lo permite, se establece la conexión SSL/TLS. Si no lo soporta, ofrece utilizar la conexión no segura.
  - El cliente se conecta al puerto 21, y se solicita explícitamente que la comunicación sea segura mediante el comando AUTH SSL o AUTH TTL:
    - Si el servidor lo permite, se establece la conexión SSL/TLS basándose en algoritmos criptográficos y certificados digitales
    - Si no lo soporta, ofrece utilizar la conexión “normal” (no segura)
  - El cliente y el servidor pueden negociar que parte de las comunicaciones, conexión de control y/o conexiones de datos serán cifradas.

No hay que confundir FTPS con SFTP ni con Secure FTP

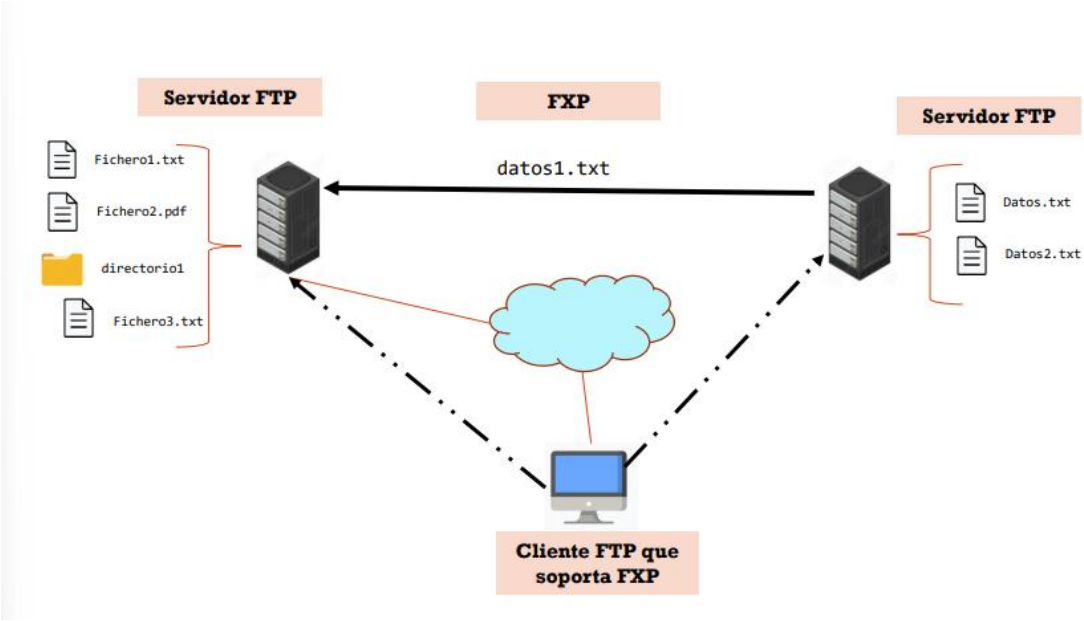
- SFTP (SSH File Transfer Protocol) protocol transferencia ficheros basado en ssh
- Secure FTP túnel FTP sobre SSH

Protocolo FXP

File eXchange Protocol (FXP) es un protocolo de transferencia de datos directa entre servidores FTP, utilizando un cliente para conectarlos inicialmente

Esto significa que el ancho de banda del cliente es solo para la conexión inicial y no para la transferencia de ficheros que se hace directamente de un servidor a otro (ver la siguiente imagen)

Para que esto sea posible los servidores FTP tienen que permitirlo



Concepto

TFTP (trivial File Transfer Protocol) 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

Existen clientes TFTP y servidores TFTP

Características

Utiliza UDP como protocolo de nivel de transporte. Los servidores TFTP usan el puerto 69/UDP

No existen mecanismos de autenticación

Al utilizar el protocolo UDP la capa de transporte no se garantiza la integridad de la información, pero es más rápido que 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.

Características SSH

Ofrece autenticación, confidencialidad e integridad

- Se autentifica a los dos extremos de la conexión
    - El servidor se autentica ante el cliente con una clave
    - El cliente se autentica ante el servidor
- Se cifran los datos intercambiados
    - Nombre de usuario y password viajan cifrados
    - La información transmitida viaja también cifrada

SSH integra mecanismos de transferencia de ficheros. Se basa en los protocolos SFTP (SSH File Transfer Protocol) y SCP (Secure Copy Protocol), los cuales se exponen en el apartado 3 de la presentación

Servicios SFTP/SCP

SSH integra mecanismos de transferencia de ficheros garantizando autenticación, confidencialidad e integridad

Se basa en los protocolos SFTP (SSH File Transfer Protocol) y SCP (Secure Copy Protocol)

La mayoría de los clientes gráficos FTP también pueden actuar como clientes SFTP o SCP