Servicios de transferencia de archivos

Las aplicaciones de transferencia de ficheros fueron una de las primeras herramientas en desarrollarse en la expansión de las redes de internet. La necesidad de poder acceder a diferentes sistemas e intercambiar información originó uno de los sistemas que actualmente se utilizan.

El **FTP** (*file transfer protocol*) o protocolo de transferencia de **ficheros** es un protocolo que proporciona el servicio de transferencia de ficheros entre sistemas de diferente naturaleza, es decir, se pueden interconectar clientes de Linux hacia un sistema de Microsoft u otros.

El protocolo FTP se basa en la arquitectura cliente/servidor y hace uso del protocolo de

control de transporte, TCP (*transporte control protocolo*) para realizar el canal de transmisión entre el cliente y el servidor, con la garantía de que la información que se envía o se lee llegara a su destino.

El servidor FTP funciona a través de los siguientes puertos configurables:

- Puerto 21: control de la conexión.
- Puerto 20 o mayor de 1024: puerto de transferencia de datos.

Estos puertos son configurables mediante los archivos de configuración, siendo los puertos anteriores los utilizados por defecto.

Se utilizan dos canales de comunicación dentro del protocolo FTP, el canal de control y el canal de datos:

- El canal **de control** envía todas las órdenes de comunicación, como pueden ser iniciar la sesión de trabajo y órdenes de ejecución como leer, escribir, listar, borrar, etc.
- El canal **de datos** envía el contenido de aquellos ficheros a trabajar, que puede ser tanto para leer el contenido del fichero como para hacer la escritura del fichero.

Tanto el cliente como el servidor gestionan dos procesos:

- **PTD** (procesos de transferencia de datos): es el encargado de establecer la

  conexión y administrar el canal de datos. Tanto el cliente como el servidor tienen su propio PTD.
- **IP** (interprete del protocolo): interpreta el protocolo y permite que el PTD pueda

  ser controlado mediante órdenes recibidas por el canal de control.

La IP del servidor:

- Escucha las órdenes que provienen de la IP del usuario mediante el canal de control por un puerto de datos.
- Establece la conexión del canal de control.
- Recibe las órdenes FTP de la IP del usuario, las responde y ejecuta al PTD del servidor.

La IP del cliente:

- Es la responsable de establecer la conexión con el servidor FTP.
- Envía órdenes FTP.
- Recibe las respuestas del servidor IP.
- Controla el PTD del usuario.

Cuando un cliente conecta al servidor FTP, la IP del usuario inicia la conexión con el servidor con el protocolo Telnet.

El cliente envía órdenes FTP al servidor, el servidor las interpreta, ejecuta el PTD y responde con un formato standard. Una vez establecida la conexión, la IP del servidor proporciona el puerto por el que se enviarán los datos al PTD del cliente, por donde escuchará y recibirá los datos del servidor.

Las órdenes FTP permiten especificar:

- El puerto que se utilizará.
- El método de transferencia de datos.
- La estructura de datos.
- Elección que se dura a cabo (leer, eliminar, listar, almacenar, etc.).

Hay tres distribuciones de órdenes FTP:

- **Órdenes de control de acceso**: especifican los identificadores del control de acceso. La mayoría de ellos controlan quién accede al servidor FTP y qué privilegios tendrá el usuario.

• **Órdenes de parámetros de transferencia**: tienen un valor por defecto del servidor FTP, y únicamente se hace uso de estos parámetros si han sido modificadas.

• **Órdenes de servicio FTP**: son las órdenes más usadas. Definen la transferencia de ficheros y la navegación de los directorios remotos para el usuario. El argumento principal de las órdenes de servicio suele ser el nombre de un directorio. Todos los datos que se envían para una orden de servicio siempre se envían por el canal de datos.

Configuración del servicio de transferencia de ficheros

En esta unidad usamos el servidor FTP llamado **ProFTPD** (*short for PRO FTP Daemon*). ProFTPD es un servidor FTP con licencia GPL (G*eneral Public License*) para Linux que permite hacer una customización de su funcionamiento dependiendo de las necesidades del entorno de trabajo por parte del administrador.

Las características principales de este software son:

• Su sistema de configuración se basa en un fichero de configuración con directrices intuitivas muy parecidas a las configuraciones dentro del servidor Apache Web Server.

• Permite la configuración de servidores virtuales.

• Permite la ejecución del servicio como servidor independiente (*standalone*) o *inetd*.

• Permite mantener la raíz del directorio anónimo.

• El código fuente está disponible para los desarrolladores.

• Permite esconder los ficheros y directorios, basándose en los permisos que utiliza Linux.

Demonios 'standalone' e 'inetd'

- El demonio **standalone** escucha las peticiones del servicio y lanza diferentes procesos para tratarlas. Se utiliza para **tráficos elevados de datos y usuarios**. El servicio siempre está activo.
- El demonio **inetd** escucha las peticiones del servicio de los puertos. Si detecta comunicación en el puerto configurado inicia el servicio pasándole la conexión. Se utiliza en situaciones de **poco tránsito**.

Configuración de ProFTPD

El sistema donde se hace la instalación y configuración está basado en un sistema Debian. El conjunto de instrucciones de instalación o configuración mediante órdenes de sistema son dependientes.

La configuración interna es independiente del sistema operativo usado, cualquier configuración que haga durante estos apartados es compatible con otros sistemas operativos basados en Unix.

Para iniciar el proceso de instalación de ProFTPD, abrimos un terminal y ejecutamos

```
sudo apt-get install proftpd
```

Una vez finalizada la instalación, procedemos a verificar el resultado, ejecutamos

```
sudo cat /etc/shadow
```

La orden que acabamos de ejecutar lista todos los usuarios del sistema. Si nos fijamos bien encontraremos unas líneas llamada ftp y proftpd. Estas líneas hacen referencia a dos usuarios que ha creado el proceso de configuración inicial de proFTPD. Los usuarios ftp y proftpd son usuarios de acceso para realizar accesos anónimos.

Podemos comprobar el mismo resultado con las órdenes siguientes:

```
sudo cat /etc/shadow | grep proftpd
```

```
sudo cat /etc/shadow | grep ftp
```

o con una orden única:

```
sudo cat /etc/shadow | grep -E "proftpd|ftp"
```

A continuación, comprobamos el estado de los procesos realizados con ProFTPD:

```
sudo ps -ef | grep proftpd
```

Vemos que hay un proceso proftpd y que está aceptando las conexiones.

Ahora, ejecutamos la orden:

```
sudo netstat -ltn
```

Esta orden mostrará aquellos procesos que están escuchando **el puerto 21 (puerto de control de la conexión del servicio FTP).**

```
Conexiones activas de Internet (solo servidores)
Proto  Recib Enviad      Dirección  local              Dirección  remota
Estado
.
.
.
tcp6       0      0      :::21                     :::*
ESCUCHAR
```

La línea indicada confirma que hay un proceso que está escuchando el puerto 21, que es el que se usa dentro del protocolo FTP.

Una vez que se han verificado los procesos y los puertos de proFTPD, la configuración del servicio FTP se realizará mediante un fichero de texto plano.

El directorio donde se encuentran las configuraciones es */etc/proftpd/* y el fichero de configuración principal es el fichero *proftpd.conf*.

Editar el fichero original puede comportar tener que modificar el fichero y perder los datos iniciales de configuración. Siempre es bueno hacer una **copia de seguridad.** del fichero. Con la orden cp (para copiar ficheros) o navegando al directorio */usr/share/proftpd/templates/* tenemos las copias de los ficheros originales, en caso de querer recuperar las configuraciones iniciales.

Uno de los ficheros que contiene la carpeta *templates* es el fichero con el mensaje de bienvenida *Welcome.msg*, que es una copia del que se ubica en la carpeta raíz */srv/ftp*.

Navegamos hasta el directorio de configuraciones de ProFTPD */etc/proftpd* y mostramos el contenido

```
total 1324
-rw-r--r-- 1 root root 1310700 feb 27  2020 blacklist.dat
drwxr-xr-x 2 root root    4096 feb 27  2020 conf.d
-rw-r--r-- 1 root root    9420 feb 27  2020 dhparams.pem
-rw------- 1 root root     701 dic  3 09:48 ldap.conf
-rw-r--r-- 1 root root    2918 dic  3 09:48 modules.conf
-rw-r--r-- 1 root root    5690 dic  3 09:48 proftpd.conf
-rw------- 1 root root     862 dic  3 09:48 sql.conf
-rw-r--r-- 1 root root    2082 dic  3 09:48 tls.conf
-rw-r--r-- 1 root root     832 dic  3 09:48 virtuals.conf
```

Como podemos ver, el contenido del directorio */etc/proftpd* contiene diferentes ficheros, incluido el proftpd.conf. Los ficheros que hay dentro hacen referencia a ficheros de configuraciones de modularidades que amplían la capacidad de ProFTPD, como pueden ser vinculaciones de datos con SQL, configuraciones de seguridad

para cifrar la información, creación de servidores virtuales, vinculación con el servicio de directorio LDAP (*Lightweight Directory Access Protocol*), etc.

Editamos el fichero *proftd.conf* y observamos el contenido.

Dentro de la configuración inicial, las directivas más importantes son:

• ***Servername***: define el nombre del servidor que mostrara, en este caso "Debian". Podéis cambiar el nombre por uno que identifique nuestro servicio.

• ***TimeoutIdle***: define el tiempo que un usuario puede estar conectado sin hacer ninguna acción.

• ***TimeoutStalled***: define el tiempo que una conexión de datos puede estar parada.

• ***DisplayLogin***: define el fichero de texto donde se mostrará el mensaje de bienvenida.

• ***DisplayChdir***: define el fichero de mensaje que se mostrará en cada cambio de navegación de directorio.

• ***ListOptions***: define la orden "-l" para listar los directorios.

• ***DefaultRoot***: encapsula a los usuarios en los directorios *home* de cada usuario.

• ***RequireValidShell***: si el valor es *on* obliga a que los usuarios de sistema tengan definido un *shell* válido en su configuración.

• **Port**: define el número de puerto que se utilizará para las conexiones de control, por defecto el 21.

• ***Umask***: máscara de permisos que tendrá por defecto.

• ***AllowOverWrite***: permite sobreescribir el fichero si el valor es: *on*

• ***QuotaEngine***: permite activar el motor de cuotas del servidor FTP.

Estas directivas están activas sin comentar y funcionan por defecto en el servidor.

Las siguientes directivas están comentadas con el símbolo *#*:

• ***#Include /etc/proftpd/virtuals.conf*** : fichero donde se habilitarán las configuraciones de servidores virtuales alternativos que se pueden configurar.

• **#Anonymous**: habilita el servidor anónimo.

• ***#Include /etc/proftpd/tls.conf*** : fichero donde se configurará el servidor para soportar conexiones seguras.

• **#Directory**: configura un directorio específico con una configuración específica, como puede ser habilitar acceso a los usuarios, permitir leer, escribir, listar, etc.

Inicio, parada, reinicio y recarga del servidor ftp

Para iniciar el servidor proFTPD podemos utilizar:

/etc/init.d/proftpd start

service proftpd start

Para parar el servidor proFTPD:

/etc/init.d/proftpd stop

service proftpd stop

Si quieres reiniciar el servidor proFTPd puedes usar:

/etc/init.d/proftpd restart

service proftpd restart

Si necesitas iniciar, parar o reiniciar el proceso de proFTPd, y utilizas el sistema **systemd**, podrás ejecutar los siguientes comandos para realizar todas las acciones.

Para iniciar el servidor proFTPD:

systemctl start proftpd

systemctl start proftpd.service

Para parar el servidor proFTPD:

systemctl stop proftpd

systemctl stop proftpd.service

Si quieres reiniciar el servidor proFTPd puedes usar:

systemctl restart proftpd

systemctl restart proftpd.service

Cuando hagamos un cambio en la configuración, necesitaremos hacer un «reload», para que automáticamente la aplique.

/etc/init.d/proftpd reload

service proftpd reload

En el caso de utilizar Systemd, deberás poner lo siguiente:

systemctl reload proftpd

systemctl reload proftpd.service

Finalmente, si quieres ver el estado actual del servidor proFTPd, puedes ejecutar los siguientes comandos, dependiendo de si utilizas SysVinit o Systemd, deberás utilizar los siguientes comandos. Si usas SysVinit tendrás que usar:

/etc/init.d/proftpd status

service proftpd status

y si utilizas Systemd:

systemctl status proftpd

systemctl status proftpd.service

Permisos

Dentro de un servicio FTP, uno de los pasos importantes es el de conceder permisos determinados para controlar el acceso al servidor o a los diferentes directorios.

Dentro de ProFTPD la directiva **<Limit>** permite hacer las configuraciones de permisos dentro del servidor FTP.

La directiva **<Limit>** se puede configurar dentro de las directivas siguientes, en la configuración general del servidor:

- ***<VirtualHost>***
- ***<Directory>***
- ***<Anonymous>***
- ***<Global>***

Los permisos generales que se pueden configurar son:

- ***ALL*** (todos los permisos excepto de LOGIN).
- ***DIRS*** (Conocer el contenido de un directorio, incluye **CDUP, CWD, LIST, MDTM, MLSD, MLST, NLST, PWD, RNFR, STAT, XCUP, XCWD, XPWD**)
- ***LOGIN*** (acceso de usuarios)
- ***READ*** (incluye **RETR, SIZE**)
- ***WRITE*** (incluye **APPE, DELE, MKD, RMD, RNTO, STOR, STOU, XMKD, XRMD**)

Estas palabras clave (ALL, DIRS, LOGIN, READ, WRITE) permiten configuraciones generales, pero podemos también configurar permisos específicos.

Otras directivas útiles que se pueden usar dentro de <Limit> son:

• ***AllowUser nombreUsuario***: da el permiso a un usuario especifico.

• ***DenyUser nombreUsuario***: deniega el permiso a un usuario específico.

• ***AllowAll***: da el permiso a todos los usuarios.

• ***DenyAll***: deniega el permiso a todos los usuarios.

A continuación, se muestran algunos ejemplos de configuraciones, que pueden ir dentro del fichero *proftpd.conf*

```
# permite entrar al servidor FTP a usuario1 y usuario2
# deniega el acceso al resto.
<Limit LOGIN>
        AllowUser usuario1
        AllowUser usuario2
        DenyAll
</Limit>
```

```
# modifica los permisos del directorio /var/ftp/carpeta1
<Directory /var/ftp/carpeta1>
        # da permisos de lectura a usuario1 y usuario2
        # impide la lectura de ficheros al resto
        <Limit READ>
                AllowUser usuario1
                AllowUser usuario2
                DenyAll
        </Limit>

        # da permisos de escritura a usuario1
        # impide la escritura de ficheros al resto
        <Limit WRITE>
                AllowUser usuario1
                DenyAll
        </Limit>
</Directory>
```

Siempre que se quiera configurar los permisos de un directorio de ProFTPD necesitaremos crear la directiva *<Directory>* e indicar la configuración de los permisos que queramos editar.

Tipos de usuarios y accesos al servicio

Hay dos tipos de usuarios dentro del servicio FTP:

- Usuario del **sistema**: usuario propio del sistema donde está el servicio FTP y que accede a su directorio personal.
- **Usuario anónimo**: usuario que no tiene contraseña de validación y de acceso público al servicio.

De este tipo de usuarios podemos especificar un tercero que deriva de los usuarios de sistema, llamados **usuarios virtuales**. La diferencia viene dada porque estos no son dependientes del sistema sino del servidor FTP directamente.

Para todos los usuarios que tienen acceso al servicio FTP se habilitarán permisos para poder manipular los ficheros y directorios del servicio. Estos permisos pueden ser lectura, escritura, listar, eliminar, etc. Son los que permiten trabajar con los directorios de acceso realizados en la configuración del servicio y los que permite la definición del protocolo.

Dentro de los tipos de usuarios diferenciaremos también los tipos de accesos al servicio.

Acceso anónimo.

Los servidores pueden ofrecer servicio libremente a todos los usuarios, acceder sin tener un identificador de usuario, leer y navegar por el contenido de los directorios libremente, independientemente de quien accede a él y del lugar donde lo hace.

El acceso anónimo es una forma cómoda de permitir que todos los clientes tengan acceso a cierta información sin que el administrador del servicio tenga que controlar las cuentas de usuarios.

La información con la que se trabaja en el acceso anónimo es de carácter público y se pueden leer los contenidos de los directorios, pero no eliminarlos ni modificarlos.

Normalmente, el contenido suele ser software de dominio público o de libre distribución, imágenes, sonido, videos, etc.

El requisito para acceder por acceso anónimo es mediante un nombre predefinido que existe en el servicio FTP y que debe estar configurado previamente.

Este usuario que permite el acceso anónimo se llama *anonymous*. Cuando se valida la conexión, el nombre del usuario que ponemos es *anonymous*, y sin contraseña (aunque pida una contraseña, no es necesario escribir nada o, si lo pide se puede poner cualquier correo electrónico como contraseña válida).

El acceso anónimo es un tipo de acceso que es inviable en el caso del despliegue web, donde el control de acceso de los usuarios es importante, ya que es de carácter privado, confidencial y depende también de nuestra aplicación web. Permitir un acceso al directorio raíz de la aplicación web con un acceso anónimo mediante FTP es una falta de seguridad.

Acceso por usuario identificado

Se da en casos de necesidad de privilegios y cuando la información con la que se trabaja es de índole privada. Se debe acceder al servicio mediante usuarios identificados dentro del servidor FTP.

Las cuentas de usuario pueden ser:

- Usuario de **sistema**: usuario definido dentro del sistema donde se ofrece el servicio.
- Usuario **virtual**: no tiene una relación directa con el sistema.

Todos estos usuarios tendrán configurado una serie de permisos dependiendo de la implicación que tengan los usuarios, por ejemplo

dentro del proyecto web. Puede ser conveniente tener usuarios que solo puedan leer la información del proyecto y otros que puedan actualizar los ficheros.

Usuario virtual en ProFTPD

Vamos a indicar como se crea un usuario virtual, así como el directorio destino donde se va a ubicar el usuario del FTP cuando se conecte.

Creamos el directorio:

mkdir /var/ftp

mk dir /var/ftp/miusuario1

A continuación, obtenemos el uid (User ID), es decir, la identificación del usuario FTP del sistema, mediante el comando:

id ftp

Obtenemos la salida siguiente en la que observamos que el uid FTP es 128, en nuestro caso.

```
uid=128(ftp) gid=65534(nogroup) grupos=65534(nogroup)
```

Para crear usuarios virtuales dentro de ProFTPD, ejecutamos la orden *ftpasswd*, que creará un fichero llamado *ftpd.passwd* en el directorio en que estemos situados (nosotros nos situaremos en */etc/proftpd*), en el que se almacenará la clave del usuario creado.

En nuestro caso vamos a crear un usuario llamado *miusuario1*, indicando como página de acceso el directorio creado anteriormente.

*sudo ftpasswd --passwd --name miusuario1 --home /var/ftp/miusuario1 --uid **128** --shell /bin/false*

Los parámetros introducidos indican lo siguiente:

--name: nombre del usuario a crear.

--***home***: directori0 de trabajo del usuario.

-- **uid**: User ID del usuario FTP.

-- **shell**: indicamos que no se requiere un Shell del sistema.

-- **file**: parámetro opcional en el que podemos indicar un fichero alternativo al fichero por defecto *ftpd.passwd*. Por ejemplo, */etc/proftpd/passwd.usuarios*.

Vamos a incluir contenido en el directorio del usuario, por ejemplo un fichero de texto.

sudo su

cat > bienvenida.txt

introducimos un texto, por ejemplo “Hola”

En el archivo *proftpd.conf* realizamos los cambios siguientes:

- Quitamos el comentario de la línea

  RequireValidShell off

- Indicamos el fichero de configuración de usuarios utilizado. En nuestro caso el fichero que se crea por defecto. Si hemos utilizado un fichero diferente mediante el parámetro file en el comando *ftpasswd*, sería ese fichero el que habría que indicar en *AuthUserFile*

  AuthUserFile /etc/proftpd/ftpd.passwd

Cambiamos la propiedad de la carpeta de usuario creada, para que sea propiedad del usuario ftp

chown -R ftp /var/ftp/miusuario1

En el archivo proftpd.conf tendremos que establecer los permisos que consideremos necesarios para el acceso de los diferentes usuarios a la carpeta del usuario creado.

Con la finalidad enjaular a todos los usuarios en sus respectivos directorios “home” y evitar que puedan navegar por las carpetas de servidor, habrá que editar el archivo proftpd.conf y eliminar el comentario en el comando indicado a continuación.

 # Use this to jail all users in their homes
DefaultRoot ~

Acceso al servidor ftp desde el cliente

Podemos acceder al servidor ftp desde el cliente de diversos modos:

- Explorador del sistema de ficheros.
  Indicamos como ruta de navegación:

  ftp://direccionIPdelServidor

  o bien

  ftp://direccionWeb

  También podemos utilizar
  ftp://nombredeusuario@direccionIPdelServidor

  En Linux puede resultar útil la opción *"Conectarse a un servidor …"* dentro del menú *Archivo* del navegador

- Cliente gráfico Filezilla

  Para instalar Filezilla ejecutamos

  sudo apt-get install filezilla

Control de usuarios conectados

Podemos expulsar a un usuario del servidor,para ello hay que con mirar el número de proceso en el que está y posteriormente matar el proceso:

```
root@linmintdaw:/etc/proftpd# ps aux | grep proftpd
proftpd     3665  0.0  0.2  23960  4548 ?        Ss   14:19   0:00 proftpd: (accepting connections)
ftp         3696  0.0  0.4  24452  9940 ?        SL   14:27   0:00 proftpd: user2 - 192.168.0.14: IDLE
root        3704  0.0  0.0  11660   728 pts/0    S+   14:29   0:00 grep --color=auto proftpd
```

Como vemos, hemos obtenido una lista de todos los procesos (usuarios) que están conectados y a su derecha su PID (en este ejemplo vamos a tirar a *user2*):

kill -9 3696

Para ver información acerca de los usuarios conectados, disponemos también de las siguientes órdenes, que nos proporcionan diferente tipo de información:

ftpcount muestra la cantidad de conexiones actuales.

ftptop muestra el estado de ejecución de las conexiones.

ftpwho muestra información sobre los procesos actuales para cada sesión.

Modos de conexión del cliente

El modo de transferencia se establece al inicio de las comunicaciones FTP y depende de cómo es el sistema de ficheros del servidor.

La mayoría de los sistemas hacen uso de la estructura de ficheros binarios, antiguos sistemas Unix y *mainframe* y pueden utilizar la estructura de ficheros ASCII. En cualquier caso, este modo se decide dentro del servidor FTP y el cliente automáticamente detectará cuál de los dos modos tiene que utilizar.

El protocolo FTP se basa en el protocolo TCP, con dos canales de datos con diferentes puertos, uno para enviar los datos y otro para enviar las órdenes.

Los puertos que se utilizan por defecto en el servidor son:

• Puerto número 21, para el canal de control

• Puerto número 20, para el canal de datos de transmisión

Dentro del protocolo FTP se definen dos modos de conexión que se configuran dentro del servicio, el modo ftp activo y el modo ftp pasivo.

- Modo FTP activo

En el modo FTP activo, el cliente conecta aleatoriamente por un puerto mayor de 1024 (llamémoslo N) hacia el puerto 21 de órdenes del servidor.

Para la transmisión de datos, el cliente inicia la escucha en el puerto (N+1). El servidor conecta de nuevo al cliente por el puerto de datos especificado por parte del cliente, que es el puerto 20 del servidor.

Cuando se trabaja en modo activo se tiene en cuenta el cortafuegos del sistema. El cortafuegos debe tener los puertos abiertos de trabajo del servidor y del cliente, para poder establecer comunicaciones.

Puertos que se abrirán en modo activo dentro del servidor:

• El cliente conecta con el puerto 21 del servidor FTP por un puerto mayor de 1024 del cliente: N. Iniciación de la conexión por parte del cliente.

• El puerto 21 del servidor FTP responde al puerto de control N del cliente.

• El puerto 20 del servidor FTP conecta a un puerto más grande de 1024 (N+1). El servidor inicia la conexión de datos hacia el puerto de datos del cliente.

• El cliente conecta por un puerto más grande de 1024 (N+1) hacia el puerto 20 del servidor FTP. El cliente envía la conexión al puerto de datos del servidor FTP.

En la figura siguiente vemos de manera esquemática lo indicado anteriormente.

- Modo FTP pasivo

Para evitar que el servidor inicie la transmisión de datos hacia el cliente hay otro método de conexión llamado pasivo.

En el método FTP pasivo el cliente inicia las dos conexiones hacia el servidor, resolviendo el problema de control del cortafuego en el filtrado del puerto de datos en el servidor hacia el cliente.

El cliente, al iniciar la conexión FTP, coge un puerto aleatorio más grande de 1024, nos referiremos a él como N, para el establecimiento de la conexión, y el siguiente N+1, parta la transferencia de información.

El primer puerto N hace la conexión por el puerto 21 del servidor y evita que la transferencia de datos se realice por el puerto 20 del servidor. El servidor abre un puerto aleatorio P más grande de 1024 y lo devuelve al cliente. El cliente inicia el canal de datos del puerto (N+1) al puerto P del servidor.

Para controlar el cortafuegos en el servidor FTP en modo pasivo abriremos los puertos siguientes:

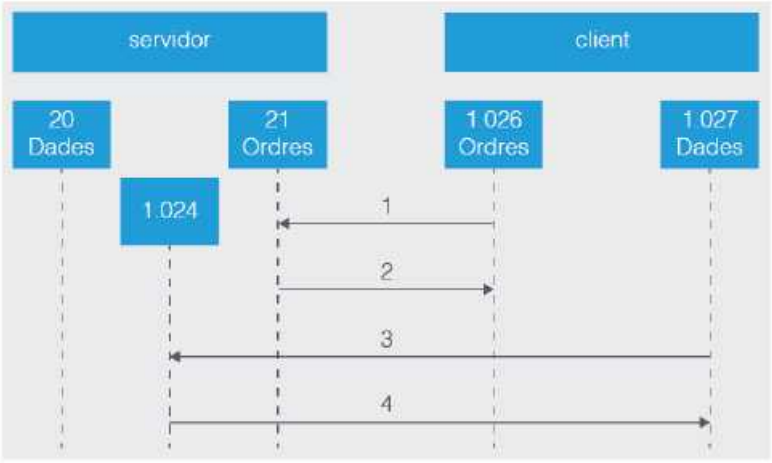
• El cliente conecta al puerto 21 del servidor FTP con un puerto más grande de 1024 del cliente (N). Inicio de la conexión por parte del cliente.

• El puerto 21 del servidor FTP responde al puerto de control N del cliente. El servidor responde al puerto de control del cliente.

• Un puerto más grande de 1024 (N+1) del cliente conecta a un puerto más grande de 1024 del servidor (P). El cliente inicia el canal de datos.

• Un puerto más grande de 1024 (P) del servidor conecta a un puerto más grande de 1024 del cliente (N+1).

En la figura siguiente vemos de manera esquemática lo indicado anteriormente.



Con el modo pasivo se resuelven muchos problemas del cliente, pero se trasladan los problemas al servidor. Uno de los principales problemas es la apertura de un gran rango de puertos en el servidor para poder iniciar canales de datos.

Una de las ventajas actualmente es que las implementaciones de servidores FTP permiten escoger el rango de puertos que se utilizarán.

Para realizar la configuración dentro de ProFTPD en el modo pasivo, hay que añadir dentro de la configuración del fichero */etc/proftpd/proftpd.conf* la directiva:

PassivePorts 1024 2000

El rango de puertos de configuración puede ir como mínimo del puerto número 1024 hasta, como máximo, el 65536.

Cuotas

ProFTPD permite configurar cuotas de espacio diferenciando entre:

- cuotas generales del servidor
- cuotas vinculadas a usuarios o grupos de trabajo.

Las cuotas generales del servidor permiten configurar:

- Restringir la velocidad de subida y descarga dentro del servidor FTP.
- Restringir el máximo de espacio de almacenamiento de un fichero en el servidor FTP.
- Restringir el máximo del tamaño del fichero que podemos descargar del

servidor.

Las cuotas de usuario o grupos de trabajo permiten:

- Restringir la velocidad de subida y de descarga del usuario o el grupo de trabajo.
- Restringir el máximo de espacio de almacenamiento de un fichero por parte del usuario o del grupo de trabajo.
- Restringir el máximo del tamaño del fichero que puede descargar el usuario o el grupo de trabajo.
- Restringir el espacio propio para almacenar datos en el directorio de configuración del usuario o del grupo de trabajo.