

TEMA 4.1. Prácticas FTP

Índice

1. Clientes FTP.....	1
1.1. Cliente FTP en línea de comandos.....	1
a) Ubuntu.....	1
b) Debian.....	3
c) Windows.....	3
2. Cliente ftp gráfico Filezilla.....	3
a) Windows.....	3
b) Linux.....	5
3. Navegadores/exploradores como clientes FTP.....	5
2. Instalación de Filezilla Server en Windows.....	5
3. Configuración de Filezilla Server en Windows.....	6
4. Instalación y configuración por defecto del servidor vsftpd para Linux.....	14
5. Configuración básica del servidor vsftpd en Linux Debian.....	17
6. Configuración de un servidor FTP para que acepte conexiones en modo pasivo detrás de un cortafuegos NAT.....	18
6.1. Configurar modo pasivo en Filezilla Server:.....	19
6.2. Configurar modo pasivo en vsftp.....	20
6.3. Conectarse desde un cliente externo usando el modo pasivo.....	20
7. VSFTP seguro.....	22
7.1. FTPS con vsftpd.....	22
7.2. FTPS con Filezilla.....	26

Los clientes FTP se pueden clasificar según la interfaz de usuario que ofrecen. En esta práctica vamos a probar varios clientes FTP para descargar archivos de un servidor FTP público.

1. Clientes FTP

1.1. Cliente FTP en línea de comandos

a) Ubuntu

1.1. Iniciar sesión en **Ubuntu3** con el usuario alumno (si no existe, iniciar sesión como administrador y crear el usuario con *adduser alumno*). **Ubuntu1** debe estar arrancado y con NAT funcionando.

1.2. Crear un directorio llamado "**pruebasFTP**" dentro de la carpeta home del usuario alumno y muévete a él.

1.3. Dentro del directorio "pruebasFTP", crear tres archivos "**datos1.txt**", "**datos2.txt**" y "**fich1.txt**", todos con contenido.

1.4. Conectarse vía FTP línea de comandos al sitio <ftp.rediris.es> usando el usuario anonymous:

```
ftp ftp.rediris.es
```

a) Introducir el usuario anonymous si lo pide.

b) Dejar la contraseña en blanco si la pide.

1.5. Ejecuta el comando **?** para mostrar los comandos ftp disponibles

```
ftp>?
```

1.6. Ejecuta el comando **pwd** para ver la ruta en la que te encuentras en el servidor.

```
ftp> pwd
```

1.7. Ejecuta el comando **!pwd** para ver la ruta en la que te encuentras en el cliente (debe ser /home/alumno/pruebasFTP). Recordar que los comandos que se ejecutan con el símbolo ! delante se ejecutan en el cliente, excepto el comando cd que para ejecutarse en local hay que usar lcd y no !cd).

```
ftp>!pwd
```

1.8. Ejecuta el comando **!ls** para ver un listado del directorio de la máquina local.

```
ftp>!ls
```

1.9. Ejecuta el comando **ls** para ver un listado del directorio de la máquina remota.

```
ftp>ls
```

Obtendrás un error de conexión debido a que entre el cliente y el servidor FTP existe un enrutador NAT. Es necesario ejecutar FTP en modo Pasivo y para ello tecleamos el comando "passive"

```
ftp>passive
```

```
ftp>ls
```

1.10. Descarga el fichero welcome.msg usando el comando get

```
ftp > get welcome.msg
```

1.11. Ejecuta el comando **!ls** para ver un listado del directorio donde estás en el cliente y comprobar que se ha descargado el fichero.

```
ftp> !ls
```

1.12. Desde el cliente ftp, crea un directorio llamado **imagenes** (dentro del directorio pruebasFTP) usando !mkdir. Muévete al nuevo directorio.

```
ftp > !mkdir imagenes
```

```
ftp > lcd imagenes
```

1.13. Vuelve al directorio pruebasFTP y sube el fichero "**fich1.txt**" al servidor usando el comando put.

```
ftp > lcd..
```

```
ftp > put datos1.txt
```

¿Se ha subido el fichero al servidor? ¿Por qué?

¿Qué comando usarías para subir al servidor los ficheros "datos1.txt" y "datos2.txt" a la vez?

1.14. Cierra la conexión ftp con el comando bye.

b) Debian

Debian 10 no tiene instalado ningún cliente FTP por defecto. Se puede instalar el cliente "lftp" que funciona prácticamente igual que el cliente ftp de ubuntu, pero usando el comando "lftp" en vez de "ftp":

```
apt-get install lftp
```

```
lftp ftp.rediris.es
```

Volver a hacer los pasos desde 1.5 hasta el final del apartado anterior en la máquina debian2. Tener en cuenta que "lftp" detecta por defecto que el servidor debe funcionar en modo pasivo y no hace falta indicárselo.

c) Windows

Windows 7 sí tiene instalado un cliente ftp desde línea de comandos, que funciona de modo similar a los anteriores, aunque algunos comandos cambian. Probar los pasos anteriores en Windows04 indicando los comandos que cambian. TENER EN CUENTA QUE EL CLIENTE FTP DE WINDOWS NO PERMITE CAMBIAR AL MODO PASIVO, POR LO QUE MUCHAS COSAS NO SE PODRÁN HACER.

Para descargar ficheros podríamos conectarnos desde un navegador introduciendo la URL: *ftp:\\ftp.rediris.es*.

2. Cliente ftp gráfico Filezilla

a) Windows

Filezilla (<http://filezilla-project.org>) es una solución FTP libre que ofrece tanto un cliente FTP gráfico multiplataforma como un servidor FTP para windows. Ambos se distribuyen bajo licencia GNU. En esta práctica vamos a instalar el cliente FTP en una máquina Windows :

2.1. Inicia sesión en **Windows04** con un usuario **administrador**.

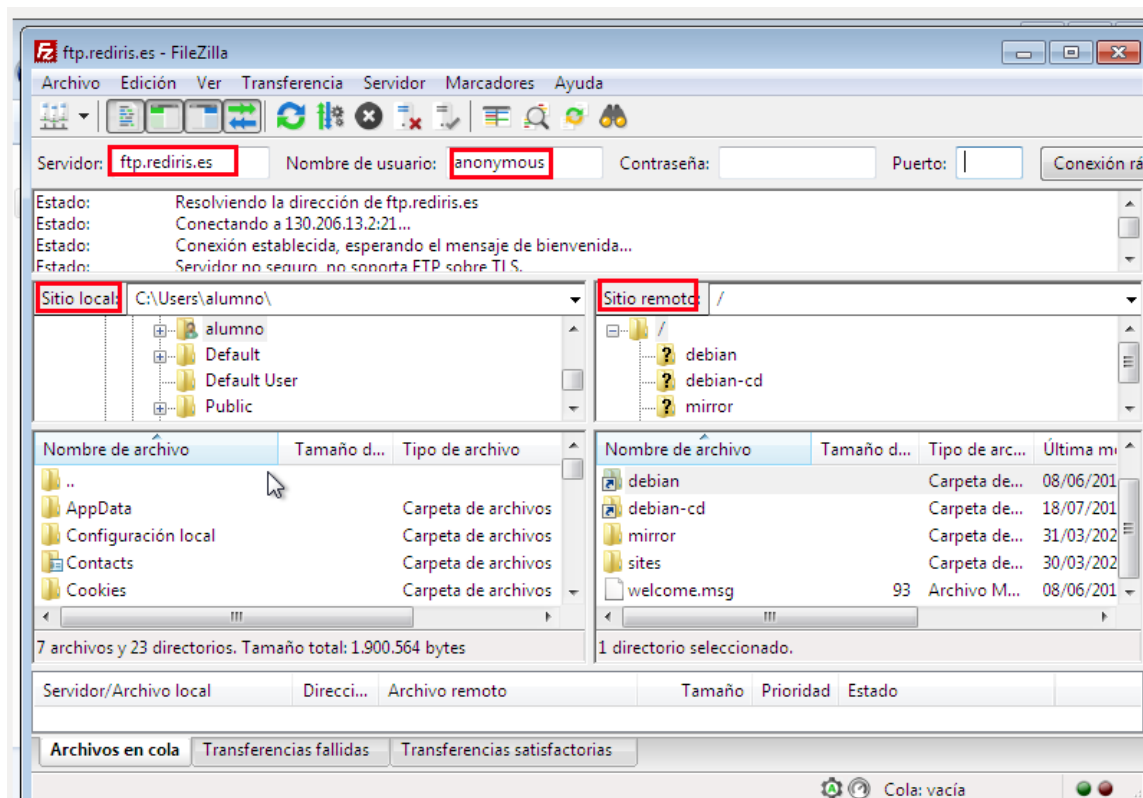
2.2. Crea la carpeta **c:\pruebasFTP** y dentro crea un fichero de texto **datos1.txt** con contenido.

2.3. Accede a la web de Filezilla y descarga el **cliente FTP**.

2.4. Instala el cliente con las opciones por defecto.

2.5. Inicia Filezilla y establece una conexión con ftp.rediris.es con el usuario **anonymous**:

- En el cuadro de texto Servidor introduce ftp.rediris.es
- En nombre de usuario introduce anonymous (o también se puede dejar en blanco, ya que es el usuario que se usa por defecto). Se usa por defecto el puerto 21.
- Haz click en conexión rápida.
- Fijarse en el mensaje sobre TLS que nos muestra. Aceptarlo.
- Una vez establecida la conexión puedes ver los mensajes del protocolo FTP intercambiados entre cliente y servidor en el área superior.
- En el panel izquierdo se muestran los ficheros y directorios del cliente (sitio local), y en el derecho vemos los ficheros y directorios del servidor FTP (sitio remoto).
- ¿Qué modo ha usado el cliente para descargar el listado de ficheros del servidor, activo o pasivo?

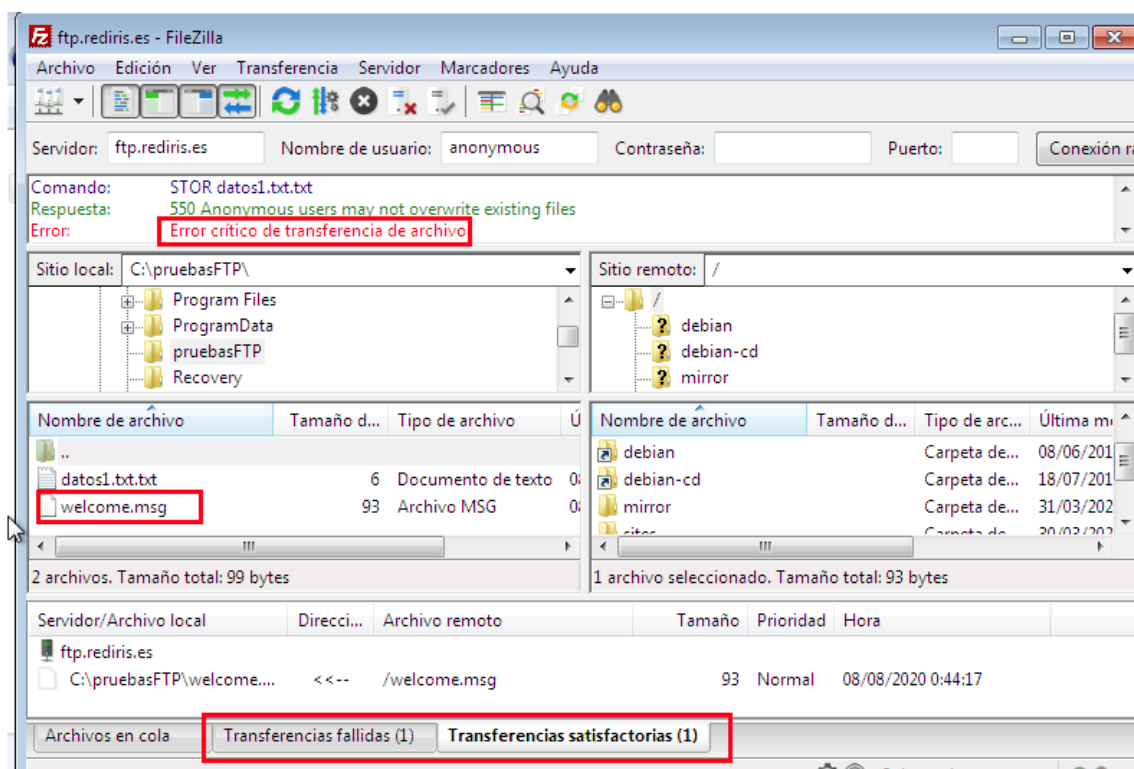


2.6. Descarga el fichero **welcome.msg** en la carpeta [c:\pruebasFTP](#)

- Accede a la carpeta [c:\PruebasFTP](#) en el Sitio Local
- Haz clic con el botón derecho sobre el fichero **welcome.msg** y selecciona **descargar**, pulsa doble click sobre él o arrástralo a la carpeta **pruebasFTP** del directorio local.

2.7. Sube el fichero datos1.txt al servidor. ¿Se sube? ¿Por qué?

2.8. Observa el resumen de transferencias fallidas y satisfactorias en el panel inferior.



2.9. Cierra el cliente FTP.

b) Linux

Instala el cliente FTP Filezilla en ubuntu3 ejecutando `sudo apt-get install filezilla`.

Realizar todos los pasos de la práctica anterior.

3. Navegadores\exploradores como clientes FTP

3.1. Inicia sesión en windows4 con un usuario administrador.

3.2. Descargar Mozilla Firefox si no está instalado.

3.3. Abrir Firefox e introducir la URL <ftp://ftp.rediris.es> para establecer una conexión con el usuario **anonymous**.

3.4. Descargar el fichero welcome.msg en la carpeta [c:\PruebasFTP](#).

3.3. Accede a **Inicio, Equipo** y en la barra de direcciones introduce la URL <ftp://ftp.rediris.es> para establecer una conexión con el usuario **anonymous**.

3.4. Mover el archivo welcome.msg a la carpeta **Documentos**

3.5. Inicia sesión en Ubuntu03.

3.6. Acceder al menú **Lugares, Conectar con el servidor** e introducir la URL <ftp://ftp.rediris.es>. Haz click en conectar.

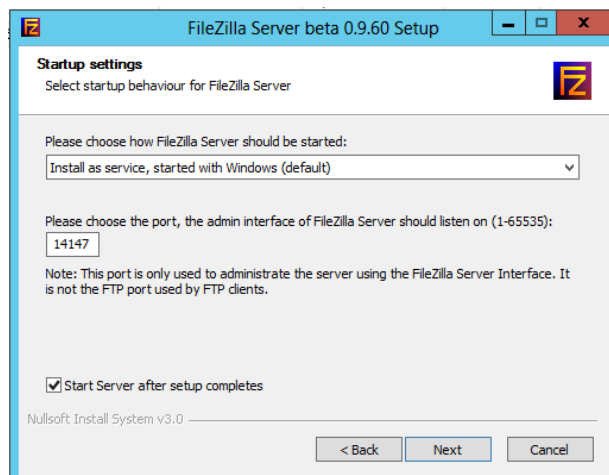
3.7. Observa que se ha montado una carpeta en el escritorio con acceso al servidor FTP.

3.8. Desmonta la carpeta haciendo clic con el botón derecho del ratón sobre ella.

2. Instalación de Filezilla Server en Windows Server 2012

Accede a la web de Filezilla (<http://filezilla-project.org>) y descarga la última versión del apartado **Filezilla Server**. Instala el servidor FTP en Wserver2012 como un servicio que se arranque manualmente. Configura como puerto de administración el 14147 (el que se propone por defecto) e instala la herramienta de administración del servidor.

1. Instalar la aplicación con las opciones por defecto (fijarse en las opciones de la ventana "Startup settings" (*Install as a service y puerto 14147*)).



2. Una vez instalado, se abrirá el interfaz de administración y nos ofrecerá conectarnos al equipo local (localhost) y al puerto 14147. Lo hacemos (nos lo permite aunque dejemos la contraseña en blanco).

3. Acceder a **Inicio, Herramientas administrativas, Servicios** y comprobar que se ha creado un servicio asociado al servidor Filezilla (Filezilla Server FTP server) que se inicia automáticamente. Observa que está iniciado.

4. Abre un terminal y ejecuta el comando **netstat -a -p TCP -n** y observa que los puertos TCP 21 y 14147 están a la escucha.

3. Configuración de Filezilla Server en Windows

Configurar el servidor Filezilla con las siguientes opciones:

- Se permitirán un máximo de **2 conexiones simultáneas** al servidor.
- Cuando un usuario accede al servidor como cliente tiene **un máximo de un minuto** para hacer *login*.
- Si un cliente conectado no inicia una transferencia en 1 minuto (**tiempo de inactividad**) o menos, se le desconectará.
- El **mensaje de bienvenida** del servidor será "Bienvenido al servidor FTP Filezilla de la red virtual".
- No se permitirán conexiones desde la IP 10.33.1.2.
- Para administrar el servidor FTP, la interfaz de administración usará el puerto 14147 y se podrá acceder desde el equipo local (donde está instalado Filezilla Server). Para acceder a través de la interfaz se usará la contraseña "Clave_00".
- Se habilitará el log del servidor con ficheros de 200 KB como máximo. Se usará un fichero de log para cada día y se borrarán los ficheros de logs con más de 10 días de

antigüedad.

- La velocidad de descarga del servidor será de 10 KB/s como máximo de lunes a viernes y el fin de semana la velocidad será la máxima permitida. Respecto a la velocidad de subida será de 5 KB/s de lunes a viernes y de 15 KB/s el fin de semana.
- Se “banearán” durante 2 horas las conexiones desde direcciones IP que fallen 10 veces en la autenticación al conectarse al servidor.
- Se crearán los siguientes usuarios:
 - Usuario anónimo (usuario **anonymous** sin contraseña)-
 - Directorio predeterminado **c:\ftp\pub**). El usuario solo tendrá permisos de lectura, es decir, de descarga de archivos.
 - No pertenece a ningún grupo.
 - Usuario **profesor** (con contraseña):
 - Directorio predeterminado **c:\ftp**. El usuario tendrá permisos de lectura, escritura, borrado y modificación de ficheros y directorios.
 - El usuario también tendrá acceso con todos los permisos a la carpeta **c:\ftp2** usando el alias “**carpeta2**”
 - No pertenece a ningún grupo.
 - Usuarios **alumno1** y **alumno2** (con contraseña):
 - Pertenecerán al grupo **alumnos**.
 - El directorio predeterminado para todos los miembros del grupo alumnos es **c:\ftp\alumnos**, y todos tendrán permisos de lectura y escritura de ficheros y directorios.
 - La velocidad de subida para todos los alumnos será de 2 KB/s.

Conectarse al servidor desde clientes FCP instalados en otros equipos de la red y comprobar que se cumple la configuración realizada.

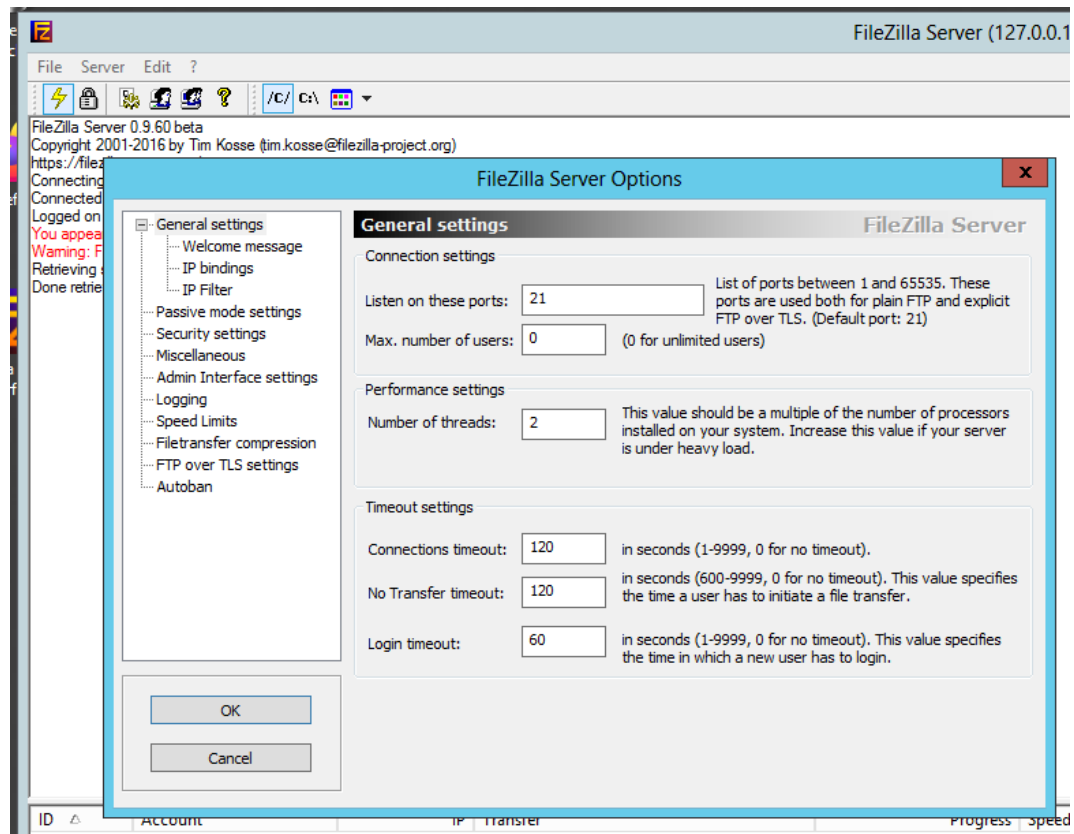
1. Configuración global del servidor

1.1. Iniciar sesión en el servidor con un usuario administrador.

1.2. Comprobar que el servidor FTP está iniciado. Si no es así, arrancarlo en **Inicio, Filezilla Server Interface**, pulsando el botón “Connect”.

1.3. En la barra de tareas acceder a Edit, Settings para configurar las opciones globales del servidor.

1.4. Navegar a través de las opciones para realizar la configuración solicitada:



- a. En *General Settings*, *Max number of users*, introducir 2.
- b. En *General Settings*, *Login Timeout*, introducir 60
- c. En *General Settings*, *No Transfer Timeout*, introducir 60.
- d. En *General Settings*, *Welcome Message*, introducir el mensaje "Bienvenido al servidor FTP Filezilla de la red virtual".
- e. En *General Settings*, *IP filter*, *the following IP addresses are not allowed to connect to the server*, introduce 10.33.1.2 para no permitir conexiones desde esta dirección.
- f. En *Admin Interface Settings* introduce la contraseña de acceso "Clave_00" y deja el puerto por defecto.
- g. En *Loggin* habilita "Enable logging to file", habilita "Limit log file size to" e introduce 200, habilita "Use a different logfile each day" y "Delete old logfiles after" e introduce 10.
- h. En *Speed Limits* habilita "Use Speed limits rules" en "Download Speed Limit" y añade una regla de 10 KB/s de lunes a viernes.
- i. En *Speed Limits* habilita "Use Speed limits rules" en "Upnload Speed Limit" y añade una regla de 5 KB/s de lunes a viernes y otra de 15 KB/s el sábado y el domingo.
- j. En *Autoban* habilita "Enable automatic bans" e introduce 10 y 2 respectivamente para "banear" durante 2 horas a las conexiones desde direcciones IP que fallen 10 veces en la autenticación al servidor.

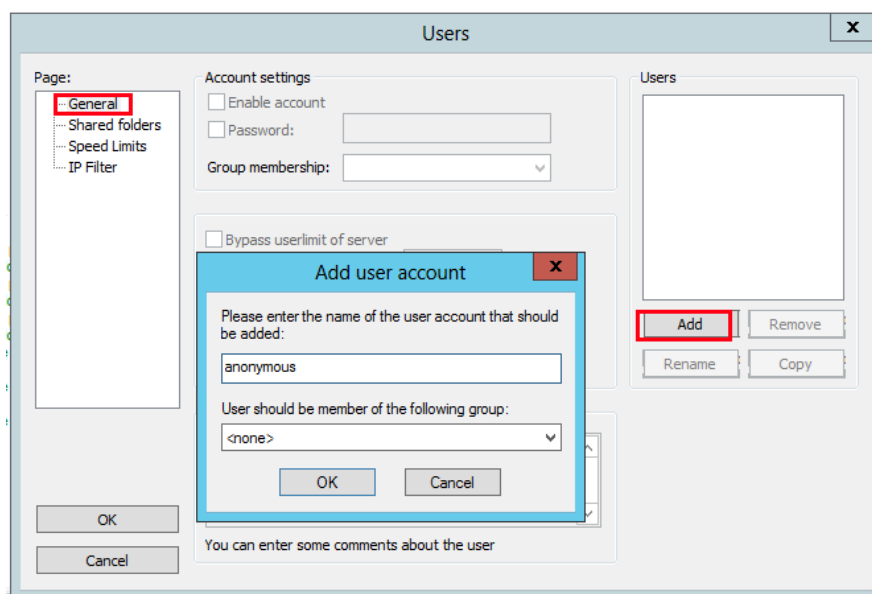
2. Configuración de usuarios y grupos

El servidor FTP Filezilla sólo permite crear usuarios virtuales, es decir, los usuarios con los que se pueden establecer conexiones FTP son usuarios propios del servidor FTP y no del sistema operativo donde se ejecuta. Otro aspecto a tener en cuenta es que los usuarios están “enjaulados” en su directorio predeterminado cuando se conectan por FTP.

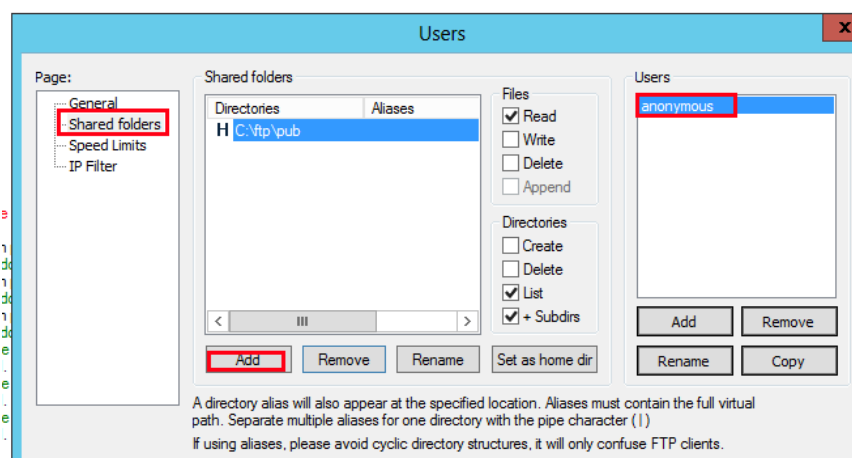
2.1. Crear los directorios **c:\ftp**, **c:\ftp\pub**, **c:\ftp\alumnos** y **c:\ftp2** en el equipo. Crear varios ficheros con contenido dentro de los directorios.

2.2. En la barra de tareas de **Filezilla Server** acceder a **Edit, Users** para configurar los usuarios virtuales y sus privilegios.

2.3. En la página **General**, hacer click en **Add** y crear el usuario **anonymous** sin que pertenezca a un grupo (none).

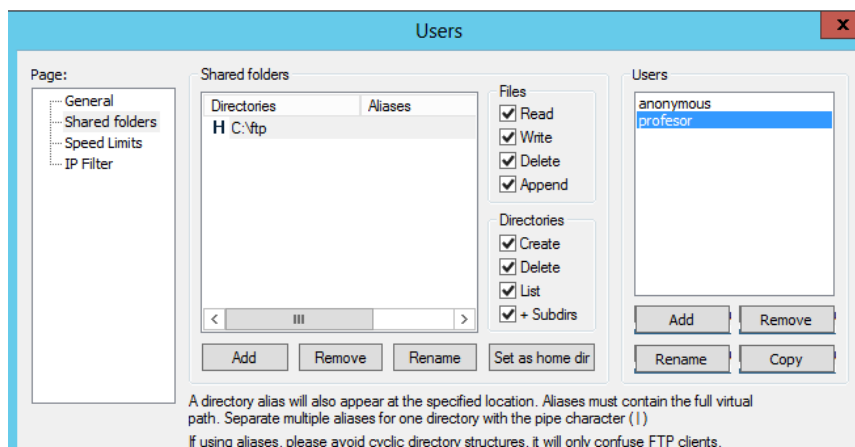


2.4. Con el usuario **anonymous** seleccionado accede a la página **Shared Folders**, haz clic en **Add**, selecciona el directorio **c:\ftp\pub** y deja los permisos por defecto (sólo permiso de lectura para ficheros).



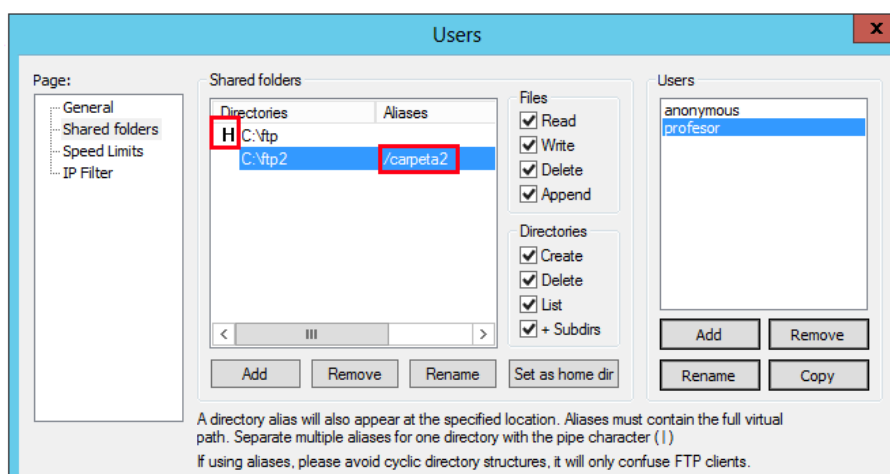
2.5. Accede a la página **General**, haz click en **Add** y crea el usuario **profesor**. Habilita la opción **Password** e introduce una contraseña

2.6. Con el usuario **profesor** seleccionado accede a la página **Shared Folders**, haz clic en **Add**, selecciona el directorio **c:\ftp** y marca TODOS los permisos.



También desde **Shared Folders**, haz clic en **Add**, selecciona el directorio **c:\ftp2** y marca TODOS los permisos. Una vez añadido el directorio, pulsar doble clic en la casilla "Aliases" y añadir el nombre que vamos a usar para acceder a esta carpeta (/carpeta2), y aceptar.

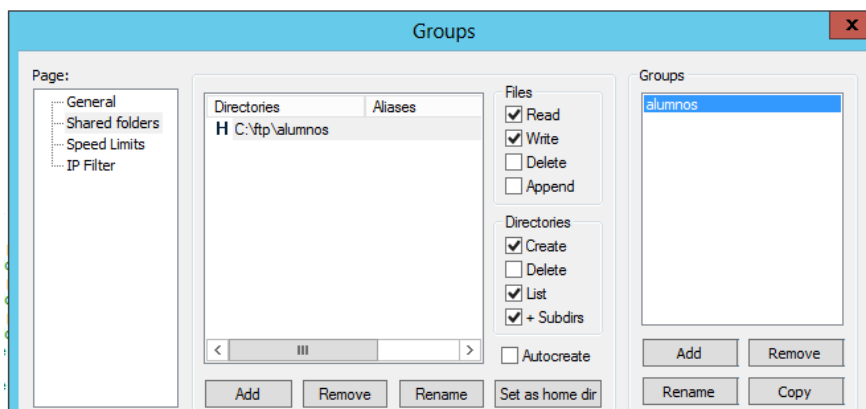
Fijarse que la carpeta **c:\ftp** lleva una **H** por delante y **c:\ftp2** no. La razón es que la carpeta **c:\ftp** es la carpeta por defecto del usuario profesor, es decir, la carpeta a la que accederá por defecto cuando se conecte al servidor Filezilla desde otro equipo.



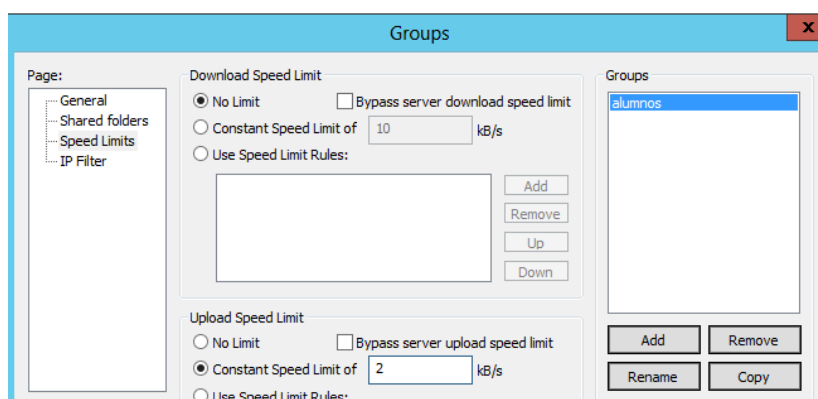
2.7. En la barra de tareas, accede a **Edit, Groups** para configurar los grupos virtuales y sus privilegios.

2.8. En la página **General**, haz clic en **Add** y crea el grupo **alumnos**.

2.9. Con el grupo alumnos seleccionado, accede a la página **Shared Folders**, haz clic en **Add**, selecciona el directorio **c:\ftp\alumnos** y marca los permisos *read* y *write* para ficheros y *create*, *list* + *subdirs* para directorios.



2.10. Con el grupo **alumnos** seleccionado, accede a la página **Speed Limits** y establece como velocidad de subida 2 KB/s.



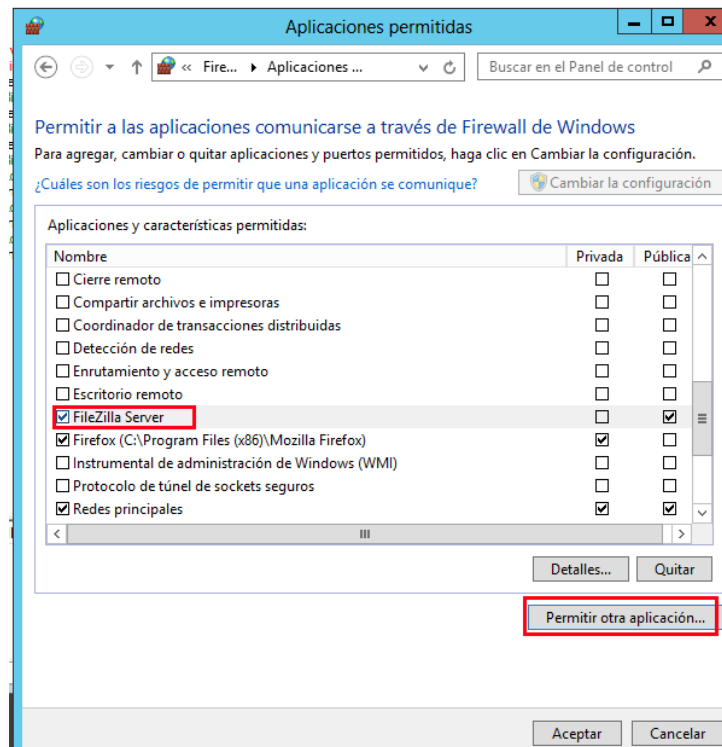
2.11. En la barra de tareas, accede a Edit, Users para crear los usuarios **alumno1** y **alumno2**, pertenecientes al grupo **alumnos**. Habilitar la opción Password e introducir una contraseña para cada uno.

3. Configuración del firewall de w2012

Debemos configurar el firewall para que permita las conexiones al servidor FTP. Utilizaremos la opción "dejar pasar un programa" que configura adecuadamente los puertos de entrada y salida.

3.1. Acceder al Firewall de Windows (*Panel de Control, Sistema y Seguridad, Permitir una aplicación a través de Firewall de Windows*).

3.2. Hacer clic en el botón **Permitir otra aplicación**, buscar y seleccionar **c:\Files(x86)Server\FilezillaServer \FilezillaServer.exe** y aceptar los cambios:



4. Comprobar la configuración

4.1. Iniciar sesión en Ubuntu1.

4.2. Usar el cliente FTP en modo línea de comandos para conectarse al servidor FTP de W2012 probando todos los usuarios (**anonymous**, **profesor**, **alumno1** o **alumno2**), fijándose en los ficheros que se ven desde cada usuario y subiendo y descargando ficheros. *No cerrar la conexión.*

*Cuando nos conectamos con el usuario "profesor", accedemos por defecto a la carpeta **c:\ftp**. Si hacemos un **ls**, comprobamos que tenemos una carpeta "carpeta2" (el alias que creamos para **c:/ftps**). Para cambiar a la otra carpeta haremos "**cd carpeta2**" y veremos el contenido de la carpeta **c:\ftp2**.*

```

administrador@administrador-VirtualBox: ~
/home/administrador
ftp> bye
221 Goodbye
administrador@administrador-VirtualBox:~$ ftp 10.33.1.100
Connected to 10.33.1.100.
220 Bienvenido al servidor FTP Filezilla de la red virtual
Name (10.33.1.100:administrador): profesor
331 Password required for profesor
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp          0 Aug 09 13:34 carpeta2
drwxr-xr-x 1 ftp ftp          0 Aug 09 00:35 alumnos
-rw-r--r-- 1 ftp ftp          4 Aug 09 00:08 fich-ftp1.txt.txt
-rw-r--r-- 1 ftp ftp          4 Aug 09 00:08 fich-ftp2.txt.txt
drwxr-xr-x 1 ftp ftp          0 Aug 09 00:09 pub
226 Successfully transferred "/"
ftp> cd carpeta2
250 CWD successful. "/carpeta2" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/carpeta2"
-rw-r--r-- 1 ftp ftp          4 Aug 09 13:34 fichero_carpeta_ftp2.txt.txt
226 Successfully transferred "/carpeta2"

```

4.3. Instalar Filezilla Client (sudo apt-get install filezilla) y acceder al servidor FTP desde esta herramienta.

4.3. Inicia sesión en **debian2** y usar el cliente **lftp** para comprobar que desde esta IP NO es posible conectarse al servidor FTP (lo hemos denegado).

```

lftp 10.33.1.100:~> ls
ls en 0 [550 No connections allowed from your IP]

```

4.4. Acceder de nuevo a la máquina **Ubuntu1** y abrir un terminal desde que el que ejecutaremos otra conexión al servidor FTP con algún usuario. Si no hemos cerrado la conexión anterior ya tenemos dos abiertas, el máximo de conexiones permitidas (puesto que así lo hemos configurado).

4.5. Abrir un terminal más en Ubuntu1 e intentar una nueva conexión al servidor FTP. Observar el mensaje obtenido:

```

administrador@administrador-VirtualBox:~$ ftp 10.33.1.100
Connected to 10.33.1.100.
220 Bienvenido al servidor FTP Filezilla de la red virtual
Name (10.33.1.100:administrador): alumno2
331 Password required for alumno2
Password:
421 Too many users are connected, please try again later.
Login failed.

```

4. Logs del servidor y usuarios conectados

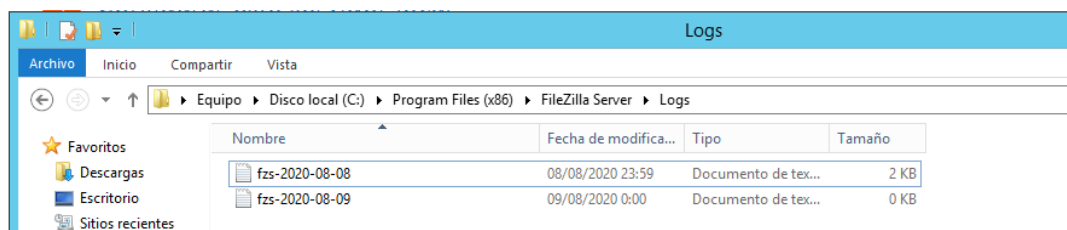
5.1. Acceder a W2012 y abrir la herramienta de administración de Filezilla. Observar los logs del servidor y los clientes conectados en el momento actual.

```

(000009)09/08/2020 0:41:21 - (not logged in) (10.33.1.1)> 220 Bienvenido al servidor FTP FileZilla de la red virtual
(000009)09/08/2020 0:41:23 - (not logged in) (10.33.1.1)> USER profesor
(000009)09/08/2020 0:41:23 - (not logged in) (10.33.1.1)> 331 Password required for profesor
(000009)09/08/2020 0:41:25 - (not logged in) (10.33.1.1)> PASS *****
(000009)09/08/2020 0:41:25 - profesor (10.33.1.1)> 230 Logged on
(000009)09/08/2020 0:41:25 - profesor (10.33.1.1)> SYST
(000009)09/08/2020 0:41:25 - profesor (10.33.1.1)> 215 UNIX emulated by FileZilla
(000010)09/08/2020 0:41:34 - (not logged in) (10.33.1.1)> Connected on port 21, sending welcome message...
(000010)09/08/2020 0:41:34 - (not logged in) (10.33.1.1)> 220 Bienvenido al servidor FTP FileZilla de la red virtual
(000010)09/08/2020 0:41:39 - (not logged in) (10.33.1.1)> USER alumno1
(000010)09/08/2020 0:41:39 - (not logged in) (10.33.1.1)> 331 Password required for alumno1
(000010)09/08/2020 0:41:42 - (not logged in) (10.33.1.1)> PASS *****
(000010)09/08/2020 0:41:42 - alumno1 (10.33.1.1)> 230 Logged on
(000010)09/08/2020 0:41:42 - alumno1 (10.33.1.1)> SYST
(000010)09/08/2020 0:41:42 - alumno1 (10.33.1.1)> 215 UNIX emulated by FileZilla
(000011)09/08/2020 0:41:46 - (not logged in) (10.33.1.1)> Connected on port 21, sending welcome message...
(000011)09/08/2020 0:41:46 - (not logged in) (10.33.1.1)> 220 Bienvenido al servidor FTP FileZilla de la red virtual
(000011)09/08/2020 0:41:49 - (not logged in) (10.33.1.1)> USER alumno2
(000011)09/08/2020 0:41:49 - (not logged in) (10.33.1.1)> 331 Password required for alumno2
(000011)09/08/2020 0:41:51 - (not logged in) (10.33.1.1)> PASS *****
(000011)09/08/2020 0:41:51 - (not logged in) (10.33.1.1)> Refusing connection. Reason: Max. connection count reached.
(000011)09/08/2020 0:41:51 - (not logged in) (10.33.1.1)> 421 Too many users are connected, please try again later.
(000011)09/08/2020 0:41:51 - (not logged in) (10.33.1.1)> disconnected.
(000009)09/08/2020 0:43:26 - profesor (10.33.1.1)> 421 Connection timed out.
(000009)09/08/2020 0:43:26 - profesor (10.33.1.1)> disconnected.
(000010)09/08/2020 0:43:43 - alumno1 (10.33.1.1)> 421 Connection timed out.
(000010)09/08/2020 0:43:43 - alumno1 (10.33.1.1)> disconnected.
(000012)09/08/2020 0:45:54 - (not logged in) (10.33.1.1)> Connected on port 21, sending welcome message...
(000012)09/08/2020 0:45:54 - (not logged in) (10.33.1.1)> 220 Bienvenido al servidor FTP FileZilla de la red virtual

```

5.2. Accede a la carpeta `c:\Program Files (x86)\Filezilla Server\Logs` y observa los ficheros de log creados.



4. Instalación y configuración por defecto del servidor vsftpd para Linux

Instalar, analizar y probar la configuración por defecto del servidor vsftpd en **debian2** (la configuración para ubuntu sería similar).

Very Secure FTP Daemons (vsftpd) es un servidor FTP rápido, seguro y fácil de configurar que **se distribuye con licencia GNU para sistemas Unix y Linux**.

1. Instalación

1.1 Abrir un terminal e instalar vsftpd desde los repositorios de Debian:

```
apt-get update
```

```
apt-get install vsftpd
```

Al instalar el servidor se crean:

- Los archivos de configuración
- El usuario **ftp** que se incluye en el grupo **ftp**
- El directorio **/srv/ftp**
 - Su propietario es el usuario **root** y el **grupo ftp**
 - Es el directorio predeterminado de los usuarios anónimos.

1.2. Comprobar que se ha creado el usuario **ftp** y que su directorio es **/srv/ftp**

```
cat /etc/passwd
```

```
cat /etc/group
```

1.3. Comprobar también que se ha creado el directorio **/srv/ftp** y que su propietario es el usuario **root** y grupo **ftp**

```
ls -l /srv
```

1.4. vsftpd se configura editando archivos de configuración. Comprobar que se ha creado el archivo de configuración principal del servidor y consultar su contenido:

- **/etc/vsftpd.conf**
 - Es el fichero de configuración principal.
 - Contiene un conjunto de directivas que determinan el comportamiento del servidor.
 - Cada directiva tiene el formato `<directiva>=<valor>`.
 - Las directivas pueden tener valores booleanos (YES o NO), numéricos o de texto.
 - **IMPORTANTE:** No debe haber espacios antes del signo `"="`.
 - Los comentarios son a nivel de línea con el símbolo `#`
 - Las directivas que no se especifiquen en el fichero de configuración usan su valor por defecto.
 - Con *man vsftpd.conf* se puede obtener información sobre todas las directivas.
- Otros ficheros de configuración:
 - Su nombre y ubicación se pueden definir en las directivas de **/etc/vsftpd.conf**.
 - Algunos que usaremos en las prácticas son:
 - **/etc/ftpusers**
 - **/etc/vsftpd.user_list** (no está creado por defecto)
 - **/etc/vsftpd.chroot_list** (no está creado por defecto)

1.5. Comprobar que el servidor está iniciado:

```
ps -ef|grep vsftpd
```

1.6. Comprobar que el servidor está escuchando en el puerto TCP 21

```
netstat -ltn
```

1.7. Hacer una copia de seguridad del fichero de configuración principal que se modificará en las prácticas (**/etc/vsftpd.conf**)

2. Usuarios y preparación para probar el servidor

vsftpd permite la conexión de:

- **Usuarios anónimos**
 - Si está habilitado (directiva ***anonymous_enable***), el servidor *vsftpd* permite la conexión de usuarios anónimos con el nombre de usuarios ***anonymous*** o ***ftp***.
 - Cuando se conecta un usuario anónimo el servidor entra en el directorio especificado en */etc/passwd* para el usuario ***ftp*** (por defecto ***/srv/ftp***).
 - Este directorio es, a efectos del usuario anónimo, su directorio raíz. Está "enjaulado"

en él.

- **Usuarios locales con cuenta en el sistema (/etc/passwd)**
 - Si está habilitado (directiva **local_enable**), el servidor vsftpd permite la conexión de usuarios locales con cuenta en el sistema.
 - Cuando se conecta un usuario local, hay dos opciones de configuración:
 - Que no se le "enjaule" en su directorio **home**. En este caso el usuario podría acceder al resto del árbol de directorios en función de los permisos definidos.
 - Que se le "enjaule" en su directorio **home**. No tendría disponible el resto del sistema de archivos.
- **Usuarios virtuales**
 - Es posible crear cuentas de usuarios virtuales (que no existan en el sistema operativo).
 - Las cuentas de usuario se almacenan en ficheros o en bases de datos, servicios de directorio, etc., y pueden ser consultados por el servidor para realizar la autenticación.
 - Las cuentas virtuales se mapean en un usuario local del sistema.

Vamos a crear usuarios locales en el sistema para probar posteriormente el funcionamiento del servidor:

2.1. Acceder al directorio /srv/ftp y crea tres archivos de texto.

2.2. Crea los usuarios locales mortadelo y filemon

```
adduser mortadelo
```

```
adduser filemon
```

2.3. Iniciar sesión como usuario **mortadelo** y crea en su home dos archivos de texto. Cerrar la sesión.

2.4. Iniciar sesión como usuario **filemon** y crea en su home dos archivos de texto. Cerrar la sesión.

3. Configuración por defecto

La configuración del servidor **Debian** por defecto es:

- Permite solo el acceso a usuarios locales (*local_enable=YES, anonymous_enable=NO*).
- Los usuarios NO están enjaulados (pueden navegar por los directorios).
- Los usuarios pueden descargar ficheros que tengan permisos de lectura para "otros".
- No pueden subir archivos (*write_enable=NO* o comentada)
- El servidor usa todo el ancho de banda disponible.
- El fichero de logs por defecto es **/var/log/vsftpd.log**

3.1. Inicia sesión en debian2 con usuario root

3.2. Consultar el fichero de configuración /etc/vsftpd.conf y comprobar que:

- Está habilitado el acceso a los usuarios locales y deshabilitado el acceso a los usuarios anónimos (*si hubiésemos instalado vsftpd en Ubuntu sería al contrario*):

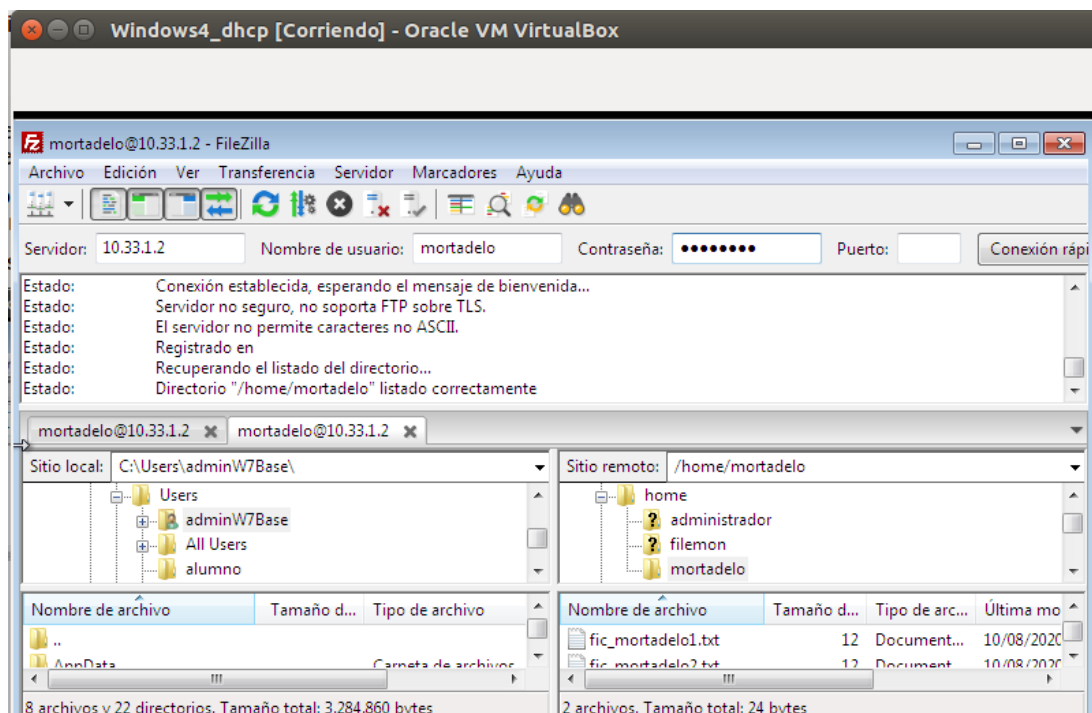
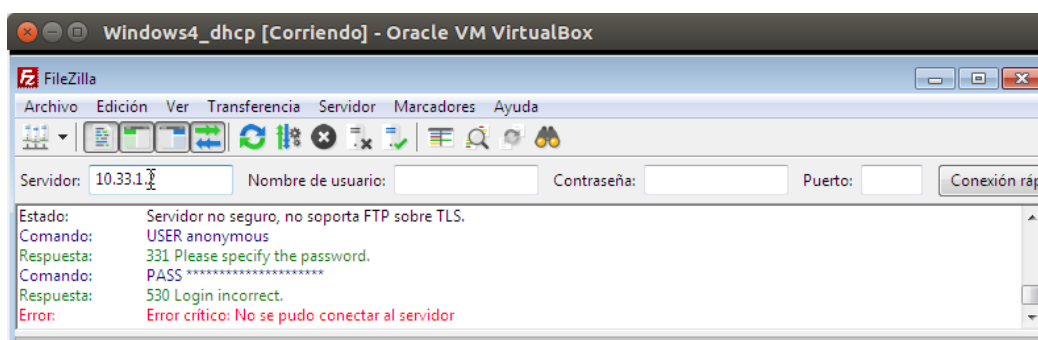

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
```

- No se permite subir archivos al servidor (directiva write_enable=NO o comentada):

```
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
```

3.3. Inicia sesión en Ubuntu1 u otra máquina de la red y conéctate al servidor ftp usando el cliente ftp que quieras. Verifica que:

- a) Es posible acceder con un usuario local y descargar archivos. Comprobar que el usuario administrador no está enjaulado (puede navegar por carpetas superiores a la suya) y que no se pueden subir ficheros.
- b) No es posible conectarse con los usuarios anónimos **anonymous** y **ftp**.



4. Logs del servidor

Consultar el fichero /var/log/vsftpd.log y observa los accesos al servidor y las transferencias

realizadas.

```

debian2_DHCP [Corriendo] - Oracle VM VirtualBox
Sun Aug 9 23:10:32 2020 [pid 933] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:10:44 2020 [pid 932] [root] FAIL LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:11:21 2020 [pid 939] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:11:26 2020 [pid 938] [mortadelo] OK LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:11:39 2020 [pid 944] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:11:45 2020 [pid 943] [anonymous] FAIL LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:11:57 2020 [pid 948] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:12:00 2020 [pid 947] [ftp] FAIL LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:13:39 2020 [pid 961] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:13:45 2020 [pid 960] [mortadelo] OK LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:14:06 2020 [pid 967] CONNECT: Client "::ffff:10.33.1.1"
Sun Aug 9 23:14:11 2020 [pid 966] [mortadelo] OK LOGIN: Client "::ffff:10.33.1.1"
Sun Aug 9 23:14:23 2020 [pid 970] [mortadelo] OK DOWNLOAD: Client "::ffff:10.33.1.1", "/home/mortadelo/fic_mortadelo1.txt", 12 bytes, 1.39Kbyte/sec
Sun Aug 9 23:14:24 2020 [pid 970] [mortadelo] OK DOWNLOAD: Client "::ffff:10.33.1.1", "/home/mortadelo/fic_mortadelo1.txt", 12 bytes, 1.39Kbyte/sec

```

5. Configuración básica del servidor vsftpd en Linux Debian

Configura el servidor *vsftpd* instalado en *debian02* con las siguientes opciones:

- Se permitirá la conexión a los usuarios anónimos
- Los usuarios locales podrán descargar y subir archivos.
- Los usuarios locales están "enjaulados" en su directorio home.

Conectarse al servidor FTP desde clientes FTP instalados en otros equipos de la red y comprobar que se cumple la configuración realizada.

5.1. Iniciar sesión en *debian02* con usuario *root*.

5.2. Modificar el fichero de configuración del servidor para que los usuarios anónimos puedan conectarse al servidor:

```
anonymous_enable=YES
```

5.3. Reinicia el servidor para que se lea de nuevo el fichero de configuración y se apliquen los cambios:

```
/etc/init.d/vsftpd stop
/etc/init.d/vsftpd start
```

5.4. Comprobar que el servidor está iniciado (si hay errores en el fichero de configuración el servidor no se iniciará).

```
ps -ef|grep vsftpd
```

5.5. Inicia sesión en *Window4* o *ubuntu1* y conéctate al servidor ftp usando el cliente FTP que quieras. Verifica que:

- Es posible acceder como usuario anónimo (**anonymous** o **ftp**) y descargar archivos.
- El usuario anónimo está enjaulado.

5.6. Modifica el fichero de configuración del servidor para que los usuarios locales puedan subir archivos al servidor:

```
write_enable=YES
```

5.7. Reinicia el servidor para que se lea de nuevo el fichero de configuración y se apliquen los cambios.

5.8. Volver a conectarse al servidor ftp desde un cliente. Verificar que al usar el usuario **mortadelo** ya se pueden subir ficheros.

5.9. Modificar el fichero de configuración del servidor ftp para que los usuarios locales sean "enjaulados" en su directorio home, es decir, que no puedan navegar por otros directorios:

```
chroot_local_user=YES
```

```
allow_writeable_chroot=YES
```

5.10. Comprobar que ahora la conexión con usuarios locales está "enjaulada".

6. Configuración de un servidor FTP para que acepte conexiones en modo pasivo detrás de un cortafuegos NAT

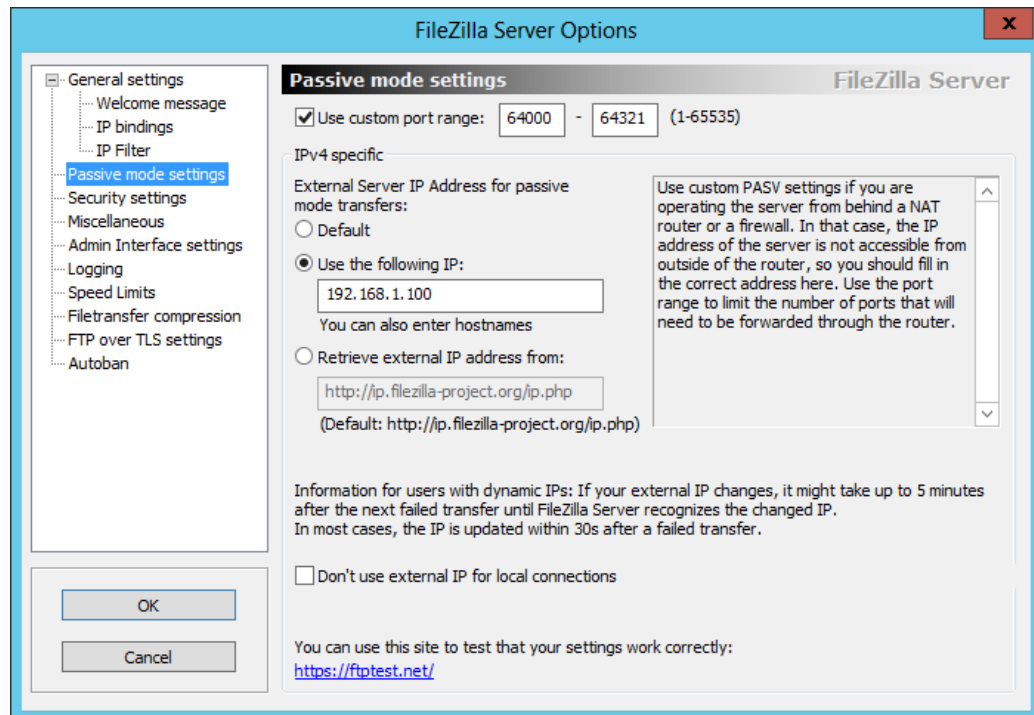
Configurar los servidores FTP instalados (Filezilla en W2012 y vsftp en Debian02) para que acepten conexiones en modo pasivo desde equipos que no estén dentro de la red virtual (por ejemplo, desde la máquina real o desde otro equipo del aula). Para ello debemos:

- Configurar en el servidor:
 - Habilitar el modo pasivo
 - Especificar el rango de puertos que se usarán para las conexiones de datos en modo pasivo.
 - Especificar la IP externa del router NAT que estamos usando (puesto que el cliente se conecta desde fuera de la LAN, lo hará a la IP pública o puente del equipo puerta de enlace. Esa es la IP que se debe especificar).
 - Si el firewall del equipo está activado (W2012), permitir conexiones al rango de puertos.
- Configurar en el router/puerta de enlace NAT:
 - Permitir el acceso al rango de puertos especificados en el servidor para el modo pasivo (aunque Iptables por defecto permite todo).
 - Redirigir el puerto 21 del router/firewall al equipo donde está instalado el servidor FTP (regla NAT PREROUTING)
 - Redirigir el rango de puertos para conexiones pasivas del router NAT al equipo donde esté instalado el servidor FTP

Una vez configurado el servidor, acceder a él la máquina real usando uno o varios clientes ftp.

6.1. Configurar modo pasivo en Filezilla Server:

- En la interfaz de control de Filezilla Server, **Configuración, passive mode settings**, se debe indicar qué *puertos del servidor se van a usar para la conexión de datos*, y la *IP que se usará para conexiones externas (desde una máquina externa no se ven las máquinas de la red interna ya que no se puede acceder a las IP's privadas. Por tanto, el cliente debe conectar a la puerta de enlace, que es la única máquina de la red interna que tiene tarjeta de la red del aula, su tarjeta puente. Esta es la IP a la que nos conectaremos y después el cortafuegos redirigirá la solicitud al servidor FTP de la red interna)*



- En el **iptables** (script de iptables) de la puerta de enlace es necesario hacer dos cosas:
 - Abrir el rango de puertos especificados en el servidor para el modo pasivo (aunque iptables por defecto permite el acceso a los puertos conocidos, no lo permite a los puertos privados, por lo que se debe habilitar):

```
iptables -A INPUT -p tcp --dport 64000:64321 -j ACCEPT
```

- Redirigir los puertos que se usan en FCT (21 para conexión de control y los indicados arriba para conexión de datos) en el cortafuegos, de modo que las conexiones desde el exterior a la puerta de enlace a través de esos puertos, se redirijan al cliente FTP:

```
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 64000:64321 -j DNAT --to 10.33.1.2:6400-64321
```

```
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 21 -j DNAT --to 10.33.1.2:21
```

```
Search your computer r@administrador-VirtualBox: ~
iptables -F
iptables -t nat -F

iptables -t nat -A POSTROUTING -j MASQUERADE

iptables -A INPUT -p tcp -m tcp --dport 64000:64321 -j ACCEPT

iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 64000:64321 -j DNAT --to 10.33.1.2:64000-64321
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 21 -j DNAT --to 10.33.1.2:21

echo "1" > /proc/sys/net/ipv4/ip_forward

iptables-save
```

Donde:

- enp0s8** es el nombre del interfaz de red de la tarjeta puente, e indica que se redireccionen las solicitudes que entran a través de ese interfaz.
- 10.33.1.2** es la IP de la máquina interna que tiene el servidor FTP
- No es necesario redirigir el puerto 20 ya que no se usa en el modo pasivo.

6.2. Configurar modo pasivo en vsftpd

- En el fichero de configuración `/etc/vsftpd.conf`, habilitamos el modo pasivo y especificamos qué *puertos del servidor se van a usar para la conexión de datos*, y la *IP que se usará para conexiones externas*. Podemos añadir estos parámetros al final del fichero de configuración:

```
pasv_enable=YES
pasv_min_port=64000
pasv_max_port=64321
pasv_address=192.168.1.100
```

Para que el servidor use la IP indicada en el parámetro `192.168.1.100`, se debe poner a YES el parámetro **listen** y comentar o poner a NO el parámetro **listen_ipv6** definidos más arriba en el mismo fichero de configuración:

```
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
#listen_ipv6=YES
```

- En el **iptables** (script de iptables) se hará exactamente lo mismo que antes (permitir el rango de puertos del modo pasivo y redigirir las solicitudes), teniendo en cuenta que la IP del servidor FTP cambia.

6.3. Conectarse desde un cliente externo usando el modo pasivo

- Abrimos un terminal de la máquina real y nos conectamos al servidor FTP. Como la máquina real no está en la red virtual no podemos usar la IP interna del servidor FTP. Pero el servidor FTP no tiene otra IP. Por tanto, nos conectamos a través de la IP puente de la puerta de enlace:

```
administrador@marta-casa:~$ ftp 192.168.1.100
Connected to 192.168.1.100.
220 (vsFTPd 3.0.3)
Name (192.168.1.100:administrador): mortadelo
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
500 Illegal PORT command.
ftp: bind: Address already in use
```

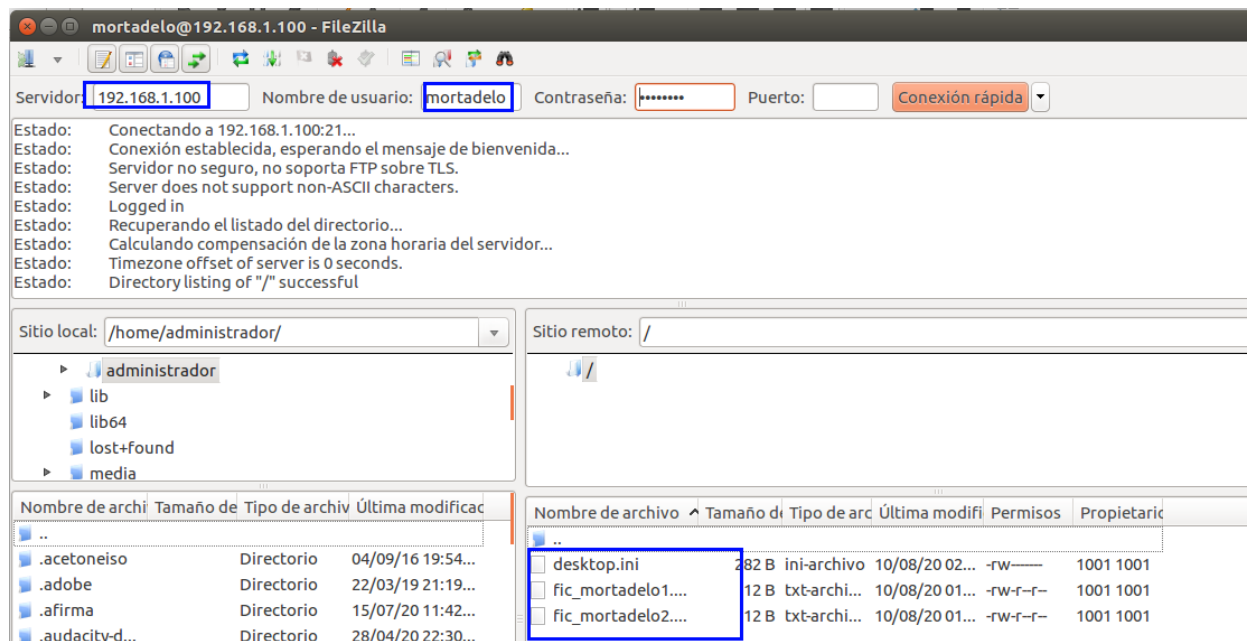
- Vemos que responde el servidor FTP de debian (vsftpd). Pero al intentar hacer un `ls` obtenemos un mensaje de error, ya que el cliente FTP de Ubuntu modo texto intenta acceder en modo activo a no ser que le indiquemos lo contrario. Para indicarle que lo haga en modo pasivo usaremos `passive` o `pas`, y entonces sí funcionarán las conexiones de datos:

```

500 Illegal PORT command.
ftp> bind: Address already in use
ftp> pas
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,1,100,250,252).
150 Here comes the directory listing.
-rw-r--r--  1 1001    1001          282 Aug 10 00:15 desktop.ini
-rw-r--r--  1 1001    1001          12 Aug 09 23:07 fic_mortadelo1.txt
-rw-r--r--  1 1001    1001          12 Aug 09 23:08 fic_mortadelo2.txt
226 Directory send OK.
ftp> mget f*
mget fic_mortadelo1.txt?

```

- También podemos usar la versión de Ubuntu de Filezilla Cliente, si lo tenemos instalado en la máquina real:



En este caso, Filezilla detecta automáticamente que la conexión en modo activo no funciona y cambia a modo pasivo sin necesidad de indicárselo.

- Si nuestra máquina real fuera Windows, el cliente FTP modo texto de Windows no permite el modo pasivo, por lo que tendríamos que usar otro cliente (p.e., Filezilla Client)

7. VSFTP seguro

7.1. FTPS con vsftpd

<https://es.linux-console.net/?p=748>

1. Debemos tener instalado OpenSSH en la misma máquina que vsftpd, ya que esta herramienta es la que nos va a permitir generar los certificados necesarios para cifrar la comunicación usando criptografía asimétrica o híbrida.

```
apt-get install openssh-server
```

2. Creamos la carpeta **/etc/ssl/private** para dejar en ella los ficheros del certificado. Para crear el certificado usaremos esta comando, que genera el certificado y la clave en un mismo fichero:

```
openssl req -x509 -nodes -keyout /etc/ssl/private/vsftpd.pem -out  
/etc/ssl/private/vsftpd.pem /etc/ssl/private/ -days 365 -newkey rsa:2048
```

Este comando pedirá unos datos. Introducimos datos apropiados para nuestro caso:

```
Country Name (2 letter code) [XX]:SP  
State or Province Name (full name) []:madrid  
Locality Name (eg, city) [Default City]:madrid  
Organization Name (eg, company) [Default Company Ltd]:jcierva.es  
Organizational Unit Name (eg, section) []:informatica  
Common Name (eg, your name or your server's hostname) []:jcierva  
Email Address []:[email protected]
```

3. Ahora sólo nos falta modificar el fichero de configuración **/etc/vsftpd.conf** para añadir los detalles SSL:

- Activar la opción **ssl_enable** (poner su valor a YES). Esta línea ya existe, pero su valor es NO, por lo que se debe cambiar. Además, restringiremos vsftpd a use TLS en lugar de SSL, (TLS es más seguro que SSL), habilitando la opción **ssl_tlsv1**:

```
ssl_enable=YES  
ssl_tlsv1=YES  
ssl_sslv2=NO  
ssl_sslv3=NO
```

- Modificaremos el valor de los parámetros **rsa_cert_file** y **rsa_private_key_file** para definir la ubicación del certificado SSL y el archivo de clave (que están en el mismo fichero=:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem  
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

- De forma adicional y optativa, podemos evitar que los usuarios anónimos usen SSL (**allow_anon_ssl=NO**), forzar a todos los inicios de sesión no anónimos a usar una conexión SSL segura para la transferencia de datos (**force_local_data_ssl=YES**) y enviar la contraseña durante el inicio de sesión (**force_local_logins_ssl=YES**):

```
allow_anon_ssl=NO  
force_local_data_ssl=YES  
force_local_logins_ssl=YES
```

- Si queremos usar el modo implícito para ftps, debemos añadir los parámetros **implicit_ssl** y **listen_port**:

```
implicit_ssl=YES  
listen_port=990
```

** Si queremos usar nuestro servidor FTP desde un equipo externo a la red (modo Pasivo) con ftps implícito, es necesario abrir y redirigir el puerto 990 en el cortafuegos, tal y como hicimos con el puerto 21 y el rango de puertos del modo pasivo en la práctica 6 de este tema.*

El fichero **/etc/vsftpd.conf** quedaría así:

```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
debug_ssl=YES
#implicit_ssl=YES
#listen_port=990
```

Los dejamos comentados

Reiniciar el servicio

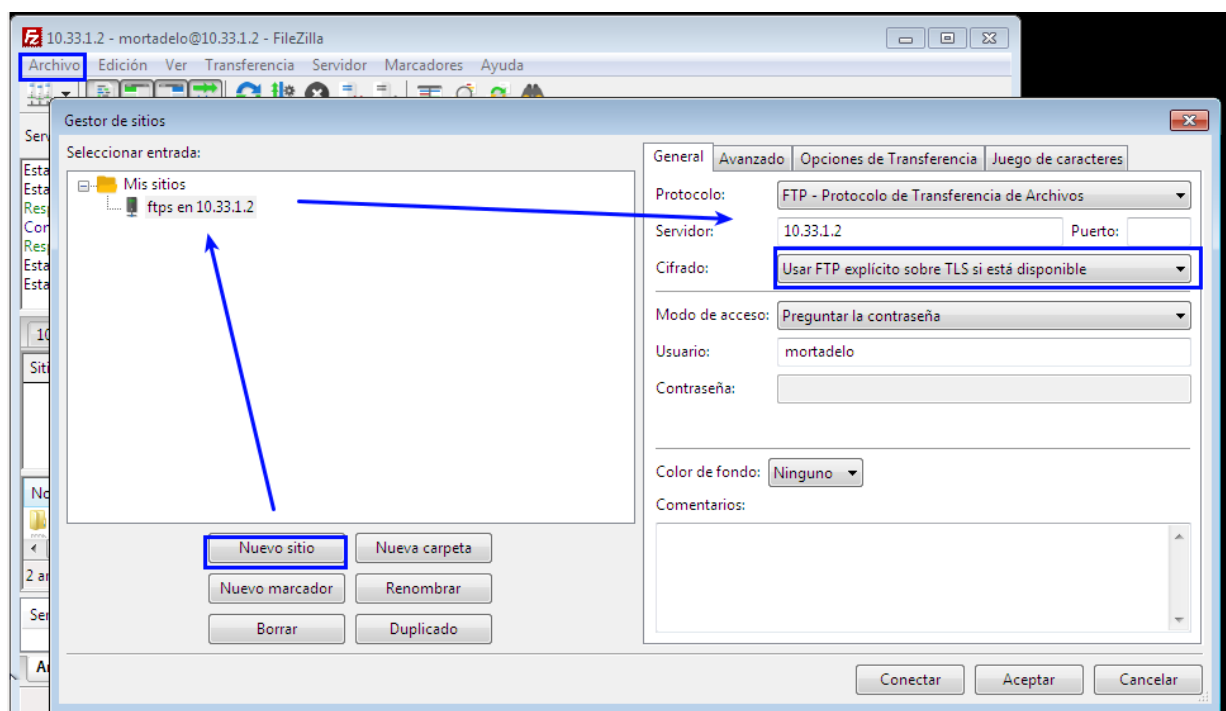
Para que los cambios surjan efecto deberéis reiniciar el servicio:

```
service vsftpd restart
```

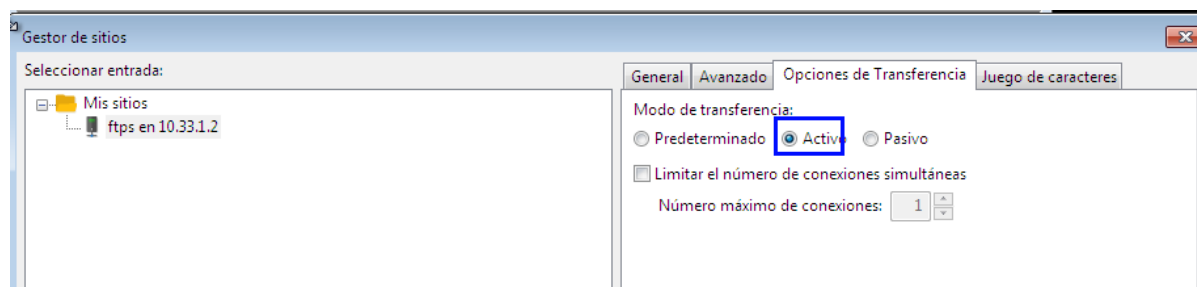
Conexión

Vamos a hacer la prueba de conexión desde el Filezilla Client de la máquina Windows4 o Ubuntu2.

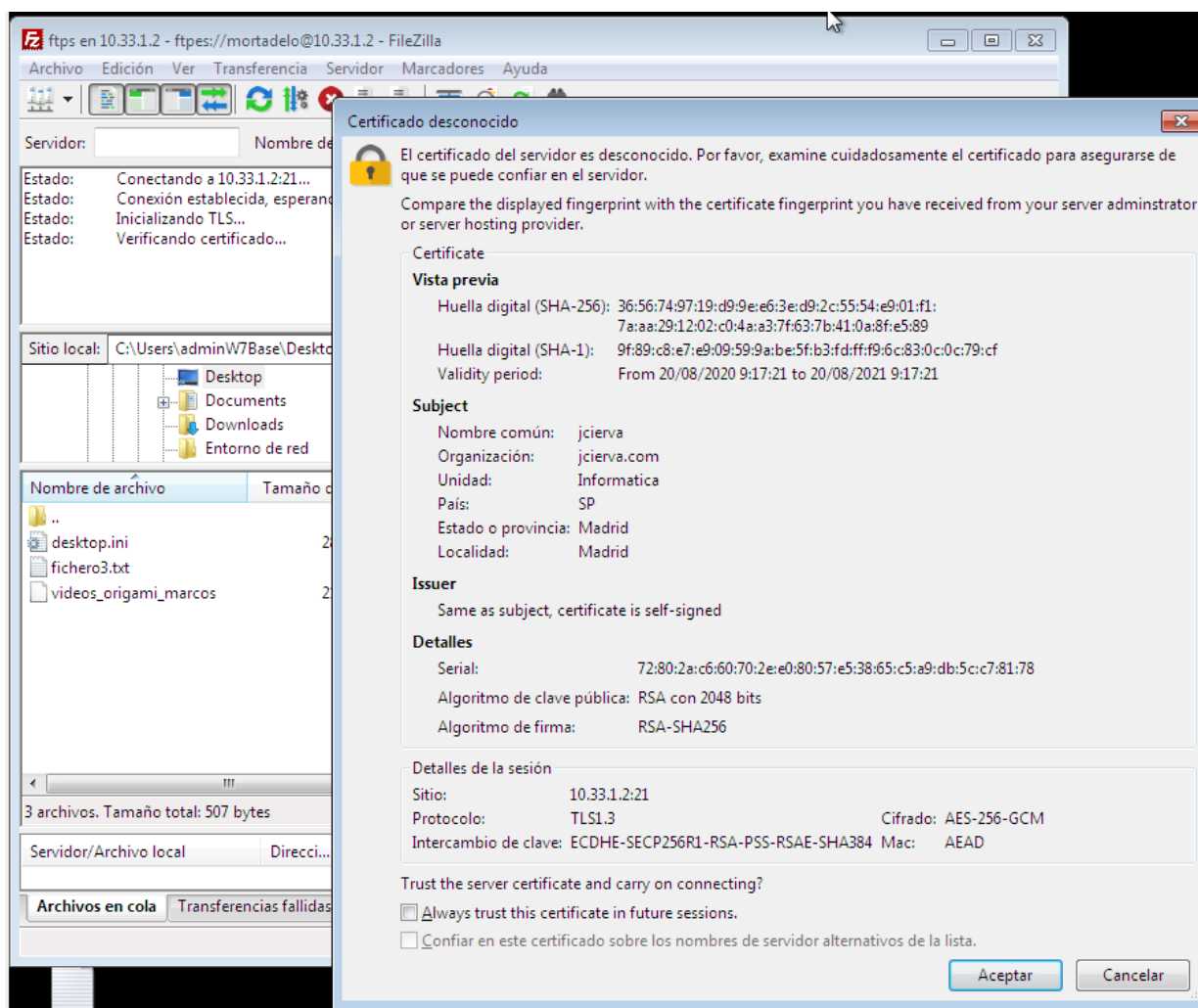
Creamos una nueva nueva conexión en Archivo-Gestor de Sitios, con los siguientes datos:

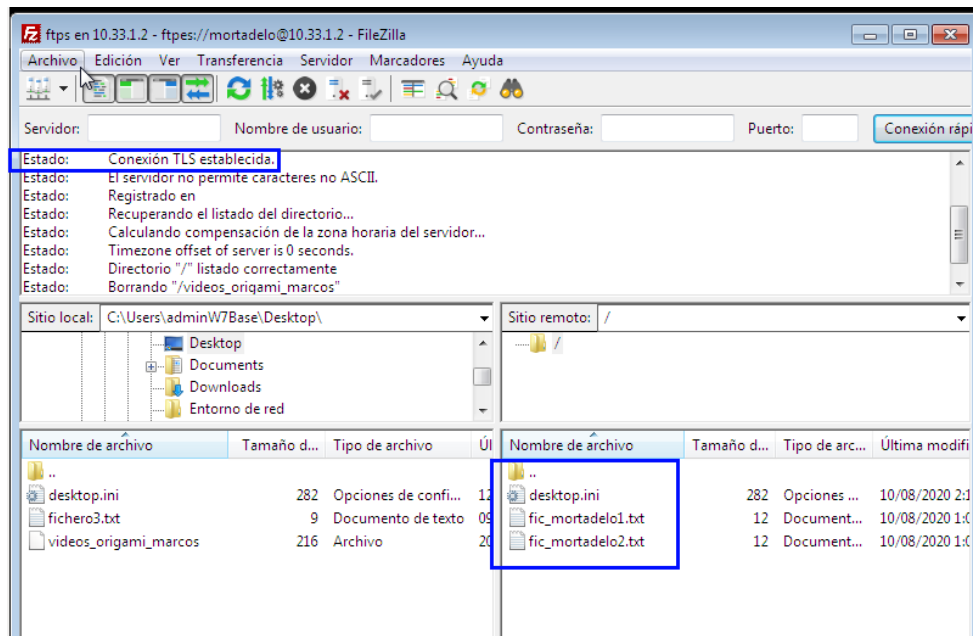


- Puesto que no hemos activado ftps implícito, en la opción "Cifrado" elegimos la opción "Usar FTP explícito sobre TLS si está disponible" o la opción "Requiere FTP explícito sobre TLS".
- Si hubiéramos activado ftps implícito, la opción elegida debería ser "Requiere FTP implícito sobre TLS" y **además habría que indicar el puerto 990**
- Además, si la máquina desde la que nos conectamos está en la red interna, debemos cambiar el modo a "Activo" en la pestaña "Opciones de Transferencia".



- Haciendo doble click sobre el nuevo sitio creado, se mostrarán los datos del certificado SSL para que confirmemos que confiamos en él y a continuación se iniciará la conexión segura:





7.2. FTPS con Filezilla

Práctica hecha en el módulo "Seguridad"

7.3. SFTP (Transferencia de ficheros con SSH)

Práctica hecha en el módulo "Seguridad"