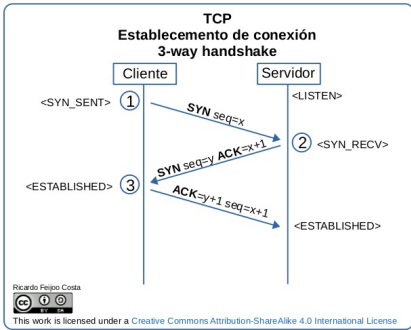# Cheat-Sheet: FTP

**Clientes FTP**
**GUI → FileZilla Client** (Modo Pasivo)
**Comandos → ftp**
  **GNU/Linux → ftp** (Modo Pasivo)
  **MS Windows → ftp** (Modo Activo)

**TCP**
**Establecemento de conexión**
**3-way handshake**

| Cliente | | Servidor |
|---|---|---|
| <SYN_SENT> ① | SYN seq=x → | <LISTEN> |
| | SYN seq=y ACK=x+1 | ② <SYN_RECV> |
| <ESTABLISHED> ③ | ACK=y+1 seq=x+1 → | |
| | | <ESTABLISHED> |

Ricardo Feijoo Costa
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

**FTP - Establecemento de conexión → 21 (Server TCP Port)**

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 0.006427614 | 10.0.2.15 | ftp.ujaen.es | TCP | 74 | 39090 → 21 [SYN] Seq=0 Win=65535 Len |
| 6 | 0.038841648 | ftp.ujaen.es | 10.0.2.15 | TCP | 60 | 21 → 39090 [SYN, ACK] Seq=0 Ack=1 Wi |
| 7 | 0.038913556 | 10.0.2.15 | ftp.ujaen.es | TCP | 54 | 39090 → 21 [ACK] Seq=1 Ack=1 Win=655 |
| 8 | 0.083003327 | ftp.ujaen.es | 10.0.2.15 | FTP | 106 | Response: 220 Servidor FTP anonimo d |
| 9 | 0.083108496 | 10.0.2.15 | ftp.ujaen.es | TCP | 54 | 39090 → 21 [ACK] Seq=1 Ack=53 Win=65 |
| 14 | 5.969206024 | 10.0.2.15 | ftp.ujaen.es | FTP | 70 | Request: USER anonymous |
| 15 | 5.969965755 | ftp.ujaen.es | 10.0.2.15 | TCP | 60 | 21 → 39090 [ACK] Seq=53 Ack=17 Win=6 |
| 16 | 6.002095887 | ftp.ujaen.es | 10.0.2.15 | FTP | 129 | Response: 331 Anonymous login ok, se |

```
┌──(kali㉿kali)-[~]
└─$ ftp ftp.ujaen.es
Connected to ftp.ujaen.es.
220 Servidor FTP anonimo de la Universidad de Jaen
Name (ftp.ujaen.es:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Acceso permitido para anonymous
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||36136|)
150 Opening BINARY mode data connection for file list
drwxr-xr-x   6 ftp      ftp           152 Nov  3  2011 pub
-rw-r--r--   1 ftp      ftp          1877 Apr 26  2007 welcome.msg
226 Transfer complete
ftp> lcd /tmp
Local directory now: /tmp
ftp> get welcome.msg
local: welcome.msg remote: welcome.msg
229 Entering Extended Passive Mode (|||28263|)
150 Opening BINARY mode data connection for welcome.msg (1877 bytes)
100% |***********************************|  1877       12.69 MiB/s    00:00 ETA
226 Transfer complete
1877 bytes received in 00:00 (56.88 KiB/s)
ftp> !
┌──(kali㉿kali)-[/tmp]
└─$ ls -l welcome.msg
-rw-r--r-- 1 kali kali 1877 Apr 26  2007 welcome.msg
┌──(kali㉿kali)-[/tmp]
└─$ exit
ftp> quit
221 Goodbye.
┌──(kali㉿kali)-[~]
└─$ █
```

**Modo Pasivo** → Inicio conexión de datos dende o cliente ftp
→ TCP Port cliente ftp ≥ 1024
→ TCP Port servidor ftp ≥ 1024

**GNU/Linux → command ftp**

**WireShark**

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 39 | 10.631906463 | 10.0.2.15 | ftp.ujaen.es | TCP | 74 | 56356 → 36136 [SYN] Seq=0 Win=65535 Len=0 MSS=146 |
| 40 | 10.665672297 | ftp.ujaen.es | 10.0.2.15 | TCP | 60 | 36136 → 56356 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le |
| 41 | 10.665786034 | 10.0.2.15 | ftp.ujaen.es | TCP | 54 | 56356 → 36136 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 45 | 10.701196316 | ftp.ujaen.es | 10.0.2.15 | FTP-DATA | 182 | FTP Data: 128 bytes (EPASV) (LIST) |
| 46 | 10.701196871 | ftp.ujaen.es | 10.0.2.15 | TCP | 60 | 36136 → 56356 [FIN, ACK] Seq=129 Ack=1 Win=65535 |
| 47 | 10.701282132 | 10.0.2.15 | ftp.ujaen.es | TCP | 54 | 56356 → 36136 [ACK] Seq=1 Ack=129 Win=65535 Len=0 |
| 48 | 10.701745304 | 10.0.2.15 | ftp.ujaen.es | TCP | 54 | 56356 → 36136 [FIN, ACK] Seq=1 Ack=130 Win=65535 |
| 49 | 10.702298799 | ftp.ujaen.es | 10.0.2.15 | TCP | 60 | 36136 → 56356 [ACK] Seq=130 Ack=2 Win=65535 Len=0 |

```
▶ Frame 45: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface eth0, id 0
▶ Ethernet II, Src: 10.0.2.2 (52:54:00:12:35:02), Dst: 10.0.2.15 (08:00:27:e7:3b:62)
▶ Internet Protocol Version 4, Src: ftp.ujaen.es (150.214.170.29), Dst: 10.0.2.15 (10.0.2.15)
▶ Transmission Control Protocol, Src Port: 36136, Dst Port: 56356, Seq: 1, Ack: 1, Len: 128
  FTP Data (128 bytes data)
    [Setup frame: 38]
    [Setup method: EPASV]
    [Command: LIST]
    Command frame: 42
    [Current working directory: ]
▼ Line-based text data (2 lines)
    drwxr-xr-x   6 ftp      ftp           152 Nov  3  2011 pub\r\n
    -rw-r--r--   1 ftp      ftp          1877 Apr 26  2007 welcome.msg\r\n
```

## Establecemento de Conexión TCP (3-way handshake)

Servidor FTP — :21  :21  :21 — Servidor FTP
SYN, ACK
SYN  ACK
Cliente FTP — :39090  :39090  :39090 — Cliente FTP
≥1024
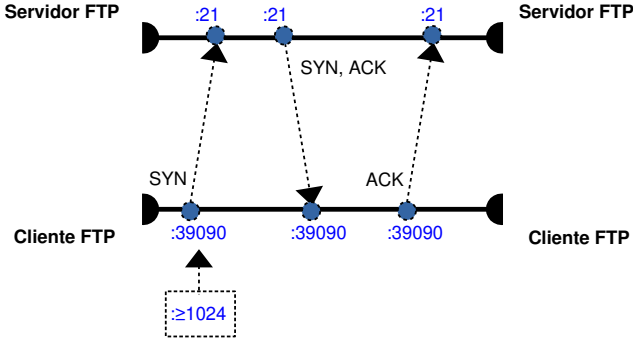
## Trasmisión de datos: Modo Pasivo

Servidor FTP — :36136  :36136  :36136 — Servidor FTP
SYN, ACK
SYN  ACK
Cliente FTP — :56356  :56356  :56356 — Cliente FTP
≥1024
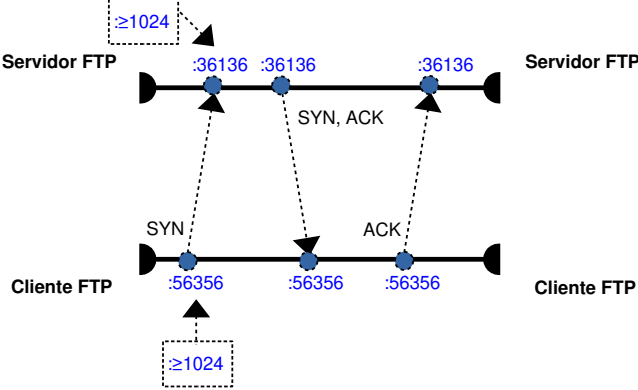
## Trasmisión de datos: Modo Activo

(Negociase o PORT entre o cliente e o servidor → O cliente envía o PORT≥1024, neste caso 56356 e o servidor emprega o porto 20)

Servidor FTP — :20  :20  :20 — Servidor FTP
SYN  ACK
Firewall
SYN, ACK
Cliente FTP — :56356  :56356  :56356 — Cliente FTP
≥1024
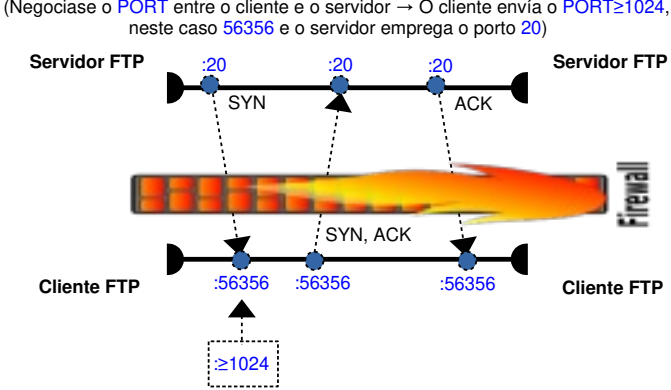
### Problema
**Atravesar o firewall, router, etc do cliente.** Débense permitir conexións entrantes hacia o cliente cando o cliente non é o host que solicitou a conexión.

**Filezilla-Server** pode empregar outro porto≥1024 e non o porto 20 (neste caso o 33979)

Link

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 15 | 8.150443686 | 10.10.10.11 | 10.10.10.10 | FTP | 79 | Request: PORT 10,10,10,11,194,21 |
| 16 | 8.151170803 | 10.10.10.10 | 10.10.10.11 | FTP | 84 | Response: 200 PORT command successful. |
| 17 | 8.178901345 | 10.10.10.11 | 10.10.10.10 | FTP | 70 | Request: RETR proba.txt |
| 18 | 8.179760217 | 10.10.10.10 | 10.10.10.11 | FTP | 83 | Response: 150 Starting data transfer. |
| 19 | 8.179998595 | 10.10.10.10 | 10.10.10.11 | TCP | 74 | 33979 → 49685 [SYN] Seq=0 Win=64240 Len |
| 20 | 8.180707029 | 10.10.10.11 | 10.10.10.10 | TCP | 74 | 49685 → 33979 [SYN, ACK] Seq=0 Ack=1 W |
| 21 | 8.180752853 | 10.10.10.10 | 10.10.10.11 | TCP | 66 | 33979 → 49685 [ACK] Seq=1 Ack=1 Win=642 |
| 22 | 8.180973949 | 10.10.10.10 | 10.10.10.11 | TCP | 73 | 33979 → 49685 [PSH, ACK] Seq=1 Ack=1 W |
| 23 | 8.181133026 | 10.10.10.10 | 10.10.10.11 | TCP | 66 | 33979 → 49685 [FIN, ACK] Seq=8 Ack=1 W |
| 24 | 8.182418944 | 10.10.10.11 | 10.10.10.10 | TCP | 66 | 49685 → 33979 [ACK] Seq=1 Ack=9 Win=206 |
| 25 | 8.182533259 | 10.10.10.10 | 10.10.10.11 | FTP | 80 | Response: 226 Operation successful |

```
▶ Frame 15: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0, id 0
▶ Ethernet II, Src: PcsCompu_dc:7f:49 (08:00:27:dc:7f:49), Dst: PcsCompu_e7:3b:62 (08:00:27:e7:3b:62)
▶ Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.10
▶ Transmission Control Protocol, Src Port: 49684, Dst Port: 21, Seq: 37, Ack: 199, Len: 25
▼ File Transfer Protocol (FTP)
  ▼ PORT 10,10,10,11,194,21\r\n
      Request command: PORT
      Request arg: 10,10,10,11,194,21
      Active IP address: 10.10.10.11
      Active port: 49685
  [Current working directory: ]
```

**Command ftp GNU/Linux → $HOME/.netrc** ( $ man netrc)

$ echo machine ftp.ujaen.es login anonymous password 1234 > /home/kali/.netrc
$ chmod 600 /home/kali/.netrc
$ ftp ftp.ujaen.es

**Command ftp MS Windows → %USERPROFILE%/file** (> ftp /?)

> echo anonymous> %USERPROFILE%file
> echo 1234>> %USERPROFILE%file
> ftp -s:%USERPROFILE%file ftp.ujaen.es

**Filezilla Server → Xestor de sitios**

File → Site Manager …
New site → ujaen
Protocol: FTP – File Transfer Protocol
Host: ftp.ujaen.es
Encryption: Only use plain FTP(insecure)
Logon Type: anonymous
OK

---

**Servidor FTP(filezilla-server)**
**eth0:**
   IP estática: 10.10.10.10/8
   Gateway: 10.10.10.1
   DNS: 1.1.1.1, 8.8.8.8
**Paquete servidor FTP:**
FileZilla_Server*.deb
**Instalación:**
# dpkg -i FileZilla_Server*.deb
**Portos TCP:**
21 → Establecemento conexión
   14148 → GUI Administración
**Ficheiros de configuración:**
/opt/filezilla-server/etc
Por defecto ningún usuario ten acceso ao
servidor. Tampouco o usuario **anonymous**
**Binarios:**
/opt/filezilla-server/bin
filezilla-server-gui & → Panel administración
**Ficheiros logs:**
Panel administración
**Panel de administración:**
   Users: sistema (posúen perfil de usuario)
   Users: virtuais (non posúen conta no sistema,
pero poden enlazarse a un perfil de usuario)

**Configuración de rede en tempo real:**
# pkill NetworkManager \
&& ip addr add 10.10.10.10/8 dev eth0 \
&& ip route add default via 10.10.10.1 dev eth0 \
&& echo -e 'nameserver 1.1.1.1\nnameserver 8.8.8.8' > /etc/resolv.conf

**Comprobar a configuración de rede:**
# ip addr show eth0 \
&& ip route \
&& cat /etc/resolv.conf

**Paquete debian: FileZilla_Server*.deb - Instalación**
# dpkg -i FileZilla_Server*.deb

**Ver accións posibles do servidor filezilla-server:**
# systemctl show filezilla-server | grep -i can #Premer Enter
CanStart=yes →Pódese utilizar a acción `systemctl start` para iniciar o servizo.
CanStop=yes →Pódese utilizar a acción `systemctl stop` para deter o servizo.
CanReload=yes →Pódese utilizar a acción `systemctl reload` para recargar o servizo.
CanIsolate=no → Non se pode utilizar a acción `systemctl isolate` para illar o servizo.
CanFreeze=yes →Pódese utilizar a acción `systemctl freeze` para conxelar o servizo.

**Arranque do servidor:**
# systemctl start filezilla-server #Premer Enter

**Comprobar estado servidor:**
# systemctl status filezilla-server #Premer Enter

**Configuración servidor en** /opt/filezilla-server/etc **a través do Panel de administración:** filezilla-server-gui
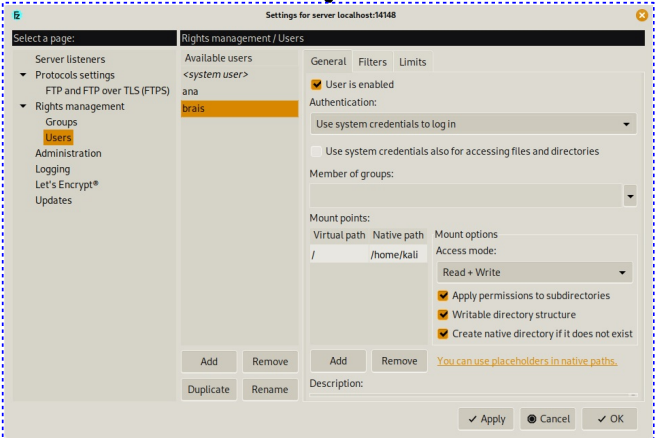
**debian → Instalar FileZilla-Server**

**Exemplo1**
Panel de administración
→ Acceso e configuración
por defecto

Ficheiro binario

**/opt/filezilla-server/bin/filezilla-server-gui**

$ cd /opt/filezilla-server/bin
$ ./filezilla-server-gui &
Connect to Server...
Host: localhost
Port: 14148
Password: ********

Usuario ftp
anonymous sen acceso

Configuración
**Sección Configure**

Server → Configure…
   Server Listeners:
      AddressPortProtocol
      0.0.0.021Explicit FTP over TLS and insecure plain FTP
      ::21Explicit FTP over TLS and insecure plain FTP

Por defecto, en IPv4(0.0.0.0) e IPv6(::) calquera NIC do
servidor está en modo "listen" para o servidor FTP

   Users…
   <system user> → Disable

Usuario de sistema
kali sen acceso

$ ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220-FileZilla Server 1.8.0
220 Please visit https://filezilla-project.org/
Name (localhost:kali): **anonymous**
331 Please, specify the password.
Password:
**530** Login incorrect.
ftp: Login failed
ftp> **user kali**
331 Please, specify the password.
Password:
**530** Login incorrect.
Login failed.
ftp> quit
221 Goodbye.
$

**Exemplo2**
Panel de administración
→ Usuarios de sistema

Configuración
**Sección Configure**

[Settings for server localhost:14148 dialog — Rights management / Users]
Select a page:
Server listeners
▼ Protocols settings
   FTP and FTP over TLS (FTPS)
▼ Rights management
   Groups
   Users
Administration
Logging
Let's Encrypt*
Updates

Available users
<system user>

General  Filters  Limits
☑ User is enabled
Authentication:
Use system credentials to log in
☑ Use system credentials also for accessing files and directories
Member of groups:
Mount points:
Virtual path  Native path  Mount options
/        %<home>    Access mode:
            Read + Write
☑ Apply permissions to subdirectories
☑ Writable directory structure
☑ Create native directory if it does not exist
You can use placeholders in native paths.
Description:

Add  Remove        Add  Remove
Duplicate  Rename

✓ Apply  ● Cancel  ✓ OK

Usuario de sistema
kali con acceso

$ ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220-FileZilla Server 1.8.0
220 Please visit https://filezilla-project.org/
Name (localhost:kali): **kali**
331 Please, specify the password.
Password:
**230** Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
$

**Apply**
Aplicar configuración

**Exemplo4**
Panel de administración →
Usuarios virtuais con
Native Path existentes
no sistema

[Settings for server localhost:14148 dialog — Rights management / Users]
Select a page:
Server listeners
▼ Protocols settings
   FTP and FTP over TLS (FTPS)
▼ Rights management
   Groups
   Users
Administration
Logging
Let's Encrypt*
Updates

Available users
<system user>
ana
brais

General  Filters  Limits
☑ User is enabled
Authentication:
Use system credentials to log in
☐ Use system credentials also for accessing files and directories
Member of groups:
Mount points:
Virtual path  Native path  Mount options
/        /home/kali    Access mode:
            Read + Write
☑ Apply permissions to subdirectories
☑ Writable directory structure
☑ Create native directory if it does not exist
You can use placeholders in native paths.
Description:

Add  Remove        Add  Remove
Duplicate  Rename

✓ Apply  ● Cancel  ✓ OK

Similar ao **Exemplo3**, pero cambiar:
→ Native Path
   → Authentication

$ ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220-FileZilla Server 1.8.0
220 Please visit https://filezilla-project.org/
Name (localhost:kali): **brais**
331 Please, specify the password.
Password:
**230** Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
$

Usuario virtual brais
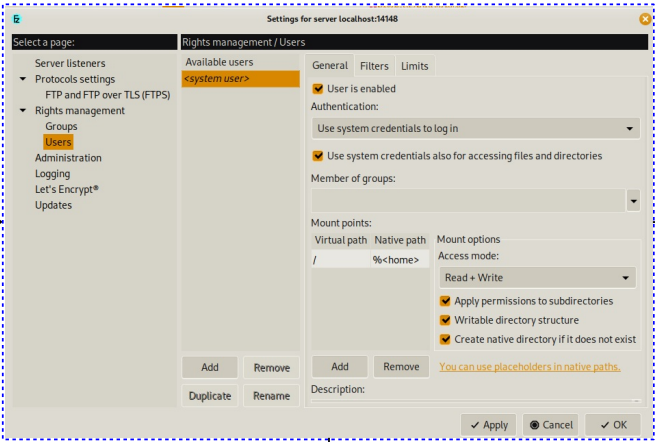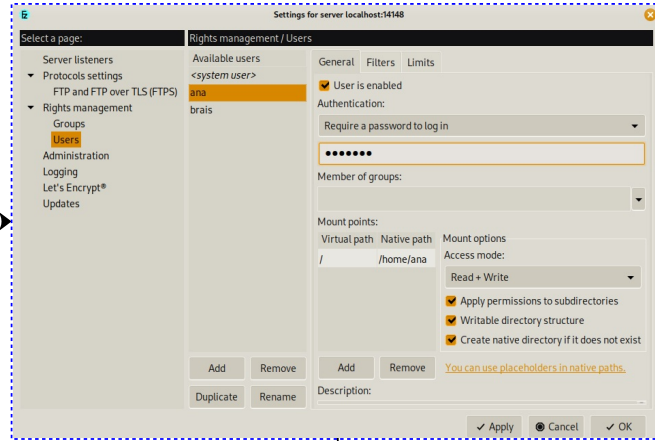Con acceso ao perfil do usuario kali
(/home/kali)

**Permisos ugo**
$ sudo chgrp -R ftp /home/kali
$ sudo find /home/kali -type f -exec chmod 664 {} \;
$ sudo find /home/kali -type d -exec chmod 775 {} \;

**Apply**
Aplicar configuración

**Exemplo3**
Panel de administración →
Usuarios virtuais
(non existentes no sistema)

Configuración
**Sección Configure**

[Settings for server localhost:14148 dialog — Rights management / Users]
Select a page:
Server listeners
▼ Protocols settings
   FTP and FTP over TLS (FTPS)
▼ Rights management
   Groups
   Users
Administration
Logging
Let's Encrypt*
Updates

Available users
<system user>
ana
brais

General  Filters  Limits
☑ User is enabled
Authentication:
Require a password to log in
●●●●●●●●
Member of groups:
Mount points:
Virtual path  Native path  Mount options
/        /home/ana    Access mode:
            Read + Write
☑ Apply permissions to subdirectories
☑ Writable directory structure
☑ Create native directory if it does not exist
You can use placeholders in native paths.
Description:

Add  Remove        Add  Remove
Duplicate  Rename

✓ Apply  ● Cancel  ✓ OK

Usuario virtual ana
Sen conta de sistema

$ ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220-FileZilla Server 1.8.0
220 Please visit https://filezilla-project.org/
Name (localhost:kali): **ana**
331 Please, specify the password.
Password:
**230** Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
$

**Apply**
Aplicar configuración