

## vsFTPD 伺服器

### 主動模式 (Active Mode) 與被動模式 (Passive Mode) FTP

FTP 是一種檔案傳輸協定 (File Transfer Protocol)，它需要利用 TCP 協定建立兩個連線通道才能順利傳輸資料，一是「命令連線」通道，另一是「資料連線」通道。而建來這個通道的方式有兩種：主動模式 (Active Mode) 和被動模式 (Passive Mode)。以下便說明這兩種模式是如何建來連線及有何不同？

#### ■ 主動模式 (Active Mode)

預設 FTP Client 連至 FTP Server 預設是採用主動模式 (Active Mode)，千言萬語比不上一張圖，筆者利用圖 1 來說明何謂主模式 (Active Mode)。

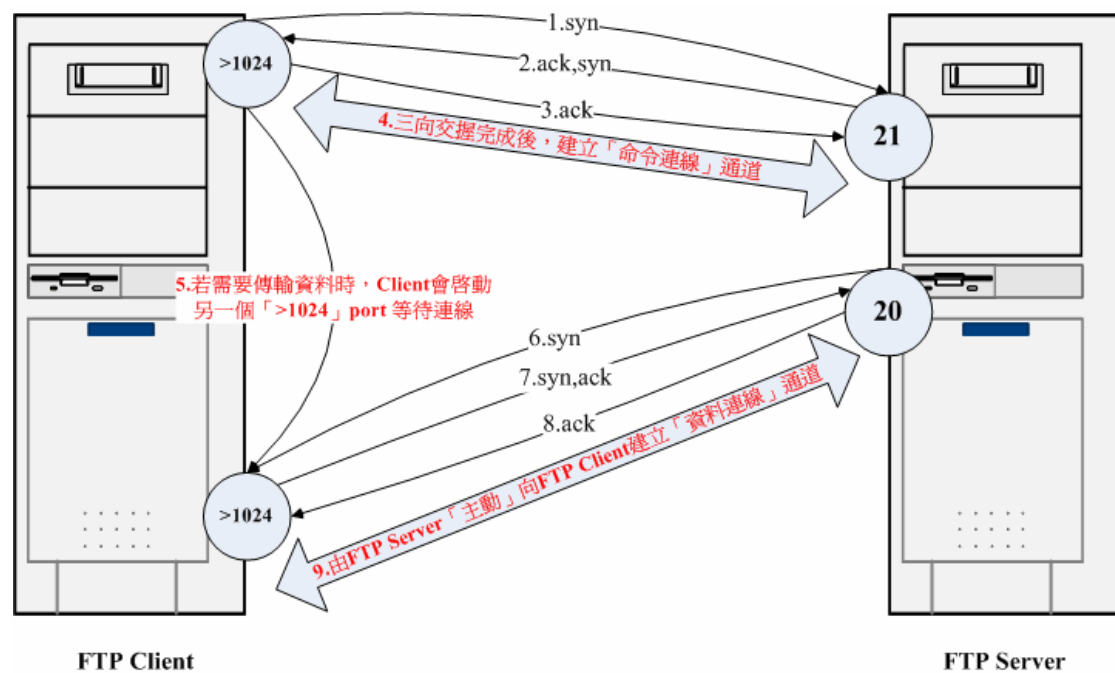


圖 1：主動模式 FTP 流程圖

FTP Client 隨機選擇的 TCP port(通常 > 1024)呼叫 FTP server 的 port 21 請求連線。進行「TCP Three-Way Handshake」(步驟 1~3) 當順利完成「TCP Three-Way Handshake」之後，便建立「命令連線」的通道 (步驟 4)，這個連線通道僅能進行 FTP 的「指令」。

如果需要資料傳送，例如上傳或下載就得再要額外建立一條資料傳輸的連

線，即是所謂的「資料連線」通道。此「資料連線」通道建立方式如下，當 Client 送出傳輸資料的指令時，此時 Client 會在另一個>1024 port 上 Listen 等待連線，並利用「命令連線」的通道告訴 Server 其 Listen 的 port number（步驟 5）。

然後 FTP Server 會利用 port 20 和剛才 FTP Client 所告知的 TCP port 進行 Three-Way Handshake 並建立「資料連線」通道連線（步驟 6~9）。因為這種「資料連線」通道建立方式是由 FTP Server 的 port 20 主動跟 FTP Client 連線，故稱「主動模式（Active Mode）」。

由上面的連線過程，我們會用到 FTP Server 主機的兩個 port number 為：

- (1)命令連線通道的 ftp（預設為 port 21）
- (2)資料連線傳輸的 ftp-data（預設為 port 20）

主動模式在實務上有時會遇到問題，當 FTP Client 在防火牆或 IP 分享器後面時，其命令連線通道可順利建立，但資料連線通道卻無法完成。

其原因為步驟 5：「Client 會在另一個>1024 port 上 Listen 等待連線，並利用命令連線通道告訴 Server 其 Listen 的 port number（假設為 port 6634）」後，由於 IP 分享器會將內部非法 IP 偽裝成 IP 分享器對外合法的 IP，所以在進行步驟 6 時，FTP Server 會嘗試連線至 IP 分享器對外 IP 的 port 6634，但是 IP 分享器並未在 port 6634 上 Listen，所以就無法建立連線。

## ■ 被動模式（Passive Mode）

上述的問題，可要求採用被動模式 FTP 便可解決，首先當然要先在你的 FTP Client 設定利用被動模式 FTP 的方式建立連線，圖 2 便是 ws\_ftp 95 指定被動模式 FTP 的畫面。

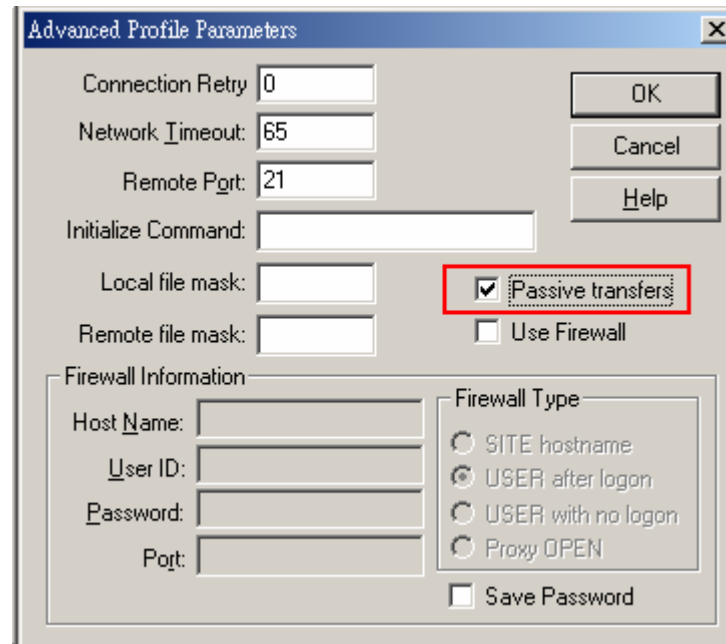


圖 2：ws\_ftp 95 Passive Mode 設定畫面

被動模式最主要想法為，竟然建立「資料連線」通道時，由 FTP Server 主動連線 FTP Client 有問題；那就反過來，FTP Server 在某個>1024 port 上 Listen 被動等 FTP Client 來建立「資料連線」通道，其流程圖如圖 3。

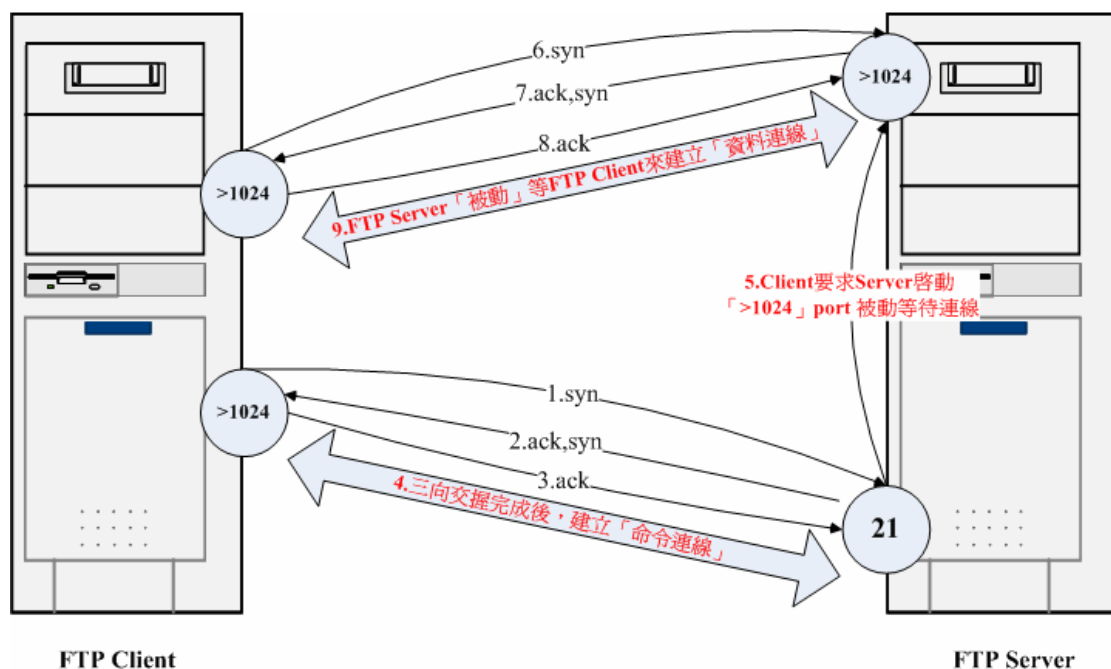


圖 3：被動模式 FTP 流程圖

建立「命令連線」的通道的方式和主動模式一樣（步驟 1~4），但是如果需

要資料傳送，就是要建立「資料連線」通道時，Client 會送出 PASV (Passive) 指令，告訴 FTP Server，要利用被動模式建立「資料連線」通道。

當 FTP Server 收到 PASV 指令時，便會在某個>1024 port 上 Listen，等待 FTP Client 來建立資料連線通道（步驟 5），並利用命令連線通道告知 FTP Client：「我在那個 Port 上等你連線」。

然後 FTP Client 會隨機再選一個>1024 的 port 向 FTP Server 所告知 port 進行 Three-Way Handshake 並建立「資料連線」通道連線（步驟 6~9）。因為這種「資料連線」通道建立方式是 FTP Server 被動等 FTP Client 來連線，故稱為「被動模式 (Active Mode)」。

### vsFTPd 相關套件及設定檔

vsftpd 的相關套件及設定檔如下：

```
Daemon : vsftpd
Daemon 類別 : System V daemon
所需套件 :
➤vsftpd-*rpm
Script : /etc/initd.d/vsftpd
Port : 21 (ftp) ,20 (ftp-data)
設定檔 : /etc/vsftpd.ftputers
         /etc/vsftpd/vsftpd.conf
```

### 1-3 vsFTPd 設定檔解說

vsftpd 中較常使用的設定檔有兩個/etc/vsftpd.ftputers 及 /etc/vsftpd/vsftpd.conf，其中以/etc/vsftpd/vsftpd.conf 最為重要。

#### ■ /etc/vsftpd.ftputers

這個設定檔很簡單，只要使用者的名字在此檔內，便不能使用 FTP。

#### ■ /etc/vsftpd/vsftpd.conf：vsftpd 的主要設定檔

vsftpd.conf 中參數眾多，首先我們先看 SLES 9 中 vsftpd.conf 的內容，筆者逐一解釋其中意義。

```
# Example config file /etc/vsftpd.conf
# Please see vsftpd.conf.5 for all compiled in defaults.
# 提示讀者可以利用 man 5 vsftpd.conf 查看 vsftpd.conf 設定檔的預設值

#####
#                      General Settings                      #
#                      通用設定部份                          #
#####

# If you do not change anything here you will have a minimum setup for an
# anonymus FTP server.
# 預設的設定只允許利用 anonymous 登入

#write_enable=YES
# write_enable=YES 為允許使用者具有寫入的權限，預設值為 NO。

dirmessage_enable=YES
# 當使用者進入某個目錄時，如果該目錄存在.message 檔案，則會顯示該檔案
# 的內容，通常用來告知此目錄存放檔案的資訊，預設值為 NO。

#nopriv_user=ftpsecure
# 指定 vsftpd 以何帳號提供 FTP 服務，預設值為 nobody。這樣即使被 cracker
# 入侵 vsftpd，cracker 僅能取得 nobody 的權限

#ftpd_banner="Welcome to FOOBAR FTP service."
# banner 是標題之意，ftpd_banner 即是一連上 vsftpd 伺服器所看到的訊息。
# 但是 ftpd_banner 只能設定一行的訊息。若是訊息超過一行，請用 banner_file
# 例如 banner_file=/etc/motd，然後再編寫/etc/motd

#ls_recurse_enable=YES
# ls_recurse_enable 預設值為 YES，代表禁用 ls -RI /，因為這個指令會耗用
# 大量系統資源

#no_anon_password=NO
# sles 9 中預設的 vsftpd.conf 並未出現 no_anon_password 設定值，
# 筆者認為跟之後 deny_email_enable,banned_email_file 相關，便將其列出
# no_anon_password 預設值為 NO，
# 代表 anonymous 不用輸入密碼就可登入 FTP 伺服器
```

```
# 若不想利用 chroot_local_user=YES 把所有 Local user 限級
# 在其家目錄，可利用 chroot_list_enable=YES 設定值，
# 將某些帳號限制在家目錄下，當 chroot_list_enable=YES 時，
# 登入的使用者的名字若在/etc/vsftpd.chroot_list內，則
```

```
# 會啟用 chroot 機制，將這個使用者限制在其家目錄下。
# chroot_list_enable 預設值為 NO
# chroot_list_file 預設值為/etc/vsftpd.chroot_list

#local_max_rate=7200
# local_max_rate 用來限制 Local user 每秒的最高傳輸速度，
# 其單位為 bytes/sec，預設值為 0，就是沒有限制。

#####
#          Anonymus FTP user Settings                                #
#          Anonymus 使用者的相關設定                                #
#####

anonymous_enable=YES
# anonymous_enable=YES，允許使用者可用 anonymous 或 ftp 帳號，
# 不用密碼就可登入 FTP 伺服器，其預設值為 YES

anon_world_readable_only=YES
# anon_world_readable_only=YES，用來限制 anonymous 使用者
# 只能下載 Other 有開放 write 的檔案，其預設值為 YES

#anon_upload_enable=YES
# anon_upload_enable 用來限制 anonymous 使用者可否上傳檔案，
# 其預設值為 NO

#anon_umask=022
# anon_umask 的意義是 anonymous 使用者上傳檔案時，
# 檔案權限會用所指定的 umask 加以運算，預設值為 077

#anon_mkdir_write_enable=YES
# anon_mkdir_write_enable 允不允許 anonymous 使用者可建立目錄
# anon_mkdir_write_enable 預設值為 NO

#anon_other_write_enable=YES
# 是否允許 anonymous 使用者有 write 的權限，
# 不過記得通過 anon_other_write_enable 的限制後，
# 還得看欲 write 目錄或檔案的權限允不允許 anonmous 使用者 write
```

```
#chown_uploads=YES
#chown_username=whoever
# chown_uploads 用來指定用 anonymous 帳號上傳的東西是否要改變其擁有者
# chown_uploads 其預設值為 NO，chown_username 用來指定新的擁有者

#anon_max_rate=7200
# anon_max_rate 用來限制 anonymous 使用者每秒的最高傳輸速度，
# 其單位為 bytes/sec，預設值為 0，就是沒有限制。

#####
#                      Log Settings                      #
#                      有關 FTP 日誌的相關設定          #
#####

syslog_enable=YES
# syslog_enable=YES 會將本來應記錄在/var/log/vsftpd.log 的訊息，
# 轉而傳給 syslogd daemon，由 syslogd 的設定檔決定存於位置
# syslog_enable 預設值為 NO

#log_ftp_protocol=YES
# log_ftp_protocol=YES 會將所有 FTP 有關的 requests 和 responses 全部記錄
# log_ftp_protocol 預設值為 NO

#xferlog_enable=YES
# xferlog_enable=YES 會詳細記錄有關上傳/下載的訊息
# xferlog_enable 預設值為 NO

#vsftpd_log_file=/var/log/vsftpd.log
# vsftpd_log_file 可用來指定 vsftpd log 檔的位置

#xferlog_std_format=YES
# xferlog_std_format 預設值為 NO，若設定為 YES，則 log 內容會採用
# 標準 xferlog 格式(wu-ftp 日誌檔所採用的格式)

#xferlog_file=/var/log/xferlog
# xferlog_file 用來指定 wu-ftp 格式的 log 存放位置

#dual_log_enable=YES
```

```
# dual_log_enable 預設值為 NO，若設定為 YES
# 則 /var/log/xferlog 及 /var/log/vsftpd.log 均會記錄 FTP 相關 log

#setproctitle_enable=YES
# setproctitle_enable 預設值為 NO，若設定為 YES
# 則查看系統 process 狀態時，會列出 ftp 連線的狀態
# 例如執行 ps -ef | grep vsftp 可看到誰正在連線
# nobody 4424 ... vsftpd: 127.0.0.1: not logged in

#####
#                               Transfer Settings                               #
#                               傳輸檔案的相關設定                               #
#####

connect_from_port_20=YES
# connect_from_port_20=YES 代表主動模式的資料連線是用 port 20
# connect_from_port_20 其預設值為 NO

#idle_session_timeout=600
# idle_session_timeout 設定 FTP Client 多久(單位:秒)
# 未執行任何 ftp 指令動作，便將其斷線，預設值為 300 秒

#data_connection_timeout=120
# 允許資料傳輸時 idle 的秒數，預設值是 300

#async_abor_enable=YES
# async_abor_enable 預設值為 NO，必須要 FTP Client 有支援 async_abort 的
機制才可打開

#ascii_upload_enable=YES
# ascii_upload_enable 預設值為 NO，若設為 YES 則使用者
# 可用 ascii 方式上傳資料，不過若啟用此參數可能會導致 Dos 攻擊，
# 所以都採用預設值

#ascii_download_enable=YES
# 同上，ascii_download_enable 預設值為 NO，若設為 YES 則使用者
# 可用 ascii 方式下載資料，不過若啟用此參數可能會導致 Dos 攻擊，
# 所以都採用預設值
```

**#pasv\_enable=NO**

# pasv\_enable 預設值為 YES，若設為 NO，FTP Client 則無法使用被動模式 FTP

**pam\_service\_name=vsftpd**

# vsftpd PAM 模組的名稱，其存放位置於/etc/pam.d/目錄

**#listen=YES**

# listen 預設值為 NO，若設定為 YES，則 vsftpd 會用 standalone 方式啟動