**Passive FTP**

Passive FTP works differently:

1. Your client connects to the FTP server by establishing an FTP control connection to port 21 of the server. Your commands such as ls and get are sent over that connection.
2. Whenever the client requests data over the control connection, the client initiates the data transfer connections to the server. The source port of these data transfer connections is always a high port on the client with a destination port of a high port on the server.

Passive FTP should be viewed as the server never making an active attempt to connect to the client for FTP data transfers. Because client always initiates the required connections, passive FTP works better for clients protected by a firewall.

As Windows defaults to active FTP, and Linux defaults to passive, you'll probably have to accommodate both forms when deciding upon a security policy for your FTP server.

**Regular FTP**

By default, the VSFTPD package allows regular Linux users to copy files to and from their home directories with an FTP client using their Linux usernames and passwords as their login credentials.

VSFTPD also has the option of allowing this type of access to only a group of Linux users, enabling you to restrict the addition of new files to your system to authorized personnel.

The disadvantage of regular FTP is that it isn't suitable for general download distribution of software as everyone either has to get a unique Linux user account or has to use a shared username and password. Anonymous FTP allows you to avoid this difficulty.

**Anonymous FTP**

Anonymous FTP is the choice of Web sites that need to exchange files with numerous unknown remote users. Common uses include downloading software updates and MP3s and uploading diagnostic information for a technical support engineers' attention. Unlike regular FTP where you login with a preconfigured Linux username and password, anonymous FTP requires only a username of anonymous and your email address for the password. Once logged in to a VSFTPD server, you automatically have access to only the default anonymous FTP directory (/var/ftp in the case of VSFTPD) and all its subdirectories.

# Testing the Status of VSFTPD

You can always test whether the VSFTPD process is running by using the netstat -a command which lists all the TCP and UDP ports on which the server is listening for traffic. This example shows the expected output.

[root@bigboy root]# netstat -a | grep ftp

tcp 0 0 \*:ftp \*:\* LISTEN

[root@bigboy root]#

If VSFTPD wasn't running, there would be no output at all.

# The vsftpd.conf File

VSFTPD only reads the contents of its vsftpd.conf configuration file only when it starts, so you'll have to restart VSFTPD each time you edit the file in order for the changes to take effect. The file may be located in either the /etc or the /etc/vsftpd directories depending on your Linux distribution.

This file uses a number of default settings you need to know about.

* VSFTPD runs as an anonymous FTP server. Unless you want any remote user to log into to your default FTP directory using a username of anonymous and a password that's the same as their email address, I would suggest turning this off. The configuration file's anonymous\_enable directive can be set to no to disable this feature. You'll also need to simultaneously enable local users to be able to log in by removing the comment symbol (#) before the local\_enable instruction.
* If you enable anonymous FTP with VSFTPD, remember to define the root directory that visitors will visit. This is done with the anon\_root directive.

anon\_root=/data/directory

* VSFTPD allows only anonymous FTP downloads to remote users, not uploads from them. This can be changed by modifying the anon\_upload\_enable directive shown later.
* VSFTPD doesn't allow anonymous users to create directories on your FTP server. You can change this by modifying the anon\_mkdir\_write\_enable directive.
* VSFTPD logs FTP access to the /var/log/vsftpd.log log file. You can change this by modifying the xferlog\_file directive.
* By default VSFTPD expects files for anonymous FTP to be placed in the /var/ftp directory. You can change this by modifying the anon\_root directive. There is always the risk with anonymous FTP that users will discover a way to write files to your anonymous FTP directory. You run the risk of filling up your /var partition if you use the default setting. It is best to make the anonymous FTP directory reside in its own dedicated partition.

The configuration file is fairly straight forward as you can see in the snippet below where we enable anonymous FTP and individual accounts simultaneously.

## Other vsftpd.conf Options

There are many other options you can add to this file:

* Limiting the maximum number of client connections (max\_clients)
* Limiting the number of connections by source IP address (max\_per\_ip)
* The maximum rate of data transfer per anonymous login. (anon\_max\_rate)
* The maximum rate of data transfer per non-anonymous login. (local\_max\_rate)

Descriptions on this and more can be found in the vsftpd.conf man pages.