

FTP es un servicio TCP inusual, en el sentido que utiliza dos puertos TCP para realizar su trabajo. El puerto 21 es para que cliente y servidor intercambien comandos (get, put, etc.) y el puerto 20 es el que se utiliza para la transferencia de los datos (listados y archivos).

En modo "activo", el cliente se conecta usando un puerto no privilegiado (el primero libre mayor que 1024, denotémoslo por N) al puerto 21 del servidor. Inmediatamente el cliente comienza a "escuchar" en el puerto N+1 y le dice al servidor "conéctate tu puerto 20 hacia mí puerto N+1". ¿Cuál es el problema? Si estás en un firewall, la segunda parte de la negociación luce como "una conexión remota desde cualquier puerto hacia un puerto no privilegiado de una máquina interna"; eso usualmente está bloqueado.

En modo "pasivo", el cliente se conecta usando un puerto no privilegiado (el primero libre mayor que 1024, denotémoslo por N) al puerto 21 del servidor. Inmediatamente indica "quiero trabajar en modo pasivo" usando esa conexión (después de todo, es el comando PASV), y abre el puerto N+1 y se conecta con el puerto 20 del servidor. Esto es "firewall-friendly" porque son solamente salidas.