**[FTP主动模式和被动模式的区别](https://www.cnblogs.com/xiaohh/p/4789813.html)**

**基础知识：**

　　FTP只通过TCP连接,没有用于FTP的UDP组件.FTP不同于其他服务的是它使用了两个端口, 一个数据端口和一个命令端口(或称为控制端口)。通常21端口是命令端口，20端口是数据端口。当混入主动/被动模式的概念时，数据端口就有可能不是20了。

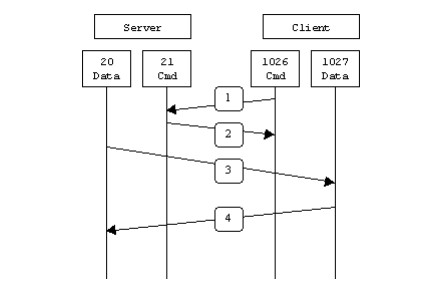
**主动模式FTP：**

　　主动模式下，FTP客户端从任意的非特殊的端口（N > 1023）连入到FTP服务器的命令端口--21端口。然后客户端在N+1（N+1 >= 1024）端口监听，并且通过N+1（N+1 >= 1024）端口发送命令给FTP服务器。服务器会反过来连接用户本地指定的数据端口，比如20端口。

　　以服务器端防火墙为立足点，要支持主动模式FTP需要打开如下交互中使用到的端口：

* FTP服务器命令（21）端口接受客户端任意端口（客户端初始连接）
* FTP服务器命令（21）端口到客户端端口（>1023）（服务器响应客户端命令）
* FTP服务器数据（20）端口到客户端端口（>1023）（服务器初始化数据连接到客户端数据端口）
* FTP服务器数据（20）端口接受客户端端口（>1023）（客户端发送ACK包到服务器的数据端口）

**用图表示如下：**



　　在第1步中，客户端的命令端口与FTP服务器的命令端口建立连接，并发送命令“PORT 1027”。然后在第2步中，FTP服务器给客户端的命令端口返回一个"ACK"。在第3步中，FTP服务器发起一个从它自己的数据端口（20）到客户端先前指定的数据端口（1027）的连接，最后客户端在第4步中给服务器端返回一个"ACK"。

　　主动方式FTP的主要问题实际上在于客户端。FTP的客户端并没有实际建立一个到服务器数据端口的连接，它只是简单的告诉服务器自己监听的端口号，服务器再回来连接客户端这个指定的端口。对于客户端的防火墙来说，这是从外部系统建立到内部客户端的连接，这是通常会被阻塞的。

**被动模式FTP**

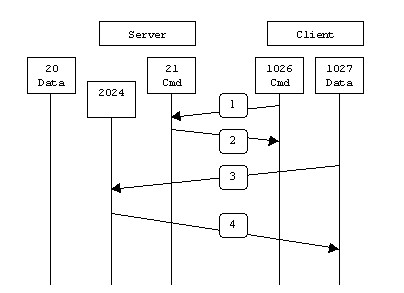
　　为了解决服务器发起到客户的连接的问题，人们开发了一种不同的FTP连接方式。这就是所谓的被动方式，或者叫做PASV，当客户端通知服务器它处于被动模式时才启用。

　　在被动方式FTP中，命令连接和数据连接都由客户端，这样就可以解决从服务器到客户端的数据端口的入方向连接被防火墙过滤掉的问题。当开启一个FTP连接时，客户端打开两个任意的非特权本地端口（N >; 1024和N+1）。第一个端口连接服务器的21端口，但与主动方式的FTP不同，客户端不会提交PORT命令并允许服务器来回连它的数据端口，而是提交PASV命令。这样做的结果是服务器会开启一个任意的非特权端口（P >; 1024），并发送PORT P命令给客户端。然后客户端发起从本地端口N+1到服务器的端口P的连接用来传送数据。

　　对于服务器端的防火墙来说，必须允许下面的通讯才能支持被动方式的FTP:

* FTP服务器命令（21）端口接受客户端任意端口（客户端初始连接）
* FTP服务器命令（21）端口到客户端端口（>1023）（服务器响应客户端命令）
* FTP服务器数据端口（>1023）接受客户端端口（>1023）（客户端初始化数据连接到服务器指定的任意端口）
* FTP服务器数据端口（>1023）到客户端端口（>1023）（服务器发送ACK响应和数据到客户端的数据端口）

**用图表示如下：**



　　在第1步中，客户端的命令端口与服务器的命令端口建立连接，并发送命令“PASV”。然后在第2步中，服务器返回命令"PORT 2024"，告诉客户端（服务器）用哪个端口侦听数据连接。在第3步中，客户端初始化一个从自己的数据端口到服务器端指定的数据端口的数据连接。最后服务器在第4 步中给客户端的数据端口返回一个"ACK"响应。

　　被动方式的FTP解决了客户端的许多问题，但同时给服务器端带来了更多的问题。最大的问题是需要允许从任意远程终端到服务器高位端口的连接。幸运的是，许多FTP守护程序，包括流行的WU-FTPD允许管理员指定FTP服务器使用的端口范围。详细内容参看附录1。

　　第二个问题是客户端有的支持被动模式，有的不支持被动模式，必须考虑如何能支持这些客户端，以及为他们提供解决办法。例如，Solaris提供的FTP命令行工具就不支持被动模式，需要第三方的FTP客户端，比如ncftp。

　　随着WWW的广泛流行，许多人习惯用web浏览器作为FTP客户端。大多数浏览器只在访问ftp://这样的URL时才支持被动模式。这到底是好还是坏取决于服务器和防火墙的配置。

**备注：**

　　有读者指出，当NAT(Network Address Translation)设备以主动模式访问FTP服务器时，由于NAT设备不会聪明的变更FTP包中的IP地址，从而导致无法访问服务器。

**总结**

　　下面的图表会帮助管理员们记住每种FTP方式是怎样工作的：  
  
　　主动FTP：  
   　　命令连接：客户端 >1023端口 -> 服务器 21端口  
   　　数据连接：客户端 >1023端口 <- 服务器 20端口   
  
　　被动FTP：  
   　　命令连接：客户端 >1023端口 -> 服务器 21端口  
   　　数据连接：客户端 >1023端口 -> 服务器 >1023端口   
  
　　下面是主动与被动FTP优缺点的简要总结：

　　主动FTP对FTP服务器的管理有利，但对客户端的管理不利。因为FTP服务器企图与客户端的高位随机端口建立连接，而这个端口很有可能被客户端的防火墙阻塞掉。被动FTP对FTP客户端的管理有利，但对服务器端的管理不利。因为客户端要与服务器端建立两个连接，其中一个连到一个高位随机端口，而这个端口很有可能被服务器端的防火墙阻塞掉。

　　幸运的是，有折衷的办法。既然FTP服务器的管理员需要他们的服务器有最多的客户连接，那么必须得支持被动FTP。我们可以通过为FTP服务器指定一个有限的端口范围来减小服务器高位端口的暴露。这样，不在这个范围的任何端口会被服务器的防火墙阻塞。虽然这没有消除所有针对服务器的危险，但它大大减少了危险。详细信息参看附录1