使用 OptiView PE 协议分析专家软件对服务器连通性进行故障诊断

美国福禄克网络公司

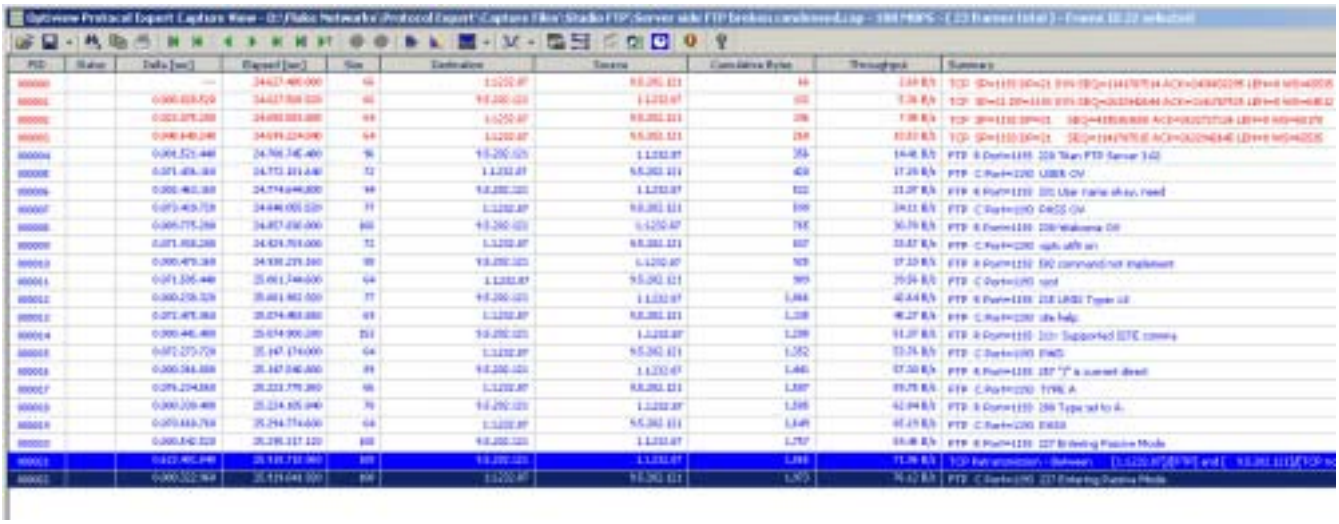
当使用 OptiView PE 协议分析软件对服务器的连通性问题进行故障诊断时，很重要的一点是要清楚数据传输的双方。客户端正向服务器发送什么？服务器正向客户端发送什么。当您了解连接的双方时，就可以更容易地查找到问题。

我们不妨拿福禄克网络的技术支援中心最近遇到的一个问题作为例子，一个客户试图连接到一台 FTP 服务器，该客户可以建立连接并看到登录屏幕，但在输入登录信息后，客户端被告之文件列表错误。同一局域网上一个相邻站点却可以登录到 FTP 服务器上并下载文件。在其它远程网络上的用户也可以连接到这台 FTP 服务器上并下载文件。这就表明这台 FTP 服务器至少是可以访问的而且功能正常（否则用户就不能接收到登录屏幕），两个网络之间的路由是正常工作的（因为邻近的站点可以下载文件）。问题可能出在客户端上。

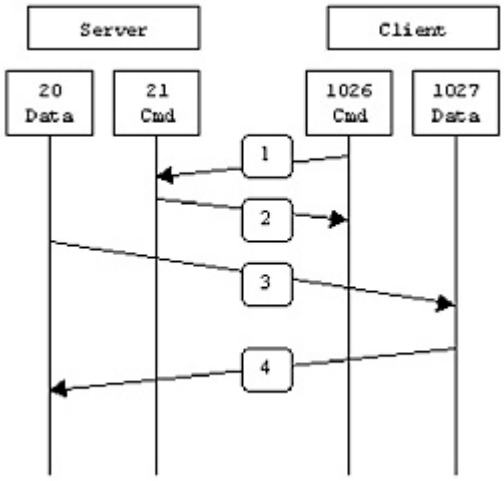
服务器已经安装了 OPV-PE 协议分析专家软件，所以我们启动了捕捉功能并要求出现问题的用户再次登录。 在用户得到错误提示后，我们停止了捕捉并开始分析协议跟踪文件。

跟踪文件已经被过滤为客户端和 FTP 服务器 IP 地址之间的对话。

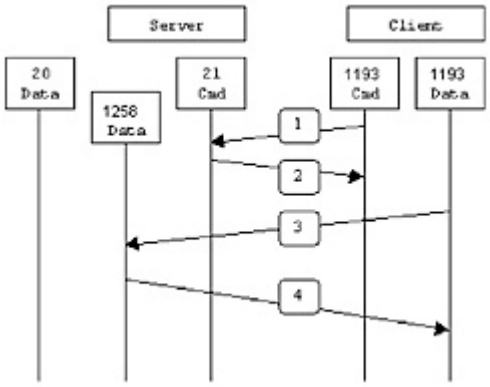
首先，在 0-2 帧客户端与服务器建立了 TCP 标准握手，这就确立了在端口 21 上的 FTP 帧可以到达服务器，且服务器可以认可该通讯。



帧 4 显示服务器开始 FTP 进程，它通知客户端所连接的 FTP 服务器类型。接下来的几个帧是登录认证信息和密码互换。一切看起来都很正常，直到我们查看第 19 帧。客户端通知服务器它要在被动 FTP 模式下进行操作。FTP 在端口 21 上不传输实际数据，这是一个用于交换密码和控制信息的控制端口——我们可以从协议文件中查看到。正常的主动 FTP 传输，服务器使用端口 20 来将文件“ 推 ”到用户所使用的端口。在某种意义上，客户端成为了服务器并接收“ 推 ”过来的文件。

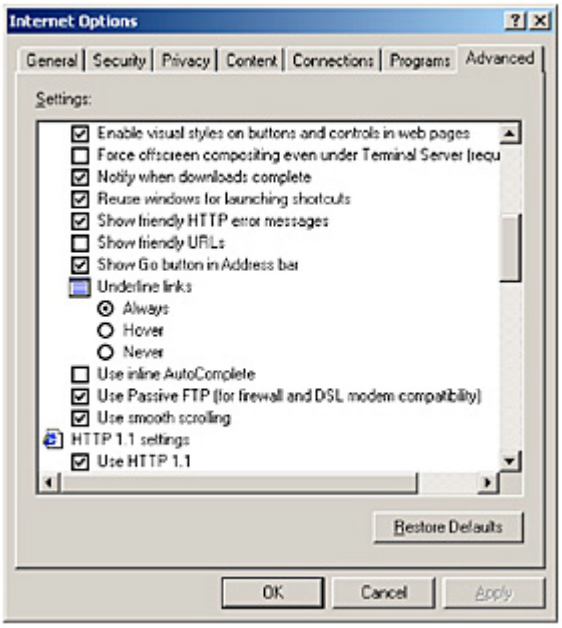


在被动 FTP 模式下，客户端要求保持客户模式并要求服务器发送给它一个安全的数据端口以要求文件传输。在这种方式下，客户端开始初始化与服务器的双方连接，保证客户端更大的安全性。防火墙不需要为 FTP 服务器开放来连接到客户端，主动模式也是一样。



我们可以不再假设服务器在使用端口 20 进行数据传输。它通知客户端在端口 21 控制帧中它将使用哪个端口。在我们的例子中，帧 20 显示出发送给客户端进行连接的 IP 和端口号。

服务器通知它可以通过 IP 地址 1.1.232.65 被联络，之后是数字 4 和 234。为了发现端口号，我们需要将第一个数字乘以 256 再加上第二个数字，即 (256*4)+234=1258。该 IP 和这对端口存在几个问题。首先，FTP 服务器的地址不是 1.1.232.65 而是 1.1.232.87。其次，防火墙仅被配置为允许在端口 20 和 21 到 FTP 服务器的流量。它没有被配置为支持被动 FTP 模式。这种模式由于它的安全性已经变得越来越普遍。可以通过 IE 配置为被动 FTP 模式，具体方法是使用“工具| Internet|选项| 高级”标签页进行设置。



特别是 Windows XP SP2 的用户，用户端安全性更高。

在这种情况下，FTP 服务器在被动模式下被配置了错误的地址。服务器中的这一变量没有正确设置。在这一问题修复后，防火墙被打开支持 1200 以上的 FTP 通讯端口，客户可以正常访问文件。毫无疑问它可以将流量发送回服务器，但它的目的地址是 1.1.232.65，它是网关的地址。这是使用 OPV-PE 协议分析专家软件很容易就解决的故障实例。