防火墙——友好 FTP

本备忘录状态

本备忘录提供了 Internet community 的信息，但不说明任何一种类型的 Internet 标准。发布本备忘录不受限制。

概要

本备忘录描述了改变 FTP 程序的行为的建议。没有协议需要修改，虽然我们大致描述了一些可能的应用。

总的看法

在实际传输文件时，FTP 协议[1]使用了二级 TCP 连接。缺省的情况下，这个连接是从 FTP 服务器主动到 FTP 客户端建立的。不过，这样设计不能在基于过滤的防火墙中以包的形式很好地工作，一般情况下还不允许调用任意的端口号。

从另一方面来讲，如果客户端使用 PASV 指令，数据信道在穿过防火墙时会变为外部调用。这样的调用更容易掌握，也不容易引起问题。

详细描述

FTP 规范提到，在缺省的情况下，所有的数据传输都是建立在一个单一连接上的。对于控制连接，服务器主动开放它的 20 号端口到客户端机器的相同端口，客户端是被动开放的。

因为效果时好时坏，大多数的 FTP 客户端不采用这种方式。每次传输都建立一个新的连接，为了避免 TCP 的 TIMEWAIT 状态的冲突，客户端每次选取一个端口号然后给服务器发一个 PORT 命令，把这个端口号告诉服务器。

这两种情况都不是友好的防火墙。如果使用一个信息包过滤器（比如，大多数的先进路由器都提供），数据信道在流入到未知端口时要求获悉。大多数的防火墙的构建只允许流入到确定的安全可信的端口，比如 SMTP。通常危及“服务器”安全的区域是 1024 号以下的端口。但是这个策略也是危险的，比如 X windows 开放更高的端口号就是危险的服务。

另一方面，不管是对防火墙的管理员还是对信息包过滤器来说，流出的信息包带来的问题少一些。任何含有 ACK 位的 TCP 信息包都不能利用信息包进行初始化 TCP 连接。过滤器能设置流出外界的信息包的规则。我们之所以想改变这个操作是因为数据信道执行了一个从客户端到服务器端的调用。

幸运的是，必要的机制已经存在于协议中。如果客户端发送了一个 PASV 指令，服务器将被动地打开在一些随机的端口，并把端口号通知客户端。客户端能主动地打开一个端口来建立连接。

实际上有少数 FTP 服务器不承认 PASV 指令。这样做并不合适（因为不符合 STD 3, RFC 1123 [2]），不过它确实不会引起问题。对于一个不被承认的操作将返回“500 指令不明”的消息，它用简单的办法使当前的操作失败。虽然攻击不可能通过防火墙，但是 PASV 在这样的情况下也失效了。

推荐

我们推荐防火墙的商家在他们的客户端程序中用 PASV 指令代替 PORT 指令（包括 FTP 代理，比如 Gopher [3] daemons）。甚至在没有防火墙的传输中也没有理由不使用它，作为标准的操作来采用它，能使一个在防火墙环境里的客户端更好用。

讨论

大多数流行的 FTP 客户端给出的操作，在 PASV 使用时不会给发送的信息带来任何附加的信息。在所有的情况下，在客户端和服务器端进行传输操作之前先进行一个附加的信息交换，如果交换包含 PORT 指令或 PASV 指令，就不会出问题。

也有一些 Gopher 风格的客户端，因为他们每次控制信道的连接都正确地传输一个文件，所以他们不需要使用 PORT 指令。如果关系到比较严肃的传输，Gopher 代理器会定位在防火墙之外，所以它不会被信息包过滤器的规则所限制。

如果允许客户端总是执行主动的开放连接，为了增强 FTP 协议完全消除额外的交换，这样做是值得的。在启动的时候，客户端会发送一个新的指令 APSV（“all passive”），服务器将总是执行被动的开放连接。在响应时，所有文件传输请求在没有接收到 PORT 或 PASV 指令之前，会发送一个 151 应答码，该消息将包含供传输使用的端口号。已经接收到先前的 APSV 指令，仍旧会发送一个 PORT 指令到服务器，这样将不理会下次传输操作的缺省操作，所以允许三方传输。

执行状态

可编辑的客户端至少存在两个不受约束的实现。其中一个是源代码可以自由地使用。我们知道，APSV 不能被实现。

安全方面的考虑

有些人觉得信息包过滤器是危险的，因为对他们来说，进行合理的配置很困难。我们也同意这点。但是这样的人群非常普遍。另一个普遍抱怨的是任意允许流出信息包也是危险的，因为它允许通过防火墙自由地输出敏感的数据。对该方法的优点的讨论已超出本文的范围。我们注意到分级应用网关的排序需要执行一个可执行的带宽限制，就像使用 PASV 和 PORT 一样容易。

使用 PASV 能提高网关机器的安全，因为它们不再需要创建端口。更重要的是，如果不需要指定一个“创建”操作，客户端主机和防火墙之间的协议可以得到简化。

已经注意到用来进行交换的 PASV 的应用会带来一个另外的问题。服务器必须同意调用任意随机的端口号，这将给防火墙引起一个同样的问题。我们认为因为有以下的原因，它不是一个严肃的解决方案。

首先，FTP 服务器相对于客户端来说是很少的。可能只是为了保护很少数量的特定目的的机器，比如网关和组织的 FTP 服务器。防火墙的过滤器能对这些机器的访问权限进行配置。为了更进一步地预防，FTP 服务器被修改成仅能使用很有限的一些端口号用来做数据信道。它很容易确保在

一个给定的端口号范围内提供安全的服务。此外，因为服务器的数量很少，所以这样做是可行的。

参考书目

[1] Postel, J., and J. Reynolds, “文件传输协议”，STD 1, RFC 959, USC/信息科学学会, 1985 年 10 月。

[2] Braden, R., Editor, “互联网主机必要条件——应用程序和支持”, STD 3, RFC 1123, USC/信息科学学会, 1989 年 10 月。

[3] Anklesaria, F., McCahill, M., Lindner, P., Johnson, D., Torrey, D., and B. Alberti, “Internet Gopher 协议（一个分布式文档搜索和获取协议）”, RFC 1436, 明尼苏达州大学, 1993 年 3 月。

作者地址

（略——译者注）

原文：RFC 1579 《Firewall-Friendly FTP》
译者：comehope 2002 年 5 月
博客：http://www.comehope.com