

P2P限速问题剖析

在使用 PatrolFlow 设备做 P2P 限速时，有时我们会发现“限速不准”，根据我们的实施经验，“限速不准”的原因多种多样，在这里一与大家分享，并着重介绍高校发现 P2P 直接下载内网资源的案例。

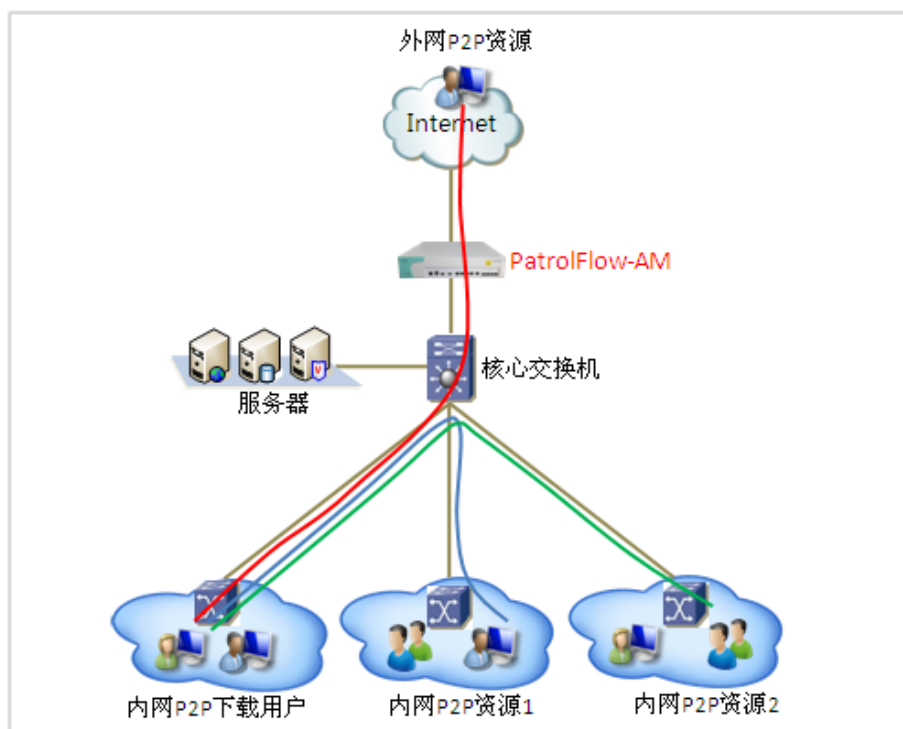
配置方面

首先要确保相关模块状态的正确性，包括“带宽控制”模块状态为“开启”，“P2P 传输识别”模块状态为“开启”，“P2P 传输识别方式”模块状态为“严格”；其次限制 P2P 的应用时同时需要限制“多线程的 P2P”和“模式识别的 P2P”，P2P 最大的一个特点就是抢占带宽，而这是通过同时发起多个连接来做到，P2P 的行为具有一定的隐蔽性，有时会使用熟知 80 端口来传输，但是 P2P 最基本的特征就是点到点的传输，所以我们需要同时限制“多线程的 P2P”和“模式识别的 P2P”；最后我们还要检查配置的对象、时间策略是否正确，有时配置的对象为组，但是测试的用户不在此组内，或者系统当前时间不在配置的生效时间内。

资源方面

在 P2P 测速时需要确认下载的资源，如使用迅雷去下载一个 FTP 的资源这种行为不能认为是 P2P 下载，而是 FTP 文件传输，所以在出现“限速不准”时也需要分析下载的资源，也可以通过设备的实时应用排名或审计日志查看；另外就是 P2P 下载会搜索并下载内网资源的情况，下面着重介绍这一现象。

在一些高校部署 PatrolFlow 设备做 P2P 流量管理时发现 P2P 软件迅雷在搜索到局域网内有资源上传时可直接通过内网下载。高校的网络具有局域网内计算机多、P2P 应用多的特点，众多的学生在下载资源的同时也被动上传资源，增加了“限速不准”的概率。通过在 P2P 流量“限速不准”的计算机上安装 Ethereal 抓包软件抓包分析到，客户端下载的资源来自 Internet 和内网两部分，来自 Internet 的资源经过 PatrolFlow，P2P 流量管理可以精确控制，但另外一部分资源在内网，直接通过局域网交换机传输，不经过 PatrolFlow 设备，这些来自内网的流量自然无法进行控制，如下图：



P2p 下载的资源来自 Internet 和内网两部分

我们知道 P2P 技术是端（Peer）到端（Peer）对等网络技术，网络主机在充当客户端获取资源的同时也充当服务器向其它对等体提供服务；向多个服务器并发多个连接抢占带宽资源是 P2P 技术最显著的特点；P2P 应用基本不使用固定端口，并且通常还会使用知名端口 80 来防止被发现，具有一定的隐蔽性。百卓网络通过 DPI+流量模型相结合的方式识别 P2P 应用，并可以精确的管控。