

## 互联网审计设备选型及旁路模式部署指导

### 审计产品选型

#### 1、处理性能

为了保证监听内容的完整性，所选择审计设备的处理性能必须大于所要监听链路实际双向数据流量的总和。例如：假设需要监听一条千兆链路的数据内容，当该链路的实际上行流量为 500Mbps，下行流量为 800Mbps 时，则要求所选择设备的处理性能不小于 1.3Gbps(500Mbps+800Mbps)即可。而如果该链路的上下行流量均满载，则要求所选择设备必须至少提供 2Gbps(2\*1Gbps)的监控数据处理性能，其它情况以此类推。

#### 2、在线用户数

不同型号的审计设备支持不同用户数量规模的监听网络，选择的审计设备所支持的最大用户数量必须大于实际监听网络的同时在线用户数。例如：假设需要监听一个网络规模为 500K 用户的网络，当该网络同时在线用户数为 50K 时，则要求所选择设备支持的最大用户数大于 50K 即可。而如果该网络所有用户都同时在线，则要求所选择设备支持的最大用户数必须大于 500K。

### 旁路部署时的注意事项

在监听骨干链路数据内容时，为了最大限度保证骨干链路的可靠性和连通性，建议采用旁路模式部署审计设备，不建议采用串接方式部署。同时，在交换机组网环境下和路由器组网环境下进行旁路模式部署时分别需要注意以下事项。

交换机组网环境下进行旁路部署时，通常采用交换机端口镜像功能将监听数据导入到审计设备中，如下图：



端口镜像图例

在交换机端口镜像环境中还存在两种不同的镜像配置方式，每种配置方式的详细描述见下图，在实际项目实施过程中强烈推荐采用双目的镜像端口方式。

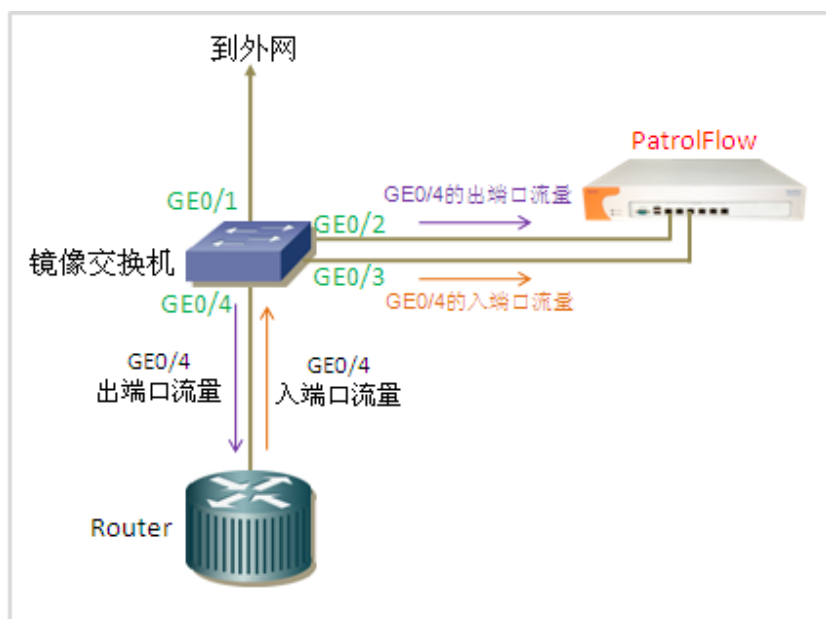


单镜像目的端口

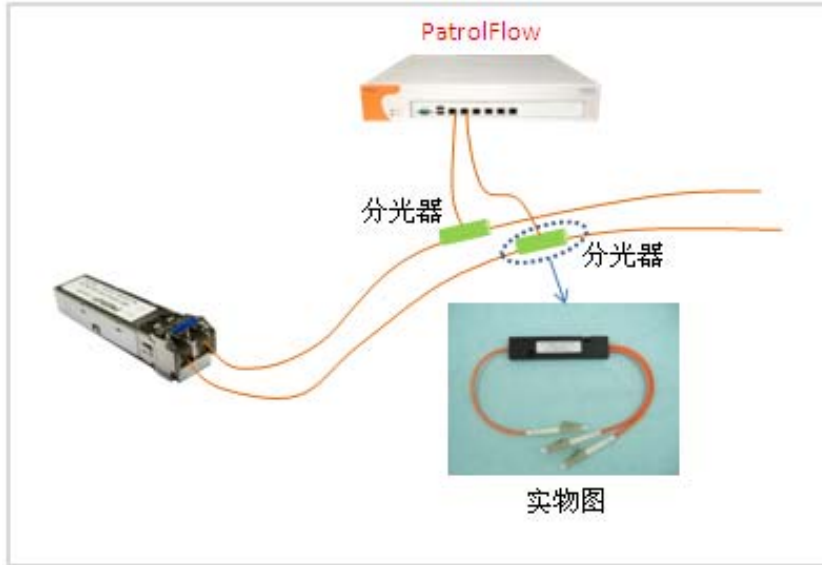


双镜像目的端口

路由器组网环境下进行旁路部署时，通常情况下路由器不具备端口镜像能力。因此，我们需要借助其它设备的帮助来将数据导入到审计设备中，通常有以下两种方式：



串接交换机做端口镜像



采用分光器进行分流