某局点ADWAN 分析器场景netstream 流分析流量不准确的经验案例

SeerAnalyzer　ADWAN解决方案　刘洋帆　2024-04-12 发表

组网及说明

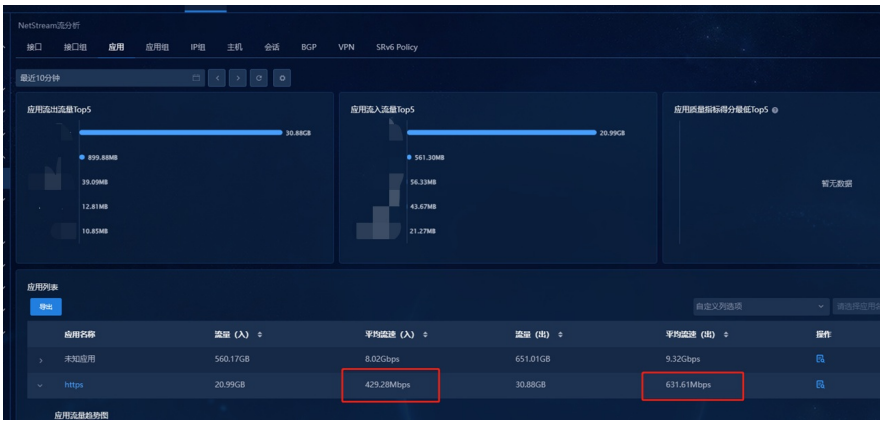
ADWAN承载网方案，在现场一台设备的所有接口均添加到了分析器netstream的接口中

告警信息

无

问题描述

现场反馈实际https流量约为带宽占比约30%-50%，但是控制器上显示的https流量远小于该数值



过程分析

由于netstream流分析存在数据，说明采集任务等配置没问题，netstream需要配置IP组，应用组和接口。

查看现场配置，IP组未具体指定，接口确认已全部添加。

查看应用组配置，发现在应用组中自定义的https应用，仅定义源为任意，目的为443 端口的https流量

解决方法

对于实际业务流量而言，源任意，目的为443 的流量为终端主动发起请求的流量，实际还存在源为服务器端回复的流量，该流量对应的源端口为443 ，目的端口为任意，而且通常实际回复流量原大于访问流量，对于分析器而言，匹配的流量为单向匹配计数。

因此根据需要，需在应用配置页面新增一条源为客户端端口443 的应用，在配置完成后，显示流量符合客户预期