# 防火墙基于应用的带宽保证不生效

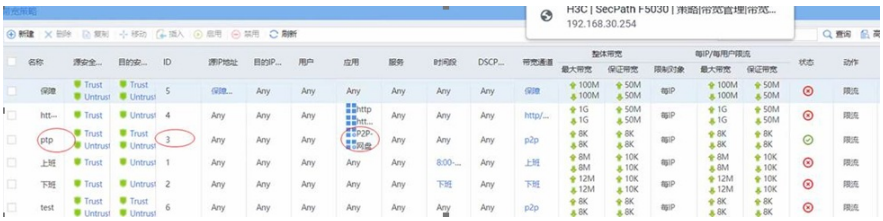
应用审计 张志潮 2021-07-29 发表

## 组网及说明

防火墙作为出口设备

## 问题描述

使用下图带宽策略对迅雷下载进行限速。




现场反馈只有前几分钟可以限住，后面速度就上去了。测试地址：192.168.30.211。

## 过程分析

后面远程上去复现，发现速度一直维持在8k左右。然后重新用迅雷换了一个资源下载测试，发现一开始速度就限不住

这时候检查流量策略信息如下：

*[H3C]dis traffic-policy statistics bandwidth downstream per-rule name ptp*

*Slot 1 :*

*Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Bytes), PR(Passed Rate:kbps), DR(Dropped Rate:kbps), FPP(Final Passed Packets), FPB(Final Passed Bytes),FPR(Final Passed Rate:kbps)*

---

*Rule name State Profile name PP PB DP DB PR DR FPP FPB FPR*

---

*ptp Enabled p2p 7292 7906420 0 0 0.0 0.0 7292 7906420 0.0*

---

同时检查对应规则命中次数，发现hit不增长

*[H3C]dis traffic-policy statistics rule-hit rule ptp*

*Slot 1 :*

---

*Rule ID Rule name State Profile ID Profile name Hit*

---

*3 ptp Enabled 3 p2p 349*

---

---

*[H3C]dis traffic-policy statistics rule-hit rule ptp*

*Slot 1 :*

---

*Rule ID Rule name State Profile ID Profile name Hit*

---

*3 ptp Enabled 3 p2p 349*

---

---

*[H3C]dis traffic-policy statistics rule-hit rule ptp*

*Slot 1 :*

---

*Rule ID Rule name State Profile ID Profile name Hit*

---

*3 ptp Enabled 3 p2p 349*

---

查看实时流量排行，发现此时流量类型主要是通用http下载，于是怀疑是应用选择p2p无法匹配到该类型。

但是现场关闭该策略后，下载同一文件速度在14M左右，看现象限速还是起了作用，但是无法限到8K。

## 解决方法

使用迅雷下载文件的时候，收集会话，检查application这个字段的内容

根据下载内容的不通，可能被设备识别为不同的类型，例如下载windows镜像的时候，识别为**Application：MICROSOFT**

由于带宽策略中并不包含该选项，导致限速无法生效。添加上后再测试，正常。