

知 F1000应用限速不生效经验案例

应用审计 曹圣琪 2024-09-27 发表

问题描述

现场配置针对腾讯应用的限速后web界面显示应用流量超限速。

1、现场配置：

名称	源安全域	目的安全域	ID	源地址	目的地址	用户	应用	服务	时间	DSCP	策略	IP协议	IPV4扩展	策略描述	整体带宽	每IP/每用户限速	状态	动作	命中数
限速	Trust	Untrust	1	Any	Any	Any	腾讯资源	Any	Any	Any	Any	限速	限速	限速	50M	50M	启用	限速	1550

修改带宽通道

名称 * (1-63字符)

带宽限流

限流方式 分别设置上下行带宽 设置总带宽

整体带宽

引用方式 策略独占 策略共享

上行带宽

最大: Mbps (1-1000000)

保证: Mbps (1-1000000)

下行带宽

最大: Mbps (1-1000000)

保证: Mbps (1-1000000)

转发优先级

每IP/每用户限流

限制对象 每IP 每用户

IP间带宽分配策略 动态均分

上行带宽

最大: Mbps (1-1000000)

保证: Mbps (1-1000000)

下行带宽

最大: Mbps (1-1000000)

2、测试结果，整体带宽超过50Mbps：

流量实时应用排行

排行	应用	下行流速	上行流速	总流速	百分比
1	腾讯资源	14.90 MB/s	714.62 KB/s	15.62 MB/s	40.30%
2	HTTPS其他应用	13.52 MB/s	656.59 KB/s	14.17 MB/s	36.57%
3	Adobe	1.62 MB/s	113.42 KB/s	1.74 MB/s	4.48%
4	UDP其他应用	470.69 KB/s	1.00 MB/s	1.47 MB/s	3.80%
5	微信	1.15 MB/s	90.59 KB/s	1.24 MB/s	3.19%
6	microsoft-ds	967.44 KB/s	259.60 KB/s	1.23 MB/s	3.16%
7	微软官网	993.62 KB/s	59.32 KB/s	1.05 MB/s	2.71%
8	腾讯视频	440.77 KB/s	77.08 KB/s	517.85 KB/s	1.33%

过程分析


1) 现场IPV4业务，但是命令行中无计数：

```
display traffic-policy statistics bandwidth downstream per-ip ipv4 rule 限速24Mbps
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  IP      PP      PB      DP      DB      PR      DR      FPP
-----
FPB      FPR
-----
<qiaonan>
```

2) 应用层检测引擎的运行状态正常:

```
<[redacted]>display inspect status
Chassis 0 Slot 1:
Running status: Normal
```

3) 怀疑有其他流量未被限制, 修改策略中的源目安全域为any-any还是不行



名称	源安全域	目的安全域	ID	源地址	目的地址	用户	应用	服务	协议	DSCP	终端	IPv4	IPv6	带宽	整体带宽	限制对象	保证带宽	最大带宽	每IP每用户带宽	状态	动作	命中	编辑
-	Any	Any	1	Any	Any	Any	腾讯资源	Any	Any	Any	Any	限速		50M	50M	限速	50M	4M	4M	限速	144165		

4) 检查测试时策略命中数是增加的



名称	源安全域	目的安全域	ID	源地址	目的地址	用户	应用	服务	协议	DSCP	终端	IPv4	IPv6	带宽	整体带宽	限制对象	保证带宽	最大带宽	每IP每用户带宽	状态	动作	命中	编辑
-	Any	Any	1	Any	Any	Any	腾讯资源	Any	Any	Any	Any	限速		50M	50M	限速	50M	4M	4M	限速	144182		

5) 特征库版本为: 1.0.180当前最新版本

6) 检查带宽策略绑定了VPN, 与现场确认确实只有几个绑定了VPN的接口应用该策略

```
traffic-policy
statistics rule-hit enable
rule 1 name 限速24Mbps
action qos profile 限速
vrf VPN1
application app TencentResource
rule 2 name 专线限速
```

解决方法

经过确认: 报文处理流程上实时流量统计的业务点在带宽管理前面, 即被限速丢包的流量也会统计在实时流量统计的范围内。所以会出现比限速值高的情况, 现场可以在全局配置flow-interval 5, 检查display counters rate inbound interface各接口速率。