

知 H3C Comware V7 平台 防火墙限速策略机制 导致部分限速策略不准确案例

通道带宽管理

设备部署方式

丁犁

2021-06-30 发表

组网及说明

组网如下图所示：



FW 防火墙型号及版本为：SecPath F1000-AK135(V7) Release 9333P37

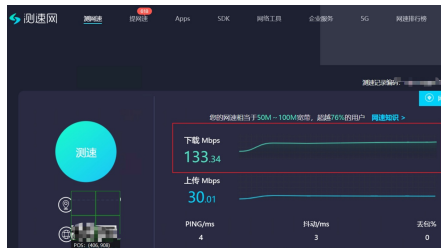
内网测速终端PC，可正常通过FW 访问外网服务器。

问题描述

FW 防火墙作为网络的出口设备，管理员在其上部署流量限速测速，限制内网每IP终端的上行和下行流量最大30Mbps。

测速终端，通过浏览器访问某运营商的测速网站，对其上行和下行网速进行测试。

测速后，出现上行流量可正常限速，但下行流量无法正常限速（下行流量速率大大超过30Mbps阈值），如下图所示：



过程分析

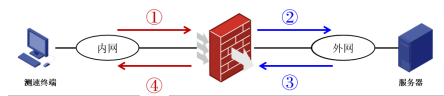
首先检查FW 防火墙上相关流量限速策略配置，其关键配置正确，未出现异常：

```
#
object-group ip address host
0 network host address 192.168.1.222 //测试终端IP地址
#
traffic-policy
rule 1 name 下行
action qos profile 30m_speed
destination-address address-set host
rule 2 name 上行
action qos profile 30m_speed
source-address address-set host
profile name 30m_speed
bandwidth downstream maximum 1000000
bandwidth upstream maximum 1000000
bandwidth upstream maximum per-ip 30000
bandwidth downstream maximum per-ip 30000
#
```

实际出现此类，限速不准确的问题，其原因为：“下行测速流量模型”与“H3C Comware V7 平台防火墙限速策略实现原理”存在差异导致，具体请将下面的分析。

测速终端，通过浏览器访问某运营商的测速网站对其上行和下行网速进行测速，其过程在web中的点击“测速”按钮后

对于 FW 防火墙，将进行如下动作：



- ① FW 收到测速终端发往服务器的请求报文。FW 查找转发表项，生成相关会话，并将流量进行转发。
- ② 将请求流量转发给服务器。
- ③ 服务器对请求流量进行回应，FW 收到回应报文后，根据之前生成是会话表项，将流量向内网测速终端进行转发出。
- ④ FW 将回应报文发给内网测速终端。

其中，①② 对应着“上行”测速流量；③④对应着“下行”测速流量。

对于 FW 防火墙设备，“上行”测速流量为请求流量，前期防火墙本地没有相关的会话表项，因此 FW 防火墙将新建会话；

对于 FW 防火墙设备，“下行”测速流量为回应流量，防火墙本地对此回应流量，FW 防火墙将不会新建会话。

H3C Comware V7 平台防火墙 流量限速策略，其实现原理是：仅能针对请求流量进行限速，对于回应流量无法进行限速处理。及按照会话表项（display session table ipv4 verbose）仅针对 Initiator->Responder 方向的流量进行限速

.....

Initiator:

Source IP/port: x.x.x.x/aa

Destination IP/port: y.y.y.y/bb

.....

Responder:

Source IP/port: z.z.z.z/cc

Destination IP/port: m.m.m.m/dd

.....

State: TCP_SYN_SENT

Application: DNS

Start time: 2019-09-23 12:35:50 TTL: 27s

Initiator->Responder: 1103 packets 45723 bytes

Responder->Initiator: 6120 packets 954690 bytes

通过了解 H3C Comware V7 平台防火墙限速策略的实现机制，再结合测速终端点击web“测速”按钮后“上行”“下行”流量模式，即可得知：

解决方法

对于“上行”测速，由于匹配了 Initiator->Responder 会话信息，因此防火墙执行限速策略动作；
对于通过上述测速模型进行测试，确实存在下行速率限制不准确的情况，该情况仅限于 H3C Comware V7 平台防火墙的实现机制，目前无法改善。

在实际的业务环境中，对于“下行”流量（比如：迅雷、IDM 等等）通常会采用不同的 TCP/UDP 端口号。对此类流量，当防火墙收到后，对于“下行”流量将会产生对应的会话信息，及“下行”流量满足会话中的 Initiator->Responder，因此在实际业务环境中，H3C Comware V7 平台防火墙可以对业务“下行”流量进行限速。

