

知 某局点SecPath F1000-AK109(V7) 业务过防火墙卡顿

域间策略/安全域 赛组亮 2021-06-28 发表

组网及说明

防火墙透明部署，属于新增设备

部署在专线和核心交换机之前，部署完成后出现两个问题：

- 1.FTP传输速率慢
- 2.视频缓存时间较长

问题描述

防火墙版本已经升级至最新版本，并且关闭DPI模块测试，故障依旧

过程分析

通过抓包分析发现

收到和发送的报文所携带的VLAN ID不稳定，下面是首包并不带VLAN ID

1 Jun 9, 2021 02:45:31.733304000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
2 Jun 9, 2021 02:45:31.733442000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
3 Jun 9, 2021 02:45:31.737856000	中国标准时间 10.81.5.21	10.81.33.18	TCP	70
4 Jun 9, 2021 02:45:34.735016000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
5 Jun 9, 2021 02:45:34.735049000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
6 Jun 9, 2021 02:45:34.742671000	中国标准时间 10.81.5.21	10.81.33.18	TCP	70
7 Jun 9, 2021 02:45:40.734631000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
8 Jun 9, 2021 02:45:40.734665000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
9 Jun 9, 2021 02:45:40.748812000	中国标准时间 10.81.5.21	10.81.33.18	TCP	66

```
<
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: 9c:06:2b:57:86:52 (9c:06:2b:57:86:52), Dst: HuaweiTe_78:40:57 (d4:6a:a8:78:40:57)
> Internet Protocol Version 4, Src: 10.81.33.18, Dst: 10.81.5.21
> Transmission Control Protocol, Src Port: 55358, Dst Port: 21, Seq: 0, Len: 0
```

但是观察回包发现：

3 Jun 9, 2021 02:45:31.737856000	中国标准时间 10.81.5.21	10.81.33.18	TCP	70
4 Jun 9, 2021 02:45:34.735016000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
5 Jun 9, 2021 02:45:34.735049000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
6 Jun 9, 2021 02:45:34.742671000	中国标准时间 10.81.5.21	10.81.33.18	TCP	70
7 Jun 9, 2021 02:45:40.734631000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
8 Jun 9, 2021 02:45:40.734665000	中国标准时间 10.81.33.18	10.81.5.21	TCP	66
9 Jun 9, 2021 02:45:40.748812000	中国标准时间 10.81.5.21	10.81.33.18	TCP	66

```
<
> Frame 3: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: HuaweiTe_78:40:58 (d4:6a:a8:78:40:58), Dst: 9c:06:2b:57:86:4a (9c:06:2b:57:86:4a)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 7
> Internet Protocol Version 4, Src: 10.81.5.21, Dst: 10.81.33.18
> Transmission Control Protocol, Src Port: 21, Dst Port: 55358, Seq: 0, Ack: 1, Len: 0
```

回包却带了VLAN ID字段

应该是该问题，来回报文异常导致业务收到影响

解决方法

现场由于来回报文VLAN ID异常（时有时无），导致丢包情况出现
所以关闭vlan检查，可以临时规避此问题
undo fast-forwarding check-vlan-id

