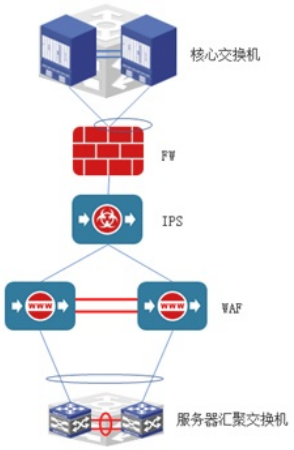
某局点S6520X 分片报文不通问题

二层转发 转发不通 **苏亚东** 2022-06-20 发表

组网及说明

测试终端192.168.212.228



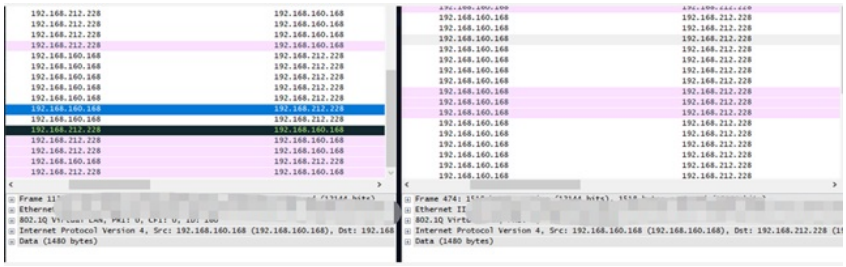
测试服务器192.168.160.168

问题描述

现场组网大致如下，核心交换机12518和S6520X之间经过透明FW和WAF聚合，由于waf侧两台设备都是单机的，如果没有会话就会将报文丢弃。因此就需要S6520X将同一条流发给同一台waf进行转发。目前现场测试发现，192.168.212.228去ping测试192.168.160.168时，小包通信正常，但是大包会出现问题。

过程分析

（1）故障时在waf侧进行抓包，发现两台waf都能从S6520X收到同一条流的流量。



（2）进一步确认设备上相关流量转发情况，发现对应流量在交换机上只进行二层转发。并且，该流量在S6520X上的上、下行口都进行了跨slot的聚合。

下行口：

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Static

Loadsharing Type: Shar

Management VLANs: None

Port	Status	Priority	Oper-Key
XGE1/0/3(R)	S	32768	1
XGE2/0/3	S	32768	1

（3）根据抓包信息看到具体流量的五元组等hash因子均相同，如果流量都从同一个slot进来，不太可能又跨slot转发出去，此时怀疑现场服务器两个口都会发送流量，服务器将报文分片后轮流从两个口发往交换机的不同slot。而交换机侧默认聚合口都是本地优转的，即流量从哪一个slot进来，只有该slot有对应出接口，就会从本slot的出接口发出。

（4）根据该理论，由于服务器侧无法进行相关信息查看，在交换机侧关闭本地优转测试，故障消除。

undo link-aggregation load-sharing mode local-first

由此可以确认，服务器侧两个口都会发包，导致交换机正常本地优转发给远端时，分片报文被中间的waf设备检查不通过导致丢包。

解决方法

（1）在交换机侧关闭本地优转：

undo link-aggregation load-sharing mode local-first

（2）调整服务器发包模式，只从一个口发出；

（3）调整waf的策略，交换机正常聚合口转发不需要考虑流量路径。