

知 某局点 SecPath F5030-D(V7)IRF透明模式部署后，部分流量不通

二层转发 接口组联动 备份组 王燕 2021-08-29 发表

组网及说明

F5030-D堆叠，透明部署双主，上下行思科设备。

问题描述

跳过防火墙，流量没有问题。上下行二层聚合，双主模式对接思科。安全域放通的。

过程分析

1、收集会话，没有回包，也没有产生在另一个框。

Slot 2 in chassis 2:

Initiator:

Source IP/port: 192.168.31.89/53757
Destination IP/port: 192.168.201.101/389
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/201/-
Protocol: TCP(6)
Inbound interface: Bridge-Aggregation10
Source security zone: Untrust

Responder:

Source IP/port: 192.168.201.101/389
Destination IP/port: 192.168.31.89/53757
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/201/-
Protocol: TCP(6)
Inbound interface: Bridge-Aggregation20
Source security zone: Trust

State: TCP_SYN_SENT

Application: LDAP

Rule ID: 0

Rule name: any

Start time: 2021-08-15 12:26:34 TTL: 25s

Initiator->Responder: 4 packets 280 bytes

Responder->Initiator: 0 packets 0 bytes

2、收集debug信息

发包vlan 201

*Aug 15 12:24:30:564 2021 H3C_F5030D FILTER/7/PACKET: -Chassis=2-Slot=2; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Trust; If-In=Bridge-Aggregation10(330), If-Out=Bridge-Aggregation20(331), **VLAN-In=201**, VLAN-Out=201; Packet Info:Src-IP=192.168.31.89, Dst-IP=192.168.201.101, VPN-Instance=, Src-MacAddr=4055-3926-3941,Src-Port=53738, Dst-Port=389, Protocol=TCP(6), Application=ldap(80), SecurityPolicy=any, Rule-ID=0.

回包的vlan标签是vlan 240

*Aug 15 12:24:03:472 2021 H3C_F5030D ASPF/7/PACKET: -Chassis=1-Slot=2; The first packet was dropped by ASPF for invalid status. Src-ZOne=Trust, Dst-ZOne=Untrust; If-In=Bridge-Aggregation20(331), If-Out=Bridge-Aggregation10(330), **VLAN-In=240**, VLAN-Out=240; Packet Info: Src-IP=192.168.201.101, Dst-IP=192.168.31.89, VPN-Instance=none, Src-Port=389, Dst-Port=53736. Protocol=TCP(6). Flag=SYN/ACK. Seq=1033371807.

解决方法

现场过设备不通，原因是出去的时候和回来的vlan不一致，临时配置undo mac fast-forwarding check-vlan-id XX后解决。

另外**F5030-D设备双机需要会话备份时，必须要配置备份组**，以免网络出现异常，后续调整组网以及增加备份组之后，完全解决现场问题。

