F1000防火墙二三层混合转发不通经验案例

二层转发 透明模式 **孙兆强** 2020-10-28 发表

组网及说明

AC上vlan20为用户的网关，上图三个设备通过vlan10互联。FW为透明部署，两个端口均放通vlan 10

问题描述

从ac上直接ping下面sw的vlan10地址可以ping通，在AC上带vlan 20的源地址ping下面sw的vlan10不通。

过程分析

1、排查三个设备的表项，路由指定正常。ARP表项学习正常。

AC：ip route-static 0.0.0.0 0 10.130.64.254

FW：ip route-static 192.168.20.0 24 10.130.64.253

SW：ip route-static 0.0.0.0 0 10.130.64.254

2、排查fw安全域及安全策略的配置均已放通

```
security-zone name Trust
 import interface Vlan-interface10
 import interface GigabitEthernet1/0/5 vlan 10
 import interface GigabitEthernet1/0/6 vlan 10
rule 3 name trust_to_trust-3
  action pass
  source-zone Trust
  destination-zone Trust
```

3、查看fw的会话

```
Slot 1:
Initiator:
  Source      IP/port: 192.168.20.254/251
  Destination IP/port: 10.130.64.252/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/10/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/5
  Source security zone: Trust
Responder:
  Source      IP/port: 10.130.64.252/251
  Destination IP/port: 192.168.20.254/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/10/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/6
  Source security zone: Trust
State: ICMP_REQUEST
Application: ICMP
Start time: 2020-10-27 21:35:37  TTL: 48s
Initiator->Responder:            5 packets        510 bytes
Responder->Initiator:            0 packets          0 bytes
```

发现会话有去无回，在下行口1/0/6抓包发现有回复报文。

Source	Destination	Protocol	Length	Info
192.168.20.254	10.130.64.252	ICMP	98	Echo (ping) request id=0x2729, seq=0/0, ttl=255 (reply in 2)
10.130.64.252	192.168.20.254	ICMP	98	Echo (ping) reply id=0x2729, seq=0/0, ttl=255 (request in 1)
192.168.20.254	10.130.64.252	ICMP	98	Echo (ping) request id=0x2729, seq=1/256, ttl=255 (reply in 4)
10.130.64.252	192.168.20.254	ICMP	98	Echo (ping) reply id=0x2729, seq=1/256, ttl=255 (request in 3)
192.168.20.254	10.130.64.252	ICMP	98	Echo (ping) request id=0x2729, seq=2/512, ttl=255 (reply in 6)
10.130.64.252	192.168.20.254	ICMP	98	Echo (ping) reply id=0x2729, seq=2/512, ttl=255 (request in 5)

在防火墙上debug aspf packet

<FW>*Oct 27 09:13:39:925 2020 FW ASPF/7/PACKET: -COntext=1; The first packet was dropped by ASPF for invalid status. Src-ZOne=Trust, Dst-ZOne=Trust;If-In=Vlan-interface10(1286), If-Out=Vlan-i

nterface10(1286); Packet Info:Src-IP=10.130.64.252, Dst-IP=192.168.20.254, VPN-Instance=none,Src-Port=225, Dst-Port=0. Protocol=ICMP(1).
从以上信息分析，直接ping走的是直连，能通正常。 带源ping不通原因是，ping下去的时候目的地址是10.130.64.252 AC上有同网段地址10.130.64.253 走的二层转发。回来的时候目的是192.168.20.254 sw走的路由，流量扔到网关fw。fw再走路由转发。对于fw来说一次是二层转发一次是三层转发。Fw认为是不同的会话，回程的时候检测到首包是ping的回包，认为不合法，首包丢弃。

解决方法

1、 开启fw的会话宽松模式session state-machine mode loose
2、 FW和AC互联用另一个vlan，让流量来回均走三层