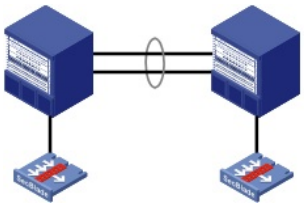
某局点S10508(V5)接口加入VPN实例后与防火墙板卡直连不通的处理经验案例

VPN实例 孙轶宁 2019-07-28 发表

组网及说明

两台S10508做IRF堆叠，slot 1均装了二代防火墙板卡。



问题描述

S10508的vlan接口与防火墙板卡接口处于同一网段，在105的vlan接口加入VPN实例之前，两个接口互ping能通，但是加入VPN实例之后，两个接口互ping不通。

过程分析

1、在两边设备debugging ip packet，发现在交换机侧只能发出icmp echo，无法收到防火墙板卡的发出的icmp echo和icmp echo-reply，而防火墙板卡能够收到交换机发出的icmp echo并且给响应的icmp echo-reply。

交换机debug

*Jun 13 09:08:29:610 2019 SW ADDR/7/debug_icmp: **ICMP Send: echo**(Type=8, Code=0), Dst = 10.0.0.61

*Jun 13 09:08:31:831 2019 SW ADDR/7/debug_icmp: **ICMP Send: echo**(Type=8, Code=0), Dst = 10.0.0.61

*Jun 13 09:08:34:058 2019 SW ADDR/7/debug_icmp: **ICMP Send: echo**(Type=8, Code=0), Dst = 10.0.0.61

防火墙板卡debug

*Jun 13 09:08:30:076 2019 FW ADDR/7/debug_icmp: ICMP **Send: echo**(Type=8, Code=0), Dst = 10.0.0.58

*Jun 13 09:08:31:737 2019 FW ADDR/7/debug_icmp: ICMP **Receive: echo**(Type=8, Code=0), Src = 10.0.0.58, Dst = 10.0.0.61

*Jun 13 09:08:31:737 2019 FW ADDR/7/debug_icmp: ICMP **Send: echo-reply**(Type=0, Code=0), Src = 10.0.0.61, Dst = 10.0.0.58

2、尝试在交换机侧做流统，发现交换机ping防火墙流统来回都是5，防火墙有回报文给交换机，但是防火墙ping交换机流统inbound方向为5，但是outbound方向为0，交换机没有回防火墙。**结合上面的debug判断交换机的内联口能够收到防火墙的报文，但是没有上送CPU处理。**

交换机ping防火墙流统结果

```
 Interface: Ten-GigabitEthernet1/1/0/1

 Direction: Inbound

 Policy: at
  Classifier: at
    Operator: AND
    Rule(s) : If-match acl 3333
    Behavior: at
     Accounting Enable:
       5 (Packets)

 Direction: Outbound

 Policy: at
  Classifier: at
    Operator: AND
    Rule(s) : If-match acl 3333
    Behavior: at
     Accounting Enable:
       5 (Packets)
```

防火墙ping交换机流统结果

Interface: Ten-GigabitEthernet1/1/0/1

Direction: Inbound

Policy: at
Classifier: at
Operator: AND
Rule(s) : If-match acl 3333
Behavior: at
Accounting Enable:
5 (Packets)

Direction: Outbound

Policy: at
Classifier: at
Operator: AND
Rule(s) : If-match acl 3333
Behavior: at
Accounting Enable:
0 (Packets)

3、经确认，客户开启了路由优化功能l3unicast-optimization enable。开启这个功能时，主控板不在承担硬件转发功能，这样可以提升主控板的处理能力和设备防攻击能力，在业务板的类型全都一致的情况下，开启路由优化功能可以提高整机的路由收敛性能。但是绑定vpn实例后，主控板相当于做一个代理功能，需要硬件表项来进行转发，所以需要关闭路由优化配置，才能正常转发。

在开启路由优化功能的时候，查看看底层l3表项，加入vpn实例后主控没有对应表项生成：

[SW-diagnose]bcm 4 0 l3/defip/show
Unit 0, Total Number of DEFIP entries: 12289
VRF Net addr Next Hop Mac INTF MODID PORT PRIO CLASS HIT VLAN

关闭路由优化功能并重启对应vlan虚接口后，主控板硬件学到了相关表项，问题解决。

[SW]undo l3unicast-optimization enable
l3uc optimization mode disabled!
[SW-diagnose]bcm 4 0 l3/defip/show
Unit 0, Total Number of DEFIP entries: 12289
VRF Net addr Next Hop Mac INTF MODID PORT PRIO CLASS HIT VLAN
0 8 10.0.0.58/32 00:00:00:00:00:00 100001 0 0 1 32 n
0 8 10.0.0.56/29 00:00:00:00:00:00 100001 0 0 1 32 n

解决方法

绑定VPN实例后，主控板相当于做一个代理功能，需要硬件表项来进行转发，所以需要关闭路由优化配置，才能正常转发。

关闭路由优化功能

[SW]undo l3unicast-optimization enable
l3uc optimization mode disabled!