某局点S7500E设备新增ipv6包过滤后ipv6业务中断

packet-filter 刘倩 2022-10-17 发表

组网及说明

组网不涉及

问题描述

河北移动某局点在原先的IPv4包过滤的基础上要新增IPv6包过滤，新增结束测试发现IPv6业务不通。

关键配置：

```
#
interface Ten-GigabitEthernet2/0/16
 port link-mode bridge
 port access vlan 110
 packet-filter 3002 inbound
 packet-filter ipv6 3002 inbound
#
acl number 3002（37条）
 rule 10 permit ip source 111.63.118.128 0.0.0.63 destination 111.63.117.0 0.0.0.63
 rule 20 permit ip source 111.63.118.128 0.0.0.63 destination 111.63.118.98 0.0.0.1
#
acl ipv6 number 3002 （20条）
 rule 140 permit ipv6 source 2409:8087:590:1021:1401::/80 destination 2409:8087:5C0:1021:140
1::/80
rule 150 permit ipv6 source 2409:8087:590:1021:1401::/80 destination
2409:8087:550:1021:1401::/80
rule 330 permit icmpv6 source 2409:8087:590:1021:1401::/80
rule 520 deny ipv6
#
```

过程分析

流统发现报文确实丢在交换机上：

（1）查看设备上配置无问题且ACL资源足够

Type	Total	Reserved	Configured	Remaining	Usage
IFP ACL	16384	5120	78	11186	31%

（2）查看acl下发情况——***[probe]debug qacl show acl-resc slot 2 chip 0***，底层占用的entry数量和ACL中rule的数量一致

但是在slice 5的资源未用完的情况下，ipv6包过滤下发到slice2/3，group 9中。包过滤可能会占用多个slice，但同一类ACL一般下到同一group中

```
------------------------------------------------------
  Pri  5, Group  9,usedEntries 19 ,mode Double, physlice 2/3/
  ======================================================
    acl type                                 usedEntries[19]
  ======================================================
    [141]PktFilter IPV6 on PORT                       19
  ======================================================
------------------------------------------------------
  Pri  7, Group  8,usedEntries 38 ,mode Single, physlice 5/
  ======================================================
    acl type                                 usedEntries[38]
  ======================================================
    [99 ]PktFilter IP on PORT                         37
    [141]PktFilter IPV6 on PORT                       1
  ======================================================
------------------------------------------------------
```

（3）查看下发到slice中的ACL详细信息***[probe]debug qacl show slot 2 chip 0 verbose 0acl-type 141***

具有更高优先级的group 8中的ipv6 packet-filter更先生效，而下发到group 8中的rule刚好是最后一条规则rule 520 deny ipv6

当流量过来时最先匹配rule 520将所有的ipv6报文都丢弃

```
========
Acl-Type PktFilter IPV6 on PORT, Stage IFP, Pipe 0, SinglePort, Installed, Active
Prio Mjr/Sub 523/1040121335, Group 8 [8], Slice/Idx 5/37, Entry 1968, Single: 9253
 ACL GroupNo : 3002, RuleID : 520
Rule Match --------
        Ports: 0x00000000000000000000000002; 0x20000000000001fffffffffff
        Lookup: STP forwarding, 0x18, 0x18
        IP Type: IPv6 packet
Actions --------
        Deny
```

解决方法

决定acl group会不会分裂要看qset中选择的模式所匹配的源目IP地址是否超规格

Qset中只有如下几种模式，总结来说同一个group中有以下4种配置组合超过两个会group分裂（括号内的，可以合起来算一个）（SrcIp4、DstIp4）、SrcIp6、DstIp6、(SrcIp6HIGH、SrcIp6HIGH(掩码<=64位时会下发))

将IPv4和ipv6过滤分别选择以MQC和packet-filter的方式下发。