某局点 S 5560X-EI 包过滤不生效问题

ACL 柯辉 2022-06-27 发表

组网及说明

暂无

告警信息

暂无

告警信息

问题描述

现场在int valn 口下下发包过滤，测试发现未生效

interface Vlan-interface1400

description JRJG

ip address 40.108.1.252 255.255.255.0

vrrp vrid 140 virtual-ip 40.108.1.254 vrrp vrid 140 priority 120 vrrp vrid 140 track 1 priority reduced 40

packet-filter name JRJG inbound

过程分析

排查发现底层包过滤都有正常下发：

```
acl advanced name JRJG
rule 0 permit icmp counting
rule 5 permit ip destination 224.0.0.0 0.0.0.255 counting
rule 10 permit ip destination 21.244.0.0 0.0.255.255 counting
rule 15 permit ip destination 21.4.0.0 0.3.255.255 counting
rule 20 permit ip destination 26.0.0.0 0.255.255.255 counting
rule 25 permit ip destination 25.0.0.0 0.255.255.255 counting
rule 30 permit ip destination 10.2.0.0 0.0.255.255 counting
rule 35 permit ip destination 10.8.0.0 0.0.255.255 counting
rule 40 permit ip destination 10.3.0.0 0.0.255.255 counting
rule 45 permit ip destination 10.9.0.0 0.0.255.255 counting
rule 50 permit ip destination 21.108.127.0 0.0.0.255 counting
rule 5000 deny ip counting

Acl-Type PktFilter IP on VRF, Stage IPCL 0, OuterPort, Installed, Active
Prio Mjr/Sub 0x202/0x11, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/930,
 ACL GroupNo : 637534213, RuleID : 0   这里的acl ruleID依次和上面的对应，也都对的上
Rule Match --------
        Global range
        Outer Vlan: 0x578, 0xfff
        IP protocol: icmp
       IP Type: Any IPv4 packet
        Account or Logging
        Mac to me: 1
Actions --------
        Account mode  packets,  green and non-green
        Permit
Accounting: Hi 0, Lo 0
========
Acl-Type PktFilter IP on VRF, Stage IPCL 0, OuterPort, Installed, Active
Prio Mjr/Sub 0x202/0x11, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/931,
 ACL GroupNo : 637534213, RuleID : 5
Rule Match --------
        Global range
        Outer Vlan: 0x578, 0xfff
        Dest IP: 224.0.0.0, 255.255.255.0
        IP Type: Any IPv4 packet
        Account or Logging
        Mac to me: 1
Actions --------
        Account mode  packets,  green and non-green
        Permit
Accounting: Hi 0, Lo 0
========
Acl-Type PktFilter IP on VRF, Stage IPCL 0, OuterPort, Installed, Active
Prio Mjr/Sub 0x202/0x11, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/932,
 ACL GroupNo : 637534213, RuleID : 10
Rule Match --------
        Global range
        Outer Vlan: 0x578, 0xfff
        Dest IP: 21.244.0.0, 255.255.0.0
        IP Type: Any IPv4 packet
        Account or Logging
        Mac to me: 1
Actions --------
        Account mode  packets,  green and non-green
        Permit
Accounting: Hi 0, Lo 0
========
```

解决方法

继续排查流量进来的物理口，发现物理口也有下发包过滤：

interface GigabitEthernet1/0/28

调整物理接口下的包过滤后，测试正常生效

port link-mode bridge

description to_HF-CB-17F-S1_XGE1/0/49

port link-type trunk

undo port trunk permit vlan 1

port trunk permit vlan 2 to 4094

packet-filter name deny-CO_To_CB inbound // 物理端口也有下发，而且对应的acl，最后一条配置为permit ip 放通所有，而 物理口下的包过滤优先级高于int vlan 口，所以int vlan 口下的包过滤无法生效

mirroring-group 1 mirroring-port both

acl advanced name deny-CO_To_CB

description deny-CO_To_CB

rule 5 deny ip source 22.0.0.0 0.255.255.255 destination 21.0.0.0 0.255.255.255

rule 10 deny ip source 28.0.0.0 0.255.255.255 destination 21.0.0.0 0.255.255.255

rule 15 deny ip source 29.0.0.0 0.255.255.255 destination 21.0.0.0 0.255.255.255

rule 20 deny ip source 24.0.0.0 0.255.255.255 destination 21.0.0.0 0.255.255.255

rule 45 deny ip source 21.0.0.0 0.255.255.255 destination 22.0.0.0 0.255.255.255

rule 50 deny ip source 21.0.0.0 0.255.255.255 destination 28.0.0.0 0.255.255.255

rule 55 deny ip source 21.0.0.0 0.255.255.255 destination 29.0.0.0 0.255.255.255

rule 60 deny ip source 21.0.0.0 0.255.255.255 destination 24.0.0.0 0.255.255.255

rule 70 permit ip source 28.0.0.0 0.255.255.255 destination 22.5.0.0 0.0.255.255

rule 71 permit ip source 22.5.0.0 0.0.255.255 destination 28.0.0.0 0.255.255.255

rule 72 permit ip source 28.0.0.0 0.255.255.255 destination 22.4.1.161 0

rule 73 permit ip source 28.0.0.0 0.255.255.255 destination 25.64.0.33 0

rule 74 permit ip source 22.4.1.161 0 destination 28.0.0.0 0.255.255.255

rule 75 permit ip source 25.64.0.33 0 destination 28.0.0.0 0.255.255.255

rule 76 permit ip source 28.0.0.0 0.255.255.255 destination 22.108.1.3 0

rule 77 permit ip source 22.108.1.3 0 destination 28.0.0.0 0.255.255.255

rule 78 permit ip source 28.0.0.0 0.255.255.255 destination 22.108.1.4 0

rule 79 permit ip source 22.108.1.4 0 destination 28.0.0.0 0.255.255.255

rule 80 permit ip source 28.0.0.0 0.255.255.255 destination 22.4.52.20 0

rule 81 permit ip source 22.4.52.20 0 destination 28.0.0.0 0.255.255.255

rule 85 permit ip source 28.0.0.0 0.252.255.255 destination 22.4.102.42 0

rule 86 permit ip source 22.108.130.35 0 destination 28.4.0.7 0

rule 87 permit ip source 28.4.0.7 0 destination 22.108.130.35 0

rule 150 deny ip source 22.0.0.0 0.255.255.255 destination 28.0.0.0 0.255.255.255

rule 151 deny ip source 28.0.0.0 0.255.255.255 destination 22.0.0.0 0.255.255.255

rule 200 permit ip