某局点S12500G adcampus 增加pbr 到FW后不通问题

策略路由 张文宁 2023-06-29 发表

组网及说明

/

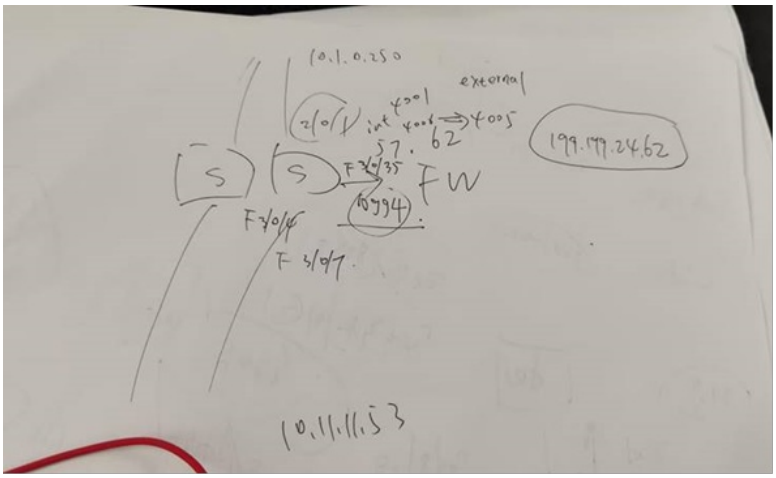
告警信息

/

问题描述

设备: S12500G

问题:设备作为spine-border角色,如下, 增加pbr 到FW后不通问题,报文到了125G,但是没有往下转发



	Time	Source	Destination	Protocol	Leng
1	2023-06-17 08:07:09.000000	10.1.0.250	10.11.11.53	ICMP	78
2	2023-06-17 08:07:09.000001	10.1.0.250	10.11.11.53	DNS	85
3	2023-06-17 08:07:09.000002	10.1.0.250	10.11.11.53	DNS	85

```
e 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
rnet II, Src: f4:e9:75:92:da:41 (f4:e9:75:92:da:41), Dst: e8:78:ee:10:4e:01 (e8:78:ee:10:4e:0
1Q Virtual LAN, PRI: 0, CFI: 0, ID: 4005
rnet Protocol Version 4, Src: 10.1.0.250, Dst: 10.11.11.53
rnet Control Message Protocol
```

过程分析

远程，发现我们设备上下发了全局安全组的PBR， 删除PBR后业务恢复。因此本问题是安全组引起的，非设备问题。

```
[PJN_074F_Spine01_10.2.16.1]dis ip poli
[PJN_074F_Spine01_10.2.16.1]dis ip policy-based-route
Policy name: 1
  node 0 permit:
    if-match acl 3500
    apply next-hop vpn-instance external 199.199.24.62

Policy name: SDN_GLB_SC3
  node 65535 permit:
    if-match acl name SDN_ACL_SC_PERMIT_ALL

Policy name: SDN_GLOBAL_SC
  node 0 permit:
    if-match acl name SDN_ACL_GLOBAL_SC_581e4b8f-c043-4726-bfdf-eaee22d4f051
    apply output-interface NULL0
[PJN_074F_Spine01_10.2.16.1]
[PJN_074F_Spine01_10.2.16.1]
[PJN_074F_Spine01_10.2.16.1]
[PJN_074F_Spine01_10.2.16.1]dis cu | inc global
lldp global enable
classification global
stp global enable
evpn global-mac 0001-0001-0001
qos apply policy zwn global outbound
ip global policy-based-route SDN_GLOBAL_SC
[PJN_074F_Spine01_10.2.16.1]dis acl na
[PJN_074F_Spine01_10.2.16.1]
[PJN_074F_Spine01_10.2.16.1]dis acl na
[PJN_074F_Spine01_10.2.16.1]dis acl name SDN_ACL
[PJN_074F_Spine01_10.2.16.1]dis acl name SDN_ACL_GLOBAL_SC_581e4b8f-c043-4726-bfdf-ea
ee22d4f051
Advanced IPv4 ACL named SDN_ACL_GLOBAL_SC_581e4b8f-c043-4726-bfdf-eaee22d4f051, 10 r
ules,
SDN_ACL_GLOBAL_SC_581e4b8f-c043-4726-bfdf-eaee22d4f051
ACL's step is 5, start ID is 0
rule 0 permit ip vpn-instance sdfyy_nw_campus destination 10.11.11.0 0.0.0.255
rule 1 permit ip vpn-instance sdfyy_nw_campus destination 10.0.146.0 0.0.1.255
rule 2 permit ip vpn-instance sdfyy_nw_campus destination 10.0.156.0 0.0.0.255
```

解决方法

设备上备控制器下发了全局安全组的PBR，命中了流量报文指向黑洞下一跳导致不通，删除该错误的全局PBR配置后业务恢复。