某局点10508设备配置pbr后telnet设备本身地址不成功的经验案例

ACL 姜霁琛 2020-11-27 发表

组网及说明

无

问题描述

现场10508设备配置了pbr策略路由，但配置后发现无法telnet到设备进行管理了，如果配置一条deny的节点，目的地址匹配设备本身地址，则可以正常telnet，看现象是pbr也会对设备本身地址生效，现场又测试了ping设备本身地址，发现ping报文不受pbr的限制，接到问题我们迅速开始分析.

过程分析

查看配置没有什么问题

#

interface Vlan-interface190

ip address 192.168.x.x 255.255.255.0

ip policy-based-route aaa

#

policy-based-route aaa deny node 5 //设备本身地址不走pbr

if-match acl 3333

#

policy-based-route aaa permit node 10

if-match acl 3555

apply next-hop 10.1.x.x

#

acl advanced 3333

rule 1 permit ip source 192.168.x.x 0.0.0.255 destination 192.168.x.x 0 //设备本身地址

但客户想要确认pbr会对telnet设备本身地址生效的原因，另外现场反馈用68设备测试却未复现该问题，怀疑是设备实现问题。

查看105设备底层acl下发情况，发现105的icmp下发acl中存在取消三层转发的动作

[SW-probe]debug qacl show chassis 1 slot 0 c 0 verbose 0 sysidx 44

========

Acl-Type RX IPv4 Middle, Stage IFP, Pipe 0, Global, Installed, Active

Prio Mjr/Sub 524/18, Group 1 [1], Slice/Idx 8/39, Entry 38, Double: 6183/6695

Rule Match --------

Ports: 0x000000000000001fffe; 0x60000000000007fffff

Lookup: VLAN ID valid[y], STP forwarding, 0x1c, 0x1c

IP protocol: icmp

IP Type: Any IPv4 packet

Dest Port: CPU

DropBit: 0x0, Mask : 0x1

SysmRule Index : 44

L3 Dest Class id: 0x20

My Station Hit

Actions --------

CAR cir 0x200, cbs 0x800, pir 0x200, pbs 0x800, mode srTCM color blind,Bytes

Account mode packets, green and non-green

L3Switch Cancel L3Switch NextHopIndex 0x4001

Change CPU pkt COS 22

Red Deny

Red_Copy_to_cpu : No

Yel Deny

Yel_Copy_to_cpu : No

68设备的telnet也有该动作，但105设备的telnet下发的acl中却没有该动作

[SW-probe]debug qacl show chassis 1 slot 0 c 0 verbose 0 sysidx 65

========

Acl-Type RX IPv4 Middle, Stage IFP, Pipe 0, Global, Installed, Active

Prio Mjr/Sub 524/18, Group 1 [1], Slice/Idx 8/42, Entry 46, Double: 6186/6698

Rule Match --------

Ports: 0x000000000000001fffe; 0x60000000000007fffff

Lookup: VLAN ID valid[y], STP forwarding, 0x1c, 0x1c

IP protocol: tcp

IP Type: Any IPv4 packet
L4 Dst Port: 23, 0xffff
Dest Port: CPU
DropBit: 0x0, Mask : 0x1
L3 Dest Class id: 0x20

Actions --------
CAR cir 0x200, cbs 0x800, pir 0x200, pbs 0x800, mode srTCM color blind,Bytes
Account mode packets, green and non-green
Change CPU pkt COS 27
Red Deny
Red_Copy_to_cpu : No
Yel Deny
Yel_Copy_to_cpu : No

MatchedName:65, TELNET/SSH
Accounting: Hi 0, LO 0
至此，问题已经很明显了。

解决方法

目前105设备的实现机制为，telnet到设备本身的报文会受pbr的影响，而icmp报文由于会在acl中下发一条取消三层转发的动作 **L3Switch Cancel L3Switch NextHop**，因此不受pbr的影响。该功能不同设备实现机制稍有不同，具体设备需具体分析不可一概而论。当前若需要规避可在pbr中配置deny节点，让访问到设备的流量不要匹配pbr。