ip source bind不生效

IP Source Guar　啃一口玛卡巴卡　2024-05-28 发表

问题描述

现场测试ip source bind功能，发现配置后icmp报文没有被拦截

过程分析

配置：

interface GigabitEthernet1/0/16

port link-mode bridge

port access vlan 100

arp max-learning-num 0

mirroring-group 1 mirroring-port both

ip verify source ip-address mac-address

#

ip source binding ip-address 10.10.10.22 mac-address 8a62-c528-5f46

后尝试在vlan口下进行调用，依然不生效

vlan 100

description GuanLi

ip verify source ip-address mac-address

#

interface Vlan-interface100

ip address 10.10.10.1 255.255.255.0

ip verify source ip-address mac-address

表项是正常的：

```
[rmyy-7003X]dis ip  source binding static
Total entries found: 1
IP address      MAC address     Interface               VLAN Type
10.10.10.22     8a62-c528-5f46 N/A                      N/A  Static
[rmyy-7003X]
```

查看acl下发情况：

[H3C-probe]debug hardware internal qacl show acl-resc slot 1 c 2

[H3C-probe]debug hardware internal qacl show 1 chip 0 verbose 0 acl-type 36

```
==========================================
Acl-Type[36] Ipsg Global, block IACL 2, Global, Installed, Active
Prio 0x49000000, Group 2, Expand to 1 Sdk Entry(ies):
Sdk Entries --------
        Key Type: MacV4 640 Key
        Entry Id: 0, Global
Rule Match --------
        Source mac: 8A62-C528-5F46, FFFF-FFFF-FFFF
        IP Type: Ipv4 packet
        Source IP: 10.10.10.22, 255.255.255.255
Actions --------
        Permit
[rmyy-7003X-probe]display hardware internal qacl show slot 1 chip 0 verbose 0 ac
l-type 34
```

是下发成功的。

测试方法以及结果：

```
以太网适配器 以太网 4:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::ce89:6c49:82:853b%2
   IPv4 地址 . . . . . . . . . . . . : 10.10.10.33
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.10.10.1

无线局域网适配器 本地连接* 1:
```

```
C:\Users\hulei>ping 10.10.10.1

正在 Ping 10.10.10.1 具有 32 字节的数据:
来自 10.10.10.1 的回复: 字节=32 时间=1ms TTL=255
来自 10.10.10.1 的回复: 字节=32 时间=1ms TTL=255
来自 10.10.10.1 的回复: 字节=32 时间=1ms TTL=255
来自 10.10.10.1 的回复: 字节=32 时间=1ms TTL=255

10.10.10.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

解决方法

入方向ACL位于L2、L3流程之后，如果报文经过L2、L3处理被丢弃或通过寄存器上送CPU，则无法命

中ACL。
Ping报文是通过寄存器上送CPU，无法被IPSG的deny规则无法丢弃该报文，所以能ping通。过路报文是可以正常被IPSG的deny规则过滤的。

```
=======================================================
 GroupType: SEC
 -------------------------------------------------------
   acl type                  usedEntries
   [ 36]Ipsg Global                1
   [191]Ipsg Default Vlan Intf     1
   [187]Ipsg Default Vlan          1
```

测试过路报文拦截无问题