某局点S7600系列交换机包过滤禁用UDP 161端口不生效问题处理经验案例

ACL 策略路由 SNMP packet-filter 孙轶宁 2023-06-30 发表

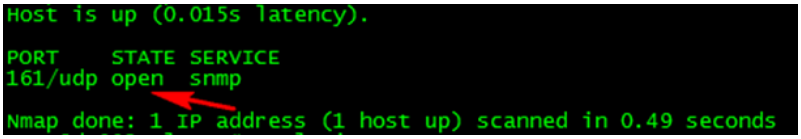
问题描述

客户在设备的公网出接口调用包过滤，ACL规则如下，想实现只允许特定地址访问设备的UDP161端口（即SNMP服务）

rule 5 permit udp source X.X.X.X 0 destination-port eq snmp

rule 100 deny udp destination-port eq snmp

但是发现其他地址仍然可以扫到这个端口处于开放状态



过程分析

1、检查ACL内容以及流量上来的接口，发现没有问题

2、查看ACL下发情况，确认这两条ACL是正常下发到硬件表项的。

========

Acl-Type PktFilter IP on PORT, Stage IFP, Pipe 0, SinglePort, Installed, Active

Prio Mjr/Sub 525/1308557306, Group 10 [10], Slice/Idx 9/2, Entry 258, Single: 13314

ACL GroupNo : 3698, RuleID : 5

Rule Match --------

Ports: 0x00000000000000000000000400; 0x200000000001ffffffffffffff

Lookup: STP forwarding, 0x18, 0x18

Source IP: X.X.X.X, 255.255.255.255

IP protocol: udp

IP Type: Any IPv4 packet

L4 Dst Port: 161, 0xffff

Actions --------

Permit

========

Acl-Type PktFilter IP on PORT, Stage IFP, Pipe 0, SinglePort, Installed, Active

Prio Mjr/Sub 525/1308557211, Group 10 [10], Slice/Idx 9/3, Entry 259, Single: 13315

ACL GroupNo : 3698, RuleID : 100

Rule Match --------

Ports: 0x00000000000000000000000400; 0x200000000001ffffffffffffff

Lookup: STP forwarding, 0x18, 0x18

IP protocol: udp

IP Type: Any IPv4 packet

L4 Dst Port: 161, 0xffff

Actions --------

Deny

3、经确认，这个为设备目前版本协议报文上送CPU的实现机制导致，只能通过配置本地PBR规避。

解决方法

通过配置本地PBR规避，方法如下：

```
acl advance 3000
 rule 5 permit udp source X.X.X.X 0 destination-port eq snmp
#
acl advance 3001
 rule 5 permit udp destination-port eq snmp
#
policy-based-route abc deny node 10
 if-match acl 3000
#
policy-based-route abc permit node 10
 if-match acl 3001
 apply output-interface NULL0
#
ip local policy-based-route abc
```