SR66 限制对ipv6 NETCONF over SSH客户端的访问控制

NETCONF ACL QoS SSH PengfeiShao 2023-08-17 发表

问题描述

用ssh server ipv6 acl命令这条命令在SR66上设置对ipv6 NETCONF over SSH客户端的访问控制不生效，在SR88上可以

过程分析

ssh server ipv6 acl命令用来设置对IPv6 SSH客户端的访问控制，但是目前这个命令在SR66上不能设置对NETCONF over SSH客户端的访问控制。而SR88没有这个限制。

【使用指导】

对IPv6 SSH客户端的访问控制通过引用ACL来实现，具体情况如下：

- 当引用的ACL不存在、或者引用的ACL为空时，不允许IPv6 SSH客户端访问设备。
- 当引用的ACL非空时，则只有匹配ACL中permit规则的IPv6 SSH客户端可以访问设备，其他客户端不可以访问设备。
- 在引用的ACL中，若某规则指定了**vpn-instance**参数，则表示该规则仅对VPN报文有效；若规则未指定**vpn-instance**参数，则表示该规则仅对公网报文有效。

该配置生效后，只会过滤新建立的SSH连接，不会影响已建立的SSH连接。

对于IPv6 SSH客户端，本命令不能设置对NETCONF over SSH客户端的访问控制。

多次执行本命令，最后一次执行的命令生效。

解决方法

中低端系列路由器会在后续版本放开这个限制，目前可先通过接口包过滤实现，过滤掉控制器的ipv6地址。

```
#
interface M-GigabitEthernet0/0/0
 ip address 172.16.99.60 255.255.0.0
 packet-filter ipv6 3000 inbound
 ipv6 address 172:16:21::99:60/64
#
return
[99.60-M-GigabitEthernet0/0/0]qu
[99.60]dis acl ipv
[99.60]dis acl ipv6 a
[99.60]dis acl ipv6 all
Advanced IPv6 ACL 3000, 1 rule,
ACL's step is 5
 rule 0 deny ipv6 source 172:16:21::100/128 (380 times matched)
```