

知 V7防火墙IPV6 ACL目的端口调用对象组配置失败

ACL 薛佳宇 2023-03-23 发表

组网及说明

不涉及

告警信息

Illegal destination port object group type.

问题描述

现场需要使用ipv6 acl的rule规则中调用对象组实现匹配tcp的目的端口，但是配置过程有报错导致配置失败

```
[H3C-acl-ipv6-adv-3000]rule permit tcp destination object-group v6add destination-port object-group v6
Illegal destination port object group type.
[H3C-acl-ipv6-adv-3000]dis this
#
acl ipv6 advanced 3000
#
```

过程分析

1、检查相关对象组配置，发现目的端口处调用的对象组类型是service

```
#  
object-group ipv6 address v6add  
0 network host address 1::1  
10 network host address 1::2  
20 network host address 1::3  
30 network host address 1::4  
  
#  
object-group service v6  
0 service tcp destination eq 443  
#
```

2、实际上我们需要调用的对象组只是用来匹配端口号，设备上还有另一种对象组类型为port，于是创建如下对象组：

```
# object-group port v6port  
0 port eq 443  
10 port eq 444  
#
```

3、重新配置成功：

```
[H3C-acl-ipv6-adv-3000]rule permit tcp destination object-group v6add destination-port object-group v  
6port  
[H3C-acl-ipv6-adv-3000]dis this  
# acl ipv6 advanced 3000  
rule 0 permit tcp destination object-group v6add destination-port object-group v6port  
#
```

解决方法

ACL中匹配目的端口调用的对象组类型应该使用“port”类，而不是“service”类。

