

组网及说明

无

问题描述

S5560X-EI在配置acl调用包过滤，设备提示

Failed to apply or refresh IPv4 ACL vlan150_in rule 170 to the inbound direction of interface Vlan-interface150. The ACL is not supported.

在进方向和出方向调用都会报错

过程分析

首先查看acl的配置内容，发现与平常的acl相比有这么一条规则

```
rule 170 permit tcp source 39.0.5.0 0.255.0.255 destination 39.0.8.31 0 destination-port range ftp-data ftp
```

怀疑跟range参数有关，确认现场版本为1118P07，查看软件版本说明有如下的解决列表

4. 201711170576

- 问题现象：引用ACL的策略不生效。
- 问题产生条件：
 - a. ACL中包含匹配报文端口范围（lt,gt,neq或range）的规则；
 - b. 配置引用此ACL的策略，并在端口的出方向应用此策略。

5. 201711180083

- 问题现象：ACL策略中匹配报文端口范围的规则错误的应用为全局。
- 问题产生条件：
 - a. ACL中包含匹配报文端口范围（lt,gt,neq或range）的规则；
 - b. 将引用此ACL的策略应用在端口上；
 - c. 此时在ACL中新增不支持的规则，导致原策略错误的应用为全局。

经实验室验证，1118P01和最新版本1119P05都可以配置

但是在1118P09上配置会一样有报错

Failed to apply IPv4 ACL 3123 to the outbound direction of interface Vlan-interface24 on slot 1.

[leaf1-Vlan-interface24]%Mar 18 02:52:58:982 2013 leaf1 PFILTER/3/PFILTER_IF_NOT_SUPPORT:

Failed to apply or refresh IPv4 ACL 3123 rule 241 to the outbound direction of interface Vlan-interface24. The ACL is not supported.

解决方法

确认之后

Port range功能是在R1119P04版本才合入支持的，在这之前的版本不支持Port range。

R1118分支的版本都不支持port range。

对于R1118P01版本，Port range可以下发，但是不会生效。为了防止客户配置port range，我们在R118P07版本中修改返回不支持。

Port range存在如下限制：

- 1、ipv4的neq不支持
- 2、ipv6的neq、lt、gt、range都不支持
- 3、如果一条rule带有range，会占用一条acl硬件资源，同时占用两个range寄存器资源（range占两个，gt、lt占一个）
- 4、Range资源是UDP 4个 TCP4个(range情况下，lt、gt是8个) 共8个且TCP与UDP资源不可共用
- 5、同一条rule/ACL下发到多个端口，acl资源成倍占用，range资源可共用，如果port range资源仅剩一条，下发需占两条range资源的rule，那么这条rule不会下发。也就是说配置range的情况下 tcp /udp 出入方向能各下4条rule；如果配置lt/gt的情况下，tcp/udp出入方向能各下8条rule。

推荐升级到1119P04及以上的版本