# 某局点 CR16010H-F 配置PPPOE用户屏蔽部分目的端口号配置不生效

QoS 林宇阳 2022-12-19 发表

## 组网及说明

设备作为在网BRAS接入，承载家宽、IPTV等业务

## 问题描述

设备替换友商BRAS上线后，用户接入业务正常，但客户要求在设备添加防攻击策略，即在设备入方向配置QOS Policy来阻断部分高危的TCP/UDP协议目的端口号。
现场配置后测试访问对应端口号发现阻断不生效。

## 过程分析

首先明确当前设备QOS机制为:

出入方向QOS策略相互独立，互不影响；

优先匹配全局策略，然后匹配接口策略；

同一条策略只会被一条RULE匹配，匹配到对应特征后，不会在继续向下匹配后续的rule和策略。

如果匹配的rule的动作为deny，此时流量直接跳出策略匹配，不执行动作。

基于以上机制进行以下检查：

1、检查QOS调用是否与已有业务配置有冲突：现场端口阻断QOS与已有业务QOS配置无冲突，不涉及全局、接口优先顺序问题；

2、检查业务流量是否可以被规则匹配：策略中rule不涉及具体地址仅有端口号特征，且直接接口调用，通过流量都尝试进行匹配。

3、检查RULE配置：阻断策略调用的ACL中阻断rule动作为deny，即会导致流量命中后跳出匹配不处理。

## 解决方法

问题确认为ACL中rule配置不符合设备实现机制，导致端口阻断不生效。
我司QOS端口阻断需要在策略classifier的ACL中permit动作标记流量，然后再对应的behavior中filter deny流量，而不是直接在ACL中deny。
现场修改后测试阻断端口号正常。

注意：目前现网较多替换友商的局点，实施时配置多为直接一比一翻译友商配置。大部分情况下这样操作没有问题，但遇到一些非路由协议之类通用模块，且涉及我司实现机制的场景，还是需要多注意从我司实现角度核对配置脚本，避免引起不必要的故障