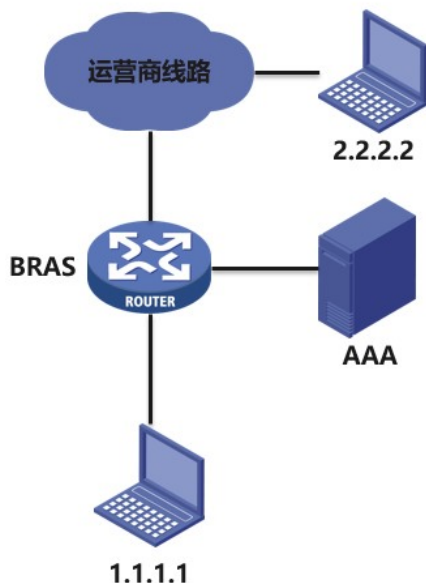


组网及说明



CR16010F做ipoe web接入。要求特定认证用户1.1.1.1上线后，AAA下发特定user-group abc。BRAS配置全局qos策略匹配用户地址 + user-group abc，控制1.1.1.1流量不能通过BRAS。

问题描述

出现问题时，现网发现公网地址2.2.2.2能够ping通1.1.1.1，怀疑BRAS的全局qos策略不生效。

过程分析

在2.2.2.2上面tracert 1.1.1.1，确认中间经过BRAS，且1.1.1.1未连接其他三层出口，确定是BRAS放通了2.2.2.2到1.1.1.1的流量。

检查BRAS上面1.1.1.1的用户状态。dis ip subscriber session ip 1.1.1.1 verbose，其携带的user-group是正确的abc，非AAA授权异常。

检查BRAS全局qos策略配置和匹配情况。2.2.2.2 ping 1.1.1.1的流量来回方向需要检查4次全局qos。ping echo request到BRAS，检查全局qos入方向策略；echo request从BRAS发到1.1.1.1，检查全局qos出方向策略；echo reply从1.1.1.1发到BRAS，检查全局入方向qos；echo reply从BRAS发给2.2.2.2，检查全局qos出方向。在此检查过程中，有几个需要注意的点：

1. BRAS的上行口没有开启ipoe认证，ping echo request到达该接口入方向时，不会匹配到带有user-group的acl，即不执行全局qos入向策略；ping echo request从BRAS下行口发出，能匹配user-group。
2. BRAS当前版本（R7951）对BRAS发给认证用户的ping echo request，以及用户发给BRAS的ping echo reply，默认存在优先级高于qos策略的free rule，即无法通过修改全局qos策略禁止此类报文。

此处不赘述现网具体qos配置。根据现网配置，以及BRAS对内网用户发出的ping echo reply默认放行，2.2.2.2确实应该能ping通1.1.1.1。需要用优先级高于默认free rule的packet filter过滤特定报文解决。

解决方法

全局配置packet filter，将用户1.1.1.1回给2.2.2.2的ping echo reply禁止，解决该问题。