BRAS做了前域阻断后, 已认证的后域用户仍能ping通未认证成功的前域用户

QoS 罗梦恺 2023-06-05 发表

问题描述

BRAS设备做了前域全阻断的全局qos。但是已认证用户可以ping通认证前用户，但是无法与认证前用户已开放的tcp端口进行通信。理论上前域用户设备策略上做了全阻断，已上线的前域用户即不能ping通后域用户，也不能和其建立tcp连接。

过程分析

理论上前域用户设备策略上做了全阻断，已上线的前域用户即不能ping通后域用户，也不能和其建立tcp连接。但是现场ping包能通，怀疑时设备有高于qos机制的放通策略放通了icmp报文。
在两个用户接入口下发qos流通，后域用户ping测试前域用户，发现后域用户接口下统计到了入方向的icmp包，前域用户的接口未统计到出去的icmp包和回程的icmp包，后域用户的接口统计到了回程的icmp包且发出。这表明报文确实通过BRAS设备转发了，但是前域用户接口侧有比qos优先级更高的策略放通了icmp包。

确认，设备的bras接入口的出方向底层放通了icmp的request报文，入方向放通了icmp的reply报文。优先级高于qos，导致匹配不到，所以qos策略阻断不掉icmp包，ping包能通。放通icmp包的初衷为：设备会有icmp包探测用户的需求，所以需要设备默认放通icmp request，已经放通用户回复的icmp reply。

解决方法

1、如果想要icmp不通的话，建议在后域用户的入接口匹配访问前域用户的icmp流量进行阻断。

2、或者在接口调用包过滤来进行阻断，因为底层默认的放通规则的优先级高于全局qos，但是低于包过滤。