防火墙全局nat情况下配置策略路由不生效

NAT 策略路由 **杨玉琦** 2022-03-21 发表

问题描述

防火墙作为出口设备，有两个出口链路。缺省情况下有两条默认路由分别指向各出口，其中指向移动出口的路由优先级更高。

此时在设备连接内网核心侧接口调用策略路由，想要实现部分终端走联通出口

配置完后发现不生效，检查策略路由配置正确，但转换时发现转换地址为移动出口地址。

解决方法

经确认：

全局NAT是通过路由从FIB表项获取源目安全域，而PBR在全局NAT模块后启用，因此无路由的情况下，全局NAT无法获取出接口所在安全域，无法匹配。

在全局nat策略中取消目的安全域的过滤条件，同时增加源IP地址的限制后，业务正常。