防火墙堆叠双出口配置NAT DNS mapping不生效

NAT 会话同步 保存上一跳 **刘洋** 2021-04-07 发表

问题描述

两台防火墙堆叠作为出口设备，需要实现内部用户通过域名域名访问内部服务器解析出地址为内部地址，配置NAT DNS mapping不生效，检查配置无问题，DNS mapping已生效

```
 Interface: Reth1
    Protocol: 6(TCP)
    Global IP/port: 125.x.x.x/80
    Local IP/port : 168.x.x.x/80
    Rule name     : 17
    NAT counting  : 0
Config status : Active

NAT DNS mapping information:
  Totally 3 NAT DNS mappings.
  Domain name  : oa.schdri.com
  Global IP    : 125.x.x.x
  Global port  : 80
  Protocol     : TCP(6)
  Config status: Active
```

解决方法

NAT DNS mapping需要满足解析出的地址是公网地址，该公网地址是nat server的global地址才行，客户现场配置要求已符合，配置正常，后续由于现场出口有两个reth1与reth2,所有出公网的流量的回程流量都从reth1回应，现场测试的情况是从reth2出去但是从reth1回应，即使再reth2做了同样的nat server绑定关系，运营商的回程流量也无法控制，通过在内网口做PBR，让出去上网的流量强制从reth1出去解决