ACG1000用户认证策略排除地址不生效问题

ACG1000 马雷勇 2019-04-08 发表

组网及说明

二层模式透明部署

问题描述

客户现网中ACG1000透明模式部署在核心交换机与出口网关之间做短信认证，做完短信认证成功后想针对内网用户访问外部的某些URL地址做放通不需要认证，但是目的地址将url域名以及dns服务器地址排除后依旧无法访问。

过程分析

一、设备配置排查

用户认证策略

策略中目的地址将dns服务器地址和几个url排除

二、测试结果------连排除的地址都无法ping通

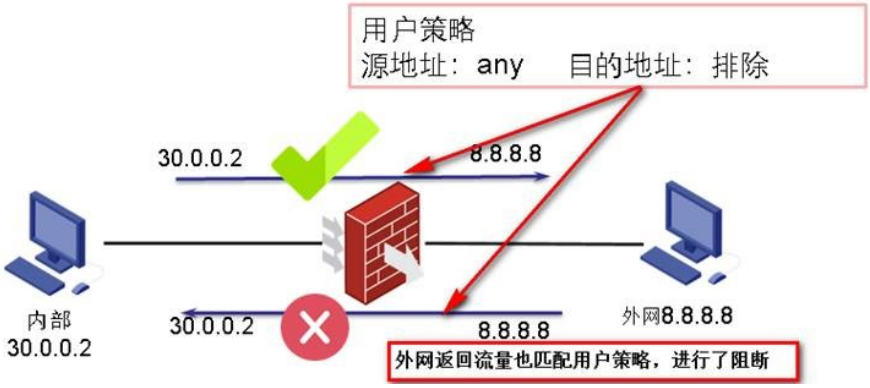
```
C:\Users\admin>ping 8.8.8.8

正在 Ping 8.8.8.8 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。

8.8.8.8 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 0, 丢失 = 3 (100% 丢失),
Control-C
^C
```

取消策略后就能正常ping通，说明外网没啥问题

怀疑排除地址功能不生效，确认原因为：
这个主要涉及到流量有两个方向，正常理解只需要排除内网访问外网一个方向的流量就行，但场景中排查原因为流表中会话内网出局方向没有阻断，回程流量被阻断，所以为了两个方向流量都不能匹配用户策略，用户策略对双向流量进行检测，所以需要源目地址都要针对免认证流量进行放通。如下图



解决方法

将用户认证策略中源地址由any改为内网用户地址对象，让回程流量不匹配用户策略，测试OK