内网终端经过防火墙dns解析异常

NAT 彭钦 2023-11-20 发表

组网及说明

无

告警信息

无

告警信息

问题描述

内网终端配置dns服务器为114.114.114.114，访问某域名时发现终端解析地址为私网地址，而非公网地址。防火墙做源地址转换。

过程分析

抓包发现，防火墙收到dns服务器回应，解析出该域名地址为公网地址，但是发给终端却是私网地址。查看配置发现，dns回应报文的内存解析地址匹配了设备的nat static outbound的global地址，防火墙nat alg dns默认开启，内层的地址转换成inside地址，即变成私网地址。

若现场想实现解析出公网地址，这种场景下需要关闭nat alg dns，内层地址不转，同时防火墙需要开启nat hairpin功能，实现内网终端访问内部服务器是通过访问公网地址方式。

解决方法

该现象为正常现象