防火墙无法做dns解析问题

NAT 王树岭 2024-11-28 发表

组网及说明

终端---防火墙---公网

问题描述

现场终端PC配置dns指向防火墙，防火墙开启dns代理，同时配置dns server。

配置后终端无法正常上网，经过简单排查发现是dns无法解析，后续定位到防火墙无法ping通域名，display dns host无法看到域名表项信息

过程分析

进一步定位，发现现场的公网地址配置在loopback口，路由出接口的ip是私网地址

由于设备dns解析默认带的源地址是路由出接口地址，所以流量不通

需要指定loopback口作为dns解析的源接口 dns source-interface xxxx

解决方法

指定公网口作为dns解析的源接口即可

dns source-interface xxx