# comwareV7 FW 配置DNS代理后业务异常

域间策略/安全域 孔德飞 2022-10-17 发表

## 组网及说明

组网如下：内网终端------核心FW1-------三层设备-----出口FW2-----互联网

## 告警信息

暂无

## 问题描述

现场内网终端与核心FW1上配置相同的DNS服务器，核心FW1开启DNS代理，出口FW2开启dns snoop吗，并且FW2是多出口 但是现场业务有问题

## 过程分析

最终定位为： 终端与设备进行DNS域名请求的时候，要保证两者从相同的运营商出口出去，因为即使相同DNS服务器，针对不同运营商的源地址，回应的解析结果也是不一致的（类似我们LB的只能DNS）

## 解决方法

解决方法有两个：
1.通过策略路由让终端与FW的DNS请求从同一个运营商出去
2.当内网终端的数量较少时，可以将内网终端的DNS指向FW，然后FW开启DNS代理

需要注意的点：
DNS代理
首先设备上要配置域名地址对象组与DNS服务器，配置之后，设备会自己配置的DNS服务器发出DNS请求报文（DNS表项老化之后，会再次主动发出请求、需要一定的版本，因为部分分支做过变动），设备如果收到DNS应答，则会记录DNS表项（display dns host）；如果域名对应的地址频繁变化，可以开启地址对象组缓存功能（object- group ageing）.

DNS snoop
需要DNS流量过设备，设备会记录DNS请求报文中的域名，如果DNS回应报文的域名与请求一致，则会记录DNS表项（probe视图：display system internal dns snooping host）
当然对于域名解析结果频繁变化的情况，也可以开启地址对象组缓存功能（object- group ageing）.

DNS常见的问题：
终端与设备记录的DNS表项不一致，此时需要注意以下几点：
1.终端与FW指定的DNS服务器要一致；
2.终端与设备进行DNS域名请求的时候，要保证两者从相同的运营商出口出去，因为即使相同DNS服务器，针对不同运营商的源地址，回应的解析结果也是不一致的（类似我们LB的智能DNS）