V7版本防火墙F5020做DNS代理不成功的经验案例

其他 叶靖 2018-09-29 发表

组网及说明

不涉及

问题描述

某局点购买了一台V7的防火墙F5020，串联在网络中作为网关设备，现在想做DNS代理。现在在防火墙上配置了一个loopback接口，其IP地址为192.168.1.1/24，该地址是作为终端配置的DNS地址用的：

interface LoopBack0

ip address 192.168.1.1 255.255.255.0

另外还在设备上配置了DNS代理的相关配置，将5.5.5.5设置为代理之后的实际DNS服务器地址，具体如下：

dns proxy enable

dns server 5.5.5.5

现场将防火墙上的各个安全域之间的安全策略完全放通，但是现场发现，DNS代理并没有生效。

过程分析

现场测试，终端将DNS地址设置为192.168.1.1，现场终端是可以ping通192.168.1.1这个地址，但是终端ping一些公网上的域名如www.baidu.com无法ping通，通过nslookup命令发现确实无法解析出域名，且终端如果直接ping www.baidu.com对应的IP地址是可以ping通的。也就是说，问题确实是出现在DNS解析这一块。

考虑到DNS代理的配置比较简单，现场的dns proxy及安全策略的相关配置都没什么问题，于是建议现场更换浏览器，清除缓存已经更换PC测试，但是都没有好转，故障依然存在。

最好现场取消使用F5020上的loopback接口地址作为终端的DNS地址，而是使用防火墙的下行接口的地址作为终端的DNS地址，测试发现，通过以上修改，DNS代理成功了，终端可以正常解析出域名并通过域名访问公网。

解决方法

在V7防火墙上配置DNS代理的功能时，如果将防火墙的loopback地址设置为终端DNS，即使在终端到loopback地址可达的情况下，可能还是会出现DNS代理不成功的情况，此时建议将终端的DNS地址设置为防火墙下行接口的地址。