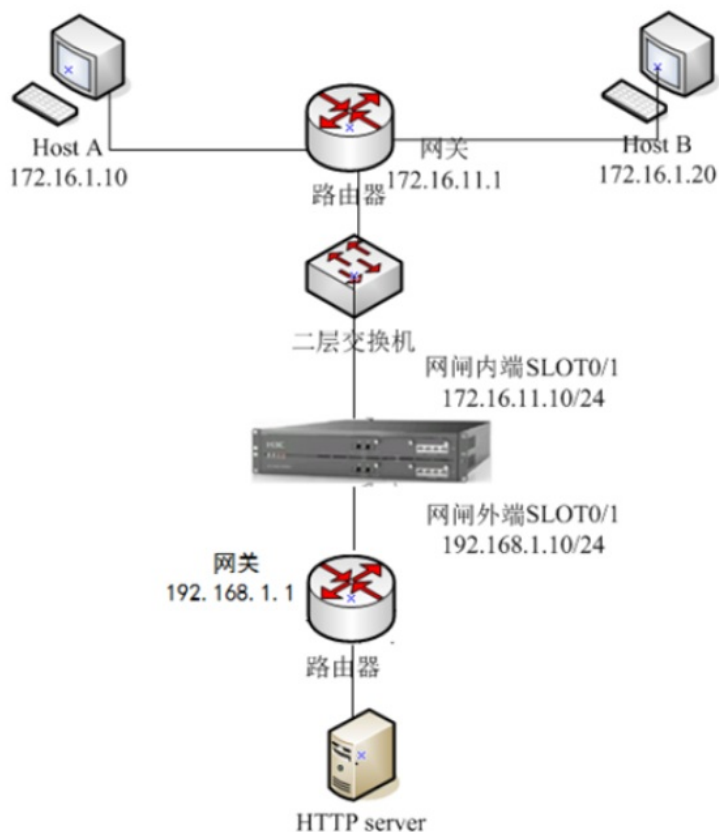


某局点GAP2000网闸设备配置HTTP代理未放通DNS通道导致访问外网异常的经验案例（二）

网闸 叶靖 2020-09-29 发表

组网及说明

某局点购买了一台网闸设备以实现了对网络的控制，客户现场组网情况如下图。



问题描述

现场客户存在内网终端访问互联网的需求，因此客户配置了HTTP代理，使用网闸作为HTTP代理设备，实现内网终端的上网功能。但是现场配置完HTTP代理之后，测试发现现场终端仍然无法访问互联网。

过程分析

现场首先检查了HTTP代理的配置，配置上没有发现任何问题。接下来我们在内网终端上测试，尝试访问百度www.baidu.com，测试确实无法访问。这时，我们再通过nslookup命令测试域名www.baidu.com地址解析情况，发现域名也无法正常解析。

原来现场在配置HTTP代理之后，并没有开启通道放通DNS的报文，导致DNS报文无法通过网闸，终端无法正常进行DNS解析。

解决方法

我们假设内网终端的DNS地址为114.114.114.114，由于内端机接口可以配置多个地址，我们可以将内端机的一个接口地址配置为114.114.114.114，并在网闸上配置放通DNS的通道，将通道的监听地址配置为内端机接口地址114.114.114.114，端口为DNS端口53，配置通道目的地址也配置为DNS服务器如114.114.114.114，配置通道的连接地址为外端机接口地址192.168.1.10。



该通道的作用是，当外网的用户访问114.114.114.114进行DNS解析时，网闸会将请求摆渡到外网。随后以192.168.1.10 这个连接IP 作为源地址，并且还会以114.114.114.114作为目标地址封装数据包，发送给公网上的DNS服务器114.114.114.114，从而实现DNS正常解析。

这种方式的优点是可以不修改终端的DNS地址，减少工作量。