

知 某局点绿洲开局注册AC设备不成功问题处理

绿洲平台 朱恺 2019-03-26 发表

组网及说明

某局点新上线AC需要结合绿洲进行上网用户认证功能。按照绿洲开局部署指导文档完成了基础配置工作。

问题描述

但是完成部署之后，发现AC依旧无法在绿洲上上线。设备ping 外网域名 及DNS解析绿洲域名均无问题。

过程分析

在问题处理中，查看了AC的配置，发现AC存在多个出口：一条默认路由，一个对外出口开启NAT。按照绿洲的地址依照了默认路由进行转发，对此进行了telnet 绿洲地址端口号80和443的对比操作，当删除了默认路由之后绿洲业务全部完成，当默认路由存在时则一直不能正常通信。与客户沟通了解到默认路由出口之后路径上存在防火墙设备，防火墙上对tcp连接存在限制，因此能得到这种现象。按照这个排查的方式，对绿洲目的地址进行静态路由配置，强制去往oasis.h3c.com 139.217.27.153地址走nat出口。

配置完成之后发现路绿洲依旧关联不上，开启绿洲隧道debug之后发现，AC去往oasisdev.h3c.com的地址无法完成tcp建链。因此加入去往oasisdev.h3c.com 139.217.27.118等其他三个域名。

修改完成之后，绿洲关联成功，无问题。

解决方法

该问题的主要核心就是AC默认去往绿洲地址会按照缺省路由进行转发，一定要确认出口设备是否对TCP等绿洲通信必要的条件进行限制。可以通过修改静态路由的方式去选择最佳转发路径。

此外修改静态路由时一定要确保写全4个绿洲使用的域名及IP目的地址。

oasis.h3c.com (139.217.27.153) (绿洲cloud-management隧道使用)

oasisdev.h3c.com (139.217.27.118) (绿洲cmtunnel隧道使用)

lvzhoudev.h3c.com (139.217.22.254) (绿洲平台与设备通信地址)

oasisauth.h3c.com (139.217.11.74) (绿洲认证使用)