某局点WX3510H绿洲平台隧道建立异常经验案例

绿洲平台 陈孙潇 2017-03-19 发表

某局点使用WX3510H对接绿洲平台，现场AC无法正常注册到绿洲上，并且两条绿洲隧道也建立异常。

无

为分析AC为何无法注册到绿洲上，于是做以下排查：

1.因为绿洲平台是一个公网的服务，所以首先要保证AC设备可以连接互联网并解析绿洲平台地址。

```
[RBCN_HZ_NCAoTi_AC]ping -a 172.25.96.1 www.baidu.com
Ping www.baidu.com (14.215.177.37) from 172.25.96.1: 56 data bytes, press CTRL_C
 to break
56 bytes from 14.215.177.37: icmp_seq=0 ttl=54 time=17.410 ms
56 bytes from 14.215.177.37: icmp_seq=1 ttl=54 time=27.908 ms
56 bytes from 14.215.177.37: icmp_seq=2 ttl=54 time=17.198 ms
56 bytes from 14.215.177.37: icmp_seq=3 ttl=54 time=17.264 ms
56 bytes from 14.215.177.37: icmp_seq=4 ttl=54 time=17.385 ms

--- Ping statistics for www.baidu.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 17.198/19.433/27.908/4.238 ms
[RBCN_HZ_NCAoTi_AC]ping -a 172.25.96.1 lvzhou.h3c.com
Ping lvzhou.h3c.com (139.219.8.159) from 172.25.96.1: 56 data bytes, press CTRL_
C to break
Request time out
Request time out
```

可以看到设备能够正常ping通公网地址，并且解析出绿洲平台的域名，因此公网链路这一块没有什么问题。

2.查看绿洲隧道建立情况

[RBCN_HZ_NCAoTi_AC]dis cloud state

Cloud connection state : Unconnected

Device state : Idle

Cloud server address : N/A

Cloud server domain name : lvzhouv3.h3c.com

Local port : 443

Connected at : Sun Nov 13 03:42:08 2016

Duration : 00d 00h 00m 00s

[RBCN_HZ_NCAoTi_AC]dis cmtunnel state

Cloud management tunnel

Server address : 139.219.8.159

Server name : lvzhou.h3c.com

Local port : 80

Connection state : Established

Device state : Request_success

可以看到cmtunnel已经成功建立，但是cloud state仍然是idle状态，且cloud server的ip地址为N/A,因此怀疑可能是域名解析的问题，所以尝试给设备配置固定的域名地址：

dns proxy enable

ip host lvzhou.h3c.com 139.219.8.159

ip host www.h3c.com 60.191.123.44

ip host lvzhoudev.h3c.com 139.217.22.254

ip host lvzhouv3.h3c.com 139.217.22.79

配置固定域名地址后发现隧道仍然不能正常建立。由于隧道主要是通过设备和上述几个地址进行交互建立的，隧道始终建立不起来，公网链路又是正常的，因此怀疑是否是组网中有地方将这个几个流量给拒绝了。

3.根据现场工程师反馈，现场公网出口为一台深信服的防火墙。查看深信服防火墙上的url日志发现有lvzhoudev.h3c.com域名的拒绝记录，因此很有可能是防火墙拒绝了绿洲的流量导致隧道不能正常建立。

在出口防火墙上放通http://lvzhoudev.h3c.com的域名之后，隧道正常建立，AC成功注册到绿洲上。

在处理AC注册到绿洲平台的问题的时候，首先就是查看设备到公网的链路是否正常，绿洲平台域名能否正常解析，然后再是查看cmtunnel和cloud两条隧道的状态，尝试固定域名地址。通过这两步可以解决大部分绿洲注册的问题。

需要注意的是我司绿洲平台后面实现机制做了修改，域名和绿洲账号都有所不同，当前的绿洲配置建议按照dmp上《绿洲上线及认证业务开局指导书V2.1》来参考操作。