某局点F5000通过SSL VPN无法访问内网VPN实例中的资源

SSL VPN VRF 窦祖尧 2020-04-28 发表

组网及说明

现场F5000做SSL VPN，客户无法通过SSL VPN访问内部VPN实例中的资源

问题描述

现场可以通过SSL VPN访问不在VPN实例中的资源的，说明SSL VPN配置是没有问题的

过程分析

由于用户的部分需求是在VPN实例中，所以需要设备上去往VPN实例中的路由并且在VPN实例中添加去往Public的路由，可以用如下方法实现

向Public路由表添加去往对应VPN实例的路由：

ip route-static X.X.X.X X vpn-instance test X.X.X.X

由于对于SSL VPN拨号的用户，对我们防火墙来说相当于是直连的关系，所以只能通过向VPN实例中引入Public直连路由的方法来实现：

[F5000]ip vpn-instance test

[F5000]address-family ipv4

[F5000]route-replicate from public protocol direct

这样通过路由引入的方式就可以打通到VPN实例的路由，实现正常访问

但是现场还有部分VPN资源，和防火墙属于直连关系，所以我们无法通过下发静态路由的方式，而且Public路由表无法引入相关直连路由，所以这种情况不下，无法通过引入路由的方式解决

解决方法

上述情况下，我们只能通过使SSL VPN拨号上来的用户属于一个VRF，然后通过同VRF之间的访问或者不同VRF之间路由相互引入实现互访的需求：

SSL VPN结合VRF的方法（只需要把AC接口和VPN实例加入对应VRF即可）：

首先把AC接口加入VPN实例：

[F5000]interface SSLVPN-AC 1

[F5000-SSLVPN-AC1]ip binding vpn-instance test

然后把SSL VPN Context加入VRF：

[F5000]sslvpn context test

[F5000-sslvpn-context-test]vpn-instance test

这样也是另外一种SSL VPN访问内网资源的一种方式