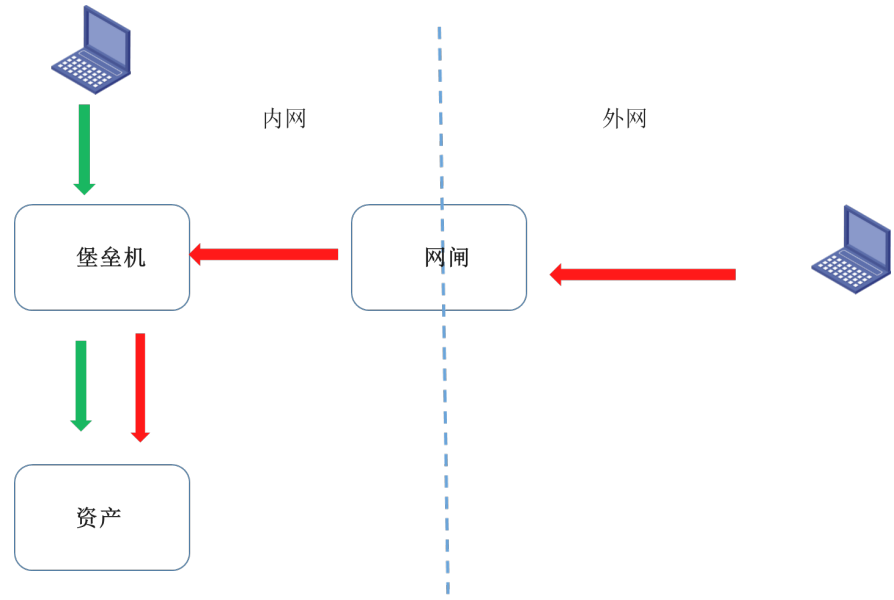
堡垒机过网闸访问资产异常问题分析

运维审计 网闸 **孔凡安** 2022-03-04 发表

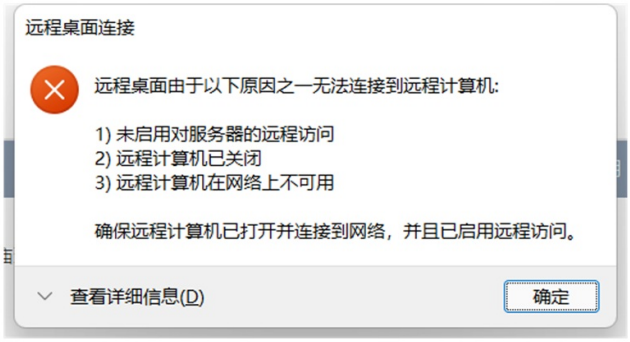
组网及说明



如图所示：内网环境，通过堡垒机可以正常访问资产，在网闸上做了对内网堡垒机地址的映射，希望通过公网也能正常使用堡垒机。结果堡垒机web界面可以正常访问，但是访问资产异常。

问题描述

在内网环境内使用堡垒机可以正常访问资产（RDP、SSH等方式）。
在网闸上做了对内网堡垒机地址的映射，希望通过公网也能正常使用堡垒机。结果堡垒机web界面可以正常访问，但是访问资产异常。

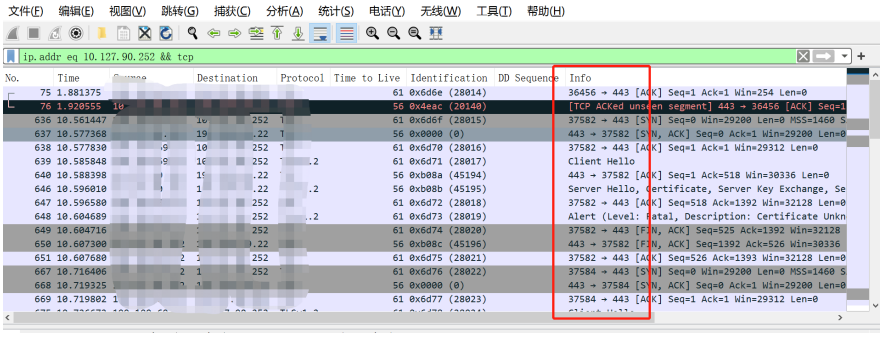


过程分析

首先，内网环境可以通过堡垒机访问资产，说明堡垒机的配置基本没问题。

其次，查看网闸侧对堡垒机地址的映射情况，发现对所有的端口都进行了映射，也没有问题。

外端机抓包发现只有访问堡垒机443端口的报文：



怀疑访问资产的报文没到网闸，发现pc到网闸地址3389和22端口都是不通的。

解决方法

PC到网闸设备之间有安全设备拦截了访问网闸地址3389、22端口的报文，放通后访问资产业务正常。
涉及开放的端口具体可以参考官网配置指导。