# 某局点使用堡垒机访问内部网站失败

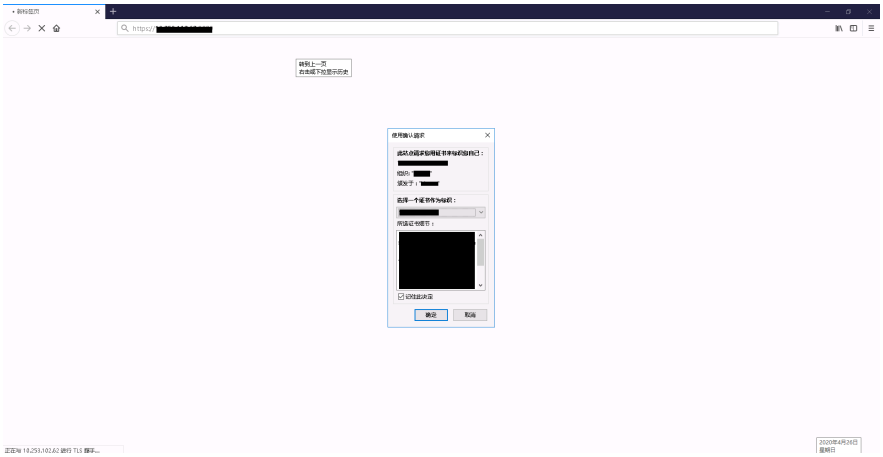
运维审计　**窦祖尧**　2020-04-26 发表

## 组网及说明

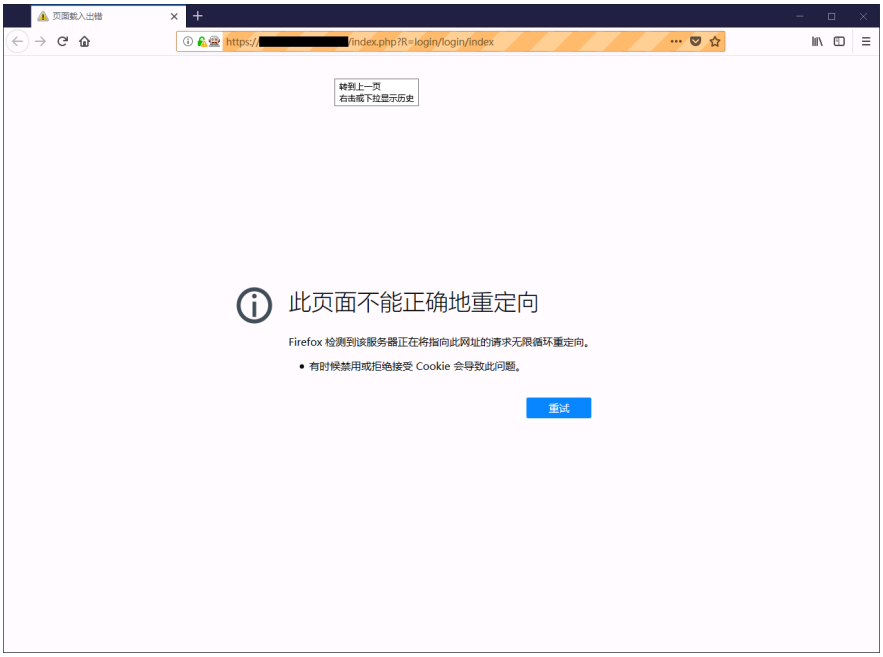
现场用户使用堡垒机中的火狐浏览器访问内网vpn网站

## 问题描述

现场访问内网vpn网站需要先进行证书认证，在应用发布服务器上访问vpn网页的时候，首先先打开浏览器，之后选择证书后才能进入vpn网页的登录界面。



但是用户无法通过堡垒机打开内网vpn网页，报错如下：

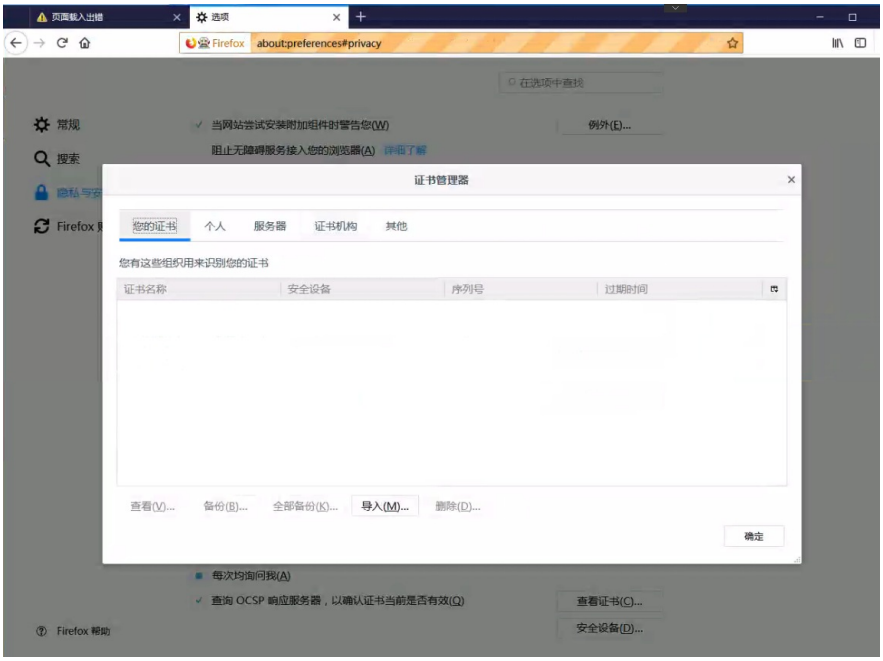



## 过程分析

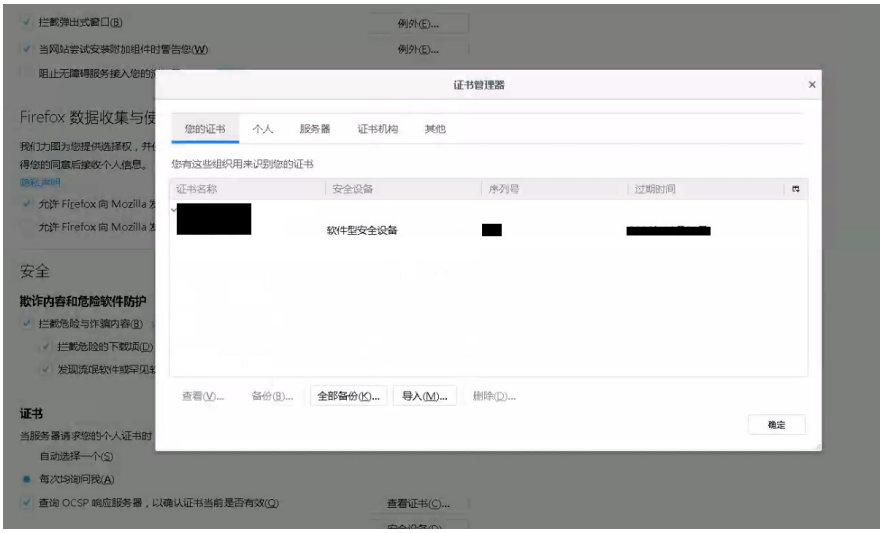
应用发布服务器发布了两个应用：谷歌浏览器和火狐浏览器。在应用发布服务器上使用谷歌浏览器也是同样的错误无法打开vpn网站

并且通过对比堡垒机打开的火狐浏览器和应用发布服务器打开的火狐浏览器的证书：

从堡垒机打开：




从应用发布服务器打开：

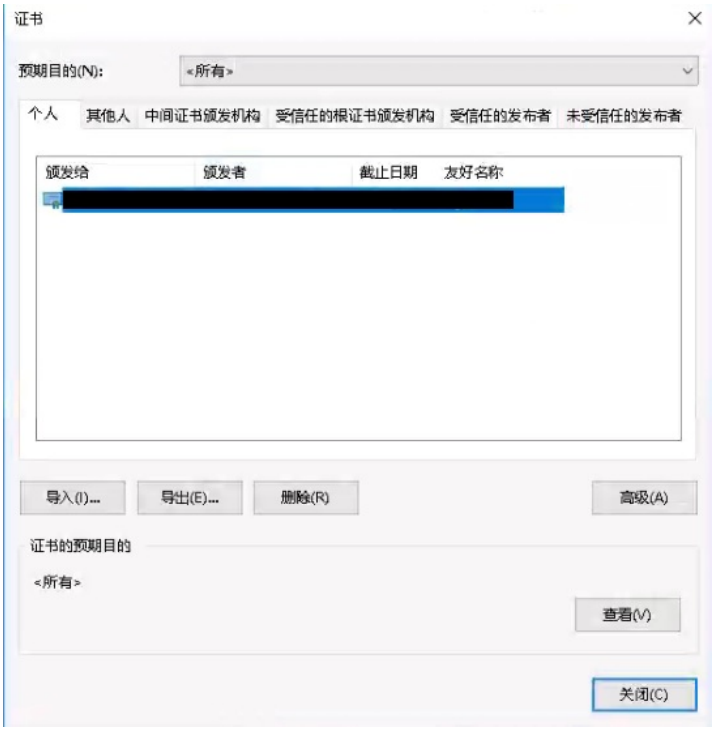



说明出现问题的原因是堡垒机调用火狐浏览器的时候并没有调用相关证书导致无法打开vpn网站

## 解决方法

通过分析，现场只给火狐浏览器导入证书，并没有导入本地证书（浏览器机制问题，火狐游览器有自己的证书库），这也说明了现场发布的谷歌浏览器业务无法打开vpn网站的原因了。

所以经过用户许可，给应用发布服务器导入本地证书，经过测试使本地谷歌浏览器可以正常打开vpn网站，同时通过堡垒机也可以访问vpn网站了（使用谷歌浏览器）


证书
预期目的(N):
<所有>
个人
其他人
中间证书颁发机构
受信任的根证书颁发机构
受信任的发布者
未受信任的发布者
颁发给
颁发者
截止日期
友好名称
[redacted]
导入(I)...
导出(E)...
删除(R)
高级(A)
证书的预期目的
<所有>
查看(V)
关闭(C)