某局点ACG1000应用控制只允许使用向日葵应用不生效的经验案例

应用审计 丁佳欣 2022-06-06 发表

组网及说明

null

告警信息

null

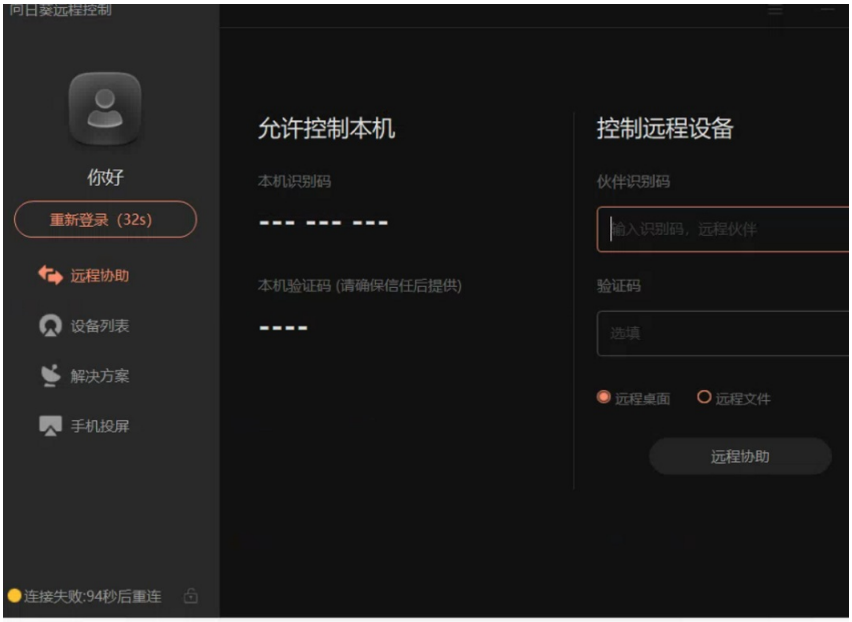
告警信息

问题描述

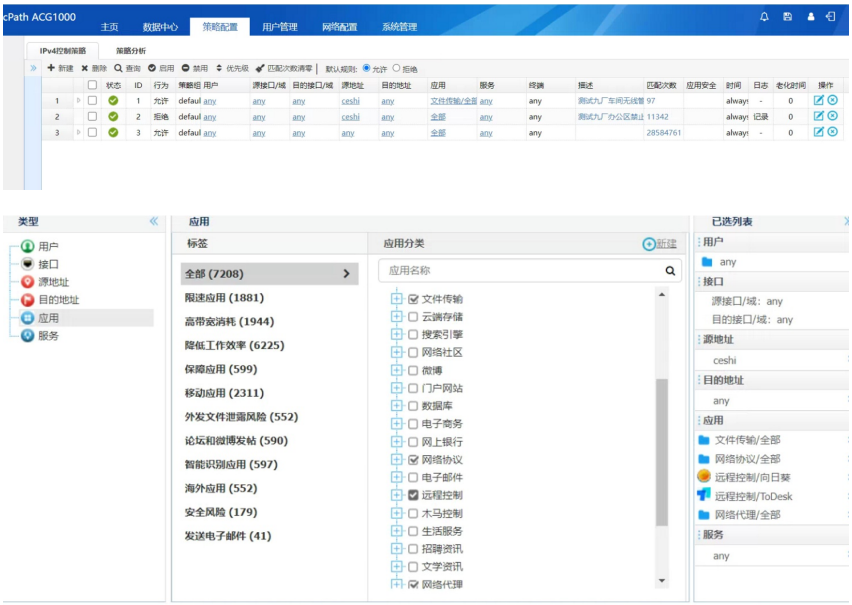
现场配置ACG1000控制策略实现只允许用户访问向日葵的需求，但是配置后无法正常登录向日葵应用。

过程分析

1、 我们知道几乎所有应用的访问都要都用tcp、udp等网络协议，于是建议现场放行网络协议后测试，可以登录向日葵了，但是仍提示无法连接到服务，现场网络设置无问题。



2、 收集现场配置，第一条策略只放行向日葵和网络协议，第二条策略拒绝所有应用，初步检查配置未发现问题。



并且经测试，取消前两条策略后向日葵应用服务正常，再次确认了是由于前两条控制策略阻断。

3、 向日葵应用服务无法正常连接时，多次点击重新连接，然后查询该用户的应用统计信息实时查看，多次测试查看后发现向日葵点击重连时该终端应用统计日志详细信息中会出现贝锐（Oray）的应用，后续实际测试，在策略中放行该应用后向日葵服务连接正常。（向日葵远程控制是贝锐旗下产品）

解决方法

在控制策略中将网络协议、向日葵和贝锐均放行后客户需求正常实现。在控制策略无法准确针对某个应用进行控制或其他存在误识别的场景下，我们可以通过查找具体用户的应用识别日志找到相关线索