

某局点SecCenter CSAP-SA-AK640 综合日志审计平台 登录策略限制ip不成功

安全监测中心 关萌 2023-09-30 发表

问题描述

某局点使用我司SecCenter CSAP-SA-AK640 综合日志审计平台，部署完成后功能使用正常。用户想限制登录IP，配置完限制登录的IP地址后，发现不在限制IP范围的用户仍然可以登录成功。配置截图如下



用户只允许了几个IP地址可以登录该设备，但发现使用所有IP都能登录设备。

过程分析

经过分析，该产品限制登录的不是打开页面的功能，是限制的账号登录IP。也就是说，限制IP后，所有IP都可以打开登录界面，而限制哪个用户可以使用哪个IP地址登录需要在用户中绑定登录策略，并不是打开登录界面的策略。

解决方法

需要在用户列表，用户下配置登录策略，将之前配置好的登录策略与用户名绑定，配置完成后可以限制登录该用的IP地址。使用其他IP无法登录成功。

The screenshot shows a web-based configuration interface for user management. On the left is a navigation menu with the following items: 组分析, 审计, 关系, 用户, 用户列表, 登录策略, 密码策略, 资产, 规则, 报表, and 告警. The '用户' (User) menu item is expanded, and '用户列表' (User List) is selected. The main content area displays a configuration form for a user named 'admin'. The fields are as follows:

- 用户名 (Username): admin
- 密码 (Password): 至少包含1个小写字母、1个大写字母、1个特殊字符、1个数字且长度最少为8个字符
- 确认密码 (Confirm Password): 请重复以上密码
- 角色 (Role): 超级管理员
- 登录策略 (Login Strategy): [Redacted]
- 邮箱 (Email): 请输入邮箱号
- 手机号 (Mobile Number): 请输入手机号
- 用户归属 (User Affiliation): 未归属
- 用户备注 (User Remark): 拥有所有权限

At the bottom right of the form, there are two buttons: '提交' (Submit) and '取消' (Cancel).

