某局点password-control导致用户无法登录

password control　zhiliao_HABbRf　2022-03-28 发表

组网及说明

无

问题描述

用户很久没有登录防火墙设备了，想要再次登录配置时，发现无法登录，使用admin或其他用户都无法登录，询问故障产生原因

过程分析

1. 在交谈中，客户提及到很久没有登录了，设备也做过等保，初步怀疑是password-control导致的
2. 让客户使用comware V7跳过密码的方式登录到设备上，收集了一份配置文件
3. 重点查看password-control的配置信息，配置信息如下，命令含义已标注

 password-control enable　　//开启password-control功能

 undo password-control composition enable　　//用户密码的组合策略为默认配置，默认的组合密码组合元素是2种

 undo password-control history enable　　//每个用户密码历史记录的最大条数，默认是四条

 password-control login-attempt 5 exceed lock-time 5　　//命令用来配置允许用户登录的最大尝试次数以及登录尝试失败后的处理措施，此处的配置表示允许用户失败5次，锁定时间为5分钟

 password-control update-interval 0　　//命令用来配置密码更新的最小时间间隔，单位为小时。0表示对密码更新的时间间隔无限制

 undo password-control complexity user-name check　　//取消指定的密码复杂度检查策略

4.查看上面的配置信息，并不会导致所用用户无法登录，故需要排查是否有其他原因

5.在官网有说明，当开启password-control功能后，会存在密码老化时间；默认是90天，会在提前15天的时候，当用户登录设备，会提示用户登录设备需要更改密码。如果过了90天，还有30天的时间有3次修改密码的机会。再次过了这个30天，账户就会失效

官网的配置指导还有另一个功能的说明，也会导致用户长时间不登录导致无法登录设备的原因；就是idle-time时间，当开启password-control功能后，会启动一个90天的密码超时时间，在此期间内，如果存在登录行为，则重新计时。如果90天内没有登录，账户也会失效，无法登录设备

6.所以存在两种情况都会导致此故障现象的发生

解决方法

通过comware v7跳过密码的方式，登录设备，修改用户的用户名和密码进行重新登录