

知 EPS联动EIA加入黑名单功能，解除黑名单后用户不能及时上线

iMC EPS

iMC

马永鸿 2022-12-28 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

现场配置了EPS联动EIA加入黑名单功能。



关联服务器	启用
IP地址 *	192.168.6.10
端口 *	8080
用户名 *	admin
密码 *	****
确认密码 *	****
联动PLAT组件	停用
联动EIA组件	启用



提示

启用自动加入黑名单时, 如果系统发现有端点满足条件, 会自动将该端点阻断并加入到黑名单中; 采用扫描器联动方式时, 只需要为端点的接入交换机配置SNMP读写团体字, 其他网关设备需要配置SNMP团体字; 启用“非直连端口加入黑名单”时, 只要有交换机学习到此端点MAC就会阻断其对应端口, 可能会影响其他端点正常接入。

加入黑名单方式	EIA联动
业务场景	业务优先
非直连端口加入黑名单	停用
非法端点自动加入黑名单	停用
新发现端点自动加入黑名单	停用
离线端点自动加入黑名单	停用
新发现端点保留时长(0-60天) *	3
离线端点保留时长(1-365天) *	7
离网告警周期(0-30分) *	30

当某端点被审批为非法后, 会被加到EIA的黑名单中, 然后这个端点就无法上线了, 已经在线的会被强制下线。

当非法端点重新审批为合法后, 正常来讲会重新上线。

而现场环境, 审批为非法然后下线没有问题, 而审批为合法后, 黑名单已经解除, 但该终端仍然无法上线。大概等10~20分钟后, 才能正常上线。

过程分析

收集uam的debug日志，查看重新审批为合法，黑名单解除后，终端的上线过程。

```
%% 2022-11-30 02:50:40.465 ; [LDBG] ; [1946154752] ; LAN ; SYS ; 3 ; ; ; Send message attribute list:
```

Code = 3 ID = 207

Reply-Message(18) = E63620: The request is dropped by UAM because of 11 consecutive authentication failures. Please try again 15 minutes later.

可以看到，上线失败的原因是E63620，意思是连续11次终端认证失败，视为该终端在攻击，防攻击处理15分钟。因此在15分钟内用户无法上线。

防攻击处理，在系统参数配置里可以配置。现场之前启用了用户认证防攻击，配置的是15分钟。加入黑名单后，用户会连续认证失败。然后即使解除黑名单，连续11次终端认证失败，视为该终端在攻击，防攻击处理15分钟。15分钟后才可以认证通过。



解决方法

将“用户认证防攻击”这个参数关闭后，当终端解除黑名单后即可立即上线。

