EIA黑名单实现机制

寻尚岩 2016-11-05 发表

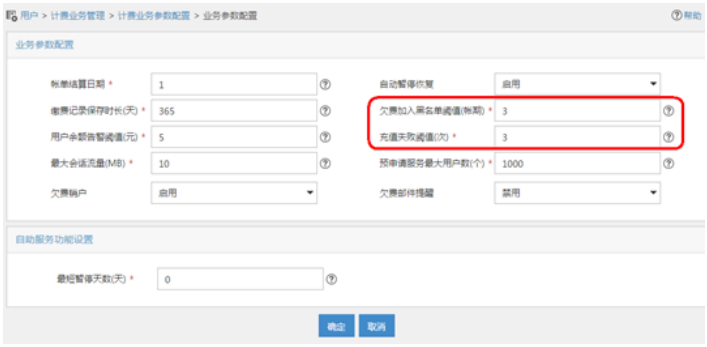
在使用iMC的认证功能组件UAM时，有将用户加入黑名单的功能，目前有五种方式可以将普通帐号加入黑名单：

(1)　管理员主动将某帐号加入黑名单。

这种情况下，黑名单功能仅仅针对帐号本身，一旦该帐号加入黑名单不论在哪台客户端PC上登录均有效。将一个在线用户加入黑名单后，UAM并不会立即发送强制下线报文，而是要等到下一个计费更新报文后才会回应session-timeout=0最长要等待12分钟才能下线，对于不支持计费更新报文的设备，只有在下次上线时才会生效，管理员接触后则可以立即上线成功。

(2)　如果采用计费功能的话，帐号因欠费加入黑名单。这种情况下，也只针对帐号本身。

(3)　用户使用充值业务时，一天内连续输入充值密码错误次数超过指定阈值。这种情况只针对用户充值时使用的IP生效，即用户使用其它IP地址仍然可以认证。



(1)　由于密码多次输入错误（比如超过10次），即恶意登录尝试加入黑名单。

这种情况和前两种有区别，它针对帐号和用户使用的那台客户端PC的MAC。也就是说，某帐号在某台PC上多次输入密码错误而加入黑名单后，如果在其他PC上用正确的用户名和密码登录则能正常上线，而不受黑名单的限制。这样做的目的是：防止当某人盗用其他人帐号，多次恶意在别的PC上登录多次而加入黑名单，但帐号拥有者本身在自己的电脑上使用正确的帐号上线不受限制。

缺省情况下是一天内输入10次错误的密码会被自动加入黑名单，到第二天凌晨自动解除。也可以配置按加入时长解除黑名单。

(1)　802.1X认证方式下，用户使用无效客户端上线。这种情况只针对认证时的终端MAC生效，用户仍然可以使用其它终端上线。

认证防攻击：

用户连续认证失败次数超阈值时（并不是只有密码错误，包含其他的认证失败情况），服务器对该用户的认证报文不再理会，收到后直接丢弃，直到15分钟后才会处理；第4点提到的凌晨解除只是针对用户密码错误达到阈值时会把用户加入黑名单，在凌晨的时候把黑名单解除。