某局点 F5040 （V7）防火墙SSLVPN拨入提示计费失败问题分析

尤良柱 2018-02-12 发表

某局点使用我司F5040设备作为SSLVPN 网关，正常运行过程中部分用户无法通过inode 客户端拨入，并提示计费失败信息。

inode客户端在认证过程中提示计费失败。

通过对无法登录用户进行排查，发现提示计费失败无法登录的用户存在直接关机等非正常下线行为，分析因为非正常下线导致设备认为该用户仍然在线，再次登录时因为配置了同时在线用户数限制提示计费失败的信息而无法登录；

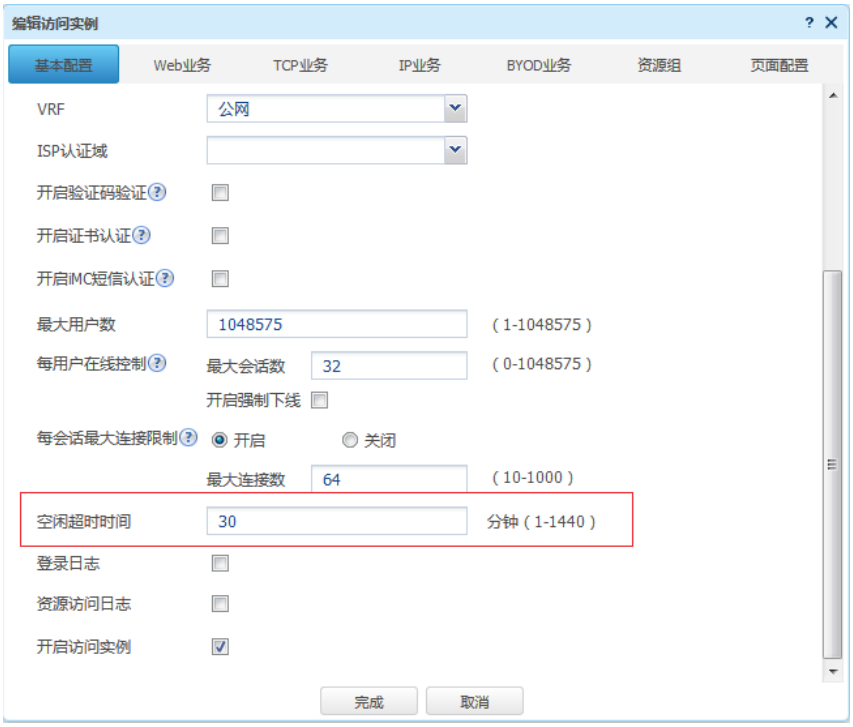
此时经过修改同时在线用户数限制（由1改为2），测试后用户可以登录；然后通过分析诊断和配置信息，发现用户配置如下：

```
#
  local-user 66001073 class network
    password cipher $c$3$yMS67jtJiN+ila9yNR9+MBMpqx9o3roi/AGB8/U=
    access-limit 1
    service-type sslvpn
    authorization-attribute idle-cut 30
    authorization-attribute user-role network-operator
    authorization-attribute sslvpn-policy-group pgroup
  #
```

用户已经配置了空闲切断时间为30分钟，为什么异常下线后没有触发空闲切断机制下线?

通过查询资料发现对于SSLVPN用户，只有授权属性authorization-attribute sslvpn-policy-group pgroup有效，配置的authorization-attribute idle-cut 30是不生效的，导致用户非正常下线后不能因为空闲超期而自动下线，最后客户再次登录时提示计费失败。

对于SSLVPN用户，在创建用户时配置的授权属性authorization-attribute idle-cut 30 是不生效的，空闲超时时间需要在web界面SSLVPN context 访问实例下配置：



配置完成后可在命令行使用display sslvpn context 命令查看配置是否生效：

```
 Context name: ctx
    Operation state: Up
    AAA domain: Not specified
    Certificate authentication: Disabled
    Password authentication: Enabled
    Authentication use: All
    Dynamic password: Disabled
    Code verification: Disabled
    Default policy group: Not configured
    Associated SSL VPN gateway: test
    Maximum users allowed: 1048575
    VPN instance: Not configured
```

Idle timeout: 30 min

1. inode客户端提示计费失败时可以先检查用户是否有非正常下线情况，同时可修改access limit 来测试是否是因为未正确配置空闲超时时间导致的。
2. SSLVPN 用户的空闲超时时间需要在web界面配置，创建local-user时授权属性仅有authorization-attribute sslvpn-policy-group pgroup有效。