

知 认证用户配置idle-cut后，强制空闲用户下线时间不精确问题

认证 金山 2016-09-10 发表

客户在防火墙上启用Portal认证，并配置idle-cut时间，希望下连的认证用户离线后执行强制下线操作。客户表示在刚开始设置的空闲时间为60分钟，字节数是5byte。但是由于自身需求，把时间改成600分钟后，就发现不生效了，后来又再改成其它时长，15分钟、60分钟和其它字节：500Byte\1000byte\5000byte都不生效了。经过测试发现时间不准，如设时长为2小时，人（手机终端WiFi接入Portal）都回家了，远程到防火墙设备上，还要等个三四小时才能下线，有部分的测试帐号还更长。

无

如果只配置时间，流量阈值缺省为10240bytes，当时间阈值到了时，会去和流量阈值比较，如果此在线用户实际使用的流量超过了流量阈值，那么就不会下线。当用户离开现场后，探测报文不通了，但此时设备是不知道终端下线的，设备只能是按终端上线时的时间为统计周期的起始时间。当重新统计的统计周期内的流量低于配置的阈值，并且到了时间阈值后，会自动下线-----现场反馈的下线时间不准是指设备强制终端下线的和终端真实下线的，这个时间间隔与配置预期不符，但这种情况其实是正常的。

```
[YZDC-BA-FW01-isp-gz-portal]display this
#
domain gz-portal
authorization-attribute idle-cut 600 10240
authentication portal radius-scheme gz-portal
authorization portal radius-scheme gz-portal
accounting portal radius-scheme gz-portal
```

无

通过下面命令可以查看当前在线用户的信息，其中包括流量统计，比如用户配置时间为2小时，流量统计超过了阈值，就是重新计时，同时有后台进程会对流量也重新进行统计。此外，需要注意的是，由于协议本身的交互报文也比较多，如果配置的时间较长，应配置流量阈值也大一些，默认这个值，在数小时内仅心跳报文就会超过这个阈值，比如实验室配置600分钟，没有任何流量的情况下，流量阈值就有下面这么多，远远超过10240bytes，因此看到的现象就是一直不下线。

```
dis portal user all verbose //以实际ip查找用户
Total portal users: 1
Basic:
Current IP address: 1.1.1.2
Original IP address: 1.1.1.2
Username: gz-portal
User ID: 0x1000000b
Access interface: GigabitEthernet2/0/15
Service-VLAN/Custom-VLAN: -/-
MAC address: 0015-e943-8218
Domain name: gz-portal
VPN instance: N/A
Status: Online
Portal server: gz-portal
Portal authentication method: Direct
AAA:
Realtime accounting interval: 720s, retry times: 5
Idle cut: 36000 sec, 10240000 bytes
Session duration: 86401 sec, remaining: 86185 sec
Remaining traffic: N/A
Login time: 2015-10-12 06:40:20 UTC
IP pool: N/A
ACL&QoS&Multicast:
Inbound CAR: N/A
Outbound CAR: N/A
ACL number: N/A
```

User profile: N/A

Session group profile: N/A

Max multicast addresses: 4

Flow statistic:

Uplink packets/bytes: 350/22589

Downlink packets/bytes: 1179/95034 //流量阈值是和上下行流量之和来对比