portal认证时的domain下idle-cut值配置多少合适

Portal 朱恺 2020-02-24 发表

问题描述

在做portal认证功能时经常会看到配置指导中带有idle-cut的值，建议配置。比如：
[AC-V7-isp-1]authorization-attribute idle-cut 10 10240
上例中的10和10240是什么含义?是不是任何地方都配置这个值?

解决方法

要弄清楚这个问题需要先知道idle cut是干什么用的以及如何工作。
portal认证在H3C的实现上是一个基于IP地址存在的认证，也就是认证开始和成功的时候AC会创建一个由用户IP地址为主要线索的认证表项。比如：
portal认证test：张三同学，IP地址是192.168.100.100/24，mac地址XXXXXX。这个表项一旦创立，没有外界干预的情况下AC是不会主动删除表项的。外界干预是指：IMC类的服务器下发了删除表项（用户下线）的指令，或者AC上有人手动操作清除portal表项。
那么这个不主动删除表项的机制有一个优点和一个缺点：
优点：张三同学的手机portal认证上了，然后突然有急事外出了5分钟，回来的时候IP地址没有发生变化依旧是192.168.100.100/24，那么张三同学就无需再次认证，因为AC已经有表项了并且完全合法，张三的感受就是毫无异常不会感觉网络受阻。
缺点：张三同学因为工作要出差一星期，离开之后这个192.168.100.100/24 IP因为DHCP租约老化了重新分配给了李四同学，李四连上wifi获取到IP地址，却怎么也无法认证连portal页面都无法打开。因为在AC上已经存在一个合法表项但是IP和mac却与李四不匹配。

通过上述的描述我们能知道AC上的portal表项，不能一直存在，也不能顺着无线用户的短暂离开就立刻删除。那么怎么解决呢?
这里就引入一个idle cut的机制。idle cut两个参数一个是时间单位是分钟，一个是流量单位是bytes。流量参数是象征意义，代表任何终端能产生的微小流量就证明这个终端依旧存活，比如10240 bytes 也就是1KB左右吧。
关键在于时间参数，这个时间参数的配置有一点点讲究，我们的经验是建议配置在DHCP租约的1/3。为什么是1/3呢?
DHCP的租约按照协议规定：终端在dhcp租约期间的1/2的时间会产生一次续约，假设dhcp的租约为1小时。我们idle cut参数设置在40分钟超过了1/2租约。 终端在30分钟依旧在线，在40分钟依旧在线，因此idle cut判断终端没有离开过ok的。
但是终端在41分钟离开了再也不回来了，dhcp在租约走完一小时后发现这个IP地址没有人使用了，会将IP地址分配给其他人了，此时idle cut需要检测到终端离开需要在下一个40分钟也就是80分钟，这样就存在一小部分终端依旧无法被idle cut给删除表项，造成另外倒霉的新终端认证失败。
为了避免这个极端情况，我们经验上往往设置idle cut的时间参数要小于dhcp租约的1/2,那么1/3看起来是个不错的选择。

举一反三：假如网络dhcp租约的时间为1天24小时，我们的portal idle cut就需要少于12小时，一般8小时挺好的。
既避免了用户离开一会儿就需要重新认证的麻烦，又避免了因为dhcp超时造成一些人压根认证不了的尴尬。