采用guest vlan和第三方服务器对接portal无感知认证失败（此案例中失败原因有很多）

裴锐霖 2015-11-26 发表

客户采用guest vlan+第三方portal服务器+远程mac认证 想实现在有限时间内的portal无感知认证。终端第一次接入时，因为没有通过portal认证，所以进入guest vlan，访问网页时重定向到第三方服务器，先做portal认证，portal认证通过后，服务器记录了已mac地址为用户名和密码的radius用户，紧接着AC触发mac认证，服务器通过mac认证后，进入业务vlan。在两个小时内第二次接入时，不需要做portal认证，直接做mac认证通过就进入业务vlan。

此局点按照经验案例配置完后，发现有诸多问题：

- 1、通过portal认证后，紧接着做mac认证，但是做完mac认证的这一段时间，就不能上网了，并且IP地址和vlan都不会变到业务vlan。
- 2、终端在进入到业务VLAN，MAC认证成功以后大约10多分钟的样子，终端在无感知的情况下，自动切换回guest VLAN，设备上使用命令查看，MAC认证的用户已经下线。服务器上也是下线的状态。
- 3、在mac和portal的domain下配置了idle-cut enable 3 10240000 命令，按理来说3分钟内不超过10M流量会踢下线，但现场3分钟过后portal认证没有踢下线。

从AC测的debug看报文交互都正常，唯一的错误就是当mac认证做第二次认证时，有时服务器会返回认证失败。

针对问题1：由于portal认证完后，第三方服务器会创建一个以mac地址为用户名和密码的radius用户，以供接下来的mac认证使用，所以mac认证也会成功，客户端被划分到业务vlan，但由于客户端没有重新关联，地址还是使用的上次guest vlan中获取的地址，只有等dhcp重新续约的时候才会获取到新vlan的地址。所以会出现短暂的不能上网。

针对问题2：因为在mac认证域下配置了idle-cut，在检测到流量不足时会让mac用户下线，正常来讲，此时还会马上再一次发起mac认证，然后认证成功。但是服务器在AC强制下线mac认证的时候，不仅把mac在线用户删掉了（正常），而且把以mac地址为用户名和密码的radius用户也删掉了（异常）。所以终端再次mac认证时就失败了，只能进入guest vlan依靠portal在线用户来上网了。这个解决办法需要第三方服务器保证在portal用户在线的情况下不能把mac认证用的radius用户给删掉，除非portal在线用户也消失了，它才可以删掉。

针对问题3：在portal的认证域下idle-cut 命令配置完之后，如果有在线用户那么是不会生效的，只能把所有在线用户都cut掉，才会生效。

针对问题1：配置mac-authentication trigger after-portal命令，当客户端通过portal认证后，就会触发客户端重关联。只要客户端重关联就会通过mac认证并且重新获取地址。

针对问题2：在mac认证域下不要配置idle-cut，需要第三方服务器查原因，为什么portal有在线用户，却把mac认证用的radius用户删掉了。

针对问题3：当在portal的认证域下配置完idle-cut时，需要cut conn all来把所用的用户删掉，idle-cut才会生效

配置guest vlan+portal认证+mac认证时建议加上命令：mac-authentication trigger after-portal
mac认证域不需要配置idle-cut，在portal认证域下配置完idle-cut后，需要用cut conn all命令把所有用户踢下线才会生效

第三方服务器需要支持portal在线用户的mac认证。