iNode 防破解配合禁用多网卡实现禁止WiFi共享的配置案例

Portal iNode **马光彬** 2014-03-19 发表

iNode防破解特性配合禁用多网卡功能实现禁止WiFi共享的配置案例

一、组网需求

一般情况下，终端用户必须通过身份认证/安全认证，才能正常访问网络。但是在学校很大一部分都是学生在使用网络，由于绝大部分学校对学生使用网络是需要收费的，学生为了节省这一部分费用，经常会使用代理软件等，只要有一个帐号通过UAM认证，其他人就可以使用网络，为了阻止此类非法用户使用网络，iMC UAM提供了客户端防破解方案，通过iNode、iMC UAM、H3C的设备相互配合阻止非法的客户端接入网络。在此方案中，需要在UAM中配置客户端管理中心。

二、组网图

无。

三、配置步骤

1、iMC侧配置

1．1 选择“用户”页签，单击左侧导航树中的接入策略管理>>业务参数配置>>系统配置>>业务参数配置菜单项，进入业务参数配置页面，启用“客户端防破解”

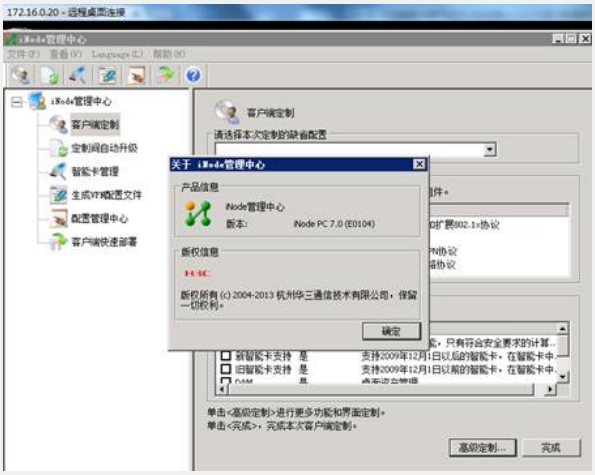
· 客户端防破解：该参数启用后，用户使用配置了“仅限iNode客户端”的服务进行认证时，用户只能使用iNode PC客户端认证接入，使用其他客户端将认证失败或不能正常在线。进行客户端防破解时，需要在 “用户>>接入策略管理>>业务参数配置>>系统配置>>客户端防破解配置”增加客户端管理中心并生效。该功能仅限与HP A series或H3C设备配合。

如果是portal认证方式，需要同时进入用户>>接入策略管理>>Portal服务管理>>设备配置>>端口组信息配置页面，portal端口组下开启“客户端防破解”。

1.2 接入策略选择“仅限iNode客户端”、“禁用多网卡”，同时根据需要选择“禁止开设代理服务器”，“禁止IE设置代理”等功能。违规处理模式根据需要选择下线或监控。

1.3 配置iNode管理中心

（1） 在一台独立的服务器（或者PC，不建议直接在UAM服务器上）安装iNode管理中心，IP地址172.16.0.20，需要与UAM服务器（172.16.0.22）正常通信。



（2） 选择“用户”页签，单击左侧导航树中的接入策略管理>>业务参数配置>>系统配置菜单项，进入系统配置页面。

（3） 点击“客户端防破解配置”对应的配置链接，进入客户端防破解配置页面。

（4） 单击<增加>按钮，进入客户端管理中心增加页面，填写iNode管理中心IP地址和备注，单击<确定>按钮保存设置。

（5） 此时状态是未生效，需要点击生效。

（6） 点击客户端管理中心IP列表中的“生效”图标，生效成功后客户端管理中心的状态更新为“已生效”。在使用防破解功能前，应确保对应客户端管理中心为“已生效”状态。

2、接入设备配置

正确配置radius方案后，要实现防破解功能，接入设备的认证方案对应的服务类型必须为eatended，如果是802.1x认证，则必须开启握手报文的安全扩展功能。下面（2）和（3）仅仅是针对802.1x认证进行的配置。

(1) 接入设备上配置认证方案（Radius Scheme）对应的服务类型必须为extended

system-view

[Sysname] radius scheme test

[Sysname-radius-test] server-type extended

(2) 在正确配置了802.1x认证的情况下，开启握手报文的安全扩展功能

假设用户连接设备的Ethernet1/0/5，则需要在以太网端口视图下配置如下命令。

system-view

[Sysname] interface Ethernet 1/0/5

[Sysname-Ethernet1/0/5] dot1x handshake secure

如果要关闭防破解功能，只需在以太网端口视图下执行如下命令。

[Sysname-Ethernet1/0/5] undo dot1x handshake secure

(3) 在正确配置了802.1x认证的情况下，部分设备需要在全局配置视图启用握手（如果设备支持该命令请启用，如果设备不支持不需要配置该命令），执行如下命令。

[Sysname] dot1x handshake enable

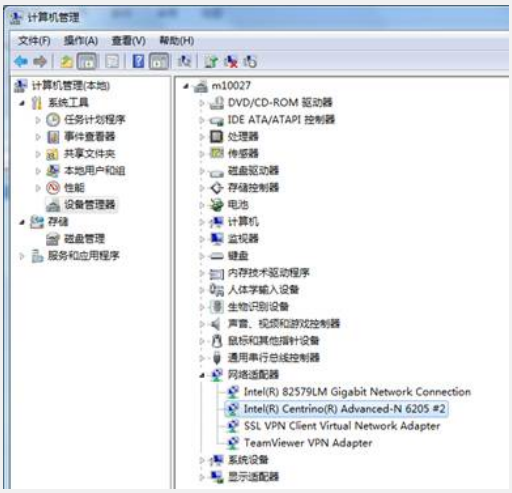
如果要关闭防破解功能，只需在全局视图执行如下命令。

[Sysname] undo dot1x handshake enable

四、测试结果：

1、使用未经破解的客户端测试

（1）查看计算机管理>>设备管理器>>网络适配器，除认证网卡Intel(R) Centrino(R) Advanced-N 6205 #2之外还有3个网卡。

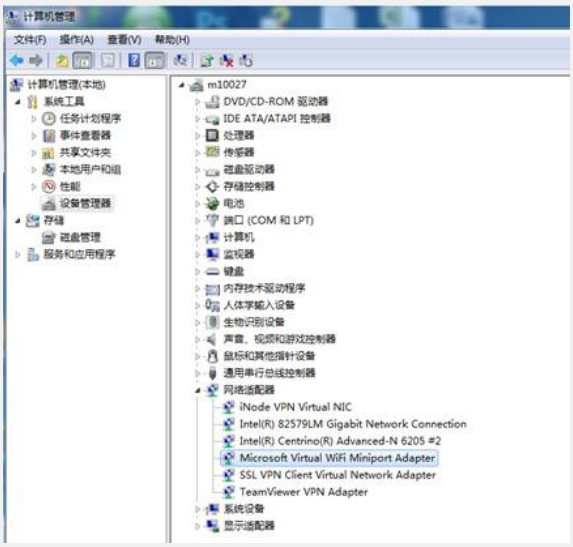


（2）为避免影响多网卡检测，定制iNode客户端时，将这三个网卡忽略。

（3）新建portal连接，认证成功上线

（4）启动WIFI共享精灵，设置热点名称和热点密码。

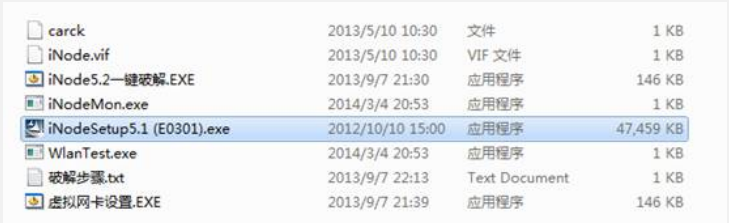
（5）查看计算机管理>>设备管理器>>网络适配器，多出一个虚拟网卡：Microsoft Virtual WiFi Miniport Adapter。



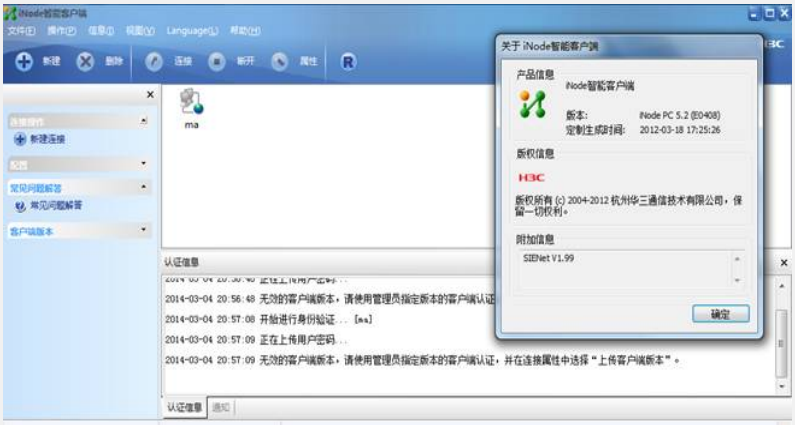
（6）经过十几秒，提示禁用多网卡检测不通过，强制下线。此时，禁用多网卡成功。

2、使用破解后的客户端测试

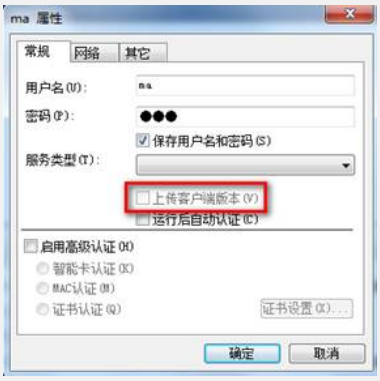
（1）本案例使用的破解客户端是平顶山学院提供的iNode5.2一键破解版，iNode 5.1 E0301破解后版本变成了iNode PC 5.2 E0408。



（2）破解客户端认证时，提示：无效的客户端版本，请使用管理员指定版本的客户端认证，并在连接属性中选择“上传客户端版本”。



（3）查看连接属性，“上传客户端版本”是灰选的。此时，客户端防破解成功。



五、注意事项

（1）防破解功能需要iMC、接入设备和iNode客户端三方配合实现，有一方不支持防破解功能，就不能实现防破解。因此请注意iMC、接入设备和iNode客户端的防破解版本。具体支持防破解特性的设备请向设备侧确认。

（2）多网卡检测功能的实现需要iMC、设备和客户端三方面同时配合，有一方不支持多网卡检测功能，就不能实现多网卡检测功能。

（3）iNode管理中心版本要与iNode客户端版本一致。