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。

系统参数配置				
老们封阔纲基(分钟)。	30	0	认证规定时长(砂)*	8 (T
施入时控预算天教(天)*	3	Ø	最大会词时代(秒)*	85400
流量统计单位(字节)。	1	1	剩余流量单位(字节)。	1
霍户阔防被解	麻用	• @	晋户诸最低版本 *	5 20-0408
双机分量	MA	• 💿	NAS控制编口号。	1812
用户认证防攻击	间用	• @	用户名前编码执方式	/E411 - @

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"。

第 用户> 推入策略管理	> Portai服务管理	> 设备配置 > 诫口相信息配置	> 俗改讓口組信息	
Participation of the second second				

始改滿口組信題			
補口組名*	192.168.10.1	提示语言 *	构造检测 -
开始端口"	0	终止端口"	222222
协议类型"	HTTP ~	快速认证*	<b>否</b> •
是否NAT。	四	错误遗语。	是 -
认证方式。	PAPikie -	炉地址组"	192.168.10.1 +
心跳间隔(分钟)*	10	心跳起时(分钟)*	30
用户线名		满口语描述	
无感知认证	不支持 -	客户;制防破船。	是 •
用户属性类型	-	耕省认证页面	PC - index_guest): +

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。

用户 > 推入解略管理 > 接入解略管理 > 经沿行	() MHE		(Dh
Mill Windowsbill Shig Pilg	□ 献用LinuxMacOS初志解音户属 自动垂连网络小钟)30 ・	MLGH02P8U 80%3/h3	
法最处理模式 ④下线 〇曲拉 -			
☑ 算止开设代理账券書 ☑ 算止认证码卡载置多产地址 □ 基用VIIWare USB服务	■ 基止运行器代理 ● 基止运行器化理 ■ 基止在虚拟机中运行	家社出版相容的MAC地址	□禁用多操作系统 □禁用vMWare NAT服务
中地址获取方式	④不禁制 〇 必须种志设置 〇 必须动态研究		

### 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月17) 至台(V) Larpage(L) 新 18日 - 19日 - 190	10 00 10 00	
<ul> <li>iSode管理中心</li> <li>資产/施定制</li> <li>空制间自动升级</li> <li>新約4管理</li> </ul>	<ul> <li>第戶施設制</li> <li>通送择本次定制的缺省配置</li> <li>关于 istede管理中心</li> </ul>	3
<ul> <li></li></ul>	产品値型 その地帯理中心 数本: Node PC 7.0 (E0104) 新校道理 14 40C 新校振興 (1) 2004-2013 杭州体三連信技术有限公司・保留	件。 Of 1数002.1-协议 和协议 品协议
	- (初代約)。 - (初代約) - (初代約)。 - (初代約) - (初代約)。 - (初代約) - (初代約)	
	单击<高级定制>进行更多功版和界面定制。 单击<完成>,完成本次容户域定制。	<u>高級定制</u> 完成

(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。

ineral E				
模板名称		Rif		NZ
系统创制政策		系统提供业务相关的案例影台信息		0.0
策略服务器长数配置		<b>碱脂除务器及安全管理相关的世数信息</b>		00
终端管理世界政策		终端管理的很关键置		00
UAIN运行日志参救配置		歐國系統运行环境相关參救		00
用户密码控制策略截置		配置用户密码的控制演奏		00
受迫权思		兼發业务的线等相关信息		00
8号自动销户权置		系统模糊各个参数的设置情况,为务号进行自由	加中地理・	0.0
PEAP认证地控制图		截置PEAP认证相应相关参数		00
王统定位参考政置		配置无规定位的相关参数		00
用户上下线通知参数数置		用户上下统通知相关的参数信息		00
E PHRINIERA2		配置専門論管理中心		0.
代理服务器检测部数		INOSH客户编绘则主机是否自用代理服务器的参	atr.	00
(3) 点击"	客户端防破解配	置"对应的配置链接,进	入客户端防破解香	记置页面。
SI 用户 > 抱入漏暗管理 > 业/	的复数配置。 系统配置 > 有户间的	就解放置		
A210 \$198				
19焼酎 0	会注。	<b>i</b> ta ≎	生效	50 I
# MERITIA # PHANCE # .				

(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。



(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

fizta Aliak				
PREMIO	会通り	Na o	1.9	82.
172 16 0 20		已生效	<u>e</u> ,	8 1

# 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eatend ed,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。

 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) Adva nced-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



<sup>(4)</sup> 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。

(Nodel)(15:19) 文(F)(1) 昭和(1) 昭和(1) F(王)(2) Languaget(2) 解取(1)					
🕀 888 🛞 889	C	ER 🔿 HE 🗞 NS 🚺 R A			
<ul> <li>○ (1995年1月1日)</li> <li>● (1995年1月1日)</li> <li>● (1995年1日)</li> <li>○ (1995年1日)</li> <li>○ (1995年1日)</li> <li>○ (1995年1日)</li> <li>○ (1995年1日)</li> </ul>	× •	受到 受到 预约Portal语 ma 接			
5/48/#		以注電息     2014-03-04 20:35:18 2019(10):25:18 2019(10):25:18 2019(10):25:18 2019(10):25:18 2019(10):25:20 不要求进行安全检查     2014-03-04 20:35:23 禁用身份科检测不通过,将强制用户下续。     2014-03-04 20:36:33 用户包下线。			

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。

Carck	2013/5/10 10:30	文件	1 KB
iNode.vif	2013/5/10 10:30	VIF 文件	1 KB
速 iNode5.2—键破解.EXE	2013/9/7 21:30	应用程序	146 KB
🗾 iNodeMon.exe	2014/3/4 20:53	应用程序	1 KB
iNodeSetup5.1 (E0301).exe	2012/10/10 15:00	应用程序	47,459 KB
📰 WlanTest.exe	2014/3/4 20:53	应用程序	1 KB
破解步骤.txt	2013/9/7 22:13	Text Document	1 KB
● 虚拟网卡设置.EXE	2013/9/7 21:39	应用程序	146 KB

(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。