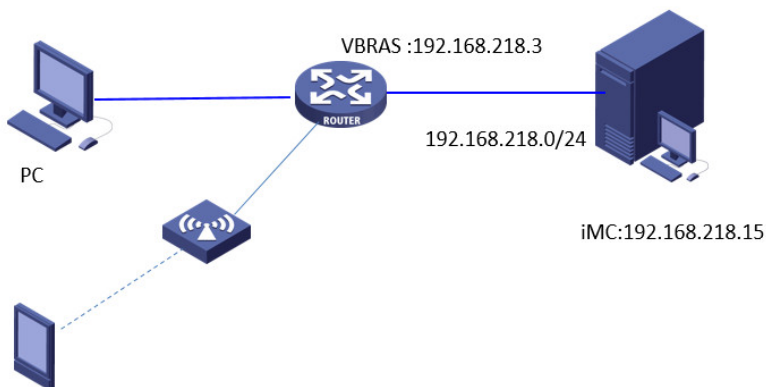


知 iMC EIA V7版本实现portal认证PC和手机终端同时只有一个在线的典型配置案例

李树兵 2017-09-18 发表

Portal认证作为一个简单快捷的认证方式，越来越多的公司采用。本文档介绍Portal认证实现手机和PC终端同时只有一个在线的配置举例。本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。本文档假设您已了解AAA、Portal认证。



认证PC的地址为192.168.200.2，网关为192.168.200.1，手机的地址为192.168.200.2，网关为192.168.200.1，位于路由器上，路由器另外一个接口地址为192.168.218.3，和iMC互联，iMC的地址为192.168.218.1，作为portal服务器和RADIUS服务器。

iMC EIA版本信息：7.1 E0302P18

VBRAS版本信息：7.1 E0321

一.设备配置：

interface GigabitEthernet1/0 //配置连接外网的接口，用于NAT转换出去

port link-mode route

description nat-shangwang-vnet8

ip address 192.168.226.4 255.255.255.0

nat outbound

#

interface GigabitEthernet2/0 //配置连接认证客户端的接口地址

port link-mode route

description qiaojie-youxian-wangka-vnet2

ip address 192.168.200.1 255.255.255.0

portal enable method direct //接口下发portal服务

portal domain imc //制定接口下portal认证的domain域为imc

portal apply web-server imc //接口应用portal服务，服务的名字为imc

#

interface GigabitEthernet3/0 //配置连接iMC的接口地址

port link-mode route

description zhuji-pc-vnet1

ip address 192.168.218.3 255.255.255.0

snmp-agent //配置SNMP参数，用于iMC网管

snmp-agent local-engineid 800063A280000C29B1FDD600000001

snmp-agent community write private

snmp-agent community read public

snmp-agent sys-info version all

trap address udp-domain 192.168.218.1 params securityname public v2c

snmp-agent trap enable arp

snmp-agent trap enable radius

radius session-control enable //使能RADIUS session control功能，这个命令比较重要。iMC使用session control报文向设备发送授权信息的动态修改请求以及断开连接请求。使能RADIUS session control功能后，设备会打开知名UDP端口1812来监听并接收RADIUS服务器发送的session control报文。

需要注意的是，该功能仅能和H3C iMC的RADIUS服务器配合使用。开启之后iMC发送的强制下线报文设备才会处理。

#

radius scheme imc //配置 radius scheme imc

primary authentication 192.168.218.1 //指定认证的服务器地址为192.168.218.1

primary accounting 192.168.218.1 //指定计费的服务器地址为192.168.218.1

accounting-on enable //打开计费功能。在accounting-on功能处于使能的情况下，若集中式设备或分布式设备上的单板重启，则设备或单板会在重启之后发送accounting-on报文通知该方案所使用的RADIUS计费服务器，要求RADIUS服务器停止计费且强制该设备的用户下线。

accounting-on extended //accounting-on扩展功能是分布式设备对accounting-on功能的增强。在分布式架构下，用户接入到设备的业务板上，当用户所在业务板重启而整机没有重启时，设备会通过accounting-on报文通知RADIUS服务器，让对应单板的用户停止计费。本扩展功能仅适用于PPP、IPoE和lan-access用户。本扩展功能不适用于Portal用户，因为所有的Portal用户数据都保存在主控板，只需要开启普通accounting-on功能即可。

key authentication cipher \$c\$3\$HxkbNWxQgnU/haGwIFivTmu4ZVkl6g== //配置认证的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。

key accounting cipher \$c\$3\$mO0sPfgT7zSvJI0UqqJerV40K39OyA== //配置计费的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。这两个密钥要保持一致，因为iMC侧只能配置一个密钥，所以认证和计费密钥要一致。

user-name-format without-domain //配置认证用户不带domain域，对应iMC侧接入服务不能添加服务后缀

#

domain imc //配置domain域imc

authorization-attribute idle-cut 10 10240000 //类似于V5设备上的idle-cut，用于在设备上检测用户是否在线。指定ISP域imc下的用户闲置切断时间为10分钟，闲置切断时间内产生的流量为10240000字节。

authentication portal radius-scheme imc //设置用户认证的radius方案为imc

authorization portal radius-scheme imc //设置用户授权的radius方案为imc

accounting portal radius-scheme imc //设置用户计费的radius方案为imc

#

portal free-rule 1 destination ip 192.168.200.1 255.255.255.255

portal free-rule 2 destination 221.130.33.52 //放通目的地址为DNS，用于用户访问域名的时候进行DNS解析

portal free-rule 3 destination 221.130.33.60

#

portal web-server imc //配置Portal Web服务器的URL为http://192.168.218.1:8080/portal

url http://192.168.218.1:8080/portal

#

portal server imc //配置portal服务器imc

ip 192.168.218.1 key cipher \$c\$3\$vr9TyOUwjLrWZsZ+9qMb8e6WT7JHcA== //配置portal服务器的地址为192.168.218.1，以及认证的密钥key，此处的key为h3c，此处的配置要和iMC侧portal服务管理里面的设备配置的key一致。

#

二.iMC配置：

第一步：将设备加入到iMC网管



资源 > 增加设备

设备基本信息

主机名或IP地址 * 192.168.218.3

设备标签

掩码

设备分组

登录方式 Telnet

☒ 将设备的Trap发送到本网管系统

☒ 设备支持Ping操作

☐ Ping不通也加入

☐ 将LoopBack地址作为管理IP

配置SNMP参数

设置

参数类型 SNMPv2c

只读团体字

读写团体字

资源 > 设备视图 > 视图-路由器

增加设备

SNMP模板

系统参数

帮助

生成图表

删除

管理

取消管理

同步

刷新

更多

视图

搜索设备IP、标签、状态

☐ 状态	设备标签	型号	IP地址	类型	操作
☐ 警告	H3C(192.168.218.3)	H3C VBRAS1000P	192.168.218.3	路由器	...

共有1条记录, 当前第1 - 1, 第 1/1 页。

<

<

1

>

>

50

数据获取时间: 2016-07-16 08:24:14

第二步: 增加接入设备

Intelligent Management Center

默认视图 admin 桌面版 帮助 关于

首页 资源 用户 业务 告警 报表 系统管理

添加设备 SNMP模板 系统参数

搜索设备IP、标签、状态

取消管理 同步 刷新 更多 视图

型号	IP地址	类型	操作
3.3) H3C VBRAS1000P	192.168.218.3	路由器	...

共有1条记录, 当前第1 - 1, 第 1/1 页。

数据获取时间: 2016-07-16 08:24:14

快速入门

接入设备管理

接入策略管理

接入设备配置

接入设备类型配置

私有属性下发策略配置

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置

加入收藏 帮助

高级查询

设备IP地址 从 至

设备名称 接入设备类型

查询 重置

增加 删除 修改 下发配置 同步端口配置 与平台设备同步 批量导入 刷新

AAA下发结果 命令下发结果

设备名称	设备IP地址	设备型号	下发配置类型	备注	下发结果	端口配置同步结果	详细信息	操作
☐ H3C	192.168.218.3	H3C VBRAS1000P	H3C有线		未下发	未同步	...	...

共有1条记录, 当前第1 - 1, 第 1/1 页。

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 修改接入设备

帮助

接入配置

认证接口 * 1812

计费接口 * 1813

组网方式 不启用混合组网

业务类型 LAN接入业务

接入设备类型 H3C(General)

接入设备分组 无

共享密钥 * ...

确认共享密钥 * ...

设备列表

设备名称	设备IP地址	设备型号	备注
H3C	192.168.218.3	H3C VBRAS1000P	

共有1条记录。

确定 取消

置共享密钥，保证和设备里面radius scheme 配置的密钥一致，增加设备，保证设备的IP地址和设备上的nas-ip地址一致。设备上如果没有指定nas-ip，设备默认是以离iMC最近的IP地址来发送radius报文，本案例中设备是以192.168.218.3来发送的。

第三步：在portal服务管理中增加portal设备

用户 > 接入策略管理 > Portal服务管理 > 设备配置

设备信息查询

设备名 版本

下发结果 业务分组

增加

设备名	版本	业务分组	IP地址	最近一次下发时间	下发结果	操作
vbras	Portal 2.0	未分组	192.168.200.1		未下发	

共有1条记录，当前第1 - 1，第 1/1 页。

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 * 业务分组 *

版本 * IP地址 *

监听端口 * 本地Challenge *

认证重发次数 * 下线重发次数 *

支持逃生心跳 * 支持用户心跳 *

密钥 * 确认密钥 *

组网方式 *

设备描述

确定 **取消**

第四步：增加portal认证的IP地址组

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置

IP地址组查询

IP地址组名 业务分组

IP地址 转换后IP地址

增加

IP地址组名	业务分组	起始地址	终止地址	类型	转换后起始地址	转换后终止地址	起始IPv6地址	终止IPv6地址	修改	删除
200	未分组	192.168.200.1	192.168.200.254	普通						

共有1条记录，当前第1 - 1，第 1/1 页。

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 修改IP地址组

修改IP地址组

IP地址组名 *

起始地址 *

终止地址 *

业务分组

类型 *

确定 **取消**

第五步：配置端口组信息管理

设备信息查询

设备名 版本

下发结果 业务分组

设备名	版本	业务分组	IP地址	最近一次下发时间	下发结果	操作
vbras	Portal 2.0	未分组	192.168.200.1		未下发	编辑 删除

共有1条记录, 当前第1 - 1, 第 1/1 页。

50

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置

端口组信息查询

端口组名

开始端口 >= 终止端口 <=

协议类型 是否NAT

端口组名	开始端口	终止端口	协议类型	是否NAT	详细信息	修改	删除
bras	0	zzzzzz	HTTP	否	编辑	编辑	删除

共有1条记录, 当前第1 - 1, 第 1/1 页。

50

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 修改端口组信息

修改端口组信息

端口组名 *

开始端口 *

协议类型 *

是否NAT *

认证方式 *

心跳间隔(分钟) *

用户域名

无感知认证

页面推送策略

提示语言 *

终止端口 *

快速认证 *

错误透传 *

IP地址组 *

心跳超时(分钟) *

端口组描述

客户端防破解 *

缺省认证页面

第六步：增加接入策略，需要增加两个接入策略，一个是针对PC的，一个是针对手机的。

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 接入策略管理

接入策略查询

接入策略名 业务分组

接入策略名	描述	业务分组	修改	删除
mac绑定		未分组	编辑	删除
PC		未分组	编辑	删除
PHONE		未分组	编辑	删除
policy		未分组	编辑	删除
portal		未分组	编辑	删除
test		未分组	编辑	删除
testAndP.1X	test	未分组	编辑	删除

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 * PC-test

业务分组 * 未分组

描述

授权信息

接入时段 无 分配IP地址 * 否

下行速率(Kbps)

上行速率(Kbps)

优先级

启用RSA认证

证书认证 ☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型 EAP-TLS认证

下发VLAN

下发User Profile

下发用户组

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 * Phone-test

业务分组 * 未分组

描述

授权信息

接入时段 无 分配IP地址 * 否

下行速率(Kbps)

上行速率(Kbps)

优先级

启用RSA认证

证书认证 ☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型 EAP-TLS认证

下发VLAN

第七步：配置接入条件，在终端类型分组里面配置PC和PHONE的分组。

用户 > 接入策略管理 > 接入条件管理 > 终端类型分组 > 修改终端类型分组

修改终端类型分组

基本信息

终端类型分组名 * PC

描述

业务分组 * 未分组

终端类型列表

共有1,130条记录。

全部展开 全部收缩

终端类型	显示名称
Access Point	

终端类型	显示名称
☐	Access Point
☐	Compad Pad
☐	Game Console
☐	IP conference
☐	IP Phone
☐	iPod
☐	NAS
☒	PC
☐	Printer
☐	Projector
☐	Residential Gateway
☐	Router
☐	Set Top Box
☐	Smartphone
	手机

1341 1.0 版权所有 © 2007-2015 杭州华三通信技术有限公司，保留一切权利。

终端类型分组名 *PHONE

描述

业务分组 *未分组

终端类型列表

共有1,130条记录。

全部展开全部收缩

	终端类型	显示名称
☐	Access Point	
☐	Compad Pad	
☐	Game Console	
☐	IP conference	
☒	IP Phone	
☐	Router	
☐	Set Top Box	
☒	Smartphone	手机
☐	Switch	
☒	Tablet	平板电脑
☐	TV	
☐	VoIP Adapter	
☐	WiFi Phone	
☐	Wireless	
☐	Wireless Controller	
☐	Wireless Router	

确定取消

第七步：增加接入服务，在里面增加接入场景，设置PC和Phone终端同时在线只有一个，同时绑定对应的接入策略，其他终端类型禁止接入的话，建议缺省接入策略选择禁止接入。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 *test

业务分组 *未分组

缺省安全策略 *不使用

缺省私有属性下发策略 *不使用

服务描述

☒ 可申请

Portal无感知认证

服务后缀

缺省接入策略 *禁止接入

缺省内网外连策略 *不使用

缺省单帐号最大绑定终端数 *0

缺省单帐号在线数量限制 *0

接入场景列表

增加

名称	接入策略	安全策略	私有属性下发策略	内网外连策略	优先级	修改	删除
未找到符合条件的记录。							

确定取消

1341 1.0 版权所有 © 2007-2015 杭州华三通信技术有限公司，保留一切权利。

增加接入场景 - Google Chrome

10.88.8.48:2123/imc/acm/acmservice/choose.jsf

终端MAC地址分组 *	不限
终端厂商分组 *	不限
终端操作系统分组 *	不限
终端类型分组 *	PC
AP分组 *	不限
接入时段策略 *	不限

接入策略

接入策略 *	PC-test
安全策略 *	不使用
私有属性下发策略 *	不使用
内网外连策略 *	不使用
单帐号最大绑定终端数 *	1
单帐号在线数量限制 *	1

确定 取消

增加接入场景 - Google Chrome

10.88.8.48:2123/imc/acm/acmservice/choose.jsf

终端MAC地址分组 *	不限
终端厂商分组 *	不限
终端操作系统分组 *	不限
终端类型分组 *	PHONE
AP分组 *	不限
接入时段策略 *	不限

接入策略

接入策略 *	Phone-test
安全策略 *	不使用
私有属性下发策略 *	不使用
内网外连策略 *	不使用
单帐号最大绑定终端数 *	1
单帐号在线数量限制 *	1

确定 取消

第八步：增加本地接入用户，绑定名为test的接入服务。

用户 > 增加用户

增加用户

基本信息

用户姓名 * 123 证件号码 * 12345678901234567890 检查是否可用

通讯地址 电话

电子邮件 用户分组 * 未分组

☐ 开通自动帐户

确定 取消

用户 > 增加用户

增加用户

基本信息

用户姓名 * 123 证件号码 * 12345678901234567890 检查是否可用

通讯地址 电话

电子邮件 用户分组 * 未分组

☐ 开通自动帐户

确定 取消

用户 > 增加用户

增加用户

基本信息

用户姓名 * 123 证件号码 * 12345678901234567890 检查是否可用

通讯地址 电话

电子邮件 用户分组 * 未分组

☐ 开通自动帐户

确定 取消

用户 > 业务 > 帐号 > 配置 > 系统配置 > 系统参数配置

用户名 * test

☐ 预开用户 ☐ 缺省BYOD用户 ☐ MAC地址认证用户 ☐ 主机名用户 ☐ 快速认证

密码 * **** 密码确认 * ****

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

生效时间 失效时间

最大闲置时长(分钟) 在线数量限制 2

Portal无感知认证最大绑定数 1

登录提示信息

接入服务

服务名	服务后援	缺省安全策略	状态	分配IP地址
☐ MAC绑定		不使用	可申请	
☐ portal	portal-wx	不使用	可申请	
☐ service		不使用	可申请	
☒ test		不使用	可申请	

第八步：设置启用同名帐号强制下线，这样后面上线的用户就可以把前面的用户踢下线。

用户 > 业务 > 帐号 > 配置 > 系统配置 > 系统参数配置

认证、授权、计费(AAA)参数

老化时间(小时/分钟) * 30 认证超时时长(秒) * 5

接入时认证预置天数(天) * 3 最大会话时长(秒) * 86400

流量统计单位(字节) * 1 剩余流量单位(字节) * 1

客户端防破解 禁用 认证失败阈值(次) * 10

双机冷备 禁用 NAS控制端口号 * 1812

用户认证防攻击 启用 用户名前缀转换方式 后缀

接入网络零点切换 禁用 检查证书中的用户名 是

同名帐号强制下线 允许

无效客户端自动加入黑名单 禁用

客户端保护密码 确认密码

自学习MAC地址最大个数 * 1 用户认证仿真模式 禁用

至此配置完成。

注意:

识别终端系统需要使用EIP的授权, 请确保一定购买了EIP授权并且授权数量足够。