

知 iMC V7实现不同终端弹不同portal页面并下发不同的策略案例

Portal 李树兵 2015-06-08 发表

Portal网页认证方式简单，无需客户端，且适用于各种终端如PC、手机、pad等。很多客户的需求是需要根据不同的终端类型推送不同的portal认证界面并下发不同的权限策略，实现灵活控制。

PC (iPhone) ---ap (wireless) ---MSR920-----ap (wireless) -----iMC

一. 设备配置:

```
portal server portal21 ip 192.168.15.6 key cipher $c$3$CLWGrRPHS7r5ZEF4y7gKaR/MNK9smg==
url http://192.168.15.6:8080/portal server-type imc //配置portal server , 密码h3c
portal free-rule 1 source ip any destination ip 8.8.8.8 mask 255.255.255.255 //放通到dns地址
portal free-rule 2 source ip any destination ip 114.64.255.148 mask 255.255.255.255
portal free-rule 3 source ip any destination ip 114.64.255.0 mask 255.255.255.0
portal free-rule 4 source ip any destination ip 192.169.199.1 mask 255.255.255.255
portal free-rule 5 source ip any destination ip 192.168.20.1 mask 255.255.255.255
#
domain default enable portal21
acl number 3000 //用于下发不同的策略的acl
rule 0 deny ip destination 111.1.1.1 0
rule 5 permit ip
acl number 3001 //用于下发不同的策略的acl
rule 0 deny ip destination 111.1.1.2 0
rule 5 permit ip
#
vlan 15
#
vlan 20 to 22
radius scheme portal21
primary authentication 192.168.15.6 key cipher $c$3$i+VDTbQz76KaYNVGCLgjxeW5hzuU/A== //
密钥h3c
primary accounting 192.168.15.6 key cipher $c$3$ESLodi1ding/kohgcCABb+W78ehsrg==
user-name-format without-domain
nas-ip 192.168.15.1
#

domain portal21
authentication portal radius-scheme portal21
authorization portal radius-scheme portal21
accounting portal radius-scheme portal21
access-limit disable
state active
idle-cut disable
self-service-url disable
interface LoopBack1 //用于测试策略的地址
ip address 111.1.1.1 255.255.255.255
#
interface LoopBack2 //用于测试策略的地址
ip address 111.1.1.2 255.255.255.255
interface Vlan-interface15 //链接iMC的接口
description ssid-imc-portal-test
ip address 192.168.15.1 255.255.255.0
#
interface Vlan-interface20 //连接认证客户端的接口
description ssid-6234
ip address 192.168.20.1 255.255.255.0
portal server portal21 method direct
snmp-agent //配置SNMP参数
snmp-agent local-engineid 800063A203B8AF67F778FC
snmp-agent community read public
```

snmp-agent community write private
snmp-agent sys-info location Location:shenzhen
snmp-agent sys-info version all

二.iMC配置

1. 配置接入设备

资源 用户 业务 告警 报表 系统管理

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

接入配置

认证端口 * 1812 计费端口 * 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

与设备侧radius上配置的密钥一致，
本案例采用h3c

设备名称	设备IP地址	设备型号	备注
cy15	192.168.15.1	H3C MSR2020	
共有1条记录。			

此ip地址需要与radius的nas-ip一致，默认是接入设备上靠近iMC侧的地址

确定 取消

2.配置portal的ip地址组

资源 用户 业务 告警 报表 系统管理

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 * portal20

起始地址 * 192.168.20.1

终止地址 * 192.168.20.254

业务分组 未分组

类型 * 普通

确定 取消

3. 配置portal设备

Management Center

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 修改设备信息

修改设备信息

设备信息

设备名 * MSR 业务分

版本 * Portal 2.0 IP地址 * 192.168.20.1

监听端口 * 2000 本地Challenge * 否

认证重发次数 * 0 下线重发次数 * 1

支持逃生心跳 * 否 支持用户心跳 * 否

密码 * ... 确认密码 * ...

组网方式 * 固定

设备描述 与设备上portal server配置的ip地址一致，本案例采用h3c

确定 取消

4. 定制页面

选择一个模板，点击增加

Management Center

admin 桌面版 帮助 关于 注销

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 终端页面定制 > Portal页面定制

加入收藏 帮助

刷新

提示：定制页面使用的浏览器及版本应为：IE10/IE11、Firefox 30 及以上版本、Chrome 35 及以上版本。否则可能会影响页面的定制、预览和使用。

PC Phone

模板1 + 增加 模板2 + 增加 模板3 + 增加 模板4 + 增加 模板5 + 增加 空白 + 增加

自定义 + 增加

查看	定制名称	模板名称	业务分组	认证类型	预览	复制	修改	删除
▶	缺省Web认证 (PC)	预定义	未分组	普通认证				
▶	缺省Web认证 (PAD)	预定义	未分组	普通认证				

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 终端页面定制 > Portal页面定制 > 增加Portal定制页面

基本信息

定制名称 * 6235pc

业务分组 * 未分组

认证类型 * 普通认证

描述

确定 取消

自定义+增加

查看	定制名称	模板名称	业务分组	认证类型	绘制	预览	复制	修改	删除
	缺省Web认证 (PC)	预定义	未分组	普通认证					
	缺省Web认证 (PAD)	预定义	未分组	普通认证					
	第三方认证	预定义	未分组	普通认证					
	另类缺省Web认证 (PC)	预定义	未分组	普通认证					
	二维码开户与认证	预定义	未分组	普通认证					
	短信开户与认证 (PC)	预定义	未分组	短信认证					
	6234pc	模板2	未分组	普通认证					

192.168.15.6:8080/imc/acm/custompage/canvas/20150605214436446/popPcPortal.shtml?customPageId=100&customPort Q



imc PC 页面测试!!!!
6234!



个人

帐号名
帐号密码
服务类型
☐ 保存密码

上线 下线

增加区段
预览
保存
发布
设置
关闭

版权所有

Portal PC 定制 - Google Chrome

192.168.15.6:8080/imc/acm/custompage/canvas/20150605214436446/popPcPortal.shtml?customPageId=100&customPort Q

恭喜成功登陆PC页面!!!

上线成功
3秒后本页面将跳转至下述页面, 如果无法跳转请手动操作:
搜索请访问 www.baidu.com

下线

增加区段
预览
保存
发布
关闭



用户 > 接入策略管理 > 终端页面定制 > Portal页面定制 > 增加Portal定制页面

基本信息

定制名称 * 6234phone

业务分组 * 未分组

认证类型 * 普通认证

描述

确定 取消



5. 配置页面推送策略

用户 > 接入策略管理 > 页面推送策略 > 增加页面推送策略

增加页面推送策略

基本信息

策略名称 * 6234

业务分组 未分组

认证方式 Portal

描述

页面推送子策略列表

增加

子策略名称	认证页面	设备用户分组	设备管理提供	优先级	修改	删除
未找到符合条件的记录。						

确定 取消

配置两个子策略，分别如下

页面推送子策略列表						
新增						
共有2条记录。						
子策略名称	认证页面	访客用户分组	访客管理员	优先级	修改	删除
pc	PC - 6234pc			1		
phone	PHONE - 6234phone			2		
确定 取消						

Windows 7 的 http 报文中的 httpuser-agent 字段是 Windows NT 6.1

修改页面推送子策略 - Google Chrome

192.168.15.6:8080/imc/acm/pushPage/choose.jsf

修改页面推送子策略

子策略名称: pc

条件

SSID分组: 不限

AP分组: 不限

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: 不限

接入时段策略: 不限

HTTP User Agent特征: Windows NT 6.1

策略

认证页面: PC - 6234pc

访客用户分组:

访客管理员:

确定 取消

通过在IMC服务器上抓包iPhone 5发过来的IOS8.3系统的http报文 user-agent字段是CPU iPhone OS

192.168.15.6:8080/imc/acm/pushPage/choose.jsf

修改页面推送子策略

子策略名称: phone

条件

SSID分组: 不限

AP分组: 不限

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: 不限

接入时段策略: 不限

HTTP User Agent特征: CPU iPhone OS

策略

认证页面: PHONE - 6234phone

访客用户分组:

访客管理员:

确定 取消

6.端口组信息管理里面调用IP地址组和页面推送策略

The screenshot shows the 'Port Profile Configuration' window in Mikrotik WinBox. The 'Port Profile Name' is 'MISA'. The 'Protocol' is 'HTTP'. The 'Authentication' is 'CHAP'. The 'Port Profile' is 'port20'. The 'Port Profile Description' is 'MISA'. The 'Port Profile' is 'port20'. The 'Port Profile' is 'port20'.

不同终端推送不同的portal页面配置好了，接着配置不同终端下发不同的侧策略

7. 接入条件里面增加终端类型分组

控制类型分组在

PC

描述

业务分组 *

未分组

控制类型列表

共有1,159条记录。

查询

全部展开 全部收起	控制类型	显示名称
	Access Point	
	Compad Pad	
	Game Console	
	IP conference	
	IP Phone	
	iPod	
	NAS	
✓	PC	

8. 配

置接入策略，不同的策略调用不同的acl，实现不同的权限控制

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 *

PC

业务分组 *

未分组

描述

授权信息

接入时段

无

下行速率(Kbps)

优先级

证书认证

☒不启用 ☐EAP证书认证 ☐WAP证书认证

认证证书类型

EAP-TLS/CA证

下发VLAN

下发VLAN-SSID

分配IP地址 *

否

上行速率(Kbps)

☐启用RSA/CA证

☒下发ACL

手工输入

3000

☐列表选择

☐插入ACL列表

acl 3000已经在设备上配置好，禁止到111.1.1.1/32的访问

用户 证书 告警 报表 系统管理

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 *

业务分组 *

描述

授权信息

接入时段

下行速率(Kbps)

优先级

证书认证 ☒ 不使用 ☐ EAP证书认证 ☐ WPA2证书认证

认证证书类型

下发VLAN

分配IP地址 *

上行速率(Kbps)

☐ 启用RSA认证

☐ 下发User Profile

☒ 下发ACL

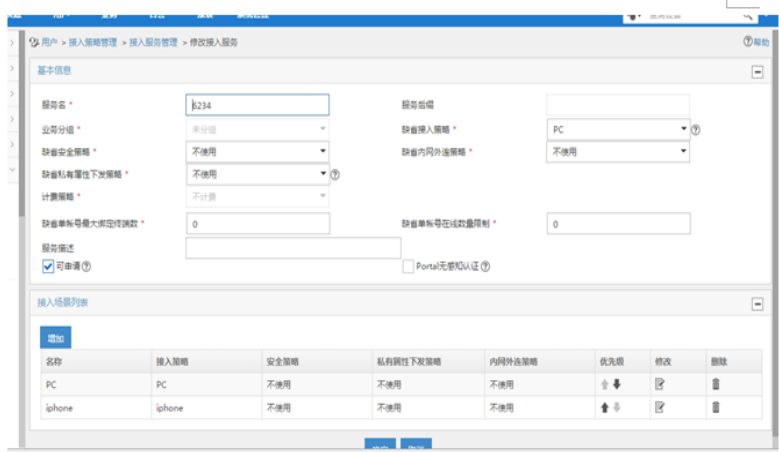
☒ 手工输入 ⑦

☐ 列表选择

接入ACL列表

acl 3001已经在设备上配置好，禁止到111.1.1.2/32的访问请求

9. 配置接入服务，不同的终端类型调用不同的接入策略



接入条件

接入设备分组 * 不限

终端IP地址分组 * 不限

SSID分组 * 不限

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

安全策略 * 不使用

私有属性下发策略 * 不使用

192.168.15.6:8080/imc/acm/acmservice/choose.jsf

终端IP地址分组 * 不限

SSID分组 * 不限

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 * iphone

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 * 0

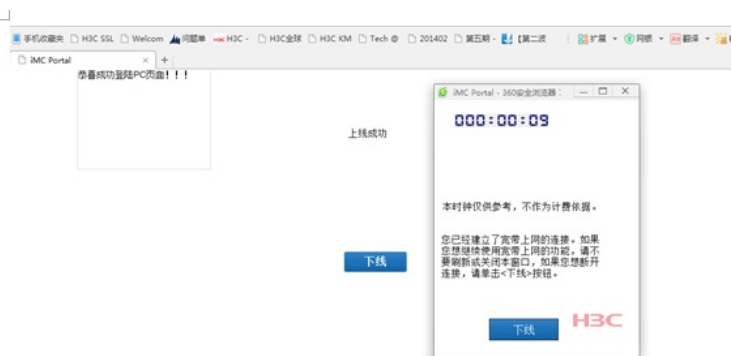
10. 配置接入用户绑定此接入服务

用户名	密码	有效期	状态	计费策略	分配IP地址
6234			可用	不计费	

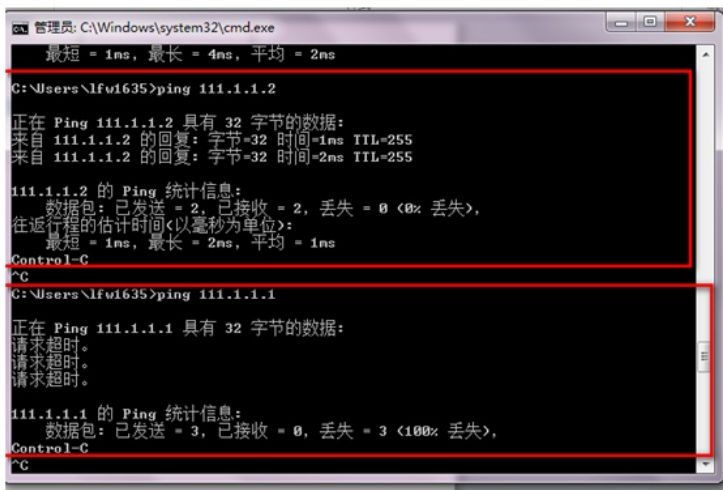
配置完成

三. 认证效果

PC端登陆:



认证通过之后



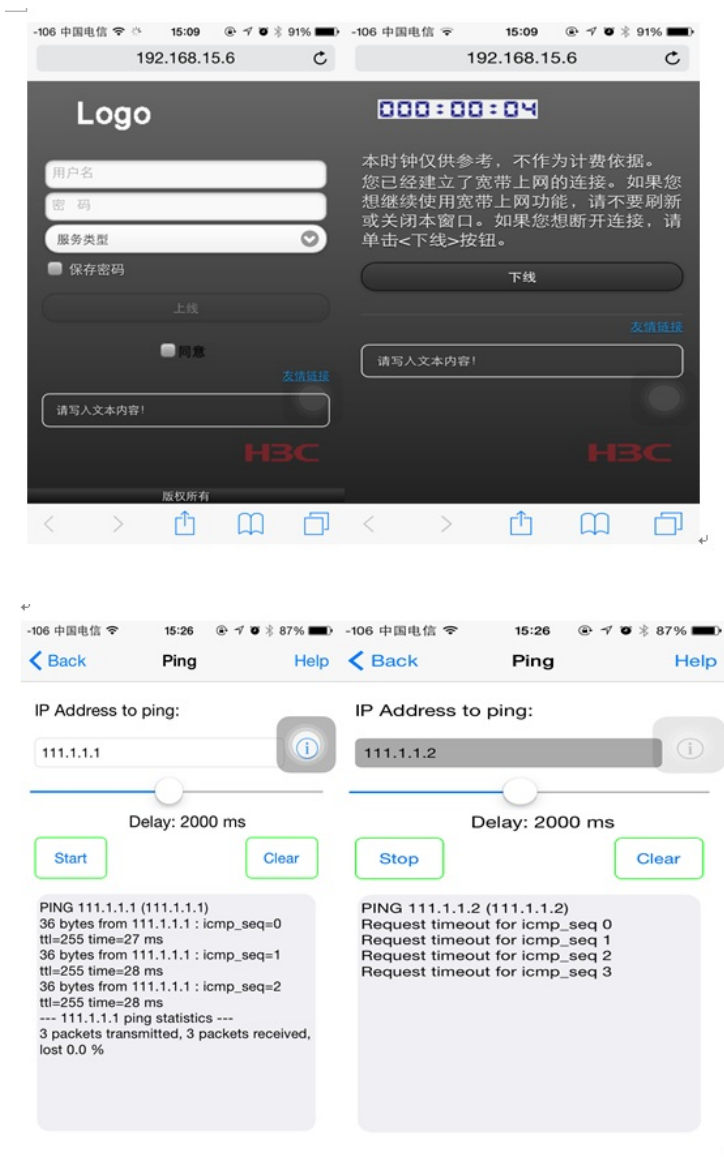
Ping的时候到设备上查看acl

dis acl 3000

Advanced ACL 3000, named -none-, 2 rules,

ACL's step is 5
rule 0 deny ip destination 111.1.1.1 0 (9 times matched)
rule 5 permit ip (5131 times matched)

iPhone客户端登陆:



设备上查看acl匹配情况

dis acl 3001
Advanced ACL 3001, named -none-, 2 rules,
ACL's step is 5
rule 0 deny ip destination 111.1.1.2 0 (23 times matched)
rule 5 permit ip (7541 times matched)