MSR810本地播存 Portal认证配置步骤

Portal　zhiliao_5ilsv　2019-10-31 发表

问题描述

一、组网

二、简介

MSR810设备作为无线网关，实现如下功能：

1、 提供无线接入点

2、 通过DHCP给接入的终端分配IP地址

3、 上行3G/4G接口通过Ipse隧道和总部的IMC服务器进行通信

4、 在MSR810上启用本地播存+Portal认证功能

5、 终端连接WIFI后，首先推送本地播存页面，客户可以浏览本地保存的视频和广告

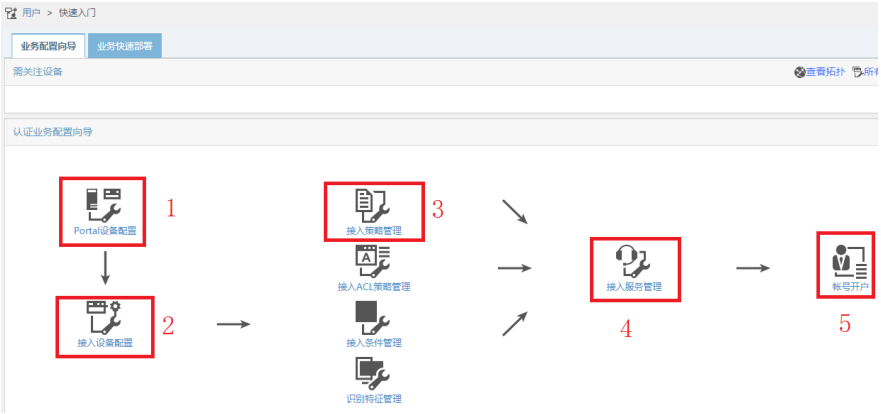
6、 点击“登陆外网”按钮后，跳转到portal认证界面，输入用户名和密码认证，认证成功后可以上外网

7、 当上行的3G/4G接口down后，终端用户只能访问到本地播存内容

解决方法

三、IMC的Portal和Radius配置

IMC转到“用户-->接入策略管理-->快速入门”界面，如下：



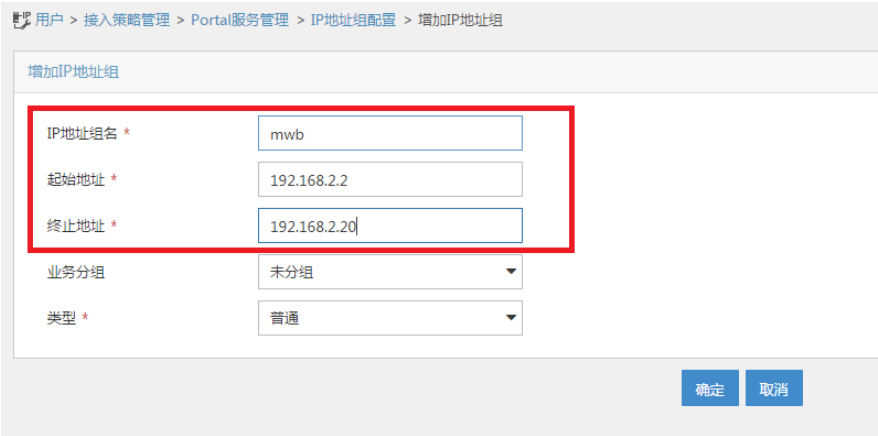
配置一共分为5步，如上图标示所示，其中第一步为配置portal服务器部分，其余4步为配置Radius部分。

1、portal配置部分

portal配置又分为3步，如下图所示：

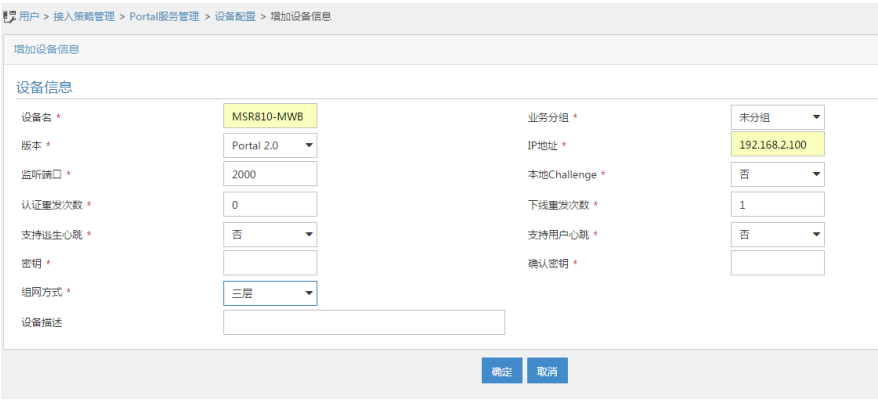
1.1 IP地址组配置

此地址组的范围是设备上DHCP给终端分配的地址范围，例如，图片中是192.168.2.2-20，对应设备上的DHCP分配地址的范围是一样的



dhcp server ip-pool 1
gateway-list 192.168.2.1
network 192.168.2.0 mask 255.255.255.0
address range 192.168.2.2 192.168.2.20
dns-list 192.168.2.1

1.2设备配置



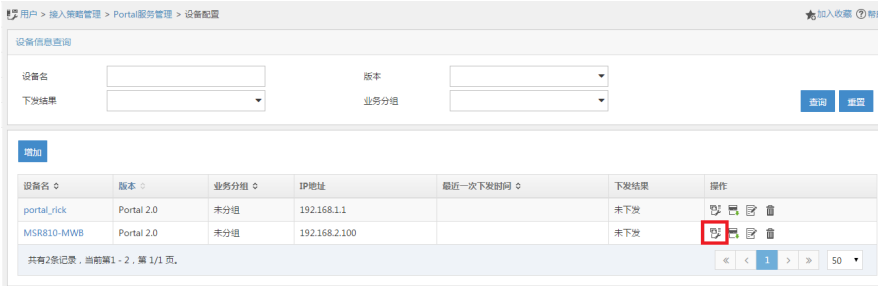
设备名：随意起名
版本：portal 2.0，现在只有portal 2.0版本
监听端口：默认2000，如果此处更改，对应设备上的portal server下的port也要更改
密钥：要和设备上portal server中配置的密钥相同

portal server test
 ip 172.32.103.254 key cipher c3$2RTZvaZ/cTFSXD+EeGUNun6Bw/Scz28= //要和此处相同
 port 2000
#

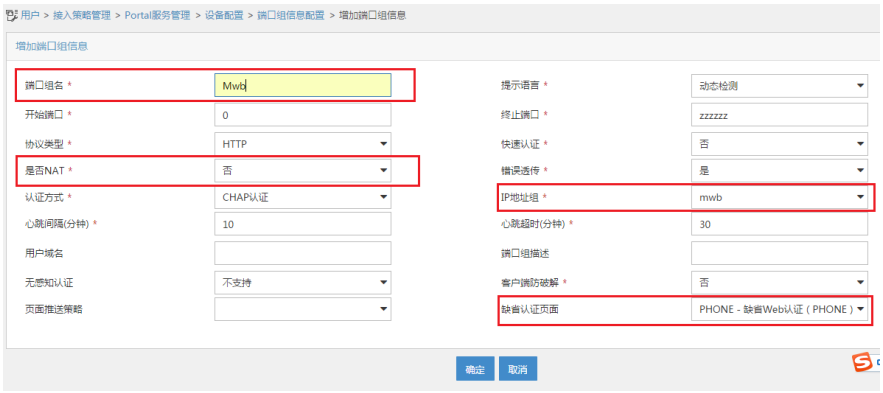
组网方式：选择三层
IP地址：此处必须和设备上下发portal的接口下配置的portal bas-ip一致，设备默认使用出接口地址作为portal bas-ip

1.3 配置端口组信息

点击配置端口组信息，会跳转到配置设备的页面，需要找到刚刚配置好的设备名称，点击后边的端口组信息管理按钮关联端口组，如下红色标示所示，例如刚刚我建立的设备名称为MSR810-MWB，选中后边的红色的端口组管理信息按钮，弹出端口组配置页面：



点击增加按钮，开始增加端口组：



端口组名：自起

是否NAT：这里选否，要依照环境而定

IP地址组：一定要选择在最开始配置的IP地址组名称，见1.1章节

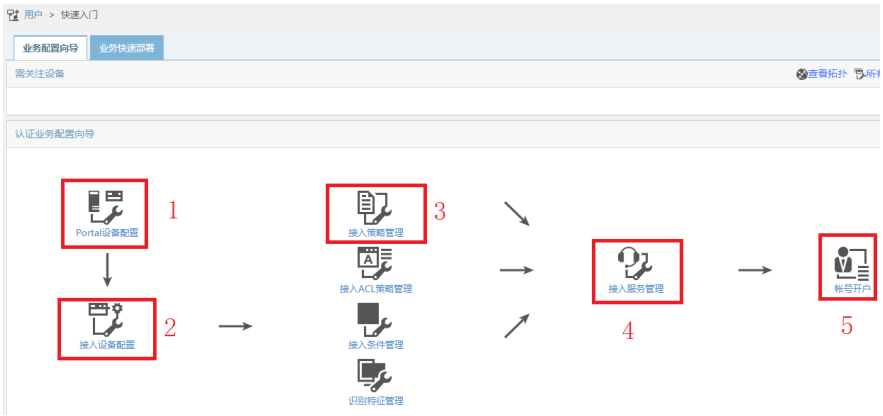
缺省认证页面：IMC默认提供了多种页面，如果使用缺省页面，建议使用图中所示的页面

点击确定，完成配置：

到此为止，portal部分，配置完毕。

2、Radius配置部分

返回到配置向导部分，开始Radius配置部分。

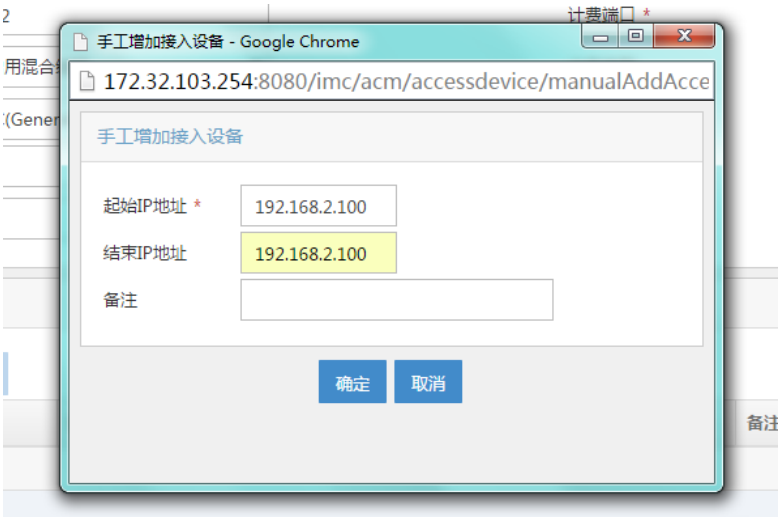


2.1 接入设备配置：

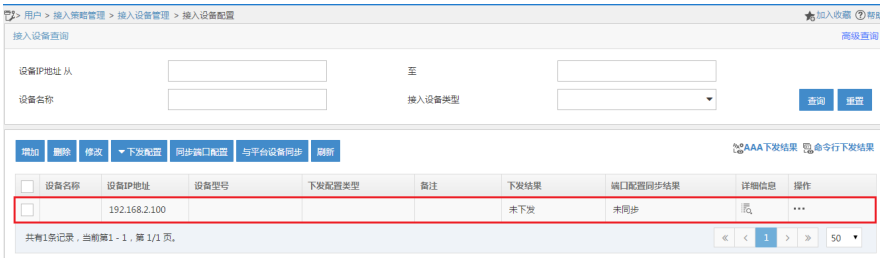
点击接入设备配置，进入接入设备配置界面后，点击增加按钮：

点击手动增加

在弹出的手动增加设备对话框中，输入设备上配置的radius nas-ip地址

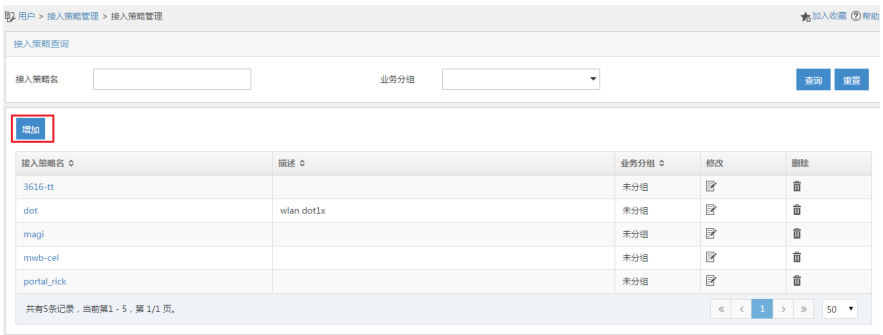


[H3C]radius scheme test
[H3C-radius-test]dis th
#
radius scheme test
 primary authentication 172.32.103.254 key cipher c3$peqNBcJL/Vc0c8V/zvk4vCHrrw9oD2M=
 primary accounting 172.32.103.254 key cipher c3$CP6s0vfPtv1kbvx82amEi8/82GKgvoc=
 user-name-format without-domain
 nas-ip 192.168.2.100 //要和此处一致
#
return
然后点击确定，在接入设备配置上出现刚刚配置的192.168.2.100



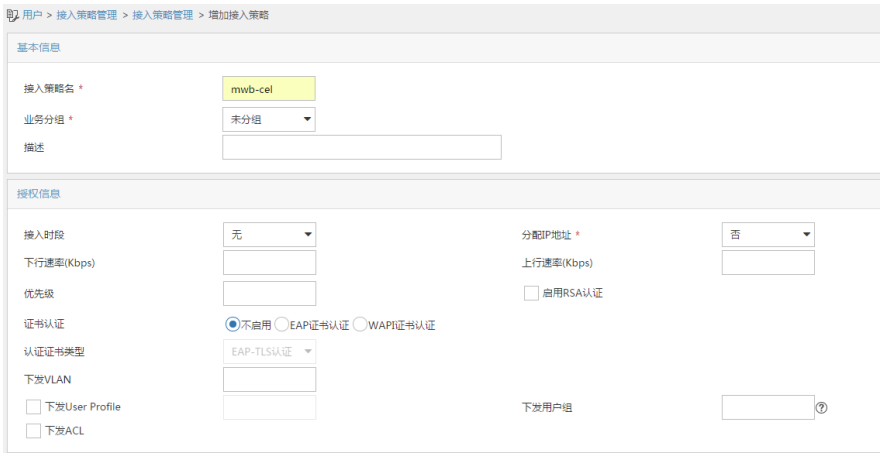
2.2 接入策略管理

返回快速向导，点击接入策略管理，点击增加按钮

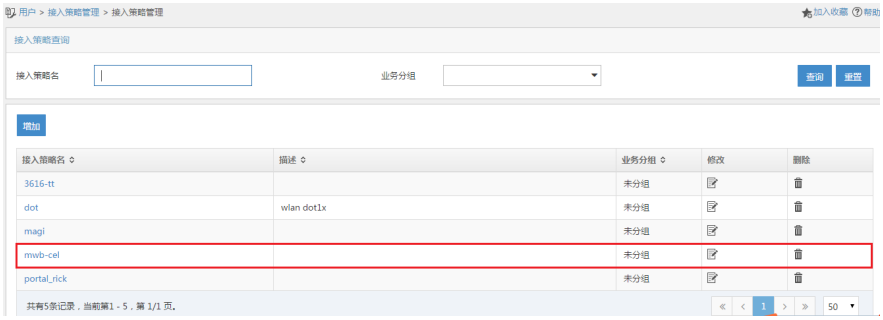


进入接入策略配置界面：

此处若无特殊要求，只需要配置接入策略名称，其他所有参数均为默认选项即可，例如此处配置的接入策略名称为mwb-cel



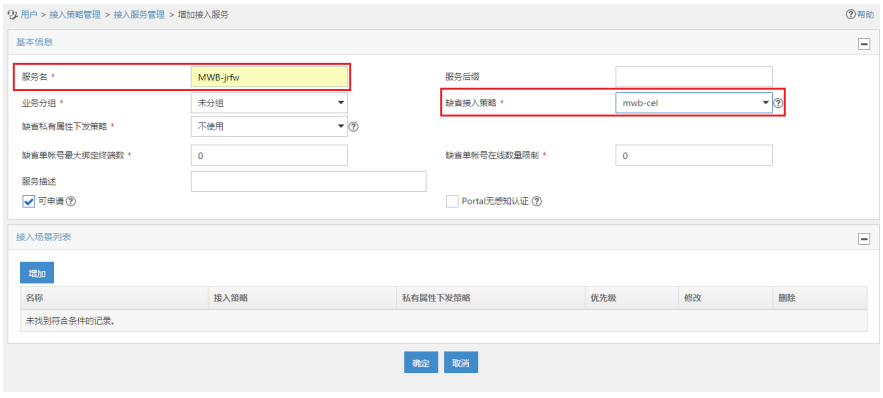
点击最下方确定后，可以看到刚刚创建的接入策略mwb-cel



2.3 接入服务管理

返回快速指导界面，点击接入服务选项，点击增加按钮

点击增加按钮后，进入接入服务配置页面



其中：

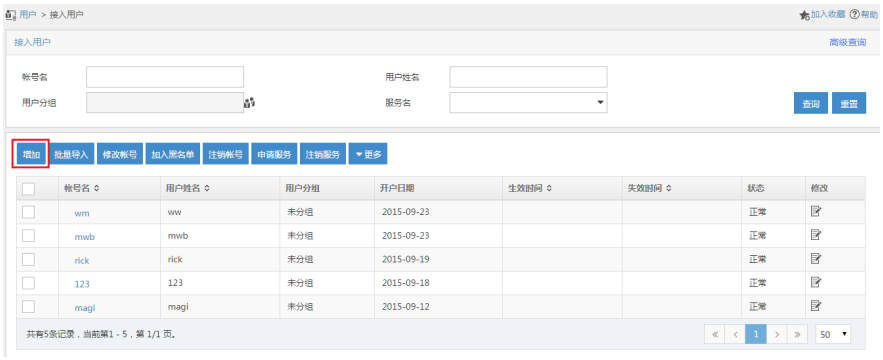
服务名：自起，例如此处我写的名称为mwb-jrfw

缺省接入策略：一定要选择刚刚通过2.2步骤创建的接入策略

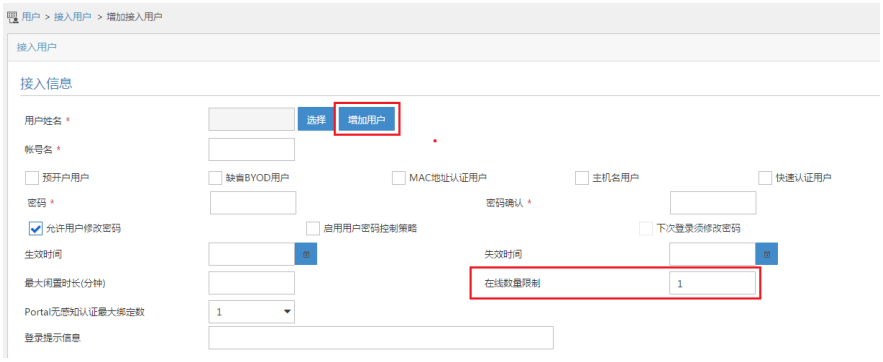
点击确定后，完成配置：

2.4账户开户

返回快速指导页面，点击账户开户选项，点击增加按钮：

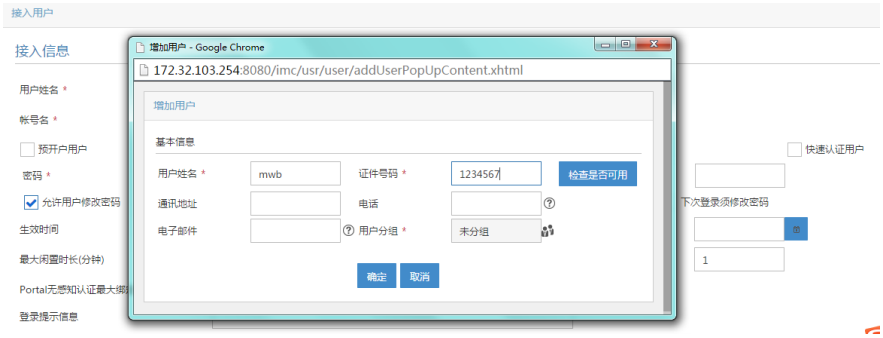


点击增加按钮，进入账户配置页面：

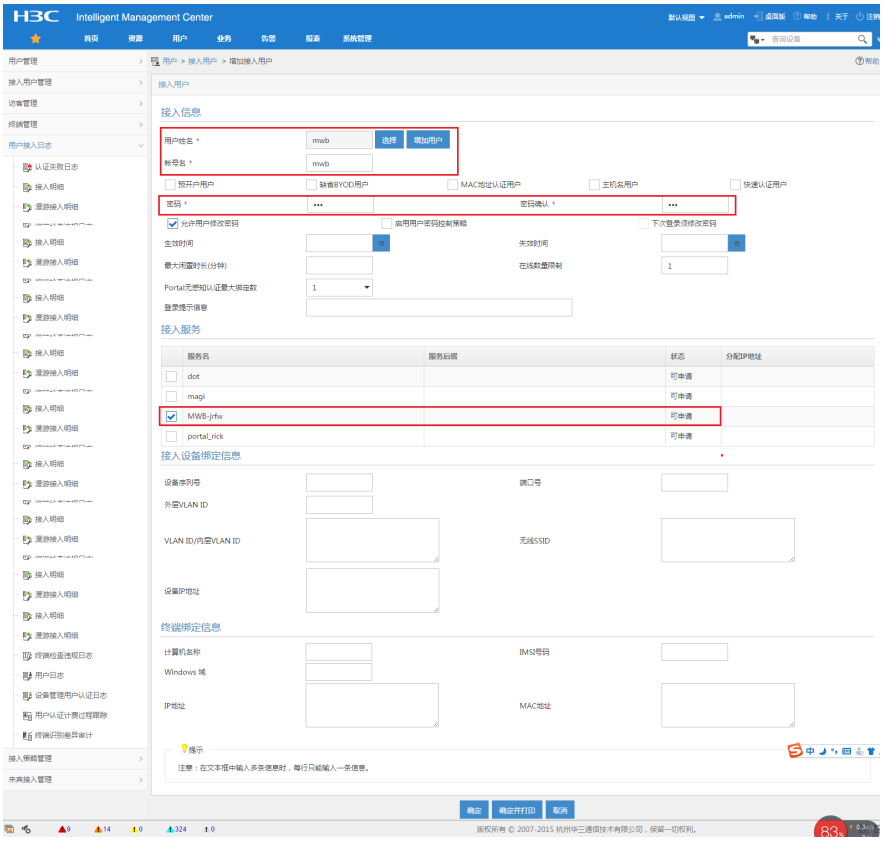


用户姓名：需要点击右侧选择，如果是新用户，需要点击增加用户新增
账号名：用于portal登陆的账户名
密码：用户portal登陆的密码
在线数量限制：限制同一时间内，同一个账号可以几个人登陆

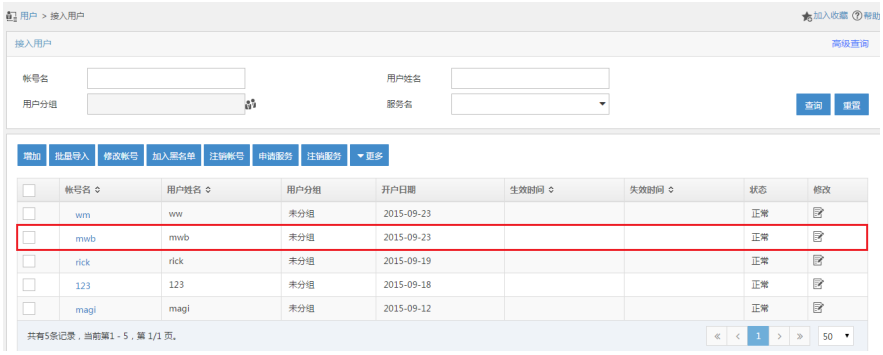
点击增加用户，新增用户，此处新增用户mwb，证件号码1234567，点击确认即可



增加用户后，给这个用户配置用户名、密码和选择使用哪个接入服务，如下方红色方框标出：
此处分配的用户民为mwb，密码为000，接入服务使用2.3步骤配置的mwb-jrfw策略



之后点击确定，可以看到用户创建成功：



配置好之后，可以使用手机连接到MSR810放出的wifi中认证
手机重定向到本地网页：

点击新闻，查看预存在MSR810 TF卡中的新闻

点击“访问外网”按钮，跳转到portal认证页面

输入用户名密码，认证成功，访问外网

三、设备侧配置

2.1 设备关键配置

```
[H3C]dis cu
#
 version 7.1.064, ESS 0401L13
#
 sysname H3C
#
 dialer-group 1 rule ip permit
#
 dhcp enable
#
 dns proxy enable
#
vlan 1
#
```

```
dhcp server ip-pool 1
 gateway-list 192.168.2.1
 network 192.168.2.0 mask 255.255.255.0
 address range 192.168.2.2 192.168.2.20
 dns-list 192.168.2.1
#
wlan service-template 1
 ssid MSR810-W
 akm mode psk
 preshared-key pass-phrase cipher $c$3$PAbUGdfVTMksnSVy+b1Nx5NSUOr1Tp67pW6j
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
controller Cellular1/0
 eth-channel 0
#
interface LoopBack0
 ip address 192.168.2.100 255.255.255.255
#
interface Vlan-interface1
 ip address 192.168.2.1 255.255.255.0
 tcp mss 1024
 dhcp server apply ip-pool 1
 portal enable method direct
 portal bas-ip 192.168.2.100
 portal apply web-server test
 web-redirect url http://192.168.2.1
 web-redirect track interface Eth-channel1/0:0
#
interface WLAN-Radio0/0
 service-template 1
#
interface Eth-channel1/0:0
 dialer circular enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 10
 dialer number *99# autodial
 ip address cellular-alloc
 nat outbound 3000
 ipsec apply policy 1
#
ip route-static 0.0.0.0 0 Eth-channel1/0:0
#
 light-http server directory slot0#sda0:/HTML
 light-http server enable
#
acl advanced 3000
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 172.32.0.0 0.0.255.255
 rule 5 permit ip
#
acl advanced 3001
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 172.32.0.0 0.0.255.255
#
radius scheme test
 primary authentication 172.32.103.254 key cipher $c$3$peqNBcJL/Vc0c8V/zvk4vCHrrw9oD2M=
 primary accounting 172.32.103.254 key cipher $c$3$CP6s0vfPtv1kbvx82amEi8/82GKgvoc=
 user-name-format without-domain
 nas-ip 192.168.2.100
#
domain test
 authentication default radius-scheme test
 authorization default radius-scheme test
```

```
 accounting default radius-scheme test
#
 domain default enable test
#
ipsec transform-set 1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3001
 remote-address 60.191.123.85
#
ike proposal 1
 dh group2
#
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$IwX119T1dk0xtZP5LMM+2B+kkljZS1c=
#
 portal free-rule 1 destination ip 172.32.103.254 255.255.255.255 //放通到IMC地址的报文
#
portal web-server test
 url http://192.168.2.1   //本地播存的地址
 captive-bypass enable
 url-parameter userip source-address
//当手机上点击“访问外网”按钮时，手机会向设备发送一个http://100.0.0.1的http请求，设备捕捉到这个请求后，重定向到http：//172.32.103.254:8080/portal页面，弹出portal认证，http://100.0.0.1是本地播存文件预制好的，这个字段以现场发出的为准
 if-match original-url http://100.0.0.1 redirect-url http://172.32.103.254:8080/portal
#
portal server test
 ip 172.32.103.254 key cipher $c$3$2RTZvaZ/cTFSXD+EeGUNun6Bw/Scz28=
#
wlan global-configuration
#
return
```

说明：

portal web-server下配置的url http://192.168.2.1和启用portal接口下的web-redirect url http://192.168.2.1，这两个作用是不一样的：

1）portal web-server是在上行链路正常时，portal web-server向用户推送本地播存页面

2）接口下的web-redirect url http://192.168.2.1，需要和web-redirect track interface Eth-channel1/0:0命令配合使用，监测到3G/4G接口down后，转到本地播存页面

配置完成后的效果：

1、 本次播存页面

2、 点击登录外网，弹出认证界面


●●●●● 中国联通
09:07
72%
172.32.87.100
欢迎使用iMC Portal
用户名
mwb
密码
●●●
服务类型
保存密码
上线
下线
修改密码
H3C
版权所有 © 2007-2014 杭州华三通信技术有限公司，保留一切权利。

3、 点击上线，认证成功


●●●●● 中国联通
09:08
72%
172.32.87.100
000:00:02
本时钟仅供参考，不作为计费依据。
您已经建立了宽带上网的连接。如果您想继续使用宽带上网功能，请不要刷新或关闭本窗口。如果您想断开连接，请单击<下线>按钮。
下线

2.2 自动获取运营商dns地址：

```
[H3C]display dns server
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   D     123.123.123.123
2   D     123.123.123.124
```

2.3 ike和IPsec信息

```
[H3C]dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   1               60.191.123.85       RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[H3C]
[H3C]
[H3C]dis ipsec sa
-------------------------------
Interface: Eth-channel1/0:0
-------------------------------

  ------------------------------
  IPsec policy: 1
  Sequence number: 1
  Mode: ISAKMP
  ------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1436
    Tunnel:
        local  address: 10.28.152.176
        remote address: 60.191.123.85
    Flow:
        sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 172.32.0.0/255.255.0.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 200775253 (0x0bf79655)
      Connection ID: 12884901889
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843112/1640
      Max received sequence-number: 186
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: Y
      Status: Active

    [Outbound ESP SAs]
      SPI: 2149607309 (0x8020678d)
      Connection ID: 12884901888
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843135/1640
      Max sent sequence-number: 216
      UDP encapsulation used for NAT traversal: Y
      Status: Active
[H3C]
```

2.4 本地播存文件存放路径

```
<H3C>cd slot0#sda0:/
<H3C>dir
Directory of sda0:
  0 drw-          - Mar 04 2015 15:02:42   HTML
  1 drw-          - Jan 01 2013 08:10:46   htm002
  2 drw-          - Jan 01 2011 00:35:52   huyue
  3 drw-          - Apr 16 2015 11:16:56   huyue1
  4 -rw-  138021888 Jan 01 2011 00:09:54   la3616-cmw710-system-a040105.bin
  5 drw-          - Jan 01 2013 00:30:14   log
  6 -rw-      88526 Apr 08 2015 14:06:06   logfile1.log
  7 -rw-       2345 Jan 01 2013 00:28:12   startup.cfg
  8 -rw-       5719 Jan 01 2011 00:20:56   startup1.cfg

30748672 KB total (26639968 KB free)

<H3C>cd html
<H3C>dir
Directory of sda0:/HTML
  0 drw-          - Mar 04 2015 15:20:54   AGENT
  1 drw-          - Mar 04 2015 15:20:02   BUSNEWS
  2 drw-          - Mar 04 2015 15:20:00   CGI-BIN
  3 drw-          - Mar 04 2015 15:19:58   CSS
  4 drw-          - Mar 04 2015 15:19:46   EMUSIC
  5 drw-          - Mar 04 2015 15:19:46   FORIOS
  6 drw-          - Mar 04 2015 15:19:44   FORWEB
  7 drw-          - Mar 04 2015 15:18:58   FUNNY
  8 drw-          - Mar 04 2015 15:18:50   HELLO
  9 drw-          - Mar 04 2015 15:18:46   HUODONG
 10 drw-          - Mar 04 2015 15:18:20   IMAGES
 11 drw-          - Mar 04 2015 15:18:16   JS
 12 drw-          - Mar 04 2015 15:17:38   NEWS
 13 drw-          - Mar 04 2015 15:10:30   PACK
 14 drw-          - Mar 04 2015 15:10:24   PRESERVE
 15 drw-          - Mar 04 2015 15:09:52   STYLE
 16 drw-          - Mar 04 2015 15:09:36   T
 17 -rw-         41 Sep 04 2014 10:27:44   VERSION.LUA
 18 drw-          - Mar 04 2015 15:09:34   WPROXY
 19 drw-          - Mar 04 2015 15:06:48   YAPP
 20 drw-          - Mar 04 2015 15:03:02   ZMEDIA
 21 drw-          - Mar 04 2015 15:20:48   banner_img
 22 drw-          - Mar 04 2015 15:20:26   banner_package
 23 drw-          - Mar 04 2015 15:20:04   bus-group
 24 drw-          - Mar 04 2015 15:20:02   bus-search
 25 drw-          - Mar 04 2015 15:19:46   forandroid
 26 -rw-       4099 Sep 04 2014 10:27:42   guide.html
 27 drw-          - Mar 04 2015 15:18:42   huodong_wap
 28 -rw-      22574 Oct 28 2014 20:56:14   index.html
 29 -rw-      22461 Sep 04 2014 10:27:42   index.html.bak
 30 -rw-       5771 Sep 04 2014 10:27:42   index.json
 31 -rw-      22613 Sep 04 2014 10:27:42   index30.html
 32 -rw-      22461 Sep 04 2014 10:27:42   index_1.html
 33 -rw-      21852 Sep 04 2014 10:27:42   index_bak.html
 34 -rw-      22590 Sep 05 2014 11:39:46   index_cmmb.html
 35 -rw-      15800 Sep 04 2014 10:27:42   index_ios.html
 36 -rw-      19693 Sep 04 2014 10:27:42   index_wap.html
 37 -rw-     139620 Sep 04 2014 10:27:44   jquery.mobile-1.3.1.css
 38 -rw-     359006 Sep 04 2014 10:27:44   jquery.mobile-1.3.1.js
 39 -rw-       1147 Sep 04 2014 10:27:42   lh.html
 40 -rw-   75125760 Sep 26 2014 17:16:56   msr8101216.ipe
 41 drw-          - Mar 04 2015 15:09:52   recommend
 42 -rw-       1158 Sep 04 2014 10:27:44   zhongjie.html
 43 -rw-       1151 Sep 04 2014 10:27:44   zhongjie2.html
 44 -rw-       1147 Sep 04 2014 10:27:44   zhongjie2_bak.html
```

45 -rw- 1151 Sep 04 2014 10:27:44 zhongjie_bak.html

30748672 KB total (26639968 KB free)

四、URL过滤配置及效果

要求实现效果：

1）认证前推送本地播存页面，可以正常播放本地播存内容

2）点击“访问外网”可弹出portal认证页面，输用户名/密码，可正常上网

3）但是不允许访问所有新浪网页

3.1 配置

```
<H3C>dis cu
#
 version 7.1.064, ESS 0401L13
#
 sysname H3C
#
 dialer-group 1 rule ip permit
#
 dhcp enable
#
 dns proxy enable
 dns spoofing 1.1.1.1
#
 password-recovery enable
#
vlan 1
#
object-group ip address urladdress   //创建IPv4地址对象组
 0 network subnet 192.168.2.0 255.255.255.0
#
traffic classifier qq operator and
 if-match app-group qq_all
#
traffic behavior qq
 filter deny
#
qos policy qq_deny
 classifier qq behavior qq
#
dhcp server ip-pool 1
 gateway-list 192.168.2.1
 network 192.168.2.0 mask 255.255.255.0
 address range 192.168.2.2 192.168.2.20
 dns-list 192.168.2.1
#
wlan service-template 1
 ssid MSR810-W
 akm mode psk
 preshared-key pass-phrase cipher $c$3$PAbUGdfVTMksnSVy+b1Nx5NSUOr1Tp67pW6j
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
controller Cellular0/0
#
controller Cellular1/0
 eth-channel 0
#
interface NULL0
#
interface LoopBack0
 ip address 192.168.2.100 255.255.255.255
#
interface LoopBack1
```

```
 ip address 2.1.1.1 255.255.255.255
#
interface Vlan-interface1
 ip address 192.168.2.1 255.255.255.0
 tcp mss 1024
 dhcp server apply ip-pool 1
 portal enable method direct
 portal bas-ip 192.168.2.100
 portal apply web-server test
 web-redirect url http://192.168.2.1
 web-redirect track interface Eth-channel1/0:0
#
interface GigabitEthernet0/0
 port link-mode route
#
interface GigabitEthernet0/5
 port link-mode route
#
interface GigabitEthernet0/1
 port link-mode bridge
#
interface GigabitEthernet0/2
 port link-mode bridge
#
interface GigabitEthernet0/3
 port link-mode bridge
#
interface GigabitEthernet0/4
 port link-mode bridge
#
interface WLAN-Radio0/0
 service-template 1
#
interface Eth-channel1/0:0
 dialer circular enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 10
 dialer number *99# autodial
 ip address cellular-alloc
 nat outbound 3000
 ipsec apply policy 1
#
object-policy ip pass
 rule 0 pass
#
object-policy ip urlsina  //创建对象策略
 rule 0 inspect urlsina source-ip urladdress  //定义对象策略规则，对于原地址处于对象组urladdress中
的IP地址进行urlsina中规定的检测
#
security-zone name Local
#
security-zone name Trust
#
security-zone name DMZ
#
security-zone name Untrust
#
security-zone name Management
#
security-zone name client  //将内网口加入client安全域
 import interface Vlan-interface1
#
security-zone name server  //公网口加入server安全域
```

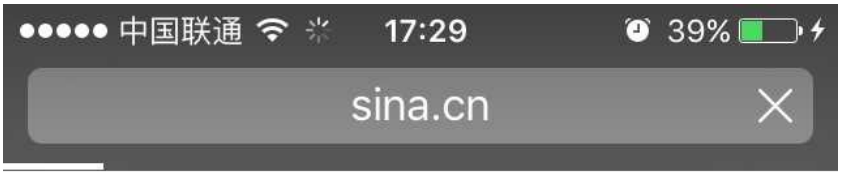
```
 import interface Eth-channel1/0:0
#
zone-pair security source Any destination Local  //定义一系列遇见策略
 object-policy apply ip pass
#
zone-pair security source client destination Local
 object-policy apply ip pass
#
zone-pair security source client destination server
 object-policy apply ip urlsina
#
zone-pair security source Local destination Any
 object-policy apply ip pass
#
zone-pair security source Local destination client
 object-policy apply ip pass
#
zone-pair security source server destination Any
 object-policy apply ip pass
#
zone-pair security source server destination client
 object-policy apply ip pass
#
 scheduler logfile size 16
#
line class console
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line con 0
 user-role network-admin
#
line vty 0 63
 user-role network-operator
#
 ip route-static 0.0.0.0 0 Eth-channel1/0:0
#
 light-http server directory slot0#sda0:/HTML
 light-http server enable
#
acl advanced 3000
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 172.32.0.0 0.0.255.255
 rule 5 permit ip
#
acl advanced 3001
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 172.32.0.0 0.0.255.255
#
radius scheme test
 primary authentication 172.32.103.254 key cipher $c$3$peqNBcJL/Vc0c8V/zvk4vCHrrw9oD2M=
 primary accounting 172.32.103.254 key cipher $c$3$CP6s0vfPtv1kbvx82amEi8/82GKgvoc=
 user-name-format without-domain
 nas-ip 192.168.2.100
#
domain system
#
domain test
 authentication default radius-scheme test
 authorization default radius-scheme test
 accounting default radius-scheme test
```

```
#
 domain default enable test
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
ipsec transform-set 1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3001
 remote-address 60.191.123.85
#
app-group qq_all
 description User-defined application group
 include application QQ_DouDiZhu_Application_TCP
 include app-group QQ_DouDiZhu
 include app-group QQ_Mail
```

```
 include app-group Tencent_QQ
#
 ike dpd interval 10 periodic
#
ike proposal 1
 dh group2
#
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$IwX119T1dk0xtZP5LMM+2B+kkljZS1c=
#
 portal free-rule 1 destination ip 172.32.103.254 255.255.255.255
#
portal web-server test
 url http://192.168.2.1
 captive-bypass enable
 url-parameter userip source-address
 if-match original-url http://100.0.0.1 redirect-url http://172.32.103.254:8080/portal
#
portal server test
 ip 172.32.103.254 key cipher $c$3$2RTZvaZ/cTFSXD+EeGUNun6Bw/Scz28=
#
url-filter policy urlsina   //定义URL过滤策略
 default-action permit  //定义默认动作
 category sina action drop logging  //引用自定义的url分类
#
url-filter category sina severity 2000  //自定义url过滤分类类型
 rule 1 host regex sina  //以模糊匹配的方式匹配，匹配url中的host字段，只要有sina即可命中
#
app-profile urlsina  //在DPI策略中引用
 url-filter apply policy urlsina
#
wlan global-configuration
#
traffic-policy
#
ips policy default
#
return
```

3.2 效果

访问sina.cn访问不到，但是可以访问其他页面



访问其他的可以：

deb可以看到：

%Jan 1 01:26:28:508 2011 H3C UFLT/6/log:
Packet matched rule:-Host=sina.cn-Category=sina-Policy=urlsina-Action=drop-From=192.168.2.2/50651-To=202.108.5.219/80

%Jan 1 01:26:49:268 2011 H3C UFLT/6/log:
Packet did not matched any rules:-Host=mat1.gtimg.com-Policy=urlsina-Action=permit-From=192.168.2.2/50661-To=125.39.213.101/80

%Jan 1 01:26:49:269 2011 H3C UFLT/6/log:
Packet did not matched any rules:-Host=mat1.gtimg.com-Policy=urlsina-Action=permit-From=192.168.2.2/50660-To=125.39.213.101/80

3.3 注意事项

1）配置完DPI应用profile（app-profile）之后，必须使用命令inspect activate命令激活，否则app-profile不生效，也就达不到url过滤效果。

2）当DPI应用profile下引用的各DPI业务模块自定义了规则或手动离线升级了特征库时，需要执行inspect activate命令来使其生效。
3）更改了profile中模块的配置，也要执行inspect activate来激活。
4）设备重启之后，所有与DPI各业务模块自定义的规则或手动离线升级的特征库会自动生效。

防火墙
每个安全域之间无法访问，如果配置了zone-pair，按照zone-pair下的策略访问，如果zone-pair下没有配置任何策略，默认dorp，路由器在安全域之间默认下发了aspf。

[H3C]zone-pair security source local destination server //不下发策略
[H3C-zone-pair-security-Local-server]ping -a 3.1.1.1 114.114.114.114
Ping 114.114.114.114 (114.114.114.114) from 3.1.1.1: 56 data bytes, press CTRL_C to break
Request time out //不通

--- Ping statistics for 114.114.114.114 ---
2 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

[H3C-zone-pair-security-Local-server]object-policy apply ip pass //下发通过策略
[H3C-zone-pair-security-Local-server]ping -a 3.1.1.1 114.114.114.114
Ping 114.114.114.114 (114.114.114.114) from 3.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 114.114.114.114: icmp_seq=0 ttl=86 time=133.291 ms   //通
56 bytes from 114.114.114.114: icmp_seq=1 ttl=91 time=41.312 ms
56 bytes from 114.114.114.114: icmp_seq=2 ttl=91 time=33.801 ms
56 bytes from 114.114.114.114: icmp_seq=3 ttl=75 time=32.297 ms
56 bytes from 114.114.114.114: icmp_seq=4 ttl=73 time=39.735 ms

--- Ping statistics for 114.114.114.114 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 32.297/56.087/133.291/38.752 ms

[H3C]undo zone-pair security sou local des server //删除
[H3C]
[H3C]
<H3C>ping -a 192.168.2.100 114.114.114.114 //不通了
Ping 114.114.114.114 (114.114.114.114) from 192.168.2.100: 56 data bytes, press CTRL_C to break
*Jan 1 01:03:05:654 2011 H3C ASPF/7/PACKET: The first packet was dropped by ASPF for nonexistent zone pair. Src-ZOne=Local, Dst-ZOne=server;If-In=InLoopBack0(17474), If-Out=Eth-channel1/0:0(17478); Packet Info:Src-IP=192.168.2.100, Dst-IP=114.114.114.114, VPN-Instance=none,Src-Port=65284, Dst-Port=2048. Protocol=ICMP(1).

Request time out
*Jan 1 01:03:07:856 2011 H3C ASPF/7/PACKET: The first packet was dropped by ASPF for nonexistent zone pair. Src-ZOne=Local, Dst-ZOne=server;If-In=InLoopBack0(17474), If-Out=Eth-channel1/0:0(17478); Packet Info:Src-IP=192.168.2.100, Dst-IP=114.114.114.114, VPN-Instance=none,Src-Port=65284, Dst-Port=2048. Protocol=ICMP(1).

--- Ping statistics for 114.114.114.114 ---
2 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<H3C>%Jan 1 01:03:08:874 2011 H3C PING/6/PING_STATISTICS: Ping statistics for 114.114.114.114: 2 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss.

若域间策略配置如下，：
zone-pair security source Local destination Any
 object-policy apply ip pass
#
zone-pair security source Local destination client
 object-policy apply ip pass
#
zone-pair security source Local destination server
 object-policy apply ip deny
则按照精确的匹配，destination Any的最后匹配。