SecBladeIAG支持认证页面与重定向URL不一致的Portal典型配置

Portal　**李晨光**　2012-08-03 发表

SecBladeIAG支持认证页面与重定向URL不一致的Portal典型配置

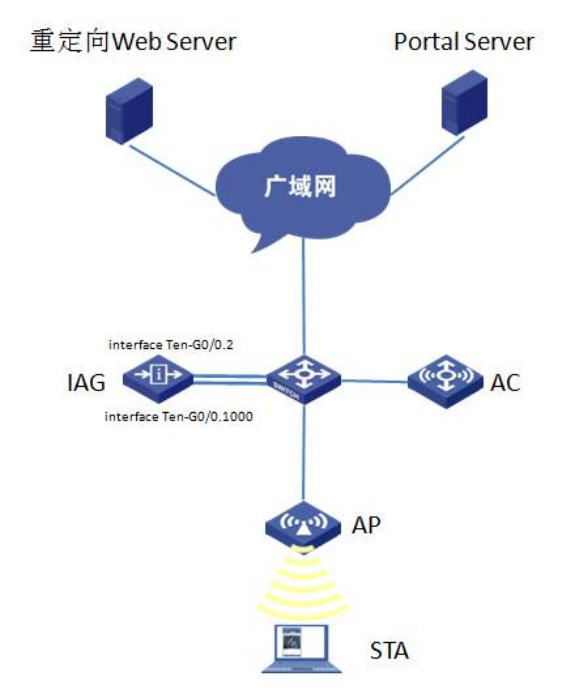
一、应用环境

一般的应用场景下，重定向URL指向Portal认证服务器，用户可以在重定向页面中直接输入用户名、密码登陆。但在部分特殊的应用需求下，重定向URL只是指向某门户网站主页，主页上另提供一个按钮到Portal认证页面的链接。用户点击该链接后才真正进入Portal认证页面，然后输入用户名、密码登陆。本例典型配置案例即为IAG实现该特殊应用需求下的Portal认证。

二、组网需求：

用户通过WX系列AC完成无线的接入，网关终结在IAG上，IAG上做Portal认证。IAG、AC无特定版本要求。

三、组网图：



五、配置方法：

1．配置思路

? 在AC上配置无线接入服务，业务网关终结到IAG上
? 在IAG上配置PORTAL认证RADIUS方案、domain。
? 在IAG上配置两个Portal Server：重定向Web Server、Portal认证Server。并手动添加Portal认证Server地址到Portal白名单。
? 在IAG上配置无线业务网关接口，起Portal认证，配置Portal重定向指向Web Server。

2．配置步骤

（1）AC上的配置信息：（略）

（2）IAG上的配置信息：

```
dis cur
#
 version 5.20, Release 7510P06
#
 sysname IAG
#
 super password level 3 cipher X7A'-%9#+WZ/3:L02.;;!Q!!
#
 configure-user count 8
#
 domain default enable system
```

```
#
 portal server real ip 10.176.1.140 url http://10.176.1.140/wlan/index.php     //配置portal 认证 s
erver
 portal server redirect_url ip 10.1.1.13 url http://10.1.1.13     //配置重定向web server
 portal free-rule 1 source any destination ip 10.176.1.140 mask 255.255.255.255     //手动放
通portal real server
 portal free-rule 2 source any destination ip 211.136.17.107 mask 255.255.255.255     //放通
DNS
 portal free-rule 3 source any destination ip 10.0.0.3 mask 255.255.255.255     //放通网关
 portal device-id 0004.0431.431.00                                  //配置AC NAME
#
radius scheme isp                                          //portal的radius策略
 server-type extended
 primary authentication 10.176.1.138 1645
 primary accounting 10.176.1.138 1646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 timer realtime-accounting 3
 user-name-format keep-original
 nas-ip 123.9.9.1
 retry stop-accounting 10
#
aaa nas-id profile mobile
 nas-id 0010043143100460 bind vlan 200
 nas-id 0011043143100460 bind vlan 201
 nas-id 0012043143100460 bind vlan 202
#
domain real                                          //portal的domain域
 authentication portal radius-scheme isp
 authorization portal radius-scheme isp
 accounting portal radius-scheme isp
 access-limit disable
 state active
 idle-cut enable 15 10000
 self-service-url disable
#
dhcp server ip-pool userclient_dhcp_server           //业务地址池
 network 10.0.0.0 mask 255.255.255.0
 gateway-list 10.0.0.3
 dns-list 211.137.58.20 211.136.17.107
 expired day 0 hour 1
#
user-group system
#
interface NULL0
#
interface GigabitEthernet0/1
 port link-mode route
#
interface GigabitEthernet0/2
 port link-mode route
#
interface GigabitEthernet0/3
 port link-mode route
#
interface GigabitEthernet0/4
 port link-mode route
#
interface Ten-GigabitEthernet0/0
 port link-mode route
#
interface Ten-GigabitEthernet0/0.300                         //nas-ip接口
ip address 123.9.9.1 255.255.255.248
#
```

```
interface Ten-GigabitEthernet0/0.2                //iag、ac漫游lactp隧道接口
 vlan-type dot1q vid 2
 ip address 192.168.3.100 255.255.255.0
#
interface Ten-GigabitEthernet0/0.200                        //业务网关接口
 vlan-type dot1q vid 200 to 207 221                        //模糊vlan终结
 ip address 10.0.0.2 255.255.255.0                         //配置实ip地址
 arp authorized enable                                     //使能授权arp
 arp send-gratuitous-arp interval 60000                    //配置免费arp发送间隔
 dhcp update arp                                           //配置授权arp
 portal server redirect_url method direct                  //配置重定向url，非portal认证页面
 portal domain real                                        //配置portal强制认证域
 portal nas-id-profile mobile                              //绑定portal nas-id-profile
 portal nas-port-type wireless
 portal nas-ip 123.9.9.1                                   //指定portal nas-ip
 access-user detect type arp retransmit 5 interval 30      //在线用户检测
#
wlan mobility-group 1                                      //配置漫游组
 member ip 192.168.3.1
 source ip 192.168.3.100
 authentication-mode MD5 123456
 mobility-group enable
#
 ip route-static 0.0.0.0 0.0.0.0 123.9.9.4
#
 undo info-center enable
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE2000001
 snmp-agent community read ^%dsU!!
 snmp-agent community write ^%dsU!!
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 221.9.0.11 params securityname public
v2c
#
 nqa schedule cl2topo ping start-time now lifetime 630720000
#
 arp timer aging 1440
#
 load xml-configuration
#
user-interface con 0
 idle-timeout 35791 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

3．配置关键点

（1）IAG上进行配置：

配置两个Portal Server：Portal认证Server、重定向Web Server。

[IAG] portal server real ip 10.176.1.140 url http://10.176.1.140/wlan/index.php

[IAG] portal server redirect_url ip 10.1.1.13 url http://10.1.1.13

手动添加Portal认证Server到Portal白名单。

[IAG] portal free-rule 1 source any destination ip 10.176.1.140 mask 255.255.255.255

创建radius方案system并进入其视图。

[IAG] radius scheme isp

配置PEAP认证/计费RADIUS服务器的IP地址。

[IAG-radius-isp] primary authentication 10.176.1.138 2645

[IAG-radius-isp] primary accounting 10.176.1.138 2646

配置Device与认证/计费RADIUS服务器交互报文时的共享密钥。

[IAG-radius-isp] key authentication 88----89

[IAG-radius-isp] key accounting 88----89

#设置设备发送RADIUS报文使用的源地址

[IAG-radius-isp] nas-ip 123.9.9.1

配置发送给RADIUS服务器的用户名不携带域名。

[IAG-radius-isp] user-name-format without-domain

[IAG-radius-isp] quit

创建域real并进入其视图。

[IAG] domain real

配置portal用户使用RADIUS方案system进行认证、授权、计费。

[IAG-isp-real] authentication portal radius-scheme isp

[IAG-isp-real] authorization portal radius-scheme isp

[IAG-isp-real] accounting portal radius-scheme isp

关闭该域最多可容纳用户限制功能。

[IAG-isp-real] access-limit disable

启动闲置切断功能，并指定正常连接时用户空闲时间超过15分钟，并且最小流量低于10000 Byte时则切断其连接。（此配置项根据实际情况可选,集团暂时没有统一规范）

[IAG-isp-real] idle-cut enable 15 10000

[IAG-isp-real] quit

指定域system为缺省的ISP域。如果用户在登录时没有提供ISP域名，系统将把它归于该缺省的ISP域。

[IAG] domain default enable real

创建TG0/0.200接口作为业务网关，并进入该视图。

[IAG] interface Ten-GigabitEthernet 0/0.200

#配置此端口模糊VLAN终结

[IAG-Ten-GigabitEthernet0/0.200] vlan-type dot1q vid 200 to 207 221

#配置此端口的实IP地址

[IAG-Ten-GigabitEthernet0/0.200] ip address 10.0.0.1 255.255.255.0

#配置授权ARP和免费ARP发送间隔

[IAG-Ten-GigabitEthernet0/0.200] arp authorized enable

[IAG-Ten-GigabitEthernet0/0.200] arp send-gratuitous-arp interval 60000

[IAG-Ten-GigabitEthernet0/0.200] dhcp update arp

#配置portal重定向server

[IAG-Ten-GigabitEthernet0/0.200] portal server redirect_url method direct

[IAG-Ten-GigabitEthernet0/0.200] portal domain real

[IAG-Ten-GigabitEthernet0/0.200] portal nas-id-profile mobile

[IAG-Ten-GigabitEthernet0/0.200] portal nas-port-type wireless

[IAG-Ten-GigabitEthernet0/0.200] portal nas-ip 123.9.9.1

[IAG-Ten-GigabitEthernet0/0.200] access-user detect type arp retransmit 5 interval 30

#配置WLAN漫游组

[IAG] wlan mobility-group 1

#配置源IP地址

[IAG-wlan-mg-1] source ip 192.168.3.100

#添加漫游组成员

[IAG-wlan-mg-1] member ip 192.168.3.1

#配置IACTP控制消息完整性认证模式(可选)

[IAG-wlan-mg-1] authentication-mode MD5 simple 123456

#开启IACTP服务

[IAG-wlan-mg-1] mobility-group enable

[IAG-wlan-mg-1] quit

六、验证结果：

第一步：用户连接wifi网络后,通过浏览器访问任意网站,被重定向到redirect_url指定的页面；
第二步：用户点击redirect_url页面上的认证链接按钮，能成功打开Portal认证页面；
第三步：用户在Portal认证页面上输入正确的用户名、密码，能成功登陆，并访问internet。