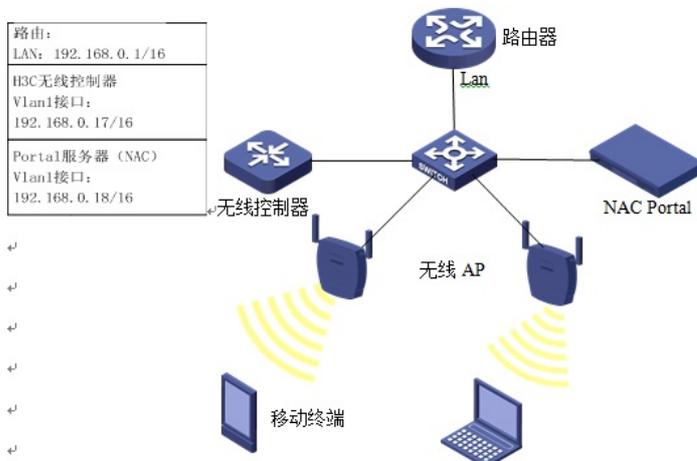


知 WX3540E与深信服NAC Portal服务器实现微信认证案例

wlan接入 Portal AAA 刘嘉炜 2016-07-06 发表

WX3540E无线控制器和深信服NAC Portal设备在同一局域网，华三的无线控制器做集中转发，通过深信服NAC Portal服务器的微信连WiFi功能认证实现手机用户微信认证。



1 配置认证服务器

除portal服务器地址外其他参数默认即可，内置radius服务器的密钥固定为123456



2 配置web认证策略

协议这里需要注意，默认WX3540E无线控制器采用的是CMCC的portal2.0协议，配置时需要修改为IMC协议（也可以采用portal2.0，也测试过可以通过认证）。确保深信服NAS Portal服务器与WX3540E无线控制器的端口正常通信。



3 WX3540E无线控制器配置

首先新建radius认证服务器



配置AAA: 点击认证->AAA, 填写域名, 并且应用



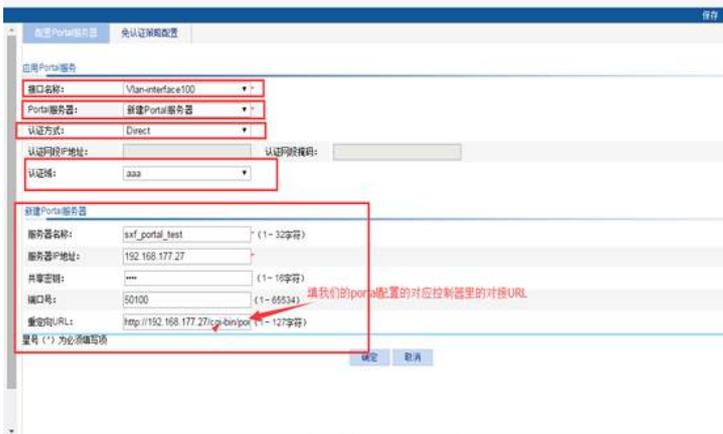
点击认证, 按如下的配置进行配置, 最后点击应用



点击认证->portal认证->新建

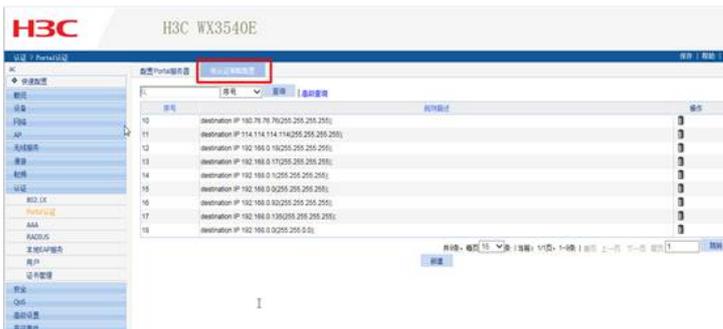


选端口名称选择之前配置好的vlan口，portal服务器选择新建portal服务器，认证方式选择Direct，认证域选择刚才配好的认证域，填写新建portal服务器信息（服务器ip为portal的ip）点击确定。



4 WX3540E无线控制器配置需要注意的是还需要放通固定的一些地址段（如下图）

- 1、portal服务器的IP地址
- 2、华三控制器的通信IP地址
- 3、网关地址、以及整个认证网段
- 4、DNS地址放通



5 WX3540E无线控制器命令行参数

- 1、接口配置
- ```

interface Vlan-interface 1
ip address 192.168.0.17 255.255.0.0
portal server wac method direct
portal domain wac

```

## 2、指向URL配置及对接协议

指向: portal server wac ip 192.168.0.18 key cipher

```
c3$OSyoLh5AXh+i5w5wf0+5xVS2+DIOKLQRg== url http://192.168.0.18/?url_id=1408525 server-type imc
```

## 3、放通免认证的白名单地址

认证网段为192.168.0.0/16的网段

白名单: portal free-rule 17 source ip any destination ip 192.168.0.135 mask 255.255.255.255

白名单: portal free-rule 18 source ip any destination ip 192.168.0.0 mask 255.255.0.0

## 4、RADIUS认证配置

192.168.0.18是深信服NAS portal服务器

radius scheme wac

server-type extended

primary authentication 192.168.0.18

key authentication cipher \$c\$3\$DaE5mTBMcl3LkbA4eqmolIBS5I5LPFZsFw==

user-name-format without-domain

retry stop-accounting 10

## 5、域设置配置

domain wac

authentication portal radius-scheme wac

authorization portal radius-scheme wac

access-limit disable

accounting optional

state active

idle-cut enable 15 10000

self-service-url disable

说明: 如果不配置“accounting optional”这条命令就会出现当用户portal认证通过后被设备踢出, 描述如下

### 【描述】

accounting optional命令用来打开计费可选开关。undo accounting optional命令用来关闭计费可选开关。缺省情况下, 计费可选开关处于关闭状态。

需要注意的是:

- 对上线用户计费时, 如果发现没有可用的计费服务器或与计费服务器通信失败时, 若配置了本命令, 则用户可以继续使用网络资源, 且系统不再为其发送实时计费更新报文, 否则用户连接将被切断。该命令适用于不是特别关心计费结果的情况下。
- 计费可选开关打开的情况下, 本地用户视图下的access-limit命令配置的本地用户的连接数限制功能不生效。

### 【举例】

```
打开ISP域(isp)的计费可选开关。
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting optional
```

## 6 认证通过后的系统状态截图



| 用户名称                    | 认证类型     | 终端IP          | 终端MAC             | RADIUS服务器 | 接入时间                |
|-------------------------|----------|---------------|-------------------|-----------|---------------------|
| spwajzmc33d9f9w_1r_jey  | 访客: 微信认证 | 192.168.0.195 | CO-A8-00-99-FF-FF | RDC_213   | 2018-04-01 14:20:04 |
| 192.168.0.115           | 访客: 免认证  | 192.168.0.115 | CO-A8-00-79-FF-FF | RDC_213   | 2018-04-01 14:15:50 |
| 192.168.0.61            | 访客: 免认证  | 192.168.0.61  | CO-A8-00-10-FF-FF | RDC_213   | 2018-04-01 14:14:09 |
| spwajz73c9d9smjrsqgfmh8 | 访客: 微信认证 | 192.168.0.68  | CO-A8-00-44-FF-FF | RDC_213   | 2018-04-01 14:13:43 |
| 192.168.0.133           | 访客: 免认证  | 192.168.0.133 | CO-A8-00-05-FF-FF | RDC_213   | 2018-04-01 14:09:31 |
| spwajzmc33d9f9w_1r_jey  | 访客: 微信认证 | 192.168.0.135 | CO-A8-00-07-FF-FF | RDC_213   | 2018-04-01 14:09:28 |
| 192.168.0.190           | 访客: 免认证  | 192.168.0.190 | CO-A8-00-18-FF-FF | RDC_213   | 2018-04-01 14:09:27 |
| 192.168.0.92            | 访客: 免认证  | 192.168.0.92  | CO-A8-00-5C-FF-FF | RDC_213   | 2018-04-01 14:08:18 |
| 192.168.0.240           | 访客: 免认证  | 192.168.0.240 | CO-A8-00-F0-FF-FF | RDC_213   | 2018-04-01 14:07:48 |

## 1、WX3540E无线控制器配置需要注意的是还需要放通固定的一些地址段

portal服务器的IP地址、华三控制器的通信IP地址、网关地址、以及整个认证网段(这样表示无线进行免认证, 只是重定向url即可)

## 2、需要保证无线控制器与Portal服务器之间联通。