无感知Portal + SAM服务器对接配置指导（V7）

Portal 陈少华 2017-12-28 发表

一、 Portal无感知方案简介

什么叫做Portal无感知认证？ 从用户体验的角度来看，就是用户首次上网时打开浏览器需要输入用户名和密码进行次认证，后续不需要输入用户名密码就能直接上网的认证方案。相当于“一次输入，永久使用”，当然这个永久是相对来说的，服务器可以控制这个时间。

当前Portal无感知方案的种类较多，主要表现为以下几种：

（1） 中国移动的Portal Mac-Trigger无感知认证方案

（2） Portal和MAC认证混合认证的无感知认证方案

（3） Portal服务器利用网页技巧实现的无感知认证方案

（4） AC内置的Portal无感知认证方案 （无须服务器，完全本地认证）

当前锐捷SAM服务器支持的无感知认证方案为第二种，也即Portal和MAC认证的无感知认证方案，该方案的具体实现原理为：

用户首次连接：

（1） 无线Client连接到AP，先触发MAC地址认证，服务器检查该MAC地址为首次认证，返回给设备认证失败；

（2） 设备发现该MAC地址认证失败，如果配置了client-security ignore-Authentication命令行，则保持client无线连接为正常状态；

（3） 用户浏览器触发http报文，Portal检查该用户没有MAC认证通过，则触发Portal认证；

（4） Portal认证成功，服务器记录该MAC地址的绑定表项，通常都是Portal sevrer跟Radius server联动，Radius server创建对应的MAC账号；

用户再次连接时：

（1） 无线Client连接到AP，先触发MAC地址认证，服务器检查该MAC地址绑定表项已经存在，返回认证成功。

（2） 用户MAC认证成功。

（3） 用户浏览器触发http报文，Portal检查该用户MAC地址认证通过，直接放行该用户的报文，不触发Portal认证。

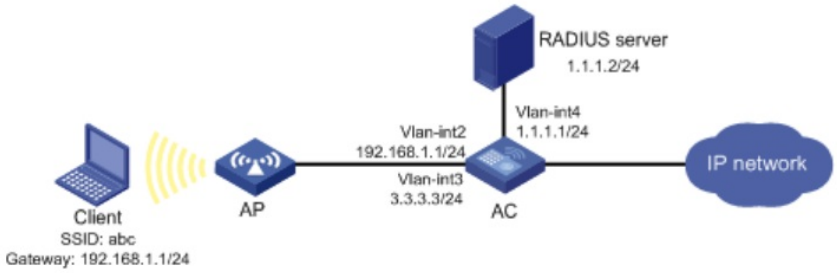
二、 配合 SAM的配置关键点

组网需求：

无线客户端通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限互联网资源。

采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。采用 RADIUS 服务器作为认证/计费服务器。

组网图：



配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案。

[AC]radius scheme rs1

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

[AC-radius-rs1]primary authentication 192.168.0.112

[AC-radius-rs1]primary accounting 192.168.0.112

[AC-radius-rs1]key authentication simple xxxxxx

[AC-radius-rs1]key accounting simple xxxxxx

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

[AC-radius-rs1]user-name-format without-domain

创建并进入名称为 dm1 的 ISP 域。

[AC] domain dm1

配置 ISP 域的 AAA 方法。

[AC-isp-dm1]authentication portal radius-scheme rs1

[AC-isp-dm1]authorization portal radius-scheme rs1
[AC-isp-dm1]accounting portal radius-scheme rs1
[AC-isp-dm1]authentication lan-access radius-scheme rs1
[AC-isp-dm1]authorization lan-access radius-scheme rs1
[AC-isp-dm1]accounting lan-access radius-scheme rs1

配置Portal认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文portal，监听 Portal 报文的端口为 50100（默认值）。
SAM 用的是 CMCC 方式，必须配置正确
[AC]portal server newpt
[AC-portal-server-newpt]ip 192.168.0.111
[AC-portal-server-newpt]server-type cmcc
配置 Portal Web 服务器的 URL 以及 URL 参数。
下面几个 URL 参数是实测得来的，就是 CMCC 的典型关键字。具体项目也可能会有变化，根据 SAM 要求配置。
[AC]portal web-server newpt
[AC-portal-websvr-newpt]url http://192.168.0.111/portal
[AC-portal-websvr-newpt]url-parameter wlanacname value H3C-AC
[AC-portal-websvr-newpt]url-parameter wlanuserip source-address
[AC-portal-websvr-newpt]url-parameter ssid ssid
在无线服务模板上开启直接方式的 Portal 认证。
Portal 必须在无线服务模板下使能，不要在 VLAN 接口下使能
[AC–wlan-st-newst]portal enable method direct
在无线服务模板上引用 Portal Web 服务器 newpt。
[AC–wlan-st-newst]portal apply web-server newpt
配置无线服务模板 Portal 认证域
[AC–wlan-st-newst]portal domain dm1
配置CMAC地址认证
配置全局的端口安全。
[AC] port-security enable
配置 MAC 地址认证用户名格式为 mac 地址格式，不带连字符，小写。这个格式是固定的
[AC]mac-authentication user-name-format mac-address without-hyphen lowercase
配置无线服务模板的 MAC 地址认证功能。
[AC–wlan-st-newst]client-security authentication-mode mac
配置无线服务模板的忽略认证结果认证功能
非常关键，必须配置
[AC–wlan-st-newst]client-security ignore-authention
配置无线服务模板 MAC 地址认证域为 dm1
[AC–wlan-st-newst]mac-authentiion domain dm1