MSR上的Portal直接认证配置

王锐 2012-07-30 发表

MSR上的Portal直接认证配置

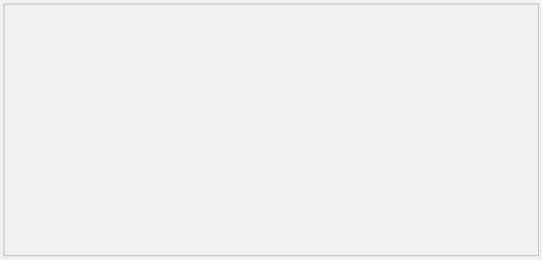
一、 组网需求：

1、用户主机与接入设备Router直接相连，采用直接方式的Portal认证。用户通过手工配置或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服务器；在通过Portal认证后，可以使用此IP地址访问非受限的互联网资源。

2、采用RADIUS服务器作为认证/计费服务器。

二、 组网图：

图1配置Portal直接认证组网图



三、 配置步骤：

(1) 配置Portal server

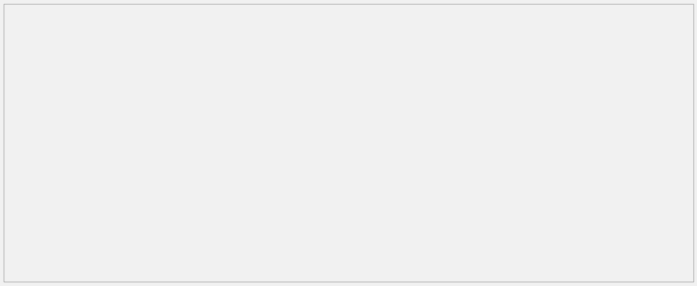
下面以iMC为例（使用iMC版本为：iMC PLAT 3.20-R2602P13、iMC UAM 3.60-E6301），说明Portal server的基本配置。

配置Portal服务器。

登录进入iMC管理平台，选择“业务”页签，单击导航树中的[Portal服务器管理/服务器配置]菜单项，进入服务器配置页面。

l 根据实际组网情况调整以下参数，本例中使用缺省配置。

图2 Portal服务器配置页面



配置IP地址组。

单击导航树中的[Portal服务器管理/IP地址组配置]菜单项，进入Portal IP地址组配置页面，在该页面中单击<增加>按钮，进入增加IP地址组配置页面。

l 填写IP地址组名；

l 输入起始地址和终止地址。用户主机IP地址必须包含在该IP地址组范围内；

l 选择业务分组，本例中使用缺省的“未分组”；

l 选择IP地址组的类型为“普通”。

图3增加IP地址组配置页面

增加Portal设备。

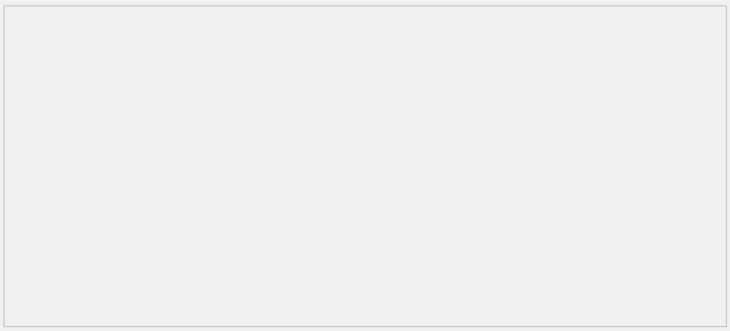
单击导航树中的[Portal服务器管理/设备配置]菜单项，进入Portal设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

l 填写设备名；

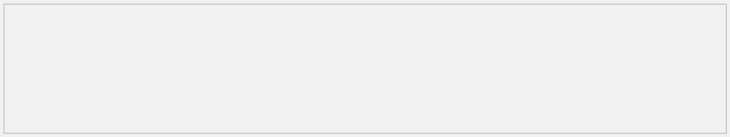
l 指定IP地址为与接入用户相连的设备接口IP；

l 输入密钥，与接入设备Router上的配置保持一致；

l 选择是否进行二次地址分配，本例中为直接认证，因此为否；
l 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。
图4 增加设备信息配置页面



Portal设备关联IP地址组
在Portal设备配置页面中的设备信息列表中，点击NAS设备的<端口组信息管理>链接，进入端口组信息配置页面。
图5 设备信息列表



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。
l 填写端口组名；
l 选择IP地址组，用户接入网络时使用的IP地址必须属于所选的IP地址组；
l 其它参数采用缺省值。
图6 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上Portal服务器配置生效。
(2)配置Router
l 配置RADIUS方案
创建名字为rs1的RADIUS方案并进入该方案视图。
<Router> system-view
[Router] radius scheme rs1
配置RADIUS方案的服务器类型。使用CAMS/iMC服务器时，RADIUS服务器类型应选择extended。
[Router-radius-rs1] server-type extended
配置RADIUS方案的主认证和主计费服务器及其通信密钥。
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key authentication radius
[Router-radius-rs1] key accounting radius
配置发送给RADIUS服务器的用户名不携带ISP域名。
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
l 配置认证域
创建并进入名字为dm1的ISP域。
[Router] domain dm1
配置ISP域使用的RADIUS方案rs1。
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1

[Router-isp-dm1] quit
配置系统缺省的ISP域dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带ISP域名，则使用缺省域下的认证方案。
[Router] domain default enable dm1
l 配置Portal认证
配置Portal服务器：名称为newpt，IP地址为192.168.0.111，密钥为portal，端口为50100，URL为http://192.168.0.111:8080/portal。（Portal服务器的URL请与实际环境中的Portal服务器配置保持一致，此处仅为示例）
[Router] portal server newpt ip 192.168.0.111 key portal port 50100 url http://192.168.0.111:8080/portal
在与用户Host相连的接口上使能Portal认证。
[Router] interface ethernet 1/2
[Router–Ethernet1/2] portal server newpt method direct
[Router–Ethernet1/2] quit
四. 验证配置结果
以上配置完成后，通过执行以下显示命令可查看Portal配置是否生效。
[Router] display portal interface ethernet 1/2
Interface portal configuration:
Ethernet1/2: Portal running
Portal server: newpt
Authentication type: Direct
Authentication domain:
Authentication network:
address : 0.0.0.0 mask : 0.0.0.0
用户既可以使用H3C的iNode客户端，也可以通过网页方式进行Portal认证。用户在通过认证前，只能访问认证页面http://192.168.0.111:8080/portal，且发起的Web访问均被重定向到该认证页面，在通过认证后，可访问非受限的互联网资源。
认证通过后，可通过执行以下显示命令查看Router上生成的Portal在线用户信息。
[Router] display portal user interface ethernet 1/2
Index:19
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC IP Vlan Interface

0015-e9a6-7cfe 2.2.2.2 0 Ethernet1/2
On interface Ethernet1/2:total 1 user(s) matched, 1 listed.
五、 配置关键点
1、 按照组网图配置设备各接口的IP地址，保证启动Portal之前各主机、服务器和设备之间的路由可达。
2、完成RADIUS服务器上的配置，保证用户的认证/计费功能正常运行。