远程portal配置案例

Portal iMC AP管理 王波 2020-04-27 发表

组网及说明

1. **配置需求和说明**

1.1介绍

通用portal认证不包含任何接入控制和安全检查，用户身份验证后便可接入网络。

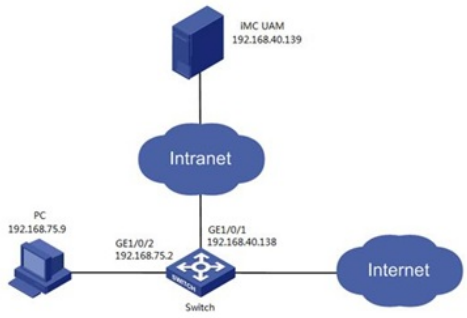
1.2使用场景

适用于需要portal认证的企业网或校园网等等。

2组网图

某公司计划启用Portal认证，用户接入网络时需要进行身份验证，具体的组网如图1所示。UAM服务器IP地址为192.168.40.139，接入设备用户侧GigabitEthernet1/0/2接口的IP地址为192.168.75.2。PC的IP地址为192.168.75.9，安装了Windows操作系统，并准备安装iNode客户端。

图1组网图



配置步骤

3.配置步骤

3.1配置 iMC 服务器

3.1.1. 增加接入设备

增加接入设备的方法如下：

(1)选择“用户”页签，单击导航树中的“接入策略管理 > 接入设备管理 > 接入设备配置”菜单项，进入接入设备配置页面，如图2所示。

图2 接入设备配置页面

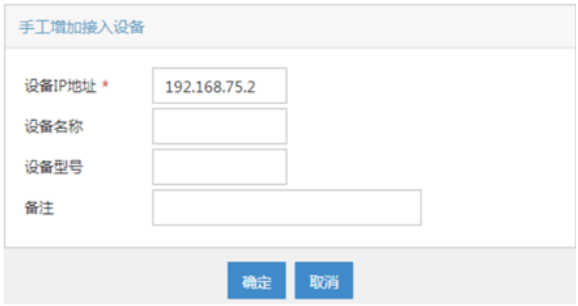
单击<增加>按钮，进入增加接入设备页面，如图3所示。

图3 增加接入设备

(3)配置接入设备。

配置接入设备有两种方法：

·在设备列表中单击<选择>按钮从iMC平台中选择设备。
·在设备列表中单击<手工增加>按钮，手工配置接入设备。
无论采用哪种方式接入设备的IP地址都必须满意以下要求：
·如果在接入设备上配置radius scheme时配置了nas ip命令，则UAM中接入设的IP地址必须与nas ip的配置保持一致。
· 如果未配置nas ip命令，则UAM中接入设备的IP地址必须是设备连接UAM服务器的接口IP地址（或接口所在VLAN的虚接口IP地址）。
从iMC平台中选择设备时，设备的IP地址无法修改。因此如果设备加入iMC平台时使用的IP地址不满足上述要求，则可以采用手工增加的方式增加接入设备。本例采用手工增加的方式进行说明。
单击设备列表中的<手工增加>按钮，弹出手工增加接入设备窗口，如图4所示。输入接入设备的IP地址，单击<确定>按钮，返回增加接入设备页面。
图4 手工增加接入设备

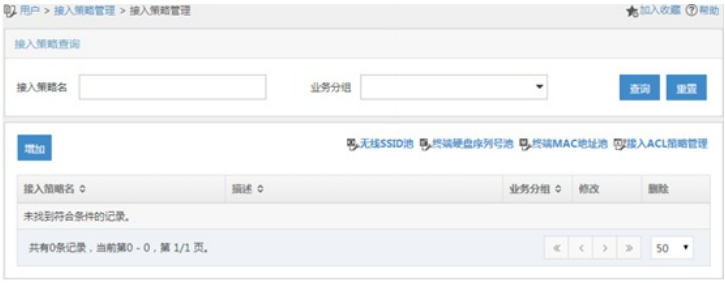


(4)　配置公共参数。
公共参数的配置要求如下：
·认证端口：UAM监听RADIUS认证报文的端口。此处的配置必须与接入设备命令行配置的认证端口保持一致。UAM和接入设备一般都会采用默认端口1812。
·计费端口：UAM监听RADIUS计费报文的端口。此处的配置必须与接入设备命令行配置的计费端口保持一致。UAM和接入设备一般都会采用默认端口1813。
本例中公共参数只需要输入共享密钥\确认共享密钥“movie”，其他保持默认即可，如图5所示。
图5 配置公共参数

(5)　单击<确定>按钮，增加接入设备完毕，进入结果显示页面。点击“返回接入设备列表”链接，返回接入设备配置页面，可在接入设备列表中查看新增的接入设备，如图6所示。
图6 查看新增的接入设备

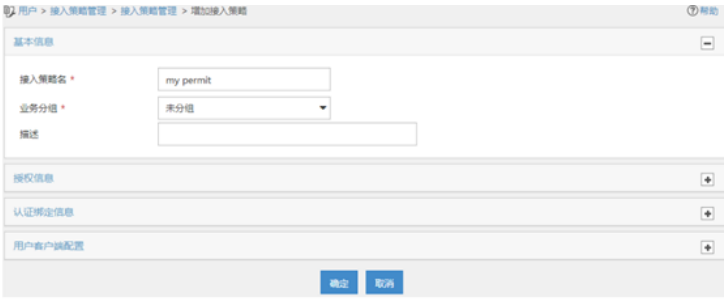
3.1.2. 增加接入策略

配置一个不进行任何接入控制的接入策略。
增加接入策略的方法如下：
(1)　选择“用户”页签，单击导航树中的“接入策略管理 > 接入策略管理”菜单项，进入接入策略管理页面，如图7所示。
图7 接入策略管理



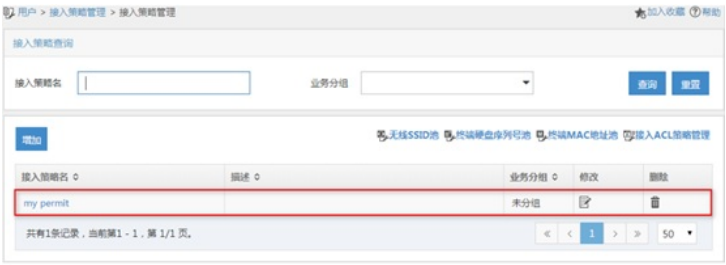
(2)　单击<增加>按钮，进入增加接入策略页面，如图8所示。由于不需要任何接入控制，所以只需输入接入策略名，其他参数保持默认即可。

图8 增加接入策略



(3)单击<确定>按钮，接入策略增加完毕。返回接入策略管理页面，可在接入策略列表中查看新增的接入策略，如图9所示。

图9 查看新增的接入策略



3. 增加接入服务

接入服务是对用户进行认证授权的各种策略的集合。本例不对用户进行任何接入控制，因此只需增加一个简单的接入服务即可。

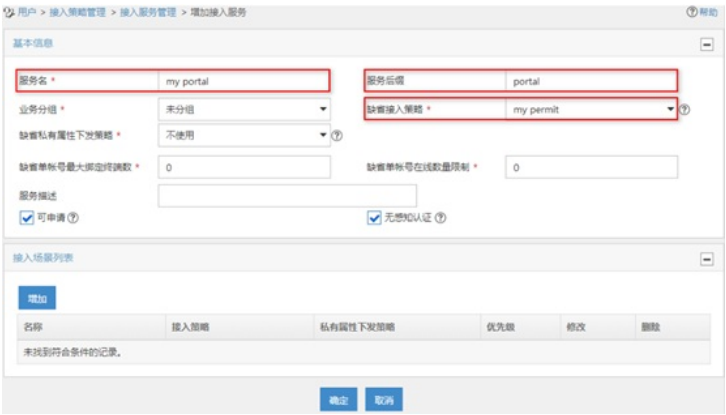
增加接入服务的方法如下：

(1)　选择“用户”页签，单击导航树中的“接入策略管理 > 接入服务管理”菜单项，进入接入服务管理页面，如图10所示。

图10 接入服务管理

(2)　单击<增加>按钮，进入增加接入服务页面，如图11所示。

图11 增加接入服务



认证连接用户名	设备用于认证的Domain	设备Radius scheme中的命令	iMC中服务的后缀

X@Y	Y	user-name-format with-domain	Y
		user-name-format without-domain	无后缀
X	[Default Domain]设备上指定的缺省域	user-name-format with-domain	[Default Domain]
		user-name-format without-domain	无后缀

配置服务的各个参数：

·服务名：输入服务名称，在UAM中必须唯一。

·服务后缀：服务后缀、认证连接的用户名、设备的Domain和设备Radius scheme中的命令这四个要素密切相关，具体的搭配关系请参见表1。

·缺省接入策略：选择之前新增的接入策略。

·其他参数：保持缺省值。

表1 iMC中服务后缀的选择

(3)　单击<确定>按钮，完成增加接入服务。返回接入服务管理页面，可在接入服务列表中查看新增的接入服务，如图12所示。

图12 查看新增的接入服务

3.1.3. 增加接入用户

(1)　选择“用户”页签，单击导航树中的“接入用户管理 > 接入用户”菜单项，进入接入用户页面，如图13所示。

图13 接入用户

(2)　单击<增加>按钮，进入增加接入用户页面，如图14所示。

图14 增加接入用户

(3)　配置接入信息和接入服务：

l 用户姓名：单击<选择>或<增加用户>按钮，在iMC平台中选择或手动增加一个用户。

l 单击<选择>按钮，弹出选择用户窗口。单击<查询>按钮，可以查询出所有已存在的平台用户，如图15所示，选择一个用户后单击<确定>按钮。

l 单击<增加用户>按钮，弹出增加用户窗口，如图16所示，输入用户名、证件号码以及其他参数后单击<确定>按钮。

图15 选择平台用户

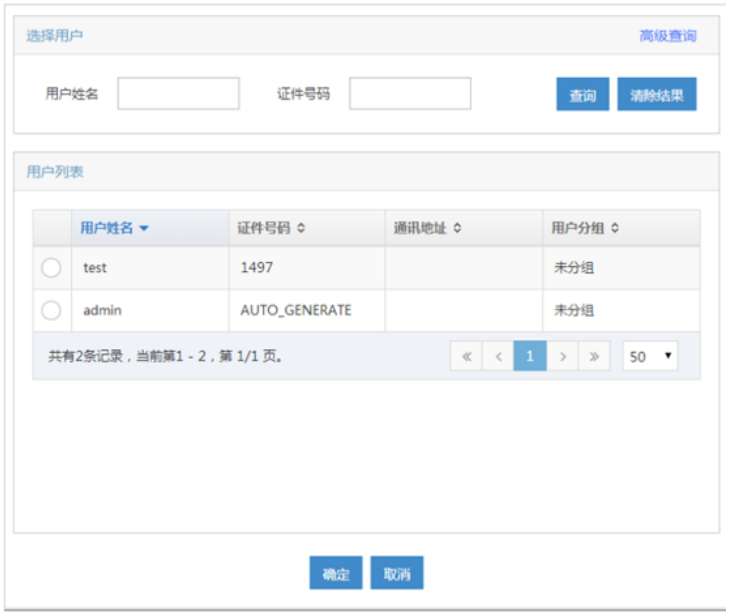


图16 新增平台用户

·帐号名：输入用于认证的帐号名，在UAM中必须唯一。

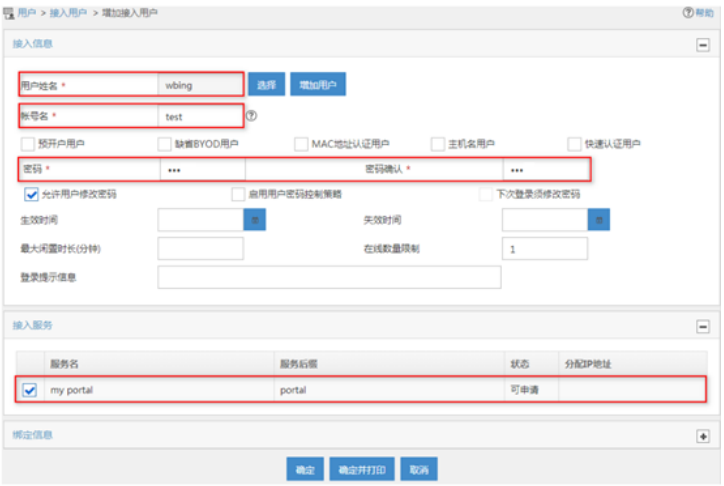
·密码/确认密码：输入两次相同的密码。

·接入服务：选择之前增加的接入服务。

·其他参数：保持缺省值。

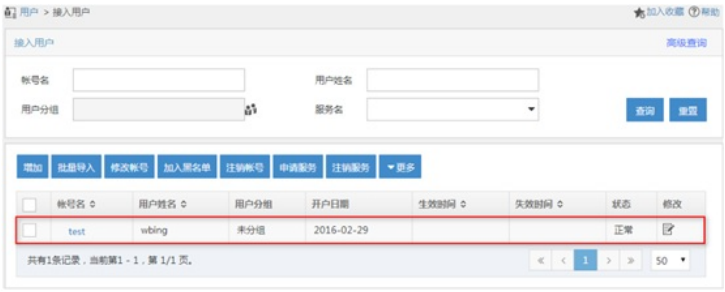
参数设置完成后的效果图如图17所示。

图17 接入用户配置信息



(4)　单击<确定>按钮，完成增加接入用户，返回接入用户页面。可在接入用户列表中查看新增的接入用户，如图18所示。

图18 查看新增的接入用户



3.2 配置Portal服务

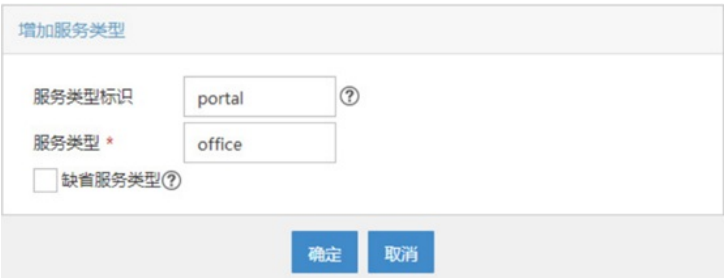
3.2.1. 服务器配置

(1) 选择“用户”页签，单击导航树中的“接入策略管理 > Portal服务管理 > 服务器配置”菜单项，进入服务器配置页面，如图19所示。

图19 服务器配置

(2) 在服务类型列表中，单击<增加>按钮，弹出增加服务类型窗口，如图20所示。

图20 增加服务类型



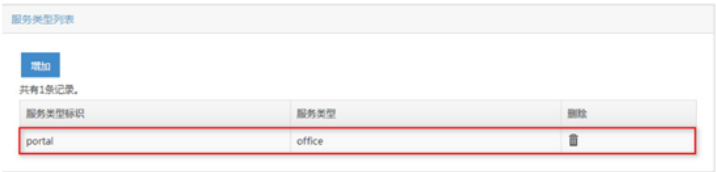
(3) 输入服务类型标识和服务类型。

·服务类型标识必须与之前增加服务的服务后缀相同。

·服务类型是对服务类型标识的说明和区分。

(4) 单击<确定>按钮，完成增加服务类型。返回服务器配置页面。可在服务类型列表中查看新增的服务类型，如图21所示。

图21 查看新增的服务类型



(5) 单击<确定>按钮，完成Portal服务器配置。

3.2.2. IP地址组配置

(1) 选择“用户”页签，单击导航树中的“接入策略管理 > Portal服务管理 > IP地址组配置”菜单项，进入IP地址组配置页面，如图22所示。

图22 IP地址组配置

(2)　单击<增加>按钮，进入增加IP地址组页面，如图23所示。

图23 增加IP地址组

(3)　输入IP地址组名“portal_test”，起始地址192.168.75.1和终止地址192.168.75.254。IP地址属于该地址段的终端都要进行认证。

(4)　单击<确定>按钮，完成增加IP地址组，返回IP地址组配置页面。可在IP地址组列表中查看新增的IP地址组，如图24所示。

图24 查看新增的IP地址组

3.2.3. 设备配置

(1)　选择“用户”页签，单击导航树中的“接入策略管理 > Portal服务管理 > 设备配置”菜单项，进入设备配置页面，如图25所示。

图25 设备配置

(2)　单击<增加>按钮，进入增加设备信息页面，如图26所示。

图26 增加设备信息

(3) 配置如下信息：

·设备名：输入设备名称“device_Portal”。

·IP地址：输入设备的IP地址“192.168.75.2”。

·密钥\确认密钥：输入“expert”。密钥要与设备上配置的Portal服务器密钥保持一致。

·组网方式：在下拉框中选择“直连”。

·其他参数：保持默认值。

(4) 单击<确定>按钮，完成增加设备信息。返回设备配置页面，可在列表中查看新增的设备信息，如图27所示。

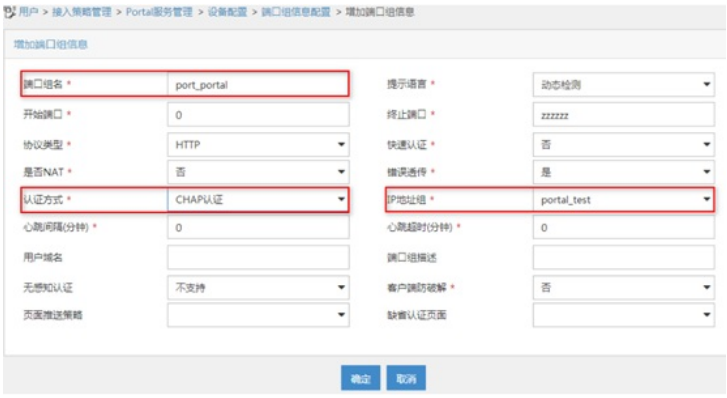
图27 查看新增的设备信息

(5) 在设备信息列表中，单击操作列的端口组信息管理图标，进入端口组信息配置页面，如图28所示。

图28 端口组信息配置

(6) 单击<增加>按钮，进入增加端口组信息页面，如图29所示。

图29 增加端口组信息



(7) 配置端口组信息：

·端口组名：输入端口组的名称“port_portal”。

·认证方式：在下拉框中选择“CHAP认证”。

·IP地址组：选择之前配置的“portal_test”。

·其他参数：保持默认值。

(8) 单击<确定>按钮，完成增加端口组信息。返回端口组信息配置页面，可在端口组信息配置列表

中查看新增的端口组信息，如图30所示。
图30 查看新增的端口组信息

3.3配置接入设备

接入设备用于控制用户的接入。通过认证的用户可以接入网络，未通过认证的用户无法接入网络。
以下使用Windows的CLI窗口telnet到接入设备并进行配置，具体的命令及其说明如下：
(1)　进入系统视图。
<Device>system-view
System View: return to User View with Ctrl+Z.
(2)　配置RADIUS策略“allpermit”。认证、计费服务器均指向UAM。认证端口、计费端口、共享密钥要与UAM中增加接入设备时的配置保持一致。
[Device]radius scheme allpermit
New Radius scheme
[Device-radius-allpermit]primary authentication 192.168.40.139 1812
[Device-radius-allpermit]primary accounting 192.168.40.139 1813
[Device-radius-allpermit]key authentication simple movie
[Device-radius-allpermit]key accounting simple movie
[Device-radius-allpermit]user-name-format with-domain
[Device-radius-allpermit]nas-ip 192.168.75.2
[Device-radius-allpermit]quit
(3)　配置domain域“portal”，引用配置好的“allpermit”策略。domain的名称必须与UAM中服务的后缀保持一致。
[Device]domain portal
New Domain added.
[Device-isp-portal]authentication portal radius-scheme allpermit
[Device-isp-portal]authorization portal radius-scheme allpermit
[Device-isp-portal]accounting portal radius-scheme allpermit
[Device-isp-portal]quit
(4)　配置Portal认证服务器：名称为myportal，IP地址指向UAM，key要与UAM上的配置一致。
[Device]portal server myportal
[Device-portal-server-myportal]ip 192.168.40.139 key simple expert
[Device-portal-server-myportal]quit
(5)　配置Portal Web服务器的URL为http://192.168.40.139:8080/portal，要与UAM上的配置一致。
[Device]portal web-server myportal
[Device-portal-websvr-myportal]url http://192.168.40.139:8080/portal
[Device-portal-websvr-myportal]quit
(6)　在接口GigabitEthernet1/0/2上开启直接方式的Portal，引用Portal Web服务器 myportal，设置发送给Portal认证服务器的Portal报文中的BAS-IP属性值。
[Device]interface gigabitethernet 1/0/2
[Device-gigabitethernet1/0/2]portal enable method direct
[Device-gigabitethernet1/0/2] portal apply web-server myportal
[Device-gigabitethernet1/0/2]portal bas-ip 192.168.75.2
[Device-gigabitethernet1/0/2]quit
4.使用inode客户端完成portal接入认证
用户使用iNode PC客户端和配置的帐号名、密码进行Portal认证，最终用户通过认证，完成Portal接入。
验证步骤如下：
4.1. 安装具有Portal接入功能的iNode客户端
iNode客户端版本必须与iMC UAM配套，具体的配套关系请参见UAM版本说明书。
4.2. 进行Portal认证连接
(1)　在iNode PC客户端主页面，选择“Portal连接”，展开Portal连接区域，如图31所示。
图31 iNode客户端主界面

(2)　点击服务器文本框右侧的“刷新”图标，iNode客户端会获取Portal服务器信息，获取成功后服务器信息自动填充在文本框中，如图32所示。

图32 成功获取服务器信息

(3)　输入用户名和密码，选择服务类型为office后，单击<连接>按钮，如图33所示，开始进行Portal认证。

图33 Portal认证页面

认证成功的界面如图34所示，验证了本案例的配置正确。

图34 Portal认证成功


En
iNode智能客户端
Portal连接
服务器
192.168.40.139
当前用户
test@portal
连接状态
已连接
安全状态
不需要检查
上线时间
2016-3-1 15:36:14
断 开
802.1X连接
SSL VPN连接
无线连接
我的场景

配置关键点