

知 ADCampus 三期B02宝鸡行政中心全网静态ip地址配置指导

ADCampus解决方案 詹继峰 2020-08-25 发表

组网及说明

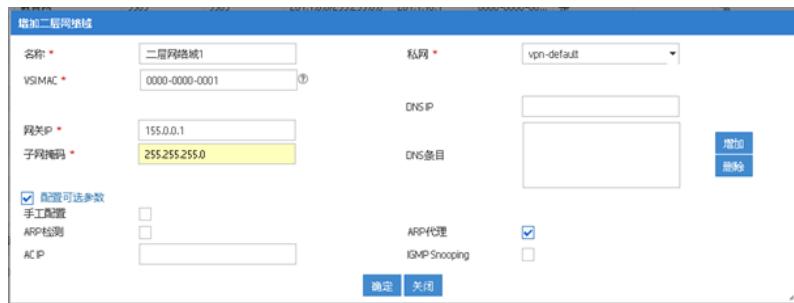
三期B02标准组网

配置步骤

每个业务组单独配置一个安全组，（安全组一、安全组二、安全组三、安全组n），针对每个安全组的ip网段增加相应个数量的接入场景，然后将这些应用场景都应用到byod安全组下。

下面以其中一个名为“安全组1”的安全组为例进行配置，具体配置步骤如下

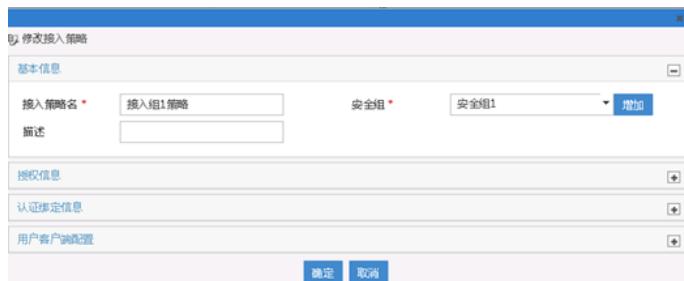
一、创建一个二层网络域，名字为“二层网络域1”，私网这里选择这个二层网络域对应要创建在哪个“私网”下即可，这里想创建在vpn-default下，所以选择vpn-default私网。



二、增加一个安全组，名字为“安全组1”，因为终端都是静态配置ip地址的，所以不用勾选DHCP。



三、增加一个接入组，名字为“接入组1”，接入策略绑定到安全组1：



四、接入条件管理à终端ip地址分组中，增加一个基于终端ip的接入场景，名字为“二层网络域1静态ip场景”：

增加终端IP地址分组

终端IP地址分组名 * 二层网络域1静态ip场景

起始地址 * 155.0.0.1

终止地址 * 155.0.0.254

确定 **取消**

五、在接入策略中，创建一个名字为“二层网络域1静态ip策略”，并且选择“安全组1”

增加接入策略

基本信息

接入策略名 * 二层网络域1静态ip策略 安全组 * 安全组1 **增加**

描述

授权信息

认证绑定信息

用户客户端配置

确定 **取消**

六、在byod接入组中，增加一个名字为“二层网络域1接入场景”，选择前面创建的接入策略和终端ip地址分组：

增加接入场景

接入场景名称 * 二层网络域1接入场景

接入条件

接入位置分组 (where , how) *	不限	增加
SSD分组 (where , how) *	不限	增加
终端ip地址分组 (whose) *	二层网络域1静态ip场景	增加
终端MAC地址分组 (whose) *	不限	增加
终端厂商分组 (what) *	不限	增加
终端操作系统分组 (what) *	不限	增加
终端机型分组 (what) *	不限	增加
AP分组 (where , how) *	不限	增加
接入时段策略 (when) *	不限	增加

接入策略

接入策略 * 二层网络域1静态ip策略 **增加**

安全组 安全组1

单帐号最大绑定终端数 * 0

单帐号在线数量限制 * 0

确定 **取消**

创建成功后，结果如下：

修改接入组

基本信息

接入组名 * byod 服务归属

缺省接入策略 * byod 增加 缺省单帐号在线数量限制 * 0

单日累计在线最长时间 (分钟) * 0

描述 无源认证

接入场景列表

增加

名称	接入策略	优先级	修改	删除
二层网络域1接入场景	二层网络域1静态ip策略	普通	<input checked="" type="checkbox"/>	<input type="checkbox"/>

确定 **取消**

增加接入用户

插入信息

用户名 * 静态用户1 **添加** **启用用户**

账号名 * 静态用户1

密码 * **...** 密码确认 * **...**

有效时间 **...** 失效时间 **...** 可用数量限制 1

最大闲置时长(分钟) 0

登录提示信息

插入组

服务名	服务所属	状态
byod	缺省	可编辑
t1	缺省	可编辑
t2	缺省	可编辑
h3c	h3c	可编辑
h3c接入组	h3c	可编辑
开心土豆	缺省	可编辑
张三	缺省	可编辑
<input checked="" type="checkbox"/> 接入组1	缺省	可编辑
静态上网接入组	缺省	可编辑

绑定信息

端口号 **...** 端口范围 **...**

计算机名称 **...** MAC地址 **...**

确定 **确定并应用** **取消**

注意：在文本框中输入多条信息时，每行只能输入一条信息。

激活 WinRAR
找到并解压缩

七、创建一个账号“静态用户1”，并绑定到“接入组1”

八、终端在mac认证中要携带用户ip地址，才能被接入场景ip匹配成功，这就需要在对应leaf下行口配

置mac-authentication carry user-ip，如果终端会移动到其它leaf下行口，则其它leaf下行口也要配置：

```
[leaf-GigabitEthernet1/0/1]dis this
```

```
#
```

```
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan all
port-isolate enable group 1
qos apply policy zwn inbound
qos apply policy zwn outbound
mac-based ac
dot1x
mac-authentication
mac-authentication carry user-ip
mac-authentication domain h3c
port-security free-vlan 1 3503 to 3504 3506 to 3509 3511 to 3515 4094
#
```

验证结果

1、使用一台静态配置ip地址为155.0.0.15的电脑接入access，在leaf的动态AC可以看到终端进入了对应的安全组，并且下发了授权url和acl：

```
[leaf-GigabitEthernet1/0/1]dis mac-au con
```

Total connections: 1

Slot ID: 1

User MAC address: 0cda-411d-4be6

Access interface: GigabitEthernet1/0/1

Username: 0cda411d4be6

User access state: Successful

Authentication domain: h3c

IPv4 address: 155.0.0.15

Initial VLAN: 101

Authorization untagged VLAN: N/A

Authorization tagged VLAN: N/A

Authorization VSI: vsi3515

Authorization ACL ID: 3001

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: http://110.0.5.93:8080/byod?usermac=%m&userip=%c&userurl=%o

Termination action: Default

Session timeout period: 86400 s

Online from: 2013/01/15 00:21:20

Online duration: 0h 0m 30s

在Director侧查看在线用户也可以看到：

2、终端随意打开1.1.1.1网站，成功跳转到认证页面，输入“静态用户1”的用户名密码后上线成功：

在leaf上也可以看到认证上线了：

用户信息	
终端类型	H3C
厂商	H3C
操作系统	Windows 8.1
MAC地址	0C DA 41 1D 4B E6

```
[leaf-GigabitEthernet1/0/1]dis mac-au con
Total connections: 1
Slot ID: 1
User MAC address: 0cda-411d-4be6
Access interface: GigabitEthernet1/0/1
Username: 0cda411d4be6
User access state: Successful
Authentication domain: h3c
IPv4 address: 155.0.0.15
Initial VLAN: 101
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: vsi3515
Authorization ACL ID: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 86400 s
Online from: 2013/01/15 00:28:24
Online duration: 0h 0m 4s
在Director上在线用户也可以看到认证通过后正确上线了：
```

3. 验证终端移动的场景，移动前在access的g1/0/1,所在接口vlan为101，此时上线成功：

后续这台电脑随意挪到了access接口的g1/0/2，所在vlan为102，不用重新认证，能够无感知上线：

配置关键点

carry user-ip配置优化

每个leaf下行口都需要手工下发mac-authentication carry user-ip，这个太麻烦，可以在imc自定义leaf下行口策略，统一自动下发。步骤如下：

1、业务—通用—自定义动作，添加这个动作：

增加自定义动作 - Google Chrome
① 192.168.1.15:8080/imc/campus/commgroup/actionUserDefined_content.xhtml

自定义动作	
动作名称 *	carry user-ip
动作类型 *	接口类
动作描述	
动作内容 *	mac-authentication carry user-ip
可恢复	<input checked="" type="checkbox"/>
恢复动作内容 *	undo mac-authentication carry user-ip
确定 关闭	

+ 增加

动作名称	动作类型	可恢复	动作描述	删除
voice vlan	接口类	是		
carry user-ip	接口类	是		删除

共有2条记录，当前第1 - 2，第 1/1 页。 < < 1 > > 50 ▾

2、在leaf下行口---组策略中添加carry user-ip这个动作：

设备组 接口组

- 提示

(1) Spine/Leaf/Access设备间的互通接口，应加入到对应角色接口分组。
(2) 增加接口到接口组时，会自动下发组策略的动作；如果加入到Leaf下行口，则同时会下发二层网域相关配置。请谨慎操作！
(3) 从组内删除接口时，会自动下发组策略的修复动作；如果从Leaf下行口删除，则同时会清除二层网域相关配置。请谨慎操作！

自动导入设备及接口	+ 增加	刷新
组名 ▲	类型 ▲	描述
Access上行接口	系统预定义	Access设备上的上行接口，需要Trunk所有VLAN。
IP电话机口组	自定义	
Leaf上行接口	系统预定义	Leaf设备上的上行接口组。
Leaf下行接口	系统预定义	Leaf设备上的下行接口组。
Spine下行接口	系统预定义	Spine设备上的下行接口组。
免认证接口组	自定义	

共有6条记录，当前第1 - 6，第 1/1 页。 < < 1 > >

Leaf下行接口 - Google Chrome
① 192.168.1.15:8080/imc/campus/strategy/info.xhtml?groupId=2&groupType=4

- 提示

Leaf下行接口，根据组网特征应配置“802.1X配置”、“MAC认证配置”动作。

+ 增加	刷新
名称	
▼ AA	
Trunk VLAN	
▼ bb	
ARP限速配置	
802.1X配置	

增加组策略 - Google Chrome
① 192.168.1.15:8080/imc/smcc/groupPolicy/ext/gpExtCfg.jsf?beanName=campusGroupStrategyBean&gpMode=0&sl

基本信息

策略名称 *

策略描述

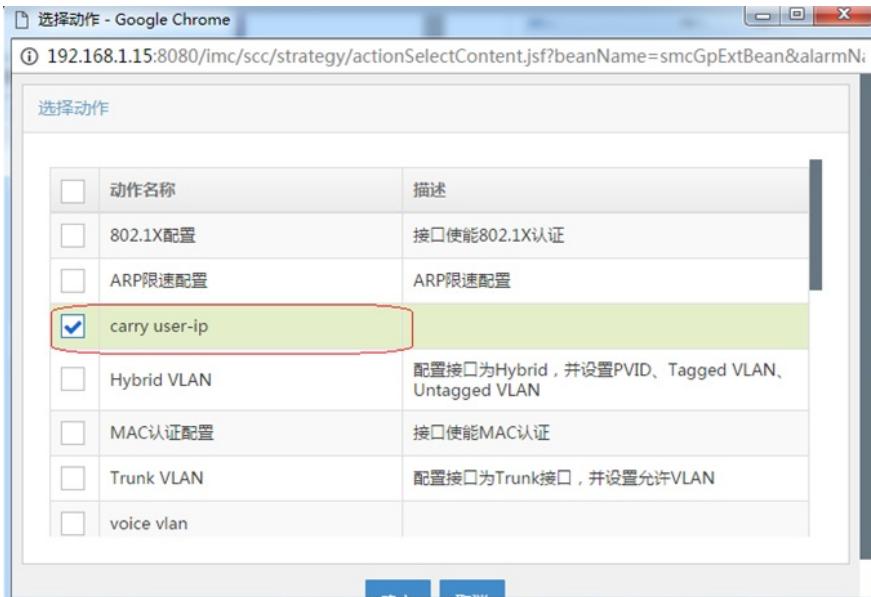
动作配置

所有动作顺序执行。但如果存在任一动作参数不合法，则所有动作均不执行。
 所有动作顺序执行，但不执行动作参数不合法的动作。
 存在一个动作执行成功即可。不执行动作参数不合法的动作。

动作列表 **选择动作**

动作名称	动作描述	可恢复	动作参数配置	排序	删除
------	------	-----	--------	----	----

未找到符合条件的记录。



4、最后查看部署结果可以看到leaf下行口自动下发成功：

接口分组部署任务信息					
组名	Leaf下行接口	已下发接口总数：	1	操作结果	全部
▼Ten-GigabitEthernet2/0/20(9.4.1.29)					
Trunk VLAN	mca	允许多 VLAN1-4094 PVID:1	2018-03-13 17:18:57	成功	
MAC认证配置	mca	域名dhc3 Guest VLAN4090	2018-03-13 17:19:32	成功	部署文件内容
接口策略配置	mca	策略组ID:1	2018-03-13 17:25:34	成功	部署文件内容
开启DHCP Snooping策略记录	mca		2018-03-13 17:26:09	成功	部署文件内容
carry user-ip	carry user-ip		2018-03-23 10:06:59	成功	部署文件内容
部署代理服务实例	test	VSI名称:vsi3502 接口策略ID:14 接口类型:Ten-GigabitEthernet2/0/20 配置类型:1502 以太网桥接规则ID:1 VLAN ID:3502 策略ID:3502 策略ARP检测配置	2018-03-13 17:08:05	成功	①
部署代理服务实例	byod	VSI名称:vsi3504 接口策略ID:14 接口类型:Ten-GigabitEthernet2/0/20 配置类型:1502 以太网桥接规则ID:1 VLAN ID:3504 策略ARP检测配置	2018-03-14 10:52:42	成功	①