

## 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p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

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

SSID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

终端类型分组 (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 策略组名

绑定接入策略 \* byod 增加 单帐号最大绑定终端数 \* 0 单帐号在线数量限制 \* 0

单帐号最大绑定终端数 \* 0 单帐号在线数量限制 \* 0

描述  无绑定认证

接入场景列表

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	1	修改	删除

确定 取消

增加接入用户

用户信息

用户名 \* 静态用户1 返回 增加用户

帐号名 \* 静态用户1

密码 \* 密码确认 \* 密码 \* 密码确认 \* 密码 \* 密码确认 \*

生效时间 生效时间

最大在线时间(分钟) 在线数量限制

登录提示信息

接入组

名称	策略名称	状态
<input type="checkbox"/> byod		可编辑
<input type="checkbox"/> s1	s1	可编辑
<input type="checkbox"/> s2	s2	可编辑
<input type="checkbox"/> h3c	h3c	可编辑
<input type="checkbox"/> h3c接入组		可编辑
<input type="checkbox"/> 禁止上网		可编辑
<input type="checkbox"/> 第三		可编辑
<input checked="" type="checkbox"/> 接入组1		可编辑
<input type="checkbox"/> 静态上网接入组		可编辑

绑定信息

端口号 无绑定

计算时延 无绑定

MAC地址

提示  
注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定 返回并打印 取消

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：

用户名	用户名	用户IP	接入方式	接入组	接入时间	设备IP	用户IP	认证状态	用户登录时间
byodanonymous	0cda411d4be6	155.0.0.15	byod	byod	2013-01-15 00:21:11	0P	155.0.0.15	无异常认证	

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：



[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

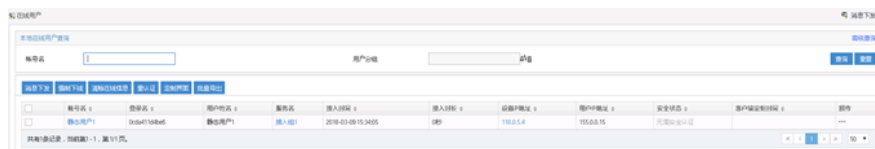
Termination action: Default

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：

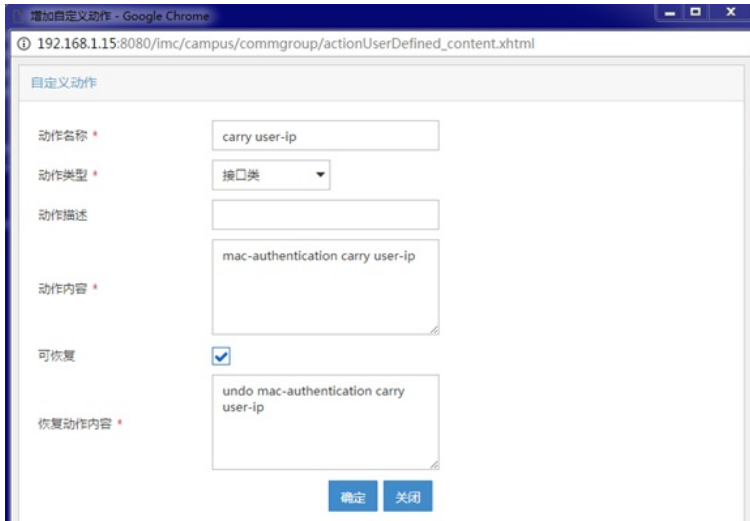


## 配置关键点

### 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、业务一通用—自定义动作，添加这个动作：

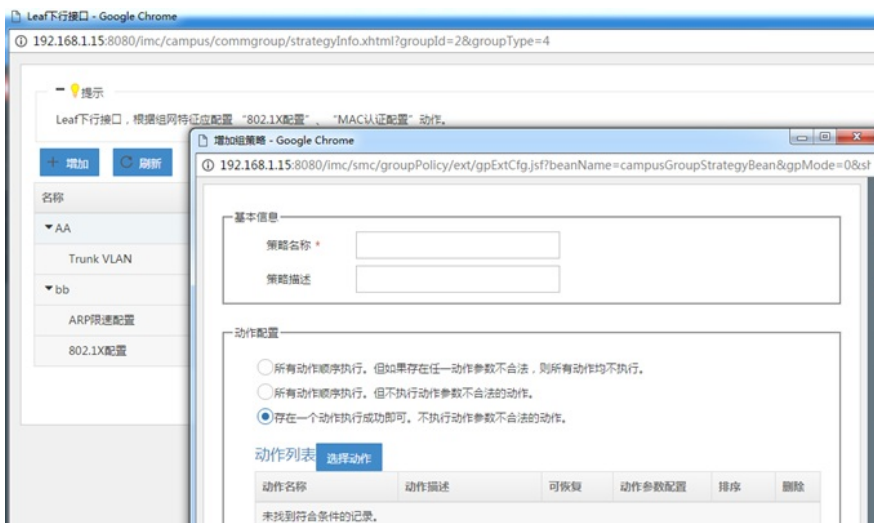


增加

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		🗑️

共有2条记录, 当前第1 - 2, 第 1/1 页。

2. 在leaf下行口---组策略中添加carry user-ip这个动作:





4. 最后查看部署结果可以看到leaf下行接口自动下发成功:

接口分租部署详情信息

接口名称	策略/二层网连接	方法参数	完成时间	操作结果	备注
▼ Ten-GigabitEthernet2/0/20(A.1.99)					
Trunk VLAN	mca	允许VLAN1-4094 PVID1	2018-03-13 17:18:57	成功	
MAC认证配置	mca	域名3c Guest VxLAN4090	2018-03-13 17:19:02	成功部署文件内容	
接口限速配置	mca	限速策略01	2018-03-13 17:25:04	成功部署文件内容	
开启DHCP Snooping事项记录	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	
部署业务实例	test	VSI名称test3502 接口策略test14 接口名称Ten-GigabitEthernet2/0/20 业务实例test3502 以本策略在策略实例testVlanId 配置允许VLAN3502 策略ARP限速策略	2018-03-13 17:38:05	成功①	
部署业务实例	byod	VSI名称test3504 接口策略test14 接口名称Ten-GigabitEthernet2/0/20 业务实例test3504 以本策略在策略实例testVlanId 配置允许VLAN3504 策略ARP限速策略	2018-03-14 10:52:42	成功①	