ADCampus 三期B02宝鸡行政中心全网静态ip地址且终端移动场景配置指导

ADCampus解决方案 詹继晔 2020-08-25 发表

组网及说明

三期B02标准组网

配置步骤

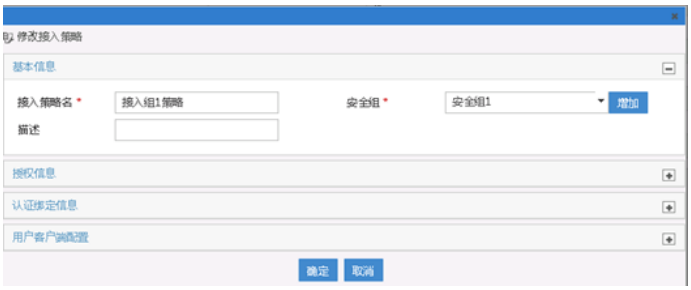
每个业务组单独配置一个安全组，（安全组一、安全组二、安全组三、安全组n），针对每个安全组的ip网段增加相应个数量的接入场景，然后将这些应用场景都应用到byod安全组下。

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。

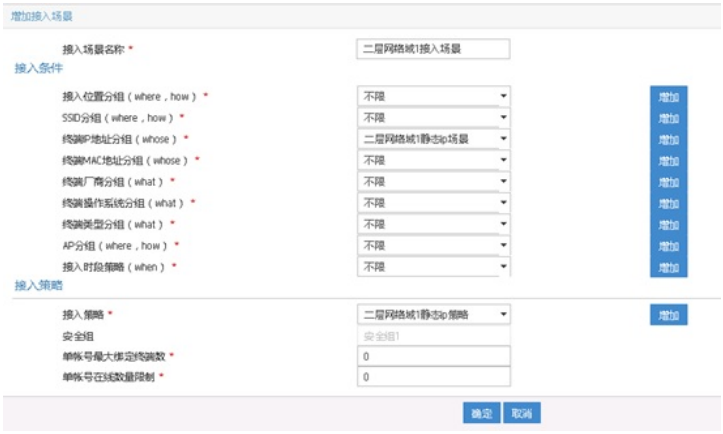
三、增加一个接入组，名字为“接入组1”，接入策略绑定到安全组1：



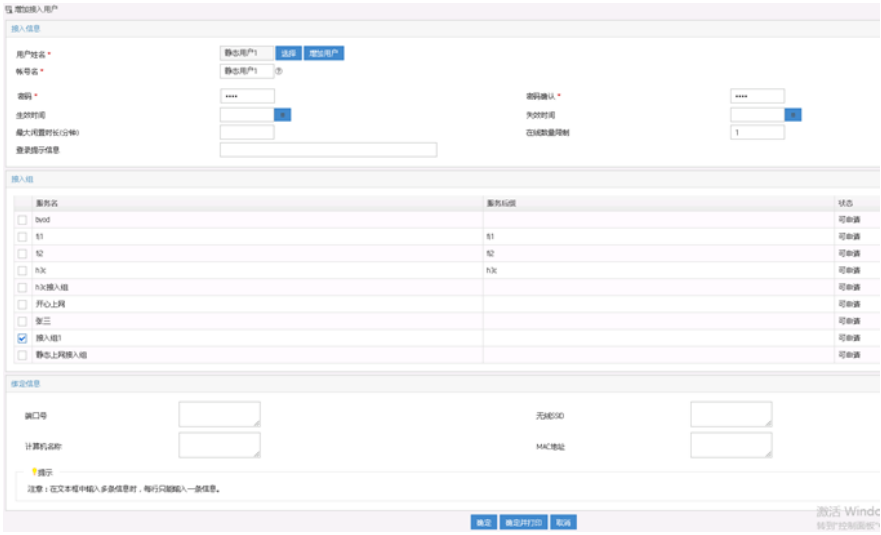
四、接入条件管理a终端ip地址分组中，增加一个基于终端ip的接入场景，名字为“二层网络域1静态ip场景”：

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”

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：



创建成功后，结果如下：



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
```

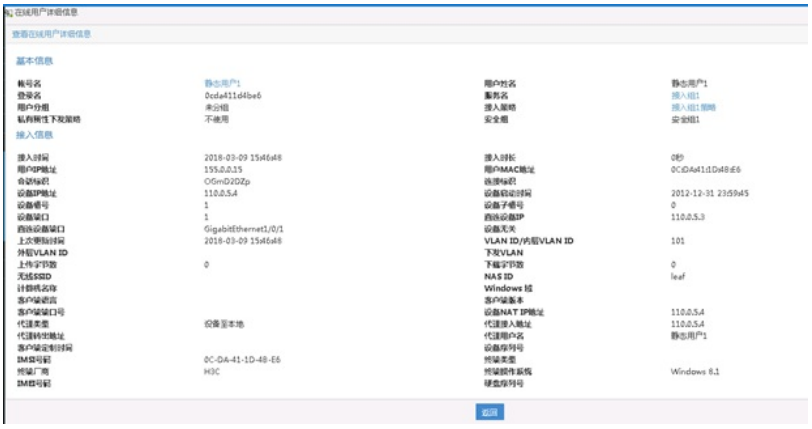
在Director侧查看在线用户也可以看到：

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：

[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：



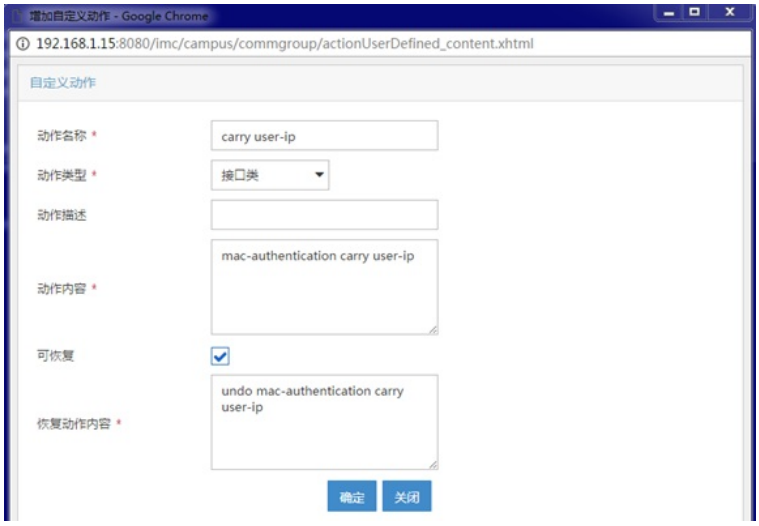
后续这台电脑随意挪到了access接口的g1/0/2，所在vlan为102，不用重新认证，能够无感知上线：

配置关键点

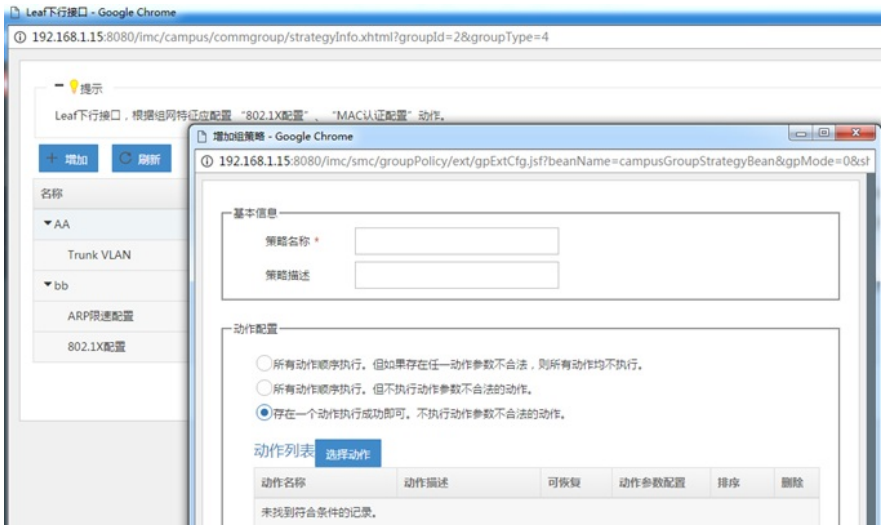
carry user-ip配置优化

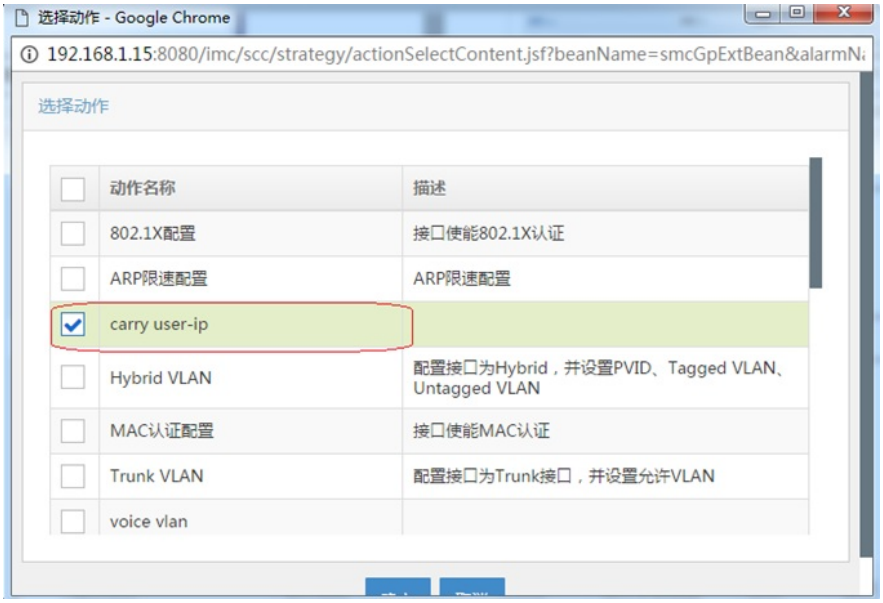
每个leaf下行口都需要手工下发mac-authentication carry user-ip，这个太麻烦，可以在imc自定义leaf下行口策略，统一自动下发。步骤如下：

1、业务—通用—自定义动作，添加这个动作：



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下行口自动下发成功：