

组网及说明

V7防火墙与IMC网络可达，V7防火墙network-operator 权限级别说明如下

network-operator	<ul style="list-style-type: none"><li>• 可执行系统所有功能和资源的相关display命令（除display history-command all、display security-logfile summary等命令，具体请通过display role命令查看）</li><li>• 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码</li><li>• 可执行进入XML视图的命令</li><li>• 可允许用户操作所有读类型的Web菜单选项</li><li>• 可允许用户操作所有读类型的XML元素</li><li>• 可允许用户操作所有读类型的OID</li></ul>
------------------	--

## 配置步骤

### 1、设备上正常配置认证相关

```
#  
radius scheme 123  
primary authentication x.x.142.178 key simple 123  
primary accounting x.x.142.178 key simple 123  
nas-ip x.x.142.130  
#  
domain 123  
authentication login radius-scheme 123  
authorization login radius-scheme 123  
accounting login radius-scheme 123  
#
```

### 2、IMC上AAA权限下发可以支持角色名的下发，所以第一种方式

#### (1) IMC上正常下发network-operator角色名

设备管理用户基本信息

帐号名 *	123@123
用户姓名	
用户密码 *	*****
密码确认 *	*****
认证密码方式	帐号密码
启用密码策略	否
电话号码	
邮箱地址 *	1223@12.com
设备管理用户分组	
登录类型	
服务类型	
私有属性下发策略	
EXEC权限级别	
角色名	network-operator

提示  
注意：输入绑定的多个角色名时，每行只能写一个角色名，且角色名占字节数与角色名个数（出现多个角色，则角色占字节数不应超过24个）。

#### (2) 可以自定义缺省level权限，比如level-5，如下

设备管理用户基本信息

帐号名 *	123@123
用户姓名	
用户密码 *	*****
密码确认 *	*****
认证密码方式	帐号密码
启用密码策略	否
电话号码	
邮箱地址 *	1223@12.com
设备管理用户分组	
登录类型	
服务类型	
私有属性下发策略	
EXEC权限级别	5

对应设备侧需要自定义wb只读的level-5权限

```
#
```

```
role name level-5
```

```
description Predefined level-5 role //系统默认的level-5权限
```

rule 1 permit read web-menu

/设置web页面只读权限

#

配置关键点  
使用账号@域名 (123@123) 登录测试结果

3C SecPath M9006



概览



监控



策略



对象



网络



系统