这也是安全认证的最后一种方式了，就是 AC 与外边 Protal 服务器对接的认证，这里采用的是华为 TSM（目前最新的已经改为 policy center 了），也支持第三方认证服务器，这里只是简单演示下，更多策略的控制跟应用，可以参考手册说明。

拓扑（省略）

拓扑其实很简单的，跟平常的无线拓扑一样，可以参考之前的文章即可，这里主要讲解 AC 上面的 Protal 定义，以及测试。

AC 初始化

```
[Huawei-AC6605]dhcp enable
[Huawei-AC6605]vlan batch 88 100

[Huawei-AC6605]interface Vlanif 88
[Huawei-AC6605-Vlanif88]ip address 192.168.88.1 255.255.255.0
[Huawei-AC6605-Vlanif88]dhcp select interface

[Huawei-AC6605]interface Vlanif 100
[Huawei-AC6605-Vlanif100]ip address 192.168.100.1 255.255.255.0
[Huawei-AC6605-Vlanif100]dhcp select interface
[Huawei-AC6605-Vlanif100]dhcp server dns-list 218.85.152.99

[Huawei-AC6605]interface Vlanif 1
[Huawei-AC6605-Vlanif1]ip address 192.168.31.100 255.255.255.0
```

配置 AC 与 AP 相连的端口。

```
[Huawei-AC6605]interface GigabitEthernet0/0/11
[Huawei-AC6605-GigabitEthernet0/0/11]port link-type trunk
[Huawei-AC6605-GigabitEthernet0/0/11]port trunk pvid vlan 88
[Huawei-AC6605-GigabitEthernet0/0/11]undo port trunk allow-pass vlan 1
[Huawei-AC6605-GigabitEthernet0/0/11]port trunk allow-pass vlan 88 100
```

配置 RADIUS 服务器模版。

```
[Huawei-AC6605]radius-server template portal
```

[Huawei-AC6605-radius-portal]radius-server authentication 192.168.31.209 1812
[Huawei-AC6605-radius-portal]radius-server accounting 192.168.31.209 1813
[Huawei-AC6605-radius-portal]radius-server shared-key simple huawei123

配置 RADIUS 授权服务器。

[Huawei-AC6605]radius-server authorization 192.168.31.209 shared-key simple huawei123

配置认证方案和计费方案。

[Huawei-AC6605] aaa
[Huawei-AC6605-aaa]authentication-scheme portal
[Huawei-AC6605-aaa-authen-portal] authentication-mode radius
[Huawei-AC6605-aaa]accounting-scheme portal
[Huawei-AC6605-aaa-accounting-portal] accounting-mode none

配置域。

[Huawei-AC6605-aaa]domain portal
[Huawei-AC6605-aaa-domain-portal]radius-server portal
[Huawei-AC6605-aaa-domain-portal]authentication-scheme portal
[Huawei-AC6605-aaa-domain-portal]accounting-scheme portal

配置 Portal 认证服务器。

[Huawei-AC6605]web-auth-server portal
[Huawei-AC6605-web-auth-server-portal]server-ip 192.168.31.209
[Huawei-AC6605-web-auth-server-portal]port 50100
[Huawei-AC6605-web-auth-server-portal]shared-key simple password
[Huawei-AC6605-web-auth-server-portal]url https://192.168.31.209:8443/newwebauth

在接口下绑定 Portal 认证服务器。

[Huawei-AC6605]interface vlanif 100
[Huawei-AC6605-Vlanif100]web-auth-server portal direct

配置免认证规则。（一个是 Protal 服务器的地址，一个是 DNS 的来触发认证）

[Huawei-AC6605]portal free-rule 0 destination ip 192.168.31.209 mask 255.255.255.255
[Huawei-AC6605]portal free-rule 1 destination ip 218.85.152.99 mask 255.255.255.255

建立 wlan-ess 接口和调用 Portal 认证服务器与认证域。

[Huawei-AC6605]interface Wlan-Ess 1
[Huawei-AC6605-Wlan-Ess1] port hybrid pvid vlan 100
[Huawei-AC6605-Wlan-Ess1] port hybrid untagged vlan 100
[Huawei-AC6605-Wlan-Ess1] web-authentication first-mac

[Huawei-AC6605-Wlan-Ess1] permit-domain name portal

配置 wlan-ess 接口，在 wlan-ess 接口调用内置 Portal 与允许的认证域。

[Huawei-AC6605]interface Wlan-Ess 1
[Huawei-AC6605-Wlan-Ess1]port hybrid pvid vlan 100
[Huawei-AC6605-Wlan-Ess1]port hybrid untagged vlan 100
[Huawei-AC6605-Wlan-Ess1]portal local-server enable
[Huawei-AC6605-Wlan-Ess1]permit-domain name default
配置 AC 的源接口，用于 AC 和 AP 之间建立隧道通信。

[Huawei-AC6605]wlan
[Huawei-AC6605-wlan-view]wlan ac source interface vlanif88

配置 AP 的认证方式为免认证。

[Huawei-AC6605-wlan-view]ap-auth-mode no-auth

添加 AP。

[Huawei-AC6605-wlan-view]ap id 0 type-id 31 mac d4b1-10ac-0b00 sn 210235582910D6000354

创建名为“wmm1”的 WMM 模版，参数采用默认配置。

[Huawei-AC6605-wlan-view]wmm-profile name wmm1 id 1

创建名为“radio1”的射频模版，绑定 WMM 模版“wmm1”。

[Huawei-AC6605-wlan-view]radio-profile name radio1 id 1
[Huawei-AC6605-wlan-radio-prof-radio1]wmm-profile id 1

创建名为“traffic1”的流量模版，参数采用默认配置。

[Huawei-AC6605-wlan-view]traffic-profile name traffic1 id 1

创建名为“security1”的安全模版，认证方式为 WEP 认证，开放认证，不加密。

[Huawei-AC6605-wlan-view]security-profile name security1 id 1

创建名为“service1”的服务集，并绑定流量模版和安全模版，WLAN-ESS 接口。

[Huawei-AC6605-wlan-view]service-set name service1 id 1
[Huawei-AC6605-wlan-service-set-service1]wlan-ess 1

[Huawei-AC6605-wlan-service-set-service1]ssid huawei-portal
[Huawei-AC6605-wlan-service-set-service1]traffic-profile id 1
[Huawei-AC6605-wlan-service-set-service1]security-profile id 1
[Huawei-AC6605-wlan-service-set-service1]service-vlan 100

配置 AP 对应的 VAP，下发 WLAN 服务

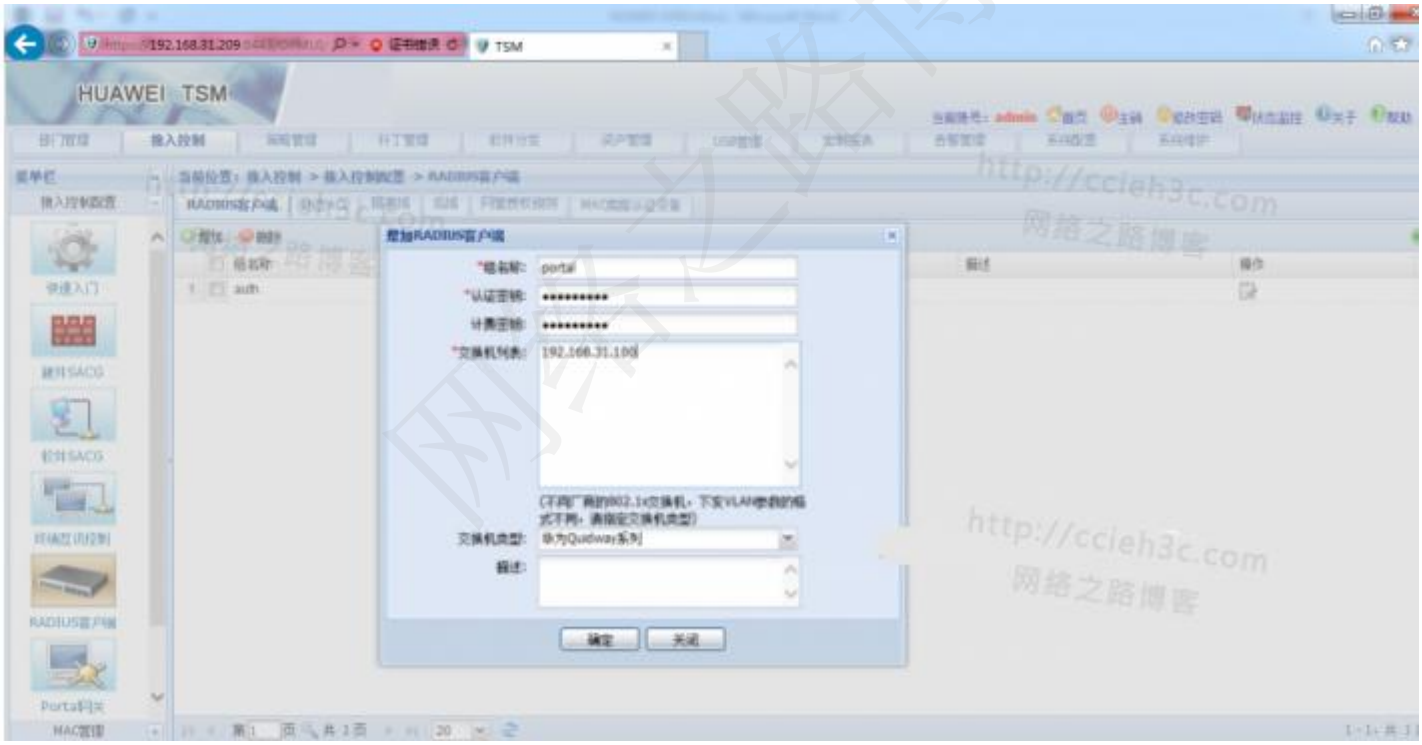
[Huawei-AC6605-wlan-view]ap 0 radio 0
[Huawei-AC6605-wlan-radio-0/0]radio-profile id 1
[Huawei-AC6605-wlan-radio-0/0]service-set id 1 wlan 1

下发 AP 的 WLAN 配置

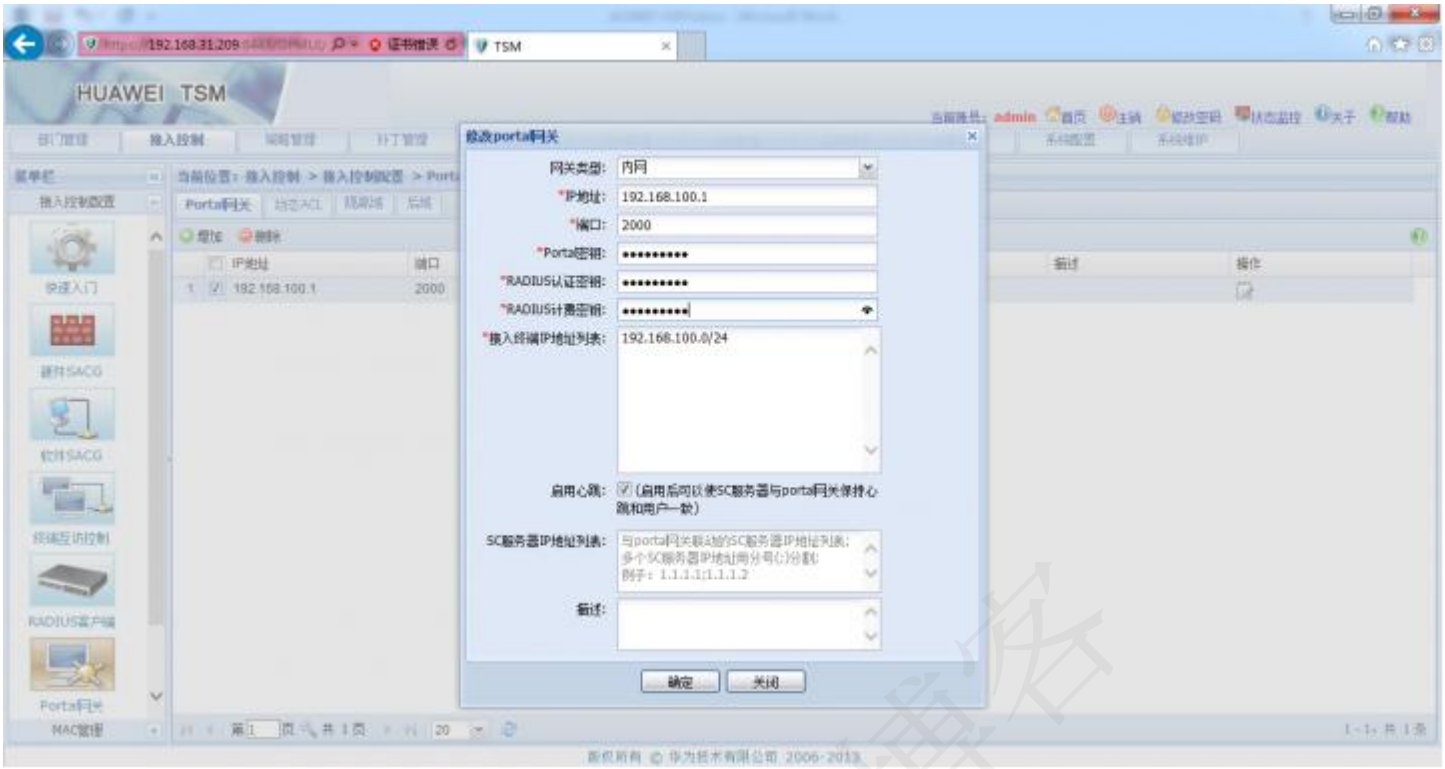
[Huawei-AC6605-wlan-view]commit all

TSM 服务器配置

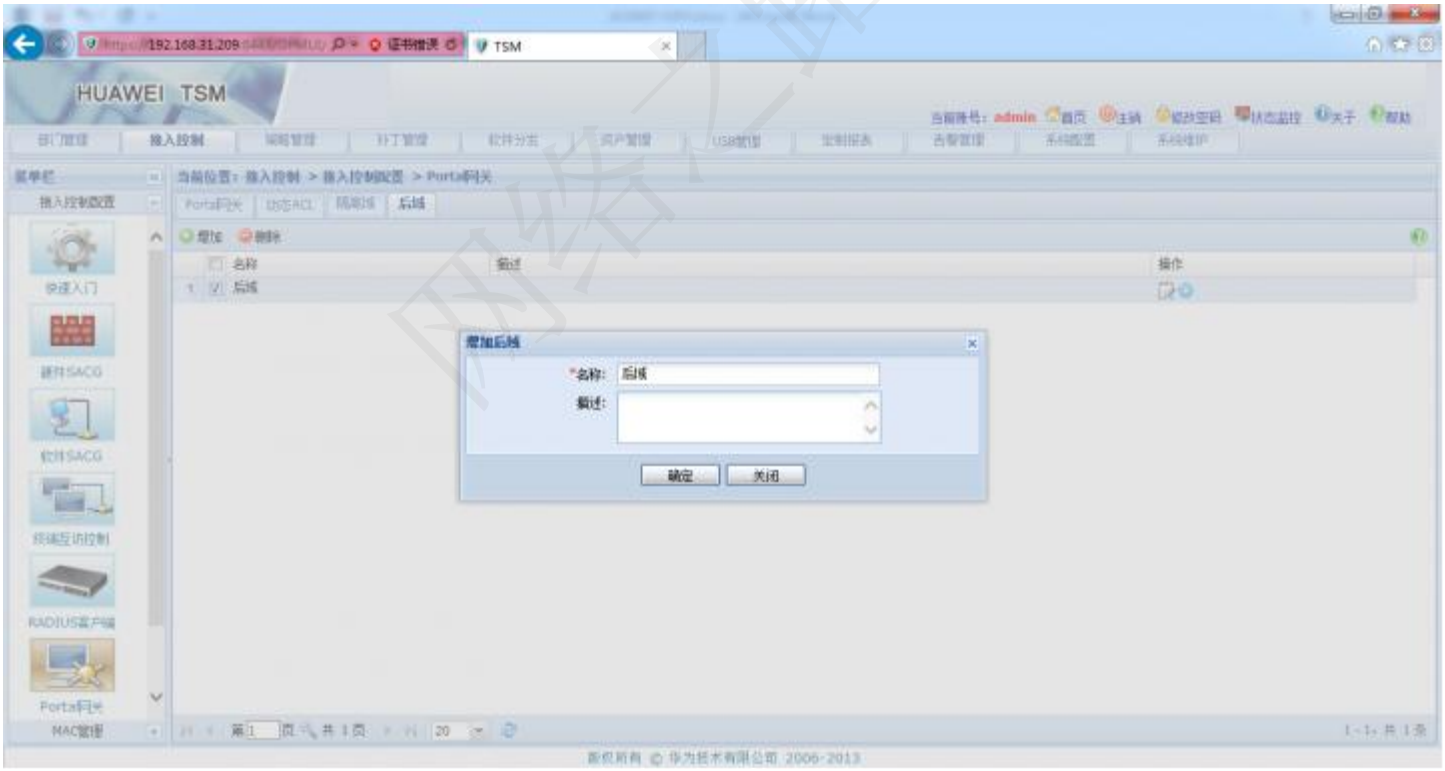
接入控制 – RADIUS 服务器 - 添加 RADIUS 服务器



接入控制 - Portal 网关 - 添加 Portal 网关



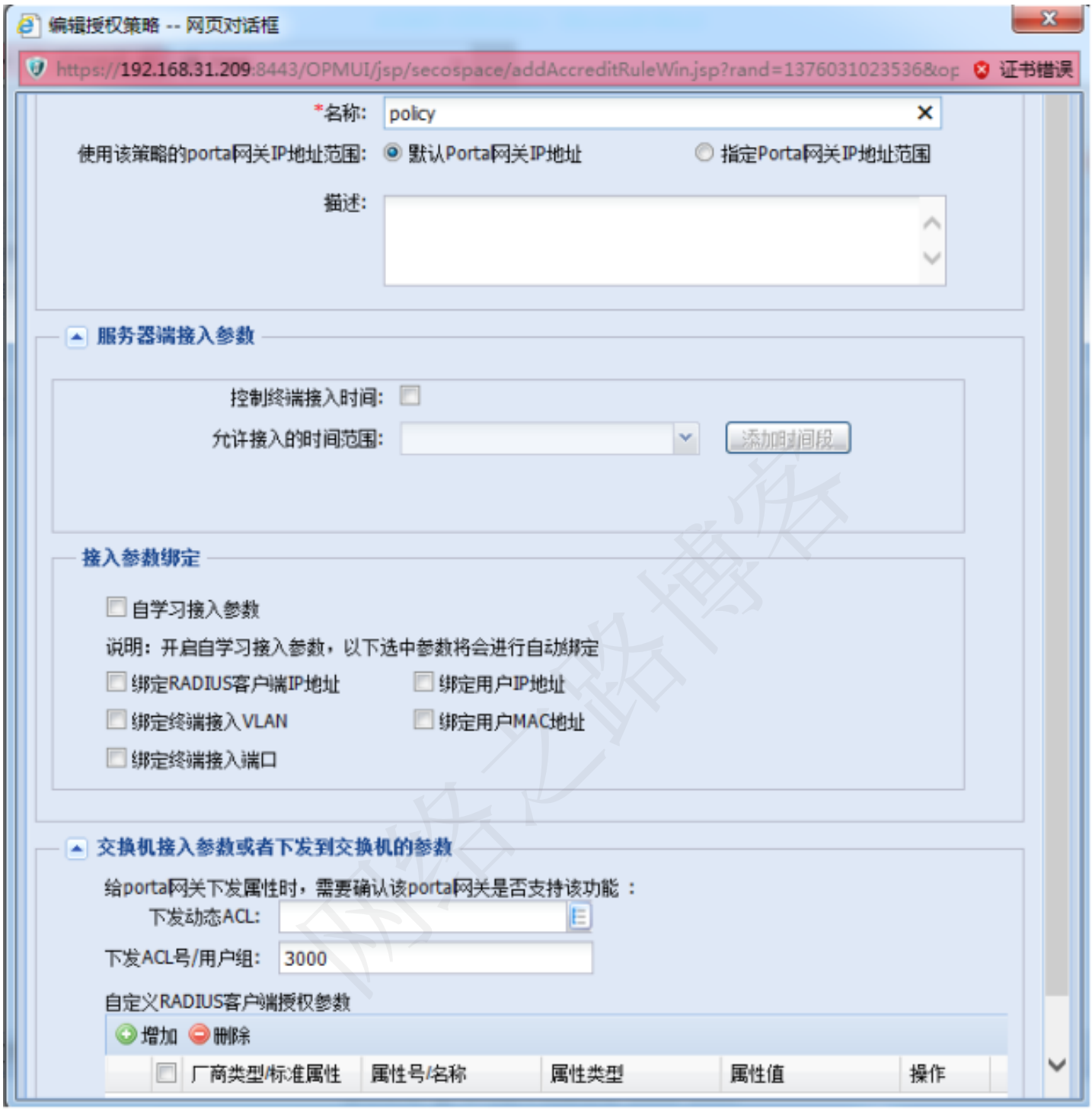
添加后域



修改后域的授权策略

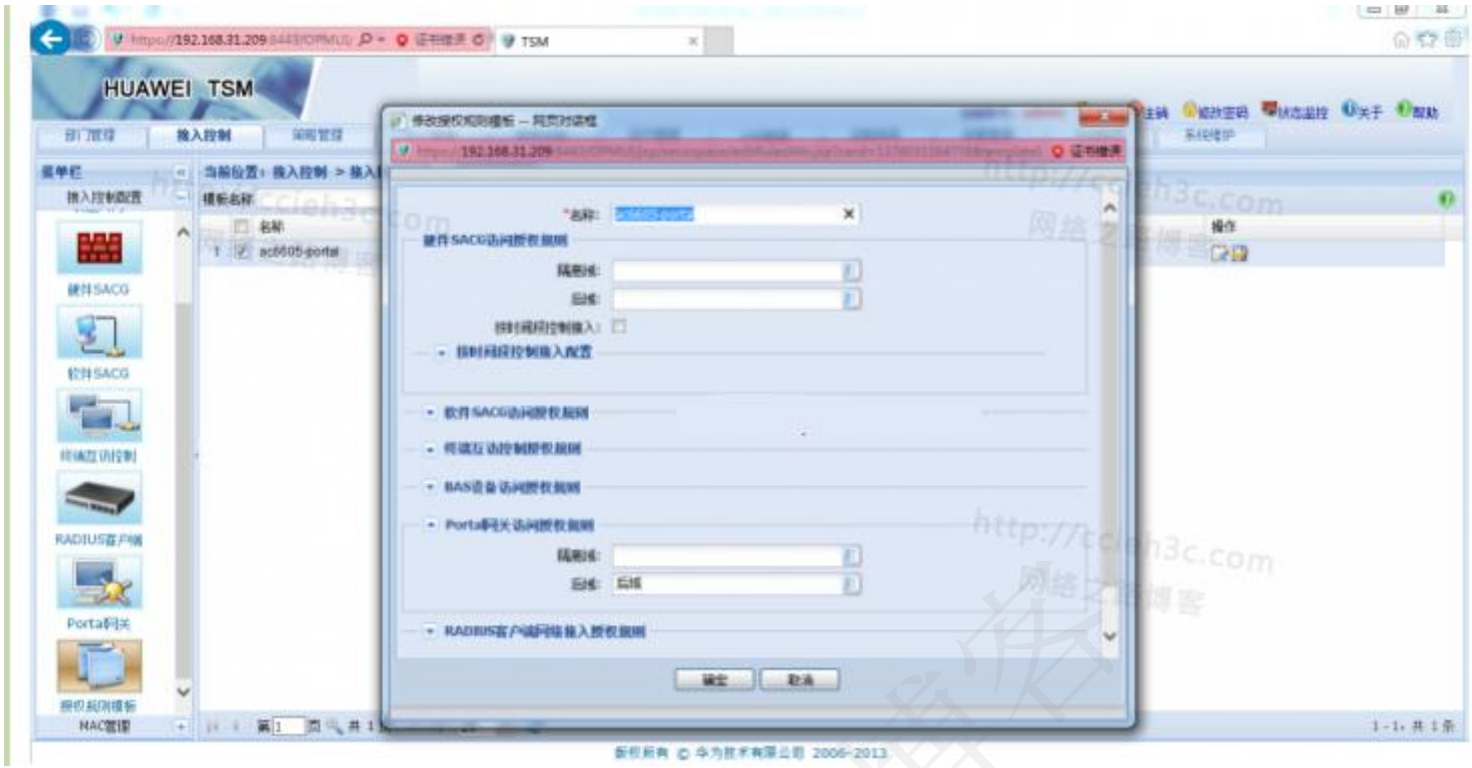
建立一个“policy”策略

下发一个 ACL，针对认证通过后的用户做访问限制

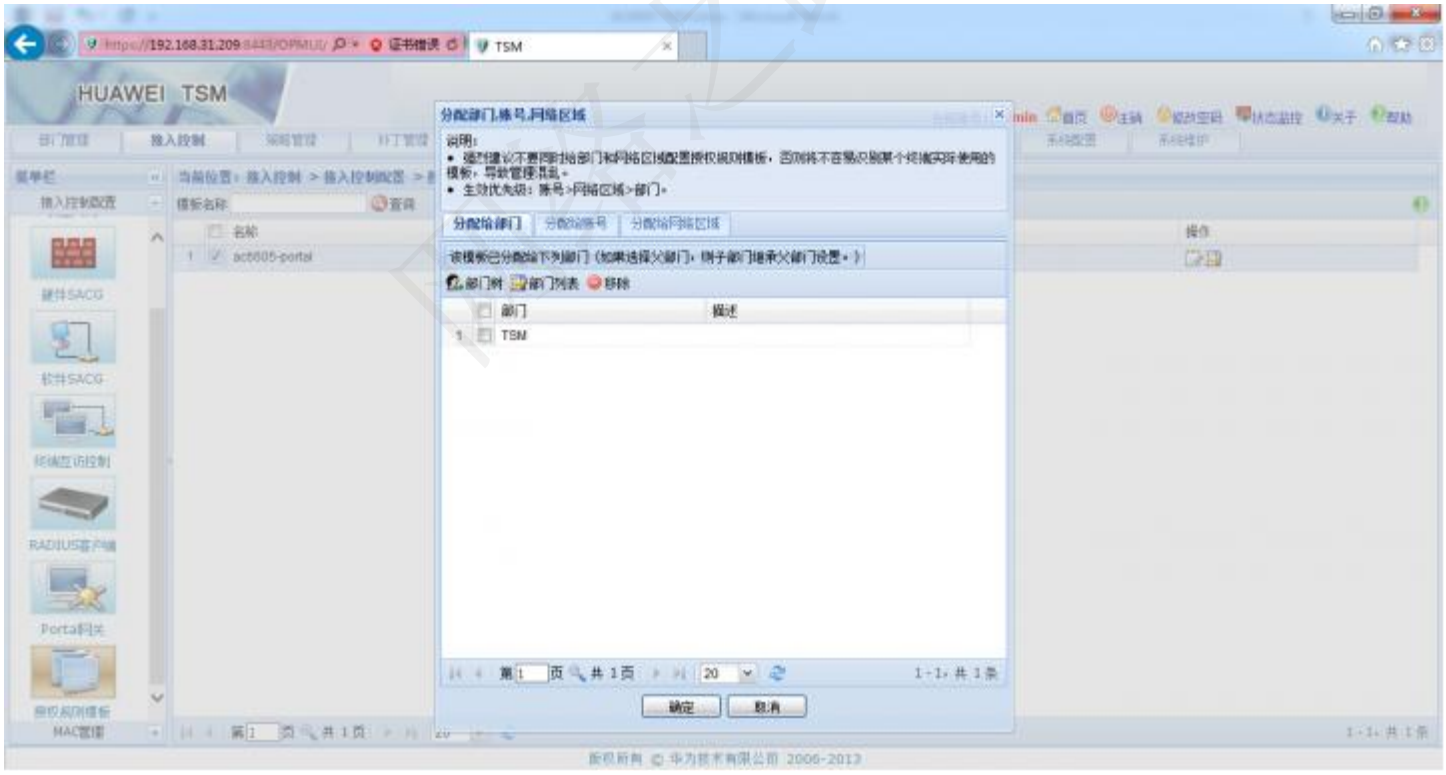


接入控制 – 授权规则模版 – 添加一个授权模版名为”ac6605-portal”

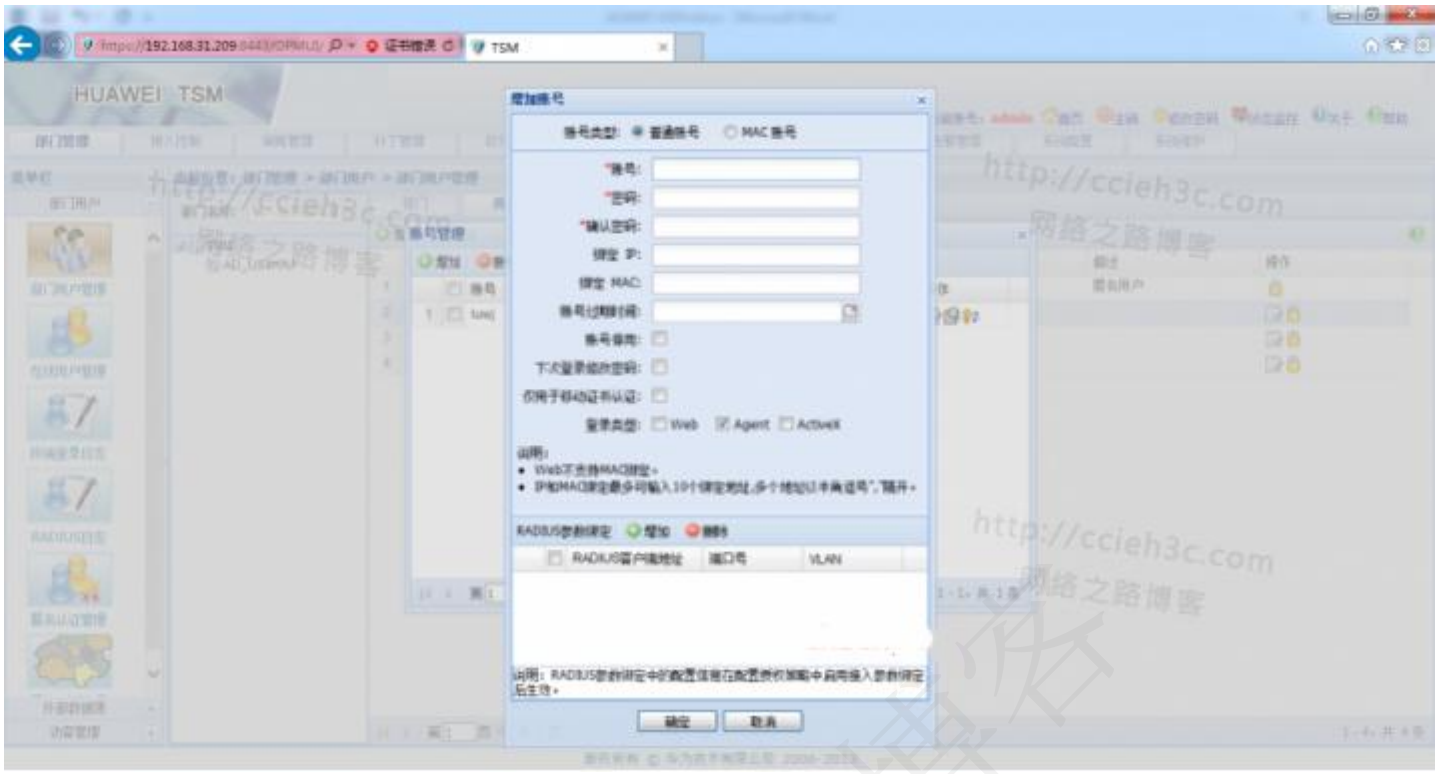
在 Portal 网关访问授权规则选择刚才创建好的后域



对创建好的授权规则模板”ac6605-portal”分配给部门
添加整个 TSM 部门包括子部门



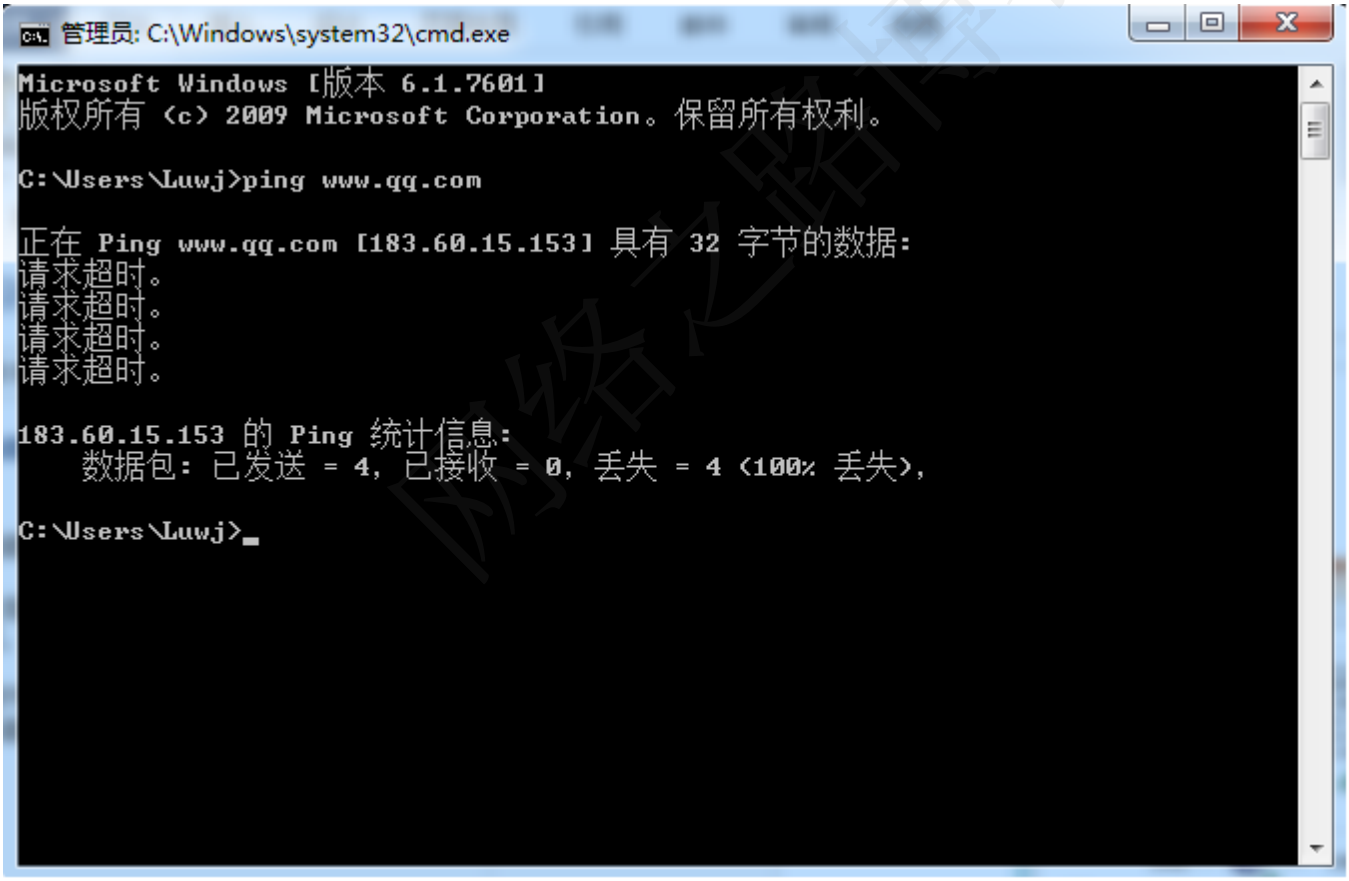
部门管理 – 部门用户管理 - 创建用户，终端认证时候用到的用户
需要勾选”Web”选项，否则默认建立的用户只能用于 TSM Agent 代理的登陆



测试结果

终端搜索 SSID，并连接。

测试 PING www.qq.com

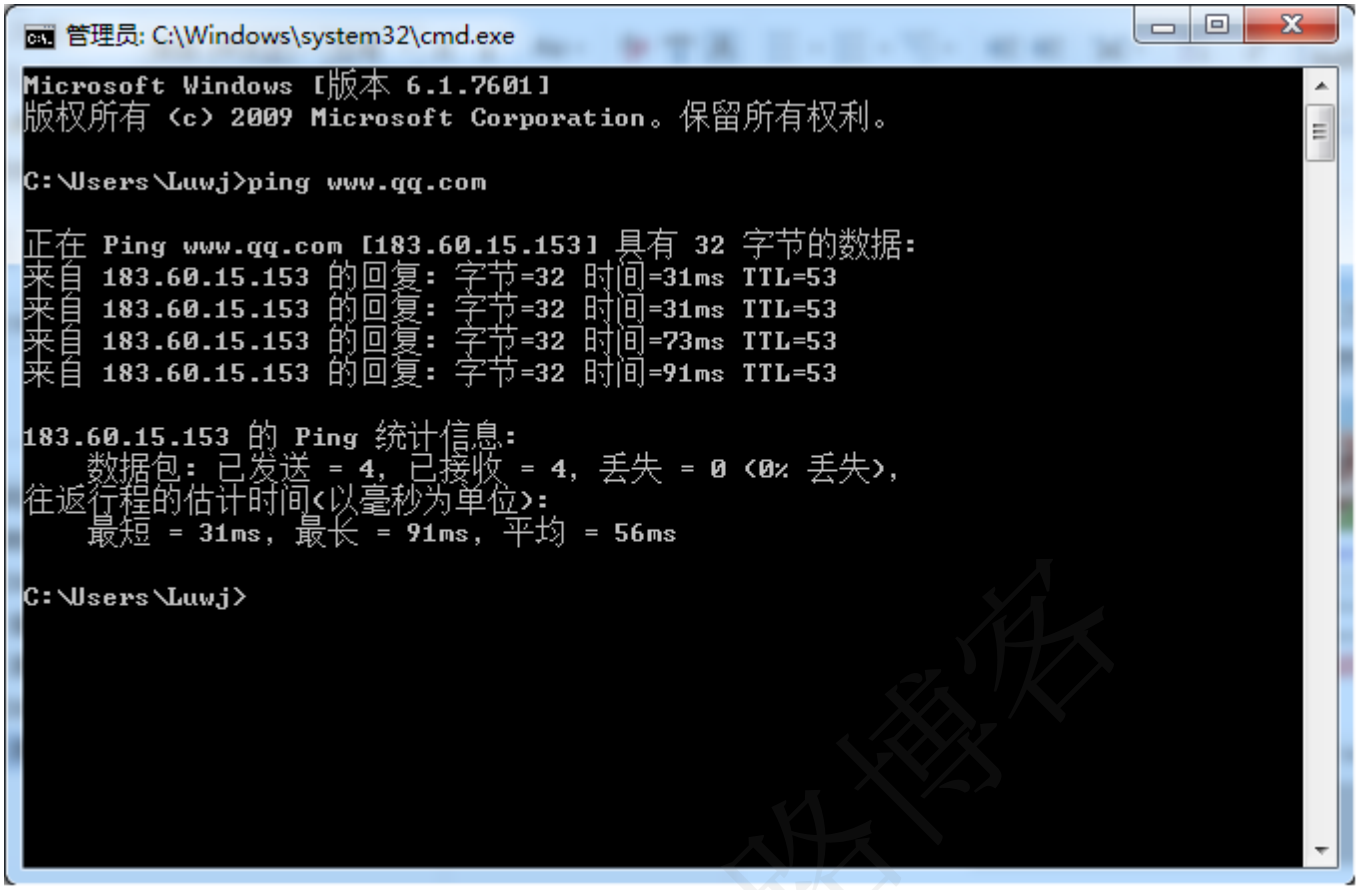


打开 IE，输入 www.qq.com

自动跳转到认证页面

输入已经在 TSM 服务器创建好的用户进行登陆

登陆成功后，测试登陆后是否可以正常访问互联网



博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多技术文章尽在网络之路博客，http://ccieh3c.com。

更多联系方式

QQ：1914756383
邮箱：1914756383@qq.com
微信：ciscohuaweih3c
博客地址:http://ccieh3c.com
远程调试服务：https://1914756383.taobao.com