

## 403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。  
注册版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。  
注册版本不会显示该信息。 [删除广告](#)

# ACG1000 portal认证配置方法 (HTTPS)

## 目录

### [ACG1000 portal认证配置方法（HTTPS）](#)

#### [1 简介](#)

#### [2 配置前提](#)

#### [3 使用限制](#)

#### [4 配置举例](#)

##### [4.1 组网需求1： HTTPS弹Portal三层组网](#)

##### [4.2 配置思路](#)

##### [4.3 使用版本](#)

##### [4.4 配置注意事项](#)

##### [4.5 配置步骤](#)

[4.5.1 登录Web网管](#)

[4.5.2 开启HTTPS弹portal功能](#)

[4.5.3 配置认证地址对象](#)

[4.5.4 配置本地web认证](#)

[4.5.5 配置本地web认证策略](#)

[4.5.6 配置认证用户](#)

[4.5.7 验证配置](#)

[4.6 组网需求2： HTTPS弹Portal二层组网](#)

[4.7 配置思路](#)

[4.8 使用版本](#)

[4.9 配置注意事项](#)

[4.10 配置步骤](#)

[4.10.1 登录Web网管](#)

[4.10.2 开启HTTPS弹portal功能](#)

[4.10.3 配置认证地址对象](#)

[4.10.4 配置本地web认证](#)

[4.10.5 配置本地web认证策略](#)

[4.10.6 配置认证用户](#)

[4.10.7 验证配置](#)

# 1 简介

本文档介绍ACG1000设备HTTPS弹Portal功能举例，HTTPS弹Portal是在访问HTTPS类型的网站时，查看页面是否会弹Portal的配置。

## 2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解HTTPS弹Portal特性。

## 3 使用限制

- HTTPS弹Portal对于HSTS网站无法弹Portal。
- IE11浏览器对于HTTPS类型网站无法弹Portal，IE11浏览器有合法证书强制检查，不信任的证书网站不允许用户继续浏览，进行强制保护，导致设备无法对https网站弹portal。
- 网银类网站无法实现HTTPS弹Portal。

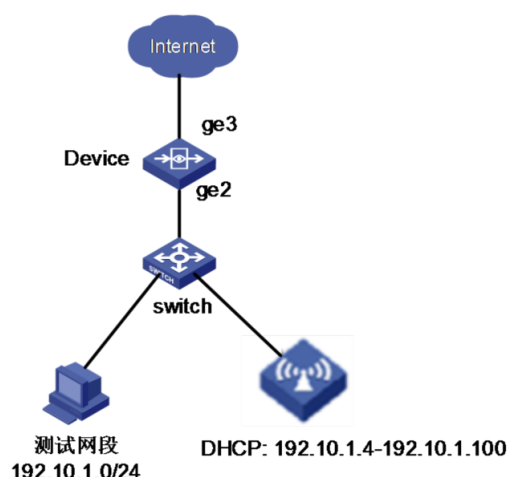
- HTTPS弹portal功能默认关闭，使用此功能前需要使用 `user-policy https-portal enable` 命令开启https弹Portal功能。

## 4 配置举例

### 4.1 组网需求1： HTTPS弹Portal三层组网

如图1所示，某公司内网存在测试网段和办公网段，测试网段IP地址为192.10.1.0/24。使用ACG1000设备的ge2和ge3接口路由模式部署在网络中，ACG作为出口网关设备，下联交换机。在ACG1000上使用命令 `user-policy https-portal enable` 启用HTTPS弹Portal功能。

图1 HTTPS弹Portal组网图



## 4.2 配置思路

- 在ACG设备上开启HTTPS弹Portal功能。
- 配置需要认证的地址对象和认证用户。
- 配置本地认证策略。

## 4.3 使用版本

本举例是在R6611P01版本上进行配置和验证的。

## 4.4 配置注意事项

HTTPS弹Portal时要保证浏览器可以进行正常的HTTPS类型网站的访问。

## 4.5 配置步骤

### 4.5.1 登录Web网管

如[图2](#)所示，使用HTTP或HTTPS的方式登录ACG1000设备的Web网管，默认的用户名和密码是admin/admin，输入验证码，并点击<登录>按钮。

图2 登录H3C ACG web网管



#### 4.5.2 开启HTTPS弹portal功能

如[图3](#)所示，使用串口或telnet进入设备后台，执行命令user-policy https-portal enable开启HTTPS弹portal功能。

图3 开启HTTPS弹portal功能

```
Username: admin
Password:
host:WD-D> en
host:WD-D# conf t
host:WD-D(config)# user-policy https-portal enable
host:WD-D(config)#
```

#### 4.5.3 配置认证地址对象

如[图4](#)所示，进入“策略配置>对象管理>地址对象>IPv4地址对象”，点击<新建>，IP地址配置为172.16.10.0/24创建认证地址网段对象，点击<提交>。

图4 配置认证地址对象

地址对象

基础配置

名称

认证用户网段

(1-31字符)

描述

(0-127 字符)

地址项目

+ 添加到列表

(例如: 192.168.1.1/24)

已添加项目

	类型	地址	操作
1	network	192.10.1.0/24	删除

排除地址

(多项用,隔开,格式如: 1.1.1.0/24,2.2...)

4.5.4 配置本地web认证

如图5所示，进入“用户管理>认证管理>认证方式>本地web认证”，这里按照默认配置，点击<提交>。

图5 配置本地web认证

本地WEB认证

用户登录唯一性检查

☐ 单一帐号登录

☒ 允许重复登录

允许个数 ☒ 无限制

☐ 允许登录数  (2-1000)

更多设置

客户端超时 ☒ 心跳超时  (10-144000分钟)

强制重登录间隔 ☐  (10-144000分钟)

无感知 ☐  (10-144000分钟, 不支持第三方认证)

页面跳转设置 ☒ 之前访问的页面 ☐ 重定向URL ☐ 认证结果页面

#### 4.5.5 配置本地web认证策略

如图6所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址为地址对象中的认证用户网段，认证方式为web认证，点击<提交>。

图6 配置本地web认证



如图7所示，配置成功的本地web认证如下：

图7 本地web认证配置成功

认证策略											
名称	描述	状态	源接口	目的接口	源地址	目的地址	认证方式	策略生效时间	用户有效时间	用户录入	操作
1	webauth	--	any	any	认证地址网段	any	WEB认证	always	永久录入	--	<a href="#">编辑</a> <a href="#">删除</a>

#### 4.5.6 配置认证用户

如图8所示，进入“用户管理>用户组织结构”，点击<新建>选择用户，输入用户账号和密码，密码和确认密码保持一致，点击<提交>。

图8 配置认证用户

用户

启用

☒

登录名

test

\*(1-63 字符)

描述

(0-127 字符)

所属组

/

用户组

☒ 本地密码

密码

\*\*\*\*\*

(6-31 字符)

确认密码

\*\*\*\*\*

(6-31 字符)

☒ 允许修改密码

☐ 初次认证修改密码

绑定范围

例:  
192.168.0.1  
192.168.0.0-192.198.1.100  
192.168.0.0/24  
192.168.1.1/255.255.255.0  
11:11:11:11:11:11  
aC~aC~aC~aC~aC~aC

排除IP

例:  
192.168.0.1  
192.168.0.0-192.198.1.100  
192.168.0.0/24  
192.168.1.1/255.255.255.0

账户过期时间

☒ 永不过期 ☐ 在此日期后过期

1984

1984

提交

取消

如图9所示，配置成功的用户界面如下：

图9 用户配置成功

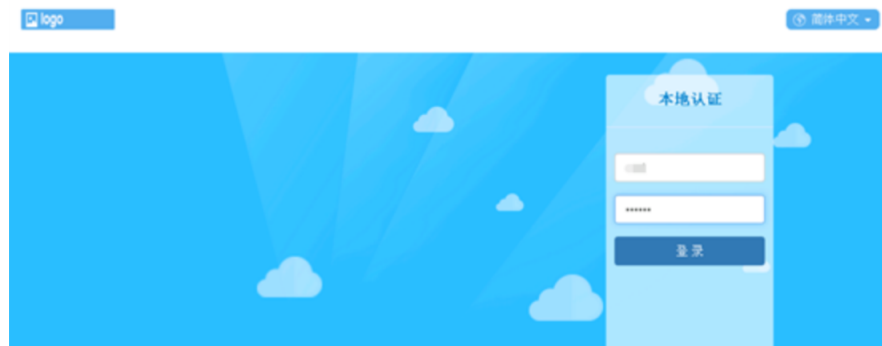
组信息								
组路径：/								
组信息：子组个数：1，直属用户个数：1，总用户个数：4								
+ 新建 选择 删除 移动 批量编辑 导入 导出								
	<input type="checkbox"/>	名称	描述	类型	所属用户组	绑定范围	状态	引用
1	<input type="checkbox"/>	默认组		用户组	/		-	0
2	<input type="checkbox"/>	test		用户	/		✓	0

### 4.5.7 验证配置

#### 1. pc端重定向方式验证

如[图10](#)所示，PC访问HTTPS类型的网站，界面会弹出本地认证界面。

图10 弹出Portal认证



#### 2. 移动端重定向方式认证

如[图11](#)所示，移动端访问HTTPS类型网站，浏览器弹出本地认证界面。

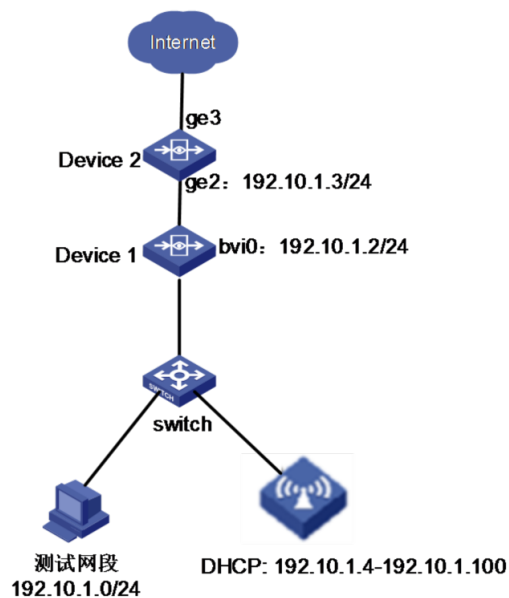
图11 移动端访问网站



## 4.6 组网需求2：HTTPS弹Portal二层组网

如图12所示，某公司内网存在测试网段和办公网段，测试网段IP地址为192.10.1.0/24。使用两台ACG1000设备路由模式部署在网络中，设备2作为出口网关设备，设备1下联交换机，配置桥模式。在设备1上使用命令`user-policy https-portal enable`启用HTTPS弹Portal功能。

图12 HTTPS弹Portal二层组网



## 4.7 配置思路

- 在ACG1设备上配置桥模式，并开启HTTPS弹Portal功能。
- 配置需要认证的地址对象和认证用户。
- 配置本地认证策略。

## 4.8 使用版本

本举例是在R6611P01版本上进行配置和验证的。

## 4.9 配置注意事项

HTTPS弹Portal时要保证浏览器可以进行正常的HTTPS类型网站的访问。

## 4.10 配置步骤

### 4.10.1 登录Web网管

如[图13](#)所示，使用HTTP或HTTPS的方式登录ACG1000设备的Web网管，默认的用户名和密码是admin/admin，输入验证码，并点击<登录>按钮。

图13 登录H3C ACG web网管



### 4.10.2 开启HTTPs弹portal功能

如[图14](#)所示，使用串口或telnet进入设备后台，执行命令user-policy https-portal enable开启HTTPs弹portal功能。

图14 开启HTTPs弹portal功能

```
Username: admin
Password:
host:WD-D> en
host:WD-D# conf t
host:WD-D(config)# user-policy https-portal enable
host:WD-D(config)# █
```

### 4.10.3 配置认证地址对象

如图15所示，进入“策略配置>对象管理>地址对象>IPv4地址对象”，点击<新建>，IP地址配置为192.10.1.0/24创建认证地址网段对象，点击<提交>。

图15 配置认证地址对象

地址对象

基础配置

名称 认证用户网段 (1-31字符)

描述 (0-127 字符)

地址项目 ☒ 子网地址 ☐ 范围地址 ☐ 主机地址 ☐ 域名 [+ 添加到列表](#)

(例如: 192.168.1.1/24)

已添加项目	类型	地址	操作
1	network	192.10.1.0/24	<a href="#">删除</a>

排除地址 (多项用,隔开,格式如: 1.1.1.0/24,2.2.2.0/24)

### 4.10.4 配置本地web认证

如图16所示，进入“用户管理>认证管理>认证方式>本地web认证”，这里按照默认配置，点击<提交>。

图16 配置本地web认证

#### 4.10.5 配置本地web认证策略

如图17所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址为地址对象中的认证用户网段，认证方式为web认证，点击<提交>。

图17 配置本地web认证



认证策略

启用 ☒

名称 webauth (1-31 字符)

描述 (0-127 字符)

源接口 any

源地址 认证用户网段 新建

目的接口 any

目的地址 any 新建

认证方式 WEB认证

时间 always

用户登录 用户组

用户有效时间

☒ 永久登录

☐ 有效期至 2019-04-23

☐ 临时登录

提交 取消

如图18所示，配置成功的本地web认证如下：

图18 本地web认证配置成功

认证策略

新增

删除

应用

禁用

上移

下移

导入

导出

下载模板

名称

描述

状态

源接口

目的接口

源地址

目的地址

认证方式

策略生效时间

用户有效时间

用户登录

操作

1	webauth	<div></div>	any	any	认证地址网段	any	WEB认证	always	永久登录	--	<div></div>
---	---------	-------------	-----	-----	--------	-----	-------	--------	------	----	-------------

#### 4.10.6 配置认证用户

如图19所示，进入“用户管理>用户组织结构>用户”，点击<新建>选择用户，输入用户账号和密码，密码和确认密码保持一致，点击<提交>。

图19 配置认证用户

用户

启用 ☒

登录名  \* (1-63 字符)

描述  (0-127 字符)

所属组  用户组

☒ 本地密码

密码  (6-31字符)

确认密码  (6-31字符)

☒ 允许修改密码

☐ 初次认证修改密码

绑定范围 

例:  
192.168.0.1  
192.168.0.0-192.198.1.100  
192.168.0.0/24  
192.168.1.1/255.255.255.0  
11:11:11:11:11:11  
aC~aC~aC~aC~aC~aC

排除IP 

例:  
192.168.0.1  
192.168.0.0-192.198.1.100  
192.168.0.0/24  
192.168.1.1/255.255.255.0

账户过期时间 ☒ 永不过期 ☐ 在此日期后过期

1984

1984

提交

取消

如图20所示，配置成功的用户界面如下：

图20 用户配置成功

组信息

组路径：/

组信息：子组个数：1，直属用户个数：1，总用户个数：4

新建

选择

删除





移动

批量编辑

导入

导出

查询

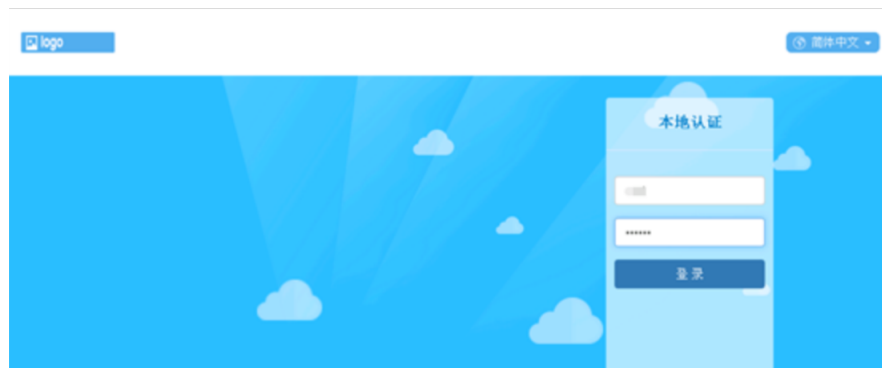
	<input type="checkbox"/>	名称	描述	类型	所属用户组	绑定范围	状态	引用	操作
1	<input type="checkbox"/>	 默认组		用户组	/		-	0	 
2	<input type="checkbox"/>	 test		用户	/			0	 

#### 4.10.7 验证配置

##### 1. pc端重定向方式验证

如图21所示，PC访问HTTPS类型的网站，界面会弹出本地认证界面。

图21 弹出Portal认证



##### 2. 移动端重定向方式认证

如图22所示，移动端访问HTTPS类型网站，浏览器弹出本地认证界面。

图22 移动端访问网站

