ACG1000 portal认证配置方法（HTTPS）

ACG1000 Portal认证 张新姿 2021-07-18 发表

组网及说明

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

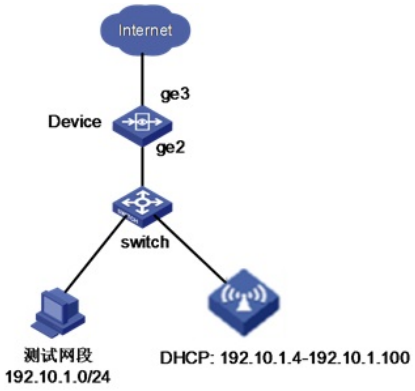
- HTTPS弹Portal对于HSTS网站无法弹Portal。
- IE11浏览器对于HTTPS类型网站无法弹Portal ,IE11浏览器有合法证书强制检查，不信任的证书网站不允许用户继续浏览，进行强制保护，导致设备无法对https网站弹portal。
- 网银类网站无法实现HTTPs弹Portal。
- HTTPs弹portal功能默认关闭，使用此功能前需要使用user-policy https-portal enable命令开启https弹Portal功能。

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。

配置步骤

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

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

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>。

配置关键点 本地web认证

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。