ACG1000本地web无感知认证综合配置及机制讲解

ACG1000 Portal认证 SNMP 曾招维 2022-10-31 发表

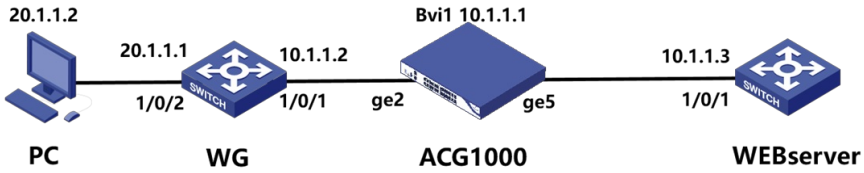
组网及说明

一、现场需求

内网用户在ACG1000上做本地web认证，用户名密码存储在本地，实现无感知功能（一次登录，一段时间内无需认证）。

备注：开启认证不弹portal页面、不用认证也可以上网、https流量触发认证、snmp用户同步等问题均可参考本案例。

二、组网



现场组网如上，实验中用交换机S6800的web登录页面充当web服务器。

配置步骤

三、配置步骤

1、基础配置：打通PC到WEB服务器路由。（根据现场组网自行写好路由）

WG网关设备：

```
# interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 #
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.1.1.1 255.255.255.0
```

ACG配置：

ACG接口加bvi口，写路由。

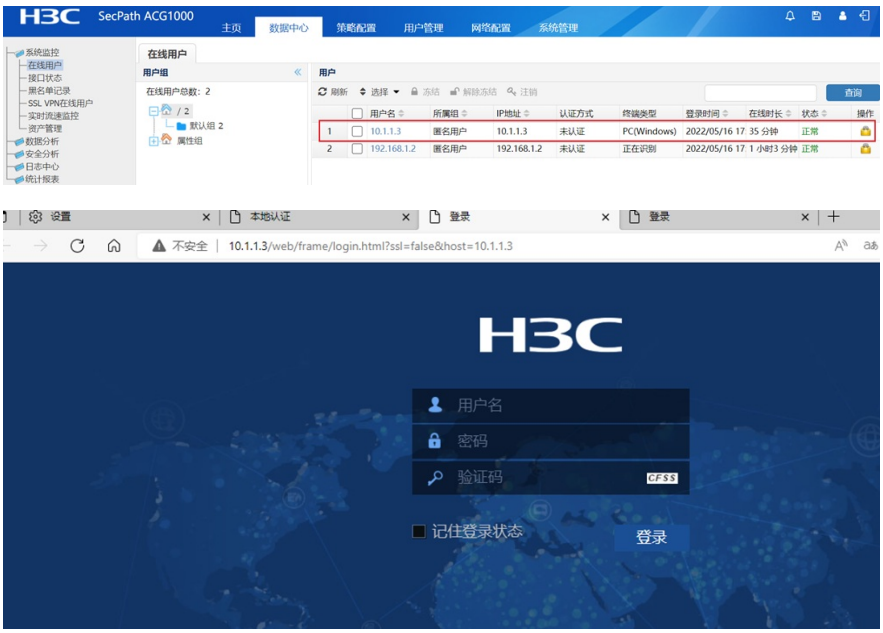
web服务器配置：

将交换机的web登录页面设置为http服务器，写好路由。

```
[WEBserver-Ten-GigabitEthernet1/0/1]dis th
#
 interface Ten-GigabitEthernet1/0/1 port link-mode route
 ip address 10.1.1.3 255.255.255.0
#
 [WEBserver]ip http enable
[WEBserver]ip https enable
```

验证开启认证前路由可达，web服务可用。（现场自己寻找web服务器，直接访问官网web页面也可以）

此时不开认证，测试终端（ip：20.1.1.2/24，网关20.1.1.1）可以正常打开交换机web登录页面。



2、ACG认证相关配置

A、创建本地用户zzw，注意此处不可以绑定IP范围，否则用户上来直接是静态绑定用户，无需认证，直接上网。

配置前注意事项：

- ACG1000设备配置Web认证时，允许用户的TCP三次握手报文、DNS报文以及ICMP报文通过，当检测到用户HTTP报文时拦截并弹出认证页面。所以，在使用Web认证功能时，需要保证终端可以进行正常的HTTP访问。
- 如果需要实现访问某些资源时免Web认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的目的IP地址排除即可。
- 网桥模式注意bvi口配置IP地址，否则无法正常弹页面。
- 关于snmp同步用户功能中的录入用户组选项，若开启该选项，对应的效果如下：录入到用户组支持手工录入和自动录入，录入的用户以IP地址作为用户名，绑定其IP及MAC地址，即此IP或MAC其中任何一个匹配均认为是此用户，此同步录入的用户属于静态绑定的用户，不会再进行其它方式的认证同时用户录入到本地后，可以针对此录入的用户组或用户进行相关功能的引用控制，比如：审计策略、控制策略、流控策略、限额策略等。

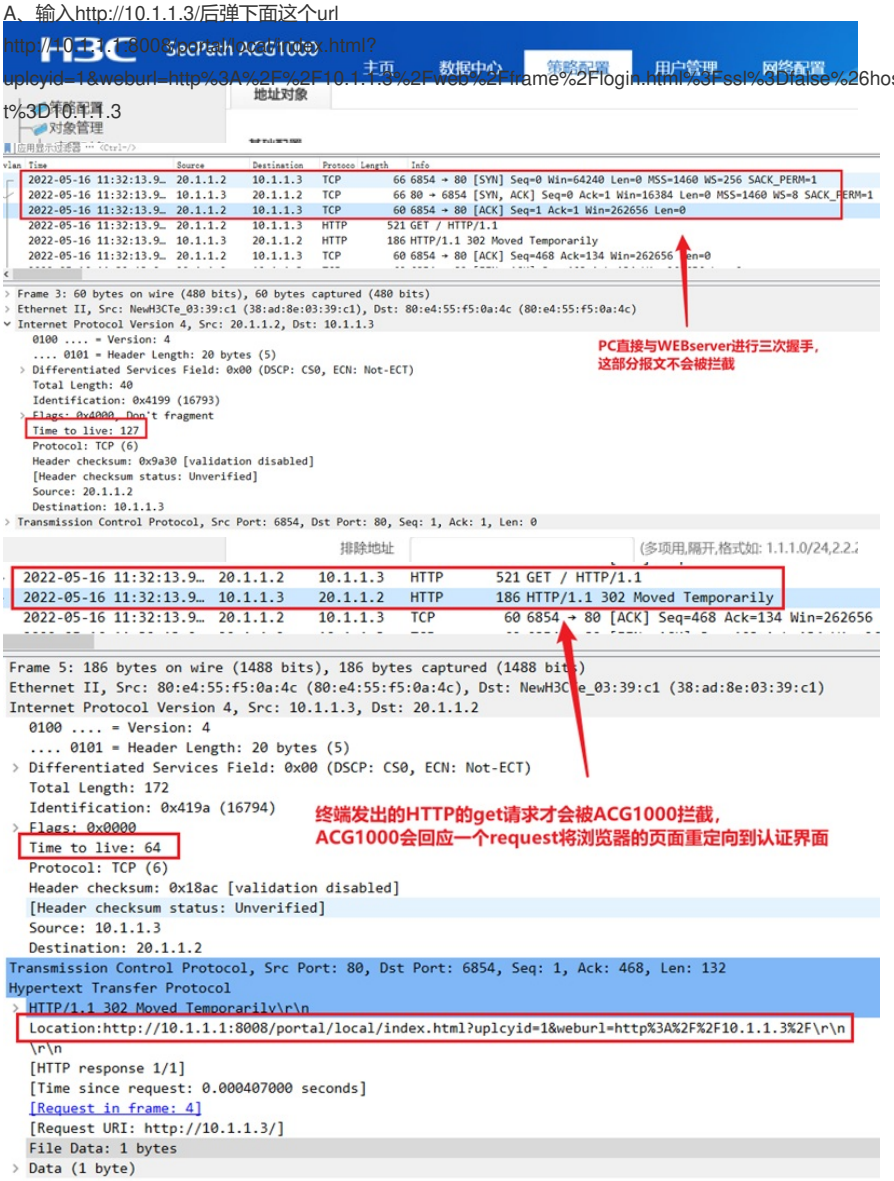
ACG1000拦截用户HTTP报文弹出认证页面机制验证：

ACG1000设备的本地web认证功能与无线和有线的portal认证机制不同，并不是拦截终端的第一个报文tcp syn，然后直接给终端重定向到认证界面（http://10.1.1.1:8008/portal/.....）,而是要与访问的目的设备或者服务进行三层握手交互之后，终端发出的HTTP的get请求才会被ACG1000拦截，ACG1000会回应一个request将浏览器的页面重定向到认证界面。所以，如果遇到ACG1000本地web认证异常时，查看配置均无问题的时候，需要确认现场的部署环境，是否有能够完成三次握手并发送get请求的环境。

B、本地认证地址范围10.1.1.0/24定义一个地址对象组，若用户想定义某些IP范围做认证动作，则需要定义这么一个地址对象。

A、输入http://10.1.1.3/后弹下面这个url

http://10.1.1.1:8008/portal/local/index.html?uplcyid=1&weburl=http%3A%2F%2F10.1.1.3%2F/web%2Fframe%2Flogin.html%3Fssl%3Dfalse%26host%3D10.1.1.3



备注：上面标注的ttl值，可以看出三次握手经过了一跳（网关三层设备）；重定向报文ttl为64，是acg

始发的报文。

但acg是网桥模式单纯看ttl值无法石锤前面的三次握手是与WEBserver交互的，直接在WEBserver镜像抓包。

```
[WEBserver]display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
```