

知 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

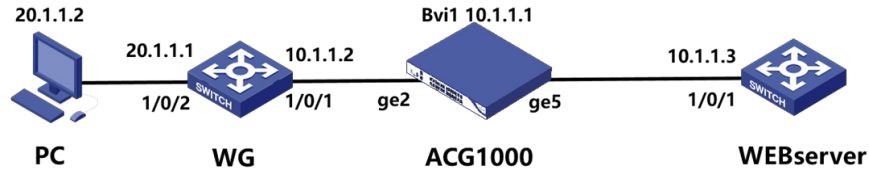
组网及说明

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。

物理接口	子接口	网桥接口	聚合接口	隧道接口	无线接口	安全域	虚拟网线
+	新建	删除					
接口名称	描述	包含接口	IP地址	IPv6地址	连接状态	启用状态	操作
1	bvi1	ge2, ge4	10.1.1.2/24		up	✓	✎

目的地址	掩码	下一跳	出口	权重	距离	地址探测	状态	启用	操作
1	0.0.0.0	219.159.107.129		1	1	⌵	✗	✓	✎
2	0.0.0.0		ge3	1	1	⌵	✗	✓	✎
3	20.1.1.0	255.255.255.0	10.1.1.2	1	1	⌵	✓	✓	✎
4	192.168.0.0	255.255.0.0	100.100.100.2	1	1	⌵	✗	✓	✎

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。

The screenshot displays the H3C SecPath ACG1000 web management interface. The top navigation bar includes 'SecPath ACG1000', '主站', '数据中心', '策略配置', '用户管理', '网络配置', and '系统管理'. The left sidebar shows a tree view with '系统监控' (System Monitoring) expanded, including '在线用户' (Online Users), '接口状态' (Interface Status), '黑名单记录' (Blacklist Records), 'SQL VPN在线用户' (SQL VPN Online Users), '实时流量监控' (Real-time Traffic Monitoring), '资产管理' (Asset Management), '数据分析师' (Data Analyst), '安全分析' (Security Analysis), '日志中心' (Log Center), and '统计报表' (Statistics Reports).

The main content area is divided into two sections. The top section, '在线用户' (Online Users), shows a table of active users:

序号	用户名	所属组	IP地址	认证方式	终端类型	登录时间	在线时长	状态	操作
1	10.1.1.3	匿名用户	10.1.1.3	未认证	PC(Windows)	2022/05/16 17:35	35分钟	正常	✎
2	192.168.1.2	匿名用户	192.168.1.2	未认证	正在识别	2022/05/16 17:11	1小时3分钟	正常	✎

The bottom section shows a '本地认证' (Local Authentication) configuration page. It includes a '设置' (Settings) tab and a '本地认证' (Local Authentication) tab. The '本地认证' tab is active, showing a '登录' (Login) form with fields for '用户名' (Username), '密码' (Password), and '验证码' (Captcha). The '验证码' field is filled with 'GFSS'. There is a checkbox for '记住登录状态' (Remember login status) and a '登录' (Login) button.

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。

H3C SecPath ACG1000

主页 数据中心 策略配置 用户管理 网络配置

用户管理

用户

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。

本地认证

描述：本地认证 (0-127 字符)

所属组：/ 用户组

本地密码： (0-31 字符)

初次认证修改密码

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，查看配置是否正确的时候，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，本地地址地址范围2.1.1.0/24定义一个地址对象组，若用一固定某些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

H3C SecPath ACG1000

主页 数据中心 策略配置 用户管理 网络配置

对象管理

地址对象

应用层过滤器

应用层过滤器

2022-05-16 11:32:13.9... 20.1.1.2 10.1.1.3 TCP 66 6854 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

2022-05-16 11:32:13.9... 10.1.1.3 20.1.1.2 TCP 66 80 → 6854 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=8 SACK_PERM=1

2022-05-16 11:32:13.9... 20.1.1.2 10.1.1.3 TCP 60 6854 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0

2022-05-16 11:32:13.9... 20.1.1.2 10.1.1.3 HTTP 521 GET / HTTP/1.1

2022-05-16 11:32:13.9... 10.1.1.3 20.1.1.2 HTTP 186 HTTP/1.1 302 Moved Temporarily

2022-05-16 11:32:13.9... 10.1.1.3 10.1.1.3 TCP 60 6854 → 80 [ACK] Seq=468 Ack=134 Win=262656 Len=0

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: NewH3CTe_03:39:c1 (38:ad:8e:03:39:c1), Dst: 80:e4:55:f5:0a:4c (80:e4:55:f5:0a:4c)

Internet Protocol Version 4, Src: 20.1.1.2, Dst: 10.1.1.3

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0x4199 (16793)

Flags: 0x0000, Don't fragment

Time to live: 127

Protocol: TCP (6)

Header checksum: 0x9a30 [validation disabled]

[Header checksum status: Unverified]

Source: 20.1.1.2

Destination: 10.1.1.3

Transmission Control Protocol, Src Port: 6854, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

排除地址 (多项用, 隔开, 格式如: 1.1.1.0/24, 2.2.2.2)

2022-05-16 11:32:13.9... 20.1.1.2 10.1.1.3 HTTP 521 GET / HTTP/1.1

2022-05-16 11:32:13.9... 10.1.1.3 20.1.1.2 HTTP 186 HTTP/1.1 302 Moved Temporarily

2022-05-16 11:32:13.9... 20.1.1.2 10.1.1.3 TCP 60 6854 → 80 [ACK] Seq=468 Ack=134 Win=262656 Len=0

Frame 5: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)

Ethernet II, Src: 80:e4:55:f5:0a:4c (80:e4:55:f5:0a:4c), Dst: NewH3CTe_03:39:c1 (38:ad:8e:03:39:c1)

Internet Protocol Version 4, Src: 10.1.1.3, Dst: 20.1.1.2

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 172

Identification: 0x419a (16794)

Flags: 0x0000

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x18ac [validation disabled]

[Header checksum status: Unverified]

Source: 10.1.1.3

Destination: 20.1.1.2

Transmission Control Protocol, Src Port: 80, Dst Port: 6854, Seq: 1, Ack: 468, Len: 132

Hypertext Transfer Protocol

HTTP/1.1 302 Moved Temporarily\r\n

Location: http://10.1.1.1:8008/portal/local/index.html?uplcyid=1&weburl=http%3A%2F%2F10.1.1.3%2F\r\n\r\n

[HTTP response 1/1]

[Time since request: 0.000407000 seconds]

[Request in frame: 4]

[Request URI: http://10.1.1.3/]

File Data: 1 bytes

Data (1 byte)

PC直接与WEBserver进行三次握手，这部分报文不会被拦截

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

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Back是WEB模式Sec2a重ACG1030石锤前面的三次握手是与WEBserver交互的，直接在WEBserver镜像抓包。

用户管理

认证策略

本地WEB认证

本地WEB认证

微信认证

State: Active

本地WEB认证

用户登录唯一性检查

☒ 单一帐号登录