一、开始

H3C SecPath ACG1000 是 H3C 公司新一代应用控制网关，是面向客户业务而量身定制的全业务网关产品,能配合创新的社交网络行为管理功能、清晰易用的管理日志功能等，提供业界最全面、完善的上网行为管理解决方案。从而保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计，为用户全面了解网络应用模型和流量趋势，优化其带宽资源，开展各项业务提供有力的支撑。ACG1000 产品常用的一种情景就是在链路当中进行访问控制，只有通过认证的终端才能访问外网，或者控制部分终端必须要进行认证，其他终端可以正常访问外网。

ACG1000 设备本地 web 认证功能异常的主要排查思路如下：查看设备上的认证策略是否正常配置，全局配置当中识别范围和识别模式是否正确，路由是否正常，设备是否开启 HTTPS 网页跳转，本地认证环境是否支持本地 web 认证。

二、流程图相关操作说明：

1、检查认证策略配置

ACG1000 系列设备上做本地 portal 认证，用户只能先通过设备认证之后才能上网，所以先要配置相应的认证策略，限制网络中需要认证的用户进行认证，其他用户无需认证。ACG1000 设备配置 Web 认证时，允许用户的 TCP 三次握手报文通过，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 IP 地址排除。目前仅支持排除 IP 地址，不支持排除域名。

认证策略包括对认证终端源目地址、出入接口、时间段的限制，如果限制的因素不包含想要做本地认证的终端的条件，那么本地认证就会失败。查看认证策略的路径为:【用户管理】-【认证策略】。

2、修改认证策略

认证策略主要是从源接口、源地址、目的接口、目的地址、时间这五个方面来对认证终端进行限制，如果认证终端的源目地址不在认证策略限制范围内，会导致认证失败，其他因素同理。另外需要强调的一点是，桥模式部署时，出入接口写桥接口或者桥接口下的物理口均可。五个因素具体的设置方式如下：

1） 确认需要进行本地认证的网段在源地址范围内，如果所有网段均需要认证的话，可以下拉选择“any”，也可以针对现网客户的需求对目的网段进行设置。配置认证策略点击【用户管理】-【认证策略】

2） 确认需要认证的终端与设备通信的出入接口是正确的，如果全部接口的流量都需要进行认证的话可以下拉选择“any”，现场 ACG1000 设备如果是二层部署，接口为桥接口的话，这个地方的源目接口可以填实际的物理接口也可以填 bvi 口。

3） 确认现场认证的时间段在当前时间段内，如果没有特殊要求可以选择“always”。

3、检查识别配置

本地认证用户的地址必须是能够被设备识别成用户，如果设备上不能将这个流量识别成用户的话，那么相当于是设备将这些流量进行了三层转发，也就不会触发本地认证的机制了，客户现场如果配置的识别范围包括认证的网段或者配置成“any”，那么识别模式配置成启发模式或者强制模式均可。如果现场配置的识别范围不包括认证的终端设备的网段，那么识别模式就必须配置成启发模式。

识别模式：

识别模式分为“启发模式”和“强制模式”两种，默认配置为强制模式，识别范围默认配置均为 private 私网地址段。

“启发模式”指的是，优先将属于识别范围的 IP 地址识别为在线用户，并且根据流量发

起方先识别源 IP，再识别目的 IP，如果源 IP 和目的 IP 都不在识别范围中时则将源 IP 识别为在线用户。

“启发模式”使用场景：对用户识别要求不严格的情况下使用启发模式，在线用户中会出现非识别范围内的用户（如：同时出现私网 IP 和公网 IP 的用户），所以统计到的在线用户数量会比较多，在此模式下需要将识别范围修改成内网实际使用的地址网段，否则会导致用户识别不精确。

“强制模式”指的是，只将属于识别范围的 IP 地址识别为在线用户，并且根据流量发起方先识别源 IP，再识别目的 IP，只有源 IP 或目的 IP 地址中的一个属于识别范围时，才会被识别为在线用户；否则此 IP 地址流量不受系统转发流程中用户识别后的所有功能模块限制，如：用户策略、安全策略、应用识别和审计、入侵检测、病毒防护、QOS。

“强制模式”使用场景：对用户识别要求严格的情况下使用强制模式，在线用户中只会存在识别范围内的用户，过滤掉了不属于内网地址段的用户，精简了在线用户列表，只显示用户真正关心的数据，同时提升了设备性能，不在识别范围内的 IP 流量不走用户认证流程，避免了对用户不关心数据的处理，在此模式下务必将识别范围修改成内网实际使用的地址网段，避免因识别范围配置错误导致的用户关心的 IP 地址流量不受用户策略控制的情况出现。

4、修改识别范围和识别模式

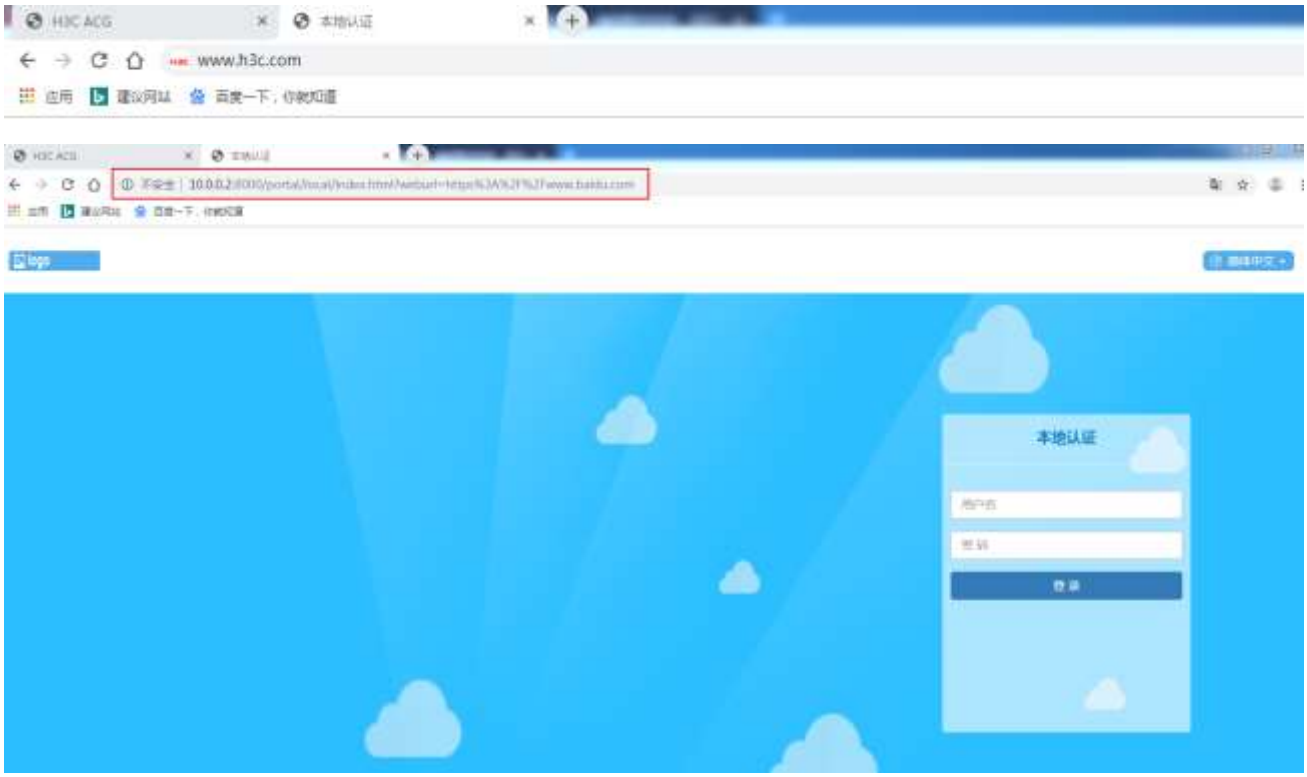
需要在【用户管理】-【全局配置】-【识别配置】对识别范围和识别模式进行配置。保证认证用户的地址可以被识别成用户，否则无法触发本地 web 认证。

5、检查是否是 HTTPS 跳转

终端在跳转认证界面时，经常性的操作方法就是打开浏览器，随意点开一个网站，例如 1.1.1.1.（https://1.1.1.1）或者百度（https://www.baidu.com）等,此时，浏览器页面无法正常跳转到 web 登录页面;如果客户打开的是新华三集团首页(http://www.h3c.com),此时页面可以正常跳转到 portal 登录界面，如果随意点开的 URL 是 HTTPS 的，设备上默认无法解析加密的 URL 链接导致跳转失败，此时需要进入设备的命令行使能 HTTPS 跳转功能。

异常跳转界面：

正常跳转界面：



6、开启 HTTPS 跳转

设备默认是没有使能 HTTPS 跳转功能的，需要登录设备的命令行（console、Telnet、SSH 等），进入命令行配置界面开启如下命令，即可实现 HTTPS 链接跳转 portal 的功能。

命令：user-policy https-portal enable

如示例在设备的命令行分别开启 HTTPS 跳转 portal。

```
H3C-ACG> enable
H3C-ACG# configure terminal
H3C-ACG(config)# user-policy https-portal enable     //开启 HTTPS 跳转
```

7、检查路由配置

ACG1000 做本地 web 认证的话，必须保证设备是用三层口与上下行设备进行通信的，桥模式部署情况下必须给桥接口配置地址，然后用这个地址与上下行设备进行通信，这样才能拦截终端的 HTTP 的 get 请求。

1) 串联部署：ACG1000 设备可以二层部署在链路当中，也可以三层部署在链路当中。如果是二层部署的话，ACG1000 与终端和外网之间的访问都是通过桥接口进行访问的，那么设备上的缺省路由的出接口应该走的是桥接口，注意桥接口一定要配置地址。如果 ACG1000 设备是三层部署，那么设备上的缺省路由应该是由指定得到三层口出去，如果路由有问题，就会导致 portal 弹出异常。

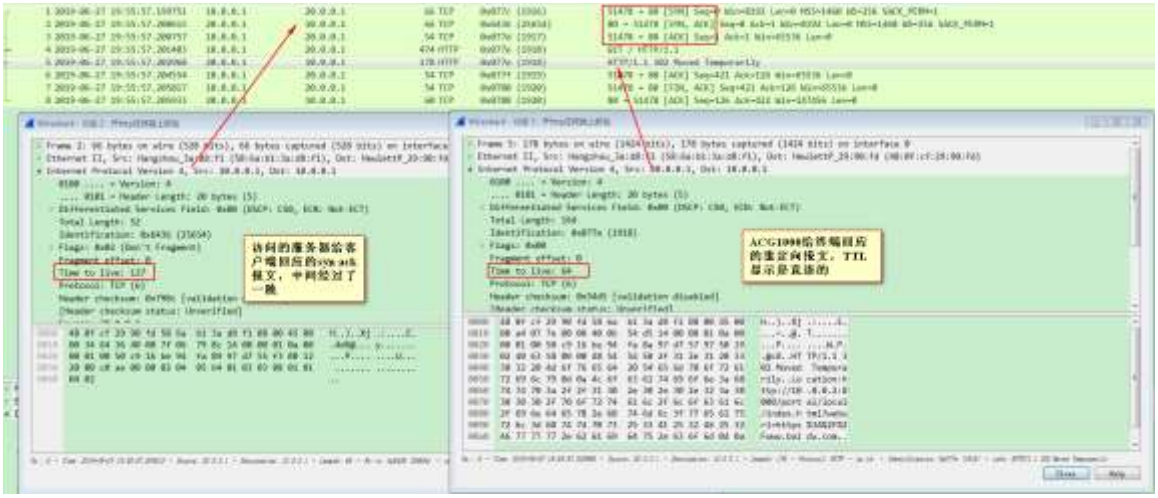
2) 旁路部署：在某些特殊组网情况下，ACG1000 设备也会旁挂部署在组网当中，此时设备上开启本地 web 认证时，需要保证来回的三次握手交互报文都要上到 ACG1000 设备上，可以在设备上指定旁挂的那个接口上进行抓包，若抓包当中有来回的报文，则证明来回报文都上到了设备上。抓包路径:【系统管理】-【系统维护】-【抓包工具】

8、修改设备路由配置

如果设备上三层口是客户端的网关，但是与外网通信的又是桥接口，这样会导致设备弹出认证界面异常，无法正常进行本地 web 认证，这种情况下就要梳理清楚现网的组网情况，确认现场是二层组网还是三层组网，如果组网有问题，需要现场修改现场配置。查看设备上路由的方式【网络接口】-【路由】-【路由表】，查看现场路由配置是否正常。

9、确认是否提供 web 环境

ACG1000 设备的本地 web 认证功能并不是拦截终端的第一个报文然后直接给终端重定向到认证界面（http://10.0.0.2:8000/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。根据实验室抓包分析如下：



实验室搭建环境测试，发现 TCP 的三次握手报文均是被访问端与客户端直接进行访问的，而 ACG1000 只是在收到客户端的 HTTP 的 get 请求包的时候就将这个报文拦截下来，然后

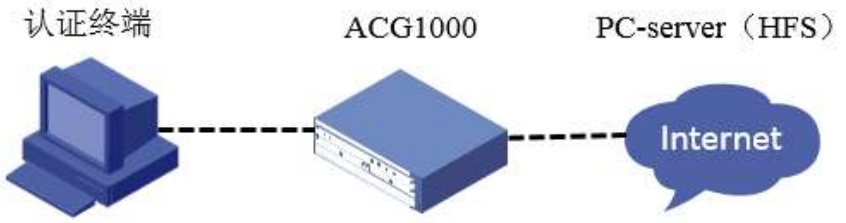
用被访问端的源地址给客户端回应一个重定向的报文将客户端的浏览器界面重定向到认证界面。所以，如果现场只是将一台 PC 接到 ACG1000 上面，开启了本地 web 认证，是无法弹出本地 web 认证页面的，因为这种情况下，无法完成三次握手的过程，也就无法拦截 get 请求对 web 界面进行重定向。所以，如果遇到 ACG1000 本地 web 认证异常时，查看配置均无问题的时候，需要确认现场的部署环境，是否有能够完成三次握手并发送 get 请求的环境。

10、本地认证环境举例

客户现场进行设备部署或是业务测试的时候，可以按如下方式搭建：

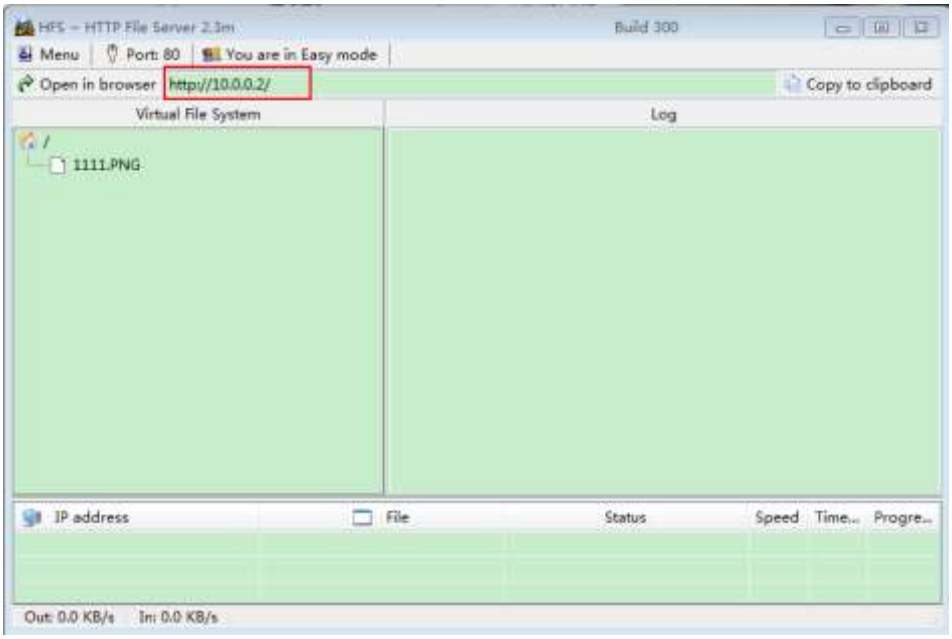
1) 现场有公网环境，可以将 ACG 串在内网终端到公网之间，正常配置本地认证策略，在终端浏览器上输入 HTTP（不加密，加密的要开启 HTTPS 跳转的命令）的链接，例如 http://www.h3c.com，有公网环境的话，就可以先与公网上的服务器进行三次握手之后然后跳转本地 web 认证界面，如果现在在设备上开启了上个步骤当中的 HTTPS 网页跳转的命令（user-policy https-portal enable），那么就能在浏览器当中随意点开一个网页，无论是 HTTP 还是 HTTPS 的链接，均会正常跳转认证界面。组网图如下：

2) 现场没有公网环境，进行功能测试。（一般是在测试的情况下可能不具备公网环境）有时候现场情况比较特殊，或者并不具备公网测试的环境，可以在局域网内搭建一个测试环境，在终端路由可达的的另外一台 PC 上面安装一个 HFS 软件，使得这个 PC 可以充当一个小型的 HTTP 服务器。



HFS（Http File Server）是一种上传文件的软件。 专为个人用户所设计的 HTTP 档案系统，下载后无须安装，只要执行 hfs.exe，直接将文件或者文件夹拖拽至 Virtual File System（虚拟档案系统）窗格下，即可新增/移除虚拟档案资料夹，这种方法可以简单可架设完成一个 HTTP 虚拟档案服务器。

认证终端的地址为 10.0.0.1，PC-server 的地址为 10.0.0.2，要保证两台 PC 之间是互通的，在 PC2 上安装 HFS 软件，可以直接在 HFS 官网上进行下载：http://www.rejetto.com/hfs/?f=dl，并上传一个任意的文件到 HFS 软件上。HFS 的安装使用方式可以自行百度，安装完成之后，直接点开下载的 hfs.exe 启动 该软件会自动使用设备的网卡地址（1.1.1.2）作为 host 字段，如下图所示：



在 PC1 上打开浏览器，输入 HFS 软件上产生的 URL，即可在 PC1 上用浏览器打开这个

文件服务器。

在认证终端上访问这个服务器 http://10.0.0.2，就会正常跳转如下认证页面，即可测试本地 web 认证功能是正常的。