

# 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](#)

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系列透明部署下HTTPS解密配置方法

### 目录

#### [1 配置需求或说明](#)

##### [1.1 适用的产品系列](#)

##### [1.2 配置需求及实现的效果](#)

#### [2 组网图](#)

#### [3 配置步骤](#)

##### [3.1 登录设备管理界面](#)

##### [3.2 配置连接路由器接口](#)

##### [3.3 配置连接局域网的接口](#)

##### [3.4 配置网桥接口](#)

##### [3.5 配置路由](#)

##### [3.6 开启设备DNS代理](#)

##### [3.7 配置HTTPS对象](#)

##### [3.8 生成CA根证书](#)

##### [3.9 导出CA根证书](#)

[3.10 将导出的CA根证书导入本地证书](#)

[3.11 配置IPV4审计策略](#)

[3.12 更改设备管理端口](#)

[3.13 配置HTTPS解密策略](#)

[3.14 配置保存](#)

[3.15 结果验证](#)

[3.16 注意事项](#)

## 1 配置需求或说明

### 1.1 适用的产品系列

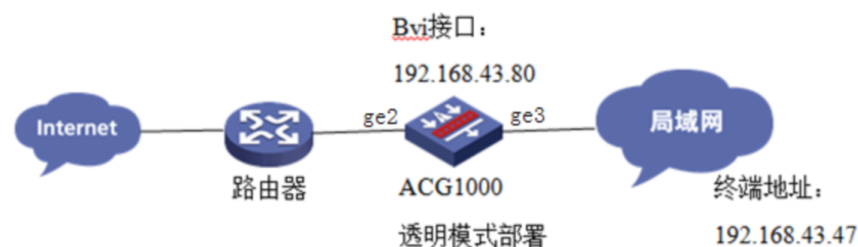
本案例适用于软件平台为ACG1000系列应用控制网关：  
ACG10X0、ACG1000-AKXXX等。

*注：本案例是在ACG1040的Version 1.10, Release 6609P06版本  
上进行配置和验证的。*

### 1.2 配置需求及实现的效果

如下组网图所示，需要在原有的网络中增加ACG1040审计内网用户访问百度、淘宝等HTTPS网站的记录，但又不想对原有网络配置进行变动，所以ACG1040采用透明模式部署。

## 2 组网图



## 3 配置步骤

### 3.1 登录设备管理界面

设备管理口（ge0）的默认地址配置为192.168.1.1/24。默认允许对该接口进行PING，HTTPS操作。将终端与设备ge0端口互联，在终端打开浏览器输入https://192.168.1.1登录设备管理界面。默认用户名与密码均为admin。



### 3.2 配置连接路由器接口

#选择“网络配置”>“接口”>“物理接口”中点击ge2接口后的编辑按钮，进行端口修改。

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											
	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0		192.168.1.1/24		58:6a:b1:c4:5	route	full	1000	up		
2	ge1				58:6a:b1:c4:5	route	full	1000	down		
3	ge2				58:6a:b1:c4:5	route	full	1000	up		
4	ge3				58:6a:b1:c4:5	route	full	1000	up		

#在接口选项下的“高级设置”>“接口属性”中将ge2接口设置

为外网接口。

高级配置

协商模式 ☒ 自动 ☐ 强制

MTU  (1280-1500)

接口属性 ☐ 内网口 ☒ 外网口

### 3.3 配置连接局域网的接口

#选择“网络配置”>“接口”>“物理接口”中点击ge3接口后的编辑按钮，进行端口修改。

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					
接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作	
1	ge0		192.168.1.1/24	58:6a:b1:c4:5	route	full	1000	up			
2	ge1			58:6a:b1:c4:5	route	full	1000	down			
3	ge2			58:6a:b1:c4:5	route	full	1000	up			
4	ge3			58:6a:b1:c4:5	route	full	1000	up			

#在接口选项下的“高级设置”>“接口属性”中将ge3接口设置为内网接口。

高级配置

协商模式 ☒ 自动 ☐ 强制

MTU  (1280-1500)

接口属性 ☒ 内网口 ☐ 外网口

### 3.4 配置网桥接口

#选择“网络配置”>“接口”>“网桥接口”>“新建”中创建网桥接口。Bvi ID设置可以从0-255数据中选取配置，将ge2与ge3端口点击箭头移动到右侧栏中，并且为bvi接口设置IP地址192.168.43.80用于管理ACG1040。

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
<div>  新建            删除         </div>						
<input type="checkbox"/>	接口名称	描述	包含接口	IP地址		

**桥接口**

名称 bvi 1 (0-255)

描述 (0-127 字符)

网桥可选接口

ge6	>	ge2
ge8	<	ge3
ge9		
ge11		
agg2		

启用 ☒

IP类型 **IPv4** IPv6

地址模式 ☒ 静态地址 ☐ DHCP ☐ PPPOE

接口主地址 192.168.43.80/24 (例如：192.168.1.1/24)

接口相关设定

管理方式 ☒ Https ☒ Http ☒ Ssh ☒ Telnet ☒ Ping ☒ Center-monitor

MTU 1500 (1280-1500)

**提交** **取消**

#在接口相关设定中将管理方式全部选择，点击“提交”按钮。

### 3.5 配置路由

#选择“网络配置”>“路由”>“静态路由”>“新建”中创建静态路由。目的地址和掩码都设置为：0.0.0.0（代表所有网段），下一跳地址配置192.168.43.0网段的网关地址：192.168.43.1，配置完成后点击提交。

**静态路由**

目的地址 0.0.0.0

子网掩码 0.0.0.0

下一跳/出接口 ☒ 下一跳 ☐ 出接口

下一跳 192.168.43.1

权重 1 (1-255)

距离 1 (1-255)

地址探测 -

**提交** **取消**

### 3.6 开启设备DNS代理

#在“网络配置”>“DNS”>“DNS服务器”，启用DNS代理并配置DNS服务器地址，下图以114.114.114.114、8.8.8.8举例，



### 3.7 配置HTTPS对象

#进入“对象管理>URL>HTTPS对象”中新建HTTPS对象。



### 3.8 生成CA根证书

#进入“对象管理>CA服务器>根CA配置管理>生成CA根证书”中生成CA根证书。



### 3.9 导出CA根证书

#进入“对象管理>CA服务器>根CA配置管理>导出CA根证书”导出CA根证书。



### 3.10 将导出的CA根证书导入本地证书

#选择“本地证书>导入”，将之前生成的CA根证书导入本地证书。



### 3.11 配置IPV4审计策略

#选择“上网行为管理”>“策略配置”>“IPV4策略”>“新建”中创建审计策略。

注：下图中各参数使用默认配置即可。

策略属性

动作 ☒ 审计 ☐ 免审计 ☐ 拒绝

老化时间  (0-100000000/秒,默认值是0,即表示使用各个协议默认的老化时间)

描述  (0-127 字符)

启用 ☒

匹配条件

用户  [选择用户](#)

源接口/域  目的接口/域

源地址  [选择地址](#)

目的地址  [选择地址](#)

时间

服务  [选择服务](#)

应用

应用策略

应用审计

☒ 新建 ☐ 匹配选项： ☒ 全匹配 ☐ 顺序匹配

应用	行为	内容	选项	关键字	级别	动作	启用	描述
----	----	----	----	-----	----	----	----	----

新建应用审计策略用来审计所有应用。



注：这里的日志级别需要设置为信息，否则设备不记录日志。

新建URL审计策略审计所有网站，配置完成后选择提交完成所有配置。

### 3.12 更改设备管理端口

#因为设备管理界面默认使用443与HTTPS解密策略冲突，因此需要将设备管理端口设置为1443，设置完成后

https://192.168.1.1:1443重新登录设备。



### 3.13 配置HTTPS解密策略

#配置HTTPS解密策略并调用之前生成的CA根证书。



### 3.14 配置保存

#在设备管理界面右上角点击配置保存，保存当前配置。

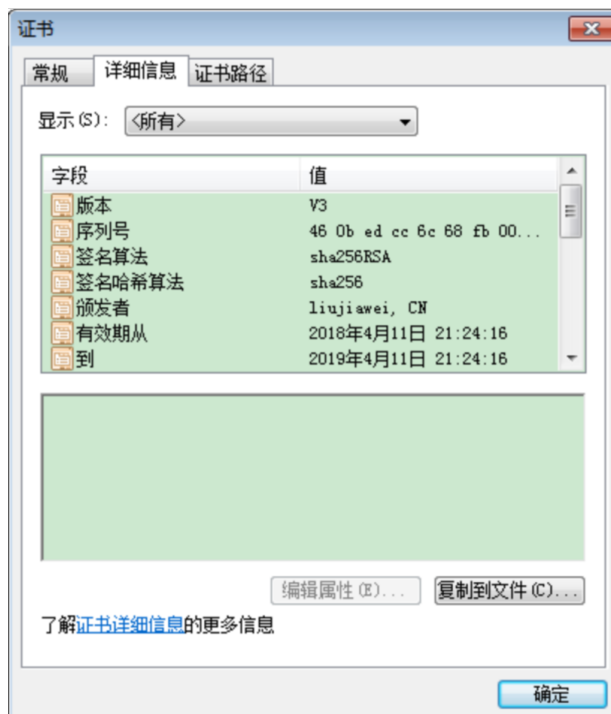


### 3.15 结果验证

#打开网页输入**www.baidu.com**验证配置结果，因为是设备颁发的证书部分浏览器可能需要验证证书的安全性，选择是即可。



查看浏览器获取到的证书是之前生成的**CA根证书**。



在“日志查询>访问网站日志”中已经可以审计到用户访问百度的记录了,说明ACG1040成功审计到了HTTPS网站。



用户	用户mac	URL分类	网页标题	URL	处理动作	级别	时间
1	192.168.1.2	48:0f:cd:27:79:24	门户网站与搜索引擎	百度一下, 你就知道	放行	信息	2018-04-12 21:25:04
2	192.168.1.2	48:0f:cd:27:79:24	门户网站与搜索引擎	百度一下, 你就知道	放行	信息	2018-04-12 21:15:09
3	192.168.1.2	48:0f:cd:27:79:24	门户网站与搜索引擎	百度一下, 你就知道	放行	信息	2018-04-12 21:14:55

## 3.16 注意事项

- 1、目前ACG1000默认情况下只能过滤HTTP网页, 如果遇到HTTPS网页如百度、淘宝、京东等需要配置HTTPS解密策略, 才能正常过滤。

**注: HTTPS解密策略需要升级ACG版本至R6608以上版本才能支持。**