

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](#)

ACG HTTPS网站过滤配置案例

目录

[ACG HTTPS网站过滤配置案例](#)

[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ACG](#)

[3.2 配置地址对象、URL对象、HTTPS对象](#)

[3.3 生成CA证书](#)

[3.4 配置IPv4策略](#)

[3.5 配置解密策略](#)

[3.6 添加DNS](#)

[3.7 安装证书](#)

[3.8 保存配置](#)

[3.9 查看与验证](#)

[4 注意事项](#)

[4.1 开启HTTPS解密时请先修改WEB登录端口。](#)

[4.2 浏览器如果可以获取证书是不需要导入客户端证书的。](#)

1 配置需求或说明

1.1 适用的产品系列

本案例适用于ACG1000系列应用控制网关：ACG1000-T、ACG1000-M、ACG1000-AG、ACG1000-SE、ACG1000-s、等。

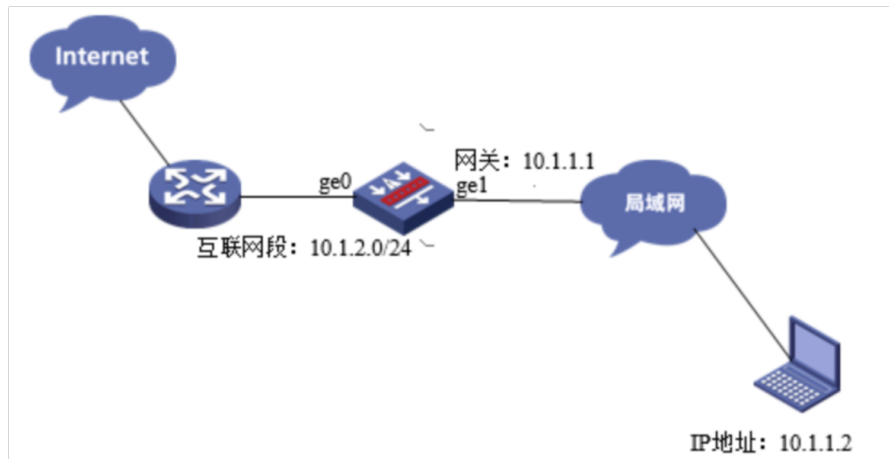
注：本案例是在ACG1000-S Version 1.10,Release 6609P02版本上进行配置和验证的。

1.2 配置需求及实现的效果

如下组网图所示，内网用户网段为：10.1.1.0/24。将ACG1000设备的ge0和ge1串接部署在核心交换机和出口路由器之间，启用URL过滤功能，实现内网用户不能访问百度网站但可以访问其他网站的需求。

注：本案例重点描述网站过滤配置，设备上网配置略。

2 组网图



3 配置步骤

3.1 登录ACG

#设备管理口（ge1）的地址配置为10.1.1.1。允许对该接口进行PING、HTTPS操作。将终端与设备ge1端口互联，在终端打开浏览器输入<https://10.1.1.1>登录设备管理界面。默认用户名与密码均为admin。



3.2 配置地址对象、URL对象、HTTPS对象

#点击“对象管理”>“地址”>“IPv4地址对象”，点击“新建”。IP地址配置为10.1.1.0/24，创建内网网段地址对象

地址对象

名称: 内网网段 (1-31字符)

描述: (0-127 字符)

地址项目: ☒ 子网地址 ☐ 范围地址 ☐ 主机地址 ☐ 域名 ☒ 添加到列表

(例如: 192.168.1.1/24)

已添加项目

	类型	地址	操作
1	network	10.1.1.0/24	删除

排除地址: (多项用, 隔开, 格式如: 1.1.1.1,3.3.3.3-4.4.4.4,baidu.com)

#点击“对象管理”>“URL”>“HTTPS对象”，点击<新建>，配置https对象，勾选域名列表中所有选项，点击“提交”确定。

HTTPS对象

名称: https对象 (1-31 字符)

描述: (0-127 字符)

自定义https对象 >>

选择域名对象

已选预定分类: BBS站点;商业;娱乐;游戏;网络资源;求职招聘;网上交易;新闻媒体;在线聊天;门户网站与搜索引擎 ... (共13个)

域名列表

		分类
1	<input checked="" type="checkbox"/>	BBS站点
2	<input checked="" type="checkbox"/>	商业
3	<input checked="" type="checkbox"/>	娱乐
4	<input checked="" type="checkbox"/>	游戏
5	<input checked="" type="checkbox"/>	网络资源
6	<input checked="" type="checkbox"/>	求职招聘
7	<input checked="" type="checkbox"/>	网上交易
8	<input checked="" type="checkbox"/>	新闻媒体
9	<input checked="" type="checkbox"/>	在线聊天
10	<input checked="" type="checkbox"/>	门户网站与搜索引擎

#点击“对象管理”>“URL”>“自定义URL”，点击<新建>，配置自定义URL对象百度，“内容”配置为baidu，点击<提交>。



自定义URL

名称 (1-31 字符)

内容 (如: www.baidu.com且URL以回车分隔, 注意:URL配置严格区分大小写)

3.3 生成CA证书

点击“对象管理” — “CA服务器” — “根CA配置管理”，点击“生成CA根证书”。输入证书名称为“https”，设置有效期为最大的18000天。



CA证书请求

证书名称 (1-31字符)

可选信息

部门

组织

位置(城市)

州/省

国家/地区

电子邮件

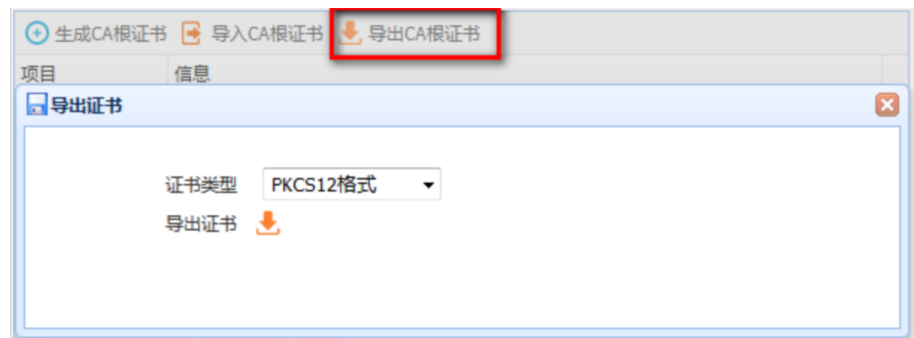
有效期 (1-18000 天)

密码 (0-63字符, 默认为空)

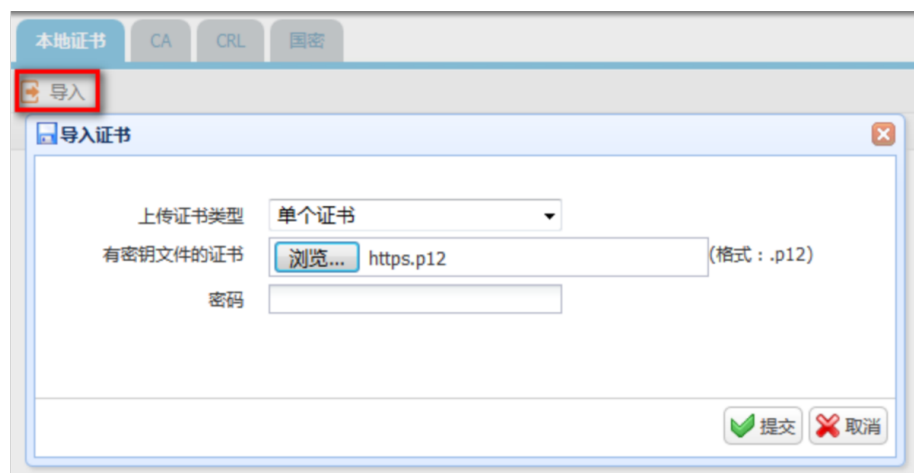
密钥大小

#生成CA证书后，点击“导出CA根证书”，将证书保存在电脑

上。



点击“对象管理” — “本地证书” — “证书”，在此页面导入刚刚保存的证书。



3.4 配置IPv4策略

点击“上网行为管理” — “策略配置” — “IPv4策略”，点击“新建”，源地地址参数选择创建的“内网网段”。

#点击URL审计下方的“新建”，在URL分类中选择创建的百度，处理动作选择拒绝（即拒绝网易的流量），日志级别选择信息。

3.5 配置解密策略

#点击“上网行为管理”——“解密策略”，选择“新建”。解密类型选择“https解密”，HTTPS对象选择创建“https对象”，并勾选启用。

解密策略

启用 ☒

入接口 any

源地址 any

目的地址 any

解密类型 https解密

HTTPS对象 https对象

排除站点 (如：www.baidu.com且URL之间使用“,”分隔,最多支持6个)

提交 取消

#在解密策略视图下，证书列表的下拉框中选择之前在本地证书中导入的证书（如连接ACG时为HTTPS方式登录，需要在系统管理—管理员—管理设定中修改https端口，否则下次无法登录）。

解密策略

新建 删除 启用 禁用 证书列表： https.cer 已选择证书：

3.6 添加DNS

#点击“网络配置”—“DNS”，进入DNS服务器页面，添加DNS服务器地址，可配置公有DNS，也可配置对应运营商的DNS。

域名管理 动态缓存 特定域名解析 DNS透明代理 DNS服务器

启用DNS代理 ☒

DNS 服务器1 114.114.114.114

DNS 服务器2 8.8.8.8

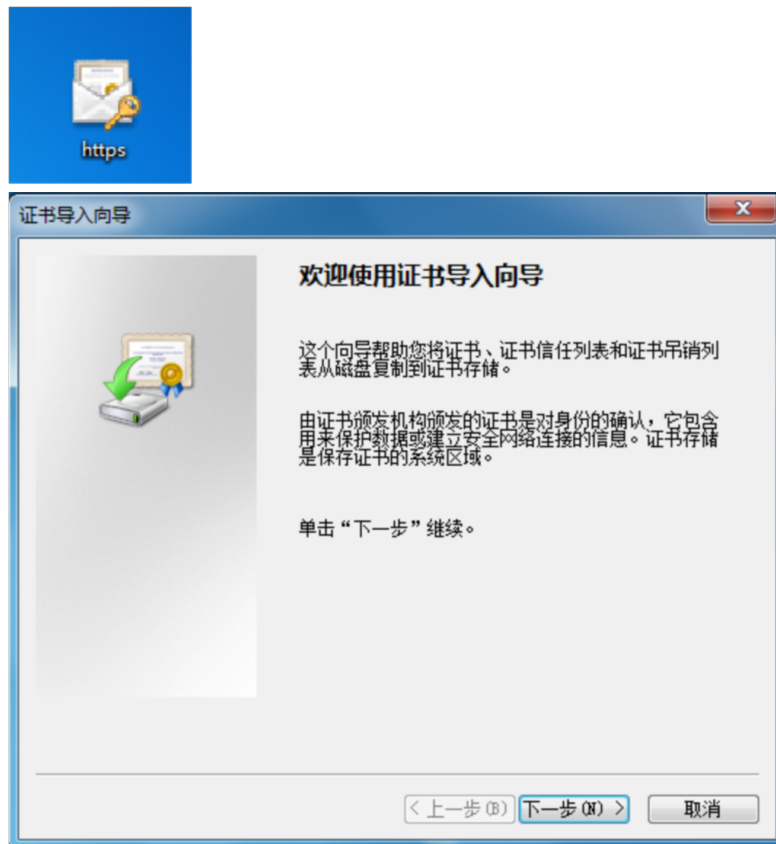
DNS 服务器3

DNS 服务器4

提交 取消

3.7 安装证书

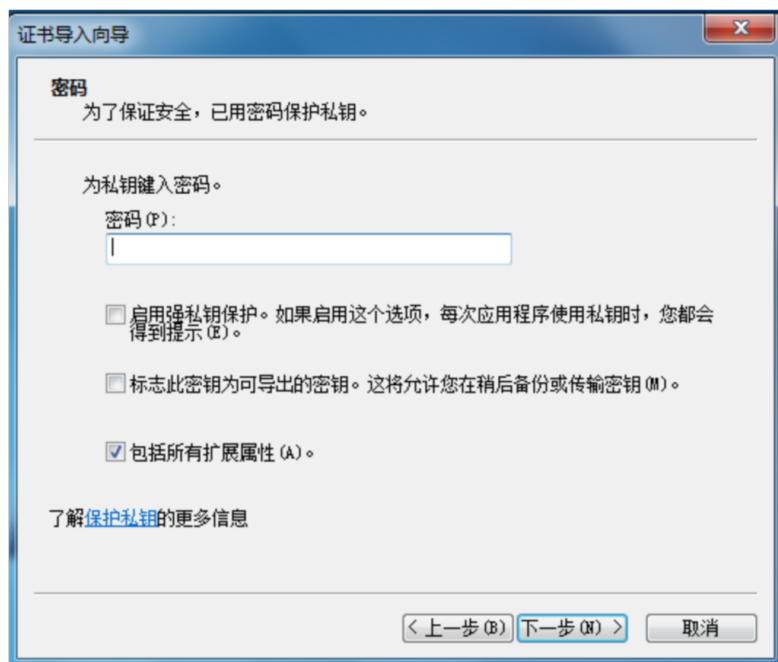
#双击打开从ACG上下载的证书。



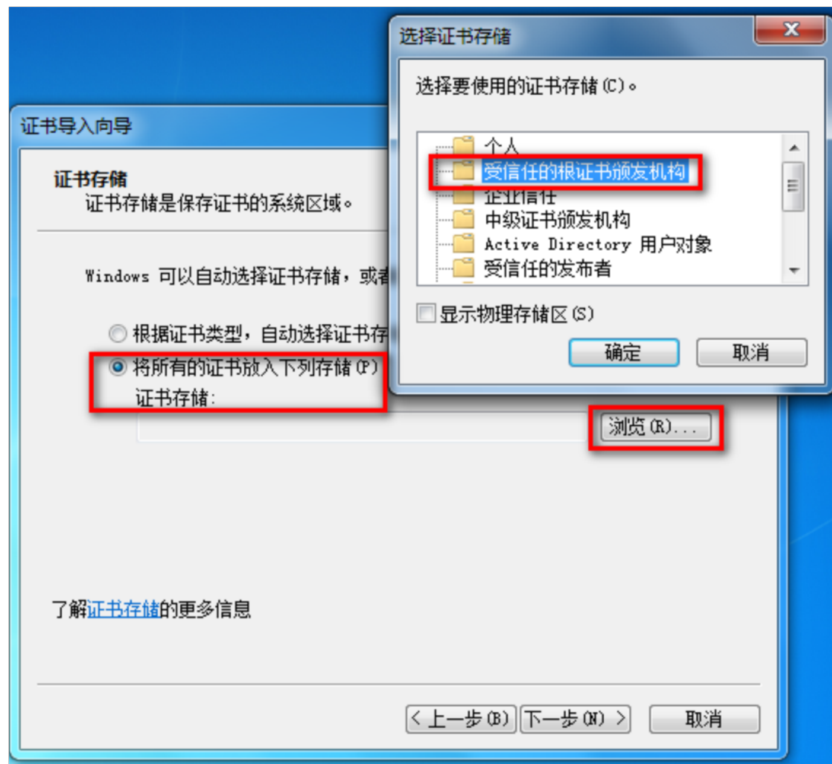
#选中证书的路径。



#输入生成证书时设置的密码，如未设置，直接点击“下一步”。



#选择“将所有的证书放入下列存储”，点击“浏览”，在弹出的对话框中选择“受信任的根证书颁发机构”，点击确定，并点击“下一步”。



#点击“完成”即可。



3.8 保存配置

#点击“配置保存”。



3.9 查看与验证

配置完成后在PC上访问百度，web界面显示访问被禁止。



注意事项

3.10 开启HTTPS解密时请先修改WEB登录端

□。

登录ACG使用的HTTPS端口为443与解密策略中的证书端口冲突，需要将WEB管理端口修改为443以外的其他端口。

点击“系统管理” — “管理员” — “管理设定”中修改https端口。

举例将HTTPS端口修改为4430，登录时使用
`https://192.168.1.1:4430`登录设备。



3.11 浏览器如果可以获取证书是不需要导入客户端证书的。

部分浏览器可以自动获取证书，这部分浏览器是不需要执行本案例中的证书导入过程的。