# 2 WEB在线代理

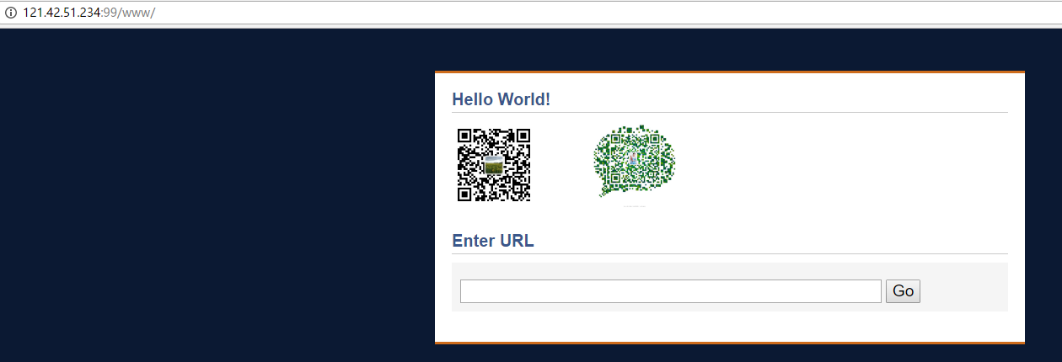
|  |
| --- |
| WEB在线代理使用示例  http://www.trustcomputing.com.cn/help/cn/dadi/proxy/online\_proxy.html |

## 2.1 使用WEB在线代理

WEB在线代理不需要事先做设置，直接打开浏览器就可以用，如图2-1所示，再在输入框中输入网址，点击“Go”按钮，就可以浏览。

HTTP协议缺省有两个端口可以用，一个是80，另一个是99（可修改），URL类似“http://121.42.51.234/www”，或者“http://121.42.51.234:99/www”。

HTTPS协议缺省有两个端口可以用，一个是443，另一个是100（可修改），URL类似“https://121.42.51.234/www”，或者“https://121.42.51.234:100/www”。



**图2-1** WEB在线代理界面

另外一个使用方法是直接指定网址浏览，URL类似“http://121.42.51.234:99/www/index.php?jump=https://www.google.com”。

如果无法正常浏览（输入URL后无反应或无限循环但是不显示内容），可以清除浏览器缓存及Cooike再试。

如有乱码，请切换浏览器的编码，Chrome浏览器可以下载安装“Set Character Encoding”插件，下载地址是

https://chrome.google.com/webstore/detail/set-character-encoding/bpojelgakakmcfmjfilgdlmhefphglae

对于https 类型的URL，而且服务器地址没有真实域名证书时，只能使用自签名证书，缺省CommonName/Subject Alternative Name/SAN是“zstdadi.com”，还需要在浏览器中导入自签名CA根证书，才能消除使用https链接时的证书安全提示，具体参见以下内容。

某些网站https证书配置错误或已被撤消（https://mawenjian.net/），无法使用chrome浏览器直接查看，可以使用WEB在线代理强制查看。

## 2.2 导入CA证书

对于https 类型的URL，而且服务器地址没有真实域名证书时，只能使用自签名证书，可以通过电子邮件、聊天软件、U盘等方式得到自签名CA证书，也可以通过在线下载的方式得到，URL类似“http://121.42.51.234/ikev2.crt”，后缀名还可以是.cer或.pem。

不同应用对于服务器证书认证的情形不一样，有的必须满足“服务器地址”和服务器证书的CommonName/Subject Alternative Name/SAN一致，否则不能连接，例如：Windows文件管理器挂载WebDAV、SSTP VPN、IKEV2 VPN，有的可以选择忽略警告继续连接(可能会受到中间人攻击)，具体情形详见下表：代表强制检查，代表非强制

|  |  |  |
| --- | --- | --- |
|  | OS及应用 | 说明 |
| WebDAV | Windows文件管理器 | 其它应用非强制，有的应用，例如winscp，没有警告；有的有警告，但是可以选择忽略继续连接 |
| WEB在线代理等其它https URL |  | 有警告，但是可以选择忽略继续连接 |
| IKEV2 VPN | 所有OS应用 |  |
| OCSERV VPN |  | 有警告，但是可以选择忽略继续连接 |
| PPTP VPN |  | 没有证书认证功能 |
| OpenVPN |  | 服务器和客户端的CA证书必须一致，但对“服务器地址”没有要求 |
| SoftEther VPN |  | 可选服务器证书验证 |
| L2TP VPN |  | 没有证书认证功能 |
| SSTP VPN | Windows内置VPN拨号 |  |

2.2.1.1 Windows系统的证书导入

IE/Chrome浏览器、WebDAV服务以及IKEV2/OCSERV/SSTP VPN等软件使用Windows系统内置的证书。双击ikev2.crt证书文件，出现“证书”窗口，如下图2-2所示。



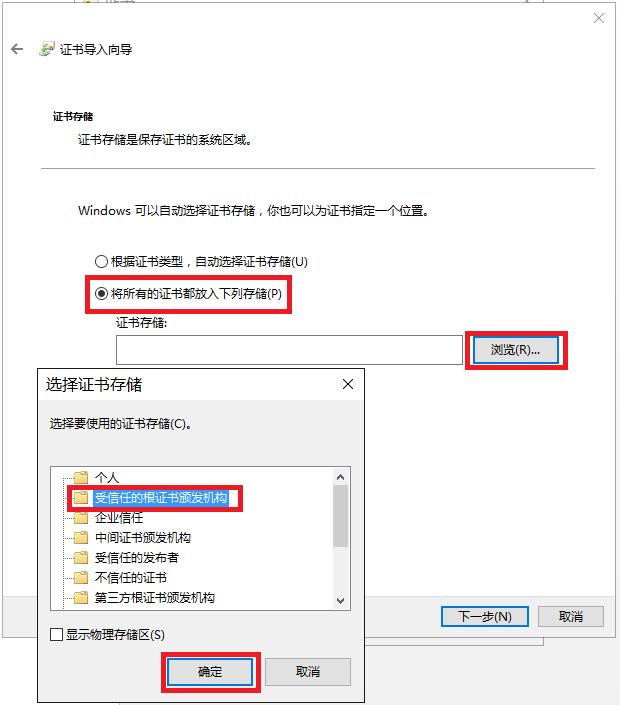
**图2-2** “证书”窗口

点击“安装证书”按钮，出现“证书导入向导”窗口1，如下图2-3-1所示。



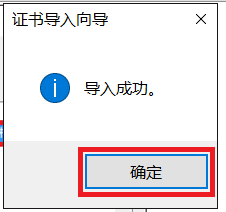
**图2-3-1** “证书导入窗口” 1

“存储位置”一定要选择“**本地计算机**”项，否则在IKEV2拨号中，会出现“IKE身份验证凭证不可接受”的错误。再点击“下一步”按钮，出现“证书导入向导”窗口2，如下图2-3-2所示。



**图2-3-2** “证书导入窗口”2

选择“将所有的证书都放入下列存储”项，再点击“浏览”按钮，出现“选择证书存储”窗口，选择“**受信任的根证书颁发机构**”项目，再点击“确定”按钮，之后，再点击窗口的“下一步”、“完成”按钮，最终会弹出导入成功窗口，如下图2-4所示，点击“确定”按钮关闭。



**图2-4** “导入成功”窗口

2.2.1.2 编辑hosts文件

导入证书后，如果证书的CommonName/Subject Alternative Name/SAN是IP，就不用域名解析或编辑hosts文件，直接使用“https://12.12.23.34/xxx”这样的链接。

如果是域名，要么修改DNS服务器配置，将该域名解析成对应的IP，客户端的DNS服务器还要能检索到该DNS服务器；要么修改Windows本地的hosts文件，即以管理员的身份编辑“C:\Windows\System32\drivers\etc\hosts”文件，

加入“12.12.23.34 zstdadi.com”这样的域名IP解析，保存文件后就可以使用“https://zstdadi.com/xxx”这样的带域名的链接，而不再出现证书安全提示了。

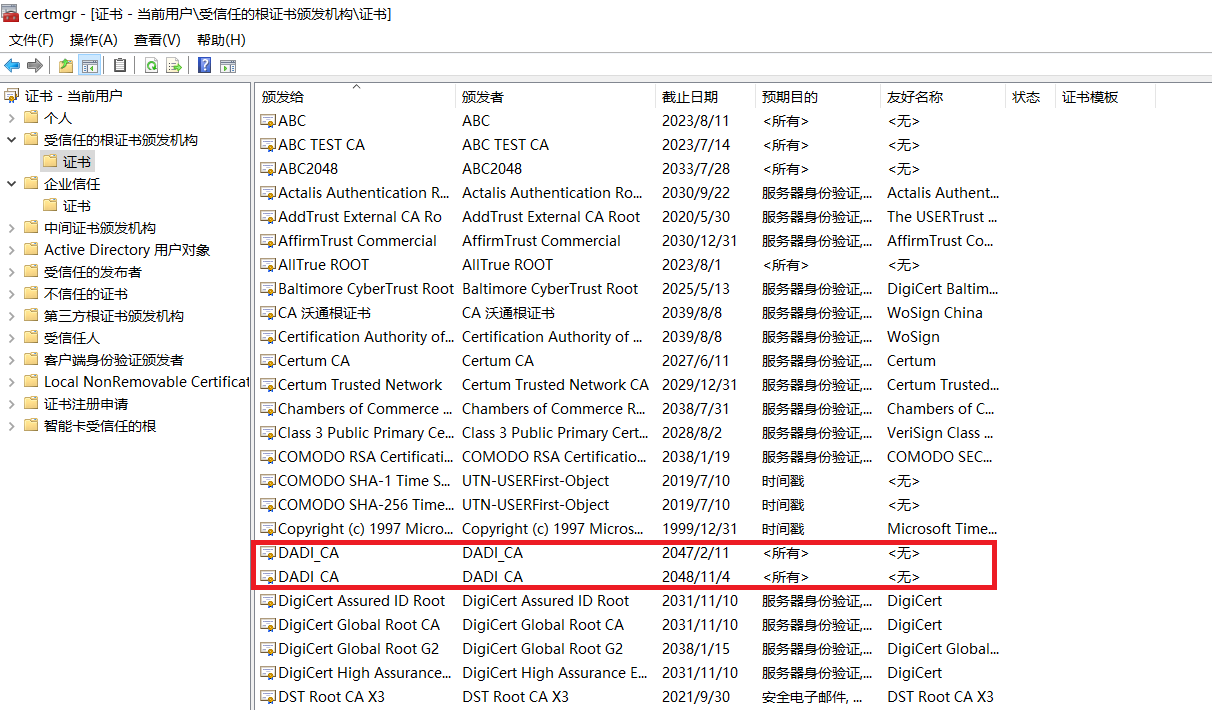
为了检验CA证书安装是否成功，可以打开测试URL“https://服务器地址”，如果没有安全警告，而且查看证书是有效的，如下图2-5所示，就表明CA证书安装成功。



**图2-5 检验CA证书有效性**

如果正常安装了自签名CA证书、修改了hosts文件后，浏览器仍然报错，可以清除SSL状态，或者重启浏览器再试。还可以运行certmgr证书管理器，如下图2-6所示，在“受信任的根证书颁发机构”证书中，找到“DADI\_CA”证书，全部删除后，重新安装自签名CA证书，再重启浏览器做测试。

访问纯IP的https地址不需要安装自签名CA证书，可以选择忽略错误并打开网页，如果浏览器报错（例如“您目前无法访问xxx，因为此网站发送了 Google Chrome 无法处理的杂乱凭据”等），并且无法进一步访问，可以删除“DADI\_CA”证书再试。

****

**图2-6** certmgr证书管理器

2.2.2 安卓系统的证书导入

可以直接通过浏览器从VPN服务器上下载得到，URL类似“http://121.42.51.234/ikev2.crt” 。crt文件下载完成后，自动弹出窗口，如下图2-7所示。



**图2-7** 安卓系统安装CA证书窗口

输入证书名称，并点击“确定”按钮，系统会提示“xxx安装成功”。

普通用户在安卓系统下无法编辑hosts文件，需要DNS服务器配合才能使用域名形式的“服务器地址”，所以尽量使用IP地址形式的“服务器地址”。

2.2.3 iOS系统的证书导入

通过浏览器下载并安装CA证书，URL类似“http://121.42.51.234/ikev2.crt”，下载成功后，会自动弹出“安装描述文件”窗口，点击右上角的“安装”按钮，安装过程中需要输入iOS的解锁密码，如下图2-8所示。

|  |  |
| --- | --- |
|  |  |

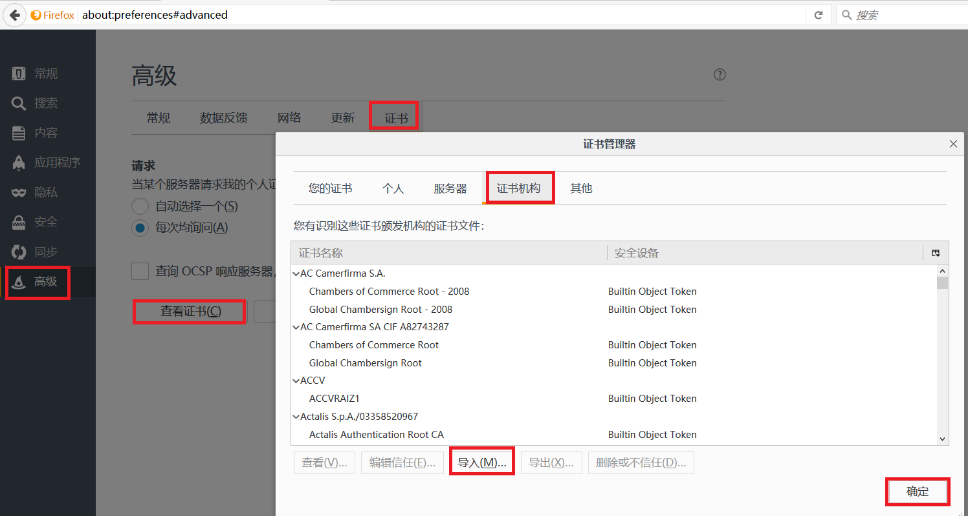


**图2-8** iOS系统安装CA证书窗口

普通用户在iOS系统下无法编辑hosts文件，需要DNS服务器配合才能使用域名形式的“服务器地址”，所以尽量使用IP地址形式的“服务器地址”。

2.2.4 Firefox的证书导入

Firefox浏览器需要单独导入CA证书，依次打开“选项>高级>证书>查看证书”，点击“证书机构”TAB，点击下方的“导入”按钮，选择ikev2.crt证书文件导入，最后再点击“确定”按钮，参见图2-9所示。



**图2-9** Firefox浏览器证书导入

如果遇到证书错误的提示，可以在“证书机构”中删除证书名称是“dadi”的所有证书，再重新导入新证书。