

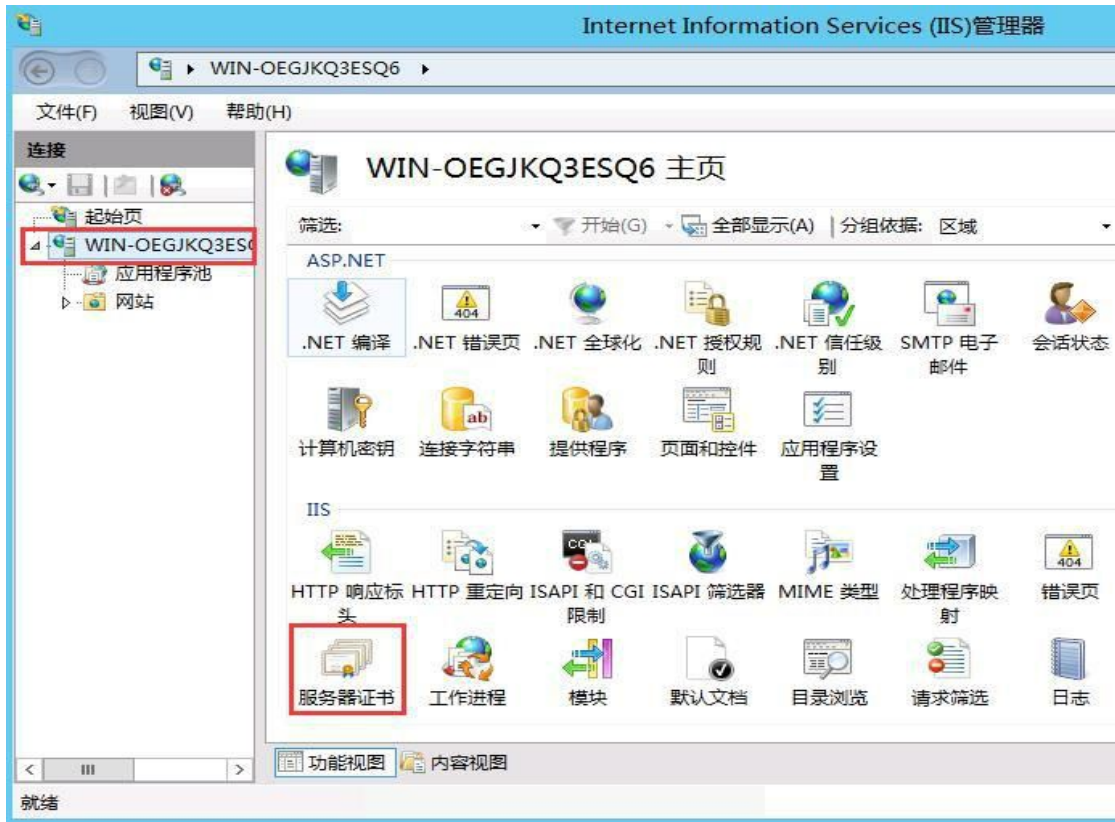
服务器 SSL 证书安装配置指南

IIS 8.0

更新日期：2016-11-7

第一步：生成证书签名请求文件(CSR)

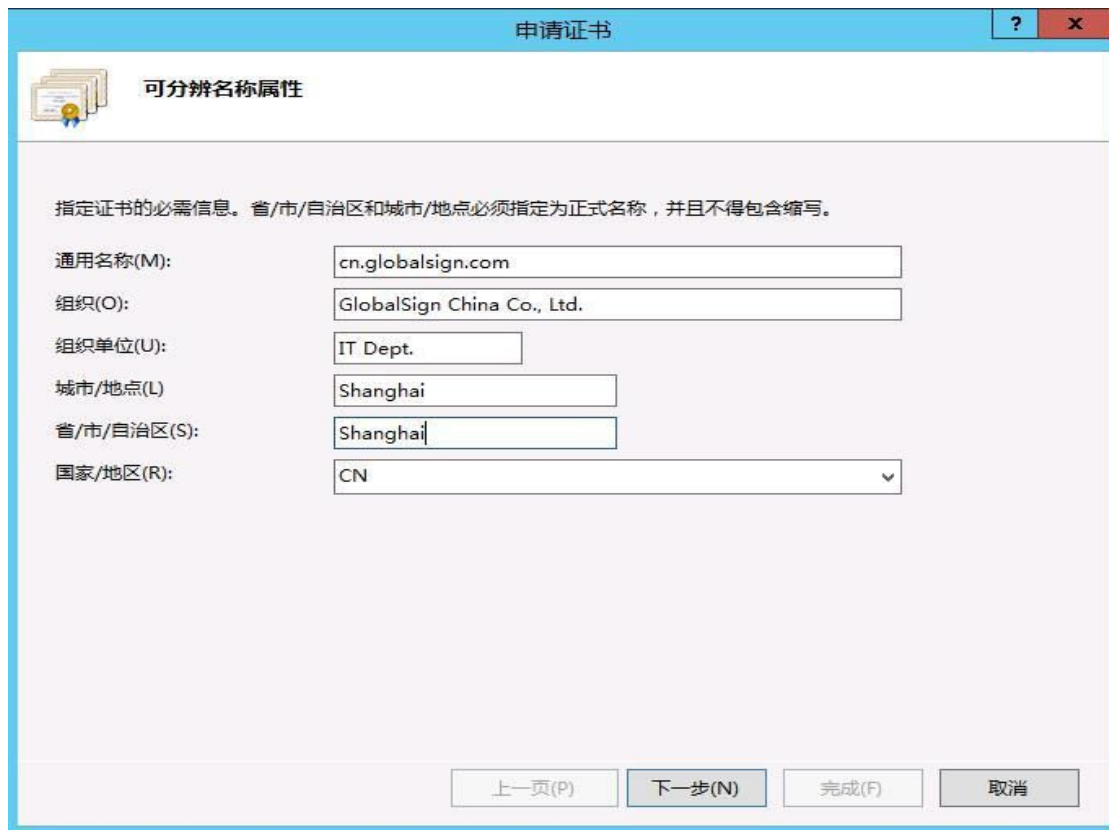
打开 IIS 服务管理器，点击**计算机名称**，双击打开右则的**服务器证书**图标



双击打开服务器证书后，点击右则的**创建证书申请**



输入申请证书信息，点击下一步

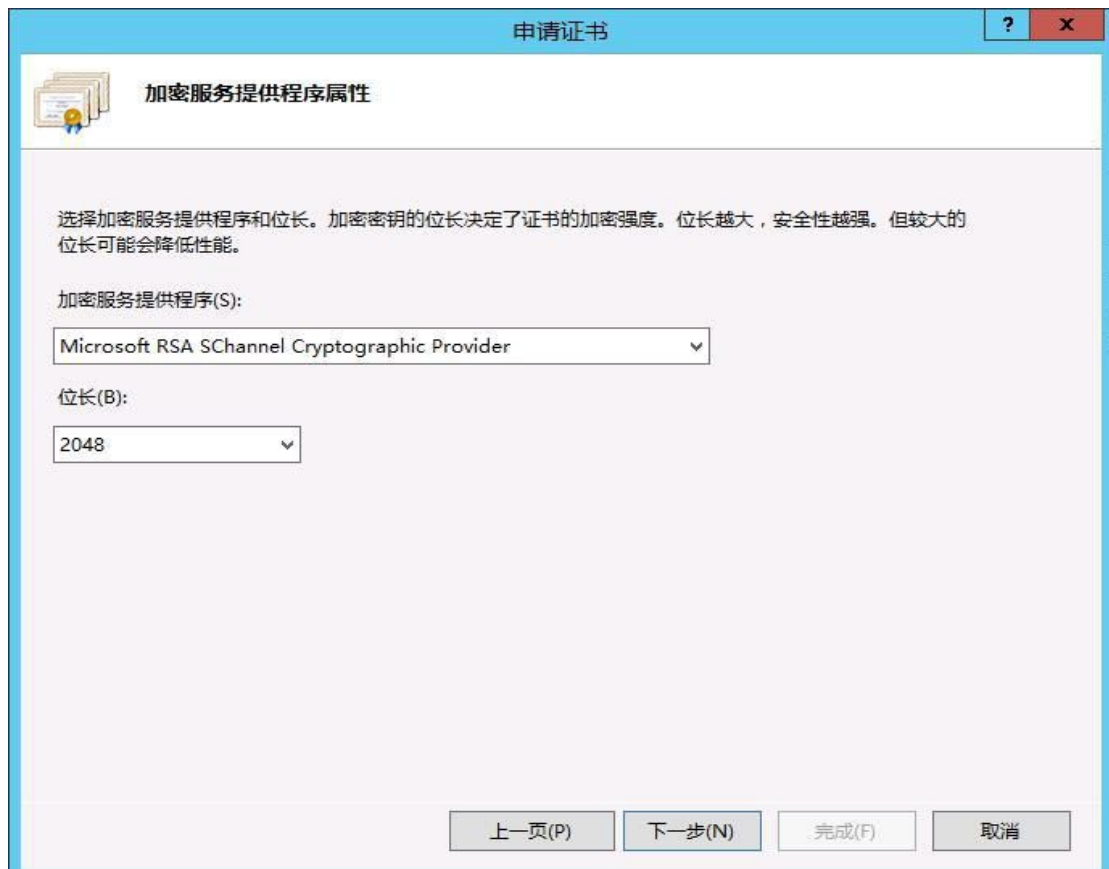


The screenshot shows a Windows dialog box titled "申请证书" (Request Certificate). The main heading is "可分辨名称属性" (Distinguished Name Properties). Below the heading, there is a note: "指定证书的必需信息。省/市/自治区和城市/地点必须指定为正式名称，并且不得包含缩写。" (Specify the required information for the certificate. Province/City/Autonomous Region and City/Location must be specified as formal names and must not contain abbreviations). The form contains the following fields:

通用名称(M):	cn.globalsign.com
组织(O):	GlobalSign China Co., Ltd.
组织单位(U):	IT Dept.
城市/地点(L):	Shanghai
省/市/自治区(S):	Shanghai
国家/地区(R):	CN

At the bottom of the dialog, there are four buttons: "上一页(P)" (Previous), "下一步(N)" (Next), "完成(F)" (Finish), and "取消" (Cancel).

选择加密服务提供程序和加密长度，建议默认，点击下一步

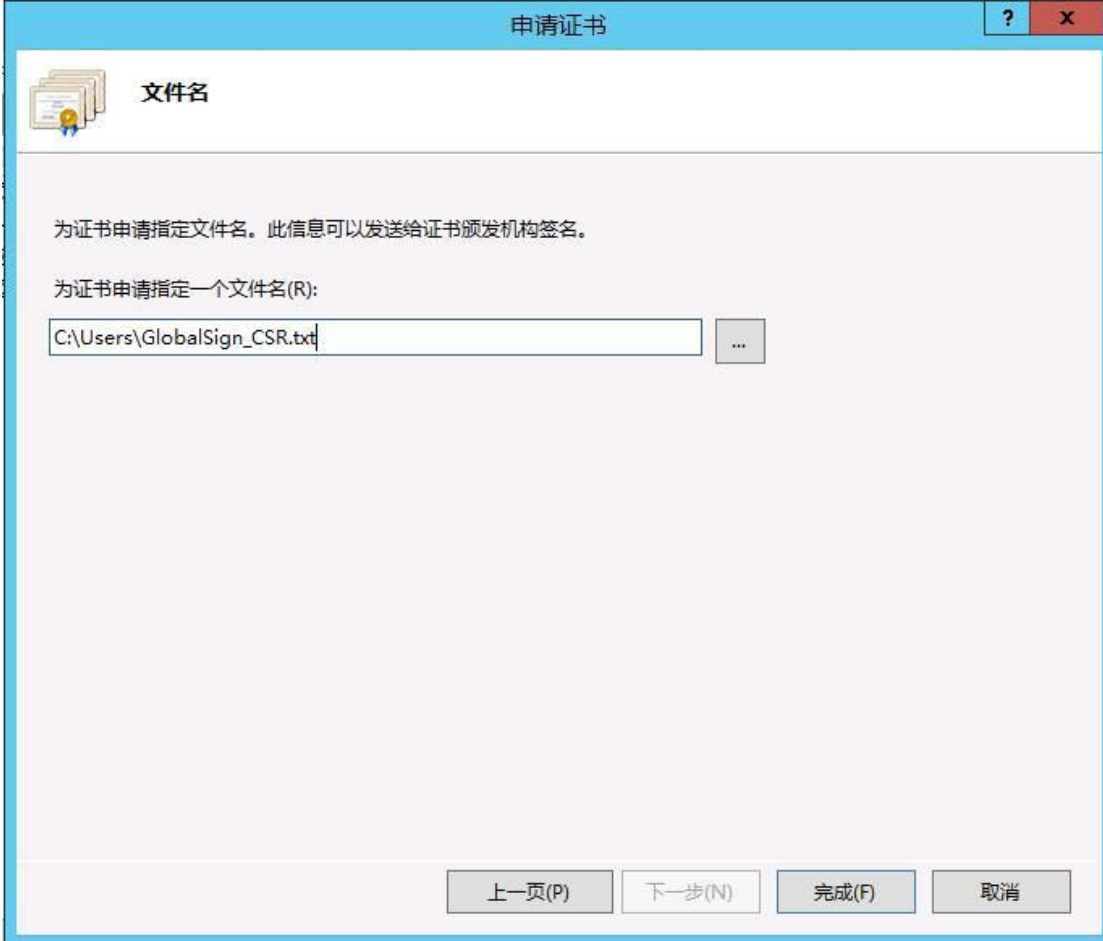


The screenshot shows a Windows dialog box titled "申请证书" (Request Certificate). The main heading is "加密服务提供程序属性" (Encryption Service Provider Properties). Below the heading, there is a note: "选择加密服务提供程序和位长。加密密钥的位长决定了证书的加密强度。位长越大，安全性越强。但较大的位长可能会降低性能。" (Select the encryption service provider and key length. The key length of the encryption key determines the encryption strength of the certificate. The larger the key length, the stronger the security. However, a larger key length may reduce performance). The form contains the following fields:

加密服务提供程序(S):	Microsoft RSA SChannel Cryptographic Provider
位长(B):	2048

At the bottom of the dialog, there are four buttons: "上一页(P)" (Previous), "下一步(N)" (Next), "完成(F)" (Finish), and "取消" (Cancel).

选择证书签名请求（CSR）文件保存的路径和文件名，点击**完成**



申请证书

文件名

为证书申请指定文件名。此信息可以发送给证书颁发机构签名。

为证书申请指定一个文件名(R):

C:\Users\GlobalSign_CSR.txt

...

上一页(P) 下一步(N) 完成(F) 取消

第二步：提交 CSR，申请证书

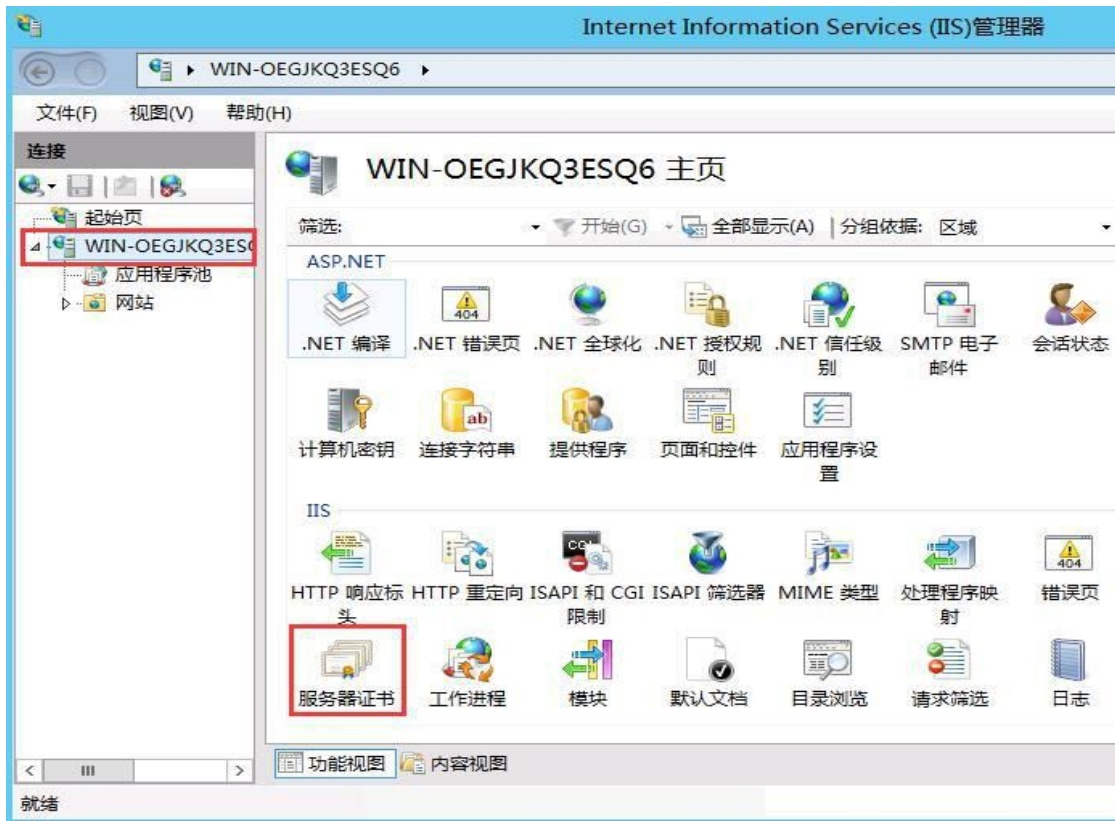
递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。
我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 server.cer（文本格式）。

第四步：安装服务器证书

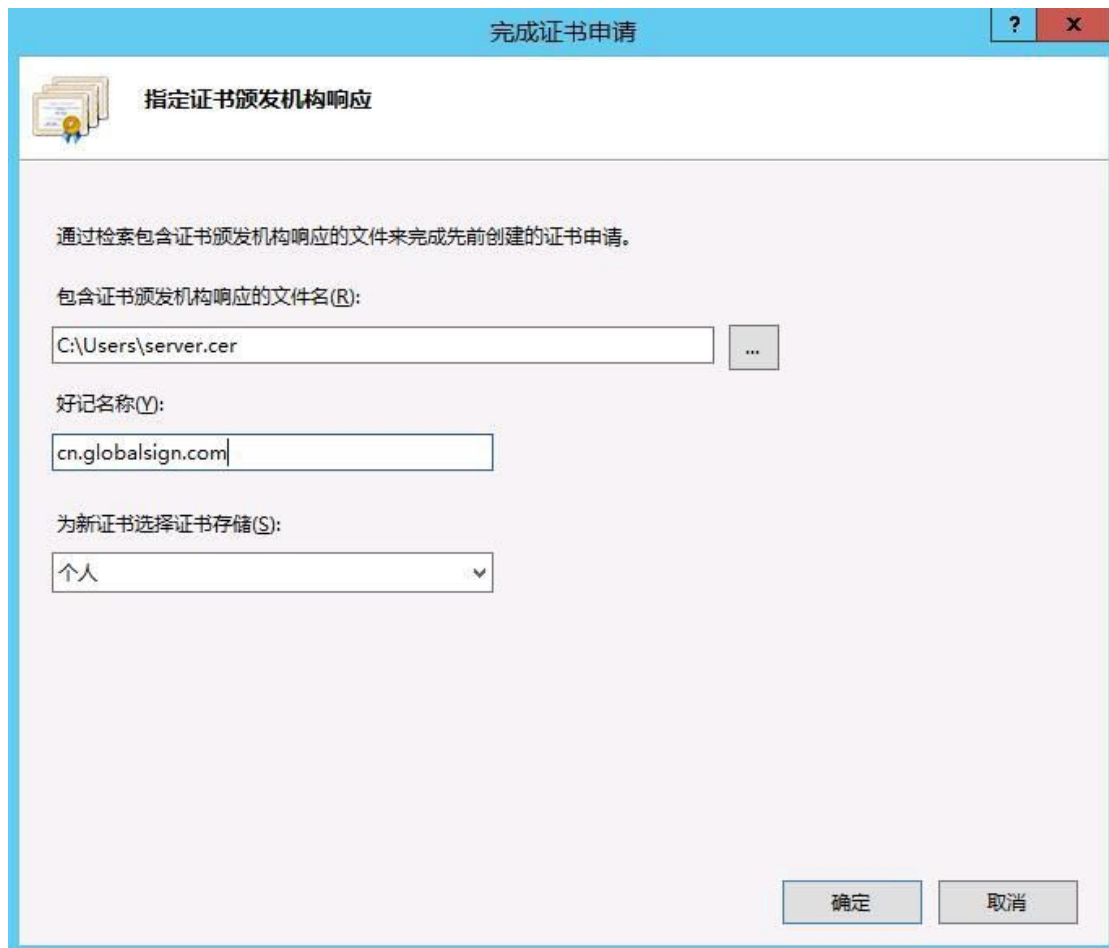
打开 IIS 服务管理器，点击**计算机名称**，双击打开右则的**服务器证书**图标



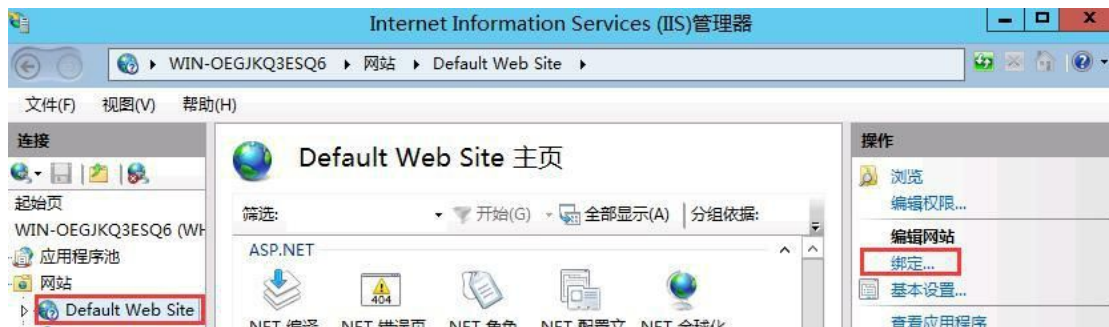
双击打开服务器证书后，点击右则的**完成证书申请**



选择 GlobalSign 颁发的服务器证书文件，并指定一个好记的名称（可选），点击确定



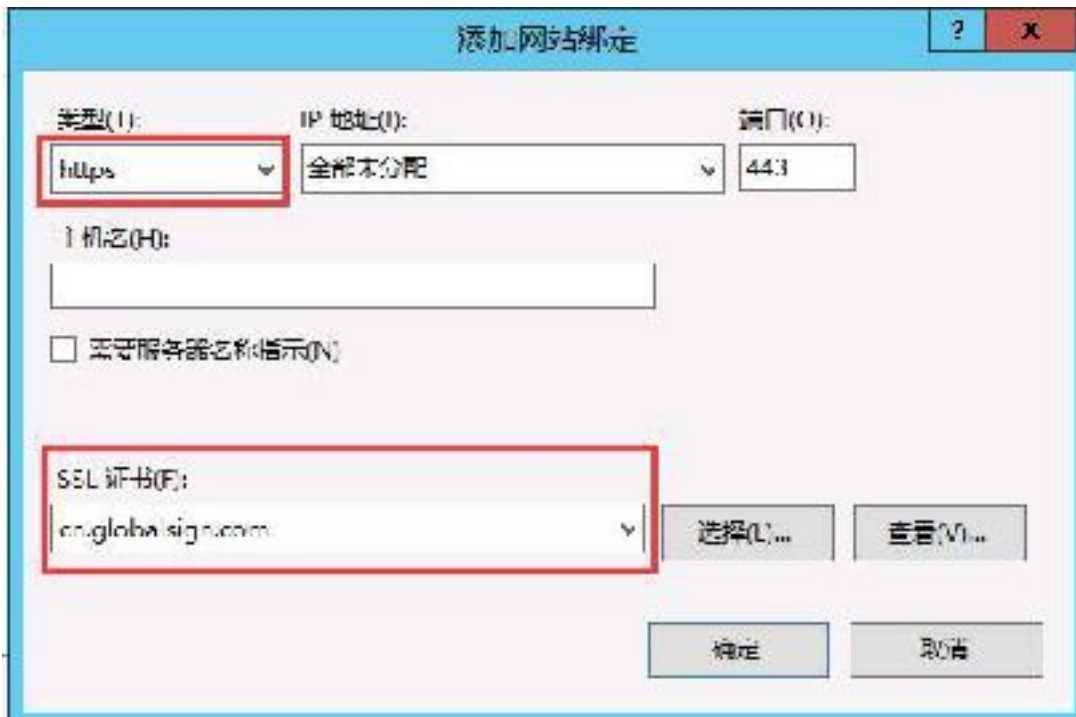
点击网站下的站点名称，点击右侧的绑定



打开网站绑定界面后，点击添加



添加网站绑定内容：选择类型为 https，端口 443 和指定对应的 SSL 证书，点击**确定**



添加完成后，网站绑定界面将会看到刚刚添加的内容



按照以上的步骤配置完成后就可以使用 <https://www.domain.com> 来访问了。

如有任何问题或疑问请直接与我们联系，谢谢！