《NCIE 培培你》

----------商宏图投稿 2005.1.6

◆*每周一讲*

在 Windows 下利用证书服务实现与 WEB 服务的安全通讯

（NCSE 二级内容）

□主讲：NCIE 考试管理中心课程策划、教学督导　商宏图（shanght@ncie.gov.cn）

在当今这样一个信息时代，互联网已经深入每一个人的生活。可以说每天的学习、工作、生活和娱乐都离不开 Internet。互联网给人们带来了很多的好处，使得每一个人都可以随心所欲的访问外面的世界。可是反过来讲互联网也带来了很大的危险性，那就是它可以让任何一个外界的用户能够看到你的计算机。所以当访问一个 Web 站点时，人们经常关心的一个问题就是如何能够安全的访问一个 Web 站点。本文所要讨论的内容就是如何在 Windows 下利用证书服务实现对 WEB 站点的安全访问。

当使用 http 协议访问 Web 站点时，客户端和 Web 服务器之间的数据是以明文方式进行传输的。要想实现用户访问 Web 站点的安全性，可以对客户端和 Web 服务器的数据传输进行加密，利用 Windows 2000 所提供的证书服务可以实现数据加密。有关证书服务和加密的基础知识请读者参阅 NCNE 培培你第 90 期的每周一讲《在 Windows 2000 下利用证书服务实现邮件加密和签名—商宏图》一文，在此不再缀述。下面是如何利用证书服务实现 Web 站点的安全访问的过程。

- **安装证书服务**

1．首先在网络中的一台 Windows 2000 Server 计算机上安装证书服务。在“控制面板”中选择“添加/删除程序”→“添加/删除 Windows 组件”，在“Windows 组件向导”对话框中选择“证书服务”，如图 1-1 所示。

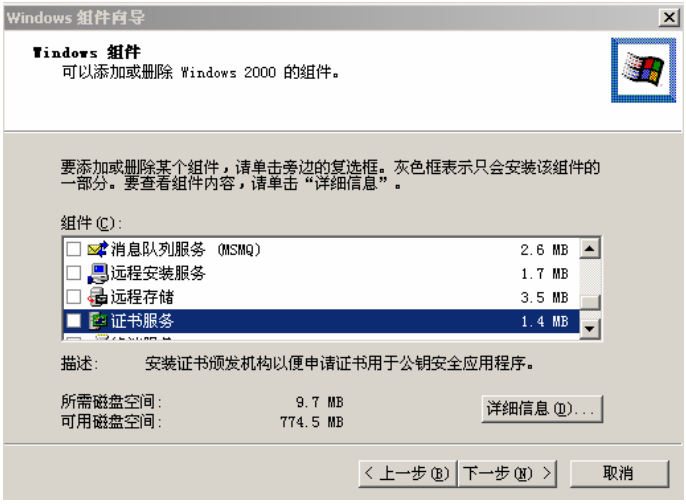

图 1-1　Windows 组件向导对话框

2．选中“证书服务”后单击“下一步”按钮，出现如图 1-2 所示对话框，提示安装证书服务后计算机不能重命名，不能加入域或从域中删除。

图 1-2　Windows 提示对话框

3．单击“是”按钮，出现如图 1-3 所示对话框，在此选择 CA 的类型。在 Windows 2000 中 CA 可以分为两大类，一种是企业级 CA，另一种是独立的 CA。其中企业级 CA 要依赖活动目录，可以提供更高的功能。独立的 CA 不依赖活动目录。

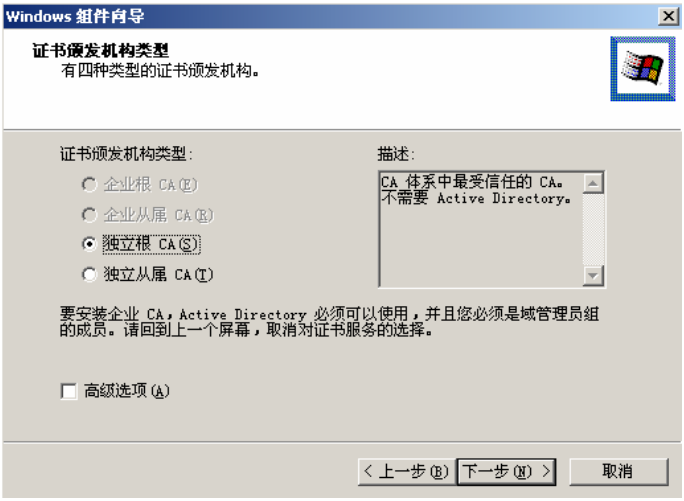

图 1-3　选择证书颁发类型

4．此处选择安装“独立根 CA”，单击“下一步”按钮出现如图 1-4 所示“CA 标识信息”对话框，在此输入标识该 CA 的信息，如图 1-4 所示。

图 1-4　输入 CA 标识信息

5．单击“下一步”按钮，出现如图 1-5 所示“数据存储位置”对话框，在此选择证书数据库和证书数据库日志文件的物理位置。

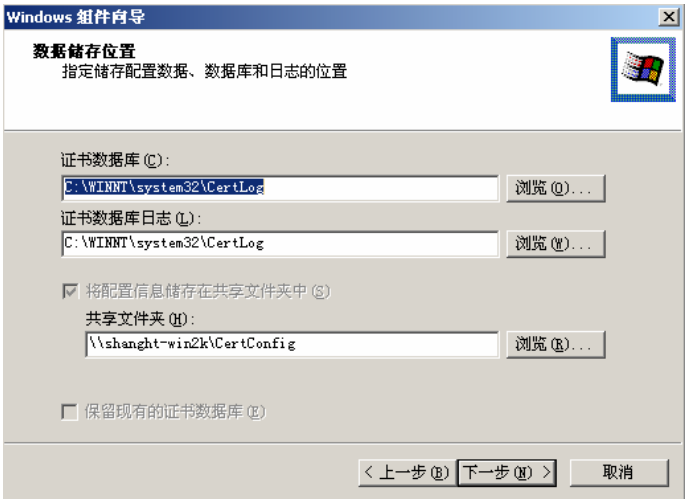

图 1-5　指定证书数据库和日志位置

6．单击“下一步”按钮，出现如图 1-6 所示对话框，提示如果要安装证书服务，必须停止 Internet 信息服务。

图 1-6　Windows 提示对话框

7．单击“确定”按钮，开始执行安装。安装过程中需要提供 Windows 2000 Server 安装源文件，如图 1-15 所示。

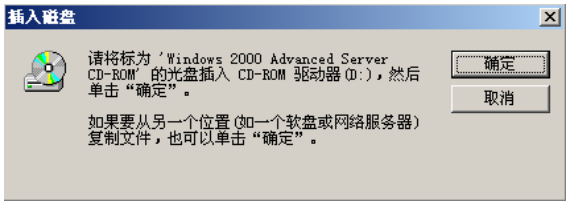

图 1-7 提示提供 Windows 2000 Server 安装源文件

8．单击“确定”按钮完成证书服务安装。

- **创建 WEB 站点**

1．在 Web 服务器上打开 Internet 信息服务控制台，创建 Web 站点“NCNE 培培你”（创建 Web 站点过程略）。

2．右键单击此 Web 站点，选择“属性”，在站点属性页中选择“Web 站点”标签，如图 1-8 所示。

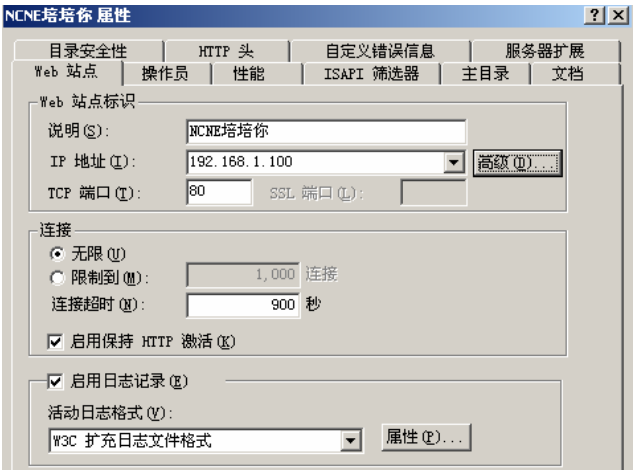

图 1-8　Web 站点属性页 Web 站点标签

3．在“Web 站点标识”栏中单击“高级”按钮，出现如图 1-9 所示对话框。

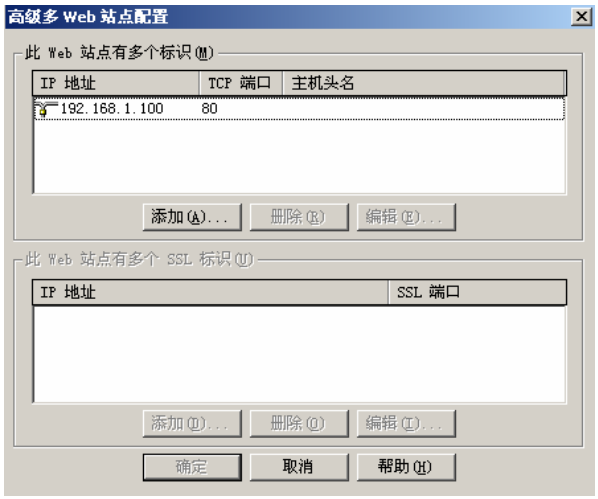

图 1-9　高级多 Web 站点配置选项卡

4．单击“添加”按钮，出现“高级 Web 站点标识”对话框，在此指定此站点的 IP 地址、TCP 端口和主机头，如图 1-10 所示.。

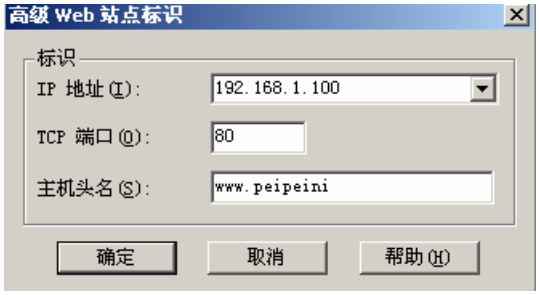

图 1-10　高级 Web 站点标识选项卡

5．连续单击“确定”按钮完成设置，停止并重新启动此 Web 站点。

6．主机头的解析需要 DNS 服务器来完成，因此要在 DNS 服务器上创建一个区域“peipeini.com”，并为此站点创建主机记录“www 192.168.1.100”，如图 1-11 所示。

图 1-11　DNS 控制台下为 Web 站点设置主机记录

7. 在客户端计算机上利用 IE 浏览器访问此 Web 站点（注意设置 DNS 选项），如图 1-12 所示。访问成功说明 Web 服务器配置正确，此时客户端和 Web 服务器的通讯是明文的

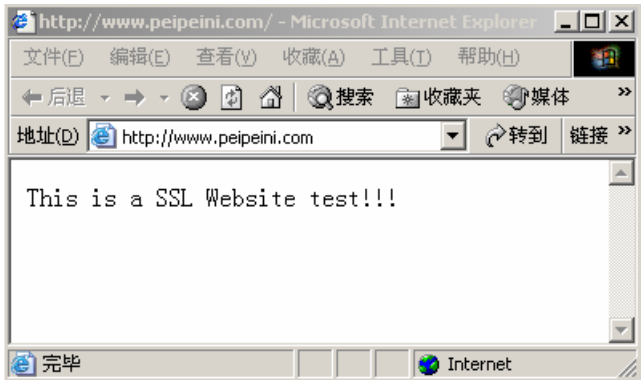

图 1-12　利用 IE 浏览器访问 Web 站点

- **为 Web 站点安装证书**

为 Web 服务器安装证书包括几个阶段，首先要在 Web 服务器上提交证书申请，然后在证书服务器上颁发证书，最后在 Web 服务器上安装证书。

- **在 Web 服务器上提交证书申请**

1. 在 Web 服务器上打开 Web 站点属性页，选择“目录安全性”标签，如图 1-13 所示。

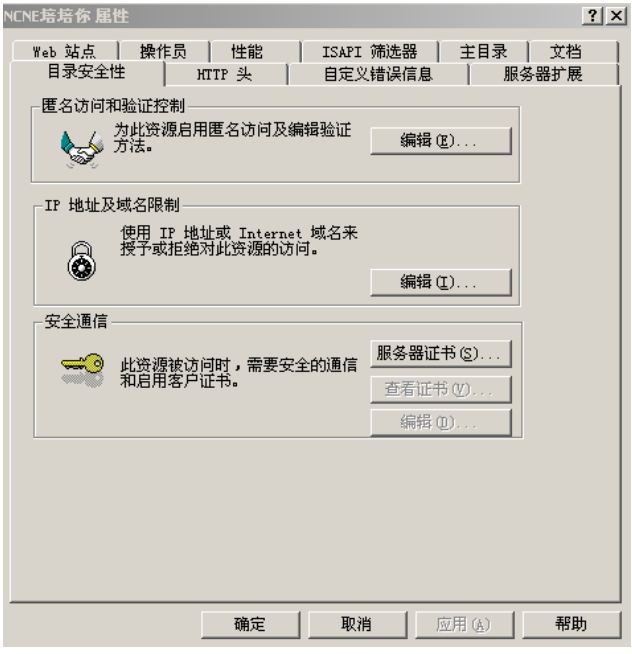

图 1-13　Web 站点属性页“目录安全性”标签

2. 在“安全通信”栏中单击“服务器证书”，出现如图 1-14 所示 Web 服务器证书向导。

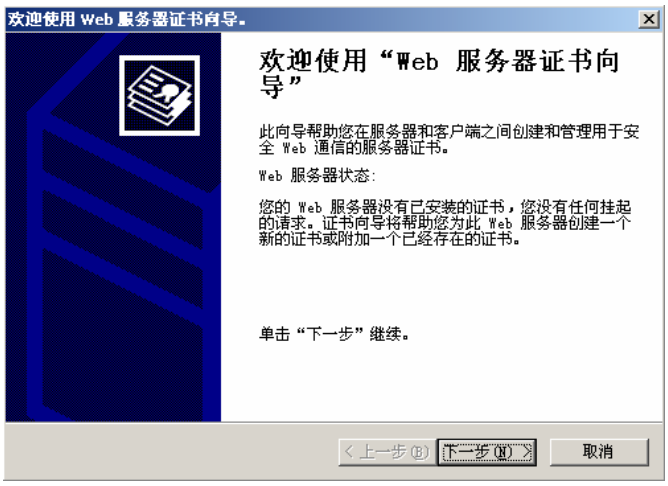

图 1-14　Web 服务器证书向导

3．单击“下一步”按钮，出现如图 1-15 所示“服务器证书”对话框。

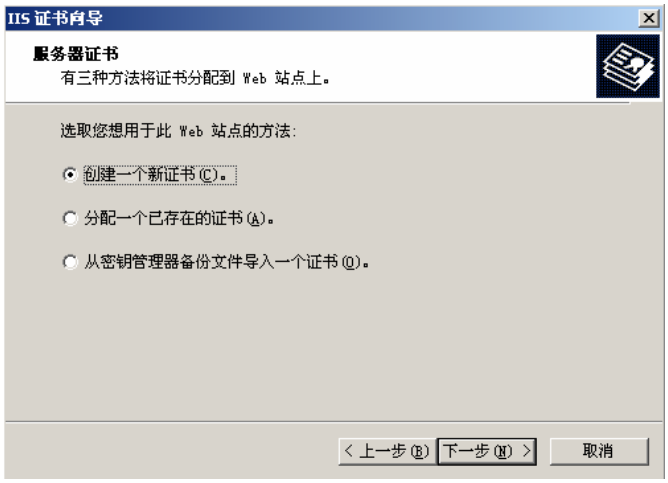

图 1-15　IIS 证书向导--服务器证书

4．选择“创建一个新证书”选项，单击“下一步”按钮，出现如图 1-16 所示对话框。

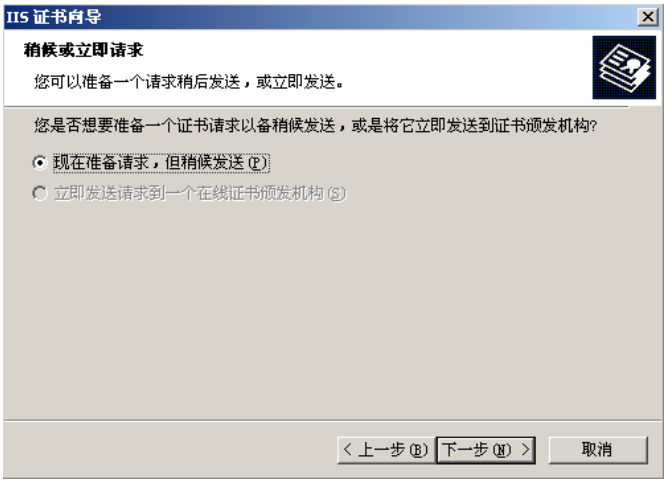

图 1-16　IIS 证书向导--稍后或立即请求

5．选择“现在准备请求，但稍候发送”，单击“下一步”按钮，出现如图 1-17 所示对话框，在此指定证书的名称和位长。

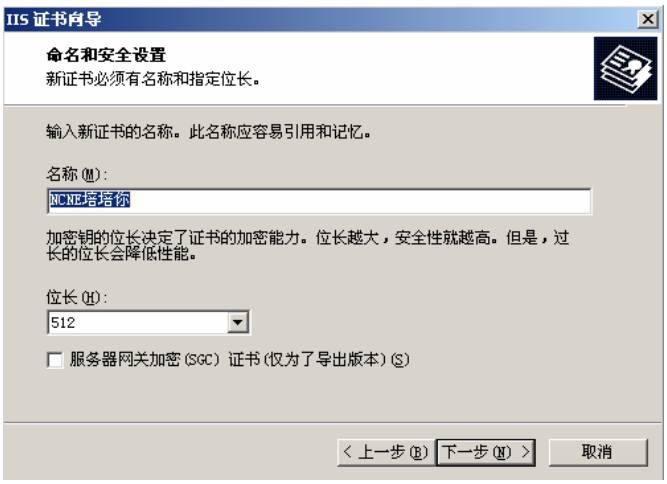

图 1-17　IIS 证书向导—命名和安全向导

6．单击“下一步”按钮，出现如图 1-18 所示对话框，在此为该证书指定组织和组织部门信息。

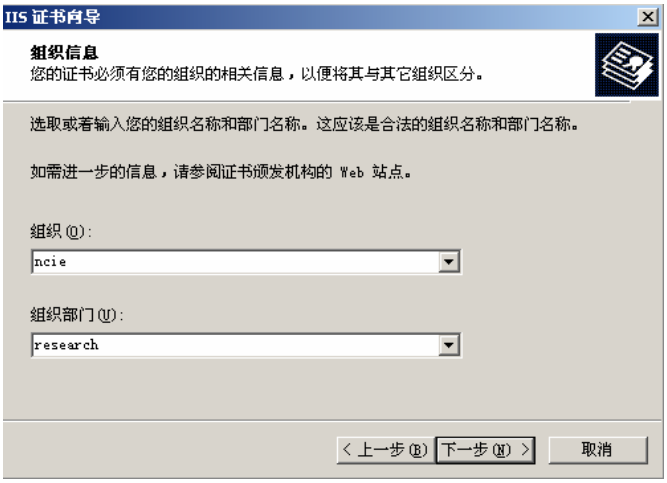

图 1-18　IIS 证书向导--组织信息

7．单击“下一步”按钮，出现如图 1-19 所示对话框，在此指定站点的公用名称信息。

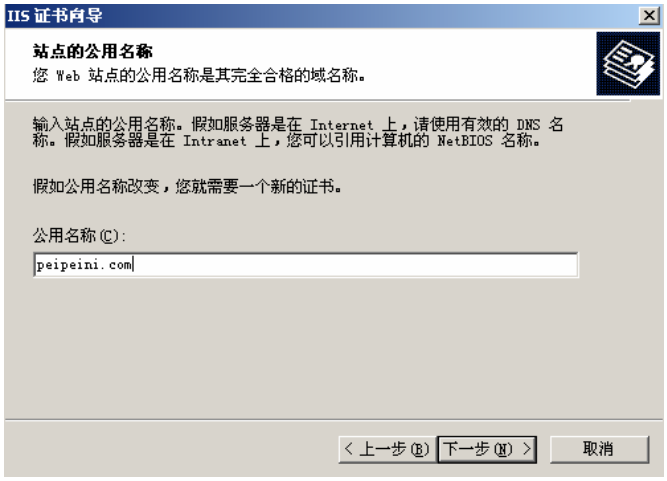

图 1-19　IIS 证书向导—站点的公用信息

8．单击“下一步”按钮，出现如图 1-20 所示对话框，在此指定相关的地理信息。

图 1-20　IIS 证书向导—地理信息

9．单击“下一步”按钮，出现如图 1-21 所示对话框，在此指定该证书请求的文件名。

图 1-21　IIS 证书向导—证书请求文件名

10．单击“下一步”按钮，出现如图 1-22 所示对话框，在此可以查看请求文件的摘要信息。

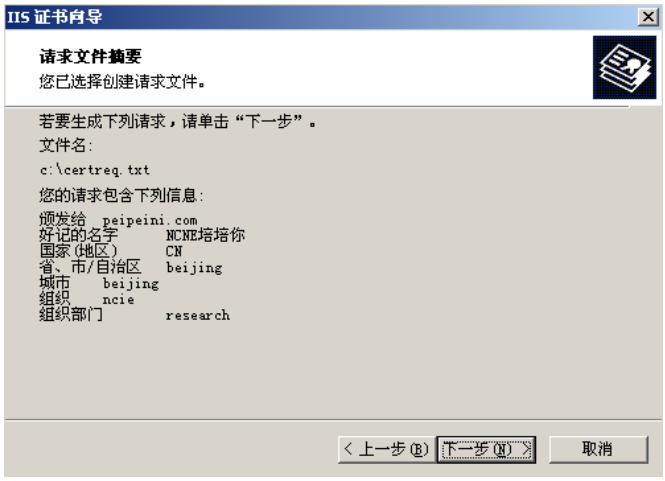

图 1-22　IIS 证书向导—请求文件摘要

11．单击“下一步”按钮，出现如图 1-23 所示对话框。

图 1-23　IIS 证书向导—完成 Web 服务器证书向导

12．单击“完成”按钮，完成证书申请。在资源管理器中可以看到生成了一个文件 certreq.txt，利用记事本打开该文件可以查看该文件的内容，如图 1-24 所示。

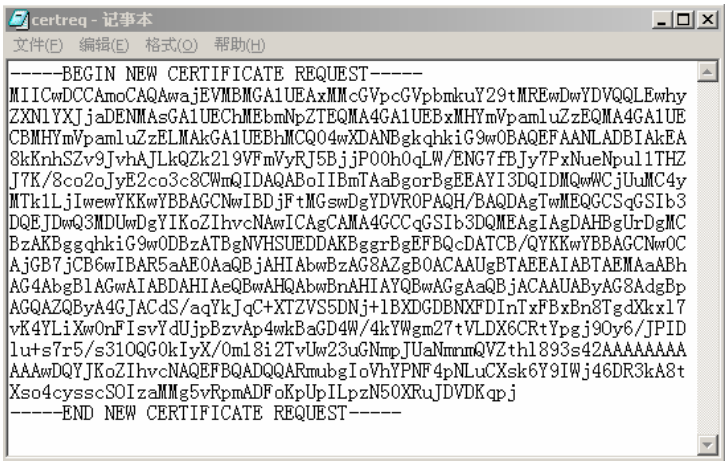

图 1-24 利用记事本查看证书请求文件

13．接下来把此证书文件提交给证书服务器 CA。在 Web 服务器上在 IE 浏览器中输入“http://192.168.1.200/certsrv”访问证书服务器，其中 192.168.1.200 是证书服务器的 IP 地址。如图 1-25 所示。

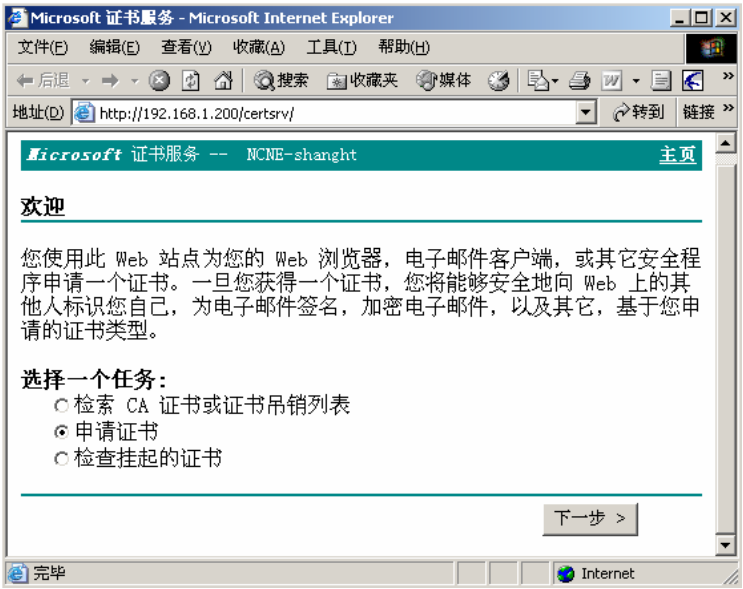

图 1-25 利用 IE 浏览器从 CA 申请证书

14．选择“申请证书”选项，单击“下一步”按钮，出现如图 1-26 所示对话框。

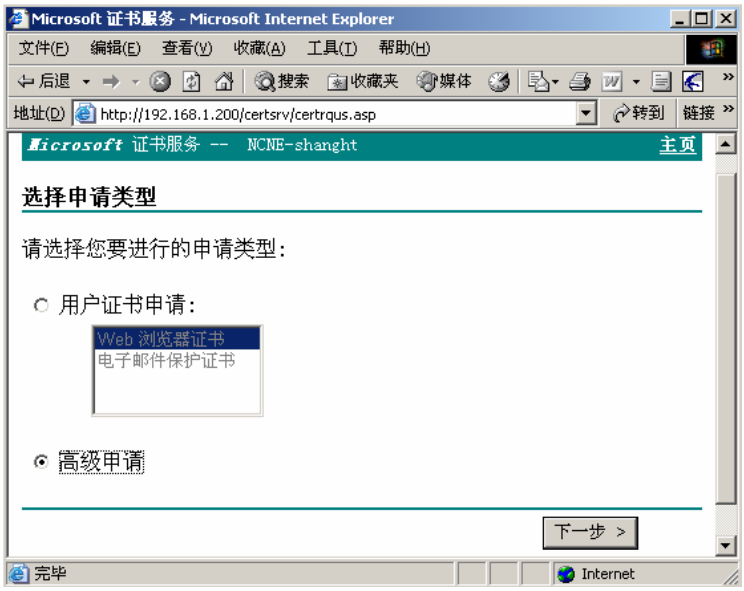

图 1-26 选择申请类型

15．选择“高级申请”选项，单击“下一步”按钮，出现如图 1-27 所示对话框。

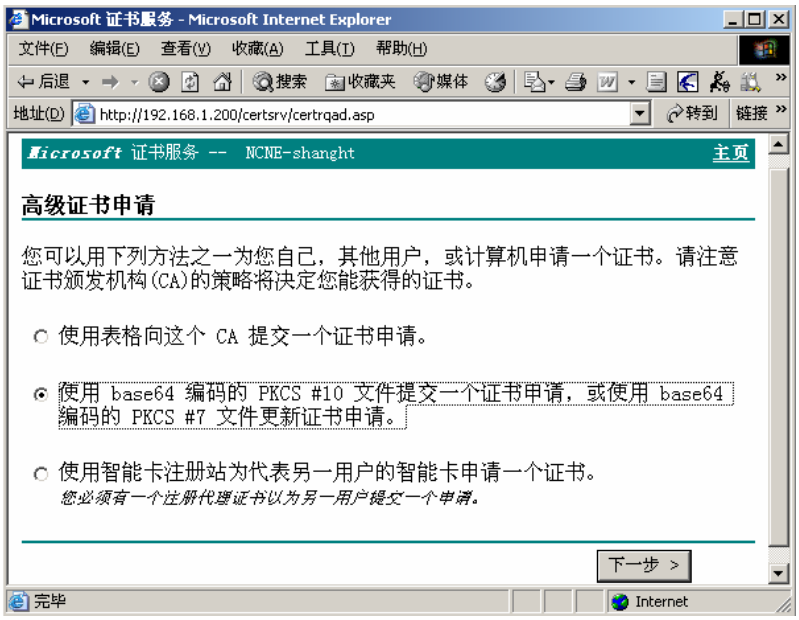

图 1-27 高级证书申请

16．选择利用 PKCS#10 文件提交证书申请，单击“下一步”按钮，出现如图 1-28 所示对话框。

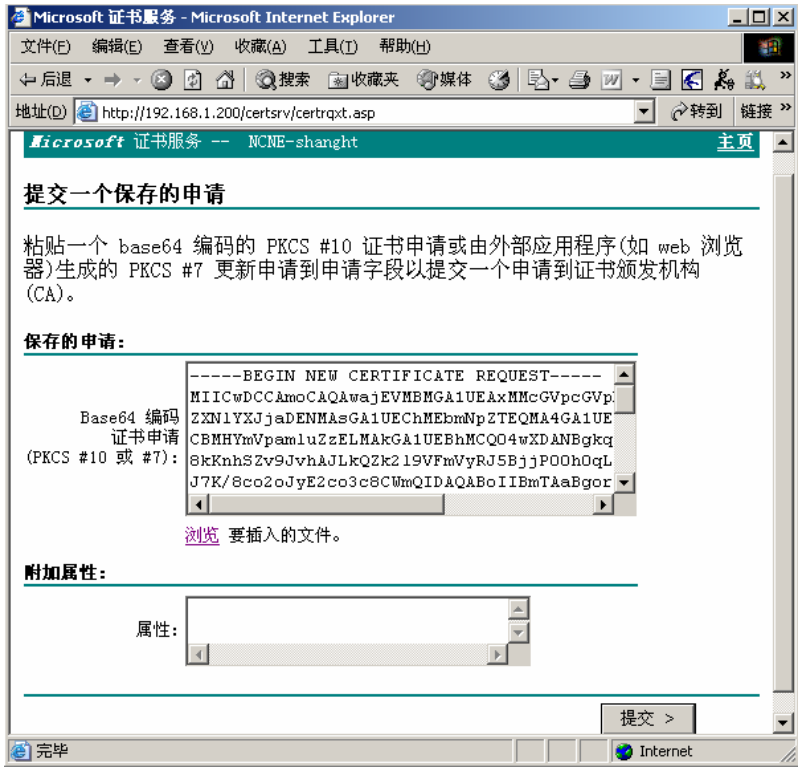

图 1-28 提交一个保存的申请

17．在保存的申请中把上面生成的文件 certreq.txt 的内容复制到这里，单击“提交”按钮，出现如图 1-29 所示画面，显示证书申请已经提交。

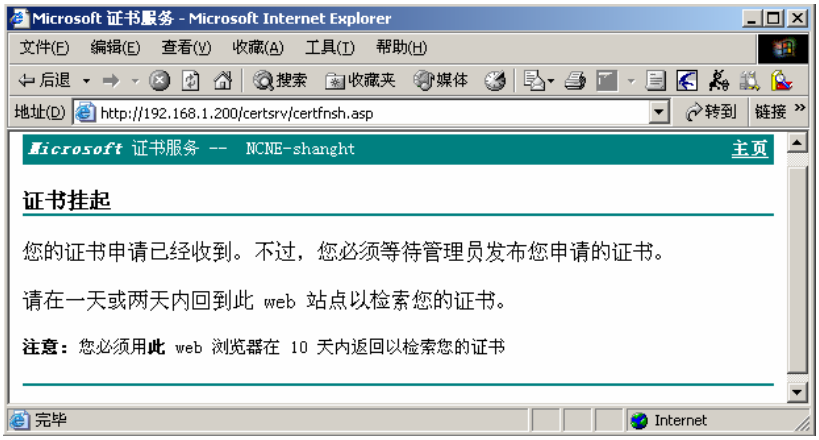

图 1-29 证书挂起

- **在证书服务器上颁发证书**

1．在证书服务器上依次打开“开始”→“程序”→“管理工具”→“证书颁发机构”，打开证书颁发机构控制台。单击“待定申请”，在右边的窗口中可以看到刚才提交的证书申请。右键单击该证书申请选择“所有任务”→“颁发”，颁发该证书，如图 1-30 所示。

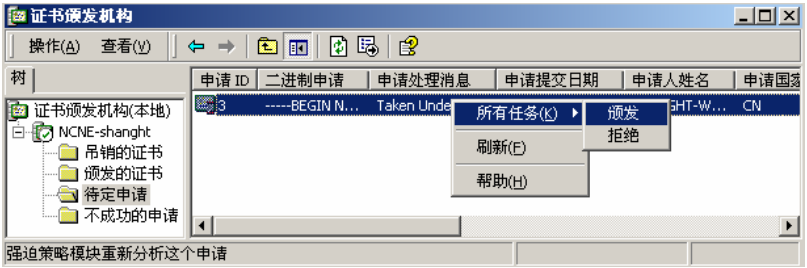

图 1-30 在 CA 中颁发证书

- **在 Web 服务器上下载证书**

1．在 Web 服务器上打开 IE 浏览器，输入“http://192.168.1.200/certsrv”，访问证书服务器，如图 1-31 所示。

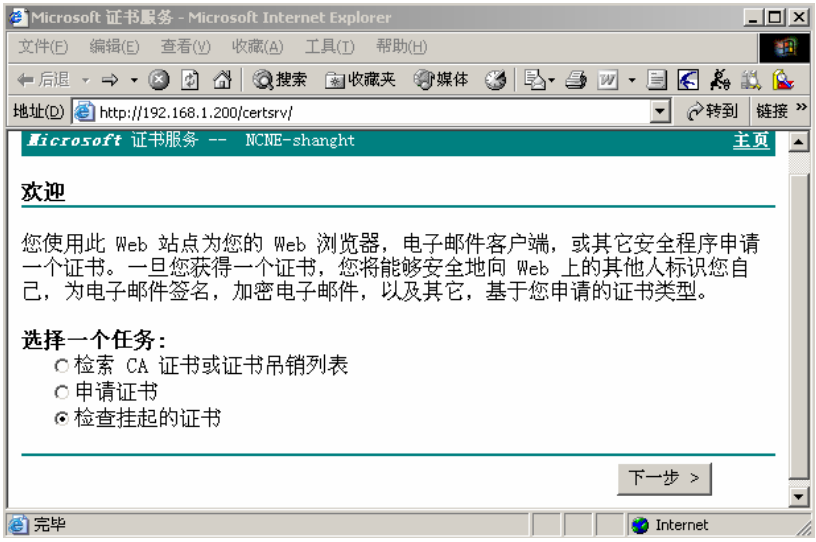

图 1-31 检查挂起的证书

2．选择“检查挂起的证书”选项，单击“下一步”按钮，出现如图 1-32 所示画面。

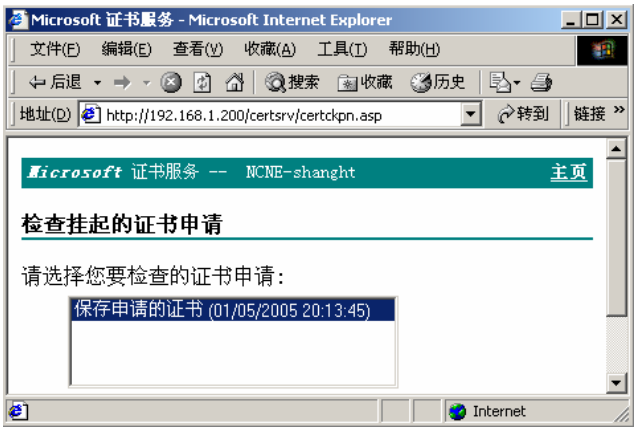

图 1-32 检查挂起的证书申请

3．单击“下一步”按钮，出现如图 1-33 所示画面，显示证书已经发布。

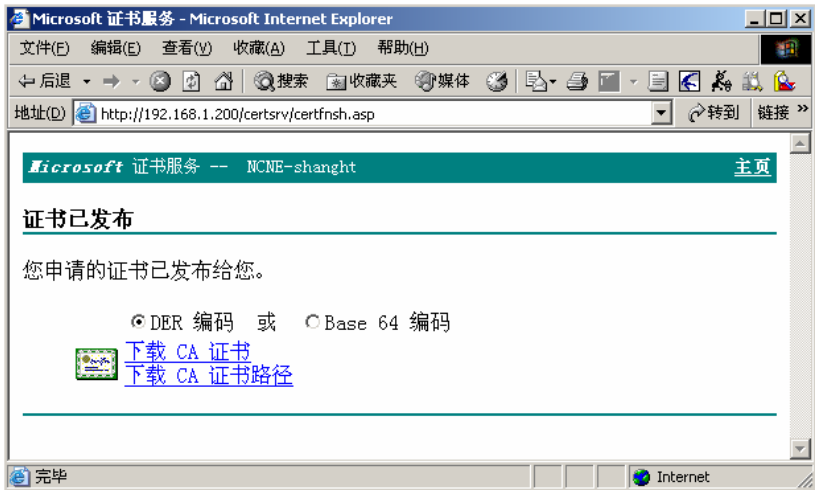

图 1-33 证书已发布

4．单击“下载 CA 证书”，出现如图 1-34 所示画面。

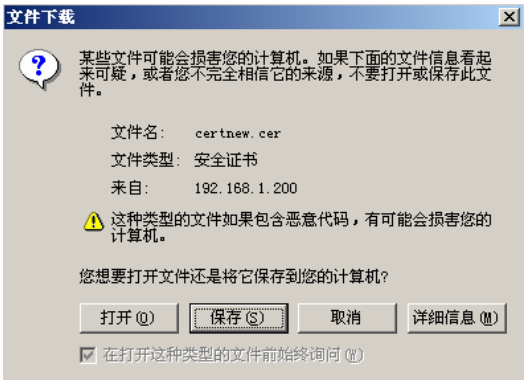

图 1-34 下载证书

5．单击“保存”按钮，下载证书并保存成文件 certnew.cer。

- **在 Web 服务器上安装证书**

1．在 Web 服务器上打开 Web 站点属性页，选择“目录安全性”标签，如图 1-35 所示。

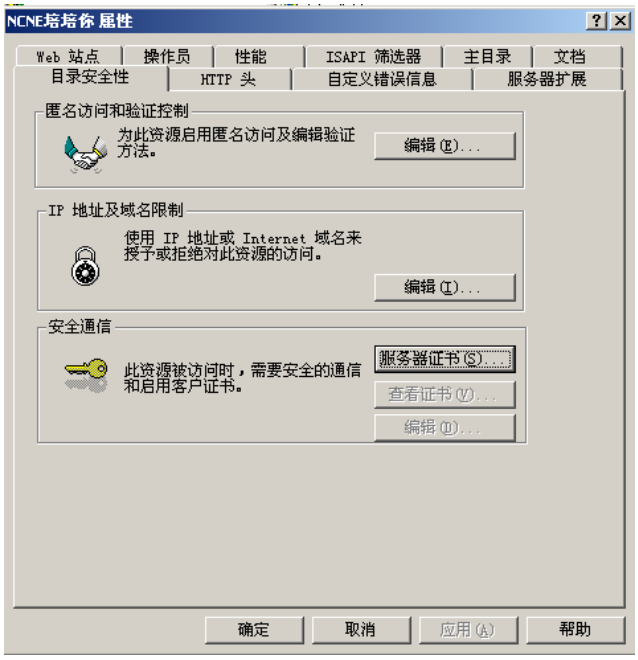

图 1-35 站点属性页“目录安全性”标签

2．在“安全通信”栏中单击“服务器证书”按钮，出现如图 1-36 所示对话框。

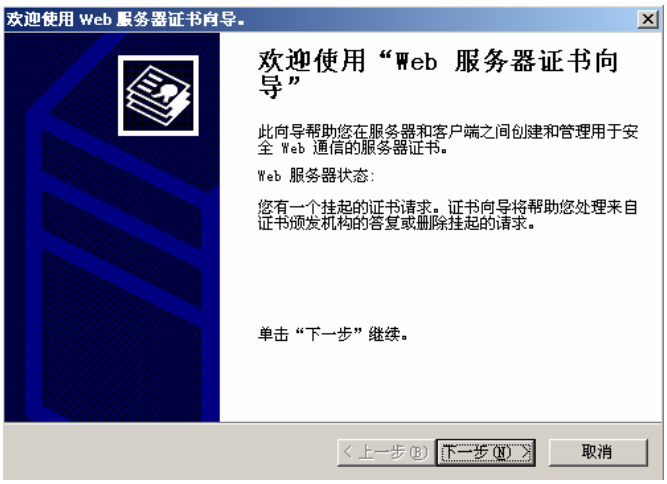

图 1-36 Web 服务器证书向导

3．单击“下一步”按钮，出现如图 1-37 所示对话框，选择“处理挂起的请求并安装证书”选项。

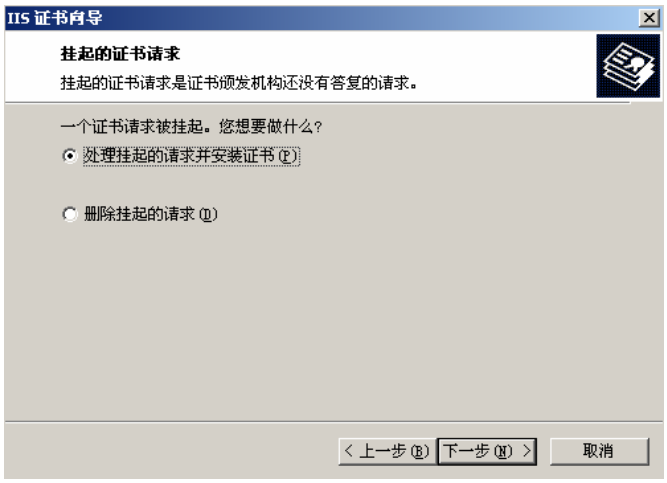

图 1-37　IIS 证书向导—挂起的证书请求

4．单击“下一步”按钮，出现如图 1-38 所示对话框，单击“浏览”按钮指定证书文件的路径和文件名。

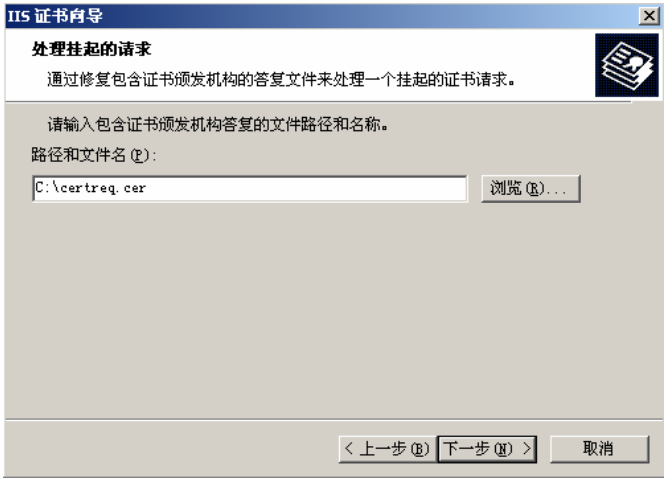

图 1-38　IIS 证书向导—处理挂起的请求

5．单击“下一步”按钮，出现如图 1-39 所示对话框。

图 1-39　IIS 证书向导—证书摘要

6．单击“下一步”按钮，出现如图 1-40 所示对话框。

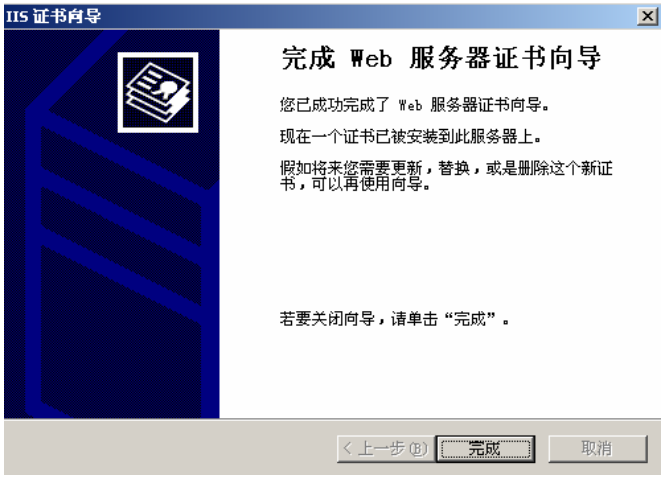

图 1-40　IIS 证书向导—完成 Web 服务器证书向导

7．单击“完成”按钮安装证书。

- **设置 Web 服务器相关选项**

1．安装证书后在 Web 服务器上打开 Web 站点属性页，选择“目录安全性”标签，可以看到“安全通信”栏中“查看证书”和“编辑”按钮由灰色变为亮度显示。单击“编辑”按钮，弹出“安全通信”对话框，选中“申请安全通道（SSL）”选项，在“客户证书”栏中选择“接收客户证书”选项，如图 1-41 所示。

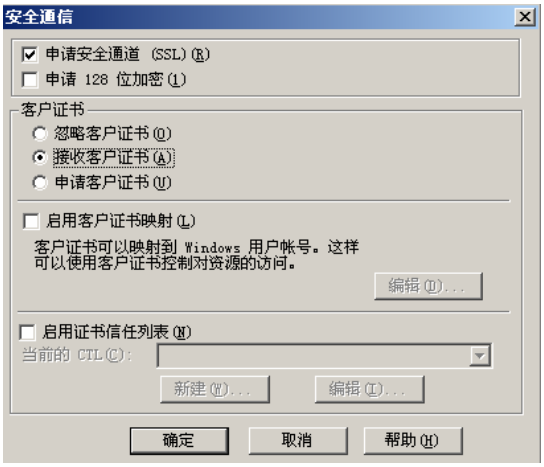

图 1-41 设置安全通道

2．单击“确定”按钮完成设置。返回站点属性页选择“Web 站点”标签，可以看到“SSL 端口”由灰色变为亮色，设置 SSL 端口为 443，如图 1-42 所示。.

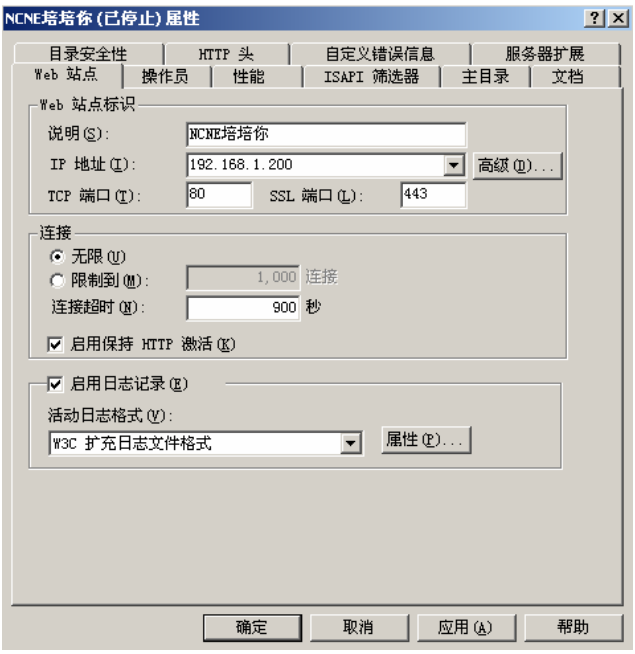

图 1-42 查看 Web 服务器的 SSL 端口

3．单击“确定”按钮完成设置，停止并重新启动此 Web 站点。

- **在客户端访问 Web 站点**

1. 此时在客户端计算机利用 IE 浏览器访问此 Web 站点，当输入 http://www.peipeini.com 时提示“该网页必须通过安全频道查看”，说明此时与 Web 站点的访问需要进行加密。如图 1-43 所示。

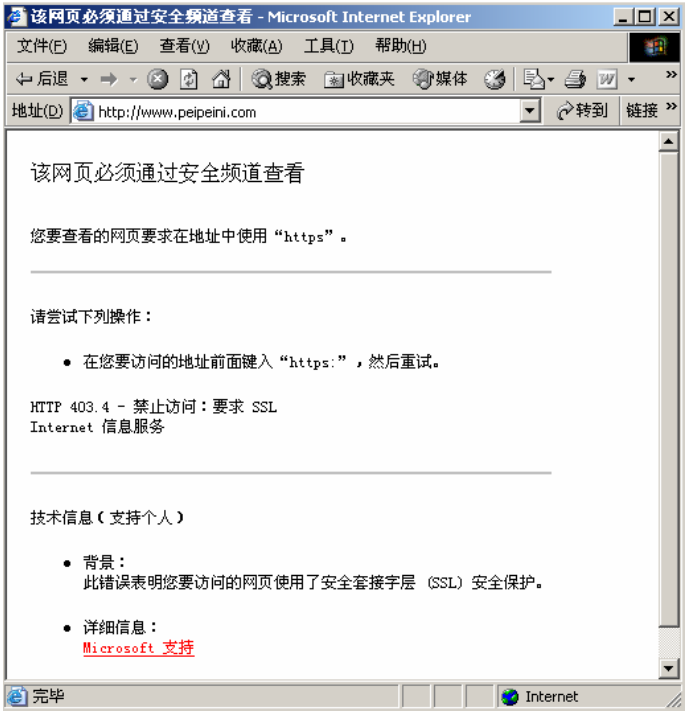

图 1-43 利用 http 协议浏览安全站点

2．在客户端的 IE 中输入 https://www.peipeini.com 访问此 Web 站点，出现如图 1-44 所示提示信息。

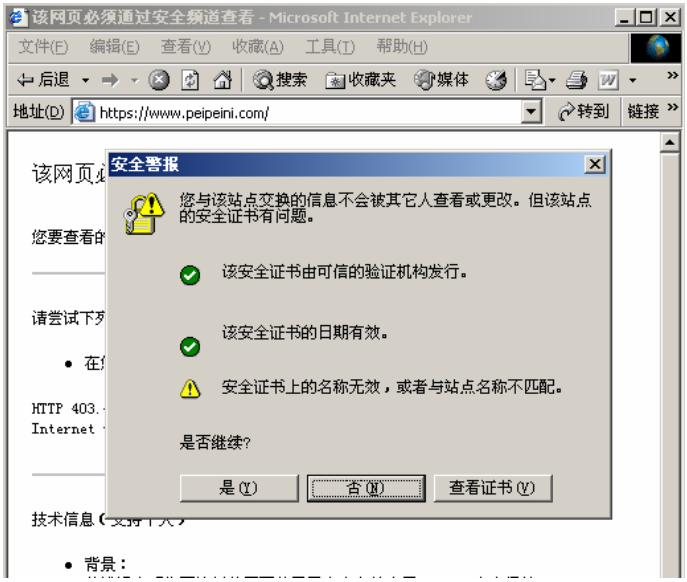

图 1-44　利用 https 协议浏览安全站点

3．单击“是”按钮，可以访问 Web 站点的内容，如图 1-45 所示。

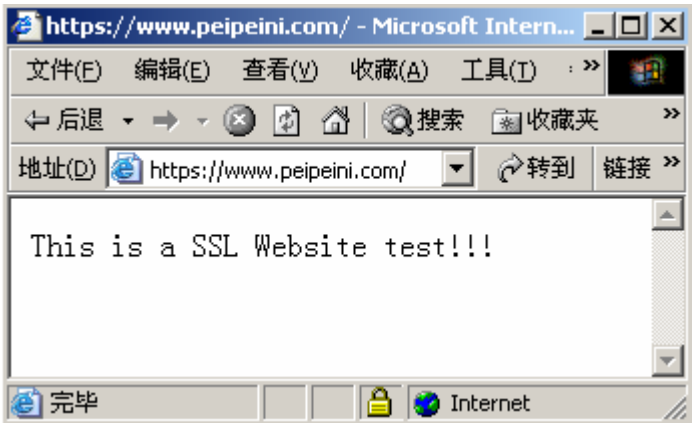

图 1-45　利用 https 协议浏览安全站点

以上是利用证书来实现 Web 站点安全访问的过程。为了验证加密的结果，有兴趣的读者可以利用 sniffer 等工具对网络通过进行监视，可以发现在没有使用证书前与 Web 服务器的通讯是明文的，而使用证书之后这个通讯是经过加密的。