目 录

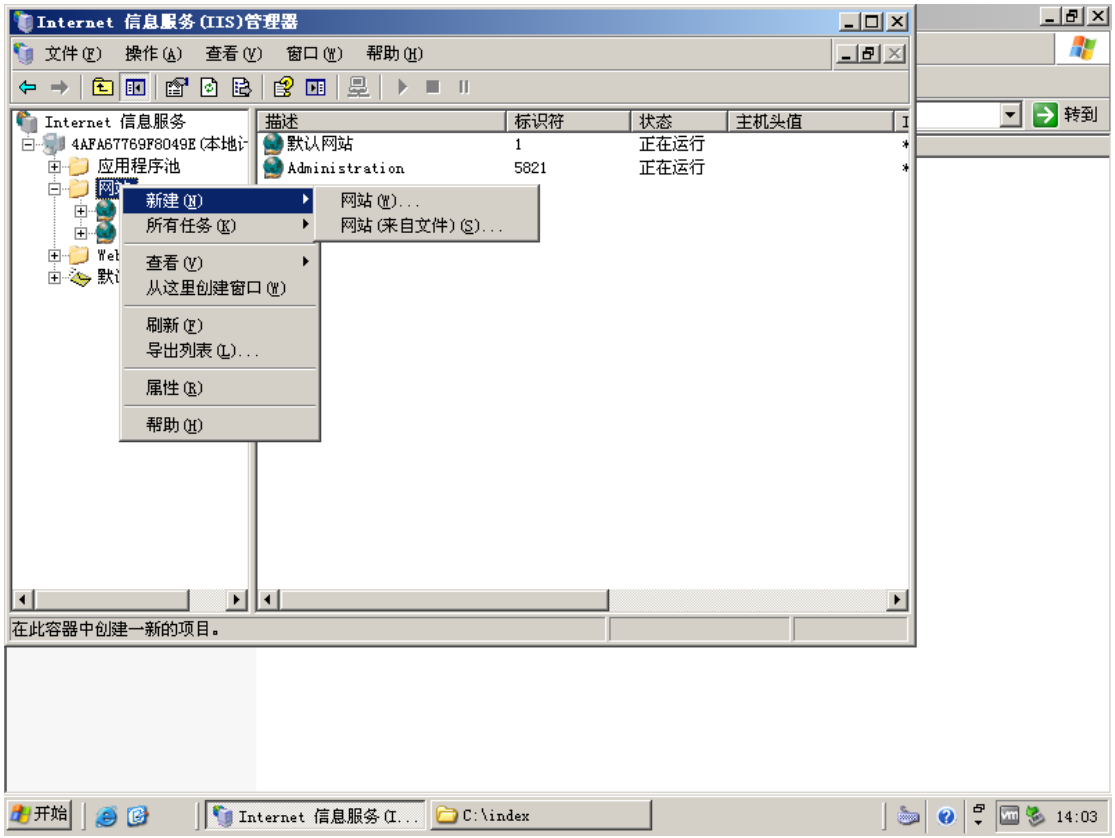
1 实验前提

这里使用两个虚拟机，一个是用户端，一个是服务器端。
用户端的 IP 为 192.168.1.2/24，服务器的 IP 为 192.168.1.1/24
用户端的系统为 xp，服务器端的系统为 WindowsServer 2003

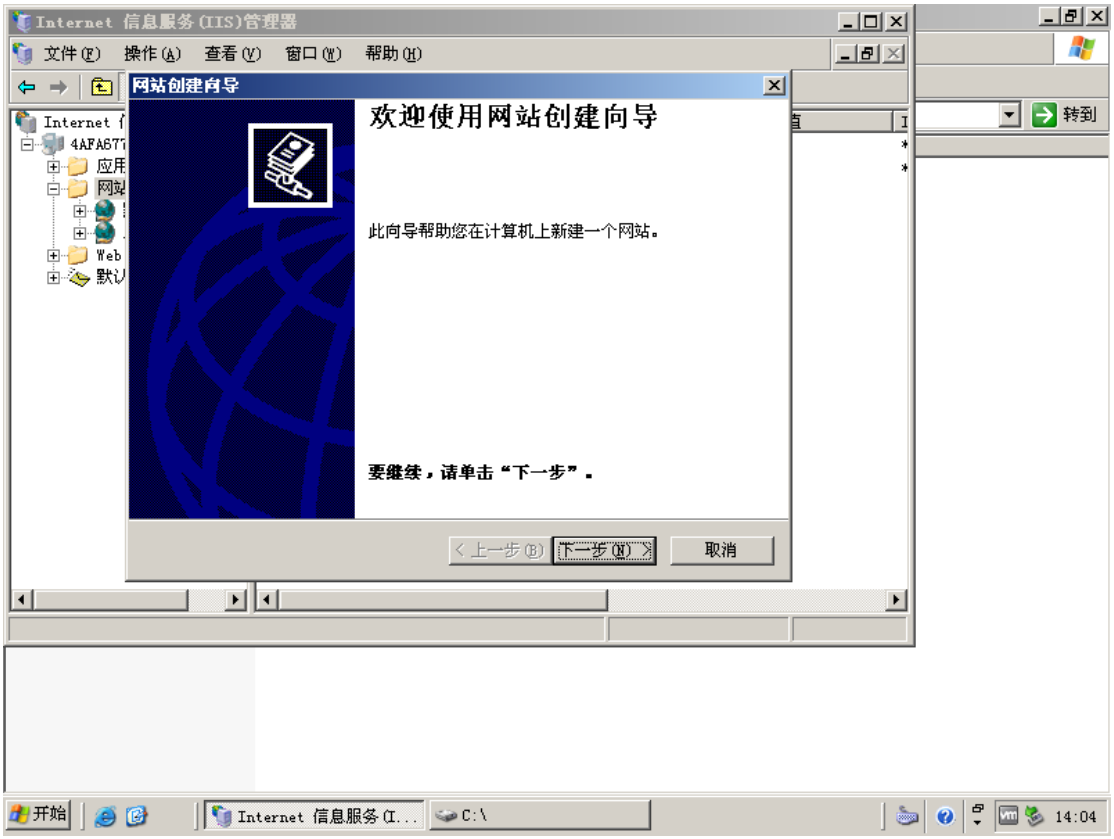
2 SSL 的配置

2.1 SSL 服务器设置

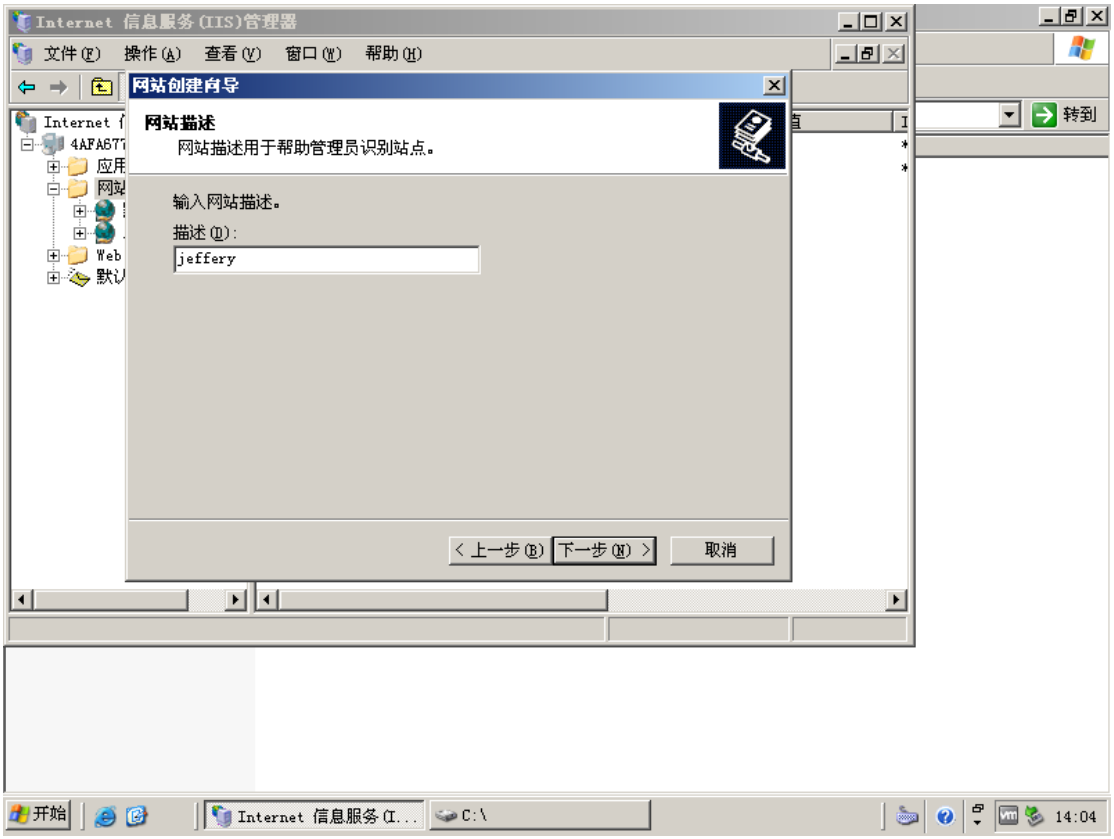
我们首先配置一下服务器(需打开 iis 管理器)：
新建一个网站：



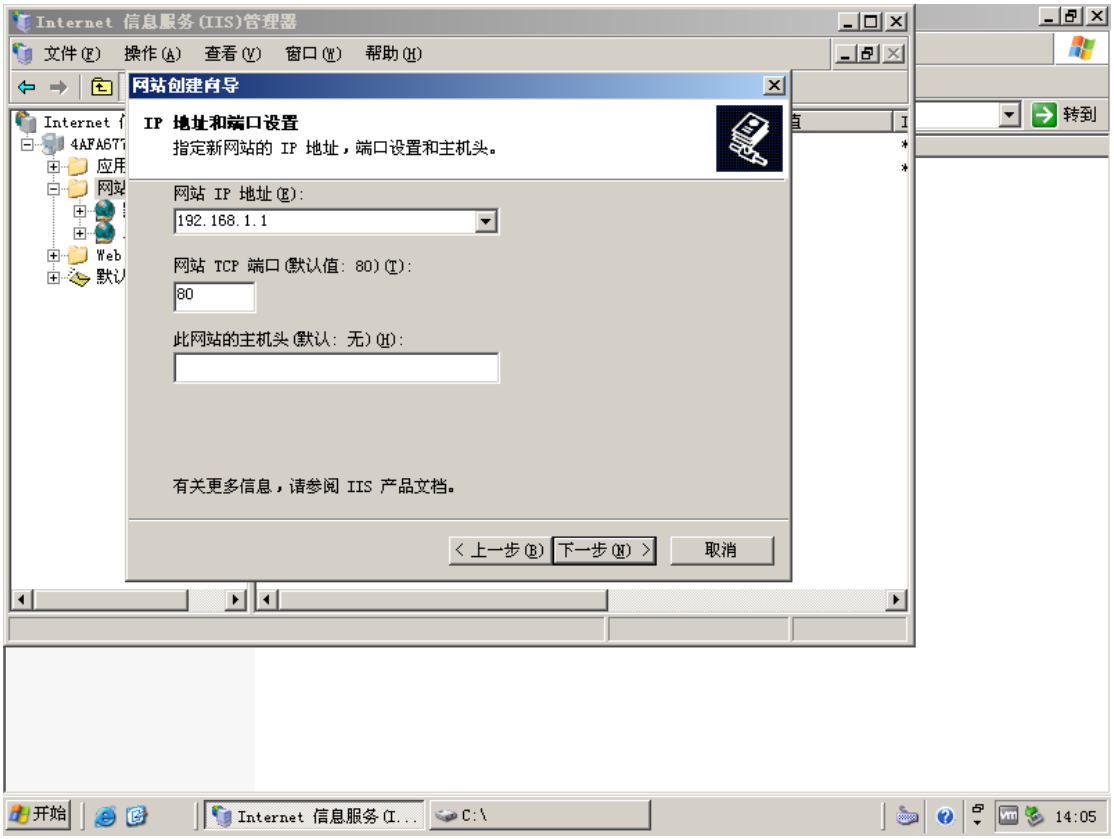
下一步



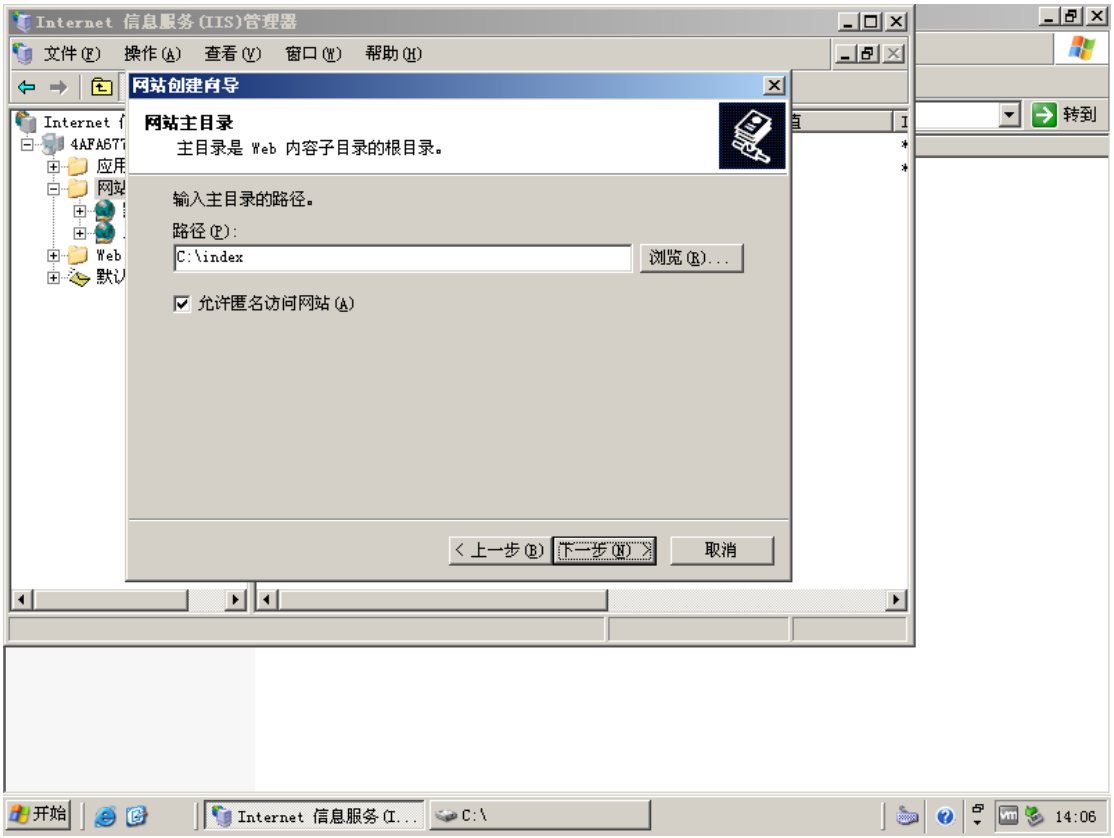
随便输入一个名称，点下一步



这些按实际情况配置，这里因服务器的 ip 地址为 192.168.1.1，默认端口为 80，点下一步

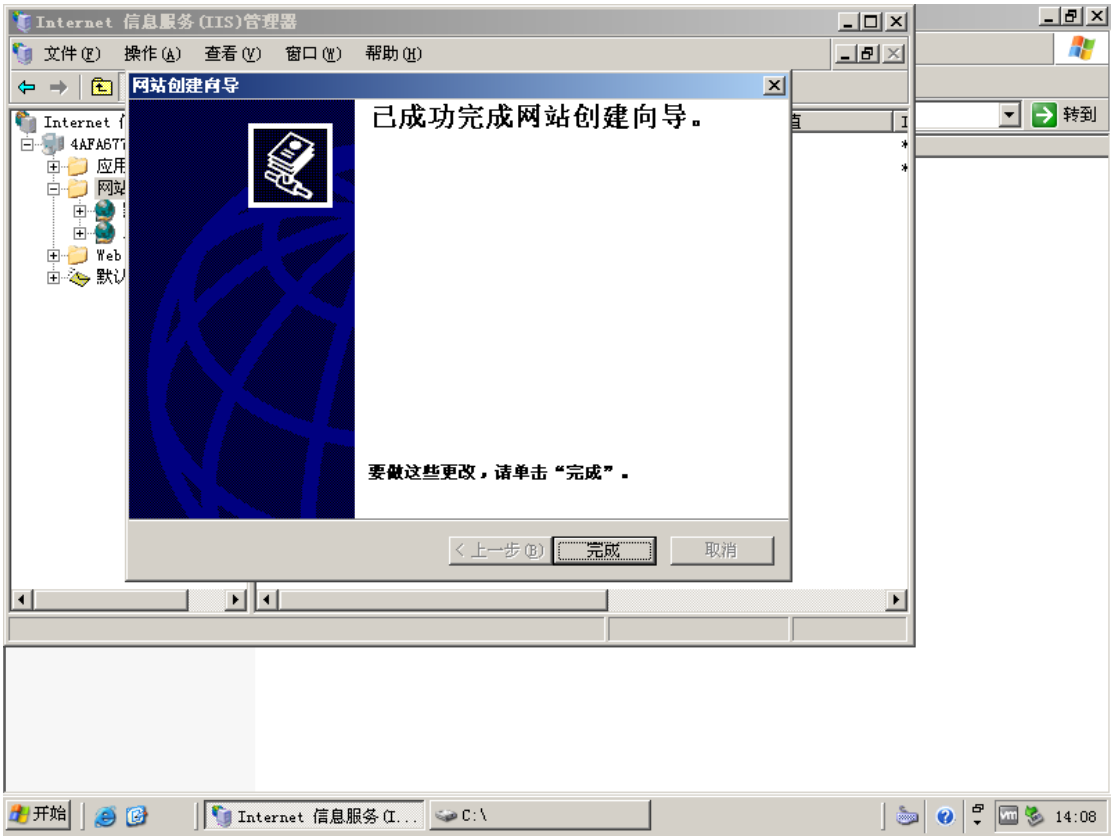


输入要做为网站的路径，点下一步

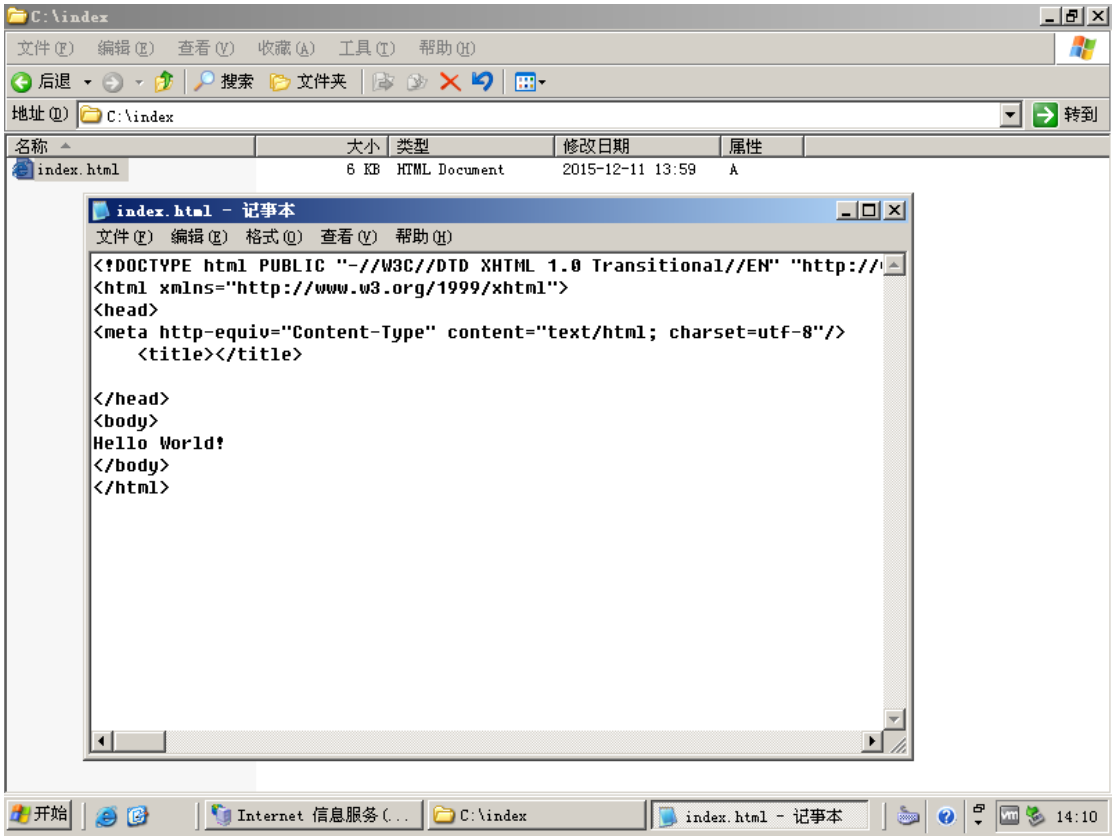


设置权限，这里用 html，选择读取就可以了，点下一步

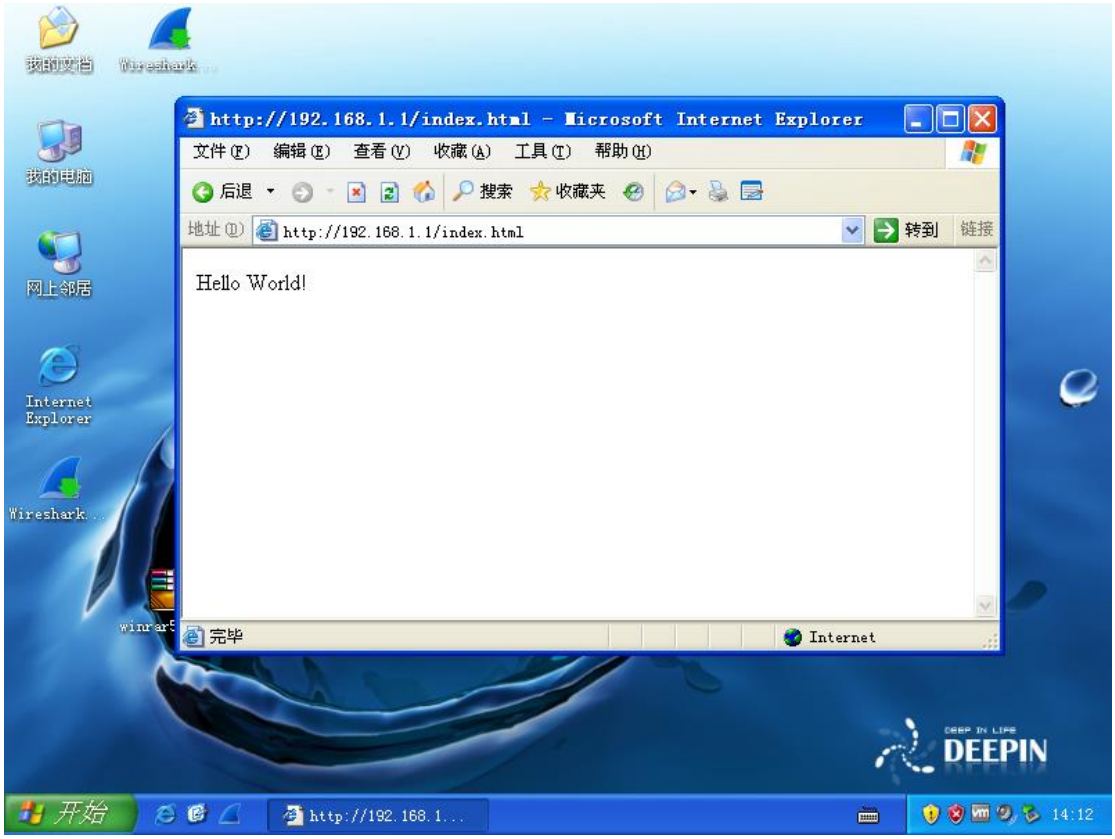
点击完成



在服务器的目录下放置一个 html 文件

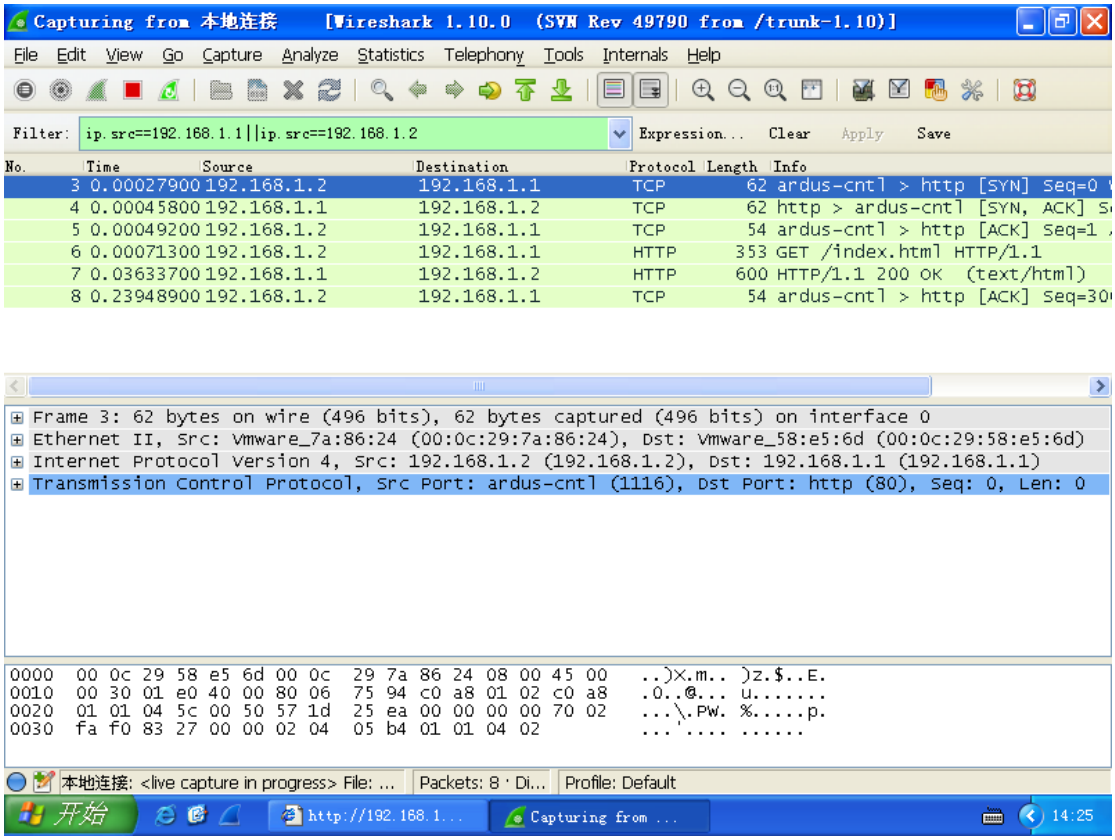


在用户端用浏览器可以浏览到服务器上的 html 文件

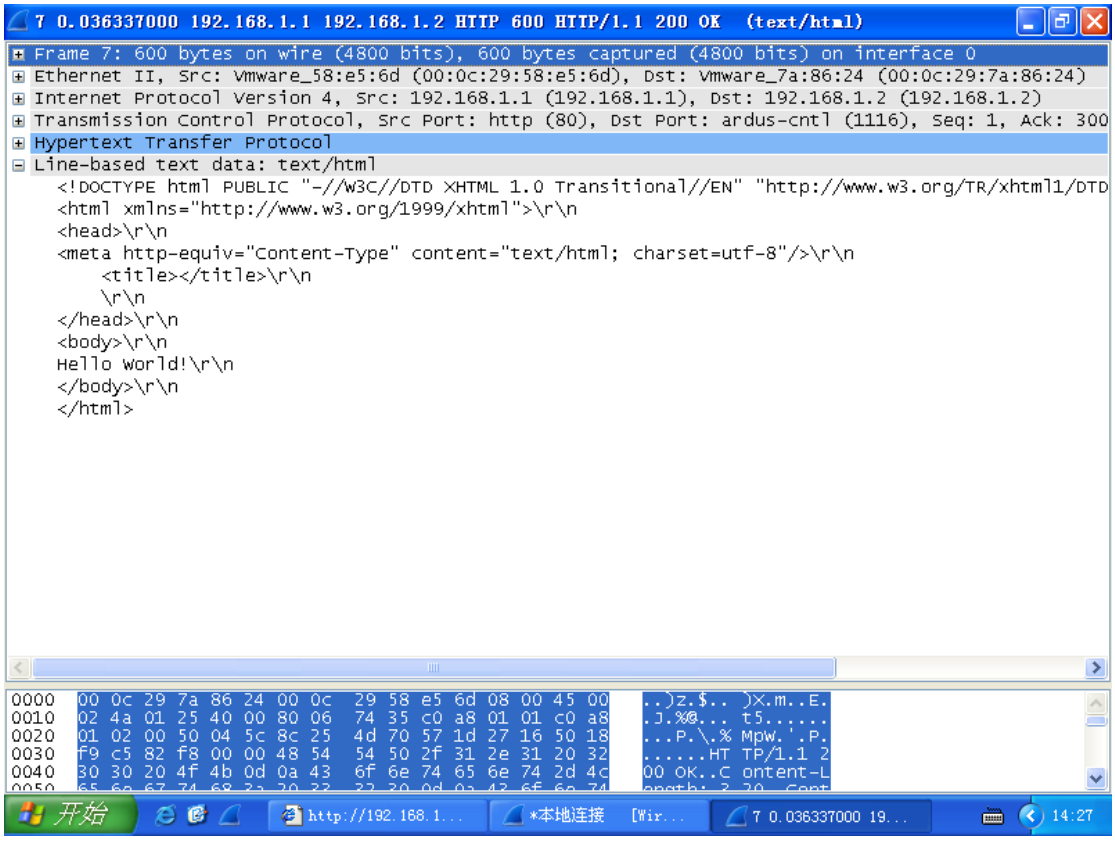


2.2 未启用 SSL 情况下抓包情况

客户端用 wireshark 抓一下包：
可以发现前三个包是做 TCP 的握手协议



查看第 7 个包，此包是服务器发过来的 http 包，双击打开可看到包里的内容完全暴露了文件的内容，并没有经过加密。可知 http 协议是明文传输的。

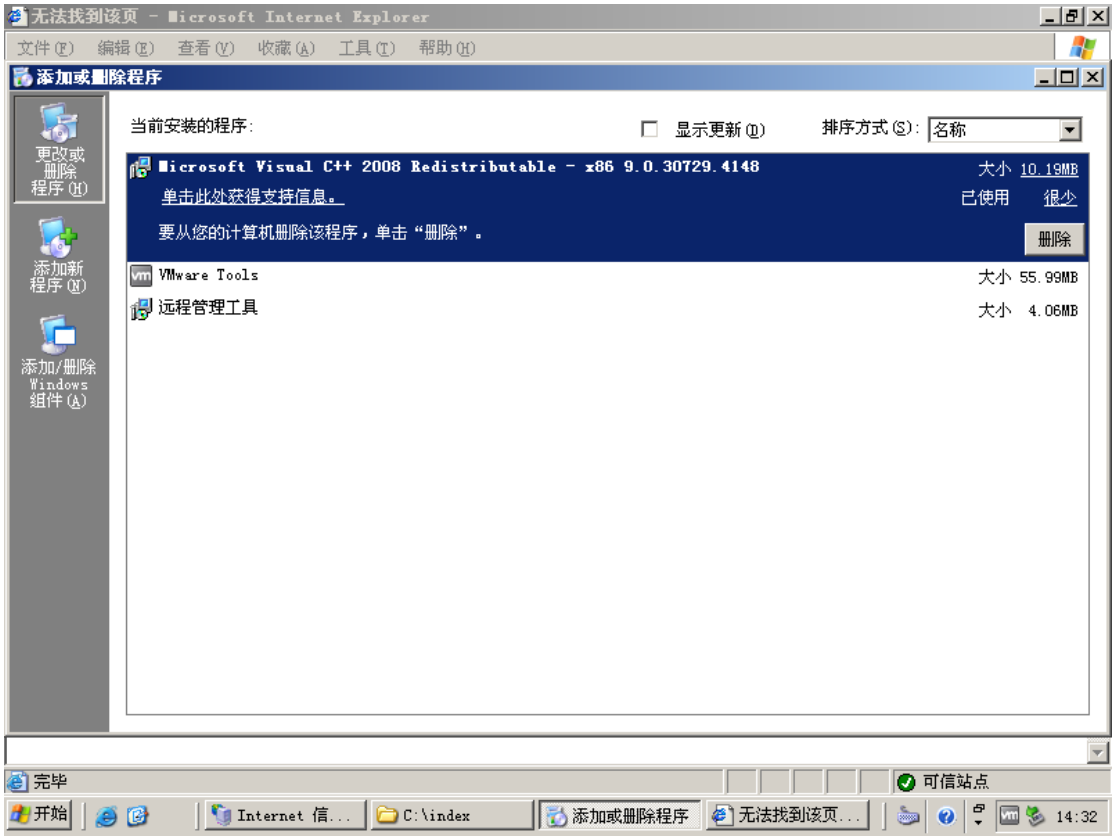


2.3 网站配置 ssl 协议

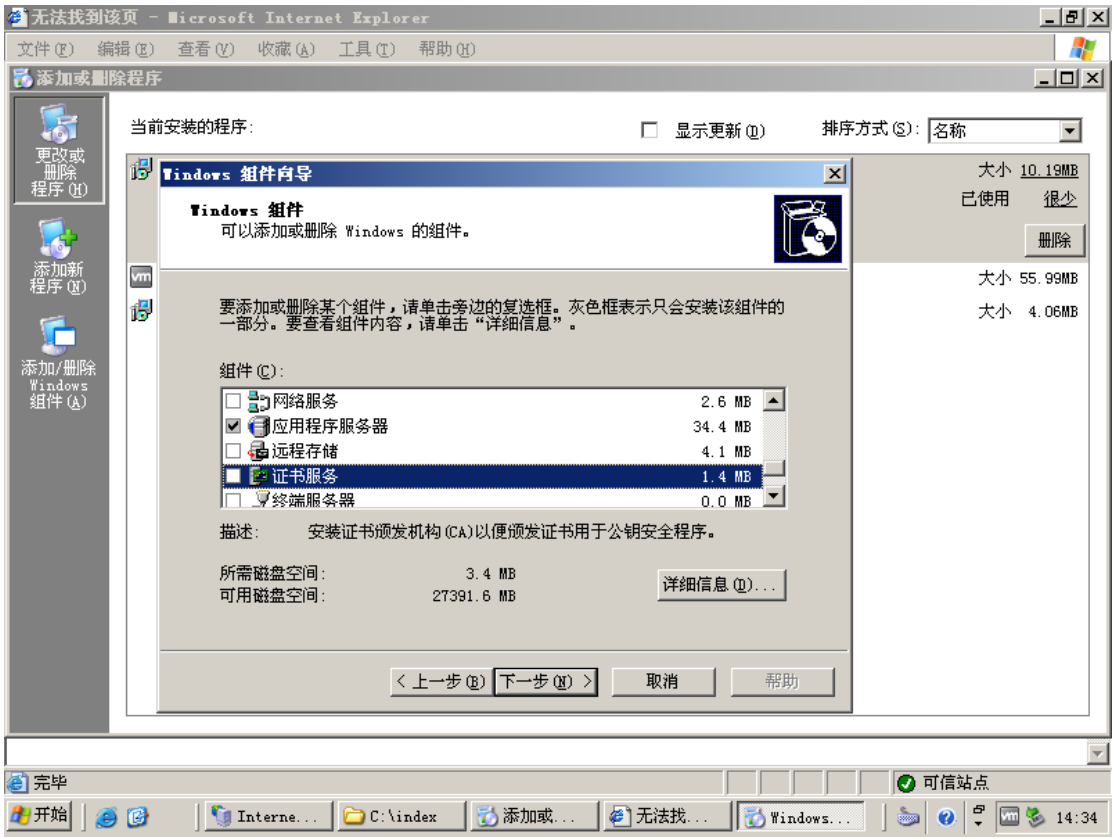
现在我们为刚才的网站配置 ssl 加密协议

2.3.1 安装证书服务

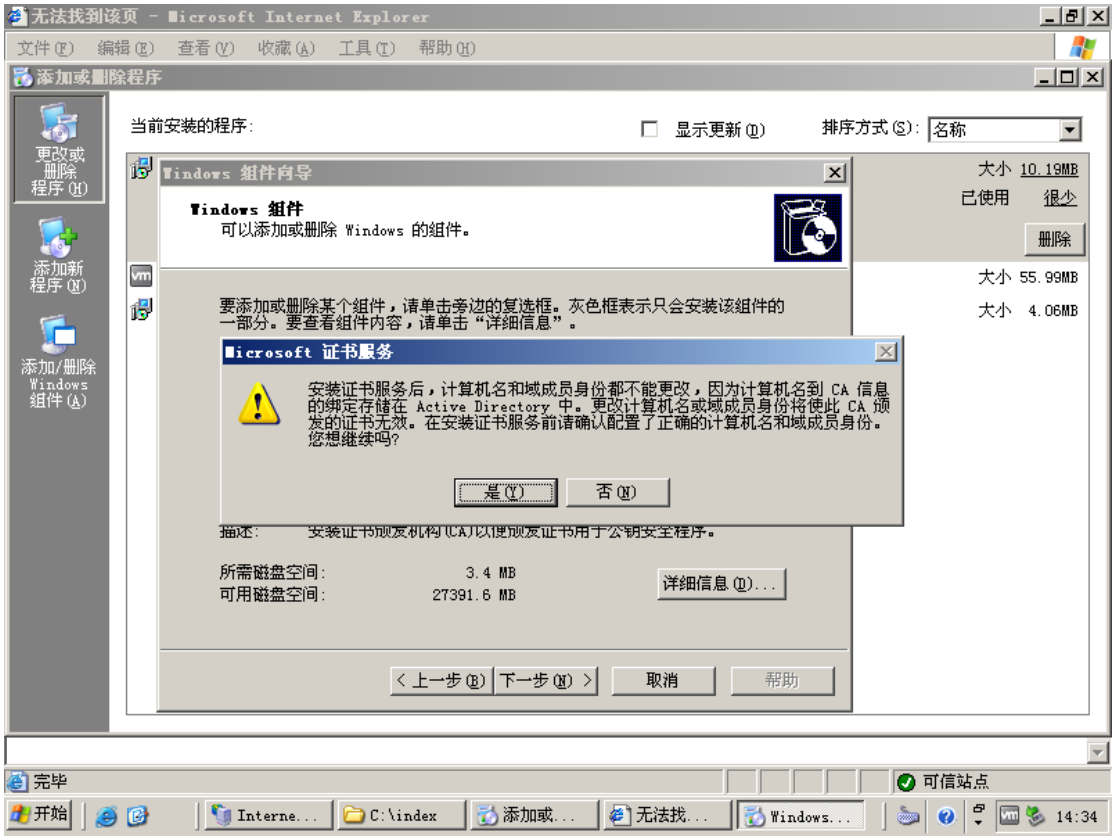
先打开添加或删除程序添加证书服务，ssl 协议需要证书



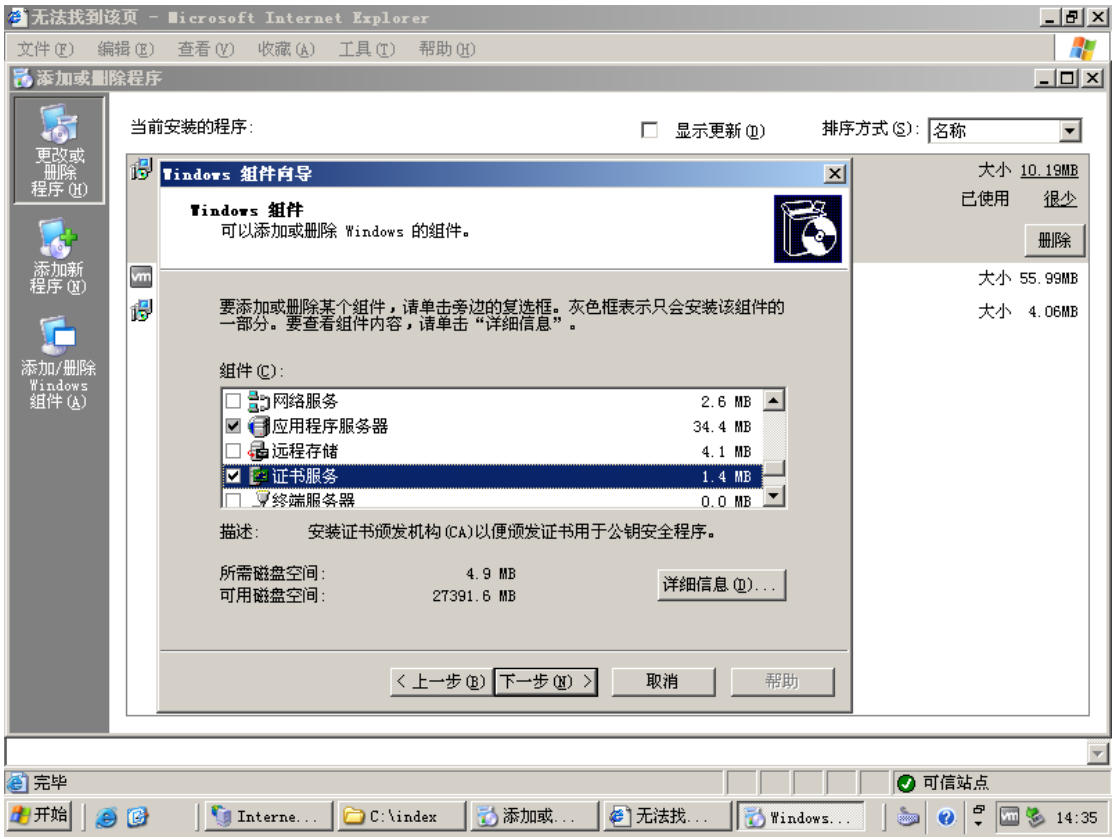
点击添加/删除 Windows 组件，勾选证书服务



这里会出现警告，确认即可

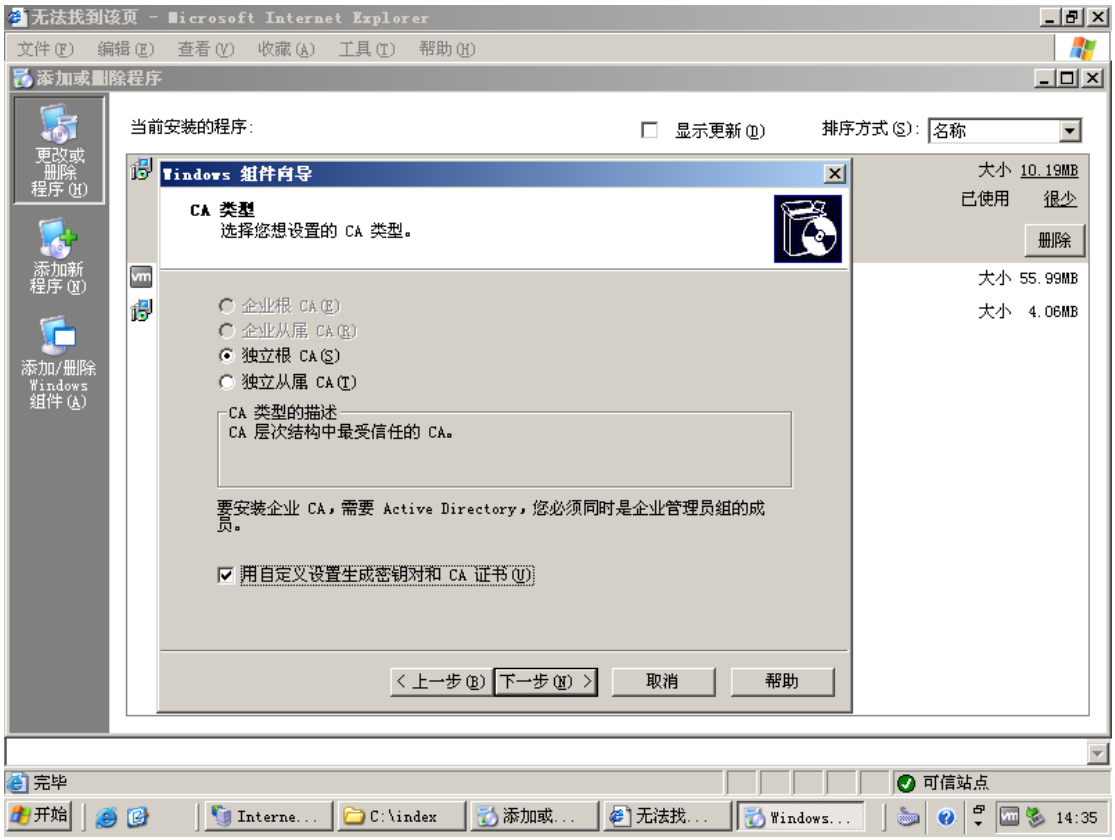


点击下一步

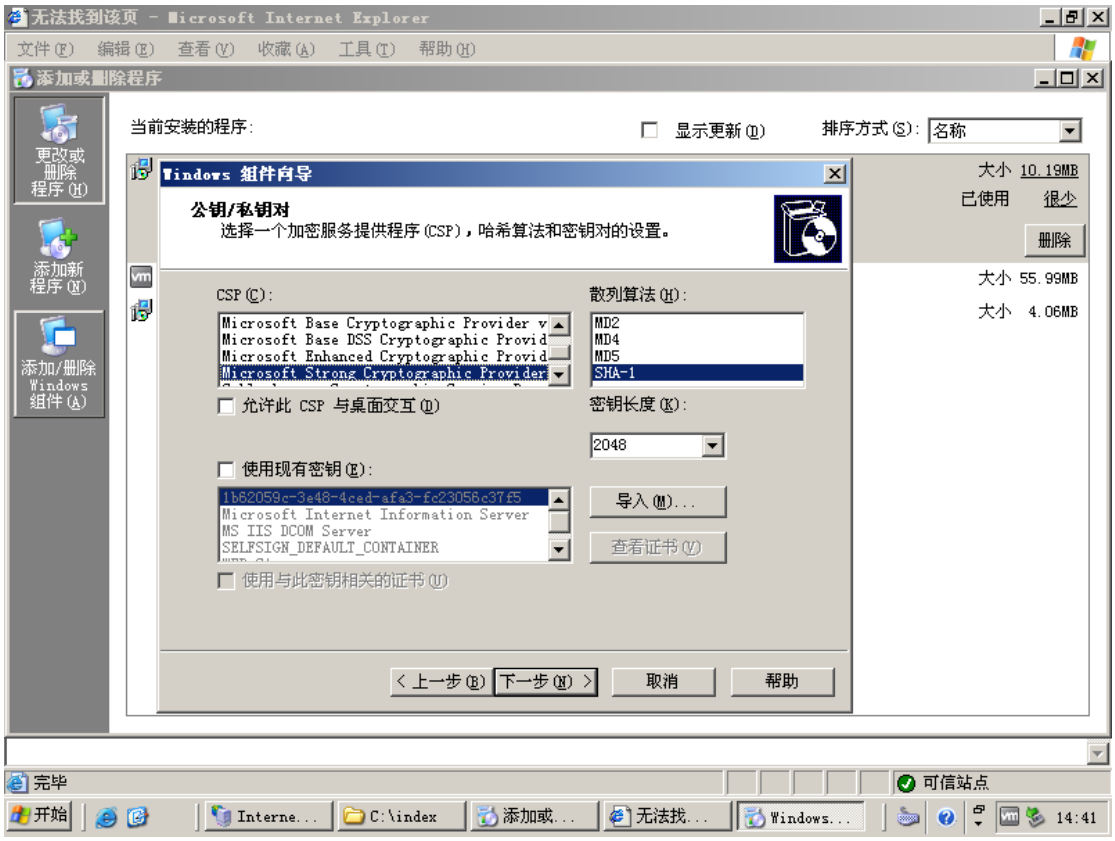


这里选择独立根 CA，和勾自定义设置生成密钥和 CA 证书，这里是以此服务器做最顶级的

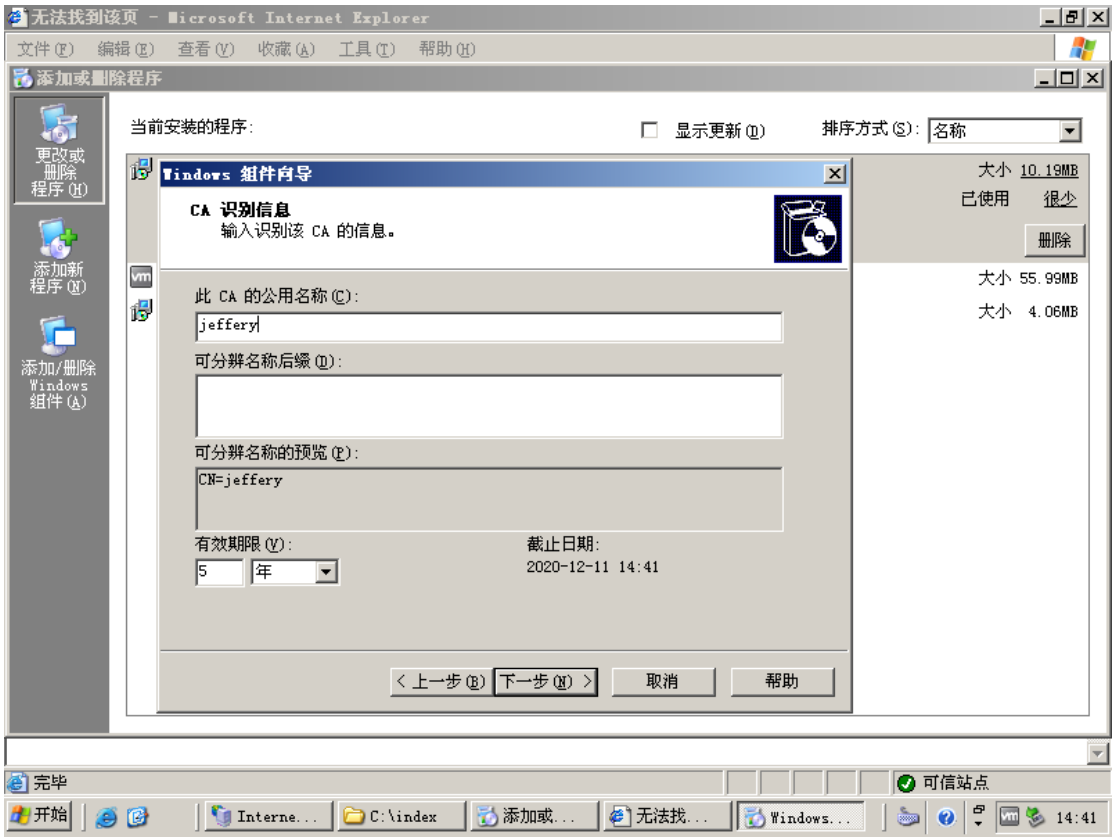
CA 服务器，点击下一步。



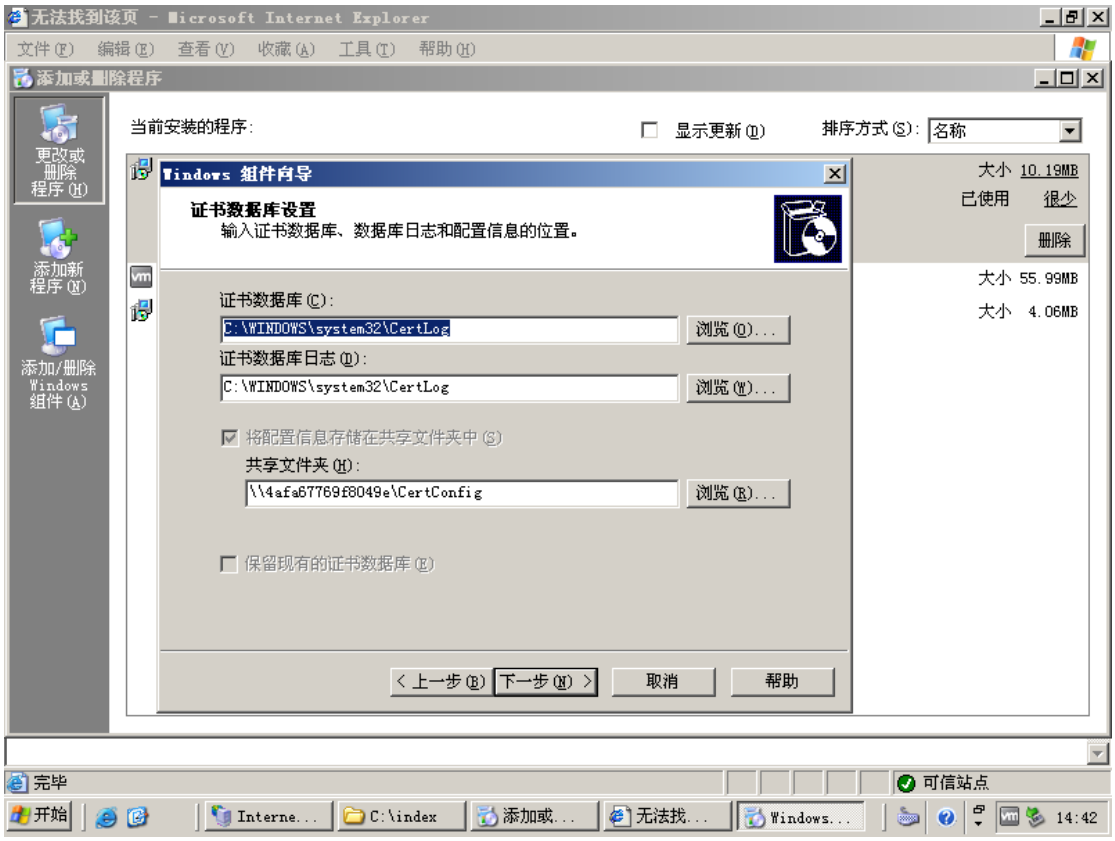
这里选择公钥私钥的算法，默认可直接点击下一步



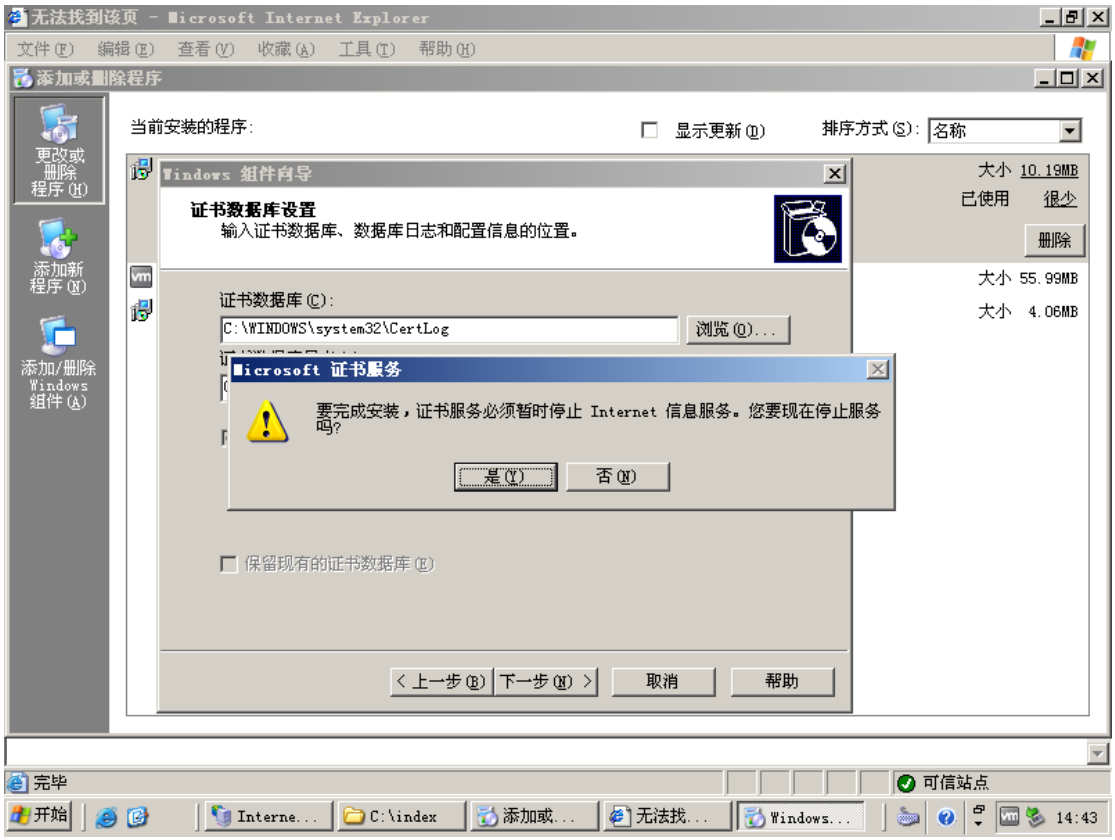
输入公有名称和有效期限，点击下一步



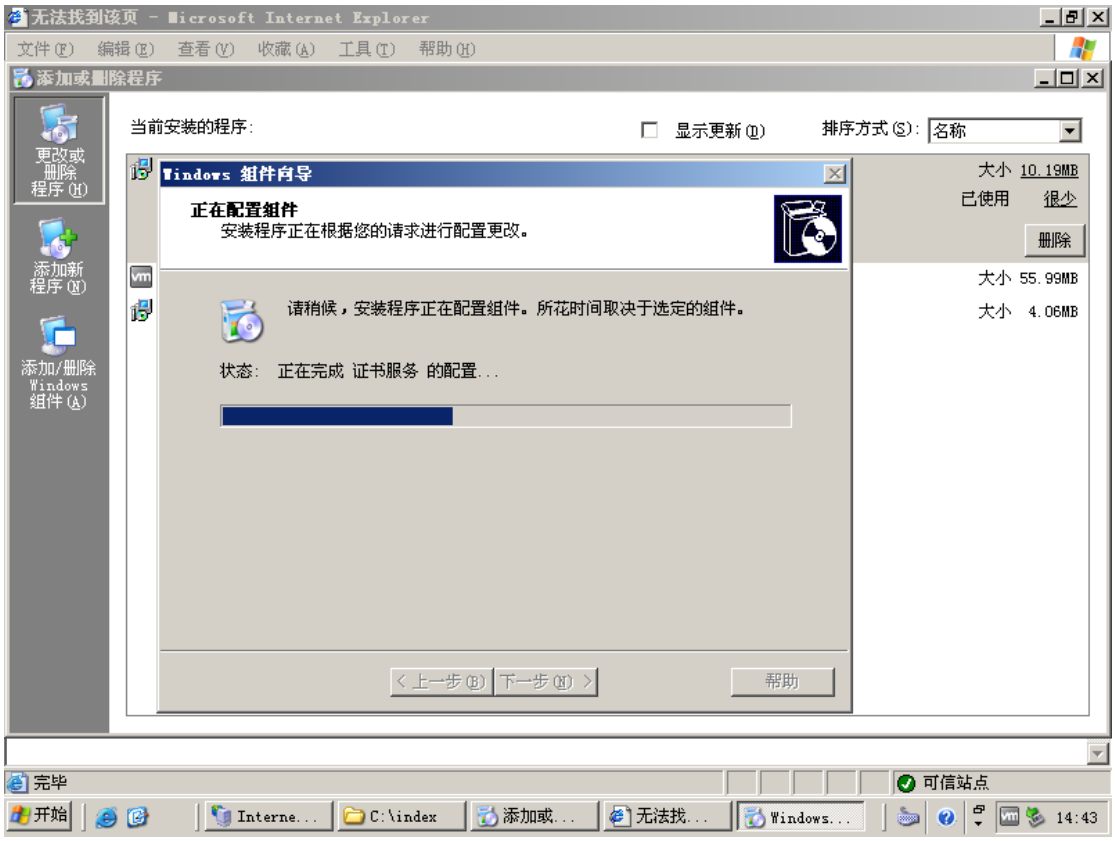
默认可直接点击下一步



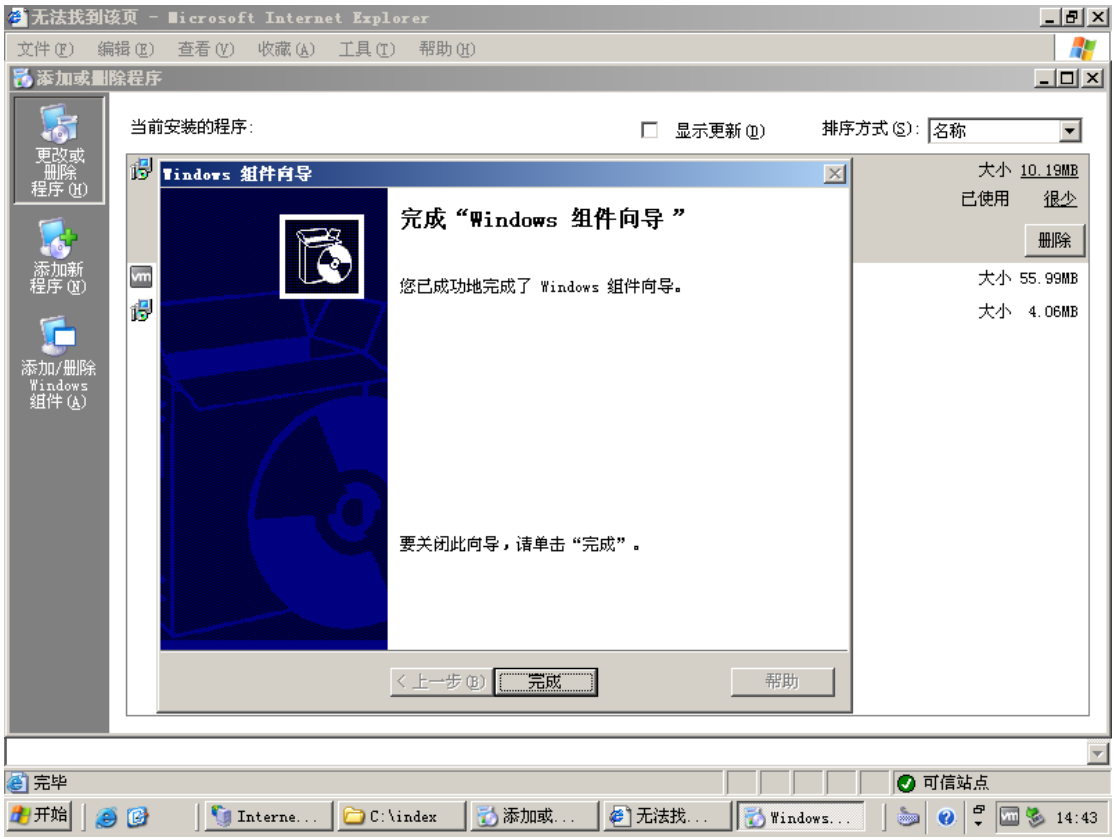
点击确认


无法找到该页 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
添加或删除程序
当前安装的程序:
显示更新(D)
排序方式(S): 名称
更改或删除程序(H)
添加新程序(N)
添加/删除 Windows 组件(A)
Windows 组件向导
证书数据库设置
输入证书数据库、数据库日志和配置信息的位置。
证书数据库(C):
C:\WINDOWS\system32\CertLog
浏览(O)...
Microsoft 证书服务
要完成安装，证书服务必须暂时停止 Internet 信息服务。您要现在停止服务吗?
是(Y)
否(N)
保留现有的证书数据库(E)
< 上一步(B)
下一步(N) >
取消
帮助
大小 10.19MB
已使用 很少
删除
大小 55.99MB
大小 4.06MB
完毕
可信站点
开始
Interne...
C:\index
添加或...
无法找...
Windows...
14:43

等待完成

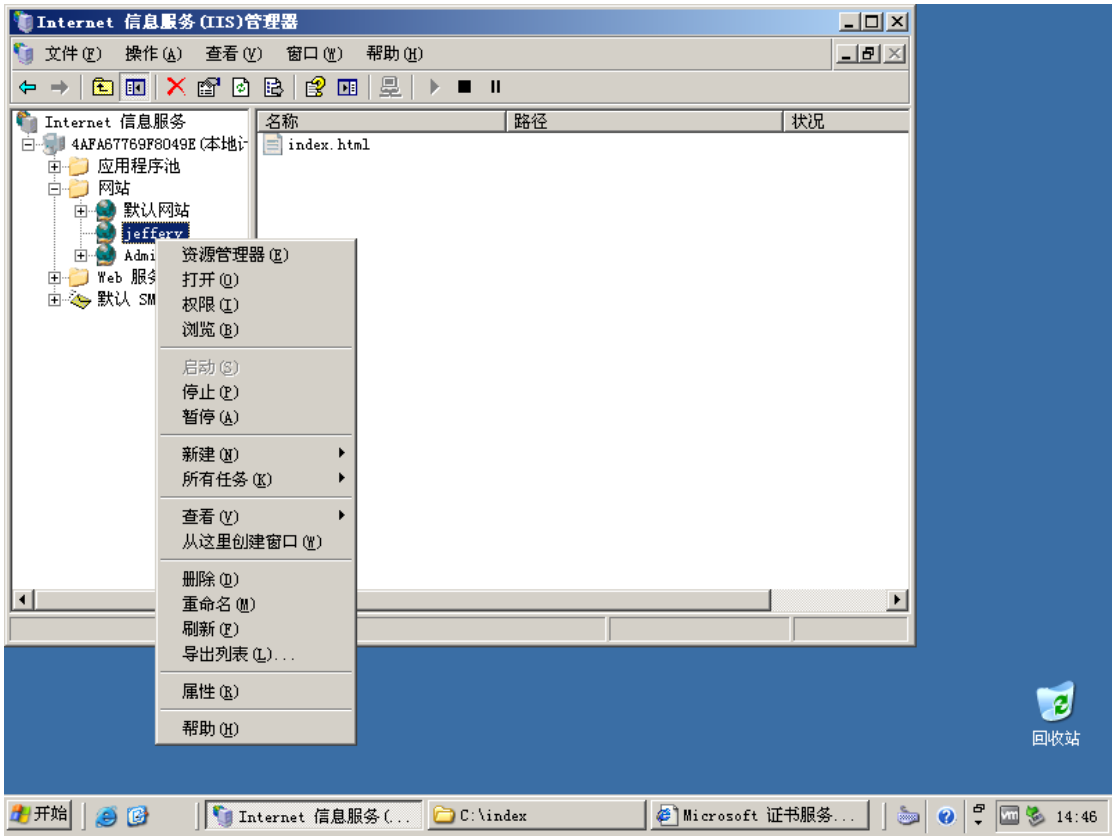

无法找到该页 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
添加或删除程序
当前安装的程序:
显示更新(D)
排序方式(S): 名称
更改或删除程序(H)
添加新程序(N)
添加/删除 Windows 组件(A)
Windows 组件向导
正在配置组件
安装程序正在根据您的请求进行配置更改。
请稍候，安装程序正在配置组件。所花时间取决于选定的组件。
状态: 正在完成 证书服务 的配置...
< 上一步(B)
下一步(N) >
帮助
大小 10.19MB
已使用 很少
删除
大小 55.99MB
大小 4.06MB
完毕
可信站点
开始
Interne...
C:\index
添加或...
无法找...
Windows...
14:43

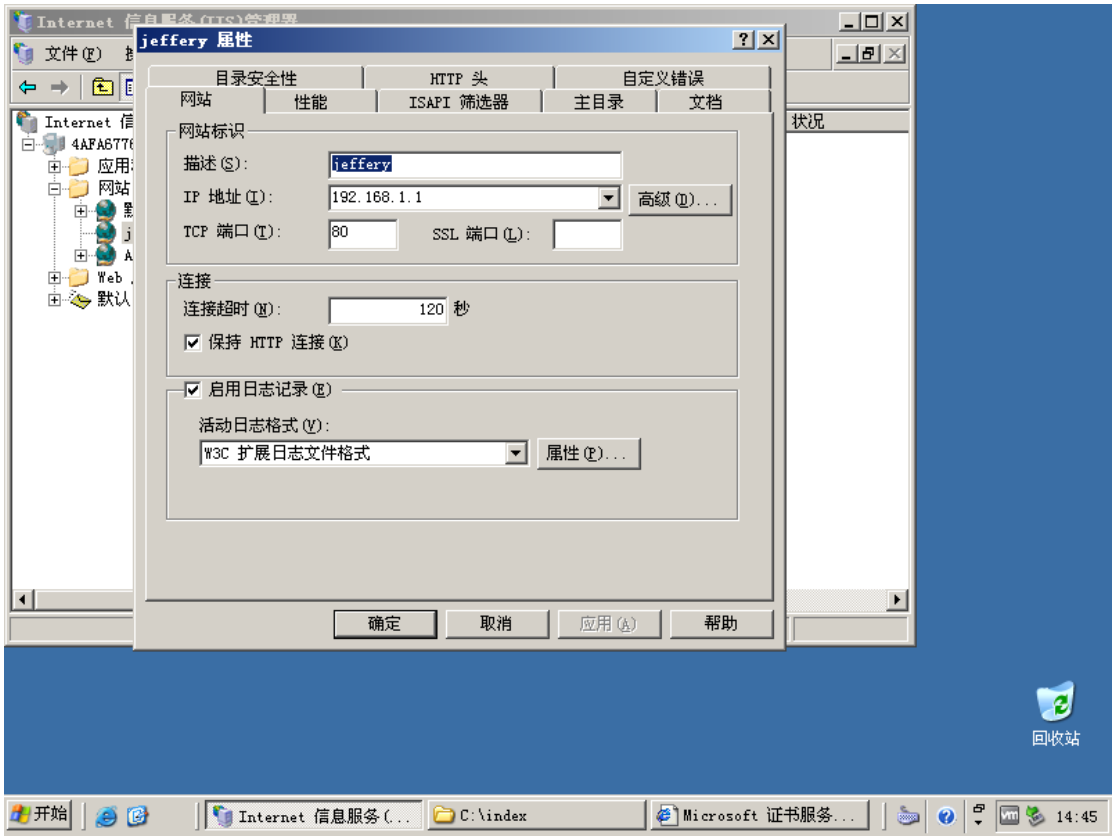
点击完成



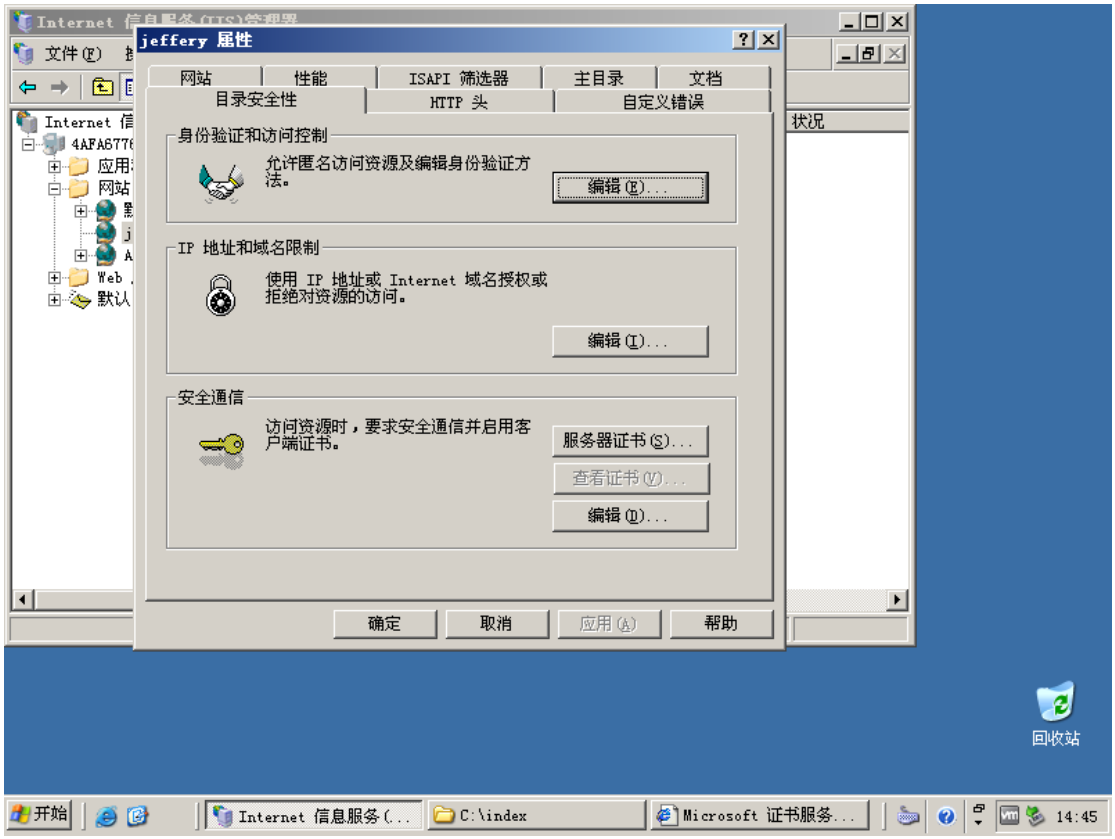
2.3.2 创建根证书

右键要配置的网站，属性

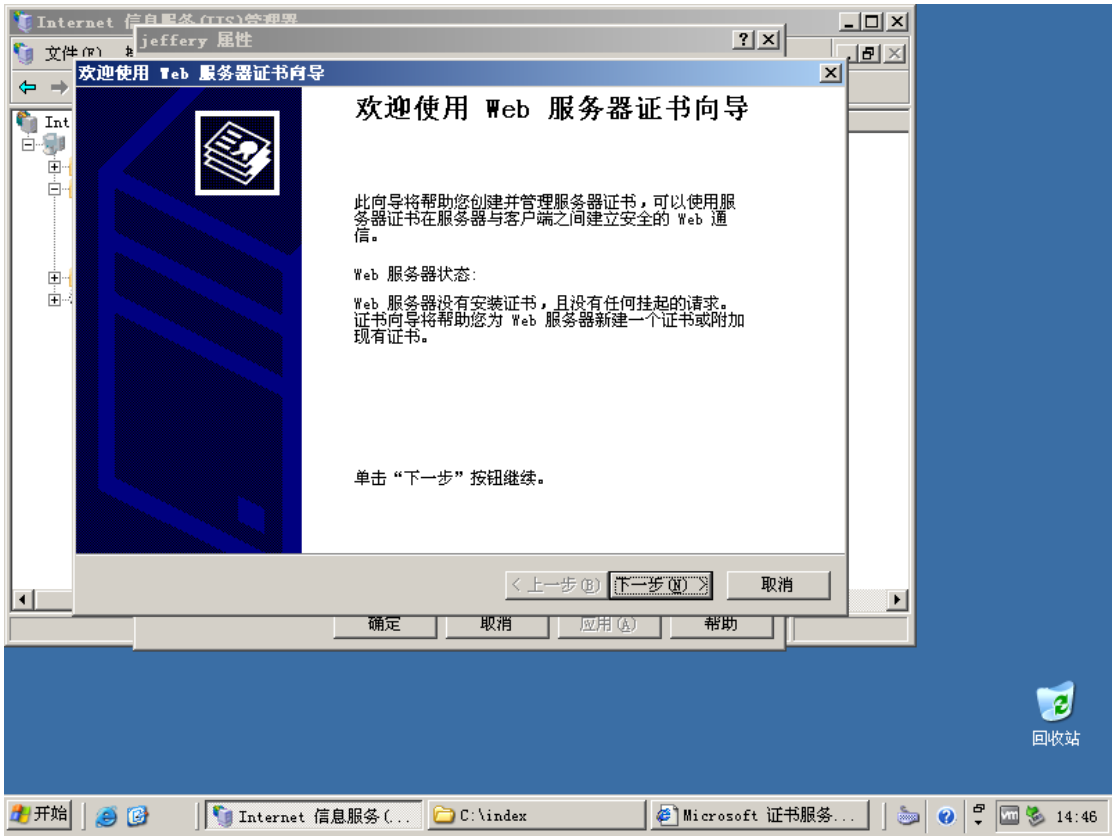




切换到目录安全性，点击服务器证书



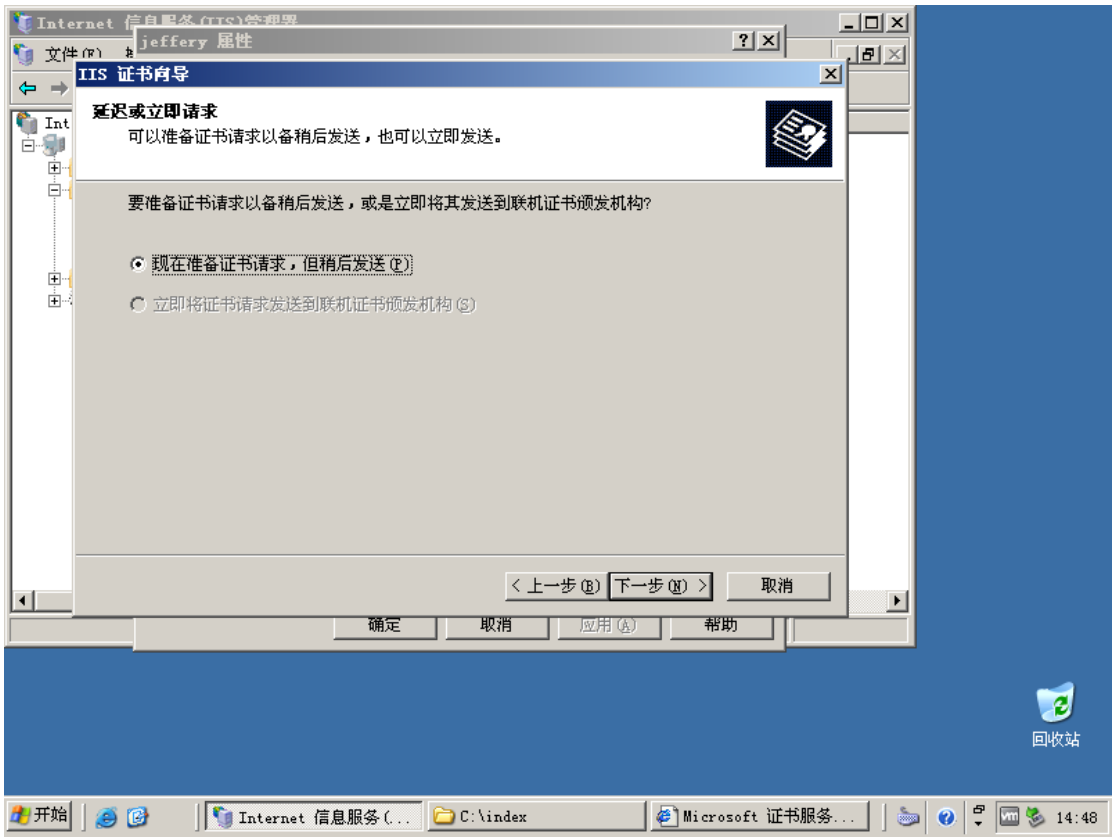
点击下一步



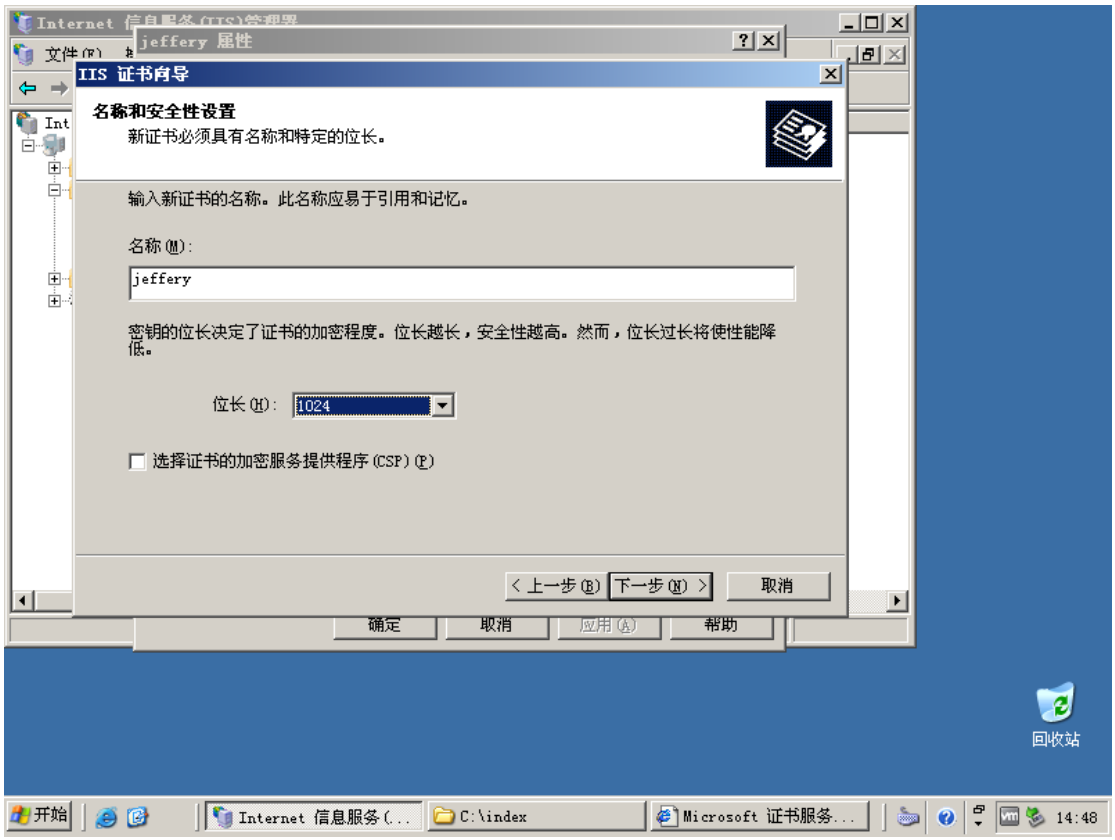
选择新建证书，点下一步


jeffery 属性
IIS 证书向导
服务器证书
以下是为网站分配证书的方法。
选择此网站使用的方法:
新建证书(C)。
分配现有证书(A)。
从密钥管理器备份文件导入证书(O)。
从 .pfx 文件导入证书(M)。
将远程服务器站点的证书复制或移动到此站点(Y)。
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(...
C:\index
Microsoft 证书服务...
14:47

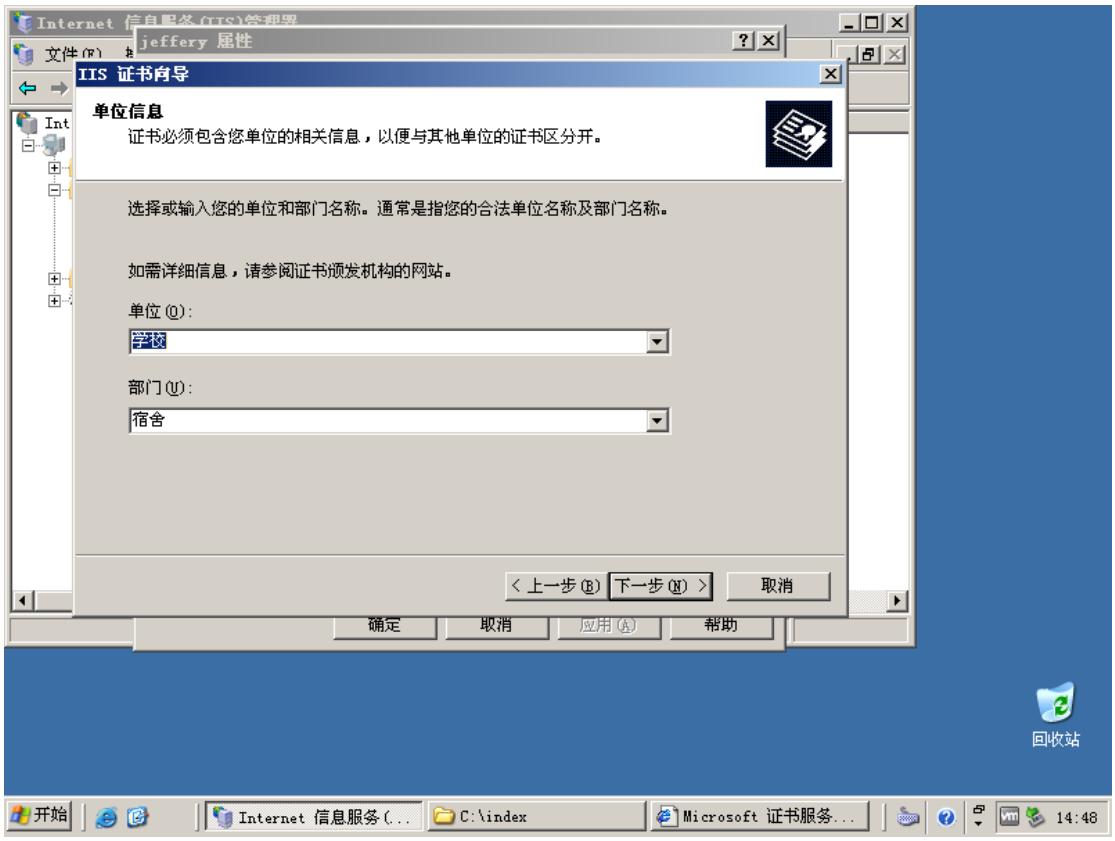
下一步


jeffery 属性
IIS 证书向导
延迟或立即请求
可以准备证书请求以备稍后发送，也可以立即发送。
要准备证书请求以备稍后发送，或是立即将其发送到联机证书颁发机构?
现在准备证书请求，但稍后发送(P)
立即将证书请求发送到联机证书颁发机构(S)
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(...
C:\index
Microsoft 证书服务...
14:48

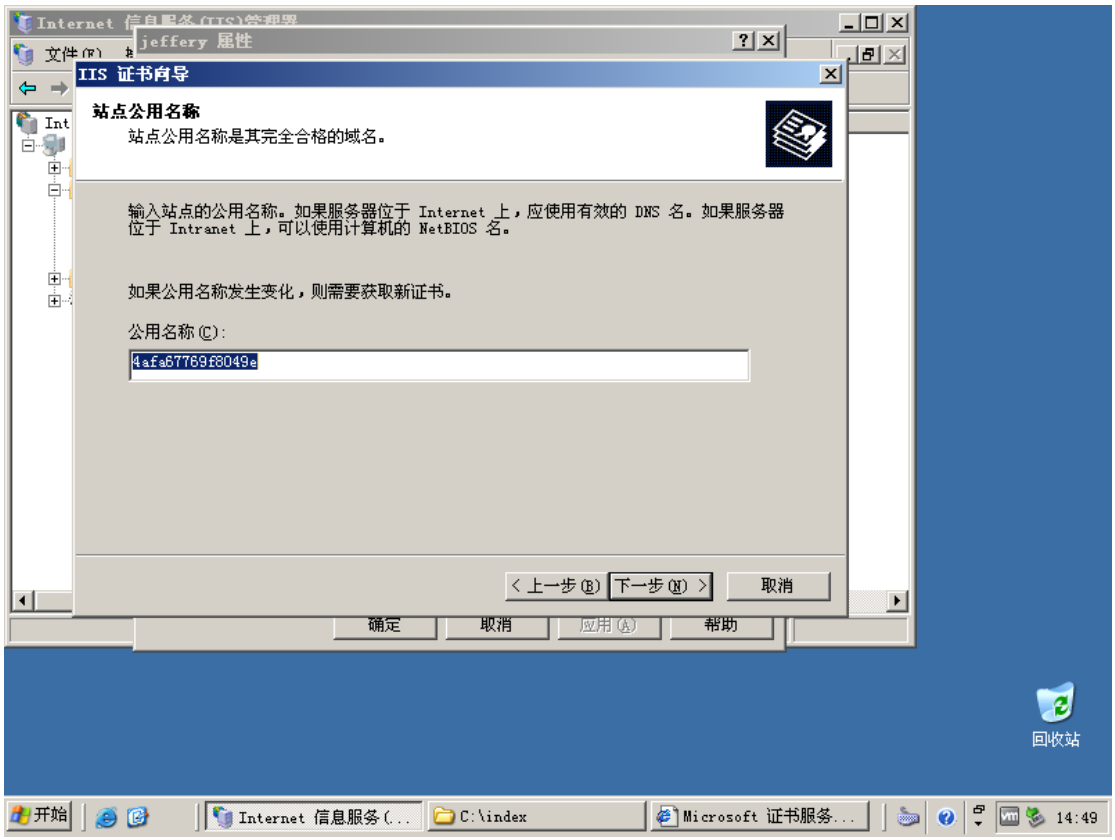
默认直接下一步


jeffery 属性
IIS 证书向导
名称和安全性设置
新证书必须具有名称和特定的位长。
输入新证书的名称。此名称应易于引用和记忆。
名称(M):
jeffery
密钥的位长决定了证书的加密程度。位长越长，安全性越高。然而，位长过长将使性能降低。
位长(H):
1024
选择证书的加密服务提供程序(CSP)(P)
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(...
C:\index
Microsoft 证书服务...
14:48

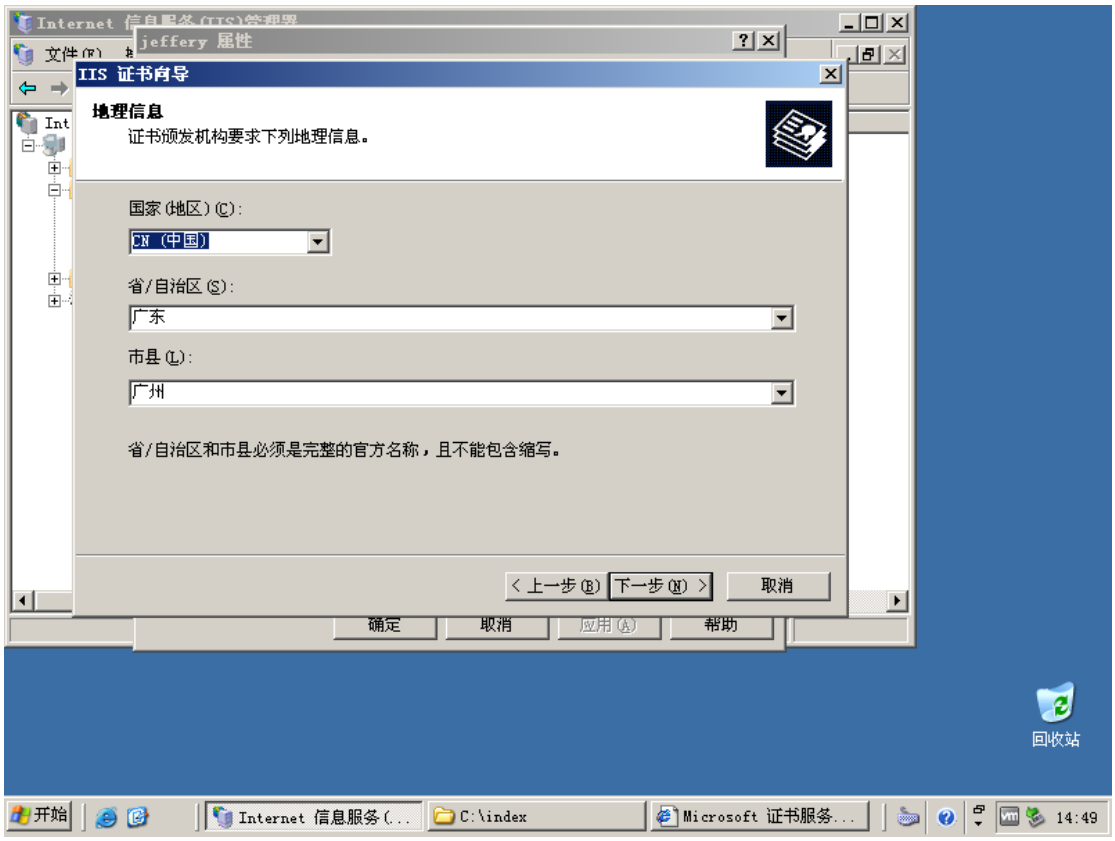
填写单位、部门


jeffery 属性
IIS 证书向导
单位信息
证书必须包含您单位的相关信息，以便与其他单位的证书区分开。
选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。
如需详细信息，请参阅证书颁发机构的网站。
单位(O):
学校
部门(U):
宿舍
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(...
C:\index
Microsoft 证书服务...
14:48

这里的公用名称的是域名，这里没有，随意



按要求填写



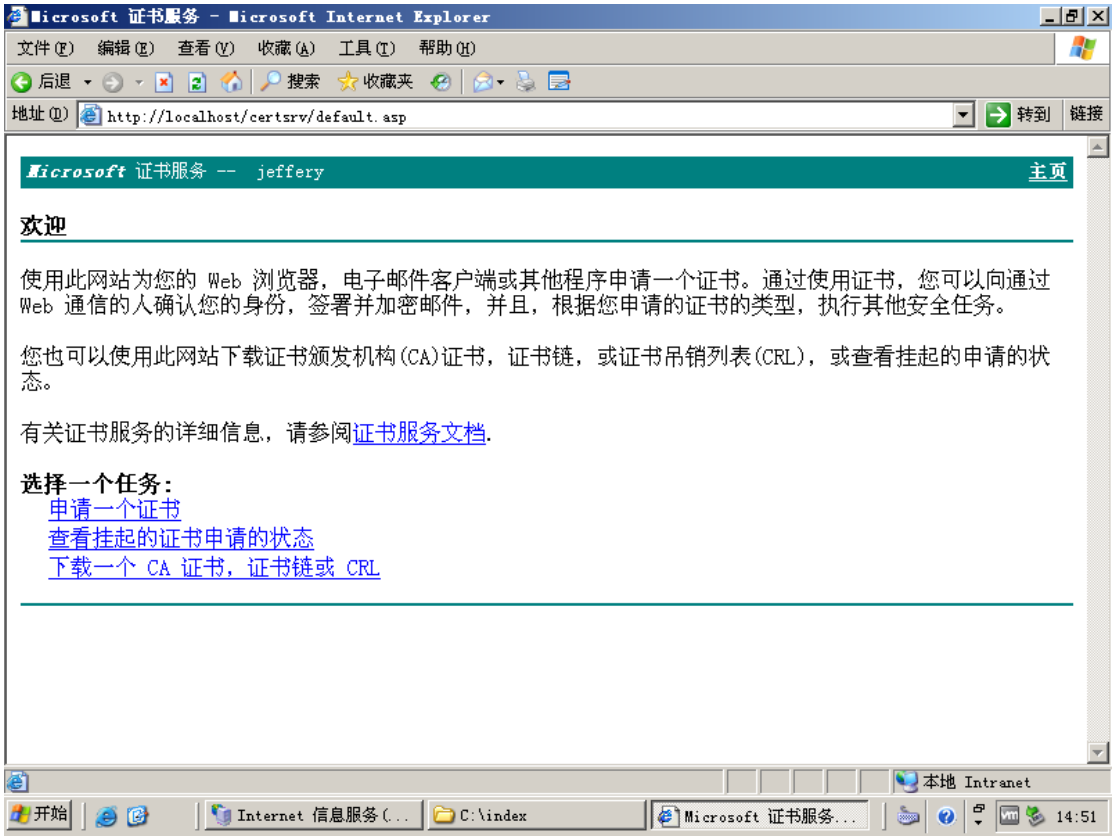
填写输出文件目录

下一步

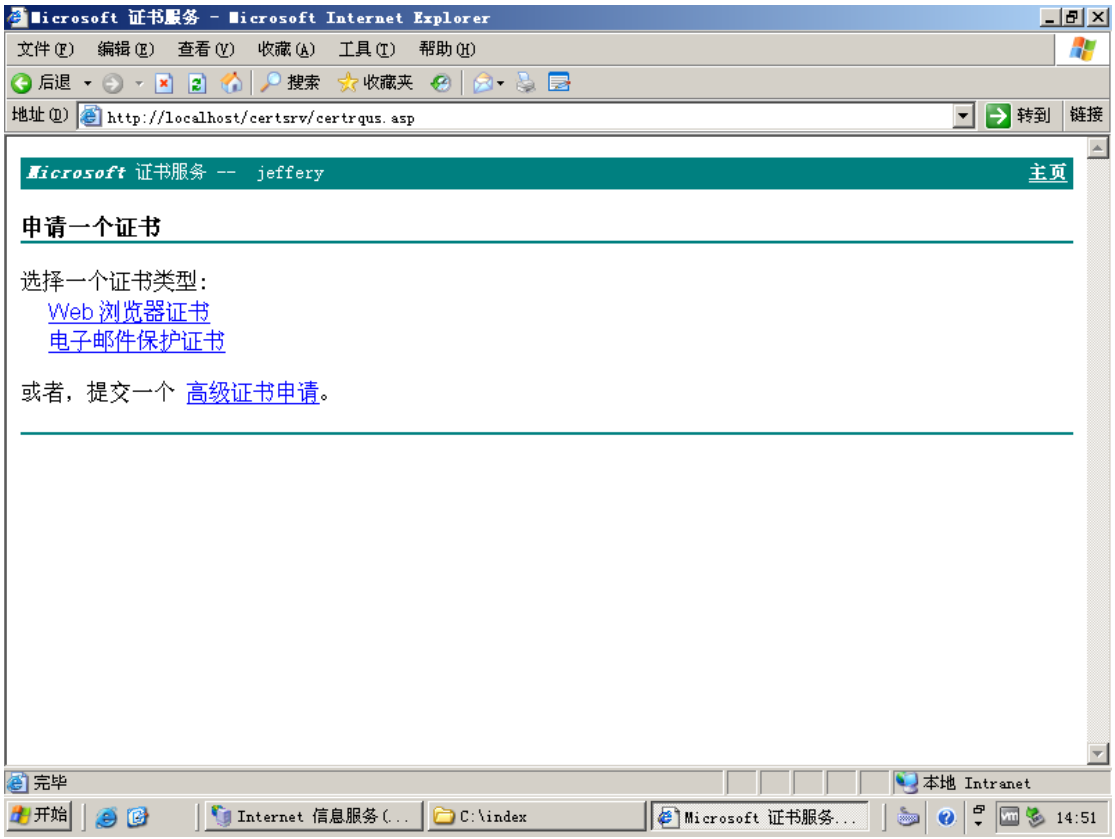
点击完成

2.3.3 创建服务器证书

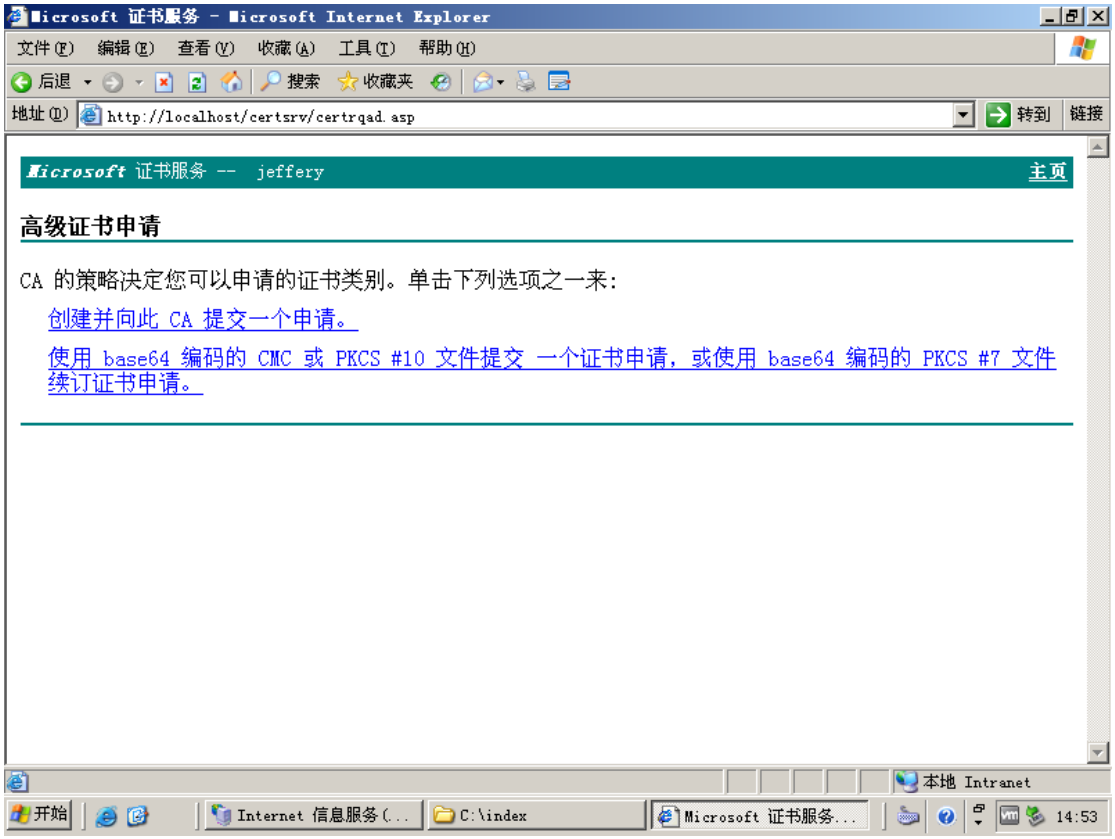
然后在服务器的浏览器输入 http://localhost/certsrv/default.asp，进入证书申请服务，点击申请一个证书



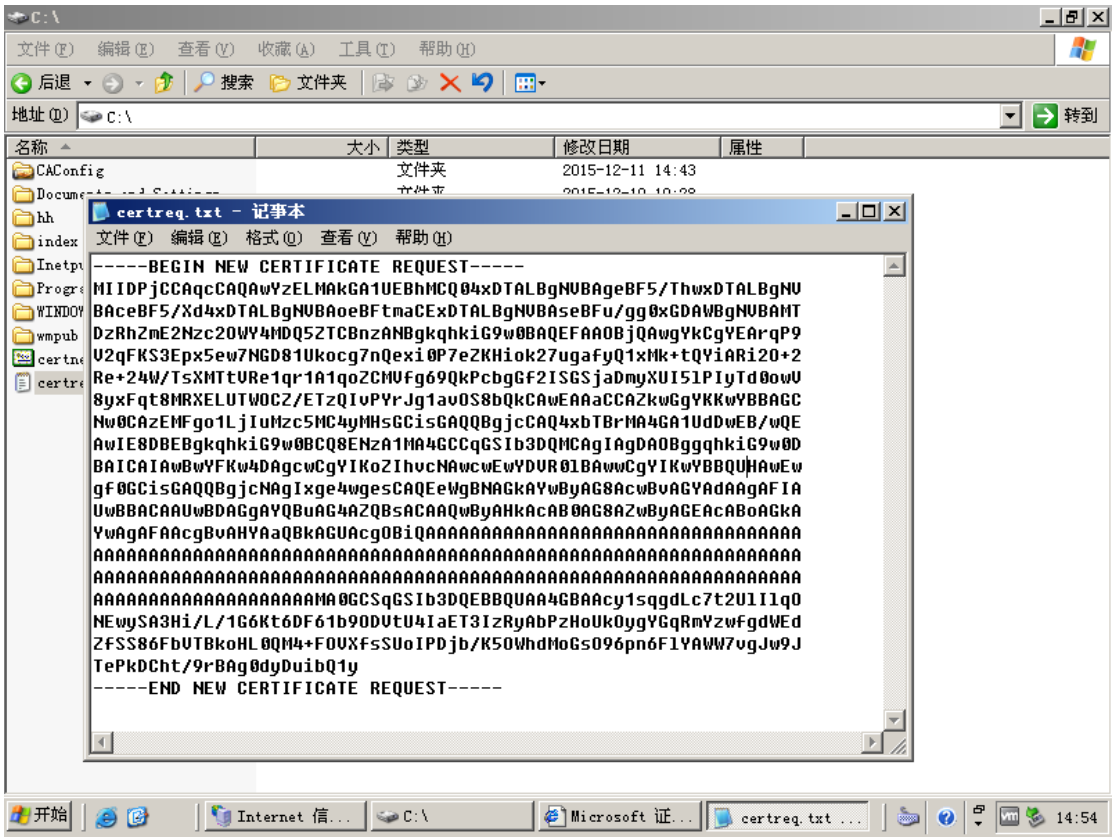
点击高级证书申请



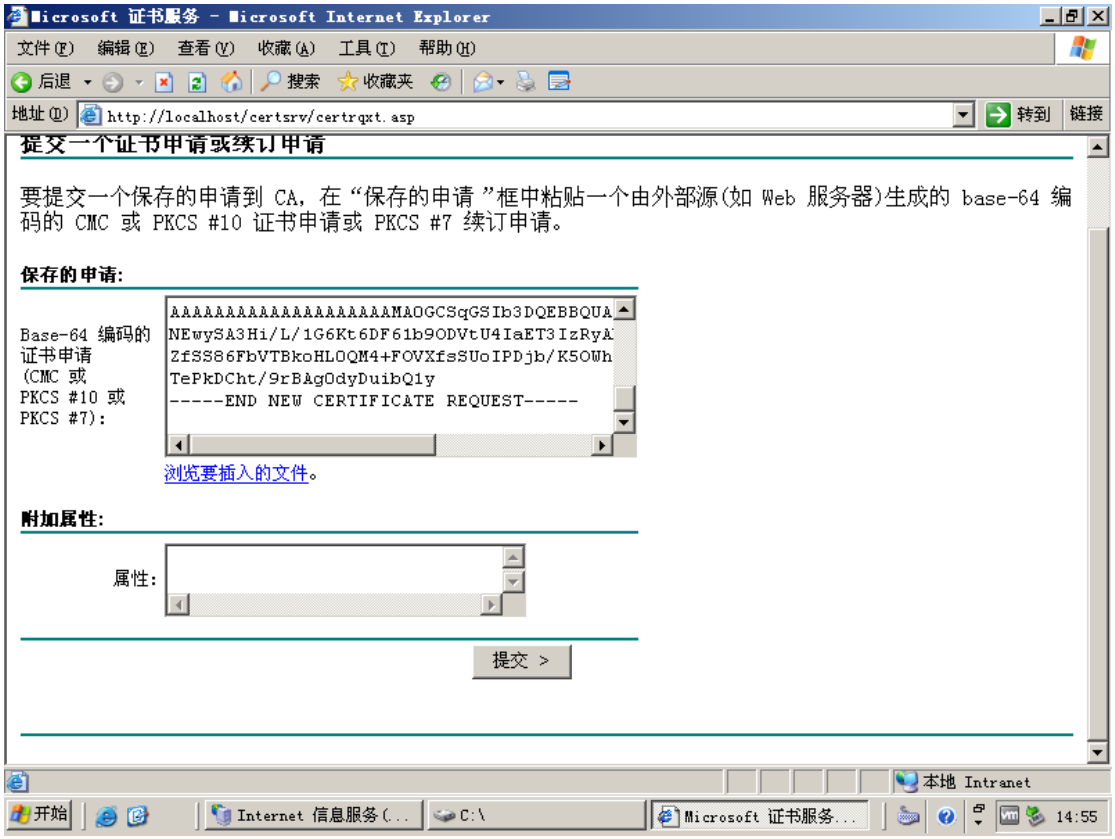
点击使用 base64 编码的 CMC 申请



然后打开刚才输出的证书请求文件，把里面的内容全部复制



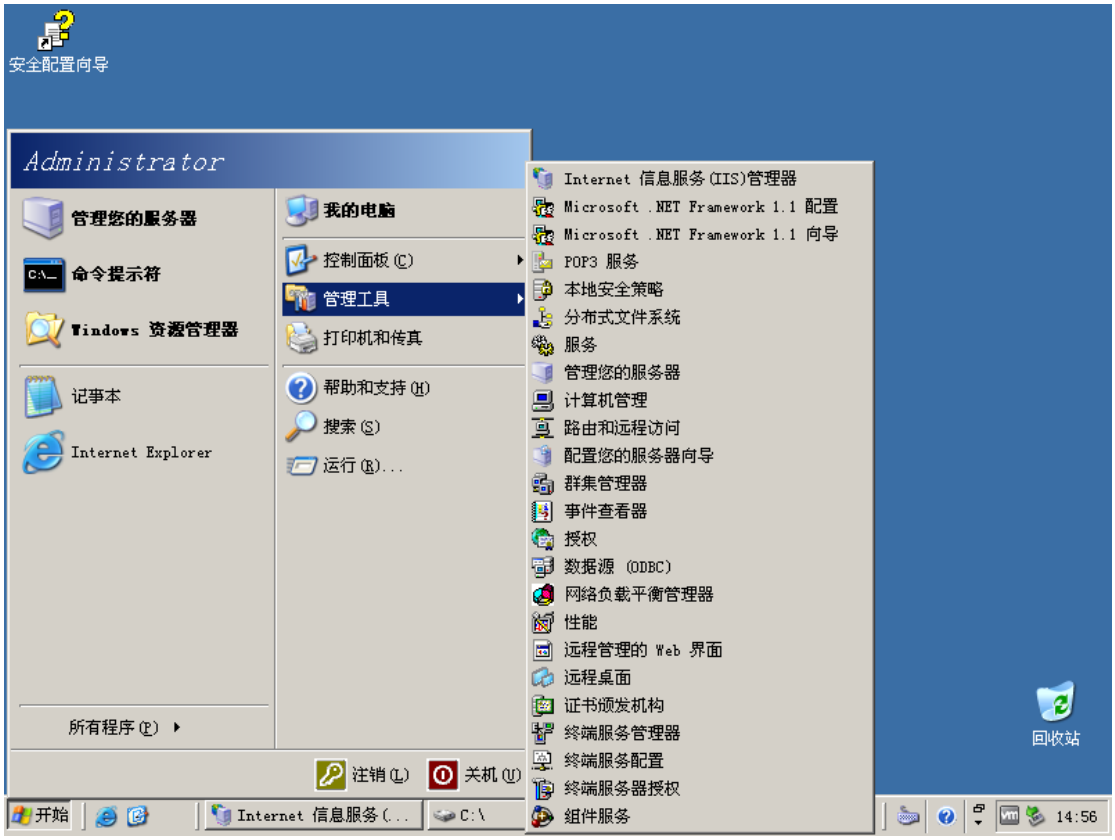
粘贴到刚才的申请网站中，点击提交


Microsoft 证书服务 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://localhost/certsrv/certrqxt.asp
转到 链接
提交一个证书申请或续订申请
要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。
保存的申请:
Base-64 编码的证书申请 (CMC 或 PKCS #10 或 PKCS #7):
AAAAAAAAAAAAAAAAAAAAAAMAOGCSqGSIb3DQEBBQUA
NEwySA3Hi/L/1G6Kt6DF61b9ODVtU4IaET3IzRyA
ZfSS86FbVTBkoHLOQM4+FOVXfsSUoIPDjb/K5OWh
TePkDCht/9rBAgOdyDuibQ1y
-----END NEW CERTIFICATE REQUEST-----
浏览要插入的文件。
附加属性:
属性:
提交 >
本地 Intranet
开始
Internet 信息服务(...
C:\
Microsoft 证书服务...
14:55

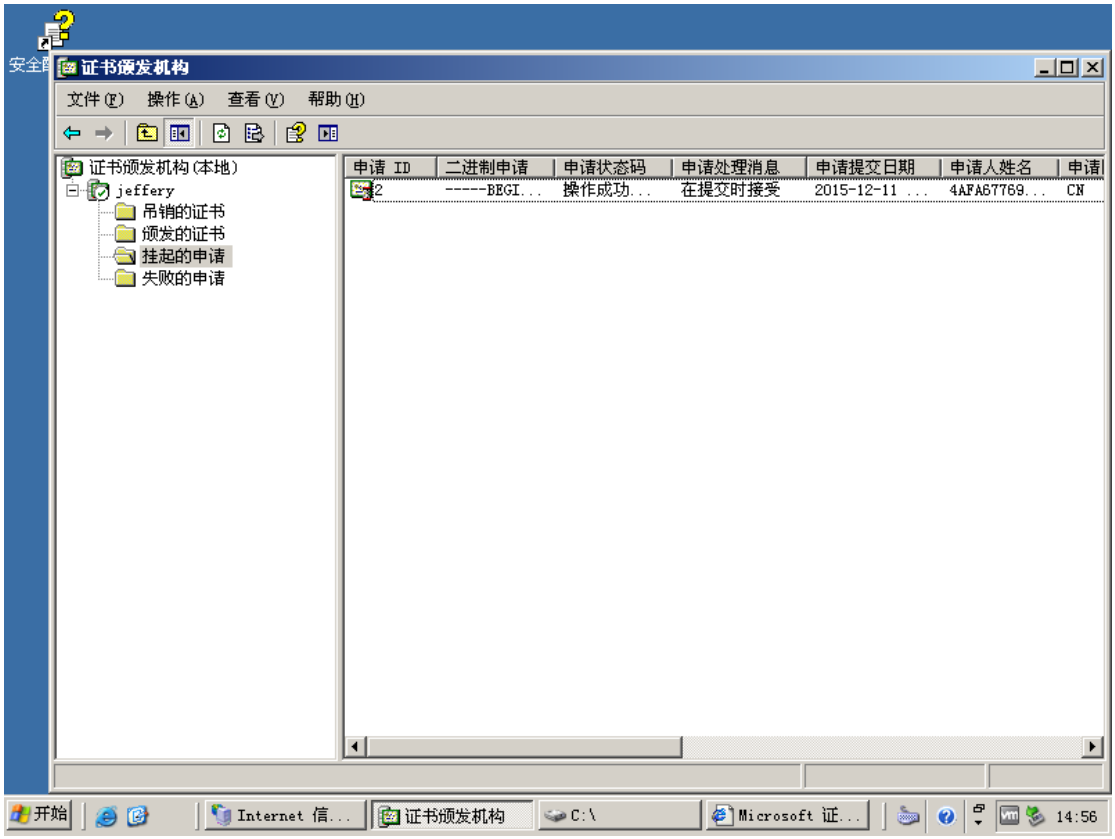

Microsoft 证书服务 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://localhost/certsrv/certfnsh.asp
转到 链接
Microsoft 证书服务 -- jeffery
主页
证书挂起
您的证书申请已经收到。但是，您必须等待管理员颁发您申请的证书。
您的申请 Id 为 2。
请在一天或两天内返回此网站以检索您的证书。
注意：您必须用此 Web 浏览器在 10 天内返回以检索您的证书
完毕
本地 Intranet
开始
Internet 信息服务(...
C:\
Microsoft 证书服务...
14:55

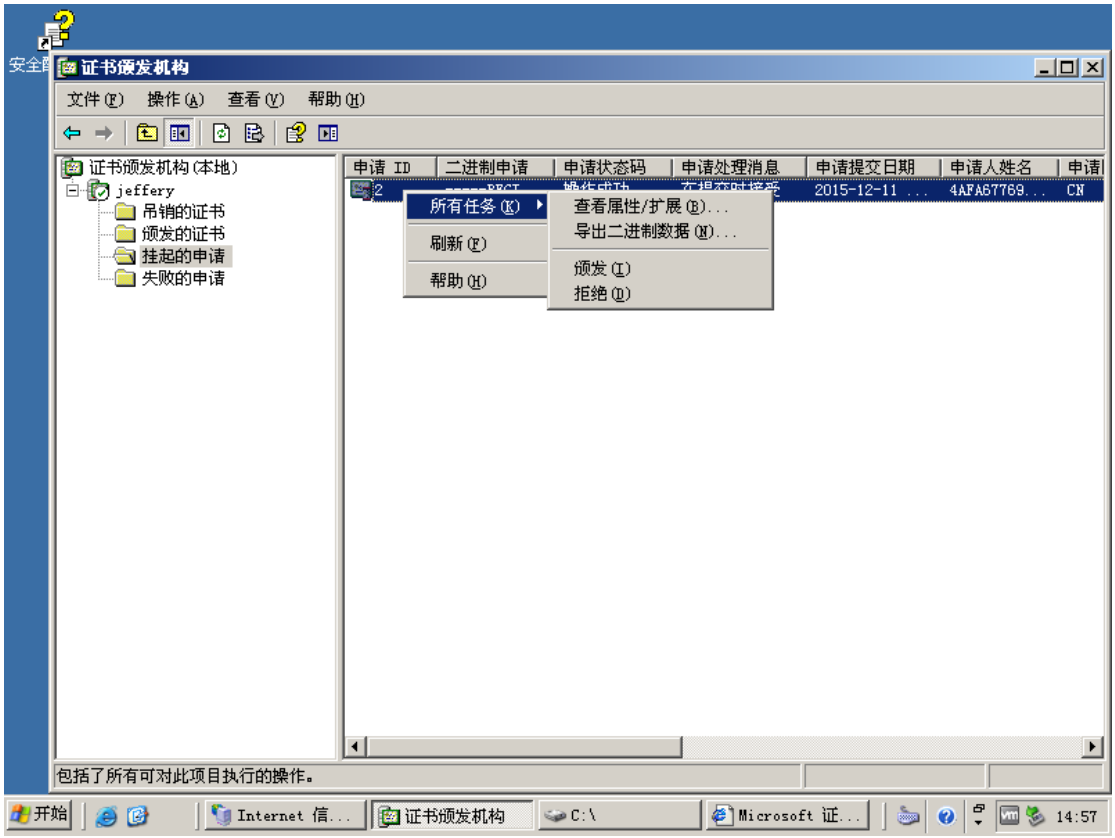
2.3.4 证书签发启用 SSL

然后打开管理工具---证书颁发机构

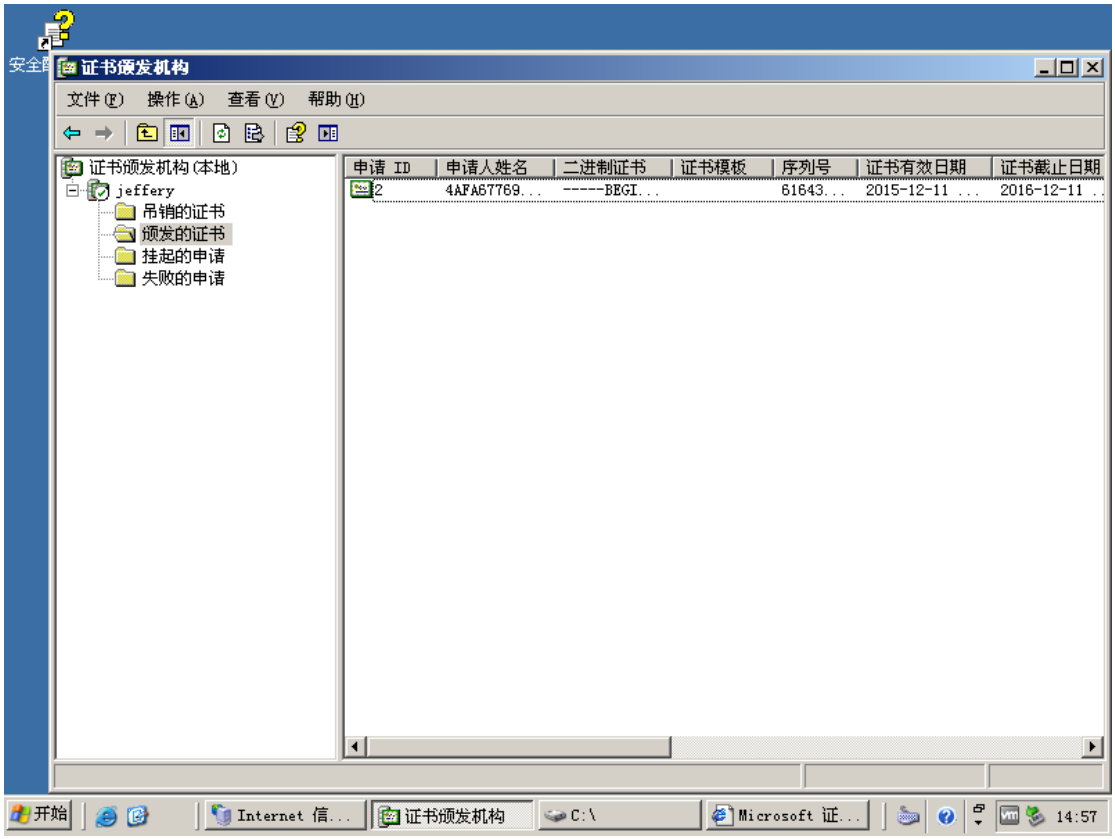


选择挂起的申请，右键颁发

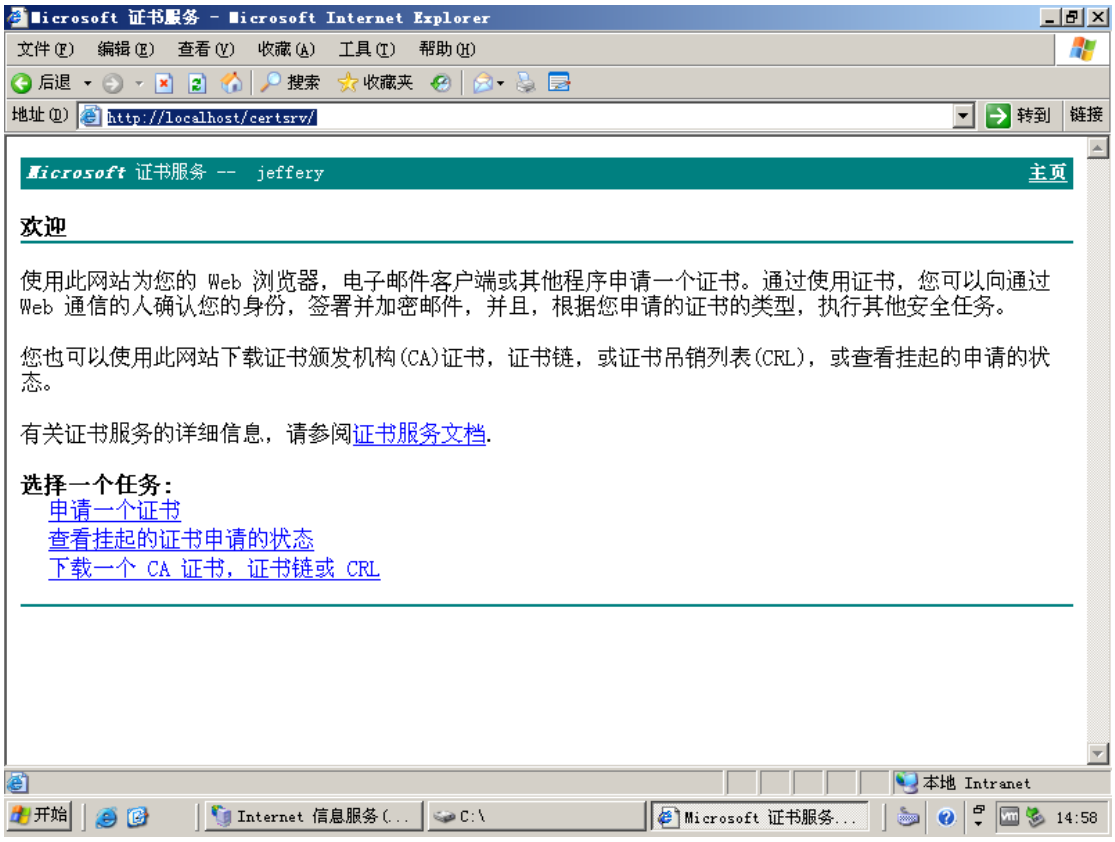




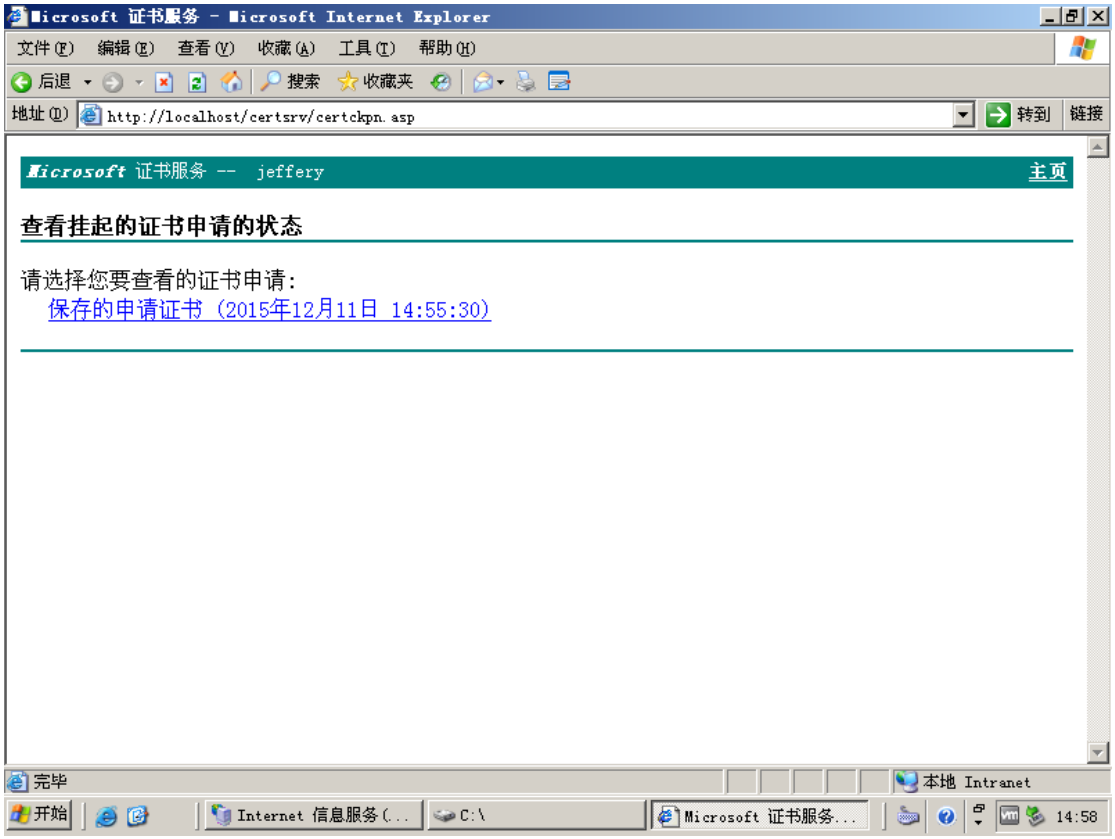
然后在颁发的证书一栏就可以看到了



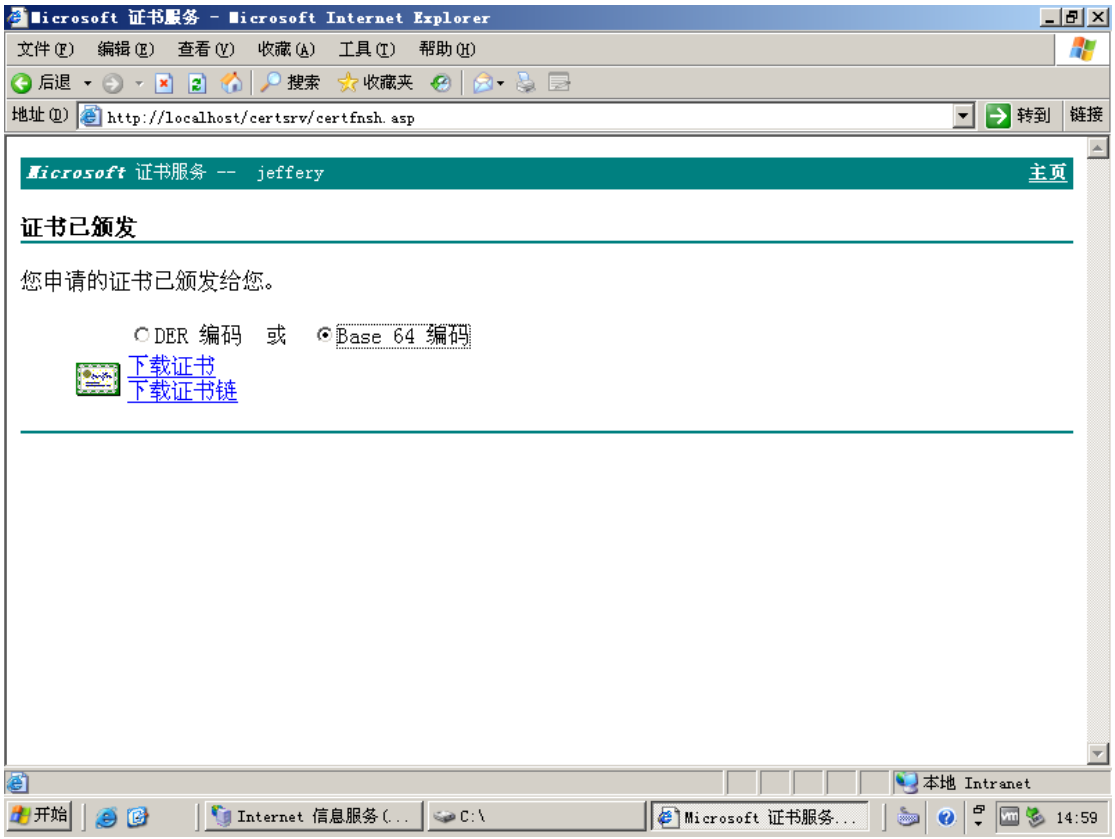
然后再次打开 http://localhost/certsrv/default.asp，点击查看挂起的证书申请的状态



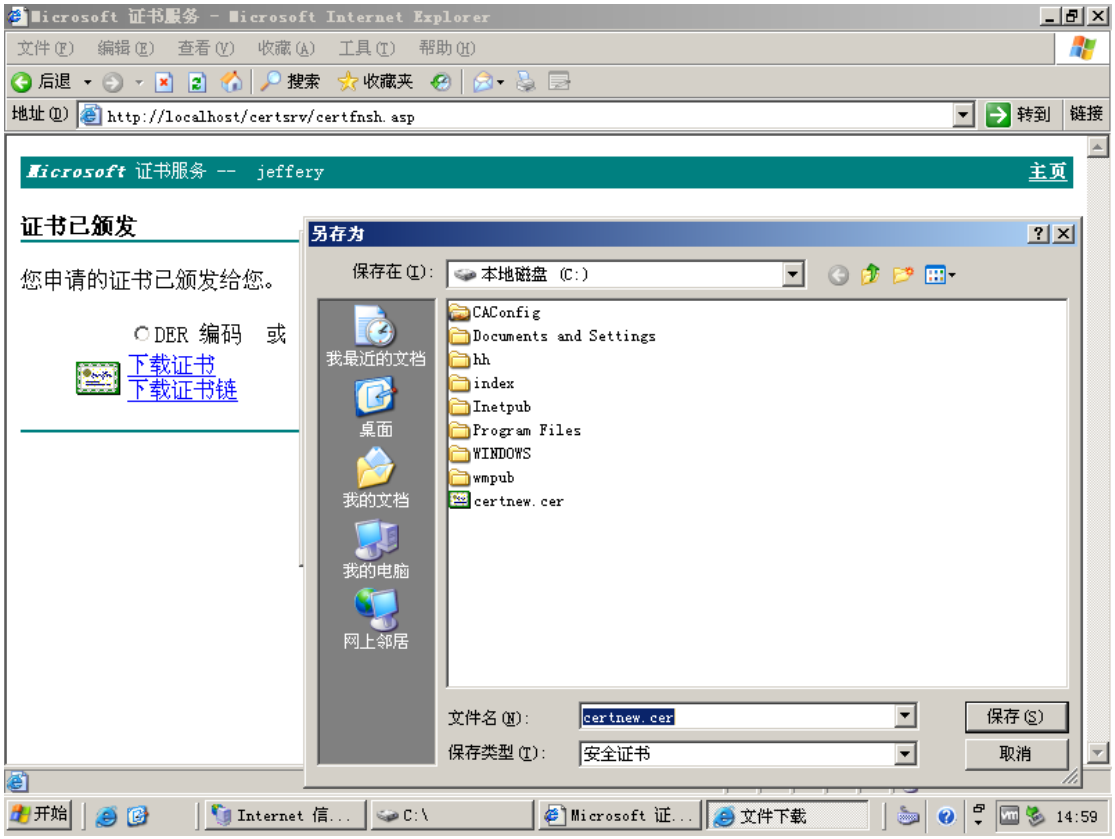
点击申请的证书



选择 Base64 编码，点击下载证书

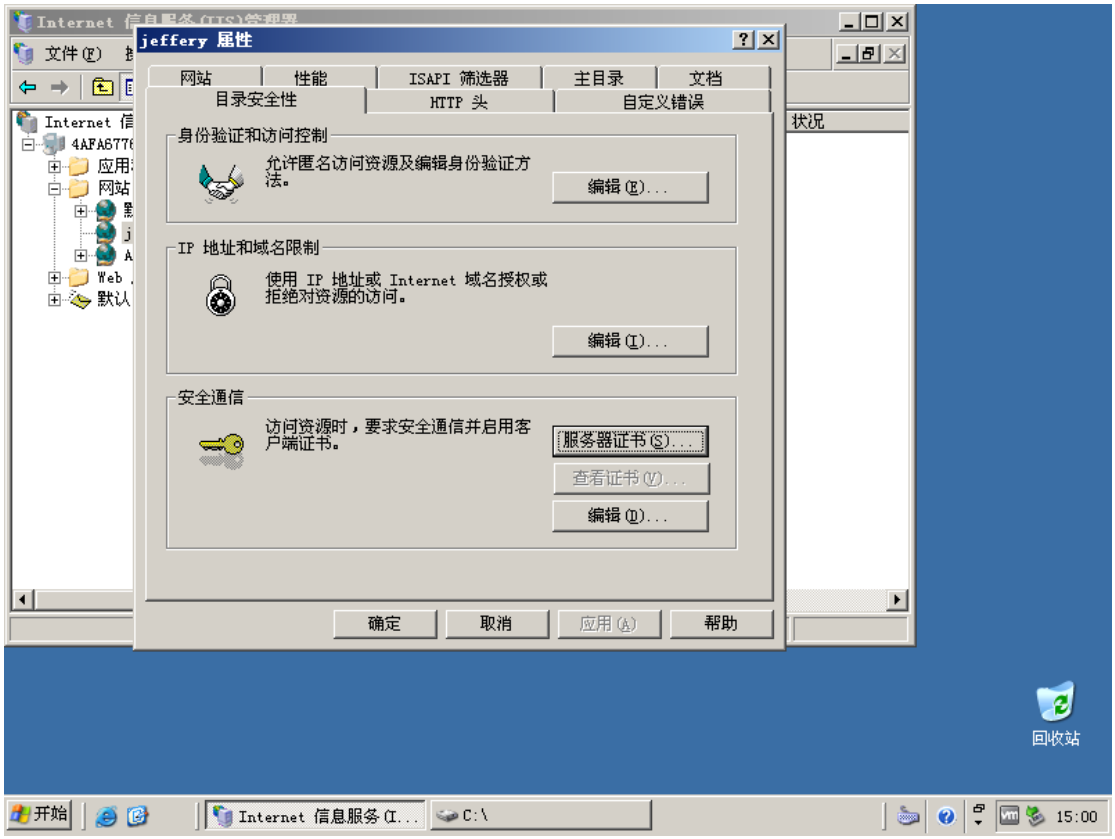


保存

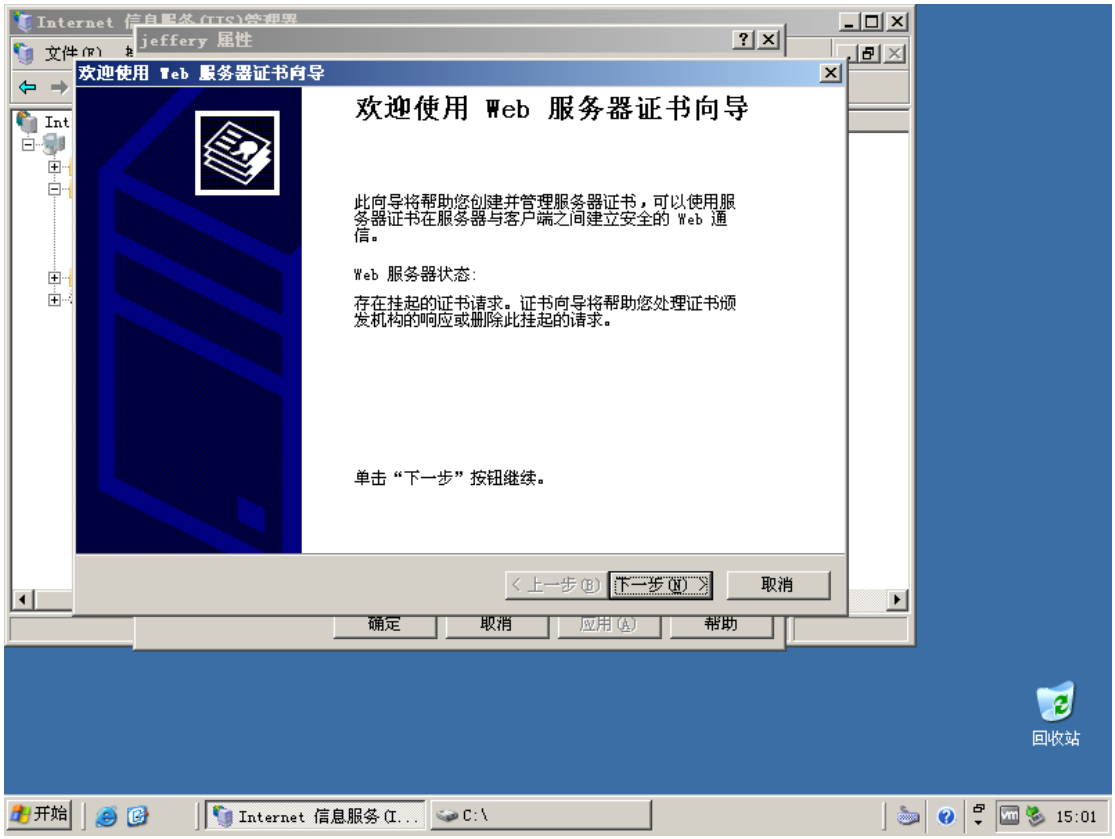


2.3.5 IIS 证书安装

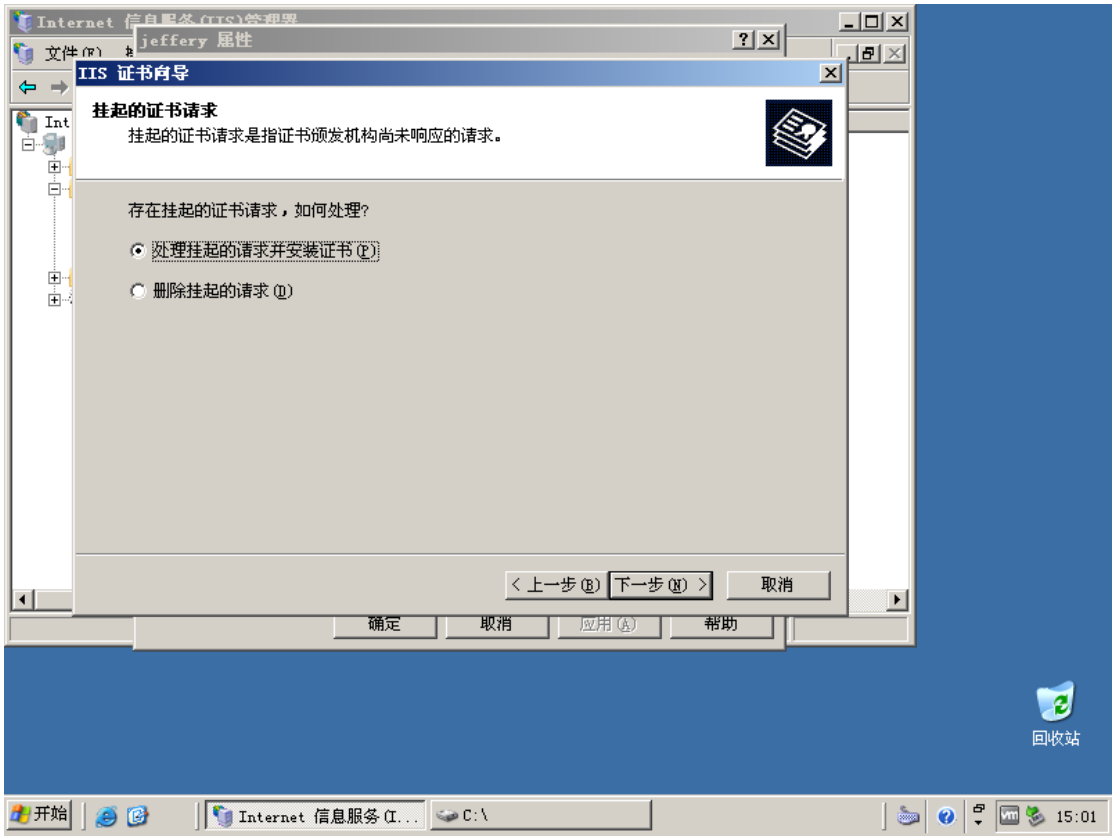
再次进入目录安全性点击服务器证书



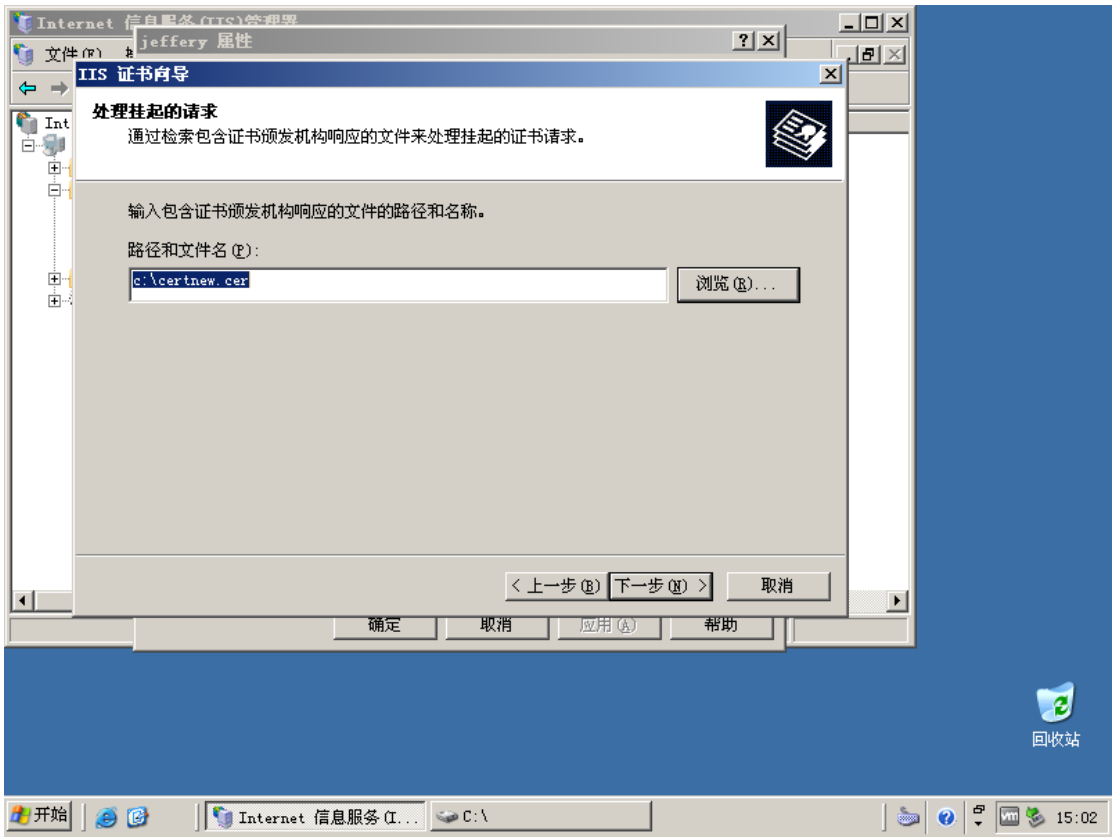
下一步



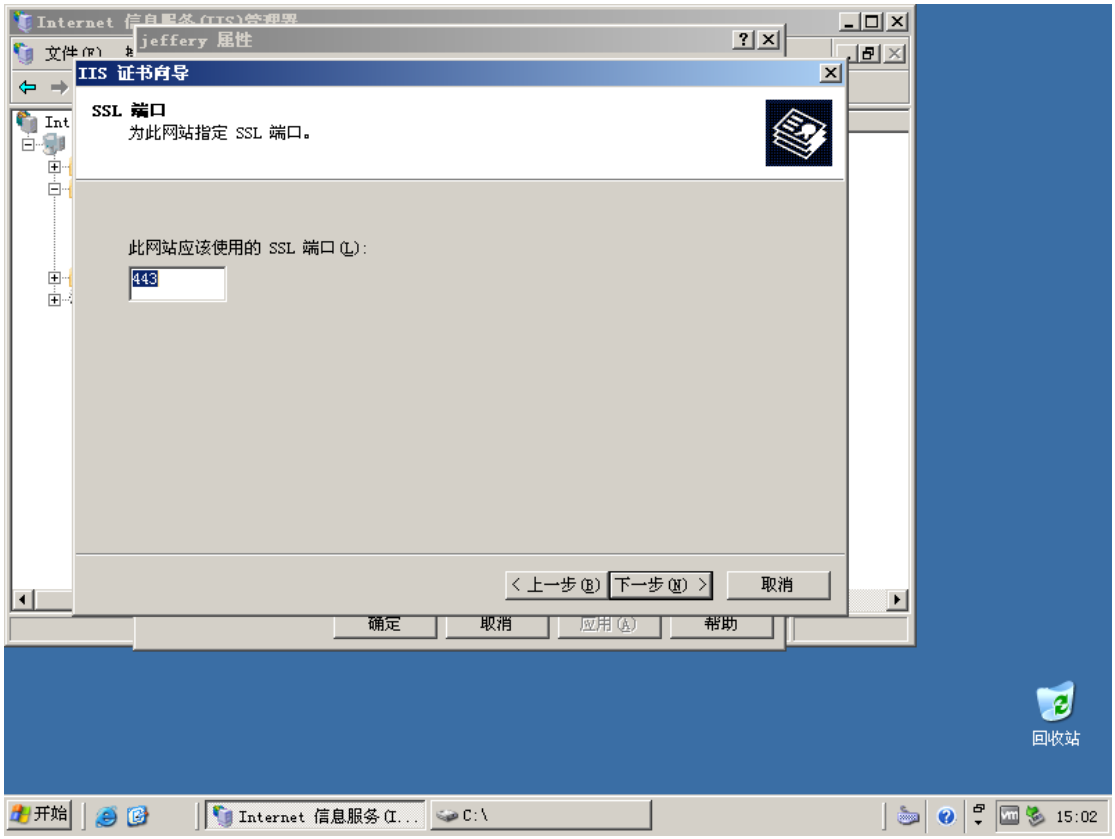
选择处理挂起的请求并安装证书，点击下一步



选择刚才下载回来的证书，点击下一步



设置默认的 SSL 端口 443

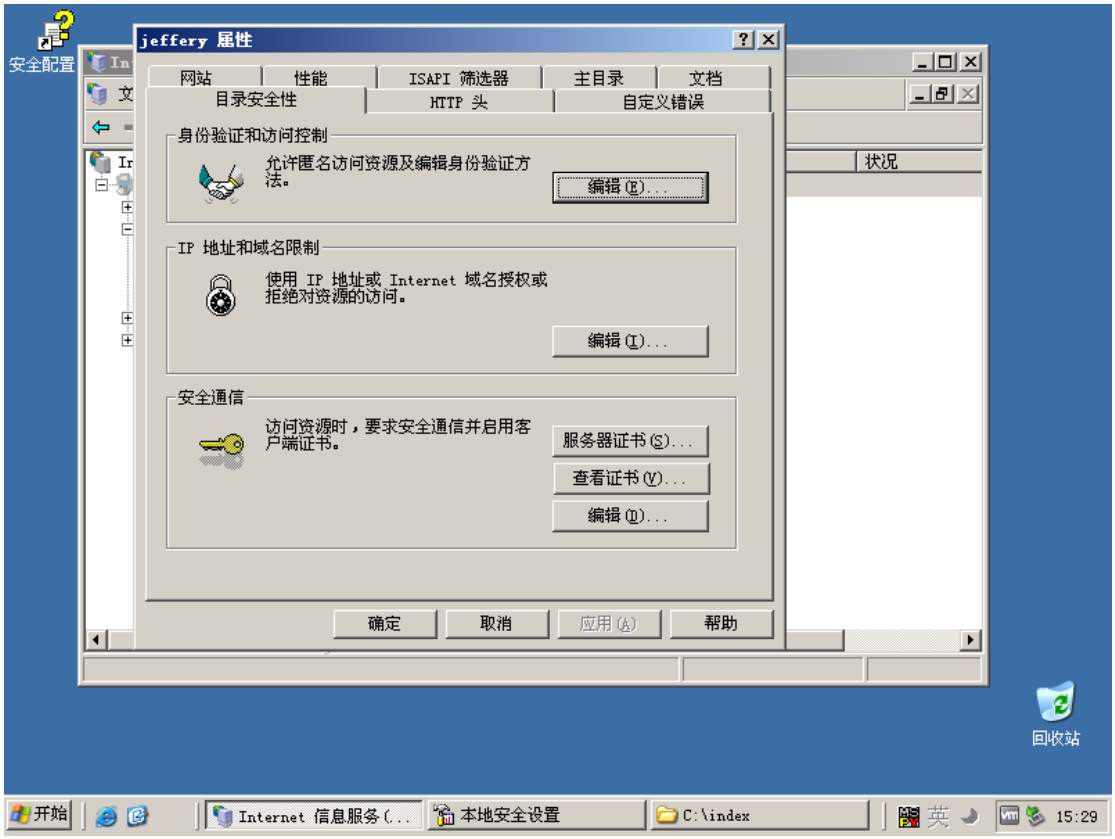

jeffery 属性
IIS 证书向导
SSL 端口
为此网站指定 SSL 端口。
此网站应该使用的 SSL 端口(L):
443
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(I...
C:\
15:02

下一步

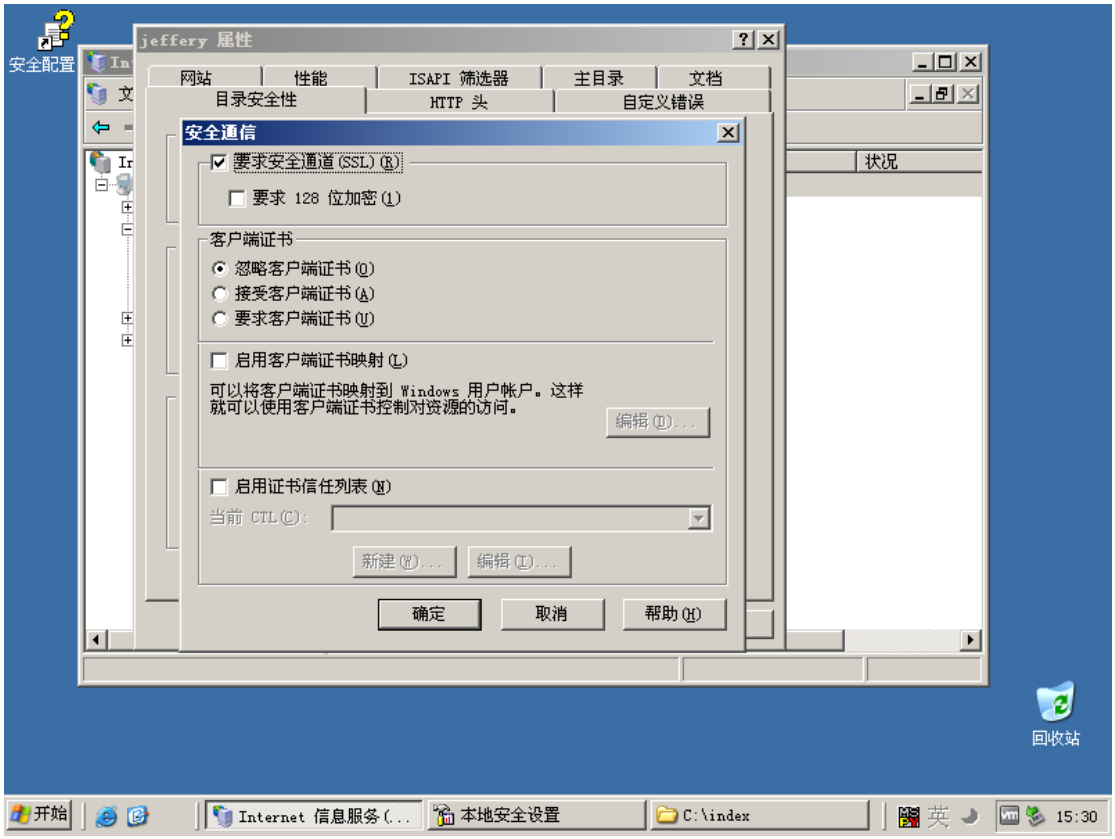

jeffery 属性
IIS 证书向导
证书摘要
已选择从响应文件安装证书。
单击“下一步”按钮安装下列证书。
文件名: c:\certnew.cer
证书详细信息:
证书颁发对象 4afa67769f8049e
证书颁发者 jeffery
过期日期 2016-12-11
用途 服务器验证
友好名称 jeffery
国家(地区) CN
省/自治区 广东
市县 广州
单位 学校
部门 宿舍
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
帮助
回收站
开始
Internet 信息服务(I...
C:\
英
15:02

完成

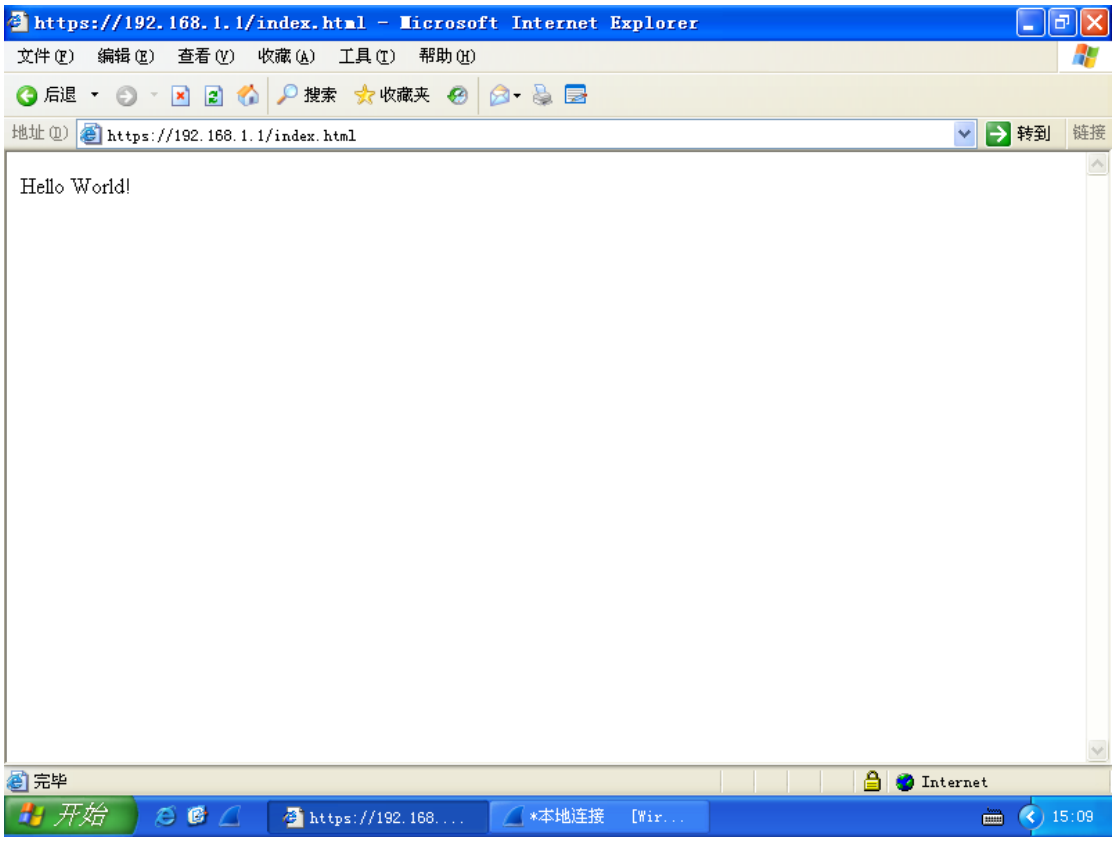
然后进入目录安全性



点击安全通讯的编辑，勾选要求安全通道

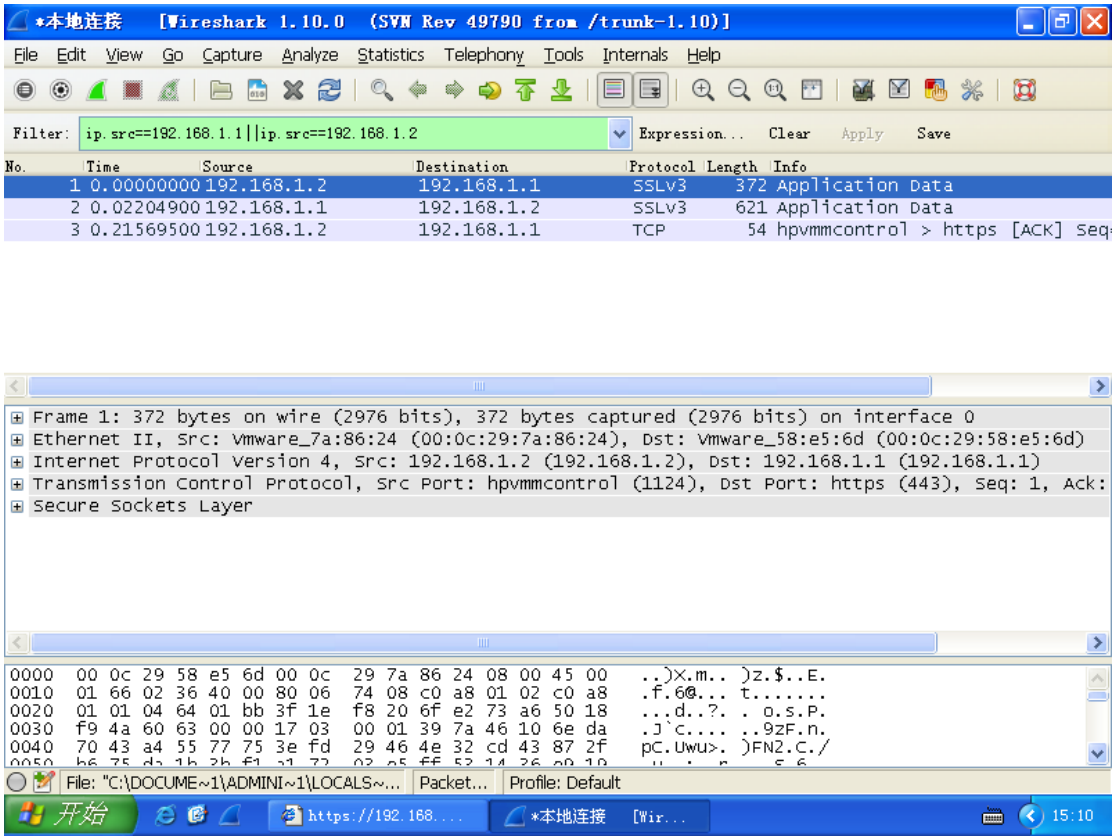


现在就可以通过 https 协议来访问了

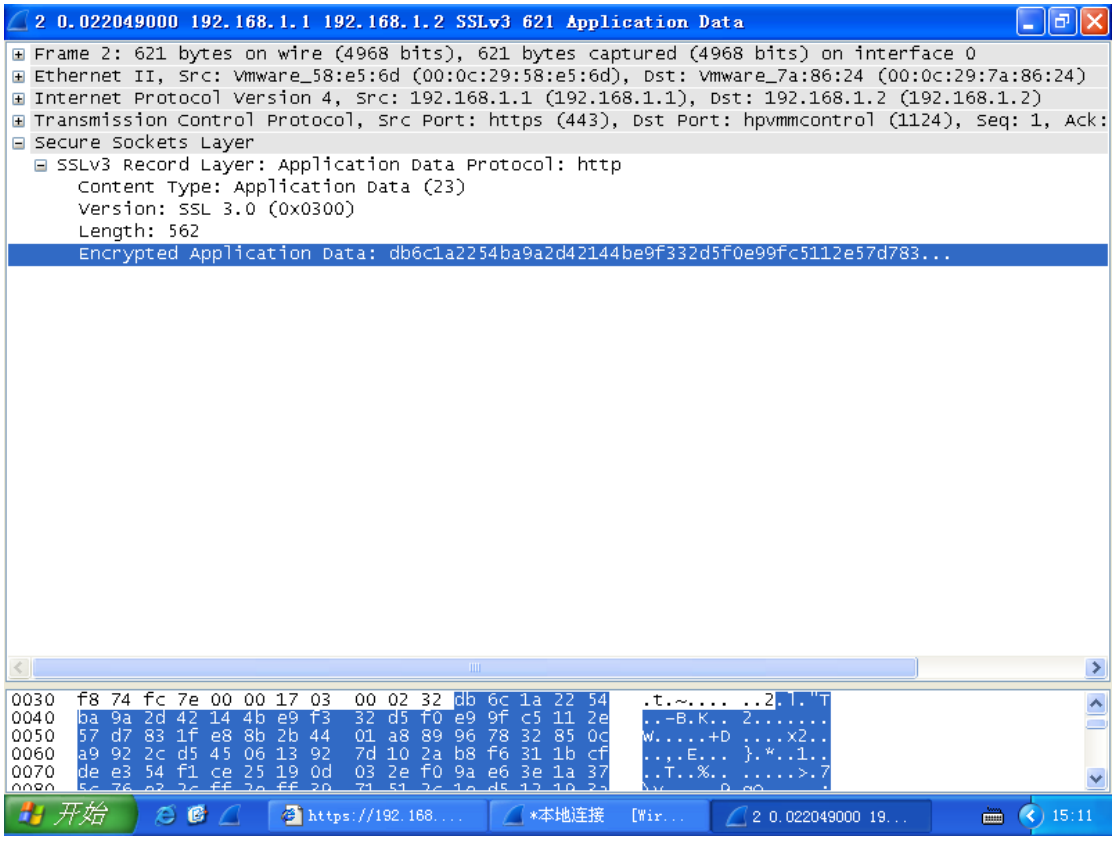


2.4 启用 SSL 情况下抓包效果

现在来抓一下包，可发现客户端发过去的请求和发回来的数据都使用了 ssl 协议加密了



可看到数据都被加密了



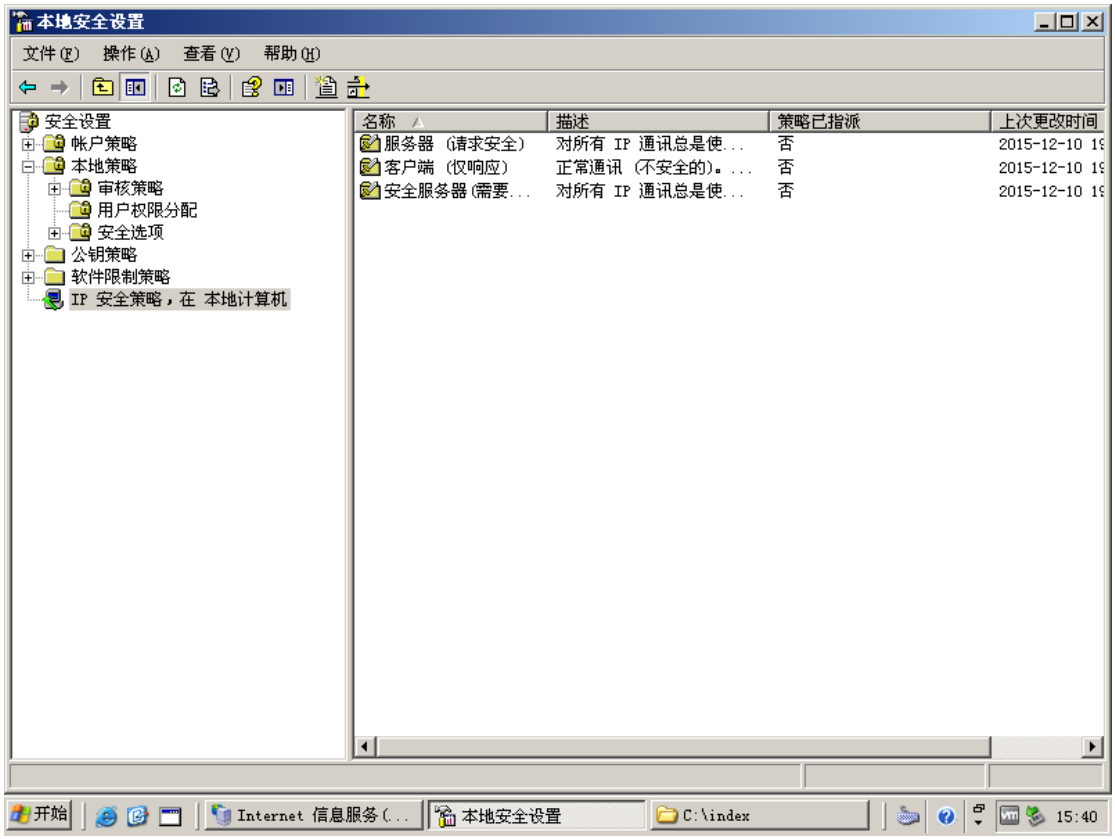
以上就是用 SSL 协议对使用 http 协议传输的数据进行加密的过程。

3 IPSec 的设置：

（目标是使客户端不能够用 TCP 协议访问服务器的 8888 端口）

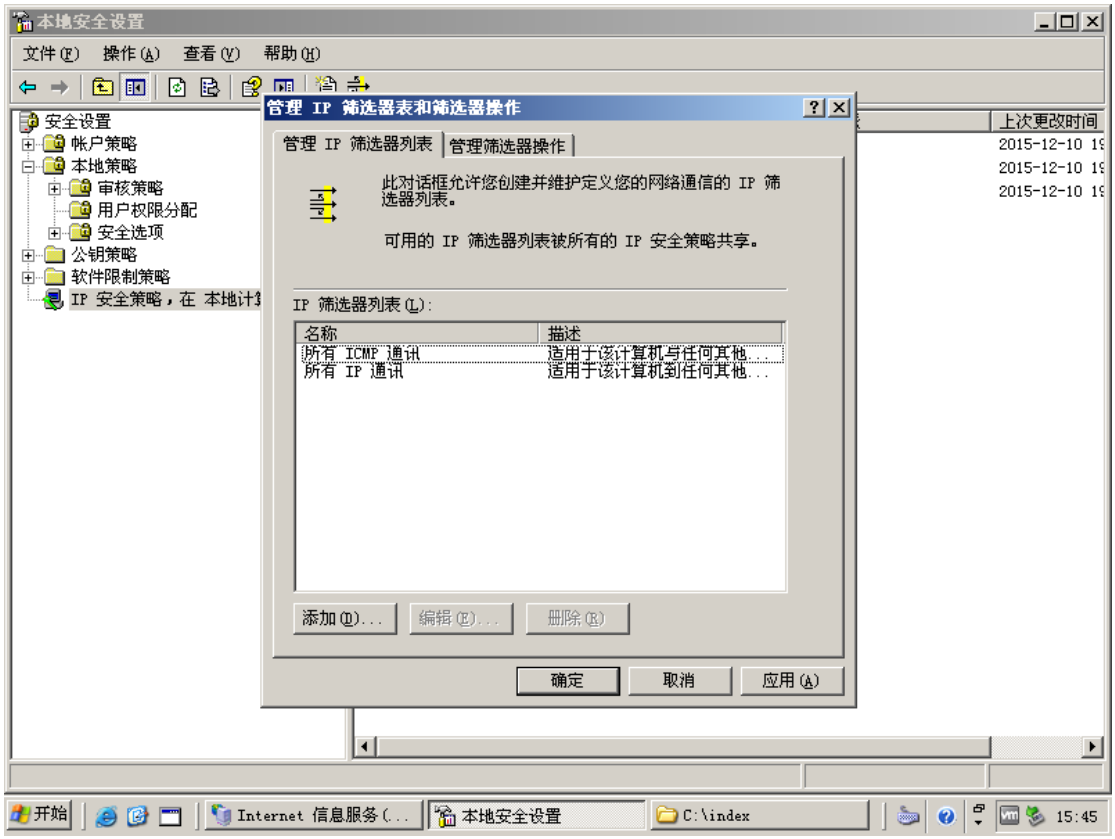
3.1 创建 IPSec 规则

打开服务器的本地安全设置

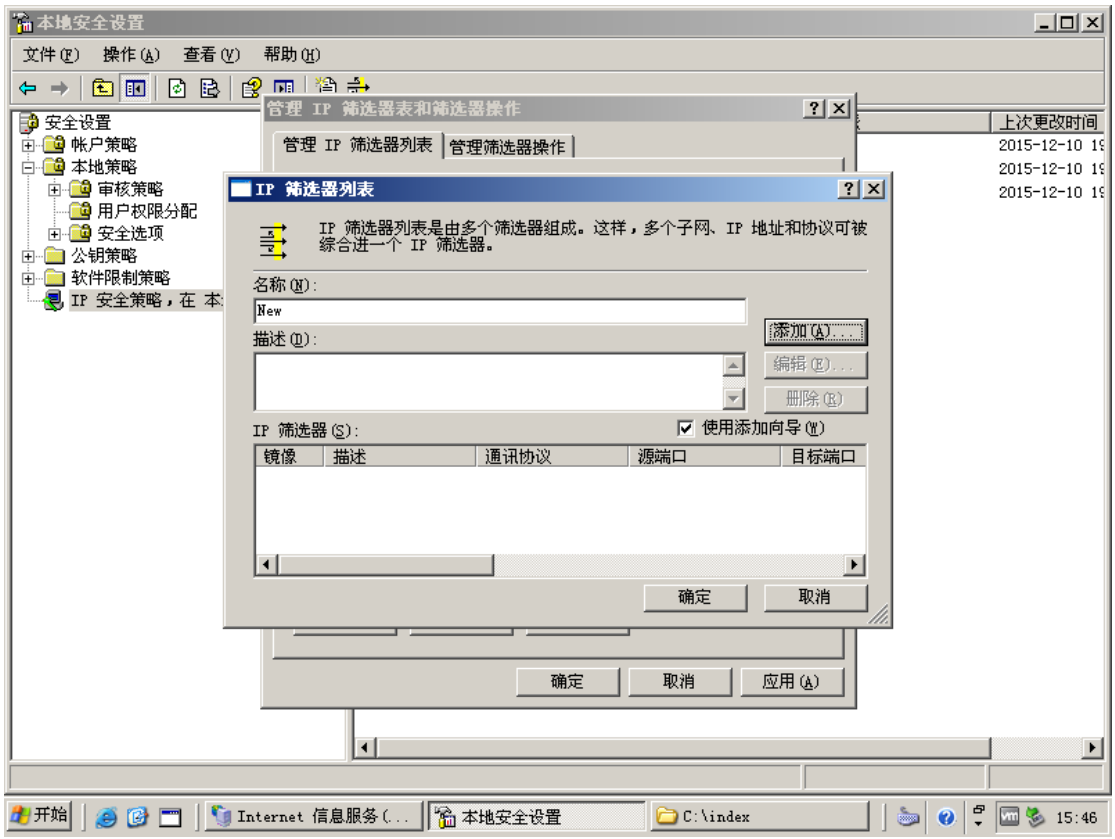


右键，点击管理 IP 筛选表和筛选器操作

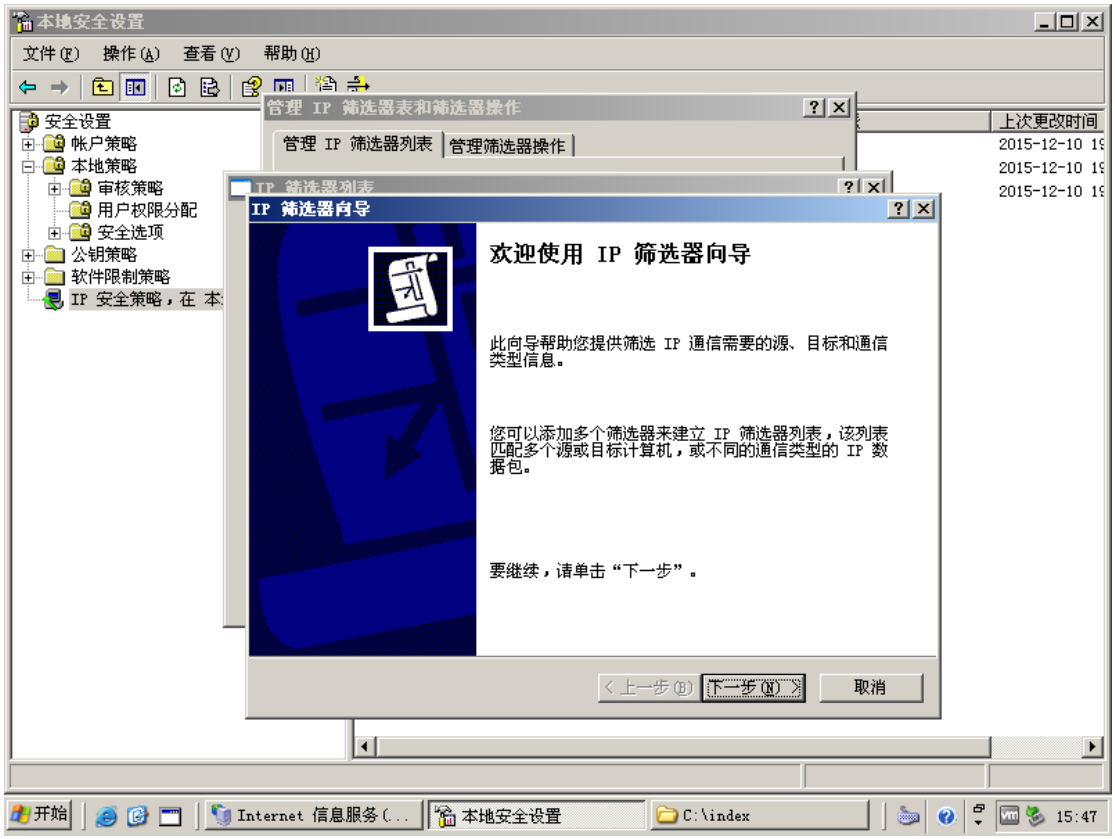
点击添加



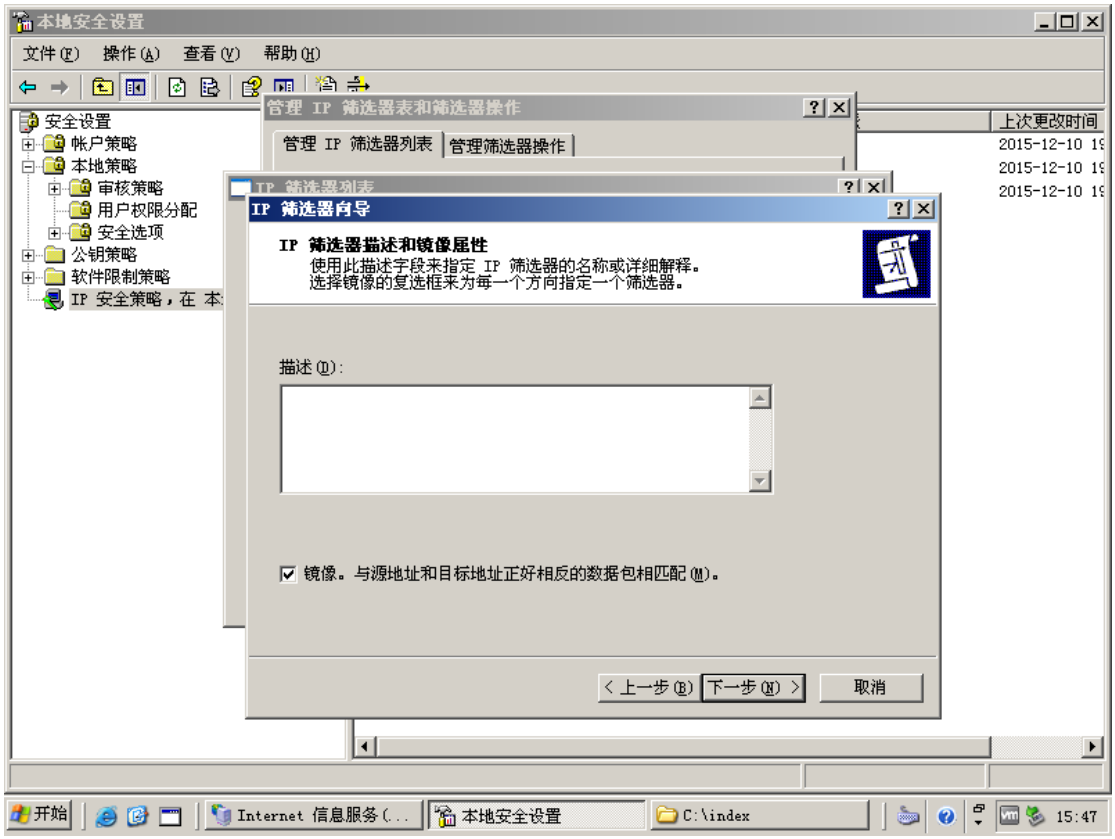
输入名称



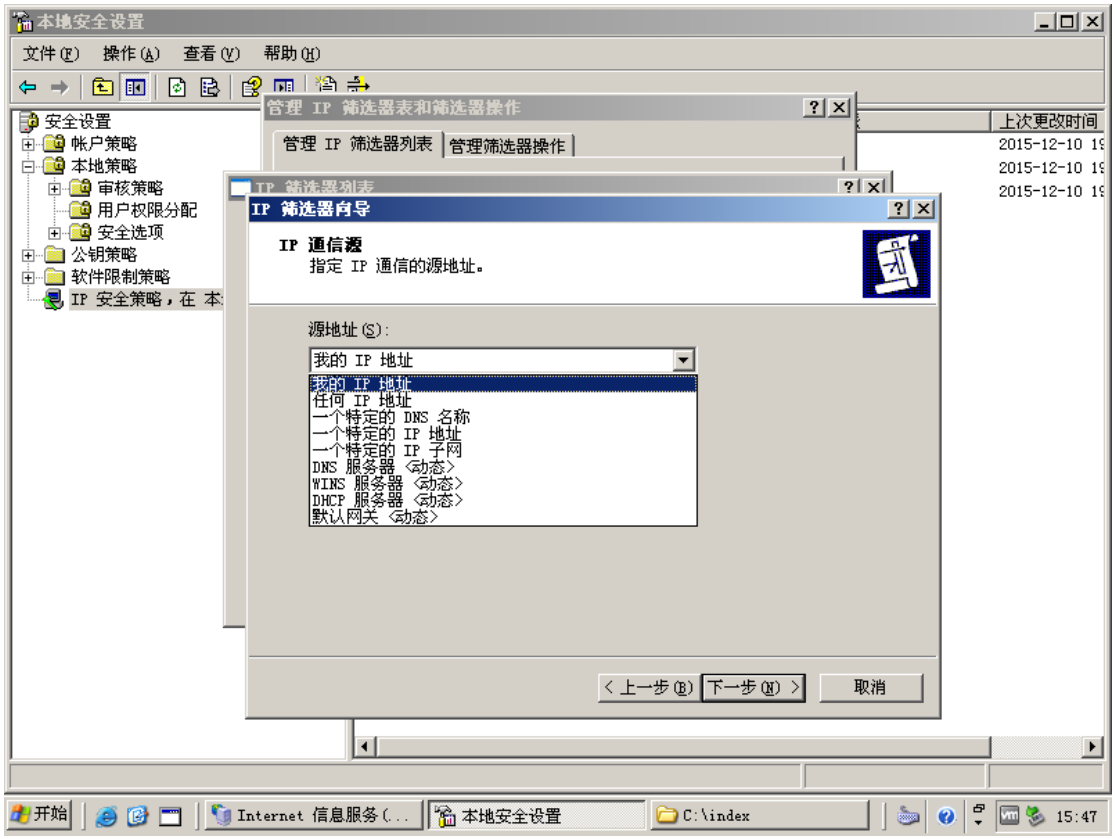
点击添加，下一步



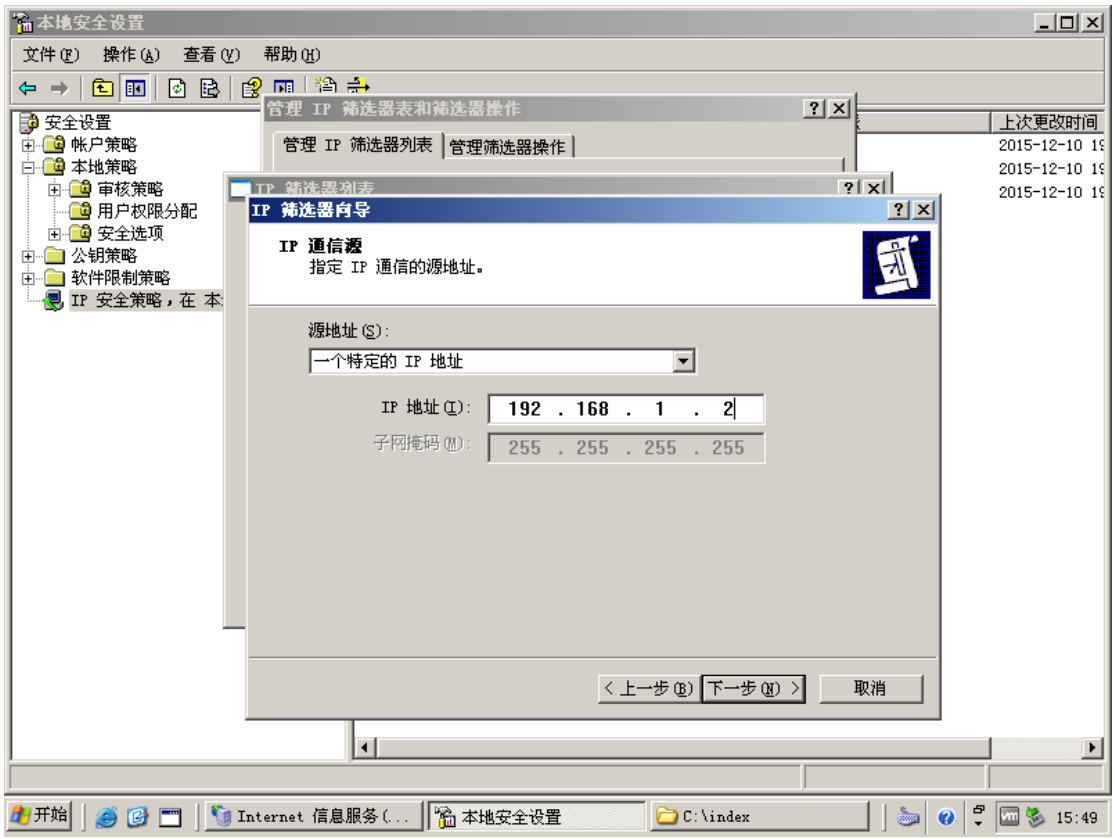
下一步



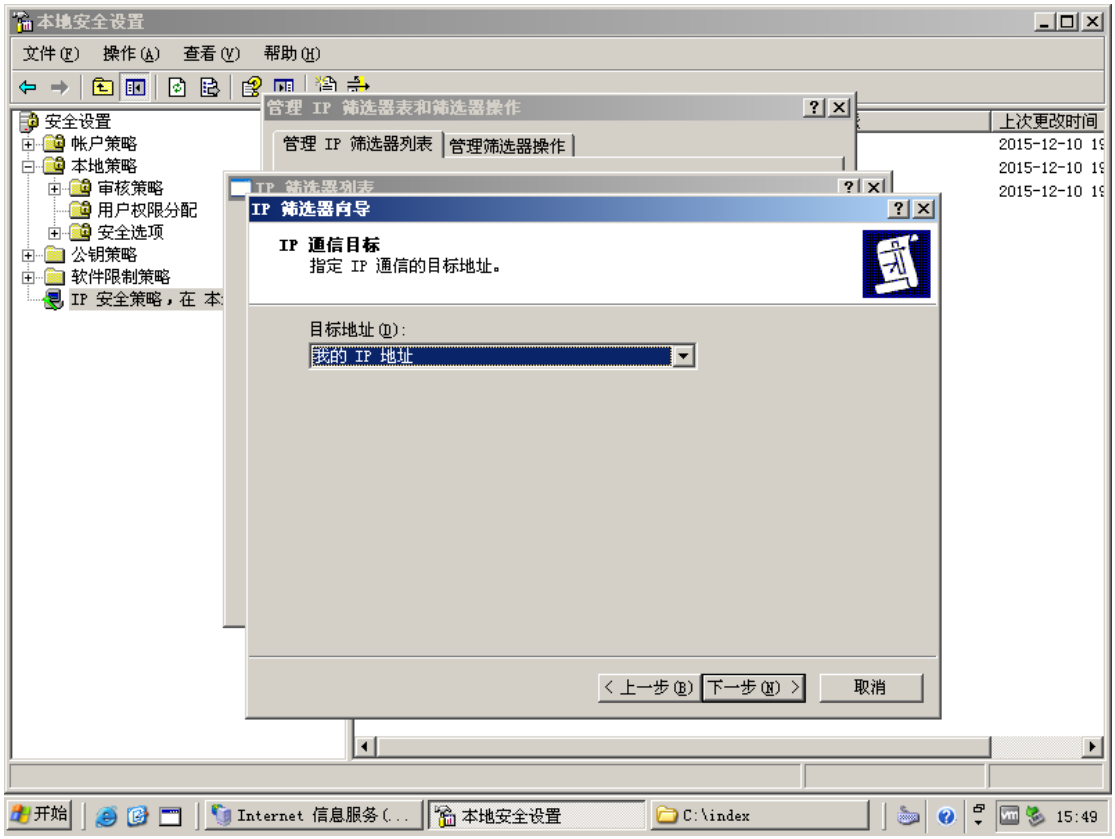
从源地址选择一个特定的 IP 地址



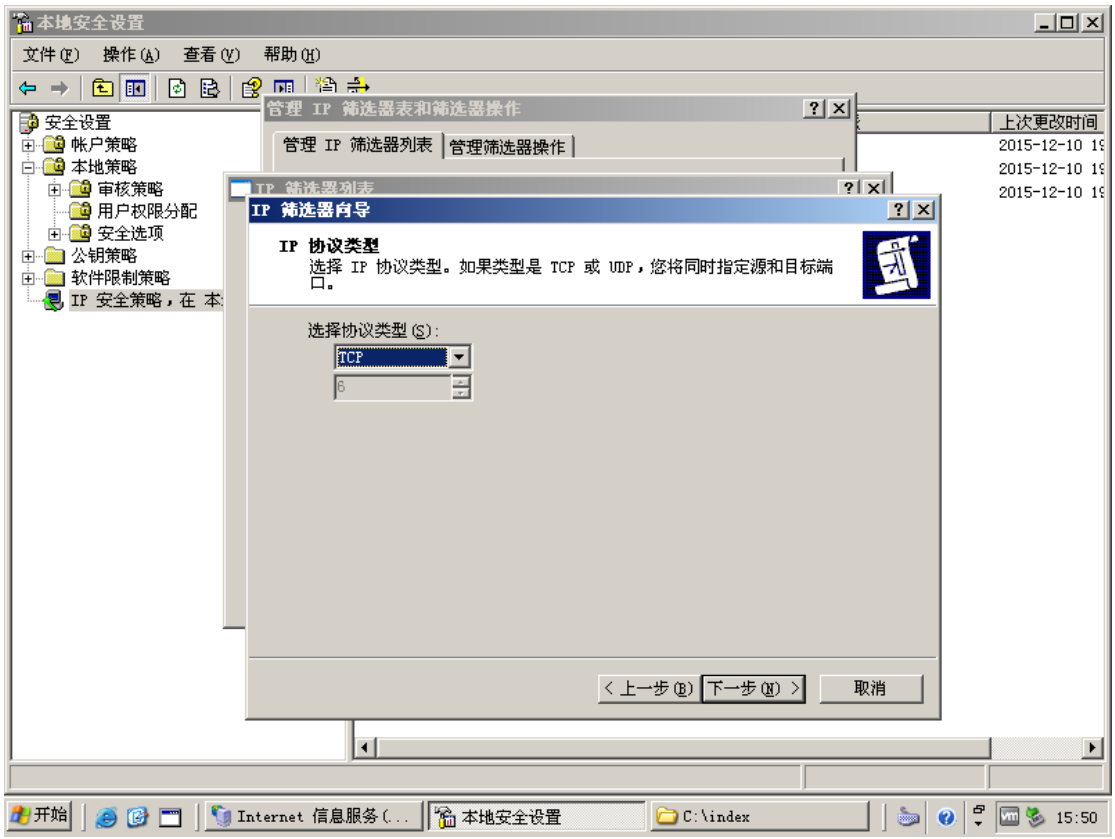
输入客户端的 IP 地址



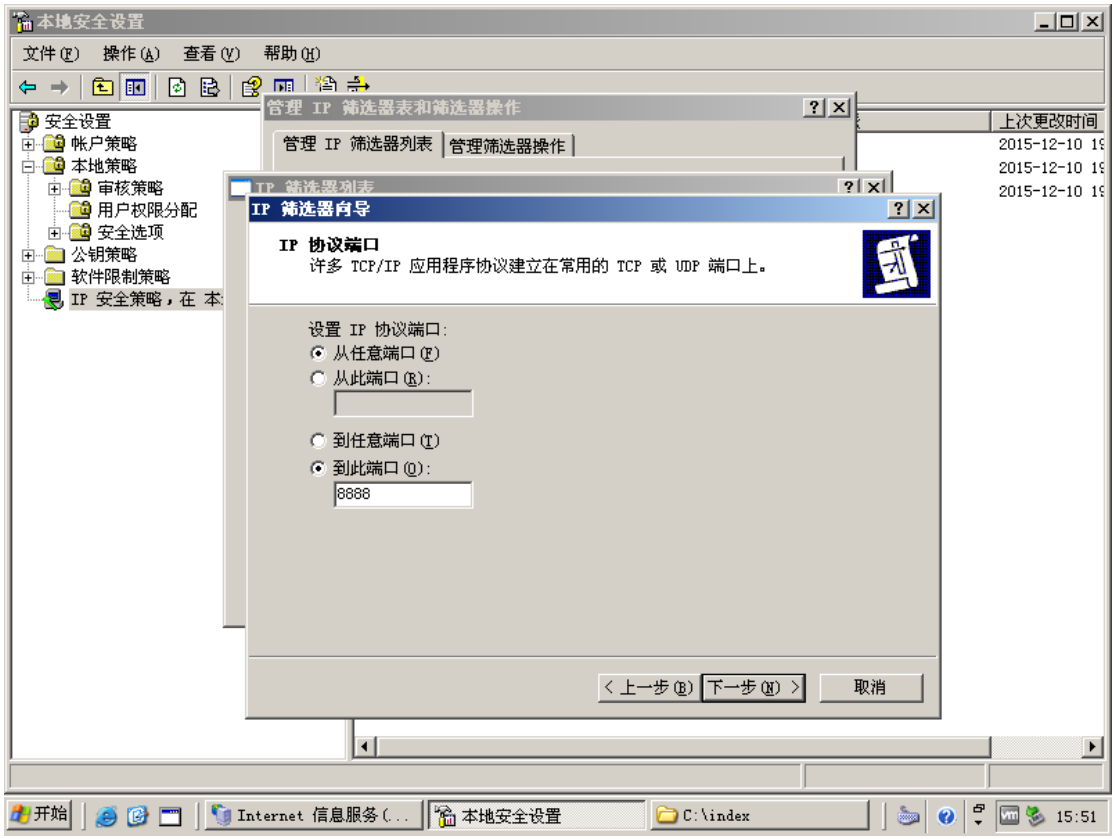
目标地址设为我的 IP 地址（也就是服务器的地址），点击下一步



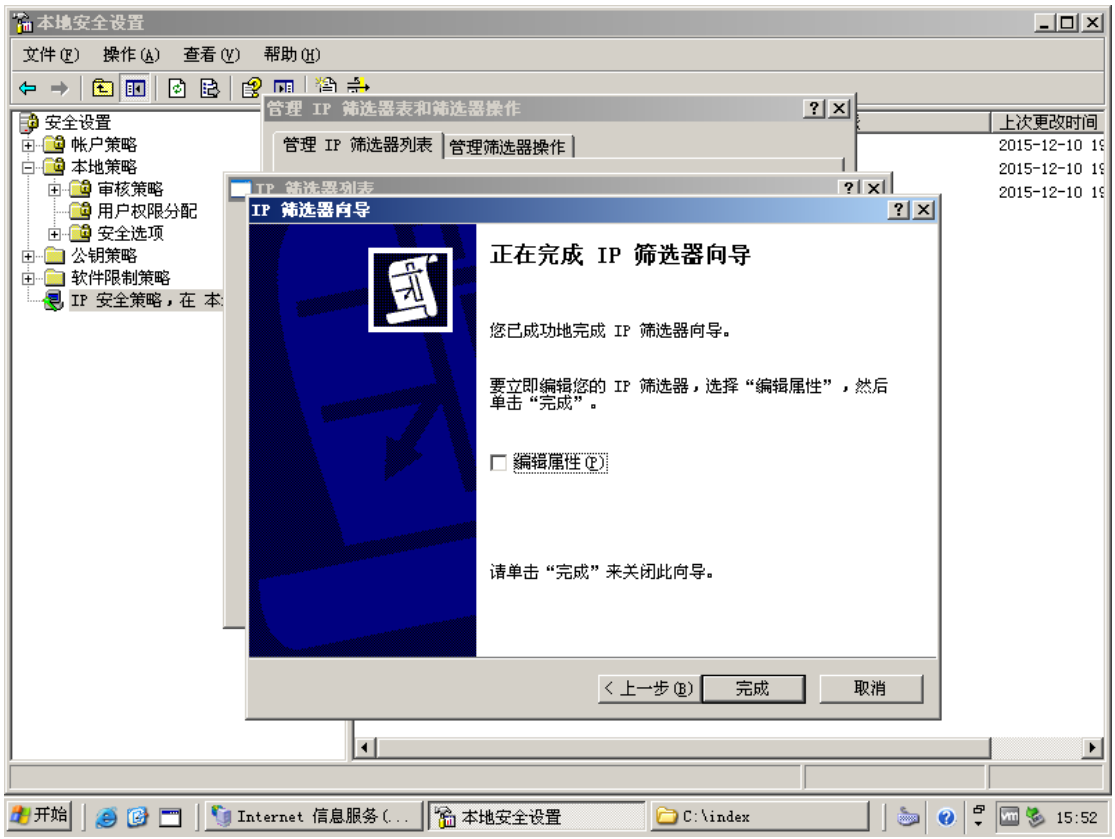
选择 TCP 协议，点击下一步



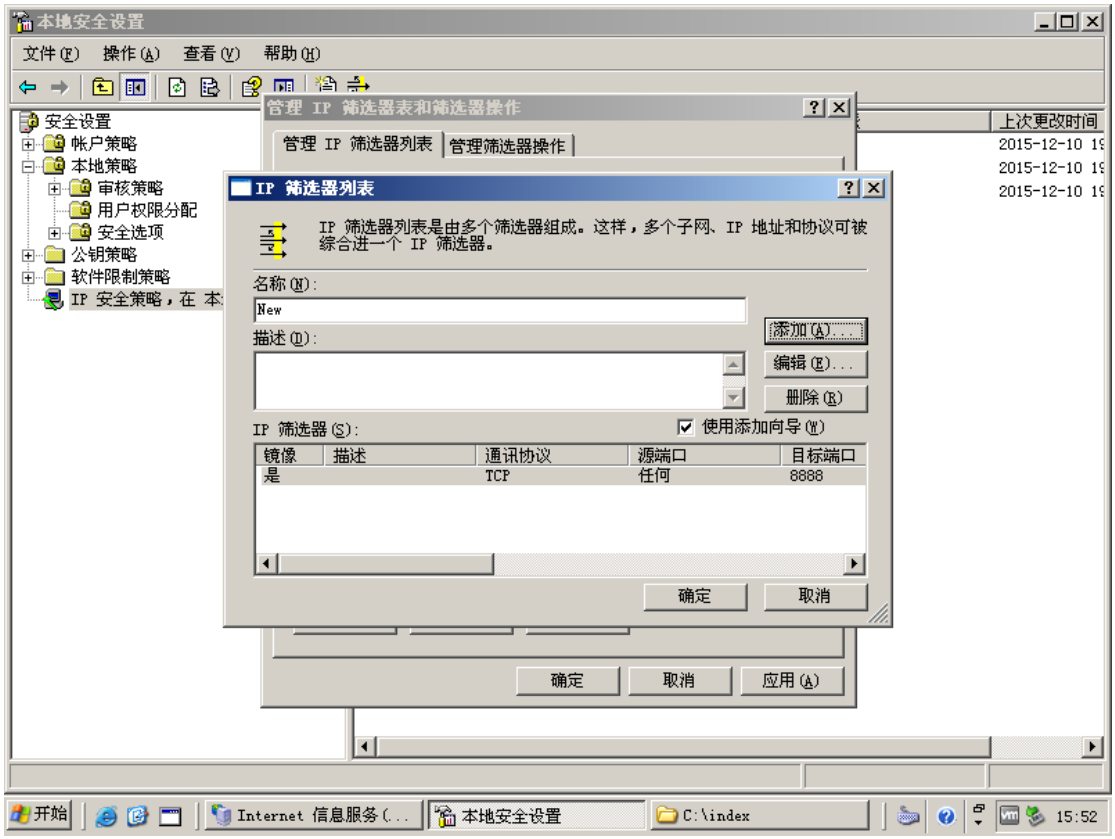
设置从任意端口到 8888 端口，点击下一步


本地安全设置
文件(F)　操作(A)　查看(V)　帮助(H)
管理 IP 筛选器表和筛选器操作
管理 IP 筛选器列表
管理筛选器操作
IP 筛选器列表
IP 筛选器向导
IP 协议端口
许多 TCP/IP 应用程序协议建立在常用的 TCP 或 UDP 端口上。
设置 IP 协议端口:
从任意端口(F)
从此端口(R):
到任意端口(T)
到此端口(O):
8888
< 上一步(B)
下一步(N) >
取消
安全设置
帐户策略
本地策略
审核策略
用户权限分配
安全选项
公钥策略
软件限制策略
IP 安全策略，在 本
上次更改时间
2015-12-10 19
2015-12-10 19
2015-12-10 19
开始
Internet 信息服务(...
本地安全设置
C:\index
15:51

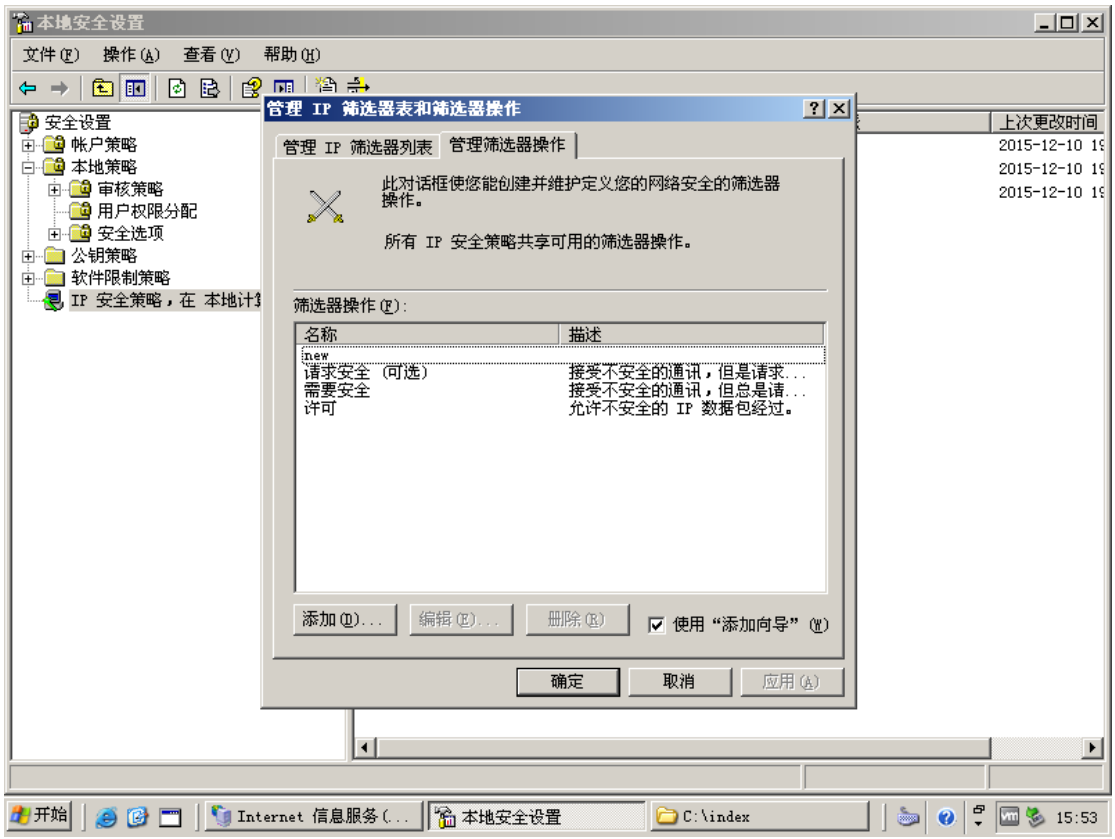
完成


本地安全设置
文件(F)　操作(A)　查看(V)　帮助(H)
管理 IP 筛选器表和筛选器操作
管理 IP 筛选器列表
管理筛选器操作
IP 筛选器列表
IP 筛选器向导
正在完成 IP 筛选器向导
您已成功地完成 IP 筛选器向导。
要立即编辑您的 IP 筛选器，选择“编辑属性”，然后单击“完成”。
编辑属性(E)
请单击“完成”来关闭此向导。
< 上一步(B)
完成
取消
安全设置
帐户策略
本地策略
审核策略
用户权限分配
安全选项
公钥策略
软件限制策略
IP 安全策略，在 本
上次更改时间
2015-12-10 19
2015-12-10 19
2015-12-10 19
开始
Internet 信息服务(...
本地安全设置
C:\index
15:52

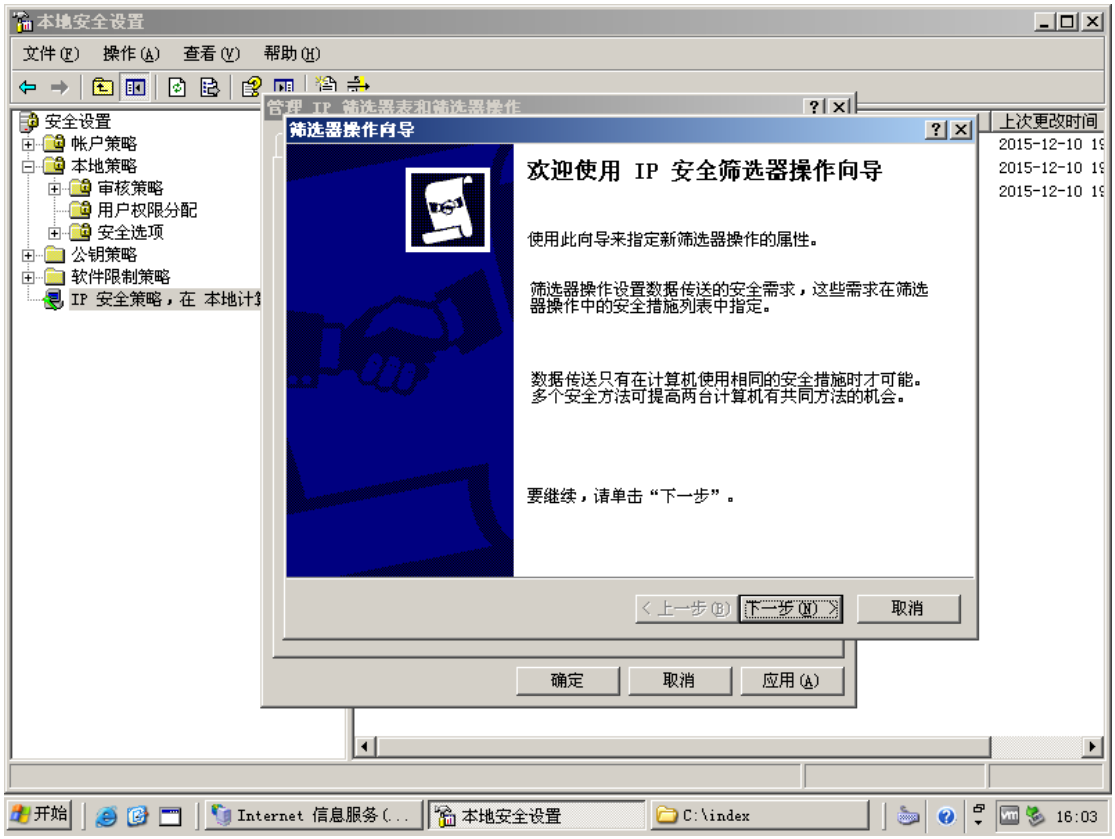
确认



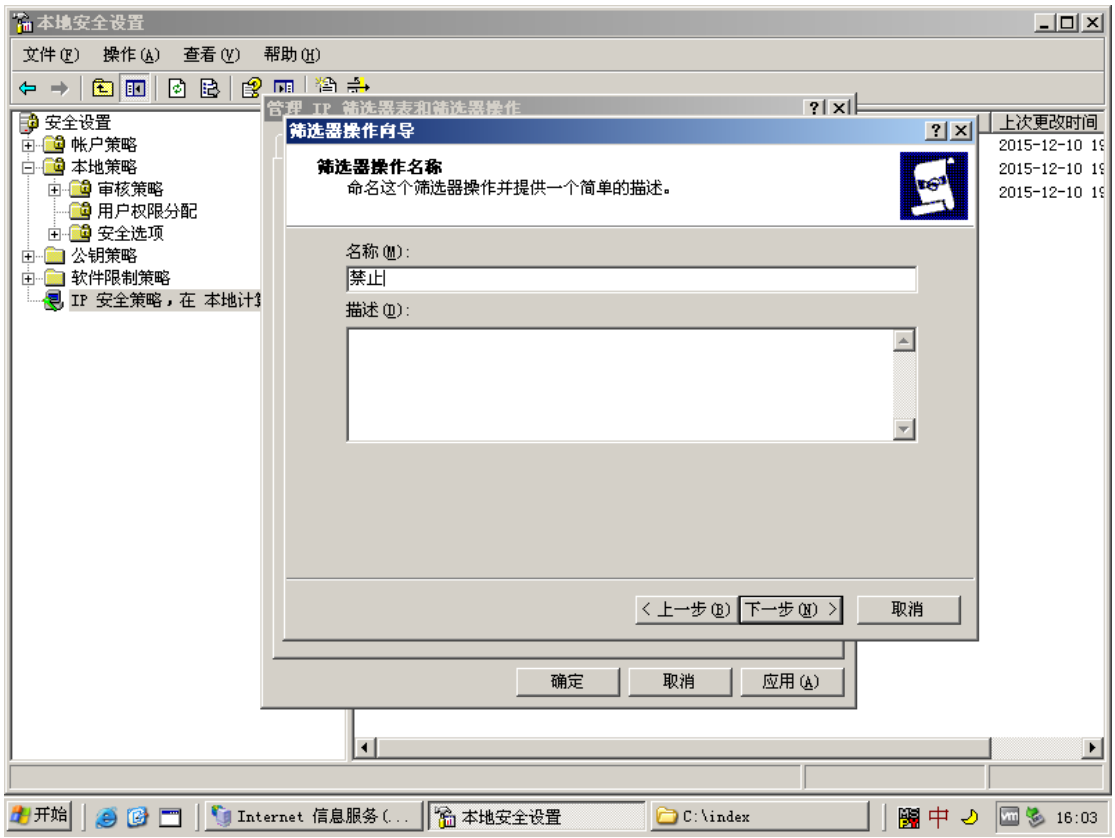
切换到管理筛选器操作，因为创建了 IP 筛选器，还需要设置是禁止还是允许，点击添加



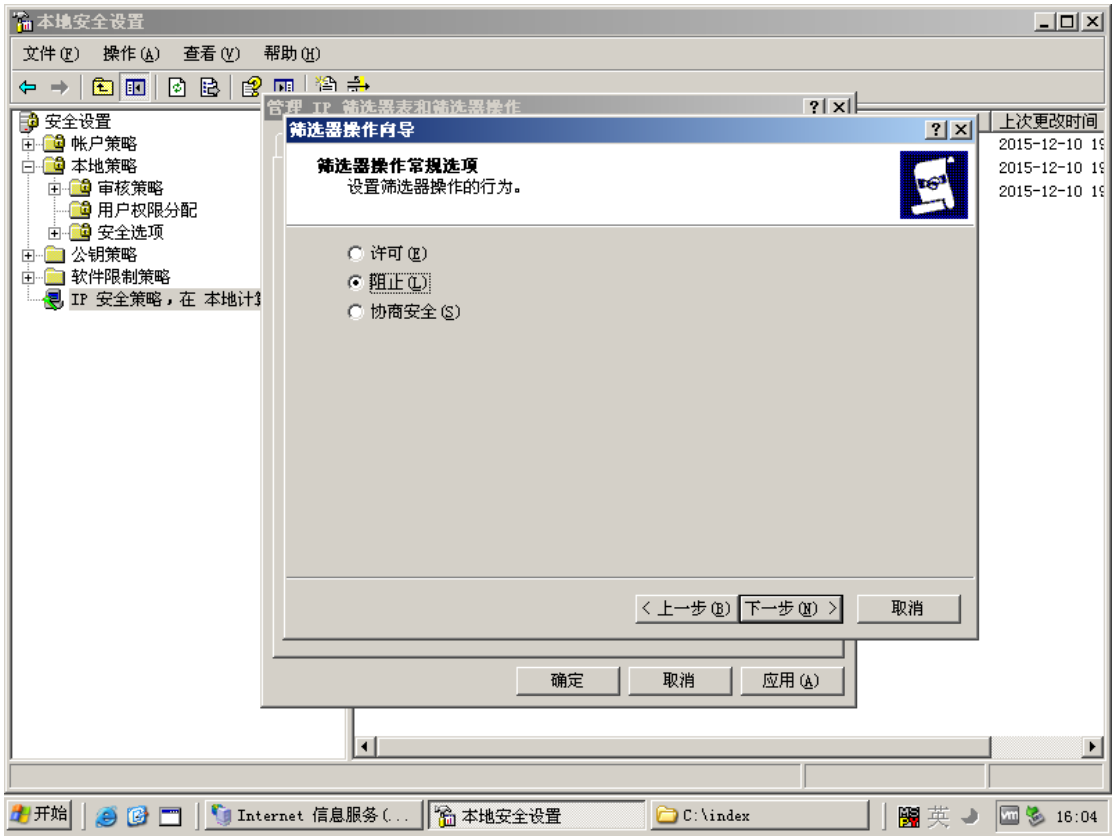
下一步



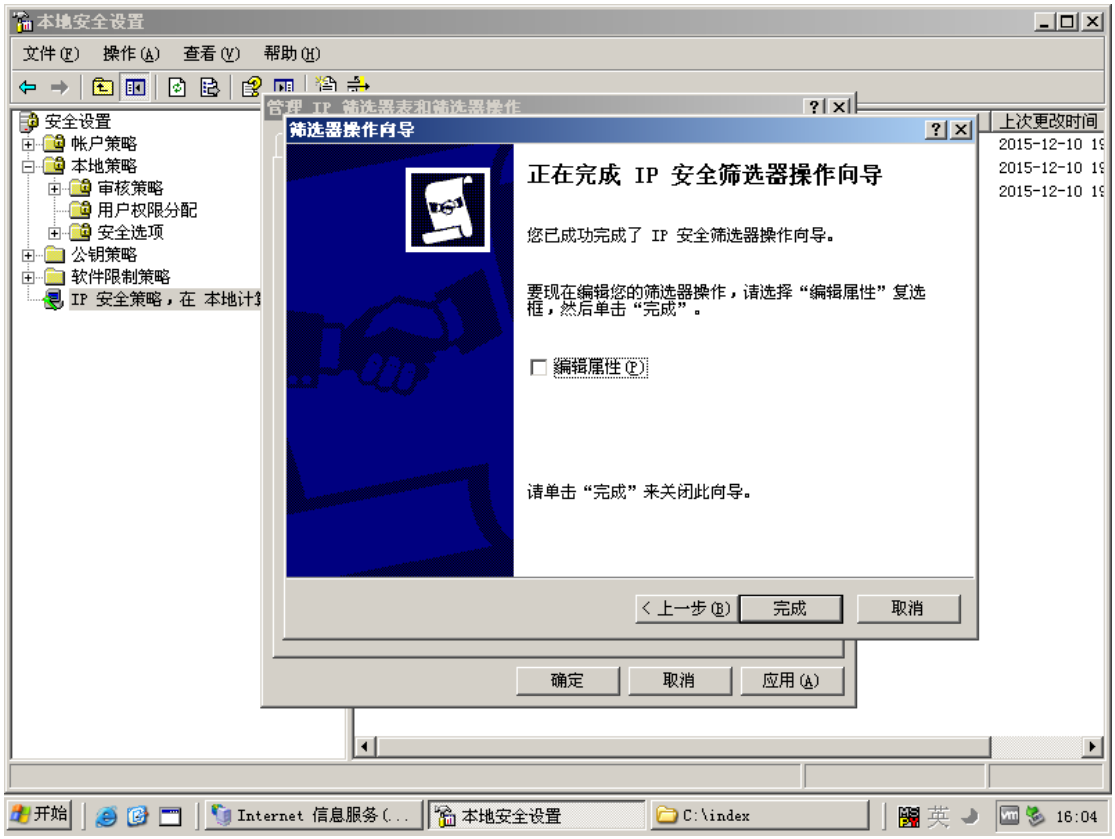
输入名称，点击下一步



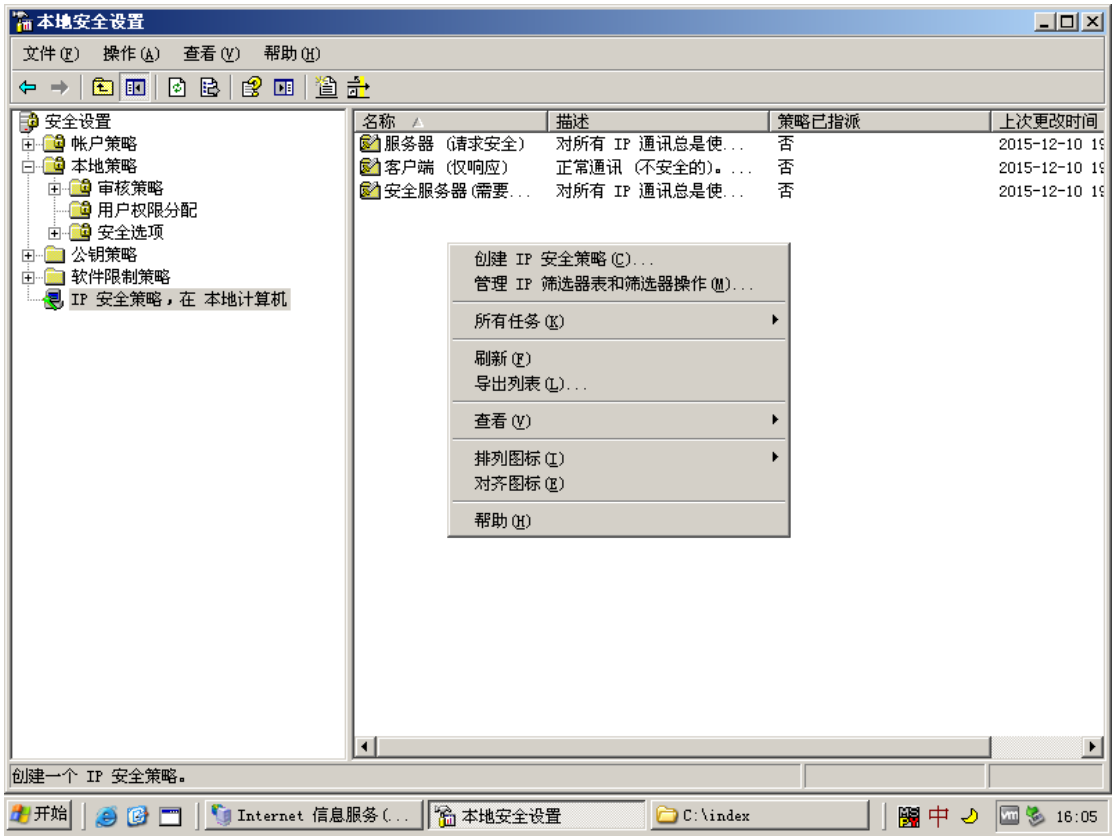
选择阻止，点击下一步



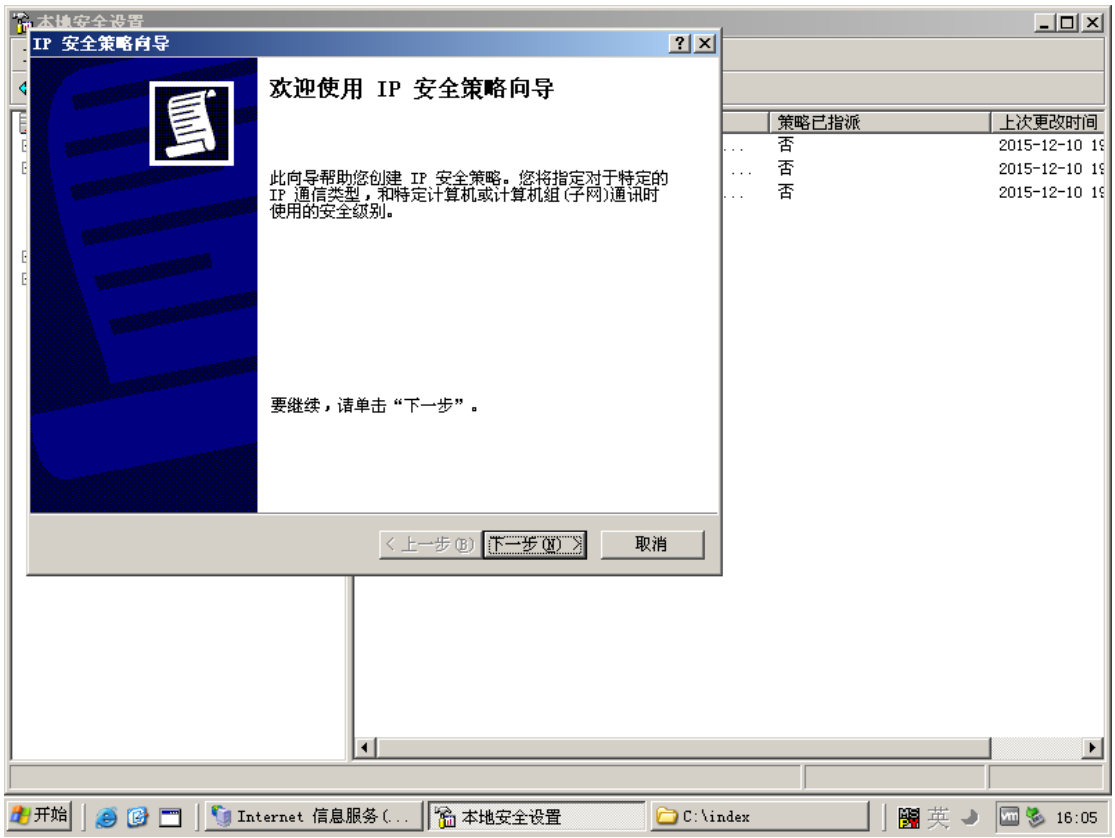
完成



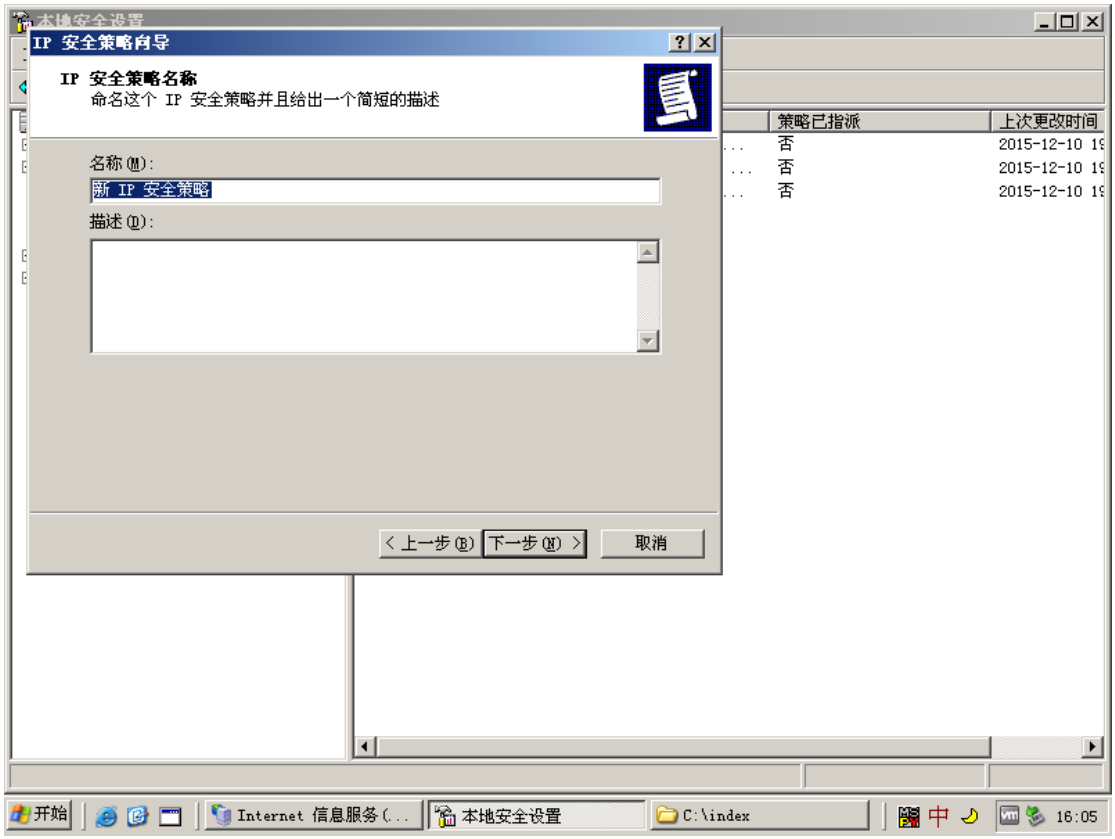
然后右键创建 IP 安全策略


本地安全设置
文件(F)　操作(A)　查看(V)　帮助(H)
安全设置
帐户策略
本地策略
审核策略
用户权限分配
安全选项
公钥策略
软件限制策略
IP 安全策略，在 本地计算机
名称
描述
策略已指派
上次更改时间
服务器 (请求安全)　对所有 IP 通讯总是使...　否　2015-12-10 19
客户端 (仅响应)　正常通讯 (不安全的)。...　否　2015-12-10 19
安全服务器(需要...　对所有 IP 通讯总是使...　否　2015-12-10 19
创建 IP 安全策略(C)...
管理 IP 筛选器表和筛选器操作(M)...
所有任务(K)
刷新(F)
导出列表(L)...
查看(V)
排列图标(I)
对齐图标(E)
帮助(H)
创建一个 IP 安全策略。
开始
Internet 信息服务(...
本地安全设置
C:\index
16:05

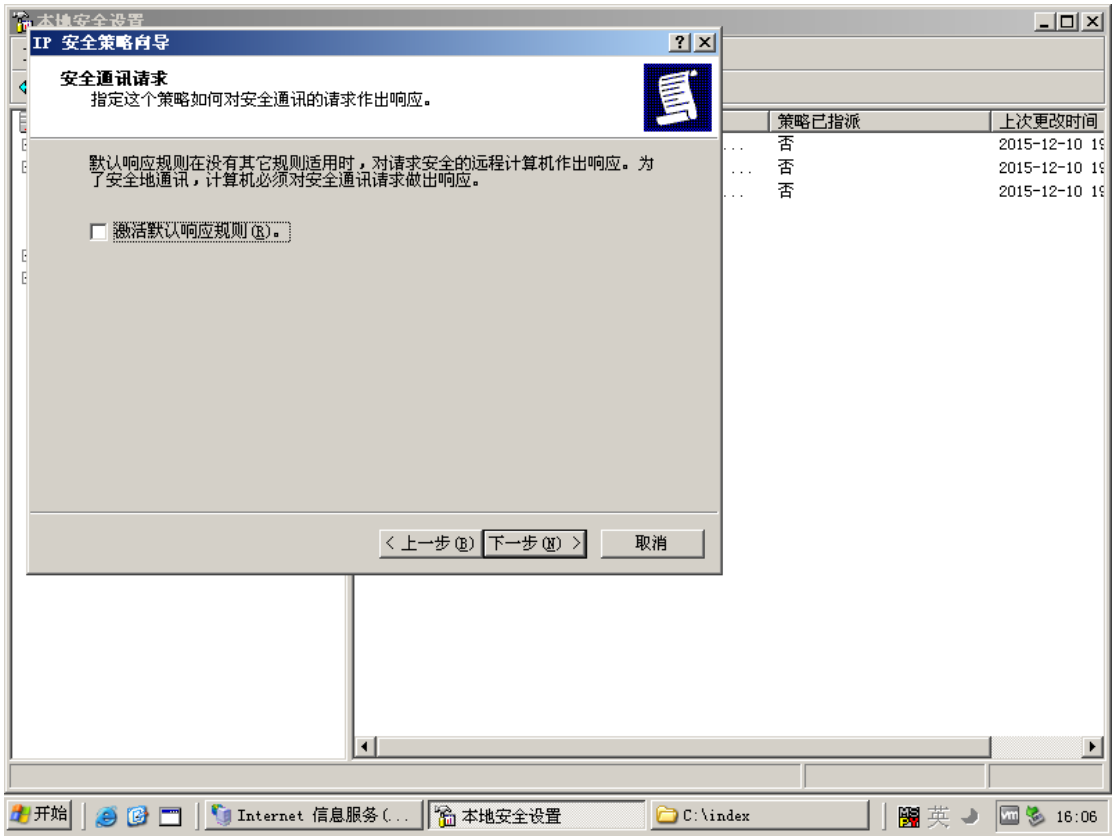
下一步


IP 安全策略向导
欢迎使用 IP 安全策略向导
此向导帮助您创建 IP 安全策略。您将指定对于特定的 IP 通信类型，和特定计算机或计算机组(子网)通讯时使用的安全级别。
要继续，请单击“下一步”。
< 上一步(B)
下一步(N) >
取消
策略已指派
上次更改时间
否　2015-12-10 19
否　2015-12-10 19
否　2015-12-10 19
开始
Internet 信息服务(...
本地安全设置
C:\index
16:05

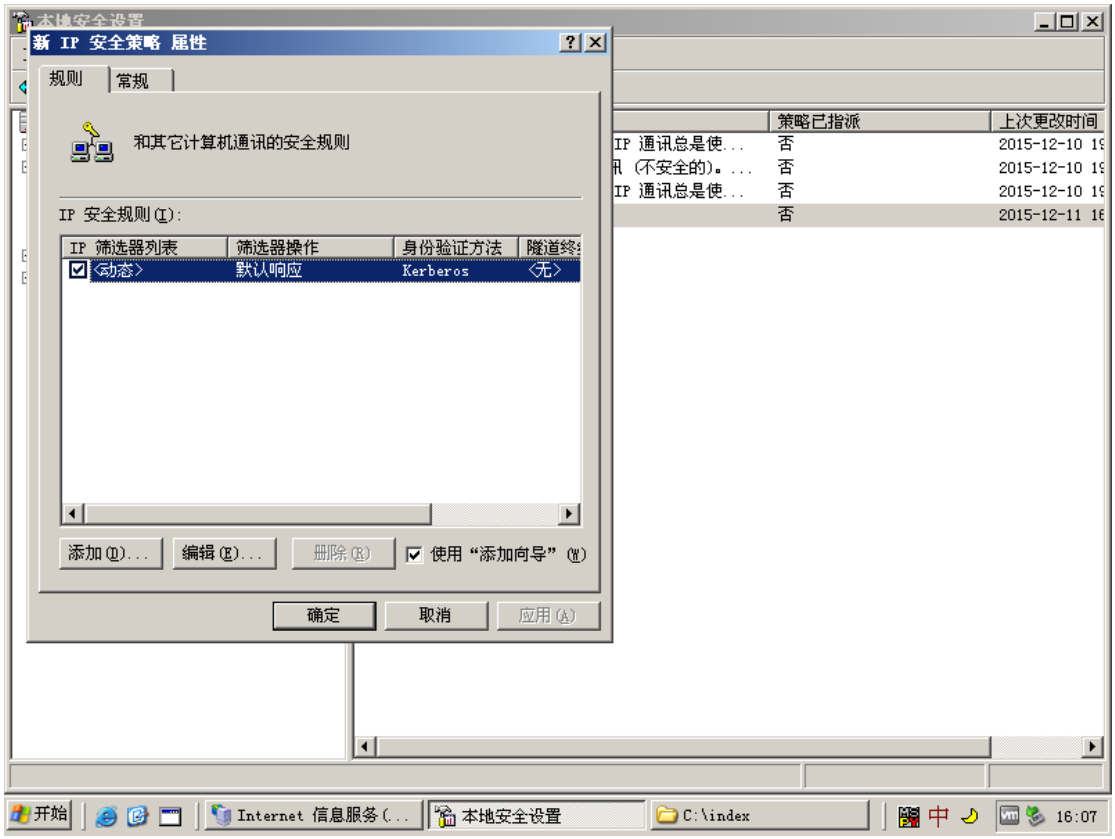
输入名称，下一步



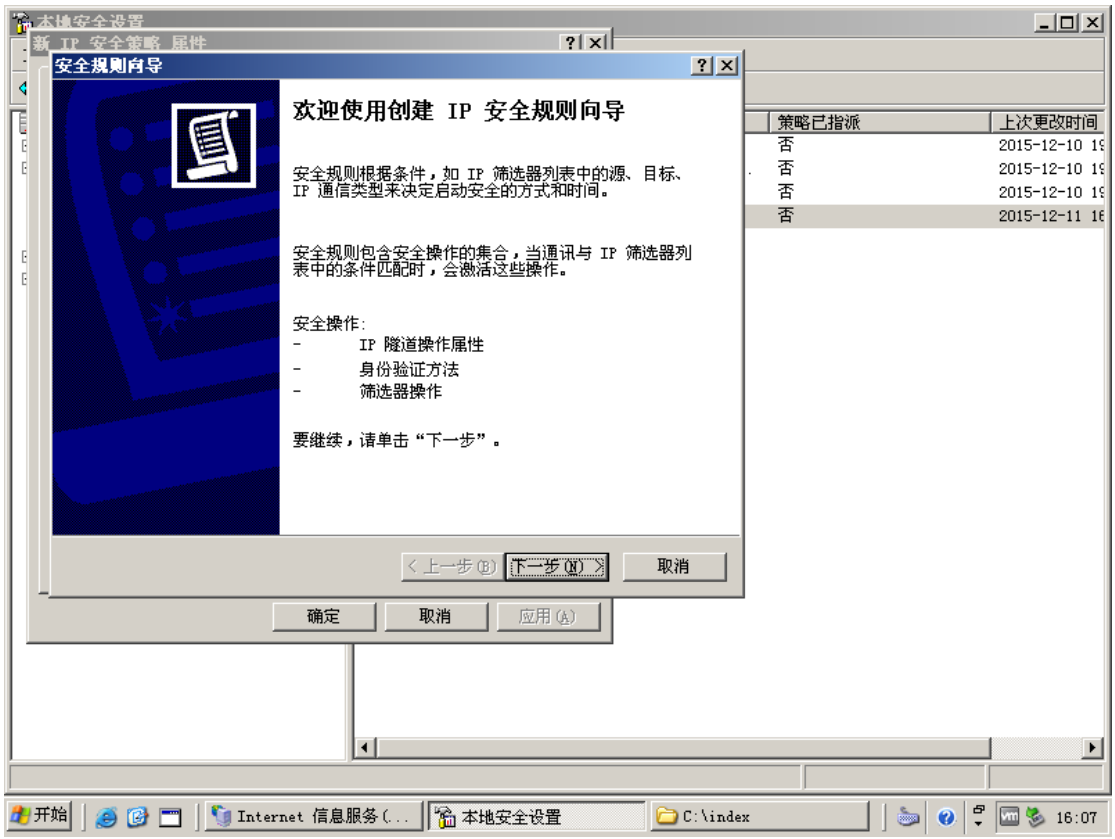
取消勾选，下一步



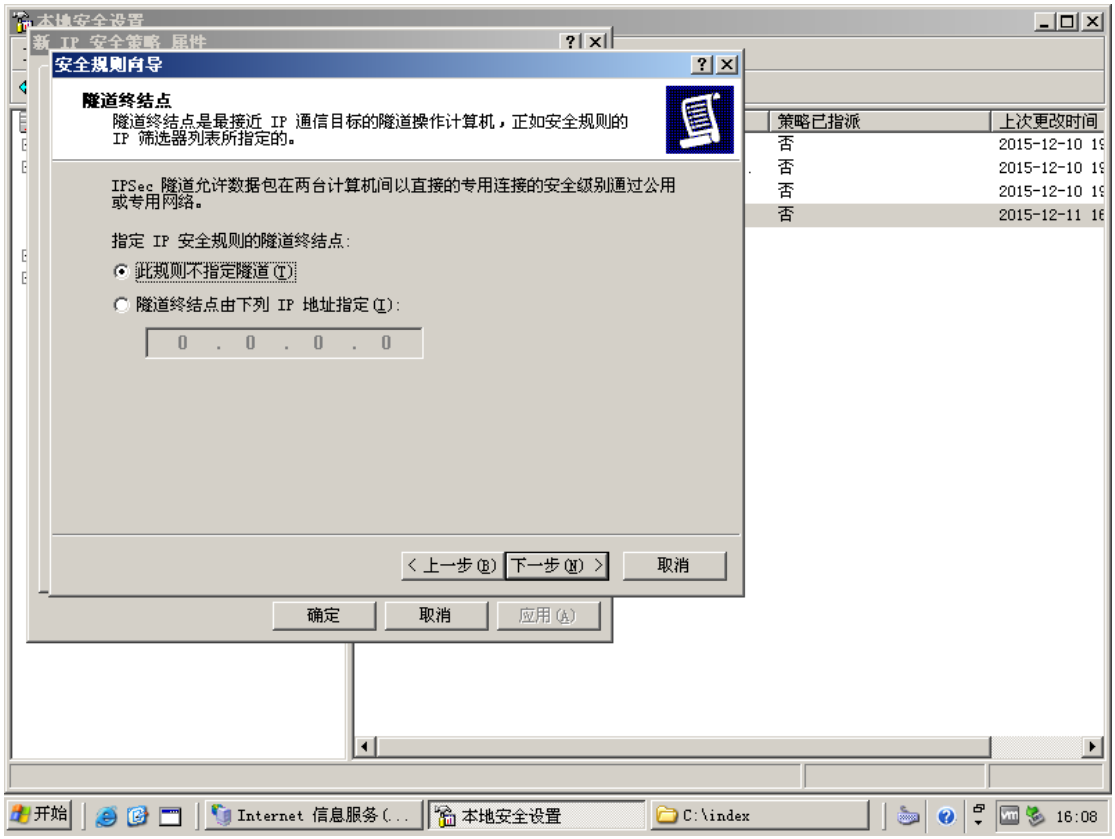
然后右键刚才新建的安全策略—属性


本地安全设置
新 IP 安全策略 属性
规则
常规
和其它计算机通讯的安全规则
IP 安全规则(I):
IP 筛选器列表
筛选器操作
身份验证方法
隧道终
<动态>
默认响应
Kerberos
<无>
添加(D)...
编辑(E)...
删除(R)
使用“添加向导”(W)
确定
取消
应用(A)
策略已指派
上次更改时间
IP 通讯总是使...
否
2015-12-10 19
(不安全的)。...
2015-12-11 16
开始
Internet 信息服务(...
本地安全设置
C:\index
16:07

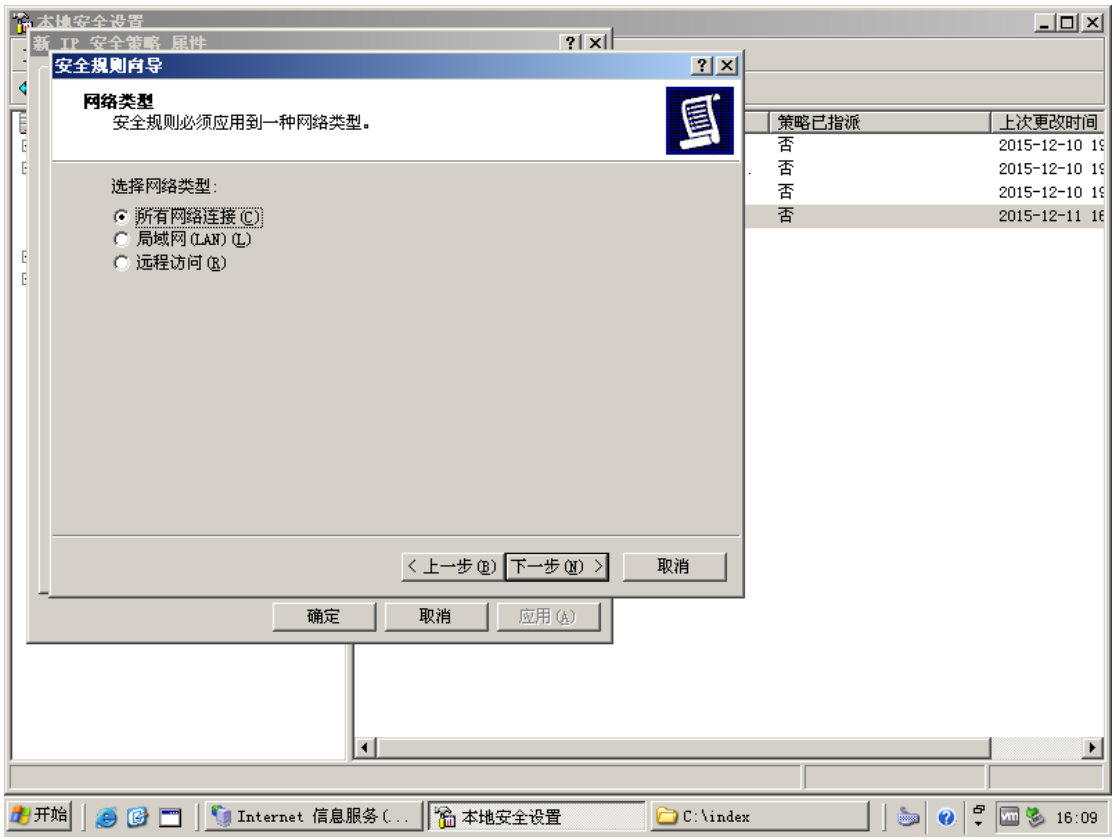
点击添加，下一步


本地安全设置
新 IP 安全策略 属性
安全规则向导
欢迎使用创建 IP 安全规则向导
安全规则根据条件，如 IP 筛选器列表中的源、目标、IP 通信类型来决定启动安全的方式和时间。
安全规则包含安全操作的集合，当通讯与 IP 筛选器列表中的条件匹配时，会激活这些操作。
安全操作:
- IP 隧道操作属性
- 身份验证方法
- 筛选器操作
要继续，请单击“下一步”。
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
策略已指派
上次更改时间
否
2015-12-10 19
2015-12-11 16
开始
Internet 信息服务(...
本地安全设置
C:\index
16:07

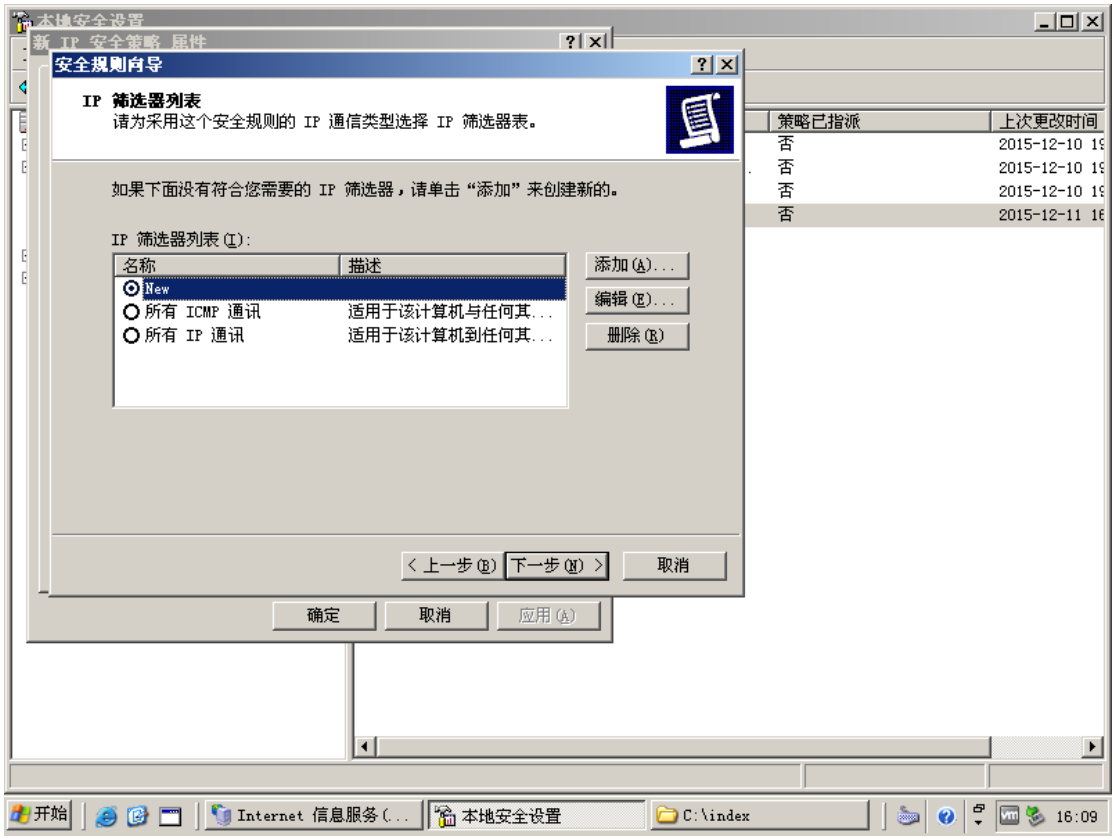
下一步



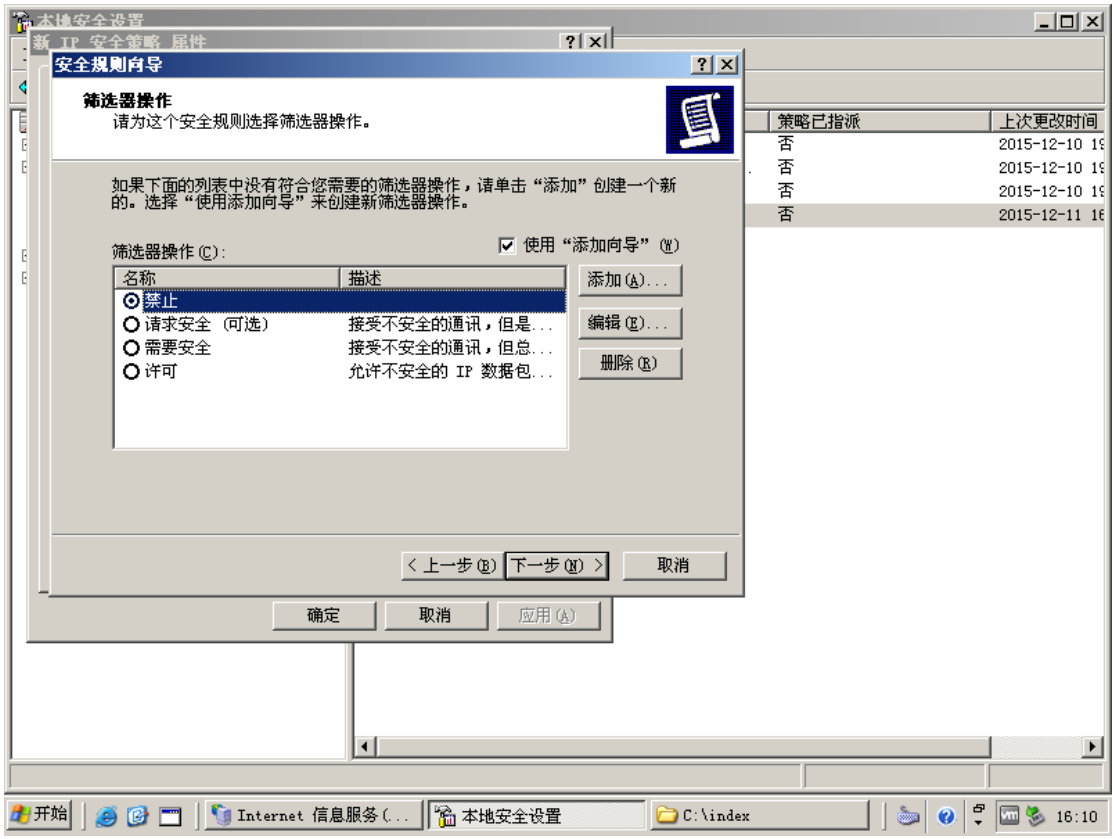
默认直接下一步



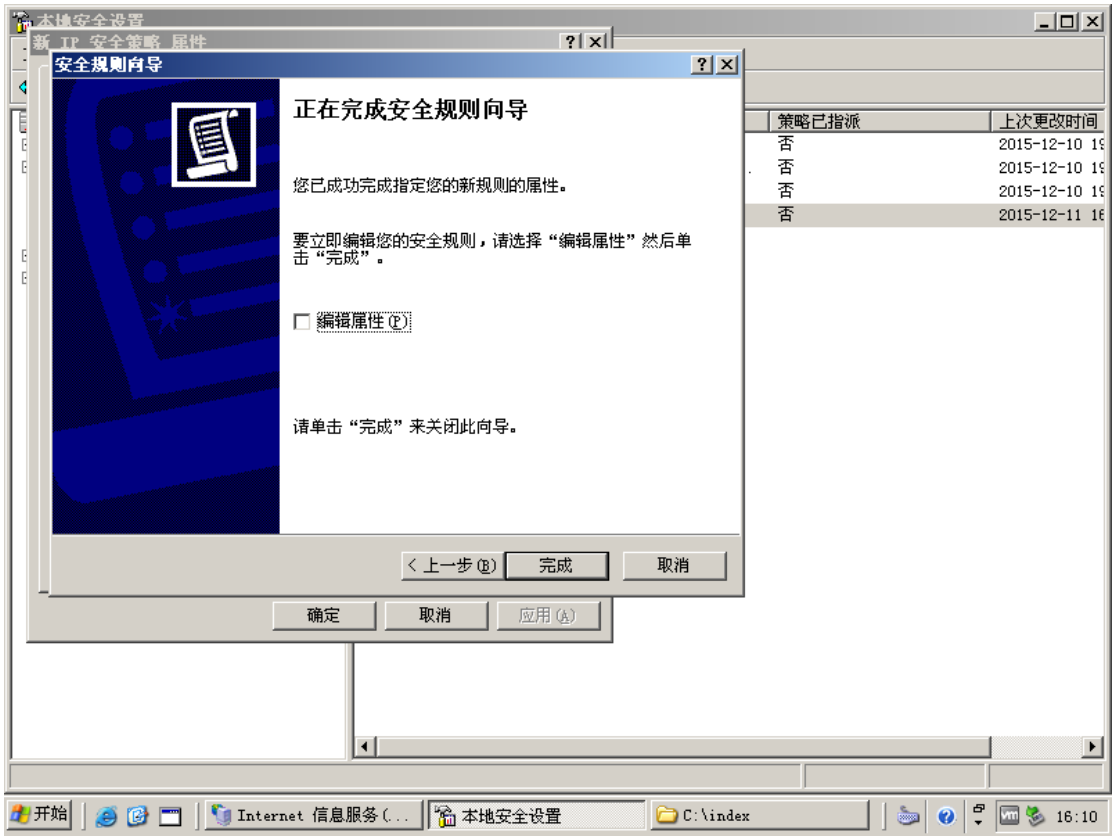
选择刚才新建的筛选表，下一步


本地安全设置
新 IP 安全策略 属性
安全规则向导
IP 筛选器列表
请为采用这个安全规则的 IP 通信类型选择 IP 筛选器表。
如果下面没有符合您需要的 IP 筛选器，请单击“添加”来创建新的。
IP 筛选器列表(T):
名称
描述
New
所有 ICMP 通讯
适用于该计算机与任何其...
所有 IP 通讯
适用于该计算机到任何其...
添加(A)...
编辑(E)...
删除(R)
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
策略已指派
上次更改时间
否
2015-12-10 19
否
2015-12-10 19
否
2015-12-10 19
否
2015-12-11 16
开始
Internet 信息服务(...
本地安全设置
C:\index
16:09

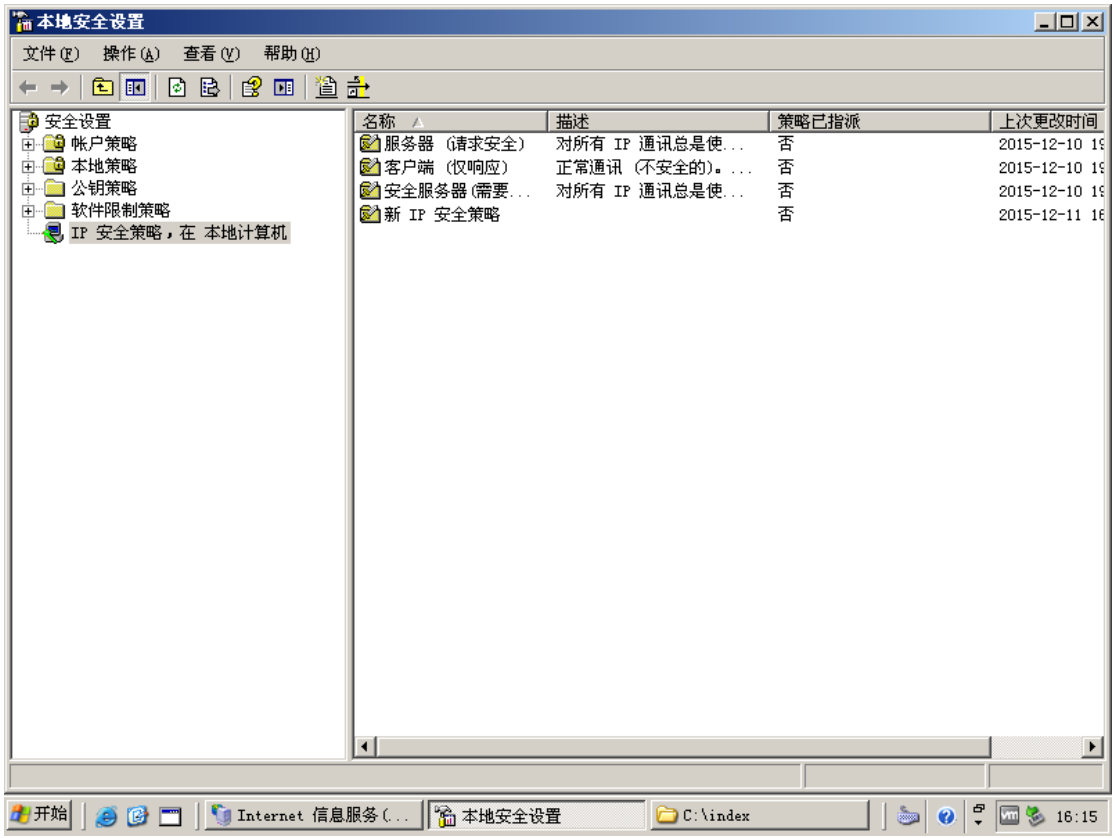
选择筛选器操作


本地安全设置
新 IP 安全策略 属性
安全规则向导
筛选器操作
请为这个安全规则选择筛选器操作。
如果下面的列表中没有符合您需要的筛选器操作，请单击“添加”创建一个新的。选择“使用添加向导”来创建新筛选器操作。
筛选器操作(C):
使用“添加向导”(W)
名称
描述
禁止
请求安全 (可选)
接受不安全的通讯，但是...
需要安全
接受不安全的通讯，但总...
许可
允许不安全的 IP 数据包...
添加(A)...
编辑(E)...
删除(R)
< 上一步(B)
下一步(N) >
取消
确定
取消
应用(A)
策略已指派
上次更改时间
否
2015-12-10 19
否
2015-12-10 19
否
2015-12-10 19
否
2015-12-11 16
开始
Internet 信息服务(...
本地安全设置
C:\index
16:10

完成

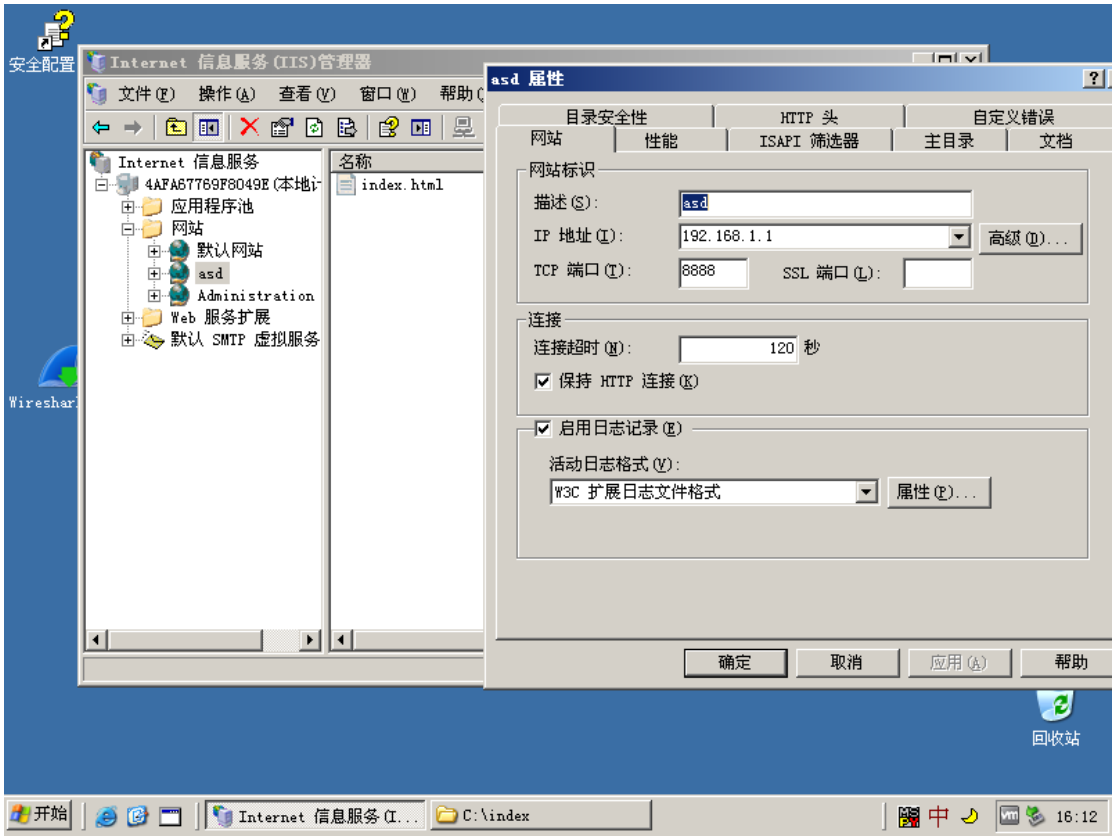


此时配置尚未完成，因为还没有指派，我们先看看指派前的效果

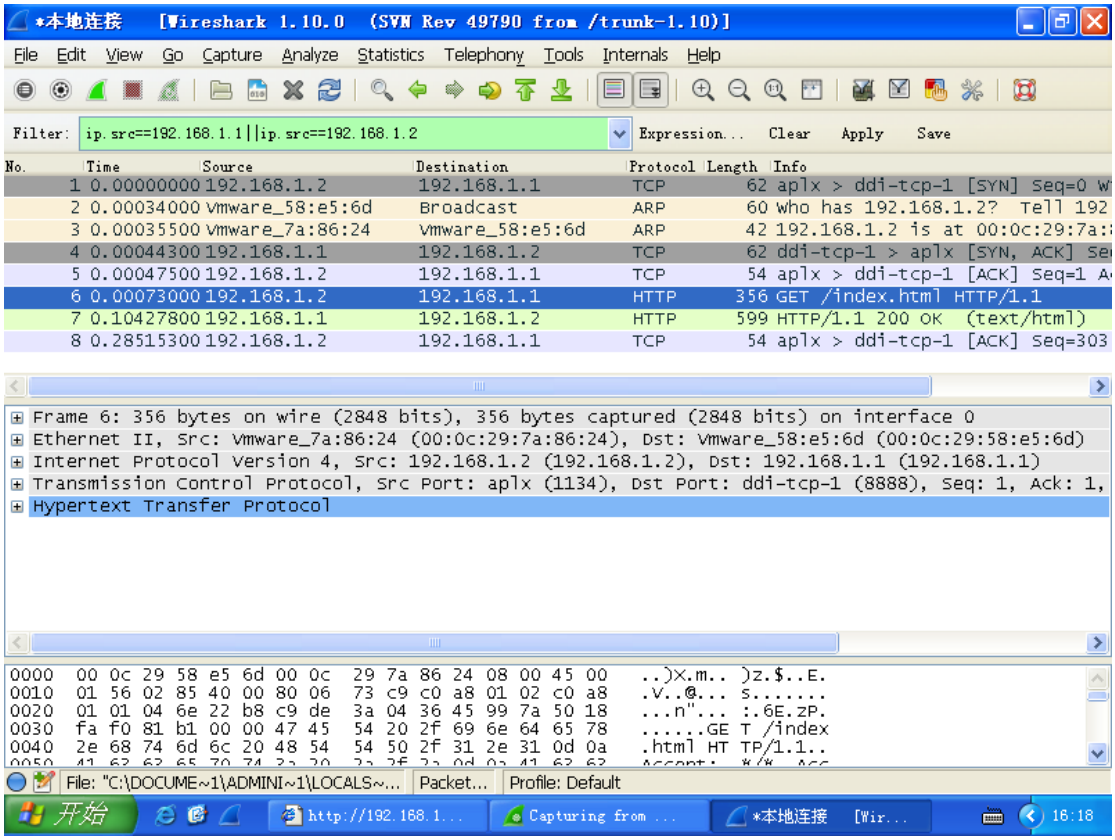


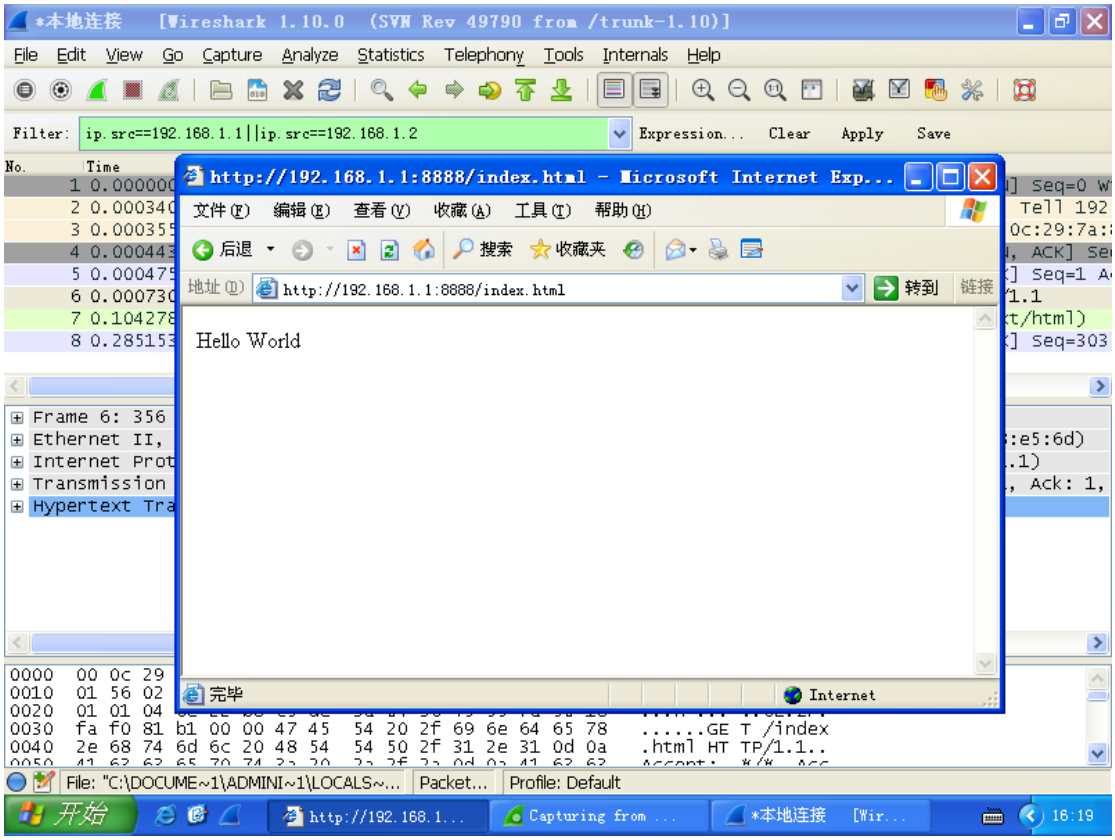
3.2 服务器配置

然后在服务器端的 iis 管理器中新建一个使用 8888 端口的网站（过程略）



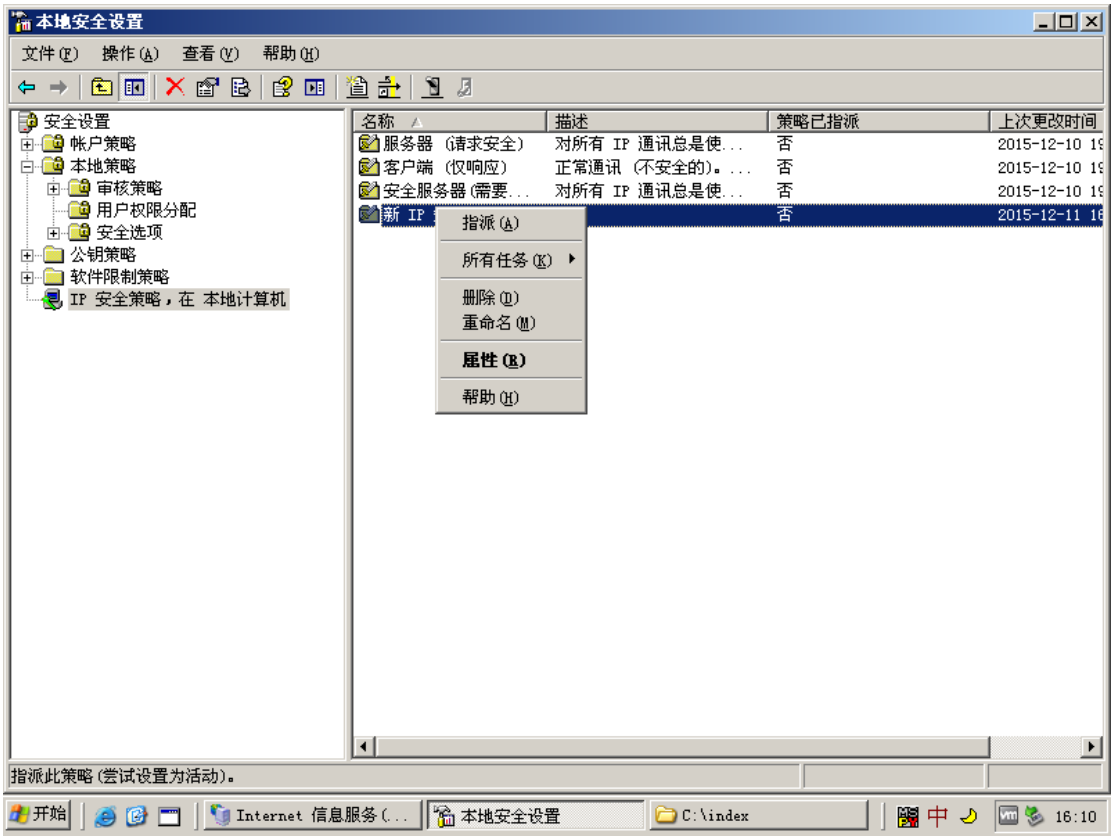
在客户端的浏览器输入 http://192.168.1.1:8888/index.html，抓包，可看到客户端向服务器端发送 TCP 请求包后，服务器端有相应的响应，完成了三次握手，发回了 http 包


*本地连接 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.src==192.168.1.1||ip.src==192.168.1.2
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 192.168.1.2 192.168.1.1 TCP 62 aplx > ddi-tcp-1 [SYN] Seq=0
2 0.00034000 vmware_58:e5:6d Broadcast ARP 60 who has 192.168.1.2? Tell 192
3 0.00035500 vmware_7a:86:24 vmware_58:e5:6d ARP 42 192.168.1.2 is at 00:0c:29:7a:
4 0.00044300 192.168.1.1 192.168.1.2 TCP 62 ddi-tcp-1 > aplx [SYN, ACK] Se
5 0.00047500 192.168.1.2 192.168.1.1 TCP 54 aplx > ddi-tcp-1 [ACK] Seq=1 A
6 0.00073000 192.168.1.2 192.168.1.1 HTTP 356 GET /index.html HTTP/1.1
7 0.10427800 192.168.1.1 192.168.1.2 HTTP 599 HTTP/1.1 200 OK (text/html)
8 0.28515300 192.168.1.2 192.168.1.1 TCP 54 aplx > ddi-tcp-1 [ACK] Seq=303
Frame 6: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface 0
Ethernet II, Src: Vmware_7a:86:24 (00:0c:29:7a:86:24), Dst: Vmware_58:e5:6d (00:0c:29:58:e5:6d)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)
Transmission Control Protocol, Src Port: aplx (1134), Dst Port: ddi-tcp-1 (8888), Seq: 1, Ack: 1,
Hypertext Transfer Protocol
0000 00 0c 29 58 e5 6d 00 0c 29 7a 86 24 08 00 45 00 ..)X.m..)z.$..E.
0010 01 56 02 85 40 00 80 06 73 c9 c0 a8 01 02 c0 a8 .V..@... s.......
0020 01 01 04 6e 22 b8 c9 de 3a 04 36 45 99 7a 50 18 ...n"... :.6E.zP.
0030 fa f0 81 b1 00 00 47 45 54 20 2f 69 6e 64 65 78 ......GE T /index
0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
File: "C:\DOCUME~1\ADMINI~1\LOCALS~... Packet... Profile: Default
开始 http://192.168.1... Capturing from ... *本地连接 [Wir... 16:18

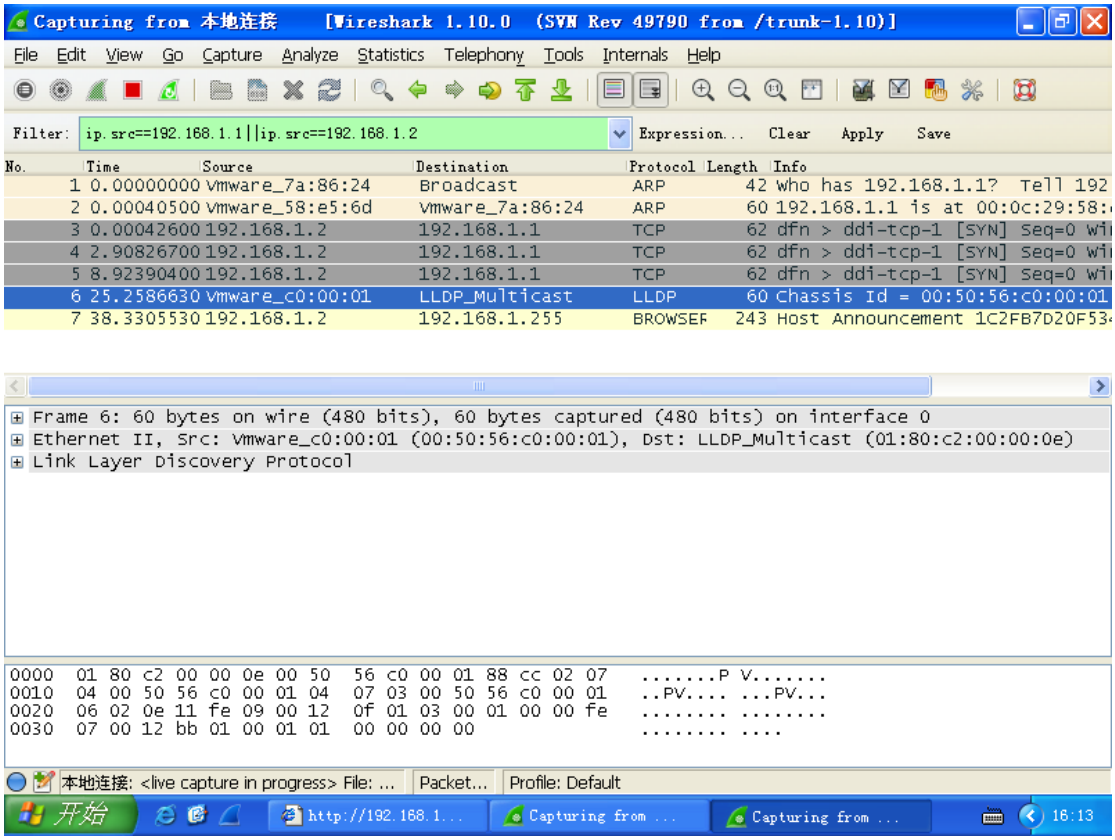

*本地连接 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip.src==192.168.1.1||ip.src==192.168.1.2
Expression... Clear Apply Save
http://192.168.1.1:8888/index.html - Microsoft Internet Exp...
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http://192.168.1.1:8888/index.html 转到 链接
Hello World
完毕 Internet
0000 00 0c 29
0010 01 56 02
0020 01 01 04
0030 fa f0 81 b1 00 00 47 45 54 20 2f 69 6e 64 65 78 ......GE T /index
0040 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
File: "C:\DOCUME~1\ADMINI~1\LOCALS~... Packet... Profile: Default
开始 http://192.168.1... Capturing from ... *本地连接 [Wir... 16:19

3.3 启用 IPSec

现在来试试 IPSec 的效果，右键指派



在客户端的浏览器输入 http://192.168.1.1:8888/index.html，抓包，可看到此时客户端连续发了 3 个 TCP 请求包给服务器端，都没有响应。证明 IPSec 配置有效。



3.4 下一步工作

后面缺少客户端配置 IPSec 及配置后与服务器之间的安全通信过程。如果有同学完成该部分，在上交作业时请在邮件标题中注明，下次将以你的作业作为下年度的参考模板