Windows安全原理与技术

— 第八章：网络传输安全

王轶骏， Eric Ericwyj@sjtu.edu.cn

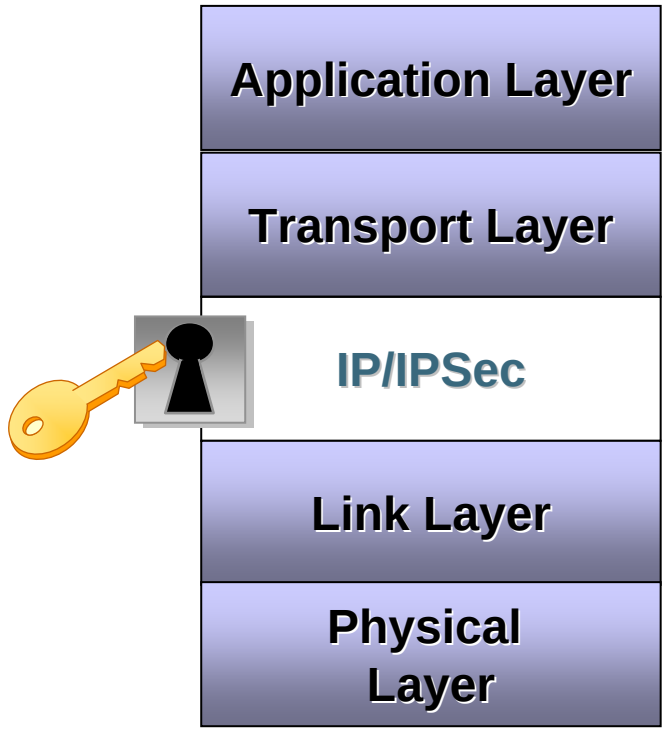
SJTU.INFOSEC.A.D.T, 2008

网络的不安全性

- 网络的诱惑太大。
- 网络协议具有缺陷。
- 网络攻击技术发展迅速。
  - 网络监听攻击
  - 协议欺骗攻击
  - 拒绝服务攻击
  - 应用层攻击
  - …

IPSec协议

- **IPSec是一种安全协议**
  - 通过对传输之前的每个IP数据包进行加密来保护网络传输。
  - IPSec是网络层加密。



IPSec的意义

- 信息完整性
  - 完整性保护信息在传输过程中免遭未经授权的修改，从而保证接收到的信息与发送的信息完全相同。
- 信息机密性
  - 机密性保证只有预期的接收者才能读出数据。
- 身份验证
  - 身份验证检查信息来源的可靠性。

IPSec协议标准

- IPSec协议是由IETF（Internet工程任务组）作为用于IP的安全体系结构而设计的，它建立在IETF所批准的一系列标准文档的基础之上。

IPSec协议基础

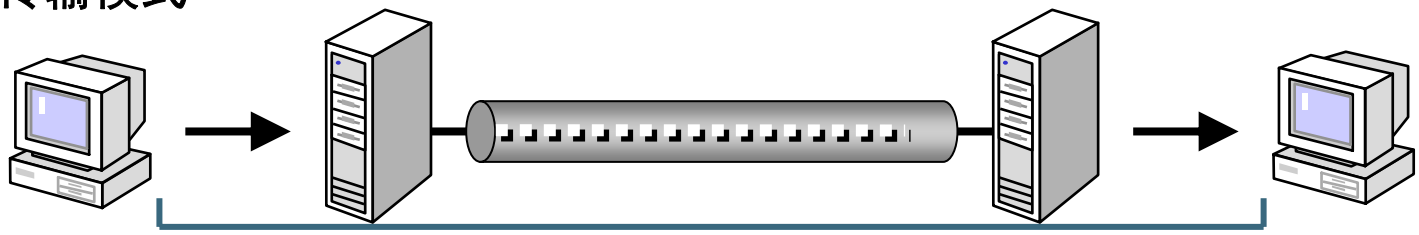
- 两种封装协议
  - 验证报头（ AH ）
  - 封装安全载荷（ ESP ）
- 两种封装模式
  - 传输模式
  - 隧道模式
- 安全联盟（SA）

传输模式和隧道模式

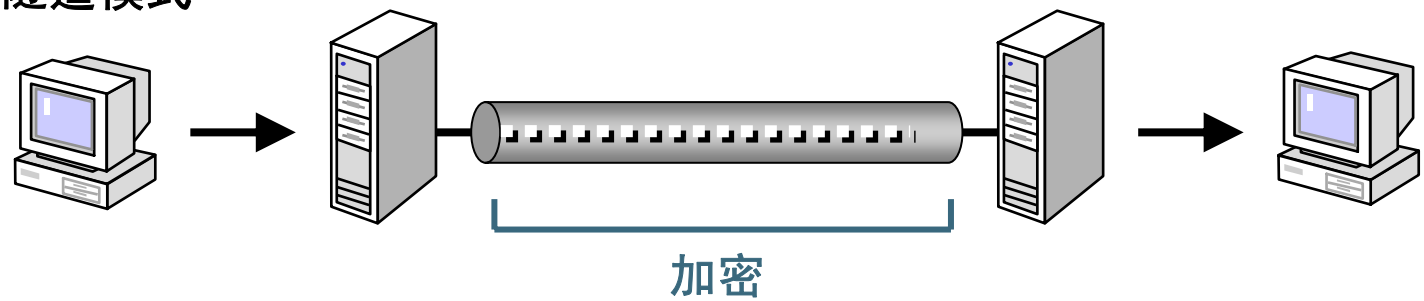

原始的IP
数据报
IP头
TCP头
数据
传输模式
受保护的数据报
IP头
IPSec头
TCP头
数据
隧道模式
受保护的数据报
新IP头
IPSec头
IP头
TCP头
数据

- 传输模式（Transport Mode）
  - 用于端到端的连接。
  - 两端的系统都必须支持IPSec，而中间节点系统则不必支持IPSec，它们只是以普通的方式转发数据包。
- 隧道模式（Tunnel Mode）
  - 用于网关对网关的连接。
    - VPN
  - 数据包的源和目的终端都不必支持IPSec，而只有提供安全服务的网关才必须支持IPSec。

传输模式

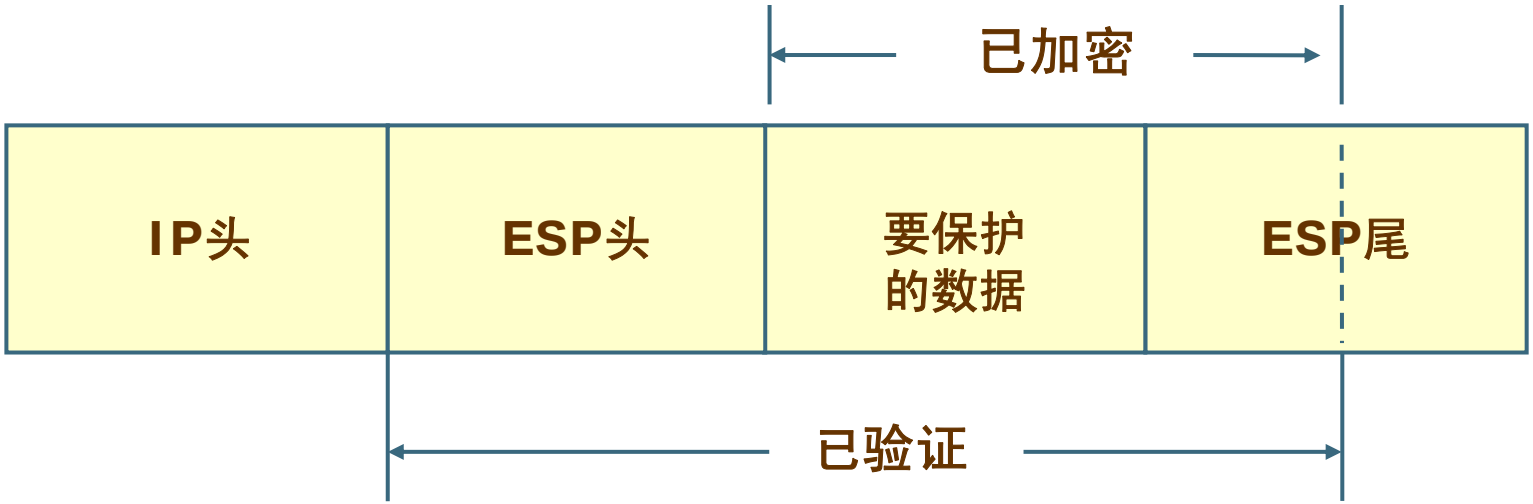


隧道模式



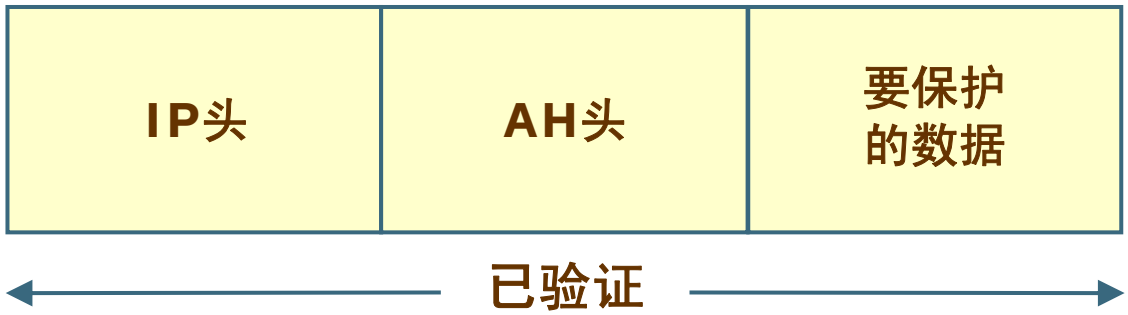
ESP和AH

- **ESP（Encapsulating Security Payload）**
  - 保证数据的机密性
  - 保证数据的完整性
  - 提供对数据源的身份验证
  - 提供对重播攻击的抵抗



AH（Authentication Header）

- 保证数据的完整性
- 提供对数据源的身份验证
- 提供对重播攻击的抵抗



ESP头部内容

- 安全参数索引（Security Parameters Index, SPI）
  - 标示该数据包和SA的对应关系。
- 序列号（Sequence Number）
  - 用来抗重播攻击，32bit长度，每次递增1。
- 填充数据
- 填充数据长度
- 认证数据
- 下一头部
  - 使用IP协议号来描述紧跟在AH头部后面的IP载荷。

AH头部内容

- 下一头部
  - 使用IP协议号来描述紧跟在AH头部后面的IP载荷。
- AH头部长度
- 安全参数索引（SPI）
  - 标示该数据包和SA的对应关系。
- 序列号
  - 用来抗重播攻击，32bit长度，每次递增1。
- 认证数据

安全联盟（SA）

- SA
  - SA是一套专门的方案，用来解决如何保护通信数据、保护什么样的通信数据以及由谁来实行保护的问题。
  - SA是单向进行的。
    - 它仅朝一个方向定义安全服务，要么对通信实体收到的包进行“进入”保护，要么对实体外发的包进行“外出”保护，即“出站SA”和“入站SA”。
  - SA是以成对的形式存在的，每个朝一个方向。
  - 既可人工创建SA，也可动态创建。
  - SA驻留在安全联盟数据库（SADB）内 。

SA协商的两个阶段

- 第一阶段SA，用于相互通讯安全的协商
  - 加密算法
    - 3DES，DES（56bit），40-bit DES，无。
  - 散列算法
    - MD5，SHA1
  - 认证方法
    - 证书，Kerberos，预先共享的密钥。
  - Diffie-Hellman小组，用于密钥材料。
- 第二阶段SA，用于传输数据安全的协商
  - IPSec协议
  - 加密算法
  - 散列算法

IPSec策略

- IPSec策略由安全策略数据库（Security Policy Database, SPD）加以维护。
  - 在SPD中，每个条目都定义了要保护的是什么通信、怎样保护它以及和谁共享这种保护。
  - 一个SPD条目可能定义丢弃、绕过以及应用等几种行为。
  - 那些定义了应用行为的SPD条目均会指向一个或一套SA，表示要将其应用于数据包。

- 假定某个SPD条目将行为定义为应用，但并不指向SADB数据库内已有的任何一个SA，那么在进行任何实际的通信之前，首先必须创建那些SA。
  - 如果这个规则用于自外入内的进入通信，而且SA尚不存在，则按照IPSec基本架构的规定，数据包必须丢弃。
  - 假如该规则用于自内向外的外出通信，则通过Internet密钥交换，便可动态的创建SA。

- IPSec通信到IPSec策略的映射关系是由选择符（Selector）来建立的。
  - 选择符标识通信的一部分组件，它既可以是一个粗略的定义，也可以是一个非常细致的定义。
  - IPSec选择符包括：目标IP地址、源IP地址、名字、上层协议、源和目标端口以及数据敏感级。

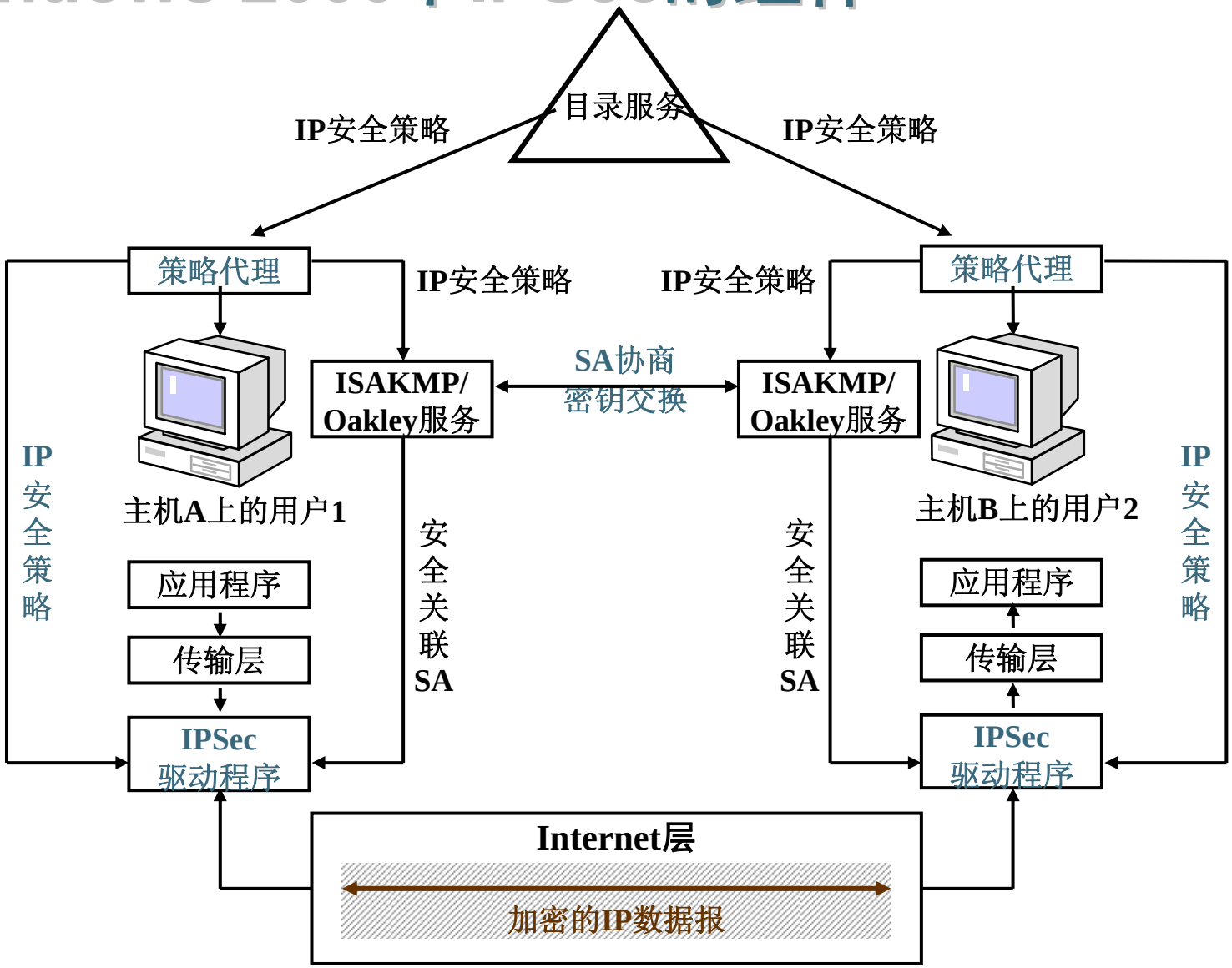
Windows 2000中的IPSec

- Windows 2000的IPSec建立于IETF的IPSec体系结构之上，与Windows 2000活动目录服务集成。
  - 由Microsoft和Cisco System, Inc共同开发。
  - 结合了Windows 2000 操作系统的内在安全。
  - 活动目录使用组策略为Windows 2000域成员提供IPSec 策略的分配和分发，提供基于策略的、支持目录的网络。

Windows 2000中IPSec的优点

- 开放的工业标准
- 对应用程序和用户透明
- 保密性、数据完整性和身份验证
- 动态重设密钥
- 端对端安全链接
- 集中管理
- 灵活性

Windows 2000中IPSec的组件



- 工作站A上的用户产生一个报文，发送给工作站B上某一应用程序。
- 工作站A上的IPSec驱动程序将报文的目的IP地址或协议与当前有效的IPSec策略中的IP过滤清单中相比较。
- 如果IPSec策略规定系统间的通信是安全的，那么IPSec驱动程序就指示IKE开始与工作站B协商。
- 工作站B的IKE收到一条来自工作站A的IKE请求安全协商的报文。
- 双方协商第一阶段的SA和第二阶段的两个SA（入站和出站SA）。
- 工作站A上的IPSec驱动程序使用为第二阶段出站SA而商定的参数，为输出数据计算完整性签名，加密数据，并通过给IP数据包增加适当的报头字段来构造IPSec数据包。
- 工作站A把完成的数据包传送到工作站B，工作站B再把它们传给自己的IPSec驱动程序。
- 工作站B的IPSec驱动程序使用入站SA的参数，解密数据，并通过重复计算签名和比较签名与数据包中的结果来验证数据包的完整性。
- 工作站B上的IPSec驱动程序把解密过的数据传送到TCP/IP协议栈，TCP/IP协议栈再依次把它上传到报文的目的地（即应用程序）

Internet密钥交换（IKE）

- IKE是一种建立SA和在两个系统之间交换密钥的协议。
- IKE包括两个阶段：
  - 第一阶段包括建立第一阶段SA和身份验证过程。建立第一阶段的SA包括对系统将要使用的加密算法、散列算法和身份验证方法的协商。
  - 第二阶段是为IPSec服务建立IPSec协议（AH和/或ESP）、散列算法（MD5或SHA1）和加密算法（DES或3DES）的协商，以及身份验证和加密密钥的交换与刷新。

- IKE提供三种身份验证方法：
  - 基于 Windows 2000 域基础结构提供的 Kerberos v5身份验证。
  - 使用证书的公钥/私钥签名。
  - 密码，即“预先共享的身份验证密钥”。

在Windows 2000中实现IPSec

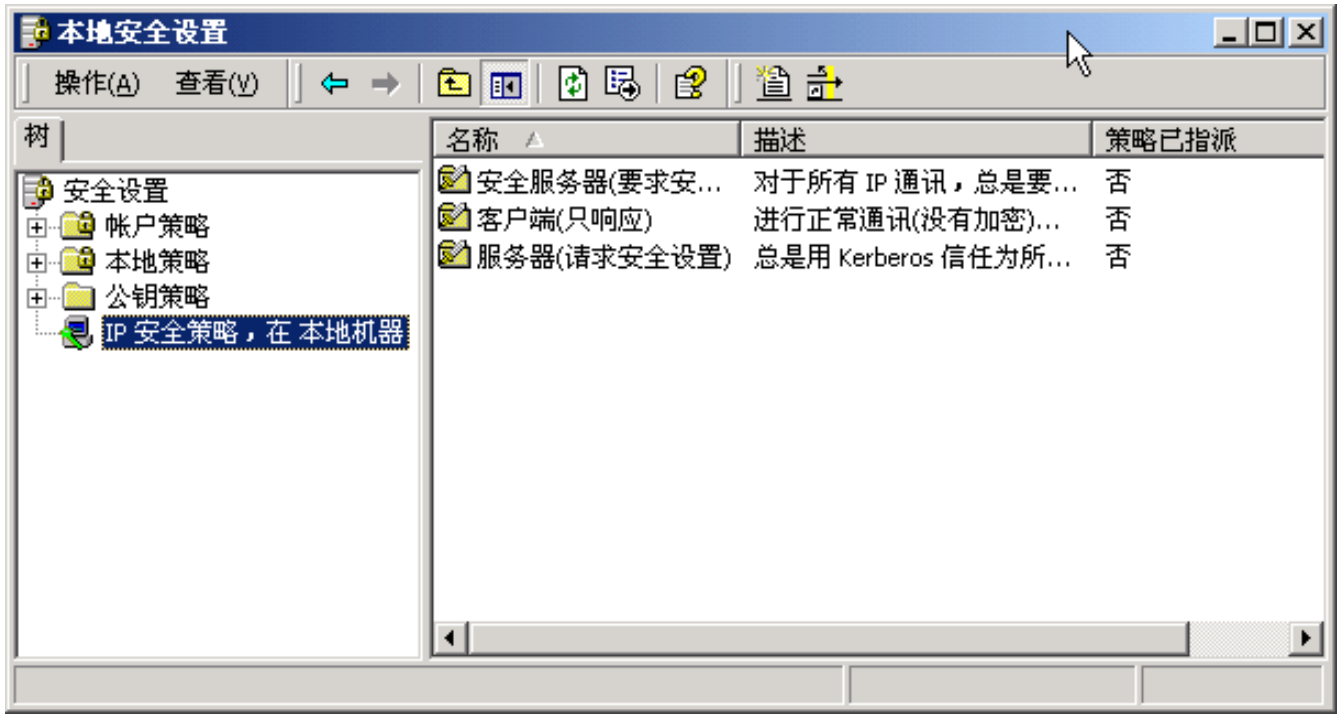
- 确定安全需求（估计威胁）
- 确定安全级别
- 定制安全策略

确定安全级别

- 最低安全性
  - 计算机不交换敏感的数据。
- 标准安全
  - 计算机（尤其是文件服务器）用来存储有价值的数据。
  - 安全必须平衡，使其不会阻碍验证试图执行任务的用户的合法性。
- 高安全性
  - 计算机包含高度敏感的数据。
  - 存在数据失窃、意外或恶意破坏系统或任何公共网络通讯的危险。

建立安全策略

- Windows 2000提供了一套预定义的IPSec策略。这些预定义的策略无需进一步的操作就可以指派，也可以对其进行修改，或者将其用作自定义策略的模板。



预定义的IPSec策略

- 客户端（只响应）
  - 用于在大部分时间都不能保证安全通信的计算机。
- 服务器（请求安全性）
  - 用于在大多数时间保证安全通信的计算机。
- 安全服务器（需要安全性）
  - 用于始终需要安全通信的计算机。

IPSec策略的基本元素

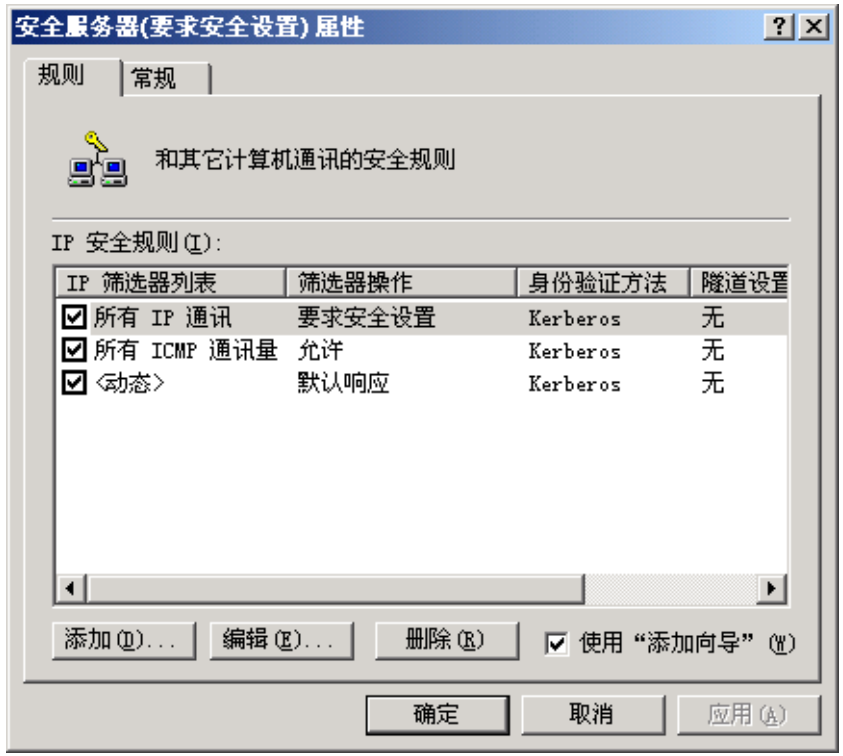
- 基本元素
  - 安全策略规则
  - IP筛选器列表
  - IP筛选器操作
- 关系
  - 规则是IP筛选器列表和IP筛选器操作的结合

指派IPSec安全策略的注意事项

- 域成员计算机
  - 应用于域的 IPSec 安全策略将优先于本地的活动 IPSec 策略。
  - 最低级组织单位IPSec策略将替代该组织单位中所有成员的较高级别组织单位的IPSec策略，而不是合并。
- 独立计算机
  - 本地计算机策略

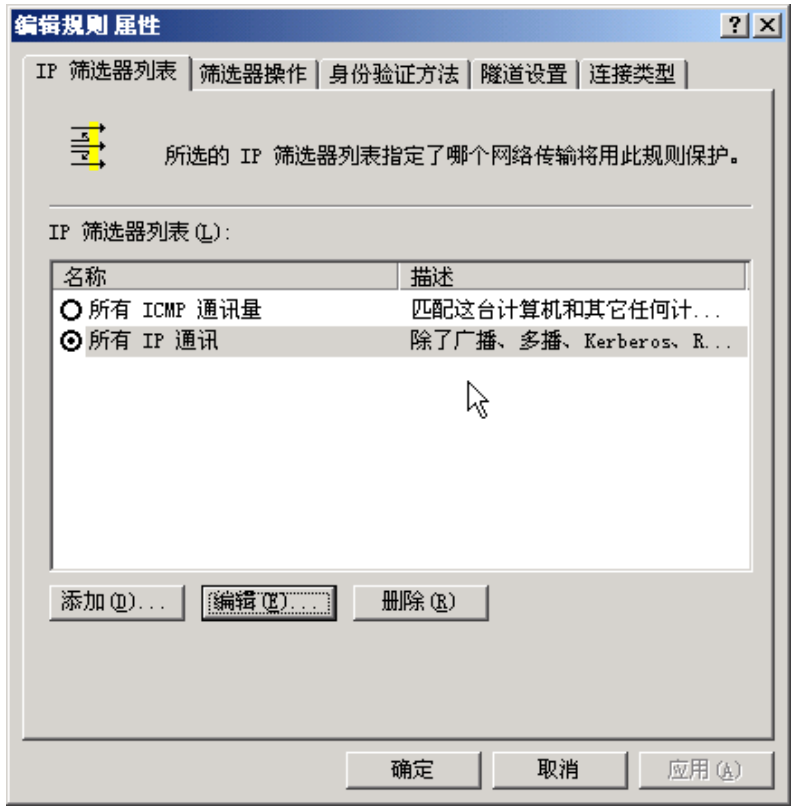
IP安全策略的规则

- IP安全策略由多条规则所组成，而每条规则是由IP筛选器列表和IP筛选器操作所组合而成的，此外还包括身份验证方法、隧道设置、连接类型等设置。



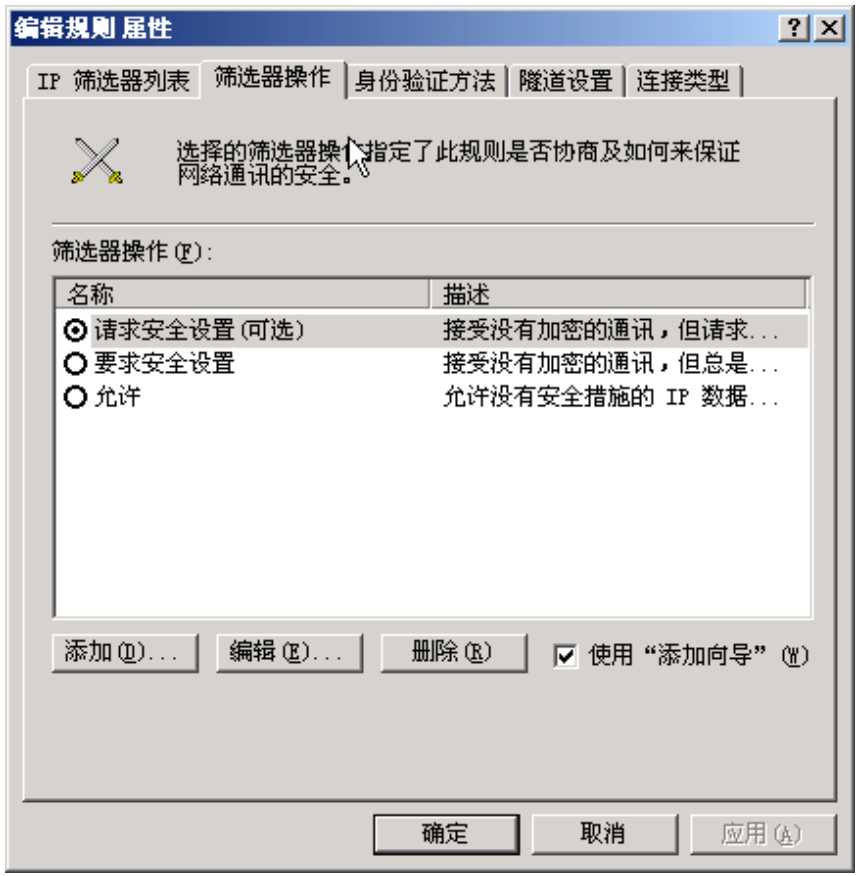
IP筛选器列表

- IP 筛选器列表触发建立在与源、目标及 IP 传输类型匹配的基础上的安全协商。
- 每个 IP 筛选器列表包含一个或多个IP筛选器。
- IP筛选器包含的设置：
  - IP数据包的源和目的地址。
  - 正在传输的数据包所使用的传输协议。
  - TCP和UDP协议的源和目的端口。



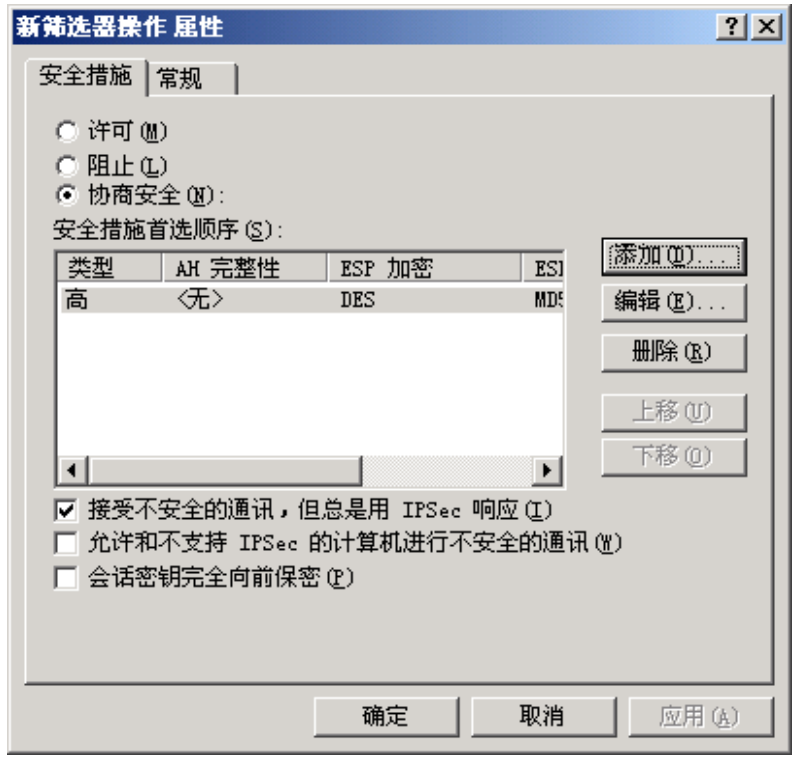
IP筛选器操作

- 筛选器操作用来定义数据传输的安全需求。



IP筛选器操作类型

- 许可
  - 以明文发送或接收数据包。这些数据包将不请求安全性。
- 阻止
  - 强制立即丢弃符合筛选器条件的数据包。
- 协商安全
  - 使用“安全措施首选顺序”中的安全方法列表为符合筛选器的数据包提供安全性。这些数据包将来的安全请求将被接受。

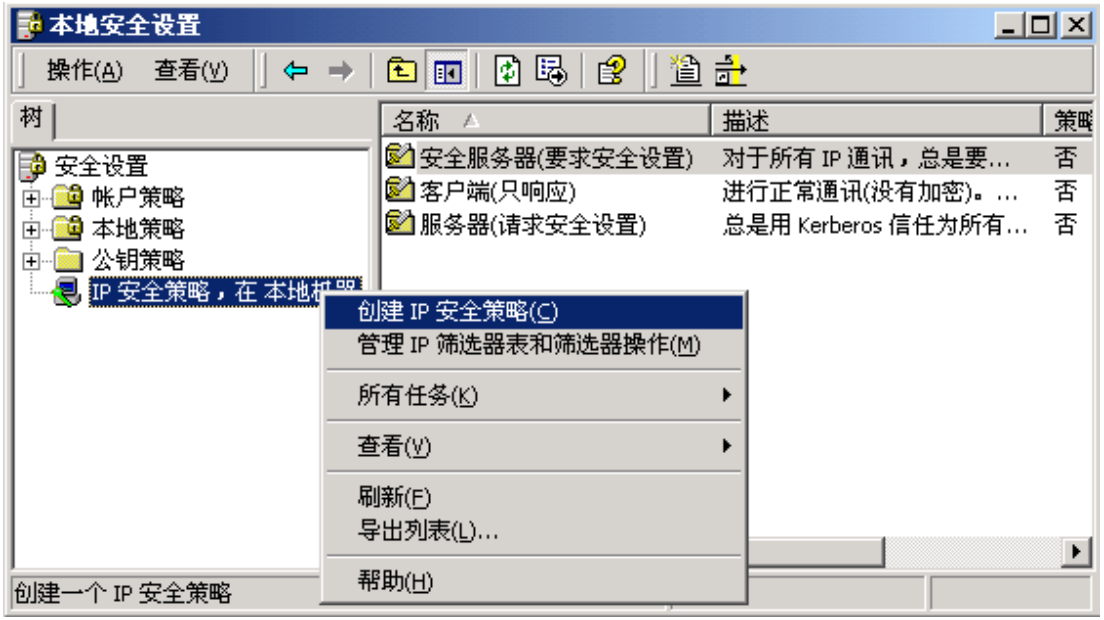


协商安全选项

- 必须对方计算机启用IPSec
- 允许和不支持IPSec的计算机进行通信
  - “接受不安全通信，但总是用IPSec响应”
  - “允许和不支持IPSec的计算机进行不安全通信”
- “会话密钥完全向前保密”

创建自定义的IPSec策略

- 要定义计算机的 IPSec 策略，必须要有访问“组策略”的适当管理员权限，或者是本地系统Administrators组的成员。



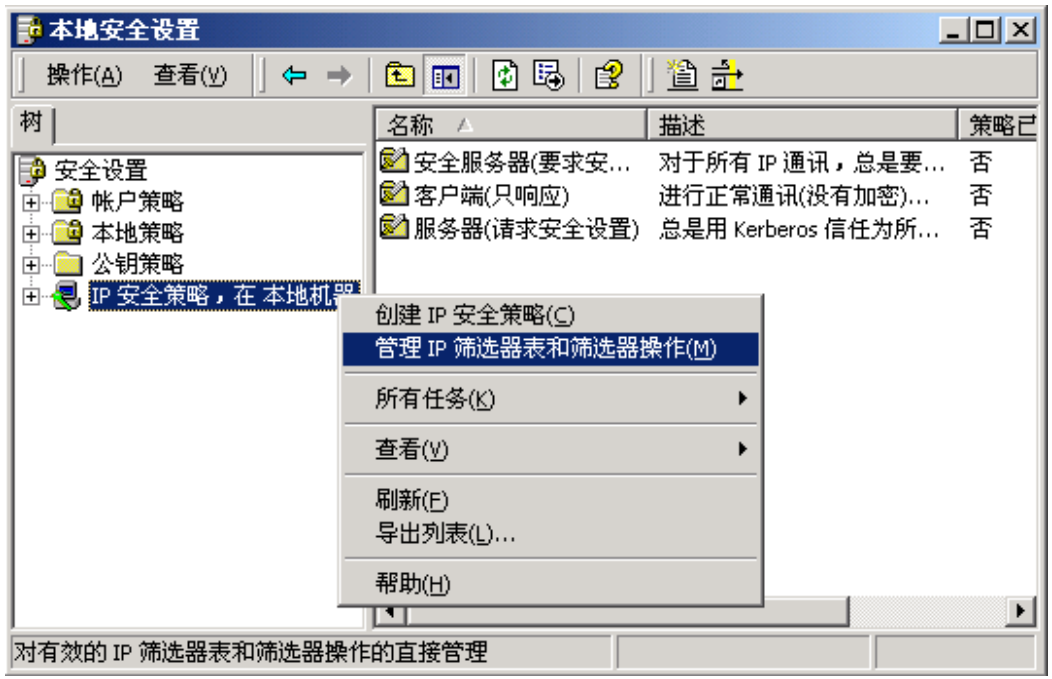
IPSec配置的简单实例

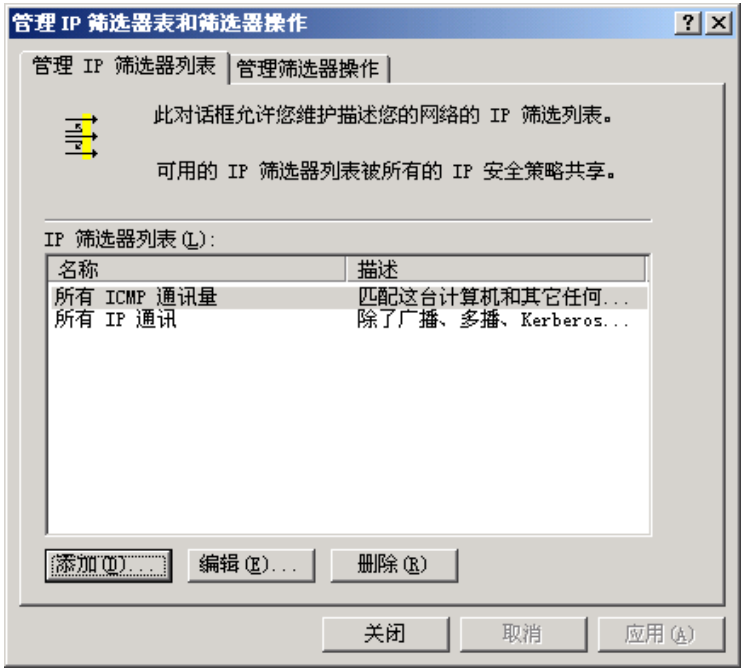
- 内容
  - 屏蔽本机对ICMP协议的响应
    - 不会被别的主机ping通
    - 不会成为受icmp广播风暴攻击影响
- 步骤
  - 设置IP筛选器表，添加有关ICMP协议的筛选器。
  - 设置IP筛选器操作，添加屏蔽操作。
  - 设置IP安全策略，添加屏蔽ICMP协议的安全策略。
  - 启用此IP安全策略。

- 运行“IP安全策略”管理工具。

（“开始”→“程序” →“管理工具” →“本地安全策略” →“IP安全策略”）

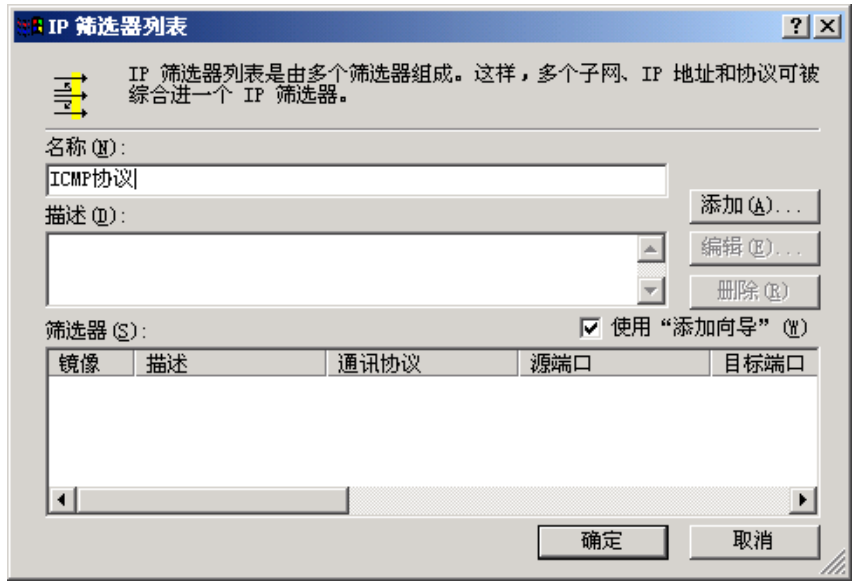
- 右键点击“IP安全策略，在本地机器”，在弹出的菜单上选择管理IP筛选器表和筛选器操作”。

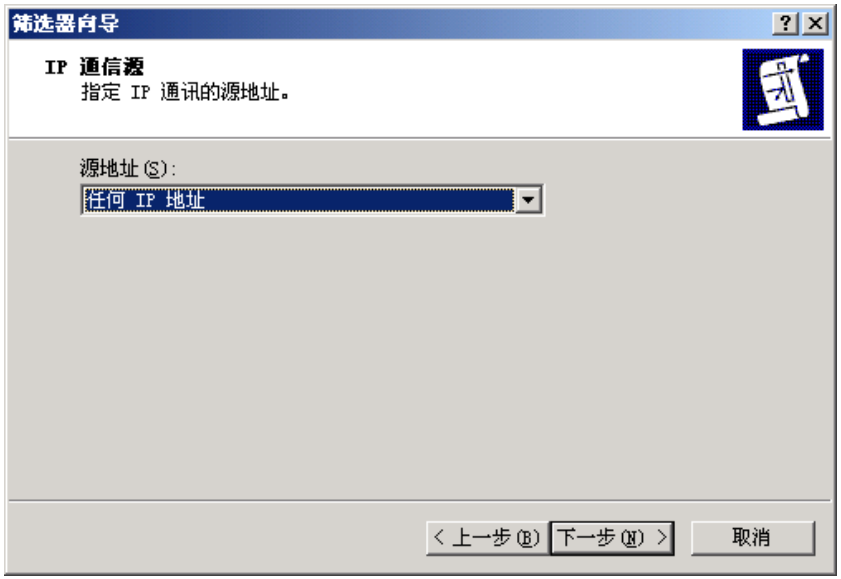




- 添加IP筛选器列表

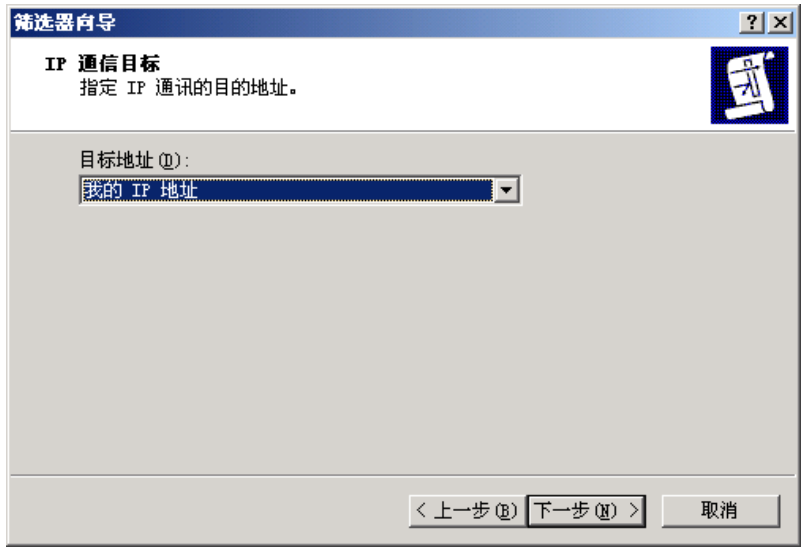
- 输入IP筛选器列表名称（“进入的ICMP通讯”）



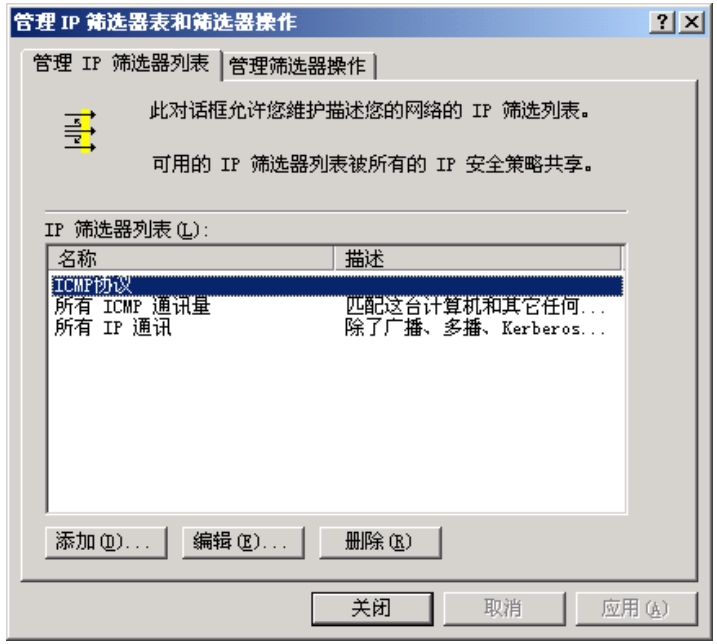


- 指定IP通讯的源地址（“任何IP地址”）

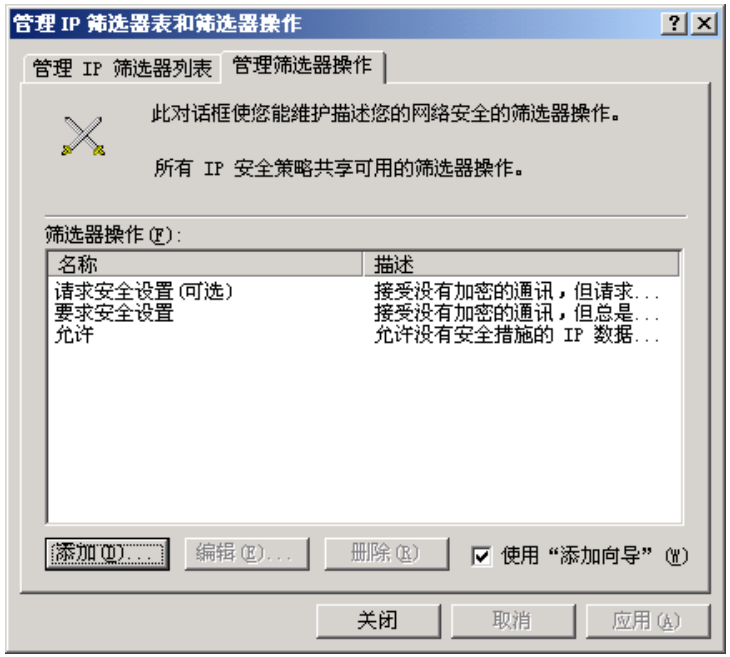
- 指定IP通讯的目的地址（“我的IP地址”）



- 指定IP通讯的协议类型（“ICMP”）

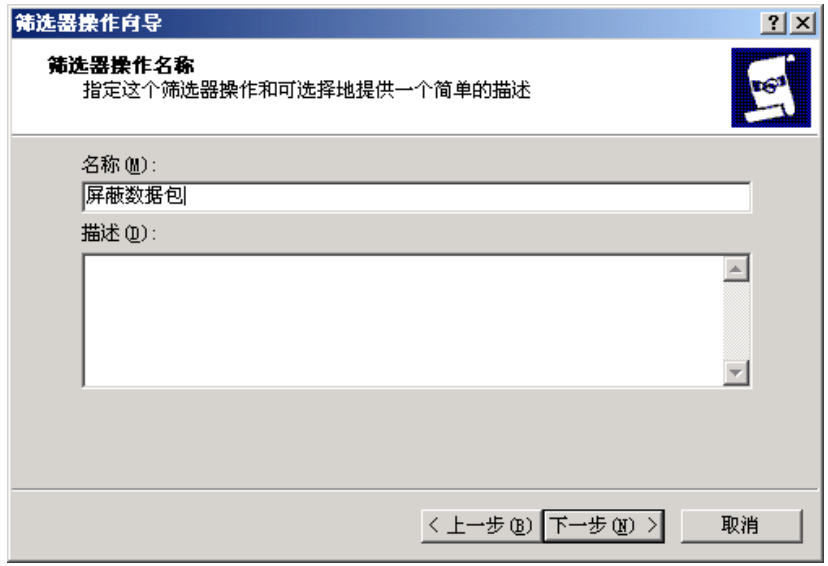


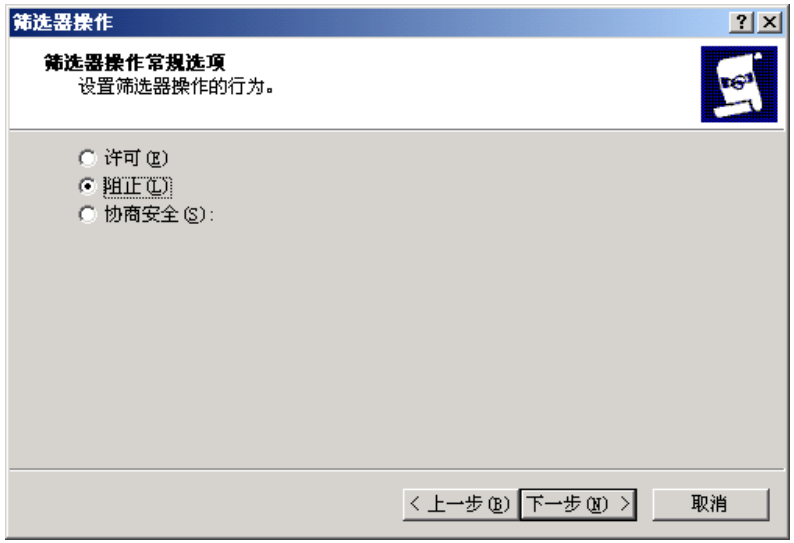
- 添加IP筛选器列表完毕



- 添加筛选器操作

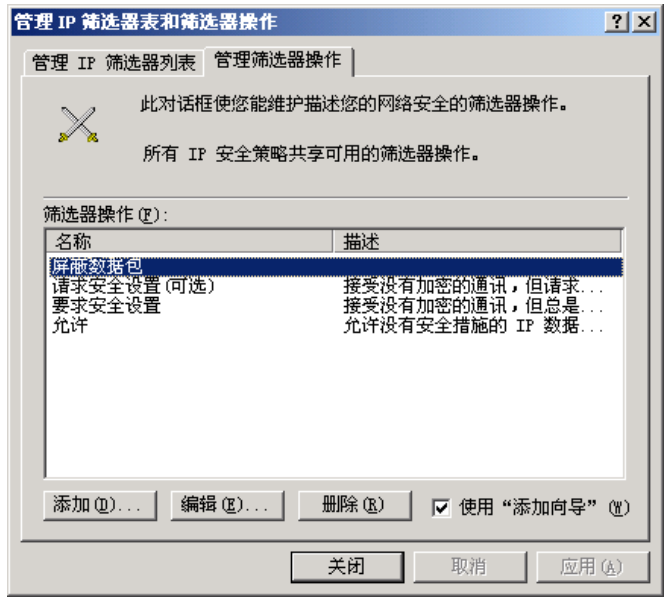
- 输入筛选器操作名称“屏蔽数据包”

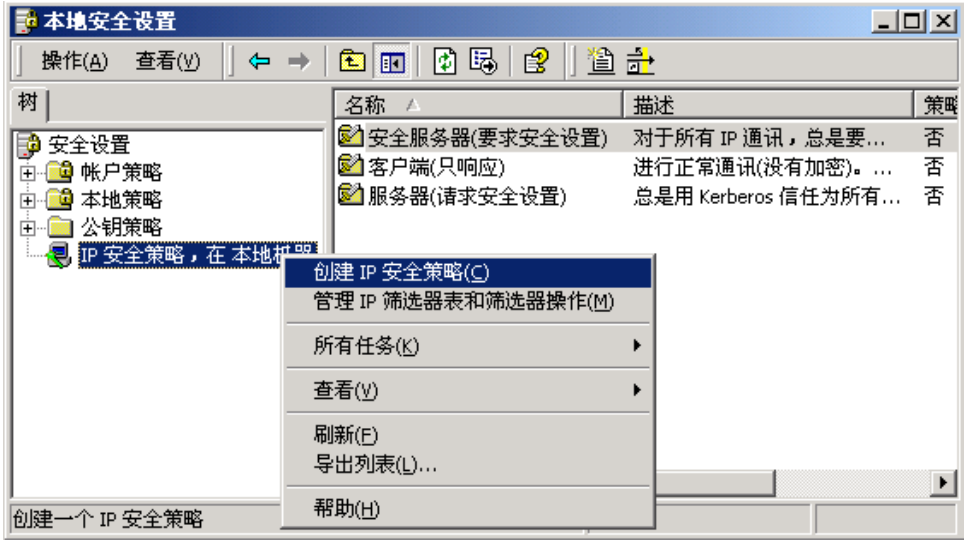




❖在“筛选器操作常规选项”中选择“阻止”

❖ 添加筛选器操作完毕

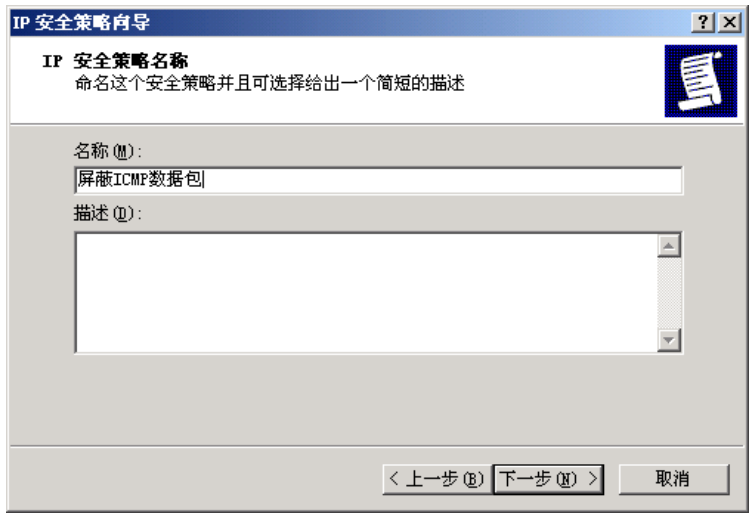


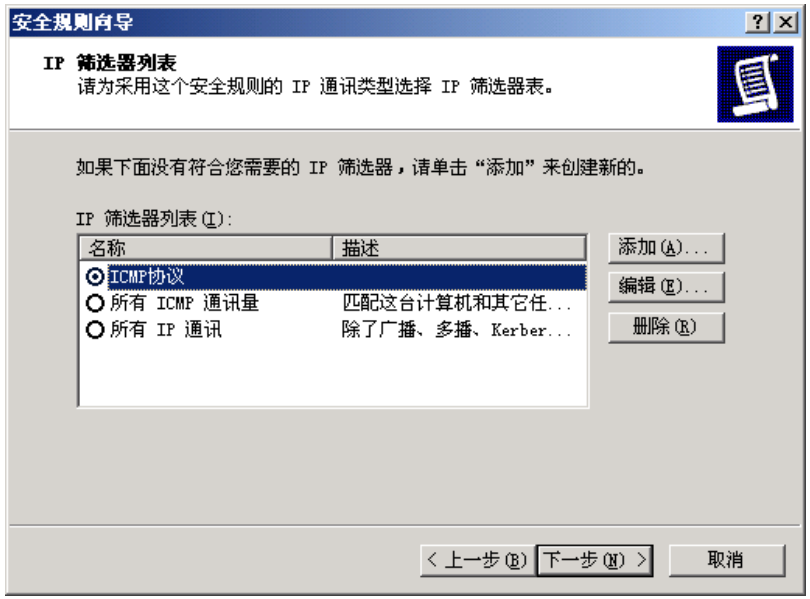


- 创建IP安全策略

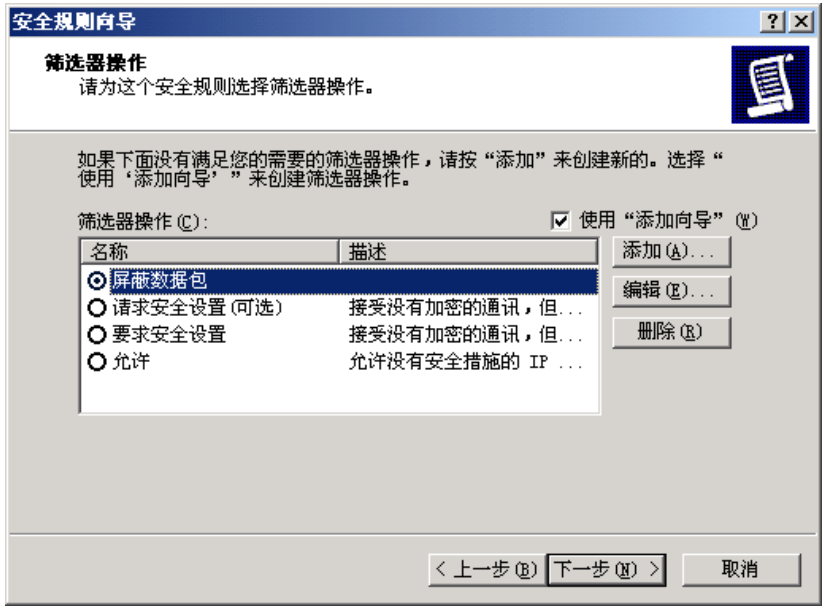
- 输入IP安全策略名称

“屏蔽进入的ICMP通讯”

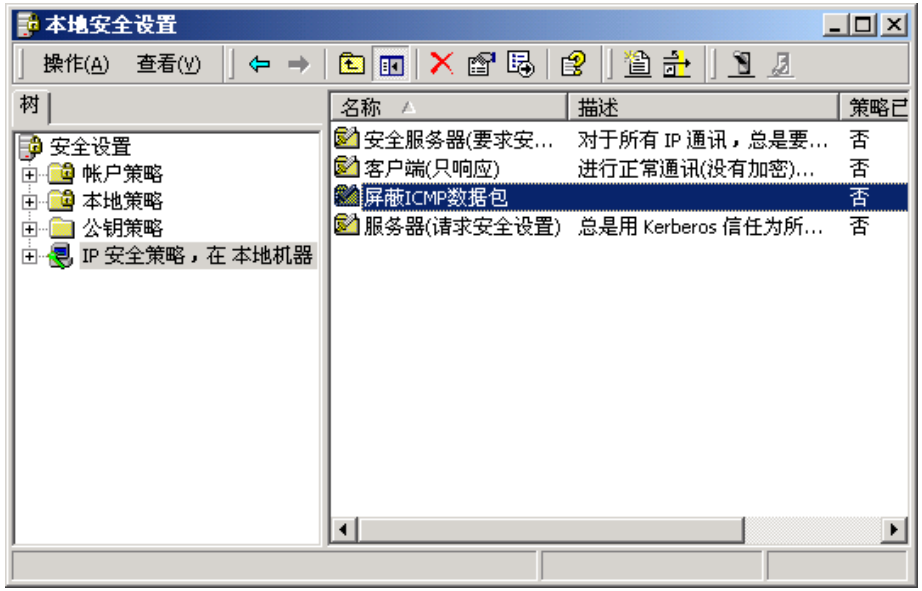




选择IP筛选器列表

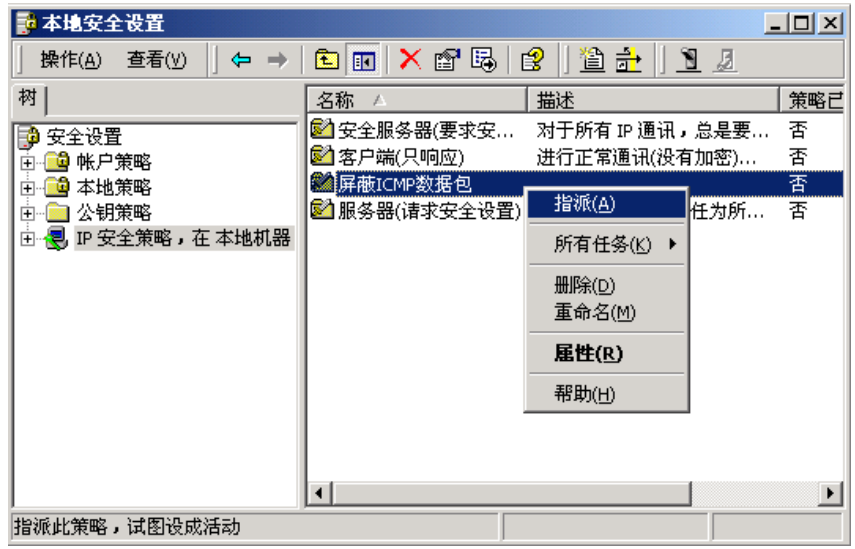


选择筛选器操作



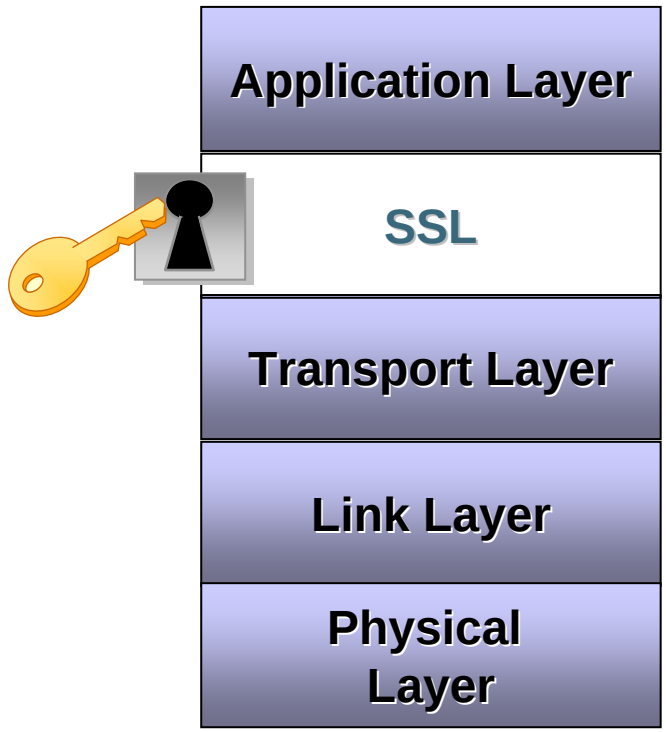
❖添加IP安全策略完毕

❖指派IP安全策略



SSL

- SSL（Secure Socket Layer，安全套接字层）协议是在传输通信协议（TCP）上实现的一种安全协议。
- SSL协议的目标是提供两个应用间通信的保密和可靠性，可在服务器和客户机端同时实现支持。
- SSL提供3种基本的安全服务：
  - 信息加密
  - 信息完整性
  - 相互认证



SSL协议的组成

- SSL记录协议
  - 用于封装不同的上层协议。涉及应用程序提供的信息的分段、压缩、数据认证和加密。
  - SSL v3提供对数据认证用的MD5和SHA以及对数据加密用的R4和DES等的支持。
- SSL握手协议
  - 用来在服务器和客户机在传输应用数据之前，交换版本号、协商加密算法、（相互）身份认证并交换密钥。
  - SSL v3提供对Diffie-Hellman密钥交换算法、基于RSA的密钥交换机制和另一种实现在Fortezza Chip上的密钥交换机制的支持。

SSL协议的实现

- 可为任何TCP/IP应用提供SSL功能的实现：
  - Netscape的实现—SSLref
  - SSLeay
- Internet号码分配当局（IANA）已为具备SSL功能的应用分配了固定的端口号。
  - 带SSL的HTTP（https）：443
  - 带SSL的SMTP（ssmtp）：465
  - 带SSL的NNTP（snntp）：563

SSL安全机制的使用过程

- 客户端与服务器建立连接，服务器把它的数字证书与公共密钥一并发送给客户端。
- 客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器。
- 服务器端使用私人密钥解密会话密钥。
- 客户端和服务器端使用会话密钥建立一个唯一的安全通道。

SSL的典型使用：HTTPS

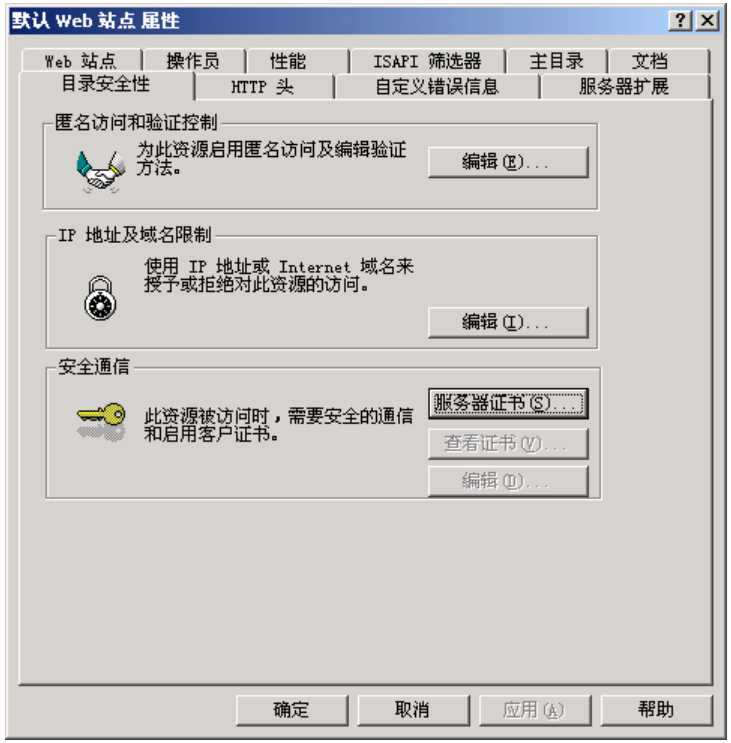
- 应用领域：
  - 需要客户端提交敏感数据的Web站点，如银行、证券、交易等电子商务站点。
- 意义：
  - 利用SSL加密HTTP通道，使得只有受信任的客户才能与该Web站点进行通信。
- 客户端访问特征：
  - https://，而非http://

在Windows 2000系统中使用SSL保护Web站点

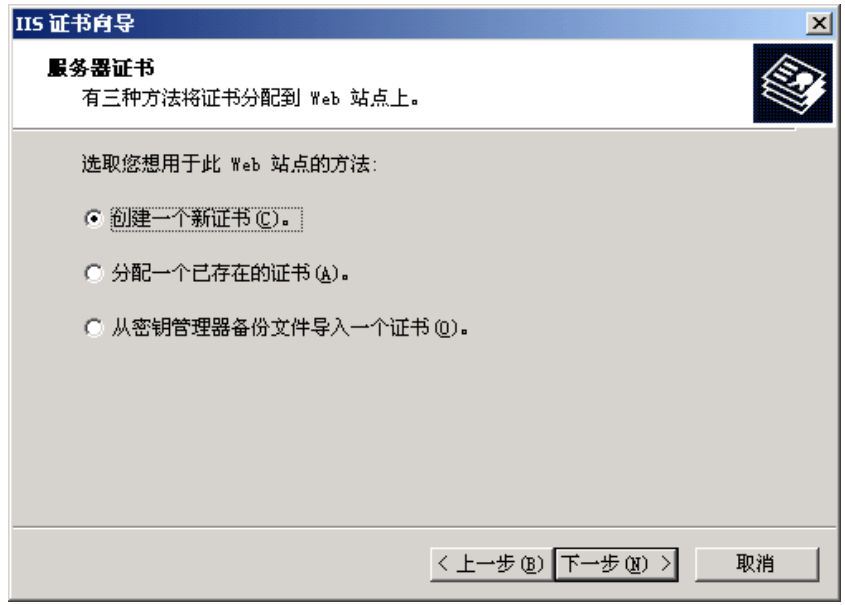
- 获取服务器端证书
  - 从第三方公司获取
  - 使用Windows 2000的“证书服务”和IIS的“服务器证书向导”
- 配置IIS的Web站点属性
  - 目录安全性→安全通信

配置实例

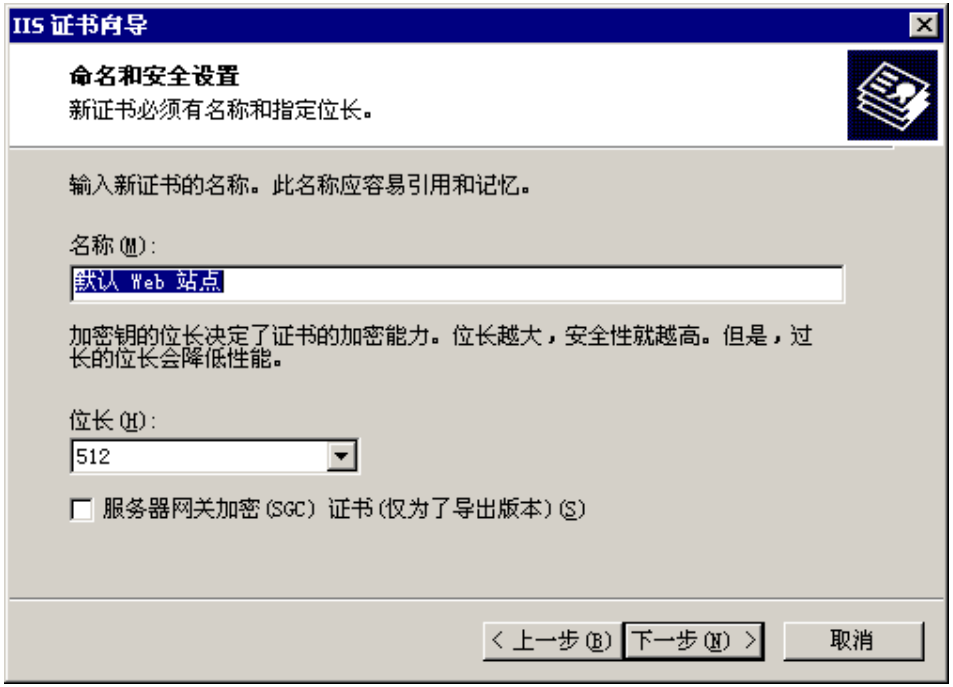
- 安装一台网络上能够到达的证书服务器
  - 通过 “Windows组件向导”→“证书服务”
- 申请服务器证书
  - “Internet服务管理器”→选择Web站点→“属性”→“目录安全性”→ “安全通信”



- 点击“服务器证书”



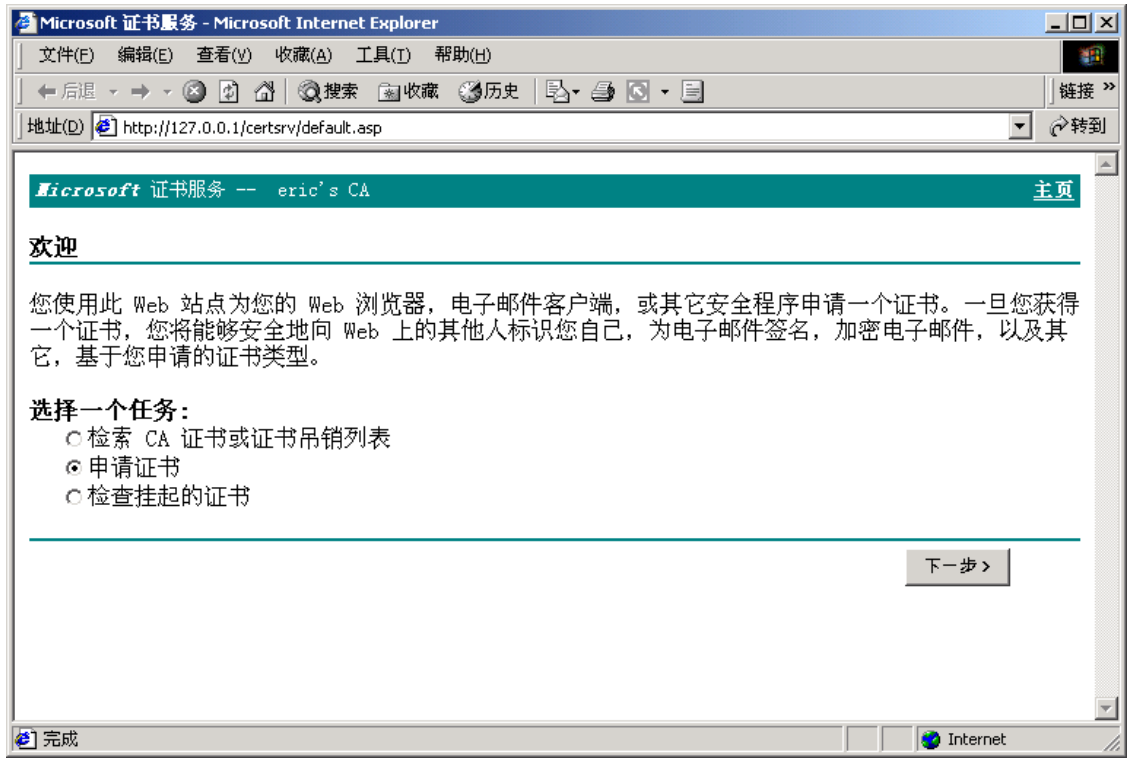
- 创建一个新证书



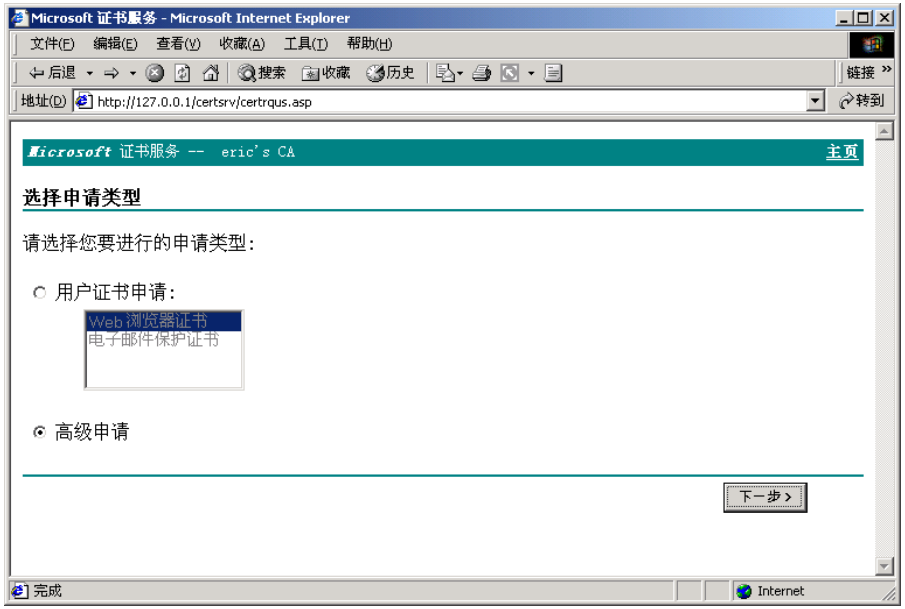
- 按照“IIS证书向导”的提示，输入默认的站点名称、加密位长、组织信息、站点公用名称、地理信息以及证书请求的本地保存文件名

（C:\certreq.txt ）

- 浏览
  http://证书服务器地址/CertSrv/default.asp

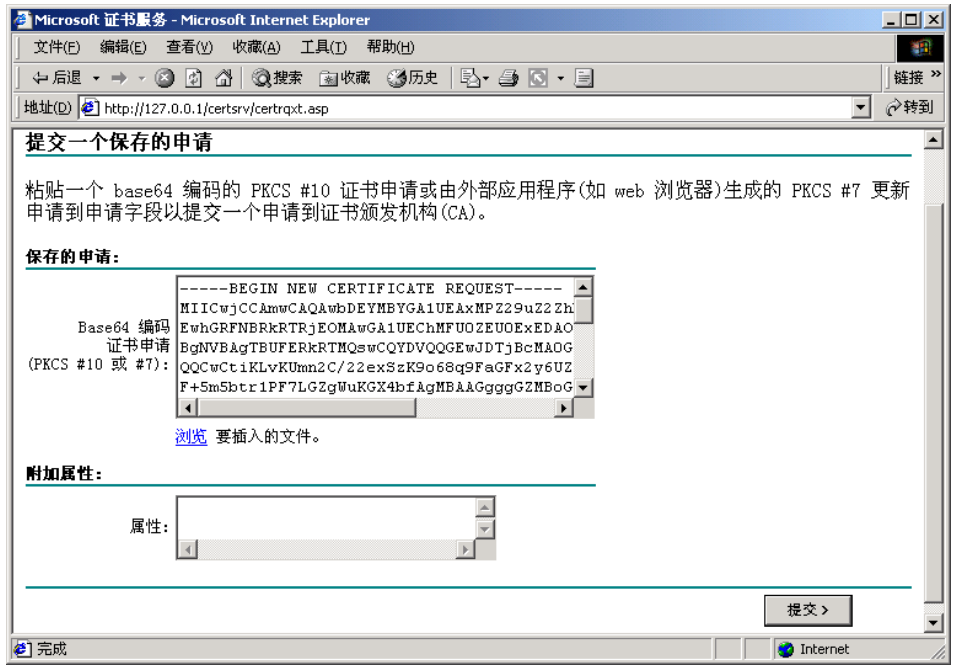


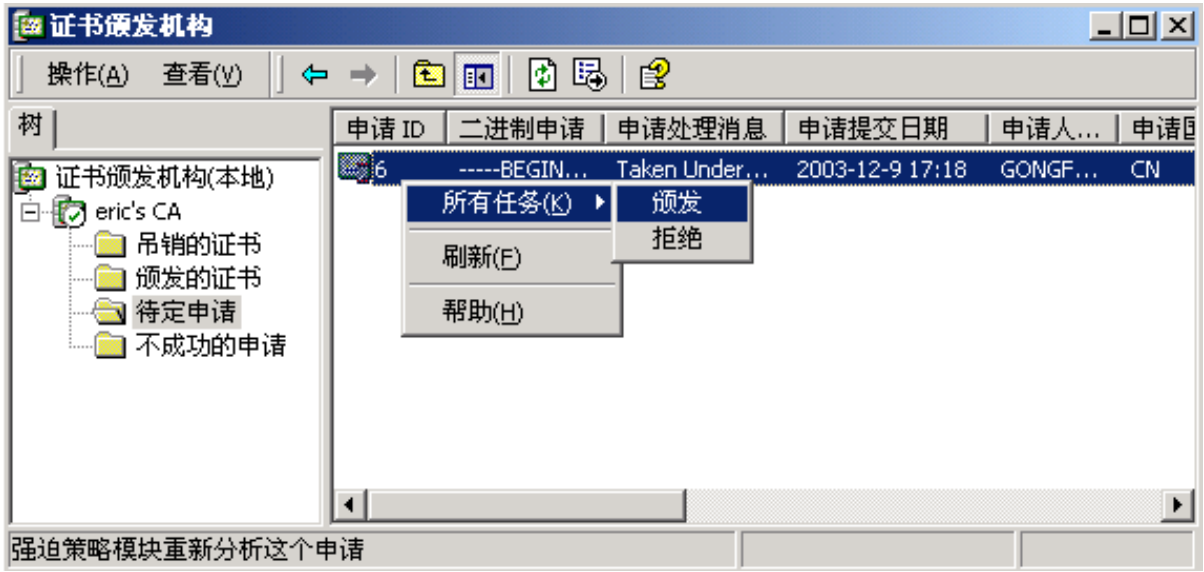
- 选择申请证书



❖选择高级申请

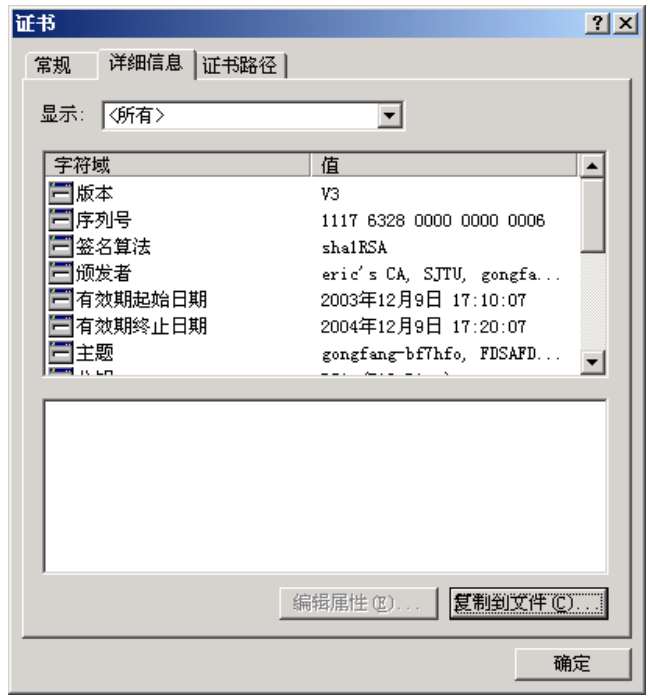
❖选择Base64编码方式，然后粘贴certreq.txt文件的内容，最后提交证书申请

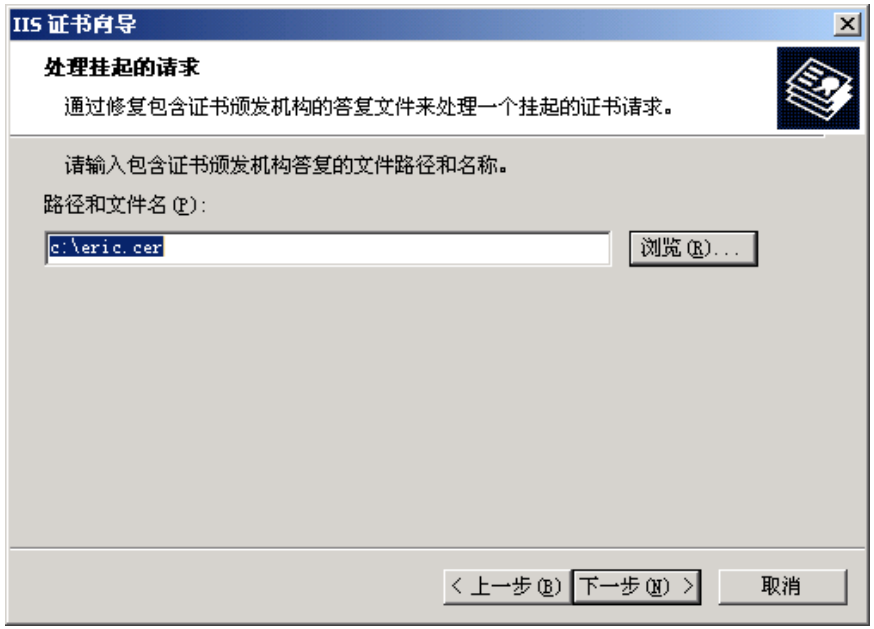




- 证书服务器通过“管理工具”→“证书颁发机构”颁发刚才挂起的申请证书

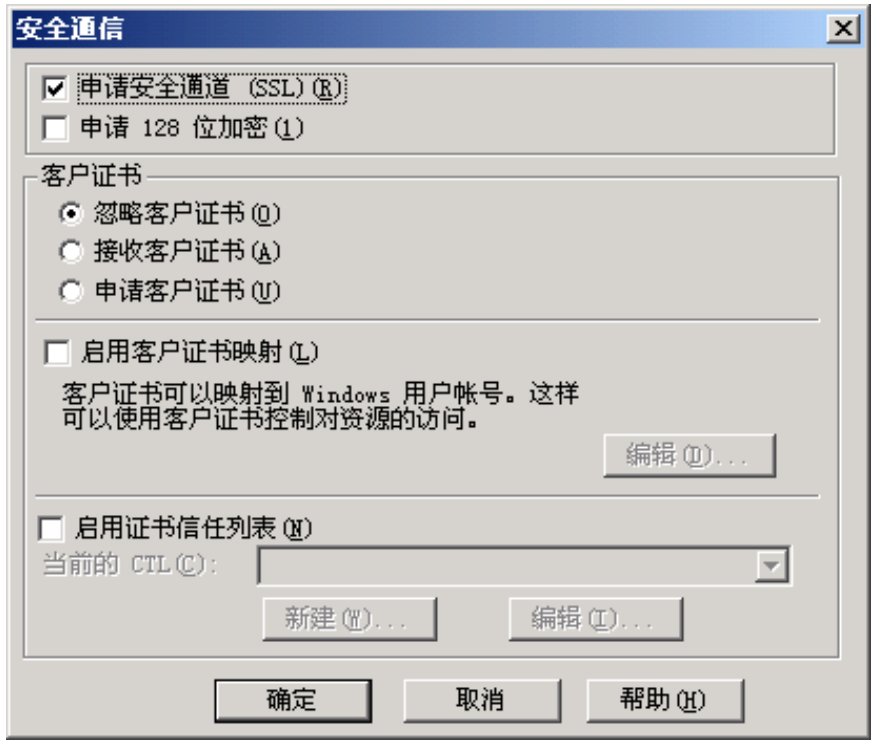
- 导出服务器证书到本地





- 回到Web站点的证书申请，出现“挂起的证书请求”，导入服务器证书。

- 设置Web站点的安全通信属性
  - 服务端证书提供
  - 加密强度
  - 客户端证书提供
  - 客户证书映射
  - 证书信任列表



“安全通信”属性的设置

- “申请安全通道（SSL）”选项
  - 不选中：允许客户端选择是否使用SSL加密传输。
  - 选中：要求客户端必须使用SSL加密传输
- “申请128位加密”选项
  - 选中：要求客户端的浏览器必须支持128位的加密程度。（建议设为不选中）
- “客户证书”选项
  - 忽略客户证书：允许任何客户访问。
  - 接受客户证书。
  - 申请客户证书：需要客户提供客户证书或者服务器端信任的证书才能访问。

该网页必须通过安全频道查看

您要查看的网页要求在地址中使用“https”。

请尝试下列操作：

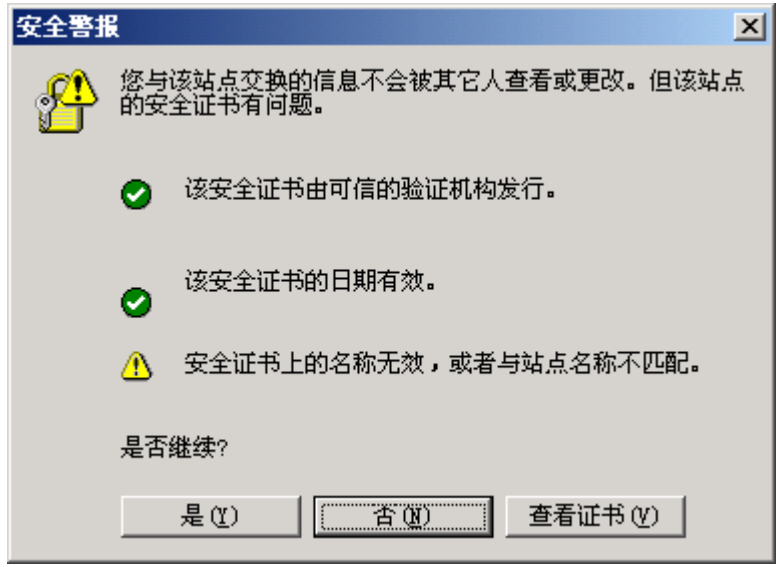
- 在您要访问的地址前面键入“https:”，然后重试。

HTTP 403.4 - 禁止访问：要求 SSL
Internet 信息服务

技术信息（支持个人）

- 背景：
  此错误表明您要访问的网页使用了安全套接字层 (SSL) 安全保护。
- 详细信息：
  Microsoft 支持

要求SSL访问



服务器端证书

客户端证书

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消