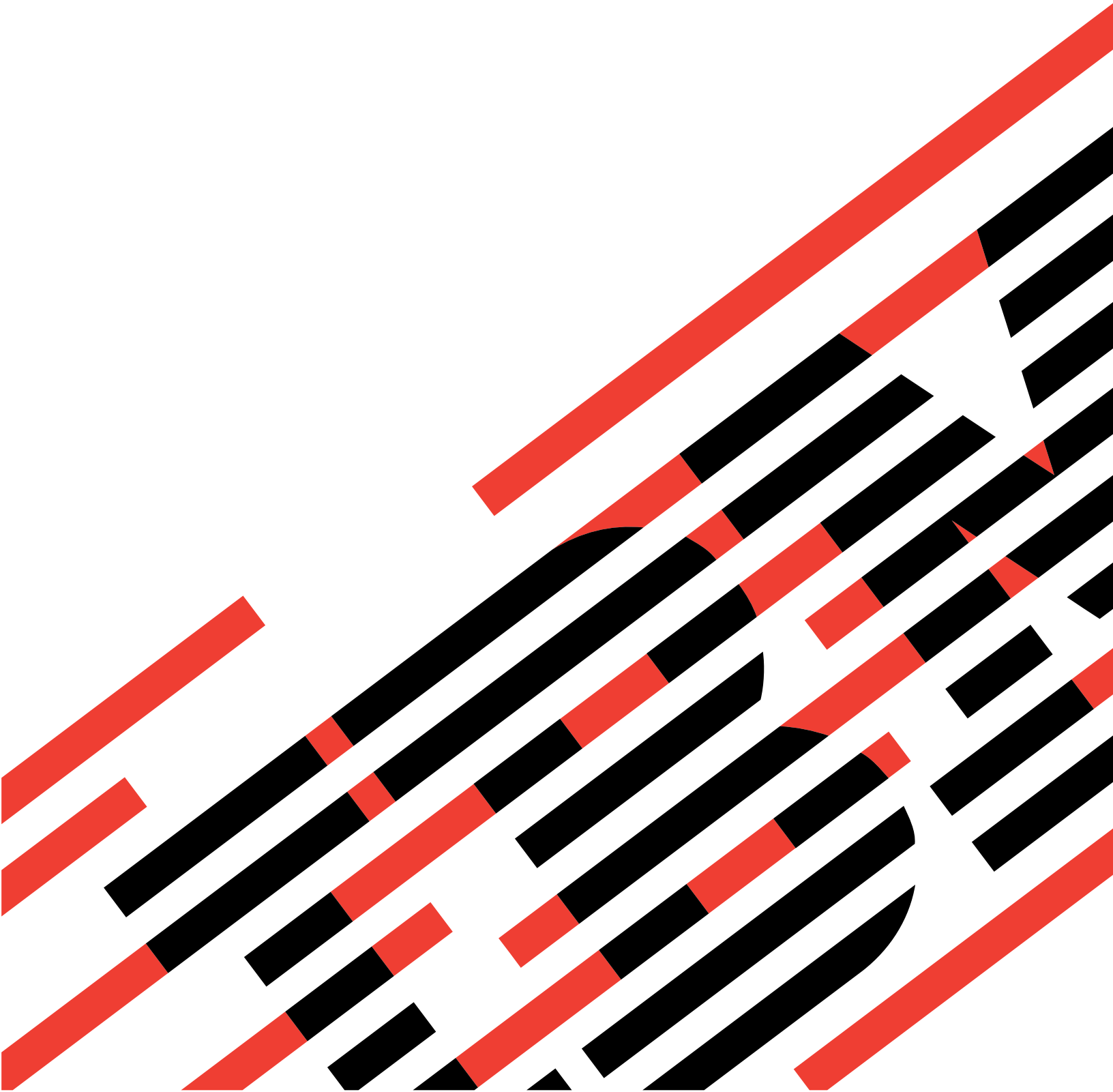
IBM

eserver

iSeries

iSeries 与因特网安全性

版本 5 发行版 3



IBM

@server

iSeries

iSeries 与因特网安全性

版本 5 发行版 3

注意

在使用本资料及其支持的产品之前，请确保阅读第 39 页的『声明』中的信息。

第 6 版（2005 年 8 月）

本版本适用于 IBM Operating System/400（产品号 5722-SS1）V5.3.0 及所有后续发行版和修订版，直到在新版本中另有声明为止。本版本不能在所有精简指令集计算机（RISC）机型上运行，也不能在 CISC 机型上运行。

目录

第 1 部分 iSeries 与因特网安全性

在您的网络发展过程中从 LAN 访问因特网是网络的巨大进步，它也需要重新鉴定您的网络安全性需求。幸运的是，iSeries™ 服务器有集成软件解决方案和安全性体系结构，允许您构建强大的防御系统以防止因特网潜在的安全性缺陷和入侵者。正确使用这些 iSeries 安全性产品，将确保您的客户、职员和业务合作伙伴可在安全的环境中获取他们与您进行商务往来所需的信息。

在此处找到的信息可帮助您了解有关众所周知的安全性威胁，以及这些风险如何危及您的因特网和电子商务目标。此外，您还将了解如何评定风险与使用 iSeries 为对付这些风险所提供的各种安全性选项所带来的利益关系。最后，就可以确定如何使用此信息开发适合您的商务需要的网络安全性规划。可以确保安全策略。

要了解有关因特网的安全性风险及可以用来保护系统与资源的 iSeries 安全性解决方案的更多知识，查看此信息:

- **打印本主题**
  使用此信息访问并打印本主题的 Adobe Acrobat 版本。
- **iSeries 与因特网安全性注意事项**
  使用此信息获取对电子商务 iSeries 安全性实力以及可用的 iSeries 安全性产品的大致了解。
- **规划因特网安全性**
  使用此信息了解如何创建满足您的因特网和电子商务安全性需求的安全策略。
- **iSeries 基本因特网就绪的系统安全级别**
  使用此信息了解在连接到因特网之前，您应该具有的适当的系统安全级别。
- **网络安全性选项**
  使用此信息了解为保护内部资源，您应考虑使用网络级别安全性措施。
- **应用程序安全性选项**
  使用此信息了解许多通用因特网应用程序和服务的常见因特网安全性风险，及处理这些风险可采取的措施。
- **传输安全性选项**
  使用此信息了解当数据在不可信网络（如因特网）上流动时可用于对其保护的安全性措施。了解有关使用“安全套接字层”（SSL）、iSeries Access Express 和“虚拟专用网”（VPN）连接的安全性措施的更多信息。
- **iSeries 因特网安全性选项**
  使用有关 iSeries 安全性选项的简短讨论，帮助您选择保护基于因特网使用和电子商务计划的系统和资源的产品。

注: 如果您对安全性和与因特网相关的术语还不熟悉，当您看完此资料后，可查看常见安全性术语。

第 1 章 打印本主题

可以查看或下载本文档的 PDF 版本以供查看或打印。必须安装 Adobe Acrobat Reader 来查看 PDF 文件。可从 Adobe 主页下载副本。 

要查看或下载 PDF 版本，选择《iSeries 与因特网安全性》（416 KB 或 60 页）。

要将 PDF 保存在工作站上以查看或打印:
1. 在浏览器中打开 PDF（单击上面的链接）。
2. 在浏览器的菜单上，单击**文件**。
3. 单击**另存为...**
4. 浏览至要保存该 PDF 的目录。
5. 单击**保存**。

第 2 章 iSeries 与因特网安全性注意事项

当 iSeries 所有者研究将系统连接至因特网的各个选项时，您通常将会询问的前几个问题之一是“如何开始将因特网用于商业目的？”第二个问题是: “关于安全性与因特网，我应该知道些什么？”。这份资料将重点帮助您解答第二个问题。

“关于安全性与因特网，我应该知道些什么？”这个问题的答案取决于您希望如何使用因特网。有关因特网的安全性问题是很重要的。您需要解决的问题基于您计划使用因特网的方式。您最初涉足因特网可能是向内部网络用户提供 Web 访问和因特网电子邮件。还可能希望具有将敏感信息从一个站点传送到另一个站点的能力。最后，您还可能计划使用因特网来进行电子商务，或在您的公司与业务合作伙伴和供应商之间创建外部网。

涉足因特网之前，应该思考希望做什么及如何去做。确定如何使用因特网及其安全性比较复杂。开发自己的因特网使用计划时，查看方案: JKL 玩具公司电子商务计划页面会有所帮助。（注: 如果对安全性和与因特网相关的术语不熟悉，看完此资料之后，可查看常见安全性术语。）

一旦明白了打算如何使用因特网进行电子商务以及安全性问题、可用的安全性工具、功能和产品，您就可以制定安全策略和目标。许多因素都将影响在制定安全策略时所做的选择。将组织扩展到因特网上之后，安全策略就是确保系统与资源安全的关键基石。

iSeries 服务器系统安全性特征

除了许多用来在因特网上保护系统的特定安全性产品之外，Series 服务器还拥有很强的系统安全性特征，如下所述:

- 集成安全性，与其它系统所提供的附加安全性软件包相比，很难绕过此功能。
- 基于对象的体系结构，使得创建与传播病毒在技术上十分困难。在 iSeries 服务器上，文件不能假装成程序，一个程序也不能更改另一个程序。iSeries 完整性功能部件需要使用系统提供的接口访问对象。不能 由对象在系统中的地址直接访问对象。不能偏移和将其改变为指针，或“加工”指针。指针操作是黑客在其它系统体系结构上常用的一种技术。
- 适应性允许设置系统安全性以满足特定需求。您可以使用 @server Security Planner 来帮助您确定哪种安全性建议适合您的安全性需要。

iSeries 高级安全性产品

iSeries 还提供几种特定的安全性产品，在连接到因特网时可用来提高系统安全性。取决于使用因特网的方式，可以利用以下产品中的一种或多种:

- 虚拟专用网（VPN）是一种企业专用内部网通过公共网络（如因特网）的扩展。可以使用 VPN 创建安全专用连接，主要是通过创建公共网络上的专用“隧道”来实现。VPN 是可从“iSeries 导航器”界面获得的 OS/400® 的集成功能部件。
- 信息包规则是可从“iSeries 导航器”获得的 OS/400 的集成功能部件。此功能部件允许配置 IP 信息包过滤规则和网络地址转换（NAT）规则以控制进出 iSeries 服务器的 TCP/IP 流量。
- “安全套接字层”（SSL）应用程序通信安全性允许配置应用程序以使用 SSL 来建立在服务器应用程序与其客户机之间的安全连接。最初开发 SSL 是为了保护 Web 浏览器和服务器应用程序，但也可以启用其它的应用程序以使用 SSL。许多 iSeries 服务器应用程序现在支持 SSL，包括 IBM® HTTP Server for iSeries、iSeries Access Express、文件传输协议（FTP）、Telnet 和许多其它的应用程序。

一旦了解了打算如何使用因特网以及安全性问题、可用的安全性工具、功能和产品，就可以制定安全策略和目标。许多因素都将影响在制定安全策略时所做的选择。将组织扩展到因特网上之后，安全策略为保护系统安全提供了关键基石。

注: 要查找有关如何开始使用因特网以开展业务的更详细信息，请参阅以下在线“信息中心”主题和 IBM 红皮书:

- *连接到因特网*
- *AS/400® Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929).

第 3 章 规划因特网的安全性

制定因特网使用计划时，必须仔细规划因特网安全性需求。必须收集有关因特网使用计划的详细信息并记录内部网络的配置。基于收集此类信息的结果，可以准确地评估您的安全性需要。

例如，您应该记录并描述如下各项:
- 当前网络配置。
- DNS 和电子邮件服务器配置信息。
- 与“因特网服务提供商”（ISP）的连接。
- 希望使用因特网上的什么服务。
- 希望对因特网用户提供什么服务。

记录此类信息有助于确定哪里有安全性漏洞且需要使用何种安全性措施以将这些漏洞最小化。

例如，您决定想允许内部用户使用 Telnet 连接到位于专用的研究位置的主机。内部用户需要此服务以帮助他们为公司开发新的产品。然而，您有些担心机密数据在因特网上不受保护的流动。如果竞争对手捕获并利用了此数据，则您的公司可能会面临财务风险。确定了使用需求（Telnet）和相关的风险（暴露机密信息）后，可以确定应该实现的附加安全性措施以确保对这种使用（启用“安全套接字层”（SSL））的数据机密性。

在制定因特网使用与安全性规划时，复查以下主题会很有帮助:
- **安全性的分层防御方法**提供了有关涉及创建综合安全性规划问题的信息。
- **安全策略和目标** 提供了帮助您深入了解涉及创建综合安全性规划问题的信息。
- **方案: JKL 玩具公司电子商务计划**提供了当您创建自己的企业因特网使用和安全性规划时可以使用的典型实例的实用模型。

安全性的分层防御方法

安全策略定义希望保护的内容及期望系统用户做什么。它在设计新的应用程序或扩展当前网络时提供了安全性规划的基础。它描述了用户的职责（如保护机密信息和创建非无效的密码）。

注: 需要为组织创建和制定安全策略以将内部网络风险最小化。如果对 iSeries 400 的固有安全性功能配置正确，则它可将许多风险降到最低。但是，当将 iSeries 系统连接到因特网时，需要提供附加安全性措施以确保内部网络的安全。

许多风险与使用因特网访问进行商务活动关联。在创建安全策略时，必须使提供服务与控制对功能及数据的访问之间保持平衡。使用联网的计算机，保持安全性更加困难，因为通信信道自身是开放的，容易受到攻击。

一些因特网服务 比其它服务更容易受到某些类型的攻击。因此，了解想要使用或提供的每个服务所强加的风险，非常关键。此外，了解可能的安全性风险会帮助您确定一系列明确的安全性目标。

因特网是对因特网通信安全性造成威胁的各种个体的发源地。下面的列表描述了可能遇到的一些典型安全性风险:
- **被动攻击**: 在被动攻击的情况下，作恶者只是监控网络流量以尝试获取秘密。这种攻击可以是基于网络的（跟踪通信链路）或者基于系统的（用“特洛伊木马”程序替换系统组件以在不知不觉中捕获数据）。检测被动攻击很困难。因此，您应该假定有人在窃听您在因特网上发送的一切消息。
- **主动攻击**: 在主动攻击的情况下，作恶者尝试突破防御进入网络系统。主动攻击有以下几种类型:
  - 在**试图访问系统**时，攻击者试图利用安全漏洞来获取对客户机或服务器系统的访问和控制。

- 在**电子欺骗** 攻击的情况下，攻击者试图通过假冒成可信系统来突破防御，或者某用户劝说您向他发送秘密信息。
- 在**拒绝服务攻击**情况下， 攻击者尝试通过重定向流量或用垃圾邮件轰击系统来干扰或关闭您的操作。
- 在**密码攻击**情况下，攻击者将试图猜测、偷取您的密码或者使用专门工具尝试对加密的数据解密。

多层防御

因为潜在的因特网安全性风险可能会发生在各种级别上，需要设置提供多层防御的安全性措施来避免这些风险。通常，当您连接到因特网时，不应对**是否**会遇到入侵尝试或拒绝服务攻击感到疑惑。而是应该认为**将会**遇到安全性问题。因此，最好的防御措施是周密的主动进攻。规划因特网安全策略时，使用分层方法可确保穿过一层防御的攻击者会被后续层阻止。

安全策略应包括对传统网络计算模型下面各层提供保护的措施。通常，您应该从最基本的（系统级别安全性）到最复杂的（事务级别安全性）来规划安全性。

系统级别安全性

系统安全性措施是防御基于因特网安全性问题的最后防线。因此，制定整个因特网的安全策略的第一步必须是正确配置 iSeries 基本系统安全性设置。

网络级别安全性

网络安全性措施控制对 iSeries 及其它网络系统的访问。将网络连接到因特网时，应该确保已有足够的网络级别安全性措施以保护内部网络资源不受未经授权的访问和入侵。防火墙是提供网络安全性的最常见的方式。“因特网服务提供商”（ISP）能够并且应该对您的网络安全性规划提供重要的元素。网络安全性计划应该概要地描述 ISP 所要提供的安全性措施（如 ISP 路由器连接的过滤规则及公共“域名服务”（DNS）预防措施）。

应用程序级别安全性

应用程序级别安全性措施控制用户与特定应用程序交互的方式。通常，您应该对所使用的每个应用程序都配置安全性设置。但是，对那些将从因特网使用或向因特网提供的应用程序和服务，应该特别注意设置安全性。未经授权的用户寻找途径以访问网络系统，使这些应用程序和服务很容易被滥用。决定要使用的安全性措施需要考虑服务器端和客户机端的安全漏洞。

传输级别安全性

传输级别安全性措施保护网络内部及网络间的数据通信。在不可信网络（如因特网）上通信时，无法控制流量从源到目的地的流动方式。它传输的流量与数据通过了许多无法控制的不同服务器。除非设置安全性措施（如配置应用程序以使用“安全套接字层”（SSL）），否则路由的数据可供任何人查看和使用。当数据在其它安全级别边界之间的流动时，传输级别安全性措施保护数据。

开发整个因特网安全策略时，应该对每个层单独开发安全策略。另外，您应该描述每套策略与其它策略的交互方式以对您的业务提供综合的安全性网络。

安全策略和目标

您的安全策略

您所使用或提供的每个因特网服务都会对 iSeries 系统和与之连接的网络造成风险。安全策略是一套规则，适用于属于某个组织的计算机和通信资源的活动。这些规则包括了几个区域（如物理安全性、人员安全性、管理安全性和网络安全性）。

安全策略定义希望保护的内容及期望系统用户做什么。它在设计新的应用程序或扩展当前网络时提供了安全性规划的基础。它描述了用户的职责（如保护机密信息和创建非无效的密码）。安全策略还应该描述将如何监控安全性措施的有效性。这种监控可帮助您确定是否有人正试图绕过您的安全措施。

要制定安全策略，必须明确定义安全性目标。创建了安全策略之后，必须采取措施来实施其所包含的规则。这些步骤包括训练员工并添加必需的软件和硬件来实施该规则。另外，当更改计算环境时，应该更新安全策略。这是为了确保处理更改所带来的任何新风险。可在“iSeries 信息中心”的“基本系统安全性与计划”主题下查找 JKL 玩具公司的安全策略示例。

您的安全性目标

创建并执行安全策略时，必须有明确的目标。安全性目标分为以下一种或几种类别:

资源保护

资源保护方案确保只有已授权的用户才能访问系统中的对象。保护所有类型系统资源的能力是 iSeries 的实力。您应该谨慎定义能够访问您的系统的不同类别的用户。还应该定义您希望授予这些用户组的访问权限并将其作为创建安全策略的一部分。

认证 会话另一端的资源（人或机器）确实是它所声称的确保或验证。可靠的认证可保护系统免受假冒的安全性风险，即发送方或接收方使用假身份来访问系统。通常，系统使用密码和用户名进行认证；数字证书能提供更安全的认证方法同时也能提供其它安全性利益。当将系统链接到公共网络（如因特网）时，用户认证变得更加复杂。因特网和内部网之间的重要差别在于您信任注册的用户身份的能力，因此，应该认真考虑这个想法 – 使用比登录程序提供的传统的用户名和密码更强的认证方法。基于用户的授权级别，已认证用户可以拥有不同类型的许可权。

授权 允许会话的另一端的个人或计算机具有执行请求的许可权的保证。授权是确定谁或什么可以访问系统资源或在系统上执行某种活动的过程。通常，授权在认证的上下文中执行。

完整性 到达信息与发送信息相同的保证。了解完整性要求您理解数据完整性和系统完整性的概念。

- **数据完整性**: 保护数据不受未授权的更改或篡改。数据完整性防御操作安全性风险，即某人拦截和更改未对他／她授权的信息。除保护存储在网络中的数据之外，当数据从不可信的源进入系统时，可能需要附加安全性来确保数据完整性。当进入系统的数据来自公共网络时，可能需要安全性方法，因此请执行以下操作:
  - 通常采用将数据加密的手段来保护数据不被“窃听”和解释。
  - 确保数据的传输没有改变（数据完整性）。
  - 证实传输发生（不可抵赖性）。将来可能需要已注册或认证的邮件的电子等效物。
- **系统完整性**: 系统按预期性能提供一致的和预期的结果。对于 iSeries，系统完整性是通常最容易忽视的安全性组件，因为它是 iSeries 体系结构的基础部件。例如，当使用安全级别 40 或 50 时，iSeries 体系结构就使得作恶者模仿或更改操作系统程序变得异常困难。

不可抵赖性

不可抵赖性是发生事务或发送或接收消息的证据。使用数字证书和公用密钥密码术来“签署”事务、消息和文档支持不可抵赖性。发送方和接收方都承认交换发生。数据上的数字签名提供了必需的证据。

机密性 敏感信息保持机密性且对偷看者不可见的保证。机密性对整个数据安全性来说非常关键。通过使用数字证书和安全套接字层（SSL）加密数据有助于确保当通过不可信网络传输数据时数据的机密性。安全策略应着重于如何对网络中的信息以及信息离开网络后提供机密性。

审计技术安全性活动

监控安全性相关的事件以提供包括成功和不成功（被拒绝）访问的记录。成功访问记录告诉您谁正在您的系统上做什么，不成功（被拒绝）访问记录告诉您某人正试图破坏您的安全性或某人访问您的系统有困难。

了解安全性目标可帮助您创建包括所有联网和因特网安全性所需要的安全策略。当定义目标和创建安全策略时，查看 JKL 玩具公司的电子商务方案会有所帮助。该方案中的公司的因特网使用和安全性规划是许多现实生活实现的代表。

方案: JKL 玩具公司电子商务计划

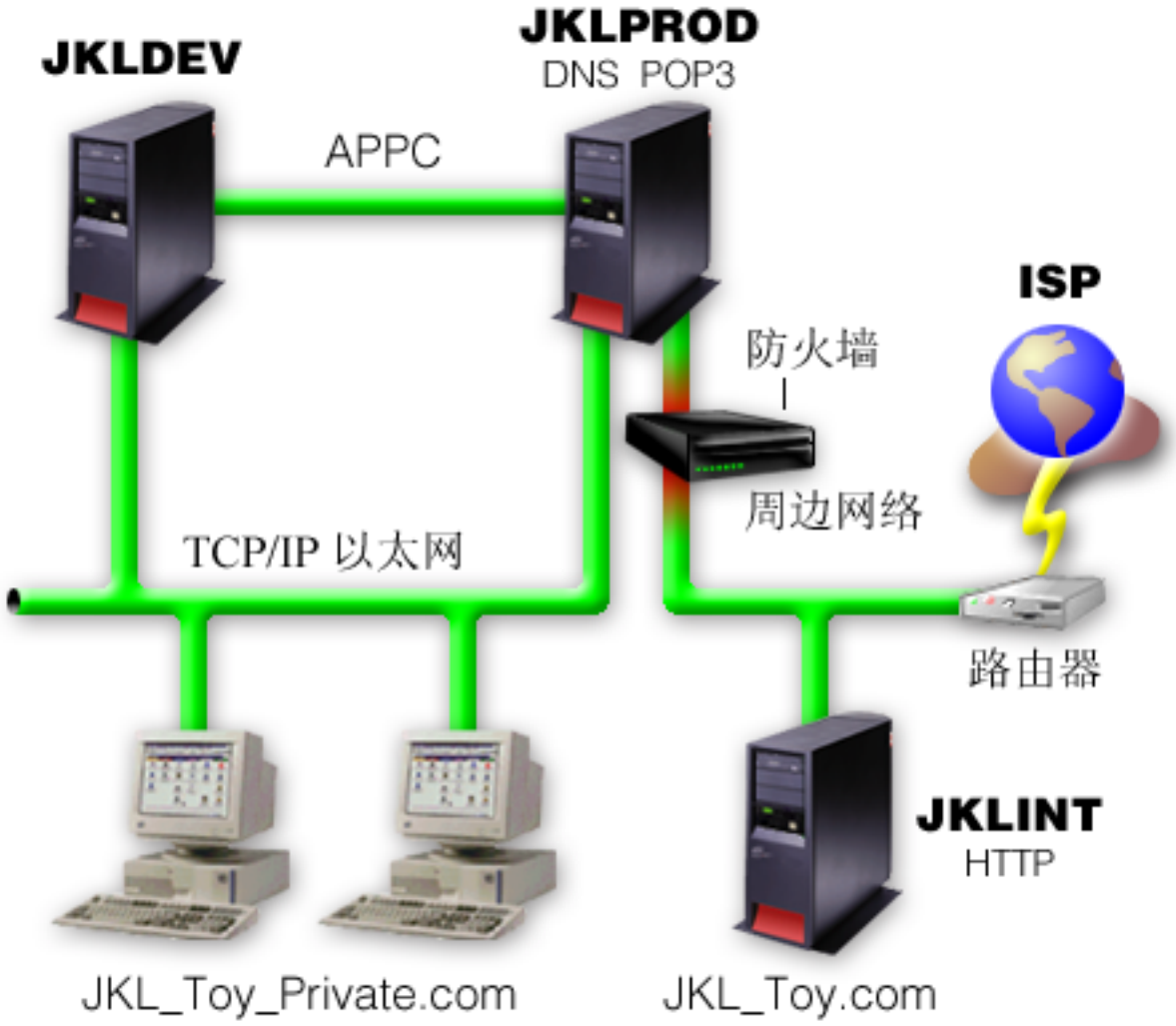
此方案描述了一个典型的企业 JKL 玩具公司,该公司已决定通过使用因特网扩展其业务目标。虽然该公司是虚构的，但其将因特网用于电子商务的计划及其引发导致的安全性需求对于现实生活中许多公司的情况来说是具有代表性的。

JKL 玩具公司是一家小型但快速成长的玩具制造公司，其产品有跳绳、风筝以及可爱的美洲豹。公司总经理非常关心业务的发展，及其新的 iSeries 系统能如何减轻发展的负担的问题。财务部经理 Sharon Jones 负责 iSeries 系统管理和系统安全性。

JKL 玩具公司对其内部应用程序已成功使用其安全策略有一年多的时间。现在公司计划建立内部网以更有效地共享内部信息。公司还计划着手使用因特网以促进其业务目标的实现。这些目标中包括创建公司因特网营销计划，其中包括联机产品目录。他们还希望能使用因特网将敏感信息从远程站点传送回公司总部。另外，公司还希望允许设计研究室的职员为了研究开发之目的拥有因特网访问权。最后，公司希望允许客户使用其 Web 站点直接进行在线购买。Sharon 正在写一个报告，描述关于这些活动特定的潜在安全性风险及公司应采取何种安全性措施使这些风险降到最低。Sharon 将负责更新公司安全策略并实施公司决定采用的安全性措施。

使用这种增强的因特网的目标如下所述
- 全面提升公司形象并作为整个营销活动的一部分。
- 为客户和销售人员提供在线产品目录。
- 改善客户服务。
- 为职员提供电子邮件和万维网访问权。

确保了其 iSeries 服务器具有强的基本系统安全性之后，JKL 玩具公司决定购买并使用防火墙产品以提供网络级别的保护。防火墙将保护其内部网络免受许多潜在的与因特网相关的风险。以下是公司因特网／网络配置的图示说明。



如图中所示，JKL 玩具公司有两个基本的 iSeries 服务器。他们将一个系统用于开发（JKLDEV），另一个系统用于生产（JKLPROD）应用程序。这两个系统都处理关键任务数据和应用程序。因此，他们对在这些系统上运行其因特网应用程序感到担心。而他们选择了添加新的 iSeries 服务器（JKLINT）来运行这些应用程序。

公司已将新系统安装在周边网络上，并在该周边网络和公司内部主网络之间使用防火墙来确保将其网络与因特网更好地隔离。这种隔离减少了其内部系统容易受到的因特网的攻击风险。通过只将新的 iSeries 指定为因特网服务器，公司也降低了管理其网络安全性的复杂性。

现在公司将不在该新的 iSeries 服务器上运行任何关键任务的应用程序。在其电子商务计划的这个阶段，新系统将只提供一个静态的公共 Web 站点。然而，公司希望实现安全性措施以保护系统及其运行的公共 Web 站点以防止服务中断和其它可能的攻击。因此，公司将用信息包过滤规则和网络地址转换（NAT）规则及强大的基本安全性措施来保护系统。

随着公司开发更高级的公共应用程序（如电子商务 Web 站点或外部网访问），他们将实现更高级的安全性措施。

第 4 章 基本因特网就绪的安全级别

系统安全性措施是防御基于因特网安全性问题的最后防线。因此，制定整个因特网的安全策略的第一步必须是正确配置 OS/400 基本安全性设置。您应该执行以下操作以确保您的系统安全性满足最低需求:

- 将安全级别（QSECURITY 系统值）设置为 50。安全级别 50 提供了完整性保护的最高级别，强烈建议在高风险环境（如因特网）中使用此级别保护您的系统。

  注: 如果您有高度定向的事务或广泛使用“集成文件系统”的应用程序，以安全级别 50 运行可能会导致系统或应用程序性能降级。

  有关每个 iSeries 安全级别的更详细信息，请参阅《保护 iSeries 的技巧与工具》。

  注: 如果当前在低于 50 的安全级别上运行，可能需要更新运行步骤或应用程序。在更改为更高安全级别之前，应查看 iSeries Security Reference  一书中的信息。
- 将安全性相关的系统值设置为至少与 推荐设置的限制级别相同。可以使用 “iSeries 导航器安全性向导” 来配置建立的安全性设置。
- 确保没有用户概要文件（包括 IBM 提供的用户概要文件） 有缺省密码。使用 “分析缺省密码（ANZDFTPWD）命令检查是否有缺省密码。
- 使用对象权限保护重要的系统资源。在系统上使用限制方法。即: 在缺省情况下限制每个人（PUBLIC *EXCLUDE）访问系统资源（如库和目录）。仅允许某些用户访问这些受限资源。在因特网环境中只通过菜单限制访问是不够的。
- **必须**在系统上设置对象权限。有关处理对象权限的更多信息，可以查找《保护 iSeries 的技巧与工具》 中的『iSeries 导航器』一章.

为了帮助您配置这些系统安全性最低需求，可使用 @server **Security Planner**（可从 “@server 信息中心 Web 站点” 获得）或**安全性向导**（可从 “iSeries 导航器” 界面获得）。Security Planner基于您对一系列问题的回答，为您提供一组安全性的推荐设置。然后可以使用这些推荐设置配置您需要的系统安全性设置。基于您对一系列问题的回答， “安全性向导” 也可为您提供推荐设置。与 “安全性顾问程序” 不同，可以让向导使用推荐设置来配置系统安全性设置。

正确配置并管理 iSeries 的固有安全性功能可将许多风险降到最低。然而，当将 iSeries 连接到因特网时，需要提供附加安全性措施以确保内部网络的安全。确保 iSeries 具有了良好的一般系统安全性之后，可准备将附加安全性措施配置为因特网使用综合安全性规划的一部分。

第 5 章 网络安全性选项

与不可信网络连接时，安全策略必须描述一个综合性的安全性计划，包括将在网络级别实现的安全性措施。安装防火墙是部署一系列综合网络安全性措施的最好方法之一。

另外，“因特网服务提供商”（ISP）能够且应该对网络安全性规划提供重要的意见。网络安全性计划应该概要地描述“因特网服务提供商”（ISP）所要提供的安全性措施，如 ISP 路由器连接的过滤规则及公共“域名服务”（DNS）预防措施。

虽然防火墙在整个安全性规划中无疑是主要防御措施之一，但它不应该是**唯一的**防御。由于潜在的因特网安全性风险可能会发生在各种级别上，因此需要设置提供多层防御的安全性措施来避免这些风险。

尽管防火墙提供了免受某类攻击的强大保护，但防火墙只是整个安全性解决方案的一部分。例如，防火墙不一定能够保护通过应用程序（如 SMTP 邮件、FTP 和 TELNET）在因特网上发送的数据。除非选择对此数据进行加密，否则，因特网上的任何人都可在数据传输到其目的地期间访问它。

将 iSeries 服务器或内部网络连接到因特网时，您应着重考虑将防火墙产品用作主要的防御措施。虽然您再不能购买 IBM Firewall for AS/400 产品，而且对该产品的支持也不再可用，但有其它许多可以使用的产品。有关不同的迁移选项详细方案，请参阅 All You Need to Know When Migrating from IBM Firewall for AS/400。

因为商业防火墙产品提供了全面的网络安全性技术，JKL 玩具公司已经在电子商务安全性方案中选择使用一种防火墙产品来保护其网络。然而，他们的防火墙对其新的 iSeries 因特网服务器不提供任何保护，因此，他们选择了实现 iSeries 信息包规则功能部件创建过滤与 NAT 规则来控制因特网服务器的流量。

关于 iSeries 信息包规则

信息包过滤规则允许根据您定义的条件拒绝或者接受 IP 信息包来保护计算机系统。NAT 规则允许通过用一个 IP 地址取代另一个 IP 地址（即，公共 IP 地址）来对外部用户隐藏内部系统信息。尽管 IP 信息包过滤法和 NAT 规则是核心网络安全性技术，但它们不能提供与功能完备的防火墙产品所提供的相同级别的安全性。要决定使用全功能防火墙产品还是 iSeries 信息包规则功能部件时，应该仔细分析您的安全性需求和目标。

查看主题选择 iSeries 网络安全性选项以帮助您确定合适的安全性需求的方法。

防火墙

防火墙是安全内部网络和不可信网络（如因特网）之间的屏障。虽然也可以使用防火墙来保护一个内部网络免受另一个内部网络的侵害，但大多数公司使用防火墙将内部网络安全地连接到因特网上。

在安全内部网络和不可信网络之间，防火墙提供受控的单一联系点（称为阻塞点）。防火墙:
- 允许内部网络用户使用位于外部网络上的授权资源。
- 防止外部网络上的未授权用户使用内部网络上的资源。

使用防火墙作为因特网（或其它网络）的网关时，就在相当程度上降低了内部网络的风险。由于防火墙功能执行许多安全策略指示，因此使用防火墙还使得管理网络安全性更加容易。

防火墙如何工作

要了解防火墙如何工作，将网络想像成您希望控制访问的楼房。楼房有一个作为唯一入口点的门廊。在此门廊里，有迎宾的接待员、监控来宾的保安员、记录来宾行为的摄像机和确认进入楼房的来宾证件阅读器。

这些措施可以很好地控制对楼房进行的访问。但是，如果未经授权的人成功进入楼房，就无法保护楼房不受此闯入者的破坏。然而，如果监控该闯入者的行动，就有机会检测他的任何可疑行为。

防火墙组件

防火墙是硬件和软件的集合，软硬件一起使用时可防止对网络某一部分的未授权访问。防火墙由以下组件组成:

- 硬件。防火墙硬件通常由一台单独的计算机或专门用来运行防火墙软件功能的设备组成。
- 软件。防火墙软件提供多种应用程序。就网络安全性而言，防火墙通过多种技术来提供这些安全性控件:
  - 因特网协议（IP）信息包过滤法
  - 网络地址转换（NAT）服务
  - SOCKS 服务器
  - 多种服务（如 HTTP、Telnet 和 FTP 等）的代理服务器
  - 邮件中继服务
  - 分割域名服务（DNS）
  - 记录
  - 实时监控

注: 一些防火墙提供虚拟专用网（VPN）服务，以便可在您的防火墙和其它兼容的防火墙之间设置加密会话。

使用防火墙技术

可以使用防火墙代理服务器、SOCKS 服务器或者 NAT 规则为内部用户提供对因特网服务的安全访问。代理服务器和 SOCKS 服务器在防火墙处中断 TCP/IP 连接，以便对不可信网络隐藏内部网络信息。服务器还提供附加记录能力。

可以使用 NAT 向因特网用户提供对防火墙后的公共服务器的轻松访问。由于 NAT 隐藏了您的内部 IP 地址，因此防火墙还保护着您的网络。

防火墙还能通过提供防火墙所使用的 DNS 服务器来保护内部信息。实际上，您拥有两台 DNS 服务器: 一台用于有关内部网络的数据，防火墙上的另一台用于有关外部网络和防火墙自身的数据。这允许控制外部访问有关内部系统的信息。

定义防火墙策略时，您可能认为禁止对组织构成风险的任何行为而允许其它任何行为就足够了。然而，由于计算机犯罪者在不断创造新的攻击方法，因此您必须预先考虑防止这些攻击的方法。就象楼房示例一样，您还需要监控是否有人以某种方式突破了防御的迹象。通常，与预防相比，恢复非法进入的损害和花费更大。

在有防火墙的情况下，最佳策略是只允许那些经过测试并信任的应用程序进行访问。如果您遵循此策略，就必须完全定义必须在您的防火墙上运行的服务列表。可以按连接方向（从内向外或从外向内）来定义每个服务的特征。还应该列示用户，您将授权这些用户使用每项服务以及可以对该服务发出连接的机器。

对于保护您的网络，防火墙所能做的

在您的网络和因特网（或其它不可信网络）的连接点之间安装防火墙。这样，防火墙会允许限制您的网络的入口点。防火墙在您的网络与因特网之间提供单一联系点（称为阻塞点）（参阅下图）。因为具有单一联系点，就可以对允许出入网络的流量有更多控制。

防火墙对外界表现为单个地址。防火墙通过代理或 SOCKS 服务器或网络地址转换（NAT）提供对不可信网络的访问，同时隐藏内部网络地址。因此，防火墙维护了内部网络的保密性。将网络信息保密是防火墙用来降低假冒攻击（电子欺骗）可能性的一个途径。

防火墙允许控制出入网络的流量，以将对网络攻击的风险降到最低程度。防火墙安全地过滤所有进入网络的流量，只允许到达特定目的地的特定类型的流量进入。这使某人可能使用 TELNET 或“文件传输协议”（FTP）来访问内部系统的风险降到最低。

对于保护您的网络，防火墙所无法做的

尽管防火墙提供了免受某类攻击的强大保护，但防火墙只是整个安全性解决方案的一部分。例如，防火墙不一定能够保护通过应用程序（如 SMTP 邮件、FTP 和 TELNET）在因特网上发送的数据。除非选择对此数据进行加密，否则，因特网上的任何人都可在数据传输到其目的地期间访问它。

iSeries 信息包规则

iSeries 信息包规则是可从 “ iSeries 导航器”界面获得的OS/400 的集成功能部件。信息包规则功能部件允许配置两种核心网络安全性技术以控制 TCP/IP 流量，保护 iSeries 系统。

- 网络地址转换（NAT）
- IP 信息包过滤法

因为 NAT 和 IP 过滤法是 OS/400 的集成部件，它们为您提供一种经济的途径来保护系统。在一些情况下，这些安全性技术可提供您所需的所有功能而不必另行购买。然而，这些技术并不能创建真正有效的防火墙。取决于安全性需求和目标，可单独使用 IP 信息包安全性，或者与防火墙一起使用。

注: 如果计划保护 iSeries 生产系统的安全，不应试图节省成本。对于这种情况，系统安全性应该优先于成本。为确保对生产系统提供最大限度的保护，应考虑使用防火墙。

NAT 和 IP 信息包过滤法是什么，它们如何一起工作?

网络地址转换（NAT）更改流经系统的信息包的源或目标 IP 地址。NAT 提供防火墙的代理服务器和 SOCKS 服务器的更透明选择。通过使具备不兼容寻址结构的网络互相连接，NAT 还可简化网络配置。因此，可使用 NAT 规则以便 iSeries 系统可用作两个具有冲突或不兼容的寻址方案的网络之间的网关。也可使用 NAT 通过动态替换一个或多个真实地址来隐藏一个网络的真实 IP 地址。因为 IP 信息包过滤法和 NAT 互相补充，通常可一起使用它们以增强网络安全性。

使用 NAT 还使得在防火墙后运行公共 Web 服务器更容易。Web 服务器的公共 IP 地址转换为专用内部 IP 地址。它减少必需的注册 IP 地址的数量并使对现有网络的影响最小化。它还为内部用户提供在访问因特网的同时隐藏专用内部 IP 地址的机制。

IP 信息包过滤法提供基于信息包头信息有选择地阻塞或保护 IP 流量的能力。可在 “iSeries 导航器” 中使用 “因特网设置向导” 快速简易地配置基本过滤规则以阻塞不需要的网络流量。

可使用 IP 信息包过滤法执行以下操作:

- 创建一组过滤规则以指定允许哪些 IP 信息包进入网络以及拒绝哪些访问网络。创建过滤规则时，将它们应用到物理接口（例如，令牌环或以太网线路）。可将规则应用于多个物理接口，或者对每个接口应用不同的规则。
- 创建规则，以允许或禁止基于以下头信息的特定信息包:
  - 目标 IP 地址
  - 源 IP 地址协议（例如，TCP、UDP 等）
  - 目标端口（例如，对于 HTTP 是端口 80）
  - 源端口
  - IP 数据报方向（入站或出站）
  - 转发或本地

- 防止不期望或不必要的流量达到系统上的应用程序。另外，还可防止流量转发到其它系统。这包括低级的不需要特定应用程序服务器的 ICMP 信息包（例如，PING 信息包）。
- 指定过滤规则是否创建包含与系统日志中的规则匹配的信息包信息的记录项。信息写入到系统日志之后，不能更改该记录项。因此，记录是审计网络活动的理想工具。

选择 iSeries 网络安全性选项

预防未授权访问的网络安全性解决方案，通常依靠防火墙技术提供保护。要保护 iSeries 系统，可以选择使用全功能防火墙产品，或者可以选择实施将特定网络安全性技术作为 OS/400 TCP/IP 实现的一部分。这个实现由“信息包规则”功能部件（包括 IP 过滤法和 NAT）和 HTTP for iSeries 代理服务器功能部件组成。

是选择使用“信息包规则”功能部件还是选择使用防火墙，取决于网络环境、访问要求和安全性需求。只要将您的 iSeries 服务器或内部网络连接到因特网或其它不可信的网络上，您应该**首先**考虑将防火墙产品用作主要的防御措施。

在这种情况下，防火墙更为可取，因为防火墙通常是专用的具有有限数目供外部访问接口的硬件和软件设备。使用 OS/400 TCP/IP 技术保护因特网访问时，所使用的就是一个对外部访问开放无数个接口和应用程序的通用计算平台。

出于许多原因，这个差别很重要。例如，专用防火墙产品不提供任何超出构成防火墙自身的其它功能或应用程序。因此，如果攻击者成功绕过防火墙并获得对防火墙的访问，攻击者也不能做出很多攻击。然而，如果攻击者绕过了 iSeries 上的 TCP/IP 安全性功能，攻击者就潜在地能够访问多种有用的应用程序、服务和数据。那时攻击者就可以利用这些对系统自身造成严重破坏或者获得对内部网络中的其它系统的访问。

因此，到底可不可以接受使用 iSeries TCP/IP 安全性功能？象您所做的所有安全性选择一样，您必须将您的决定建立在所希望的成本收益比上。您必须分析业务目标，并决定您希望接受什么样的风险与提供安全性所花费的成本，以使这些风险降到最低。下表提供了有关何时适合使用 TCP/IP 安全性功能或者适合使用全功能防火墙设备的信息。可以使用此表来确定您应该使用防火墙、TCP/IP 安全性功能还是二者的组合来为您的网络和系统提供保护。

安全性技术	OS/400 TCP/IP 技术的最佳使用	全功能防火墙的最佳使用
IP 信息包过滤法	• 要对单个 iSeries 服务器（如公共 Web 服务器或敏感数据的内部网系统）提供**附加**保护。 • 当 iSeries 服务器对于网络的其余部分充当网关（临时路由器）时，保护企业**内部网**的子网。 • 控制与**专用网络**上或 iSeries 服务器在其中充当网关的外部网上的部分可信的伙伴的通信。	• 保护整个企业网络不受**因特网**或您的网络所连接的其它不可信网络的侵害。 • 保护具有很大流量的大型子网不受企业网络的其余子网的侵害。
网络地址转换（NAT）	• 启用具有不兼容寻址结构的两个**专用网络**的连接。 • 在子网中对较不可信网络隐藏地址。	• 隐藏访问**因特网**或其它不可信网络的客户机地址。用作“代理服务器”和“SOCKS 服务器”的替代。 • 使专用网络中的系统服务对**因特网**上的客户机可用。
代理服务器	• 当中央防火墙提供对因特网的访问时，在企业网络的**远程位置**代理。	• 访问**因特网**时，代理整个企业网络。

要了解有关如何使用OS/400 TCP/IP 安全性功能的更多信息，请参阅以下资源:
- 信息包规则（过滤和 NAT）。

- HTTP Server 文档中心。 
- AS/400 Internet Security Scenarios: A Practical Approach  （SG24-5954）。

第 6 章 应用程序安全性选项

应用程序级别安全性措施控制用户与特定应用程序进行交互的方式。通常，您应该对所使用的每个应用程序都配置安全性设置。然而，对那些将从因特网使用或向因特网提供的应用程序和服务，应该特别注意设置安全性。未经授权的用户寻找途径以访问网络系统，使这些应用程序和服务很容易被滥用。您所使用的安全性措施需要同时涉及服务器端和客户机端的安全性漏洞。

尽管保护您所使用的每个应用程序很重要，但安全性措施只占全局安全策略实现的很小一部分。您应该采取的安全性措施

要了解为保护几个公共因特网应用程序您应该做什么的更多信息，查看以下页面:
- 『Web 服务安全性』
- 第 22 页的『Java 因特网安全性』
- 第 24 页的『电子邮件安全性』
- 第 25 页的『FTP 安全性』

Web 服务安全性

在向访问者提供 Web 站点访问时，并不希望将关于如何设置站点和生成页面所使用的编码信息暴露给浏览者。又希望这些访问者可容易、迅速又无缝地访问您的页面，且所有工作都在后台进行。作为管理员，您希望确保安全性习惯不致对 Web 站点有负面影响。将 iSeries 用作 Web 服务器时，应考虑以下几点:

- 客户机可以与 HTTP Server 交互之前，服务器管理员必须为该服务器定义伪指令。有两种创建安全性检查的方法: 常规服务器伪指令和服务器保护伪指令。对 Web 服务器的任何请求，都必须在服务器履行该请求之前就满足这些伪指令所提供的任何及所有限制。
- 通过使用服务器配置的服务器管理 Web 页面可以创建和编辑这些伪指令。服务器伪指令允许控制 Web 服务器的全部行为。服务器保护伪指令允许指定并控制服务器用于 Web 服务器处理的特定 URL 的安全性模型。
- 可以使用映射或发送伪指令及服务器管理 Web 页面以配置服务器。
  - 在 iSeries Web 服务器上使用映射或发送伪指令掩盖文件名。更特别的是，有 PASS 和 MAP 服务器伪指令，用于控制 Web 服务器服务 URL 所用的目录。还可以查找控制 CGI-BIN 程序驻留其中的库的 EXEC 服务器伪指令。

    对每个服务器 URL 定义保护伪指令。虽然不是所有的 URL 都需要保护伪指令，但如果希望控制访问 URL 资源的方式及访问者，那么就需要该 URL 的保护伪指令。
  - 还可以使用服务器“管理 Web 页面”而不是 WRKHTTPCFG（与“HTTP 配置”命令一起使用）并输入这些伪指令来配置服务器。通过命令行接口使用保护伪指令可能非常复杂。因此，建议使用“管理 Web 页面”以确保正确设置伪指令。

  HTTP 提供了显示数据的能力，但不能修改数据库文件中的数据。然而，将需要编写一些应用程序以更新数据库文件。为此，可以使用 CGI-BIN 程序。例如，要创建一些表单，一旦用户填完这些表单，则将更新一个 iSeries 数据库。作为安全性管理员，您应该监控该用户概要文件的权限和 CGI 程序执行的功能。另外，还一定要评估敏感对象可能具有的不适当的公共权限。

注: “公共网关接口”（CGI）是在 Web 服务器与服务器外部的计算机程序之间进行信息交流的业界标准。这种程序可以用 Web 服务器运行其中的操作系统支持的任何编程语言编写。

Web 页面上除了使用 CGI 程序之外，还可使用 Java™。在将 Java 添加到 Web 页面之前，应该了解 Java 安全性。

HTTP Server 提供了访问记录，可以用于监控通过该服务器的访问与试图访问。

代理服务器从 Web 浏览器接收 HTTP 请求并将这些请求重新发送至 Web 服务器。接收到这些请求的 Web 服务器仅仅知道代理服务器的 IP 地址，而不能确定最初发出这些请求的 PC 机的名称或地址。代理服务器可以对 HTTP、“文件传输协议”（FTP）、Gopher 和 WAIS 处理 URL 请求。

还可使用 IBM HTTP Server for iSeries 的 HTTP 代理支持以巩固 Web 访问。代理服务器还可以记录所有 URL 请求以达到跟踪目的，然后可以查看这些记录以监控对网络资源的使用与滥用。

可在《保护 iSeries 的技巧与工具》 一书中查找有关此主题的更多信息。

Java 因特网安全性

在当今的计算环境中，Java 编程日益普及。例如，您可能正在系统上使用 IBM Toolbox for Java 或者 IBM Development Kit for Java 以开发新的应用程序。因此，必须准备处理与 Java 关联的安全性问题。虽然防火墙能够很好地防御大多数常见因特网安全性风险，但它不能对使用 Java 所带的许多风险提供保护。安全策略应该包括保护系统不受涉及 Java 的应用程序、applet 和 servlet 这三个方面干扰的详细信息。还应该了解在 Java 程序的认证和授权方面，Java 和资源安全性是如何进行交互的。

Java 应用程序

作为一种语言，Java 具有一些防止 Java 程序员犯粗心错误的特征，这些粗心错误会导致完整性问题。（其它 PC 机应用程序常用的语言，例如 C 或 C++，不如 Java 那样能有效防止程序员犯粗心错误。）例如，Java 使用强类型化，可防止程序员在无意中使用对象。Java 不允许指针操作，这防止程序员偶然超出程序的内存边界。从应用程序开发的角度来看，可以象查看其它高级语言一样来查看 Java。您对应用程序设计应用的安全性规则应该与在 iSeries 服务器上对其它语言应用的安全性规则相同。

Java applet

Java applet 是可以包括在 HTML 页面的小型 Java 程序。因为 applet 在客户机上运行，这些 applet 所做的会关系到客户机。然而，一个 Java applet 具有访问您的 iSeries 服务器的潜力。（在您的网络中某台 PC 机上运行的 ODBC 程序或高级程序间通信（APPC）程序也能访问您的 iSeries。）通常，Java applet 仅可以与产生它的服务器建立会话。因此，仅当 applet 来自于您的 iSeries 服务器（例如来自于您的 Web 服务器）时，Java applet 才能从一台连接的 PC 机访问您的 iSeries。

Applet 能够试图连接到服务器上的任何 TCP/IP 端口。它并非必须同用 Java 编写的软件服务器进行通话。但是，对于用 IBM Toolbox for Java 编写的服务器，applet 在建立对服务器的连接时必须提供用户标识和密码。这份资料中所描述的所有服务器都是 iSeries 服务器。（用 Java 编写的服务器并不一定要使用 IBM Toolbox for Java）。通常，IBM Toolbox for Java 类在第一次连接时向用户提示用户标识和密码。

仅当用户概要文件具有对那些功能的权限时，applet 才能在 iSeries 服务器执行那些功能。因此，当开始使用 Java applet 来提供新的应用程序功能时，好的资源安全性规划是必要的。当系统处理来自 applet 的请求时，并不使用在用户概要文件中的有限功能值。

Applet 查看器允许在服务器系统上测试 applet; 然而这并不受浏览器安全性限制的限制。因此，您应该仅使用 applet 查看器来测试自己的 applet，而不要从外部源运行 applet。Java applet 经常写入用户的 PC 机驱动器，这就可能给 applet 提供了执行破坏性操作的机会。然而，可以使用数字证书签署 Java applet 以建立其真实性。签署了的 applet 就可以写入 PC 机的本地驱动器，即使浏览器的缺省设置防止这样做。已签署的 applet 还可以写入 iSeries 服务器的映射驱动器，因为对 PC 机来说这些映射驱动器就是本地驱动器。

注: 对于 Netscape Navigator 和 MS Internet Explorer，上面所描述的行为通常也适用。实际所发生的情况取决于您配置和管理所使用的浏览器的方式。

对于从您的 iSeries 服务器产生的 Java applet，可能需要使用已签署的 applet。然而，您应该通知您的用户通常不要接受来自未知源的签署了的 applet。

从 V4R4 开始，可以使用 IBM Toolbox for Java 设置“安全套接字层”（SSL）环境。还可以使用 IBM Developer Toolkit for Java 使 Java 应用程序受 SSL 的保护。将 SSL 与 Java 应用程序配合使用可确保数据的加密，包括在客户机和服务器之间传递的用户标识和密码。可以使用数字证书管理器配置已注册的 Java 程序来使用 SSL。

Java servlet

Servlet 是用 Java 编写的服务器端组件，可动态扩展 Web 服务器的功能而不必更改 Web 服务器代码。随 IBM HTTP Server for iSeries 交付的 IBM WebSphere® Application Server 对 iSeries 系统上使用 servlet 提供支持。

必须在服务器使用的 servlet 对象上使用资源安全性。然而，对 servlet 应用资源安全性并不能足够保护 servlet。一旦 Web 服务器装入 servlet，资源安全性就不能防止其他人也运行该 servlet。因此，除了使用 HTTP Server 安全性控件和伪指令之外，还应该使用资源安全性。例如，不要允许 servlet 仅在 Web 服务器的概要文件下运行。另外，应该通过使用 HTTP Server 组及访问控制表（ACL）来控制可以运行 servlet（保护伪指令中的掩码关键字）的人。还应该使用由 servlet 开发工具（如在 WebSphere Application Server for iSeries 中所找到的）提供的安全性功能。

查看以下资源以了解有关 Java 的一般安全性措施的更多信息:
- IBM Developer Kit for Java Java 安全性。
- IBM Toolbox for Java 安全性类。
- 《保护 iSeries 的技巧与工具》。

Java 对资源的认证与授权

IBM Toolbox for Java 包含安全性类以提供对用户身份的验证，并可选择将该身份分配到正在 iSeries 系统上运行的应用程序或 servlet 的操作系统线程。资源安全性的后继检查以已分配的身份进行。有关这些安全性类的更详细信息，请参阅 IBM Toolbox for Java 认证服务。

IBM Developer Kit for Java 为 Java 认证和授权服务（JAAS）提供支持，JAAS 是 Java 2 Software Development Kit (J2SDK) 标准版的标准扩充。目前，J2SDK 提供访问控制，这种控制基于代码的产生源和代码的签署者（基于代码源的访问控制）。要了解有关使用 J2SDK 的更多信息，请参阅 Java 认证和授权服务。Java 认证和授权服务主题。

用 SSL 保护 Java 应用程序

可以使用“安全套接字层”（SSL）来保护用 IBM Developer Kit for Java 开发的 iSeries 应用程序通信。使用 IBM Toolbox for Java 的客户机应用程序也可以利用 SSL。为自己的 Java 应用程序启用 SSL 的过程与为其它应用程序启用 SSL 的过程有所不同。

有关“安全套接字层”对 Java 应用程序管理的更多信息，请参阅以下“信息中心”主题:

- IBM Toolbox for Java “安全套接字层”（SSL）环境。
- IBM Developer Toolkit for Java 使 Java 应用程序受 SSL 的保护。

电子邮件安全性

在因特网或者其它不可信网络上使用电子邮件存在使用防火墙可能无法保护的安全性风险。您必须了解这些风险以确保您的安全策略描述了如何才能将这些风险将到最低。

电子邮件同其它通信形式一样。通过电子邮件发送任何机密信息之前先要进行判断，这点很重要。因为在收到电子邮件之前，它经过了许多服务器传送，他人很可能拦截且阅读您的电子邮件。因此，您可能要使用安全性措施来保护电子邮件的机密性。

常见电子邮件安全性风险

以下是使用电子邮件所存在的一些风险:

- **溢流**（拒绝服务攻击类型）在系统有多个电子邮件消息而变得过载时发生。攻击者很容易便能创建一个简单的程序，将数百万个电子邮件消息（包括空消息）发送给单个电子邮件服务器以试图使该服务器发生溢流。没有适当的安全性，目标服务器就可能会遇到服务器拒绝，因为无用的消息填充了该服务器的存储磁盘。或者该服务器停止响应，因为所有的服务器资源都参与处理这些攻击邮件。
- **垃圾邮件**（垃圾电子邮件）是另一种常见的电子邮件攻击类型。随着通过因特网提供电子商务业务量的增长，我们收到了大量不需要或未请求的商务性电子邮件。这就是垃圾邮件，这类邮件发送给涵盖范围很广的分发列表上的电子邮件用户，占满了每个用户的电子邮件箱。
- **机密性**是一种通过因特网将电子邮件发送给另一人时存在的风险。此电子邮件到达预期的收件人之前，要通过许多服务器。如果未对消息加密，黑客就可能在电子邮件传输路由上的任何点拦截且阅读您的电子邮件。

电子邮件安全性选项

要预防溢流及垃圾邮件的风险，必须正确配置电子邮件服务器。大多数服务器应用程序提供了对付这些攻击类型的方法。还可以与“因特网服务提供商”（ISP）合作以确保 ISP 提供一些免受这些攻击的附加保护。

所需要的附加安全性措施取决于所需要的机密性级别，以及电子邮件应用程序提供的安全性功能。例如，保持电子邮件消息内容的机密性是否就足够了？或者您是否希望保持与电子邮件关联的所有信息（如源及目标 IP 地址）足够的机密性?

一些应用程序集成了可以对您提供所需要保护的安全性功能。例如 Lotus® Notes® Domino® 提供一些集成安全性功能，包括对整个文档或者文档的个别字段提供加密功能。

为了加密邮件，Lotus Notes Domino 对每个用户都创建了唯一的公用密钥和专用密钥。可以使用专用密钥对消息进行加密，以便该消息只对那些拥有公用密钥的用户可读。必须将公用密钥发送至预期的消息接收方，以便他们能够使用该公用密钥对加密的消息进行解密。如果他人向您发送了加密的邮件，那么 Lotus Notes Domino 将使用发送方的公用密钥为您解密该消息。

可以在程序的联机帮助文件中查找有关使用这些 Notes 加密功能部件的信息。

有关 iSeries 上 Domino 的安全的更详细信息，请参阅以下资料:

- Lotus Domino 引用库  。
- Lotus Notes 用户帮助 Web 站点  。

- Lotus Notes and Domino R5.0 Security Infrastructure Revealed  （SG24-5341）。
- Lotus Domino for AS/400 Internet Mail and More  （SG24-5990）。

如果您希望对在分支办事处、远程客户或者业务合作伙伴之间流动的电子邮件或者其它信息提供更高机密性，有几种选择。

如果电子邮件服务器应用程序支持“安全套接字层”（SSL），则可使用它创建在服务器与电子邮件客户机之间的安全通信会话。当编写客户机应用程序以使用 SSL 时，SSL 也对可选的客户机端认证提供支持。由于整个会话是加密的，因此 SSL 也确保数据传输时的数据完整性。

另一种可用的选择是配置虚拟专用网（VPN）连接。从 V4R4 起，可使用 iSeries 配置多种 VPN 多连接，包括远程客户机与 iSeries 系统之间的连接。使用 VPN 时，在通信端点之间流动的所有流量都被加密，这样可确保数据机密性与数据完整性。

FTP 安全性

FTP（文件传输协议）提供了在客户机（另一系统上的用户）与您的系统之间传输文件的功能。可使用远程命令功能向服务器提交命令。因此，FTP 对使用远程系统或在系统之间移动文件非常有用。然而，在因特网上或者其它不可信的网络上使用 FTP 会使您面临某些安全性风险。您必须了解这些风险以确保您的安全策略可描述您如何才能将这些风险将到最低。

- 当在系统上允许 FTP 时，您的对象权限规划可能不能提供足够的保护。

  例如，对象的公共权限可能是 *USE，但是您现在正在通过使用“菜单安全性”防止大多数用户访问那些对象。（菜单安全性防止用户做不在其菜单选项中的任何事情。）由于 FTP 用户不受菜单的限制，他们可以读取您系统上的所有对象。以下是控制此安全性风险的一些选项:
  - 在系统上实施全面 iSeries 对象安全性（换句话说，将系统的安全性模式从“菜单安全性”更改为“对象安全性”）。它是最好的且最安全的选项。
  - 编写 FTP 的出口程序以限制对可能通过 FTP 传送的文件进行访问。这些出口程序应该至少提供与菜单程序提供的安全性等同的安全性。许多客户可能希望使 FTP 访问控制受到更多的限制。此选项仅适用于 FTP，不适用于其它的接口（如 ODBC、DDM 或者 DRDA®）。

  注: 文件的 *USE 权限允许用户下载该文件。文件的 *CHANGE 权限允许用户上载该文件。
- 黑客可能对您的 FTP 服务器进行“拒绝服务”攻击，以禁用系统上的用户概要文件。通过重复尝试使用用户概要文件的错误密码登录，直到该用户概要文件被禁用，来实现攻击。如果这种类型攻击的注册数达到最多次数 3 次，概要文件就会被禁用。

  要避免这类风险，您所能做的是分析对希望增强安全性以使攻击最小化与向用户提供轻松访问之间的权衡方案。FTP 服务器通常实施 QMAXSIGN 系统值以防止黑客无限次尝试猜测密码，从而进行密码攻击。以下是您应该考虑使用的一些选项:
  - 使用 FTP 服务器登录出口程序，以拒绝任何系统用户概要文件和指定不允许 FTP 访问的那些用户概要文件的登录请求。（使用这样的出口程序时，对于不允许用户概要文件，服务器登录出口点拒绝的登录试图**不**计入概要文件的 QMAXSIGN 的计数。）
  - 使用 FTP 服务器登录出口程序以限制允许给定的用户概要文件访问 FTP 服务器的客户机。例如，如果允许“财务部”的一个人访问 FTP，则只允许该用户概要文件从具有“财务部”IP 地址的计算机访问 FTP 服务器。
  - 使用 FTP 服务器登录出口程序以记录进行所有 FTP 登录尝试的用户名和 IP 地址。定期查看这些记录，当概要文件被最大密码尝试数禁用时，使用该 IP 地址信息以识别作恶者并采取适当的措施。

另外，可以使用 FTP 服务器出口点对临时用户提供匿名 FTP 功能。安装安全且匿名的 FTP 服务器同时要求 FTP 服务器登录**和** FTP 服务器请求确认出口点的出口程序。

从 V5R1 起，可以使用“安全套接字层”（SSL）对您的 FTP 服务器提供安全的通信会话。使用 SSL 确保所有的 FTP 传输是加密的以维护 FTP 服务器与客户机之间传输的所有数据（包括用户名和密码）的机密性。FTP 服务器也支持使用数字证书进行客户机认证。

要了解有关使用 FTP、其风险以及对您可用的安全性措施的更多信息，请复查以下资源:
- 安全 FTP。
- 使用 SSL 以保护 FTP 服务器。

除了这些 FTP 选项，您可能要考虑使用“匿名 FTP”以为用户提供容易便捷地访问非机密资料。“匿名 FTP”启用对选定的远程系统上的信息的未保护访问（无需密码）。远程站点决定可用于一般访问的信息。此类信息被视为可公共访问的信息，且可由任何人阅读。在配置“匿名 FTP”之前，您应权衡安全风险并考虑使用出口程序保护您的 FTP 服务器。
- 配置匿名 FTP。
- 使用 FTP 出口程序管理访问。

第 7 章 传输安全性选项

记住 JKL 玩具公司方案有两个主要 iSeries 系统。他们将一个系统用于开发，另一个系统用于生产应用程序。这两个系统都处理关键任务数据和应用程序。因此，他们选择了在周边网络上添加新的 iSeries 系统以处理其内部网应用程序和因特网应用程序。

建立周边网络以确保在内部网与因特网之间具有某些物理隔离。这种隔离减少了其内部系统容易受到的因特网的攻击风险。通过只将新的 iSeries 服务器指定为因特网服务器，公司也降低了管理其网络安全性的复杂性。

由于对因特网环境安全性的普遍需求，IBM 仍在不断地开发安全性产品，以确保在因特网上实施电子商务的安全联网环境。在因特网环境下，必须确保同时提供特定系统及特定应用程序的安全性。然而，通过企业内部网或者因特网连接传输机密信息，更增强了对实现更强的安全性解决方案的需求。要拒绝这些风险，就应该实现保护数据在因特网上传输时的安全性措施。

您可以使用 iSeries 的两种特定传输级别安全性产品，将在不可信系统上传输信息所关联的风险降到最低，这两个产品是: “安全套接字层”（SSL）安全通信与“虚拟专用网”（VPN）连接。

使用 SSL 保护应用程序

“安全套接字层”（SSL）协议是保护客户机和服务器之间通信的通用业界标准。SSL 最初是为 Web 浏览器应用程序开发的，但是现在越来越多的其它应用程序也能使用 SSL。对于iSeries 服务器，这些应用程序包括:

- IBM HTTP Server for iSeries（最初由 Apache 开发并提供支持）
- FTP 服务器
- Telnet 服务器
- 分布式关系数据库体系结构（DRDA）与分布式数据管理
- （DDM）服务器
- “iSeries 导航器”中的“中央管理”
- 目录服务服务器（LDAP）
- iSeries Access Express 应用程序，包括“iSeries 导航器”和写入应用程序编程接口（API）的 iSeries Access Express 集的应用程序
- 用 Developer Kit for Java 开发的程序和使用 IBM Toolkit for Java 的客户机应用程序
- 用可以在应用程序上用来启用 SSL 的“安全套接字层”（SSL）“应用程序编程接口”（API）开发的程序。有关如何编写使用 SSL 的程序的更多信息，请参阅安全套接字层 API。

这些应用程序中的一些程序还支持使用数字证书进行客户机认证。SSL 依靠数字证书对通信各方进行认证并创建安全连接。

iSeries 虚拟专用网（VPN）

可以使用 iSeries 系统的 VPN 连接在两个端点之间建立安全通信信道。像 SSL 连接一样，可以对在端点之间传输的数据加密，因而可以同时提供数据机密性与数据完整性。然而，VPN 连接允许限制流动到指定端点的流量并限制可以使用该连接的流量类型。因此，VPN 连接通过帮助保护网络资源免受未授权者的访问，提供某种网络级别的安全性。

您应该使用哪种方法?

这两种安全性方法都对安全认证、数据机密性和数据完整性提出需求。您应该使用这些方法中的哪种方法，取决于以下几个因素。要考虑的因素是: 您正在与谁通信、与其通信所使用的应用程序、需要通信的安全级别和为保护此通信您希望所做的性能价格比的权衡方案。

另外，如果您希望特定的应用程序与 SSL 配合使用，则必须将该应用程序设置为使用 SSL。虽然许多应用程序尚无法利用 SSL，但许多其它的应用程序（如 Telnet 和 iSeries Access Express）已添加了 SSL 能力。另一方面，VPN 允许保护在特定的连接端点之间流动的所有 IP 流量。

例如，当前可以通过 SSL 使用 HTTP 以允许业务合作伙伴与内部网络上的 Web 服务器通信。如果 Web 服务器是在您与业务合作伙伴之间所需的唯一安全应用程序，那么您可能不希望切换至 VPN 连接。然而，如果您希望扩展通信，则可能要使用 VPN 连接。另外，可能有需要保护部分网络中的流量的情况，但是不希望为使用 SSL 单独配置每个客户机和服务器。可以对网络的该部分创建网关至网关的 VPN 连接。这种 VPN 连接可保护流量，但是对该连接任一端上单独的客户机和服务器来说，该连接是透明的。

对 SSL 使用数字证书

数字证书是使用“安全套接字层”（SSL）进行安全通信的基础并作为一种更强的认证手段。iSeries 服务器提供用 OS/400 的集成功能部件，即数字证书管理器（DCM）来轻松地创建并管理系统数字证书和用户数字证书的能力。

另外，可配置一些应用程序（如 IBM HTTP Server for iSeries），以将数字证书用作代替用户名和密码的更强的客户机认证方法。

数字证书是什么?

数字证书是一种验证证书所有者身份的数字凭证，类似于护照的功能。可信的第三方，称为**认证中心（CA）**， 向用户和服务器发出数字证书。对 CA 的信任是将该证书作为有效凭证的信任基础。

每个 CA 都有一个策略来确定为发出证书 CA 所需要标识的信息内容。某些因特网 CA 可能需要非常少的信息（如只需要专有名称）。它是 CA 向其发出数字证书地址和数字电子邮件地址的个人或服务器的名称。为每个证书生成一个专用密钥和一个公用密钥。证书包含公用密钥，而浏览器或安全文件则存储专用密钥。证书所有者可使用这些密钥“签署”并加密数据（如在用户和服务器之间发送的消息和文档）。这种数字签名确保项的来源的可靠性并保护该项的完整性。

虽然许多应用程序尚无法利用 SSL，但许多其它的应用程序（如 Telnet 和 iSeries Access Express）已添加了 SSL 能力。要了解如何对 iSeries 应用程序使用 SSL，请参阅“iSeries 信息中心”中的**使用 SSL 保护应用程序**:

使用 SSL 保护 Telnet 访问

可使用“配置 Telnet 服务器”以用“安全套接字层”（SSL）保护 Telnet 通信会话。要配置 Telnet 服务器以使用 SSL，必须使用“数字证书管理器”（DCM）配置证书供 Telnet 服务器使用。缺省情况下，Telnet 服务器处理安全与非安全的连接。然而，可以配置 Telnet 以便它只允许安全 Telnet 会话。另外，可以配置 Telnet 服务器以使用数字证书进行更强的客户机认证。

在选择对 Telnet 使用 SSL 时，您将获得一些强安全性的好处。对于 Telnet，除服务器认证外，数据在任何 Telnet 协议数据流动之前就可加密。一旦 SSL 会话建立，对所有 Telnet 协议（包括用户标识和密码交换）进行加密。

使用 Telnet 服务器时，要考虑的最重要的因素是在客户机会话中所使用的信息的敏感性。如果信息是敏感的或专用的，那么您可能会发现使用 SSL 设置 iSeries Telnet 服务器是很有好处的。对 Telnet 应用程序配置数字

证书时，可通过 SSL 与非 SSL 客户机运行 Telnet 服务器。如果安全策略要求总是对 Telnet 会话加密，则可禁用所有非 SSL 的 Telnet 会话。不需要使用 SSL Telnet 服务器时，可关闭 SSL 端口。可使用 ADDTCPPORT 命令禁用这些端口。关闭该端口后，服务器将为客户机提供非 SSL 的 Telnet，并禁用 SSL Telnet 会话。

要了解更多有关 Telnet 以及使用和不使用 SSL 的 Telnet 的安全性技巧，请参阅以下资源:
- Telnet “信息中心” 主题提供了在 iSeries 服务器上使用 Telnet 所需的信息。
- 《保护 iSeries 的技巧与工具》  在 TCP/IP 一节提供了有关 Telnet 安全性的详细信息。

使用 SSL 保护 iSeries Access Express

可使用 “将 iSeries Access Express 服务器配置为使用安全套接字层（SSL）” 以保护 iSeries Access Express 通信会话。例如，随着 JKL 玩具公司的发展，他们已经在其职员中增加了许多区域移动销售代理。这些销售代理需要从其总公司 iSeries 产品系统上访问有关玩具供应情况及生产日期的信息。由于此数据是敏感数据，JKL 玩具公司选择了仅允许其销售代理通过安全 iSeries Access Express 访问该信息。

使用 SSL 确保对 iSeries Access Express 会话的所有流量加密。它防止数据在本地与远程主机之间传输时被他人读取。

有关将 iSeries Access Express 与 SSL 配合使用的更多信息，请参阅以下资源:
- 安全套接字层管理
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

进行安全专用通信的 “虚拟专用网”（VPN）

随着虚拟专用网（VPN）的使用及其提供的安全性的增加，JKL 玩具公司正在研究在因特网上传送数据的选项。他们最近收购了另一家小型玩具制造公司，打算将其作为子公司来经营。JKL 将需要在这两个公司之间传递信息。两家公司都使用 iSeries 服务器，且使用 VPN 连接可提供他们在两个网络之间通信需要的安全性。创建 VPN 比使用传统的租用线路更合算。

使用 VPN 连接可以控制并保护同分支办事处、流动员工、供应商、业务合作伙伴和其他人的连接。

以下是一些可能从使用 VPN 连接获益的用户:
- 远程用户和移动用户。
- 总公司到分支办事处或其它非现场位置。
- 企业对企业的通信

如果不限制用户访问敏感系统，就会发生安全性风险。如果不限制可以访问系统的用户，就会增加公司信息不能保密的可能性。需要制定一个计划，仅允许那些需要共享系统信息的用户访问该系统。VPN 提供重要的安全性功能（如认证和数据保密性）的同时还允许您控制网络流量。创建多个 VPN 连接允许对于每个连接控制谁可以访问哪些系统。例如，“财务部” 和 “人力资源部” 可能通过其自己的 VPN 来链接。

当允许用户通过因特网连接到系统时，可能会通过公共网络发送敏感的企业数据，从而使这些数据暴露于攻击之下。保护传输的数据的一个选择是使用加密和认证方法确保数据的保密性和安全性防止无关的人访问。VPN 连接为特定安全性需求提供了解决方案：保护系统之间的通信。VPN 连接为在连接的两个端点之间流动的数据提供保护。另外，还可以使用 “信息包规则” 安全性定义允许什么 IP 信息包通过 VPN。

可以使用 VPN 创建安全连接来保护在受控的和可信的端点之间流动的流量。然而，您还必须知道对 VPN 伙伴提供了多少访问。当数据在公共网络上传输时，VPN 连接可以加密该数据。但是，取决于配置 VPN 连接的

方式，当数据在通过 VPN 连接进行通信的内部网络上流动时，VPN 连接可能不加密数据。因此，应该仔细规划设置每个 VPN 连接的方式。确保只允许 VPN 伙伴访问那些希望他们访问的内部网络上的主机或资源。

例如，可能有某位供应商需要得到有关您库存有哪些部件的信息。可以在内部网上在用于更新 Web 页面的数据库中获得此信息。您想允许这位供应商通过 VPN 连接直接访问这些页面。但并不希望该供应商能够访问其它系统资源（如数据库自身）。幸运的是，您可以配置 VPN 连接，以便将两个端点之间的流量限制在端口 80 上。端口 80 是 HTTP 流量使用的缺省端口。因此，您的供应商只能通过该连接发送和接收 HTTP 请求和响应。

由于可以限制通过 VPN 连接流动的流量类型，因此该连接提供了一种网络级别安全性方法。然而，VPN 控制进出系统流量的工作方式与防火墙不同。另外，VPN 连接并不是保护 iSeries 和其它系统间通信的唯一可用的方法。取决于您的安全性需求，可能会发现使用 SSL 是一种更合适的方法。

VPN 连接是否能提供您所需要的安全性，取决于您希望保护什么。另外还取决于为了提供该安全性希望所做的权衡方案。象对有关安全性的所做的任何决定一样，应该考虑 VPN 连接如何才能实现支持安全策略。

第 8 章 因特网安全性术语

要建立讨论因特网安全性的基础，先要定义一些因特网术语。如果您已熟悉因特网术语，可能希望跳过本节。

认证（Authentication）

认证是验证远程客户机或服务器实际上是不是他们声称的身份。认证确保您信任将要连接的远程对等对象。

非法闯入者（Cracker）

有不良企图的黑客。

密码术（Cryptography）

保持数据安全的科学。密码术允许您存储信息或与其它各方通信，同时防止无关各方了解存储的信息或者了解该通信。 加密将可以理解的文本转换为不可理解的数据段（密文）。解密将不可理解的数据复原为可理解的文本。这两个过程都涉及数学公式或算法及秘密数据序列（密钥）。

密码术有两种类型:

- 在共享密钥／密钥（**对称**）密码术中，密钥是在通信双方之间共享的秘密。加密和解密都使用同一个密钥。
- 在公用密钥（**非对称**）密码术中，加密和解密分别使用不同的密钥。一方有两个密钥: 一个公用密钥和一个专用密钥。虽然两个密钥在算法上相关，但事实上不可能从公用密钥派生出专用密钥。用某人的公用密钥加密的消息仅可用关联的专用密钥解密。或者，服务器或用户可以使用专用密钥来“签署”文档，并使用公用密钥对数字签名解密。这样可以验证文档的源。

数字证书（Digital certificate）

数字证书是一种验证证书所有者身份的数字文档，类似于护照的功能。称为“认证中心”（CA）的可信方向用户和服务器发出数字证书。对 CA 的信任是将该证书作为有效凭证的信任基础。可以将它们用于下列目的:

- 身份证明 – 用户是谁。
- 认证 – 确保用户与其声称的身份相符。
- 完整性 – 通过验证发送方的数字“签名”来确定文档的内容是否已修改。
- 不可抵赖性 – 保证用户无法声称尚未执行某些操作。例如，用户不能否认曾授权使用信用卡进行电子购买。

数字签名（Digital signature）

电子文档上的数字签名等同于书面文档上的个人签名。数字签名提供文档来源的证明。证书所有者使用与证书关联的专用密钥“签署”文档。文档的收件人使用相应的公用密钥对签名进行解密，来验证作为源的发送方。

数字证书管理器（DCM）（Digital certificate manager）

“数字证书管理器”允许 OS/400 成为本地的“认证中心”（CA）。可以使用 DCM 创建服务器或者用户使用的数字证书。可以导入其它 CA 发出的数字证书。还可将数字证书与 OS/400 用户概要文件关联。也可使用 DCM 配置应用程序，以使用“安全套接字层”（SSL）进行安全的通信。

专有名称（Distinguished name）

专有名称是“认证中心”（CA）向其发出数字证书的个人或服务器的名称。证书提供此名称以指示证书所有权。取决于发出证书的 CA 的策略，专有名称可以包括其它权限信息。

域名服务器（DNS）（Domain name server）

是将因特网名称转换为 IP 地址的因特网主机，常常与因特网上的其它 DNS 服务器进行交互。例如，许多 DNS 服务器可以识别

```
vnet.ibm.com
```

但是也许只有几个知道以下名称的完整的 IP 地址:

```
system1.vnet.ibm.com
```

当连接到因特网时，因特网客户机使用域名服务器确定希望与其通信的主机系统的 IP 地址。

加密（Encryption）

加密将数据转换为对不具有正确解密方法的任何人都不可阅读的一种格式。未授权方仍然可以拦截该信息。然而，没有正确的解密方法，就不能理解该信息。

外部网（Extranet）

由位于企业防火墙之外的若干个协作组织组成的专用商务网络。外部网服务使用现有的因特网基础结构，包括标准服务器、电子邮件客户机和 Web 浏览器。这使外部网比创建和维护专有网络更经济。它允许有共同利益的贸易伙伴、供应商和客户使用扩展的因特网来形成紧密的商务关系和强大的通信纽带。

防火墙（Firewall）

是内部网络与外部网络（如因特网）之间的逻辑障碍。防火墙由一个或多个硬件与软件系统构成。它控制在安全或可信系统与不安全或不可信系统之间的访问和信息流量。

黑客（Hacker）

是试图闯入您系统的未授权的任何人。

超文本链接（Hypertext Links）

通过各信息片段（称为超文本节点）之间的连接（称为超文本链接）在线提供信息的方法。

超文本标记语言（HTML）（Hypertext markup language）

用来定义超文本文档的语言。使用 HTML 来指示文档的外观（如突出显示和字型样式）及如何将其链接到其它文档或对象。

超文本传输协议（HTTP）（Hypertext transport protocol）

访问超文本文档的标准方法。

因特网（Internet）

互相连接的全球“网际网”。一套协作应用程序，允许连接到此“网际网”的计算机互相通信。因特网提供了可浏览的信息、文件传输、远程登录、电子邮件、新闻和其它服务。因特网常常称为“网络”。

因特网客户机（Internet client）

使用因特网向因特网服务器程序提出请求并接收来自因特网服务器程序结果的程序（或用户）。不同的客户机程序可用于请求不同类型的因特网服务。Web 浏览器是客户机程序的一种类型。“文件传输协议”（FTP）是另一种类型。

因特网主机（Internet host）

是连接到因特网或内部网的计算机。因特网主机可以运行一个以上的因特网服务器程序。例如，因特网主机可以运行 FTP 服务器以响应来自 FTP 客户机应用程序的请求。同一主机可以运行 HTTP Server 以响应来自使用 Web 浏览器的客户机的请求。服务器程序通常在主机系统的后台（以批处理方式）运行。

因特网密钥交换（IKE）（Internet key exchange）

IKE 协议与 IPSec 一起使用时，支持安全性关联的自动协商以及密钥的自动生成和刷新。通常，IKE 作为虚拟专用联网的一部分使用。

因特网名称（Internet name）

是 IP 地址的别名。IP 地址以一种长的数字格式出现且难以记忆（如 10.5.100.75）。可以将此 IP 地址指定为因特网名称，例如

```
system1.vnet.ibm.com
```

因特网名称还被称为标准域名。当您看到一则广告说“访问我们的主页”时，“主页地址”指的是因特网名称，而不是 IP 地址，因为因特网名称更容易记忆。

标准域名有几个部分。例如，

```
system1.vnet.ibm.com
```

有如下几个部分:

com:
所有的商务网络。域名的这部分由*因特网*权威机构（外部组织）分配。对不同类型的网络分配不同的字符（如 com 用于商业，而 edu 用于教育机构）。

ibm:
该组织的标识符。域名的这部分也由因特网权威机构分配，而且它是唯一的。全世界只有一个组织具有该标识符

```
ibm.com
```

vnet:
内部的系统分组

```
ibm.com
```

此标识符由内部分配。ibm.com 的管理员可创建一个或多个分组。

system1:
vnet.ibm.com 组内的因特网主机名称。

因特网服务器（Internet server）

通过因特网接受来自对应客户机程序的请求并通过因特网响应那些客户机的程序（或程序集）。可以将因特网服务器看作因特网客户机可以存取或访问的站点。不同的服务器程序支持不同的服务，如下所述:

- 浏览（“主页”以及其它的文档和对象的链接）。
- 文件传输。例如，客户机可以请求将文件从服务器传送至客户机。该文件可能是软件更新、产品列表或文档。
- 电子商务，如请求信息或订购产品的能力。

因特网服务提供商（ISP）（Internet service provider）

将您连接到因特网的组织，其方式与本地电话公司将您连接到全球电话网络的方式基本相同。

内部网（Intranet）

使用因特网工具（如 Web 浏览器 或 FTP）组织的内部网络。

IP 地址（IP address）

“因特网协议”（IP）地址是在 TCP/IP 网络上他人访问您的路径（因特网是一个非常大的 TCP/IP 网络）。通常对因特网服务器分配一个唯一的 IP 地址。因特网客户机可使用临时但唯一的、由 ISP 分配的 IP 地址。

IP 数据报（IP datagram）

通过 TCP/IP 网络发送的信息单元。IP 数据报（又称为信息包）包含数据和报头信息（如源 IP 地址与目标 IP 地址）。

IP 过滤器（IP filters）

IP 过滤提供防火墙的基本保护机制。它允许基于 IP 会话的详细信息确定在其上传送什么流量。它保护安全网络不受使用简单技术（如扫描安全服务器）或者以至最复杂的技术（如 IP 地址电子欺骗）的外来者的侵入。您应该将过滤功能部件看作是构造其它工具的基本部件。它提供了这些工具运行的基础结构，并拒绝几乎大多数认定的非法闯入者的访问。

IPSec 支持软件包在 IP 层进行安全交换的一组协议。IPSec 是 iSeries 和许多其它系统用于执行 VPN 的一组标准。

IP 电子欺骗（IP spoofing）

假冒为您通常信任的某个系统（IP 地址）来访问您的系统的一种企图。这个想要成为闯入者的人用您信任的 IP 地址设置了系统。路由器制造商已在其系统中构建了保护以检测并拒绝电子欺骗企图。

网络地址转换（NAT）（Network address translation）

对代理服务器和 SOCKS 服务器提供更透明的选择。通过使不兼容寻址结构的网络互相连接，它还可简化网络配置。NAT 提供两个主要功能。它可保护希望在内部网络运行的公用 Web 服务器。NAT 通过允许将服务器的“真实”地址隐藏在对公共网络可用的地址之后来提供了此保护。它还为内部用户提供在访问因特网的同时隐藏专用内部 IP 地址的机制。因为可隐藏用户的专用地址，NAT 在允许内部用户访问因特网服务时提供了保护。

不可抵赖性（Non-repudiation）

不可抵赖性是发生事务或发送或接收消息的证据。使用数字证书和公用密钥密码术来“签署”事务、消息和文档支持不可抵赖性。

信息包（Packet）

是包括有关线路协议（如以太网令牌环或帧中继）信息的数据报。

代理（Proxy）

代理服务器是在安全内部网络上的客户机与不可信网络上的服务器之间重新发送请求和响应的 TCP/IP 应用程序。代理服务器中断了 TCP/IP 连接以隐藏内部网络信息（如内部 IP 地址）。网络之外的主机将代理服务器当作通信源对待。

公用密钥基础结构（PKI）（Public key infrastructure）

验证并鉴定参与因特网事务的各方的有效性的数字证书、CA 和其它注册权威机构。

安全套接字层（SSL）（Secure Sockets Layer）

SSL 由 Netscape 创建，它是客户机和服务器之间进行会话加密的实际业界标准。SSL 使用对称密钥对服务器与客户机（用户）之间的会话进行加密。在数字证书交换期间，客户机和服务器协商此会话密钥。会对每个客户机和服务器之间的 SSL 会话创建不同的密钥。因此，即使未授权的用户拦截并解密会话密钥（这是不可能的），他们也无法使用它偷听当前、将来或过去的 SSL 会话。

窃听（Sniffing）

是在电子传输时监控或窃听的行为。通过因特网发送的信息在达到目的地之前，可能经过了许多个路由器传递。路由器制造商、ISP 和操作系统开发者都致力于确保在因特网主干网上不会发生“窃听”。成功“窃听”的情形日益减少。大多数“窃听”发生在连接到因特网的专用 LAN 上，而不是发生在因特网主干网自身上。然而，您需要了解有发生“窃听”的可能性，因为大多数 TCP/IP 传输都没有加密。

SOCKS

SOCKS 是通过安全网关传输 TCP/IP 流量的客户机／服务器体系结构。SOCKS 服务器执行的许多服务与代理服务器相同。

电子欺骗（Spoofing）

攻击者冒充为可信系统以尝试说服您向其发送秘密信息。

TCP/IP

是因特网上所使用的主要的通信协议。TCP/IP 表示“传输控制协议／因特网协议”。还可以在内部网络上使用 TCP/IP。

“特洛伊木马”程序（Trojan horse）

“特洛伊木马”程序是似乎在执行有用的、无害的功能的计算机程序。然而，它包含了隐藏功能，当用户启动该程序时这些功能使用分配给用户的已批准的权限。例如，它可以复制计算机的内部权限信息并将其发送回“特洛伊木马”程序的编写者。

虚拟专用网（VPN）（Virtual private network）

是企业的专用内部网的扩展。可以通过公共网络（如因特网）使用它，它实质上是通过专用“隧道”创建的安全专用连接。VPN 通过因特网连接其它用户将信息安全地传送到您的系统。其它用户包括:

- 远程用户
- 分支办事处
- 业务合作伙伴和供应商

Web 浏览器（Web browser）

是 HTTP 客户机应用程序。Web 浏览器解释 HTML 以对用户显示超文本文档。用户可以通过单击（选择）当前文档某区域来访问超链接对象。该区域常常称为**热点**。Internet Connection Web Explorer 和 Netscape Navigator 就是 Web 浏览器的示例。

万维网（WWW）（World Wide Web）

使用相同标准格式创建文档（HTML）和访问文档（HTTP）的互相连接的服务器和客户机的网状结构。从服务器到服务器及从文档到文档的链接的网状结构形象地称为 **Web**。

第 2 部分 附录

附录. 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

有关双字节（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区: International Business Machines Corporation “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。IBM 可以随时对本出版物中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

| IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

| IBM Corporation
| Software Interoperability Coordinator, Department 49XA
| 3605 Highway 52 N
| Rochester, MN 55901
| U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议、IBM 机器代码许可协议或任何同等协议中的条款提供。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息仅用于规划目的。在所述产品上市之前，可以更改此处的信息。

本信息包含日常业务经营中使用的数据和报告的示例。为了尽可能完整地说明这些示例，这些示例中包括个人、公司、品牌和产品的名称。所有这些人名或名称均系虚构，如有实际的企业名称和地址与此雷同，纯属巧合。

如果您正以软拷贝格式查看本信息，图片和彩色图例可能无法显示。

商标

下列各项是 International Business Machines Corporation 在美国和 / 或其他国家或地区的商标:

Application System/400
AS/400
Domino
DRDA
e(logo) server
IBM
iSeries
Operating System/400
OS/400WebSphere

Lotus、Freelance、Notes 和 WordPro 是 International Business Machines Corporation 和 Lotus Development Corporation 在美国和 / 或其他国家或地区的商标。

Java 和所有基于 Java 的商标是 Sun Microsystems, Inc. 在美国和 / 或其他国家或地区的商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

用于下载和打印出版物的条款和条件

如果符合以下条款和条件并且由此您表示接受它们，则授予您使用您选择下载的信息的准用权。

个人使用: 只要保留所有的专有权声明，您就可以为个人、非商业使用复制此信息。未经 IBM 明确同意，您不可以分发、展示或制作此信息或其中任何部分的演绎作品。

商业使用: 只要保留所有的专有权声明，您就可以仅在企业内复制、分发和展示此信息。未经 IBM 明确同意，您不可以制作此信息的演绎作品，或者在您的企业外部复制、分发或展示此信息或其中的任何部分。

除非本准用权中有明确授权，不得把其他准用权、许可或权利（无论是明示的还是暗含的）授予其中包含的信息或任何数据、软件或其他知识产权。

| 当使用该信息损害了 IBM 的利益，或者根据 IBM 的规定，未正确遵守上述指导说明时，则 IBM 保留自主决
| 定撤销本文授予的准用权的权利。

| 您不可以下载、出口或再出口本信息，除非完全遵守所有适用的法律和法规，包括所有美国出口法律和法规。
| IBM 对本信息的内容不作任何保证。本信息“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）
| 保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。

| 从此站点下载或打印信息，即表明您同意这些条款和条件。

中国印刷