 我们知道，企业的电子商务系统包括Intranet，它最大的好处是方便了企业内部以及企业与外部的信息交流，提高了工作效率。然而，与Internet这样一个世界范围的开放网络连接，在获得利益的同时，也要付出安全性代价。一旦企业内部网连入Internet，就意味着Internet上的每个用户都有可能访问企业网。如今，计算机和计算机网络有关的犯罪活动呈上升趋势，不仅表现在数量上，而且表现在复杂性上。如果没有一个安全性保护措施，未授权用户可能会在毫不觉察的情况下进入企业网，非法访问企业的资源。因此，计算机安全总体规划，应该考虑到这些新的危险和其不断增长的可能性，意识到任何私有网络系统(包括Intranet)都有可能成为一台计算机“ 进攻 ”的目标。而对于企业的Intranet来说，防火墙是一种保护本地系统或网络，抵制基于网络的安全威胁的有效手段。本章主要介绍防火墙的一些基本概念。第一节 防火墙的概念在大厦构造中，防火墙被设计用来来防止火从大厦的一部分传播到另一部分。因特网防火墙服务于类似的目的，它主要是防止因特网的危险传播到内部网络。一、防火墙“ 防火墙 ”是一个通用术语，是指在两个网络之间执行控制策略的系统。图7.1 防火墙的结构 防火墙通常是由软件系统和硬件设备组合而成，在内部网和外部网之间构建起安全的保护屏障。其一般结构如图7.1所示。防火墙可以被看成是阻塞点。所有内部网和外部网之间的连接都必须经过此阻塞点，在此进行检查和连

接，只有被授权的通信才能通过此阻塞点。防火墙使内部网络与外部网络在定条件下隔离，从而防止非法入侵及非法使用系统资源。同时，防火墙还可以执行安全管制措施，记录所有可疑的事件。可以说，防火墙为网络安全起到了把关的作用。尽管防火墙对内部网起到了很好的保护作用，但是，作为管理人员应当注意，防火墙并不是坚不可摧的。首先，防火墙不能防范恶意的知情者。尽管防火墙可以禁止系统用户经过网络连接发送保密信息。但是用户可以将数据复制到磁盘、磁带、或者纸上，放在公文包里带出去。因此，如果侵袭者已经在防火墙的内部，防火墙实际上是无能为力的。内部用户能偷窃数据，破坏硬件和软件，并且巧妙地修改程序而从不接近防火墙。这种威胁只有靠加强内部安全防范来予以解决。其次，防火墙不能控制不通过它的连接。防火墙仅能有效地控制穿过它的信息传输。然而，却无法控制不穿过它的信息传输。比如，用户或者系统管理员为了一时方便，临时地或者永久地设置了他们自己的网络“ 后门 ”（诸如拨号调制解调器连接等等）。这就为网络安全埋下了隐患，而且，这种隐患轻易不会被发现。实际上，实现一个有效的防火墙比给您的个人计算机买一个防病毒软件要复杂得多。防火墙不仅仅是一段单独的计算机程序或一件设备，而是整个Intranet安全策略的体现。简单地将一个防火墙产品置于Intranet上并不能提供企业所需要的保护。相反地，如果这种方式误导了管理员对安全的感觉，而致使其忽略了易受攻击之处的话，反而会增加企业的风险。事实上，对非法通信的完全防御和对授权通信的完全开放是存在对立性的两个方面。如果您的安全策略能够提供对外部侵入的完全保护，那

么达到这一策略的最有把握的方式是删除所有与网络相连的路径。这种情况下的Intranet是完全与外界没有联系的。然而，当今世界的内外部联系在不断加强，这种极端的安全策略对企业是不合适的。建立一个有效的防火墙来实施安全策略，应选择最适合企业需求的技术，并正确地创建防火墙。二、包过滤在实际应用中，防火墙有时可能只是一个具备包过滤功能的简单路由器，用来支持Internet安全。这是实现企业内部网与Internet安全联接的一种简单方法，因为包过滤是路由器的固有属性。