8.9 运行安全性：防火墙和入侵检测系统

遍及本章我们已经看出，因特网不是一个很安全的地方，即有坏家伙出没，从事着各种各样的破坏活动。给定因特网的不利性质，我们现在考虑一个机构网络和管理它的网络管理员。从网络管理员的角度看，世界可以很明显地分为两个阵营：一部分是好人，他们属于本机构网络，可以用相对不受限制的方式访问该机构网络中的资源；另一部分是坏家伙，他们是其他一些人，访问网络资源时必须经过仔细审查。在许多机构中，从中世纪的城堡到现代公司的建筑物，都有单一的出口/入口，无论好人坏人出入该机构，都需要进行安全检查。在一个城堡中，可以在吊桥的一端的门口执行安全检查；在公司大厦中，这些工作可在安全台完成。在计算机网络中，当通信流量进入/离开网络时要执行安全检查、做记录、丢弃或转发，这些工作都由被称为防火墙、入侵检测系统（IDS）和入侵防止系统（IPS）的运行设备来完成。

8.9.1 防火墙

防火墙（firewall）是一个硬件和软件的结合体，它将一个机构的内部网络与整个因特网隔离开，允许一些数据分组通过而阻止另一些分组通过。防火墙允许网络管理员控制外部和被管理网络内部资源之间的访问，这种控制是通过管理流入和流出这些资源的流量实现的。防火墙具有3个目标：

- 从外部到内部和从内部到外部的所有流量都通过防火墙。图8-33显示了一个防火墙，位于被管理网络和因特网其余部分之间的边界处。虽然许多大型机构可使用多级防火墙或分布式防火墙［Skoudis 2006］，但在对该网络的单一接入点处设置一个防火墙，如图8-33中所示，这使得管理和施加安全访问策略更为容易。
- 仅被授权的流量（由本地安全策略定义）允许通过。随着进入和离开机构网络的所有流量流经防火墙，该防火墙能够限制对授权流量的访问。
- 防火墙自身免于渗透。防火墙自身是一种与网络连接的设备，如果设计或安装不当，将可能危及安全，在这种情况下它仅提供了一种安全的假象（这比根本没有防火墙更糟糕！）。

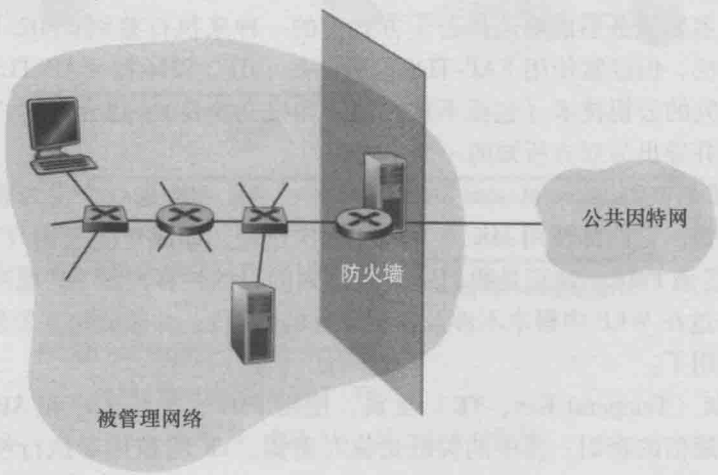

图8-33 在被管理网络和外部之间放置防火墙