内部用户。这个用户必须首先和应用程序网关建立一个 Telnet 会话。在网关（网关监听进入的 Telnet 会话）上一直运行的应用程序提示用户输入用户 ID 和口令。当这个用户提供这些信息时，应用程序网关检查这个用户是否得到许可向外 Telnet。如果没有，网关则中止这个内部用户向该网关发起的 Telnet 连接。如果该用户得到许可，则这个网关：①提示用户输入它所要连接的外部主机的主机名；②在这个网关和某外部主机之间建立一个 Telnet 会话；③将从这个用户到达的所有数据中继到该外部主机，并且把来自这个外部主机的所有数据都中继给这个用户。所以，该 Telnet 应用程序网关不仅执行用户授权，而且同时充当一个 Telnet 服务器和一个 Telnet 客户，在这个用户和该远程 Telnet 服务器之间中继信息。注意到过滤器因为该网关发起向外部的 Telnet 连接，将允许执行步骤②。

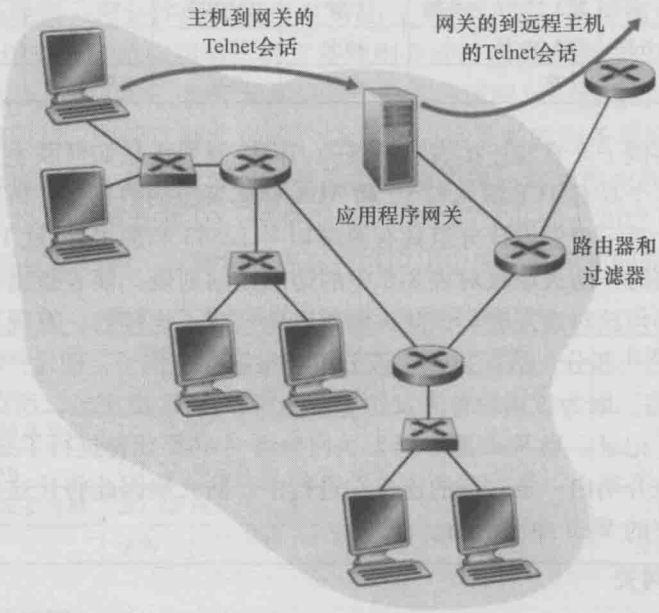

图 8-34 由应用程序网关和过滤器组成的防火墙

历史事件

匿名与隐私

假定你要访问一个有争议的 Web 网站（例如某政治活动家的网站），并且你：①不想向该 Web 网站透漏你的 IP 地址；②不想要你的本地 ISP（它可能是你住家或办公室的 ISP）知道你正在访问该站点；③不想要你的本地 ISP 看到你正在与该站点交换的数据。如果你使用传统的方法直接与该 Web 站点连接而没有任何加密，你无法实现这三个诉求。即使你使用 SSL，你也无法实现前两个诉求：你的源 IP 地址呈现在你发送给 Web 网站的每个数据报中；你发送的每个分组的目的地址能够容易地被你本地 ISP 嗅探到。

为了获得隐私和匿名，你能够使用如图 8-35 所示的一种可信代理服务器和 SSL 的组合。利用这种方法，你首先与可信代理建立一条 SSL 连接。然后你在该 SSL 连接中向所希望站点的网页发送一个 HTTP 请求。当代理接收到该 SSL 加密的 HTTP 请求，它解密请求并向 Web 站点转发该明文 HTTP 请求。接下来 Web 站点响应该代理，该代理经