过 SSL 再向你转发该响应。因为该 Web 站点仅看到代理的 IP 地址，并非你的客户 IP 地址，你的确获得了对该 Web 站点的匿名访问。并且因为你和代理之间的所有流量均被加密，你的本地 ISP 无法通过对你访问的站点做日志和记录你交换的数据来侵犯你的隐私。今天许多公司（例如 proxify. com）提供了这种代理服务。

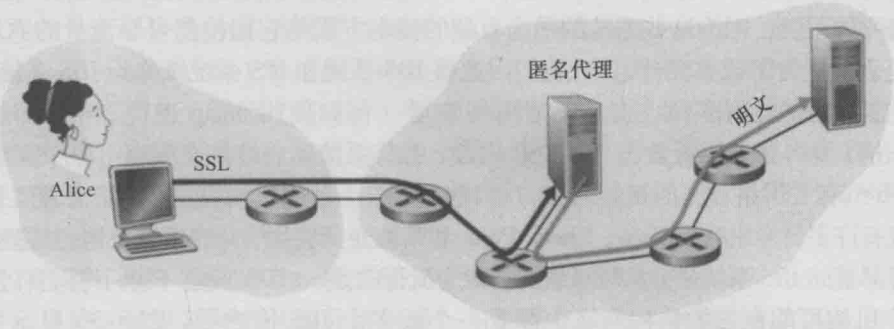

图 8-35 利用代理提供匿名和隐私

当然，在这个解决方案中，你的代理知道一切：它知道你的 IP 地址和你正在冲浪的站点的 IP 地址；并且它能够看到你与该 Web 站点之间以明文形式交换的所有流量。因此，这种解决方案的好坏取决于该代理的可信度。由 TOR 匿名和隐私服务所采用的一种更为健壮的方法是，让你的流量路由通过一系列“不串通”的代理服务器［TOR 2012］。特别是，TOR 允许独立的个体向其代理池贡献代理。当某用户使用 TOR 与一个服务器连接，TOR 随机地（从它的代理池）选择一条三个代理构成的链，并通过该链在客户和服务器之间路由所有流量。以这种方式，假设这些代理并不串通，无人知道在你的 IP 地址和目标 Web 站点之间发生的通信。此外，尽管在最后的代理和服务器之间发送明文，但这个最后代理并不知道哪个 IP 地址正在发送和接收明文。

内部网络通常有多个应用程序网关，例如 Telnet、HTTP、FTP 和电子邮件网关。事实上，一个机构的邮件服务器（见 2.4 节）和 Web 高速缓存都是应用程序网关。

应用程序网关也有其缺陷。首先，每一个应用程序都需要一个不同的应用程序网关。第二，因为所有数据都由网关转发，付出的性能负担较重。当多个用户或应用程序使用同一个网关计算机时，这成为特别值得关注的问题。最后，当用户发起一个请求时，客户软件必须知道如何联系这个网关，并且必须告诉应用程序网关如何连接到哪个外部服务器。

8.9.2 入侵检测系统

我们刚刚看到，当决定让哪个分组通过防火墙时，分组过滤器（传统的和状态的）检查 IP、TCP、UDP 和 ICMP 首部字段。然而，为了检测多种攻击类型，我们需要执行**深度分组检查**（deep packet inspection），即查看首部字段以外部分，深入查看分组携带的实际应用数据。如我们在 8.9.1 节所见，应用程序网关经常做深度分组检查。而一个应用程序网关仅对一种特定的应用程序执行这种检查。

显然，这为另一种设备提供了商机，即一种不仅能够检查所有通过它传递的分组的首部（类似于分组过滤器），而且能执行深度分组检查（与分组过滤器不同）的设备。当这