表 8-7 用于状态过滤器的连接表

源地址	目的地址	源端口	目的端口
222. 22. 1. 7	37. 96. 87. 123	12699	80
222. 22. 93. 2	199. 1. 205. 23	37654	80
222. 22. 65. 143	203. 77. 240. 43	48712	80

表 8-8 用于状态过滤器的访问控制列表

动作	源地址	目的地址	协议	源端口	目的端口	标志比特	核对连接
允许	222. 22/16	222. 22/16 的外部	TCP	>1023	80	任意	
允许	222. 22/16 的外部	222. 22/16	TCP	80	>1023	ACK	X
允许	222. 22/16	222. 22/16 的外部	UDP	>1023	53	—	
允许	222. 22/16 的外部	222. 22/16	UDP	53	>1023	—	X
拒绝	全部	全部	全部	全部	全部	全部	

我们浏览某些例子来看看连接表和扩展的访问控制列表是如何联手工作的。假设一个攻击者通过发送一个具有 TCP 源端口 80 和 ACK 标志置位的数据报，试图向机构网络中发送一个异常分组。进一步假设该分组具有源端口号 12543 和源 IP 地址 150. 23. 23. 155。当这个分组到防火墙时，防火墙核对表 8-8 中的访问控制列表，该表指出在允许该分组进入机构网络之前还必须核对连接表。该防火墙正确地核对了连接表，发现这个分组不是某进行中的 TCP 连接的一部分，从而拒绝了该分组。举第二个例子，假设一个内部的用户要在外部 Web 站点冲浪。因为该用户首先发送了一个 TCP SYN 报文段，所以该用户的 TCP 连接在连接表中有了记录。当 Web 服务器发送回分组（ACK 比特进行了必要的设置），该防火墙核对了连接表并明白一条对应的连接在进行中。防火墙因此将让这些分组通过，从而不会干扰内部用户的 Web 冲浪活动。

3. 应用程序网关

在上面的例子中，我们已经看到了分组级过滤使得一个机构可以根据 IP 的内容和 TCP/UDP 首部（包括 IP 地址、端口号和 ACK 比特）执行粗粒度过滤。但是如果一个机构仅为一个内部用户的受限集合（与 IP 地址情况正相反）提供 Telnet 服务该怎样做呢？如果该机构要这些特权用户在允许创建向外部的 Telnet 会话之前首先鉴别他们自己该怎样做呢？这些任务都超出了传统过滤器和状态过滤器的能力。的确，有关内部用户的身份信息是应用层数据，并不包括在 IP/TCP/UDP 首部中。

为了得到更高水平的安全性，防火墙必须把分组过滤器和应用程序网关结合起来。应用程序网关还除了看 IP/TCP/UDP 首部外，还基于应用数据来做策略决定。一个**应用程序网关**（application gateway）是一个应用程序特定的服务器，所有应用程序数据（入和出的）都必须通过它。多个应用程序网关可以在同一主机上运行，但是每一个网关都是有自己的进程的单独服务器。

为了更深入地了解应用程序网关，我们来设计一个防火墙，它只允许内部客户的受限集合向外 Telnet，不允许任何外部客户向内 Telnet。这一策略可通过将分组过滤（在一台路由器上）和一个 Telnet 应用程序网关结合起来实现，如图 8-34 所示。路由器的过滤器配置为阻塞所有 Telnet 连接，但从该应用程序网关 IP 地址发起的连接除外。这样的过滤器配置迫使所有向外的 Telnet 连接都通过应用程序网关。现在考虑一个要向外部 Telnet 的