过滤也可根据 TCP ACK 比特是否设置来进行。如果一个机构要使内部客户连接到外部服务器，却要防止外部客户连接到内部服务器，这个技巧很有效。3.5 节讲过，在每个 TCP 连接中第一个报文段的 ACK 比特都设为 0，而连接中的所有其他报文段的 ACK 比特都设为 1。因此，如果一个机构要阻止外部客户发起到内部服务器的连接，就只需直接过滤进入的所有 ACK 比特设为 0 的报文段。这个策略去除了所有从外部发起的所有 TCP 连接，但是允许内部发起 TCP 连接。

在路由器中使用访问控制列表实现防火墙规则，每个路由器接口有它自己的列表。表 8-6 中显示了对于某机构 222.22/16 的访问控制列表的例子。该访问控制列表适用于将路由器与机构外部 ISP 连接的某个接口。这些规则被应用到通过该接口自上而下传递的每个数据报。前两条规则一起允许内部用户在 Web 上冲浪：第一条规则允许任何具有目的端口 80 的 TCP 分组离开该机构网络；第二条规则允许任何具有源端口 80 且 ACK 比特置位的 TCP 分组进入该机构网络。注意到如果一个外部源试图与一台内部主机建立一条 TCP 连接，该连接将被阻挡，即使该源或目的端口为 80。接下来的两条规则一起允许 DNS 分组进入和离开该机构网络。总而言之，这种限制性相当强的访问控制列表阻挡所有流量，但由该机构内发起的 Web 流量和 DNS 流量除外。[CERT Filtering 2012] 提供了一个推荐的端口/协议分组过滤的列表，以避免在现有网络应用中的一些周知的安全性漏洞。

表 8-6 用于某路由器接口的访问控制列表

动作	源地址	目的地址	协议	源端口	目的端口	标志比特
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
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	—
拒绝	全部	全部	全部	全部	全部	全部

2. 状态分组过滤器

在传统的分组过滤器中，根据每个分组分离地作出过滤决定。状态过滤器实际地跟踪 TCP 连接，并使用这种知识作出过滤决定。

为了理解状态过滤器，我们来重新审视表 8-6 中的访问控制列表。尽管限制性相当强，表 8-6 中的访问控制列表仍然允许来自外部的 ACK = 1 且源端口为 80 的任何分组到达，通过该过滤器。这样的分组能够被试图用异常分组来崩溃内部系统、执行拒绝服务攻击或绘制内部网络的攻击者使用。幼稚的解决方案是也阻挡 TCP ACK 分组，但是这样的方法将妨碍机构内部的用户在 Web 上冲浪。

状态过滤器通过用一张连接表来跟踪所有进行中的 TCP 连接来解决这个问题。这种方法是可能的：因为防火墙能够通过观察三次握手（SYN、SYNACK 和 ACK）来观察一条新连接的开始；而且当它看到该连接的一个 FIN 分组时，它能够观察该连接的结束。当防火墙经过比如说 60 秒还没有看到该连接的任何活动性，它也能够（保守地）假设该连接结束了。某防火墙的一张连接表例子显示在表 8-7 中。这张连接表指示了当前有 3 条进行中的 TCP 连接，所有的连接都是从该机构内部发起的。此外，该状态过滤器在它的访问控制列表中包括了一个新栏，即“核对连接”，如表 8-8 中所示。注意到表 8-8 与表 8-6 中的访问控制列表相同，只是此时它指示应当核对其中两条规则所对应的连接。