Cisco 和 Check Point 是当今两个领先的防火墙厂商。你也能够容易地从 Linux 套件使用 iptables（通常与 Linux 装在一起的公共域软件）产生一个防火墙（分组过滤器）。

防火墙能够分为 3 类：**传统分组过滤器**（traditional packet filter）、**状态过滤器**（stateful filter）和**应用程序网关**（application gateway）。在下面小节中，我们将依次学习它们。

1. 传统的分组过滤器

如图 8-33 所示，一个机构通常都有一个将其内部网络与其 ISP（并因此与更大的公共因特网相连）相连的网关路由器。所有离开和进入内部网络的流量都要经过这个路由器，而这个路由器正是**分组过滤**（packet filtering）出现的地方。分组过滤器独立地检查每个数据报，然后基于管理员特定的规则决定该数据报应当允许通过还是应当丢弃。过滤决定通常基于下列因素：

- IP 源或目的地址。
- 在 IP 数据报中的协议类型字段：TCP、UDP、ICMP、OSPF 等。
- TCP 或 UDP 的源和目的端口。
- TCP 标志比特：SYN、ACK 等。
- ICMP 报文类型。
- 数据报离开和进入网络的不同规则。
- 对不同路由器接口的不同规则。

网络管理员基于机构的策略配置防火墙。该策略可以考虑用户生产率和带宽使用以及对一个机构的安全性关注。表 8-5 列出了一个机构可能具有的若干可能的策略，以及它们是如何用一个分组过滤器来处理分组的。例如，如果该机构除了允许访问它的公共 Web 服务器外不希望任何入 TCP 连接的话，那么它能够阻挡所有的入 TCP SYN 报文段，但具有目的地端口 80 的 TCP SYN 报文段除外，并且该目的 IP 地址对应于该 Web 服务器。如果该机构不希望它的用户用因特网无线电应用独占访问带宽，那么它能够阻挡所有非关键性 UDP 流量（因为因特网无线电经常是通过 UDP 发送的）。如果该机构不希望它的内部网络被外部绘制结构图（被跟踪路由），那么它能够阻挡所有 ICMP TTL 过期的报文离开该机构的网络。

表 8-5　对于 Web 服务器在 130. 207. 244. 203 的某机构网络 130. 207/16，其策略和对应的过滤规则

策略	防火墙设置
无外部 Web 访问	丢弃所有到任何 IP 地址、端口 80 的出分组
无入 TCP 连接，但那些只访问机构公共 Web 服务器的分组除外	丢弃所有到除 130. 207. 244. 203、端口 80 外的任何 IP 地址的入 TCP SYN 分组
防止 Web 无线电占据可用带宽	丢弃所有入 UDP 分组，但 DNS 分组除外
防止你的网络被用于一个 smurf DoS 攻击	丢弃所有去往某“广播”地址（例如 130. 207. 255. 255）的 ICMP ping 分组
防止你的网络被跟踪路由	丢弃所有出 ICMP TTL 过期流量

一条过滤策略能够基于地址和端口号的结合。例如，一台过滤路由器能够转发所有 Telnet 数据报（那些具有端口号 23 的数据报），但那些包括在一个特定的 IP 地址列表中的去往和来自的地址除外。这些策略允许在许可列表上的地址进行 Telnet 连接。不幸的是，基于外部地址的策略无法对其源地址被哄骗的数据报提供保护。