 二、不应该过滤的包 在开始过滤某些不想要的包之前要注意以下内容： ● ICMP包 ICMP包可用于检测TCP/IP失败的情形。如果阻挡这些包将导致不能得到“ Host unreachable ”或“ No route to host ”等信息。ICMP包还用于MTU发现，某些TCP实现使用了MTU发现来决定是否进行分段。MTU发现通过发送设置了不进行分段的位的包探测，当得到的ICMP应答表示需要分段时，再发送较小的包。如果得不到ICMP包（“ destination unreachable ”类型的包），则本地主机不减少MTU大小，这将导致测试无法停止或网络性能下降。 ● 到DNS的TCP连接 如果要拦阻出去的TCP连接，那么要记住DNS不总是使用UDP。如果从DNS服务器过来的回答超过512字节，客户端将使用TCP连接，并仍使用端口53接收数据。若禁止了TCP连接，DNS大多数情况下会正常工作，但可能会有奇怪的延时故障出现。如果内部网络的DNS查询总是指向某个固定的外部DNS服务器，可以允许本地域端口到该服务器的域端口连接。 ● 主动式FTP的TCP连接 FTP有两种运作方式，即传统的主动式（active）方式和目前流行的被动式(passive)方式。在主动式FTP模式下，FTP 服务器发送文件或应答LS命令时，主动和客户端建立TCP连接。如果这些TCP连接被过滤，则主动方式的FTP将被中断。如果使用被动方式，则过滤远地的TCP连接没有问题。因为数据连接是从客户端到服务器进行的（包括双向的数据）。 三、针对可能的网络攻击 防火墙的性能是

否优良关键在于其配置能否防护来自外界的各种网络攻击。这要求网络管理者能针对可能的网络攻击特点设定完善的安全策略。以网络常见的“ ping of death ”攻击为例，“ ping of death ”攻击通过发送一个非法的大ICMP包使接收者的TCP堆栈溢出从而引起混乱。针对这种攻击可将防火墙配置为阻挡ICMP分段。因为普通的ICMP包大都不需要到分段的程度，阻挡ICMP分段只拦阻大的“ ping ”包。 这种防护策略也可用于针对其他协议安全缺陷的网络攻击。 