

深入理解防火墙 屏蔽外界攻击 PDF转换可能丢失图片或格式
，建议阅读原文

https://www.100test.com/kao_ti2020/461/2021_2022__E6_B7_B1_E5_85_A5_E7_90_86_E8_c101_461738.htm 当无论任何人或事物都可以在任意时间进入你的电脑，你的电脑就处在了易被攻击的脆弱地位。你可以用防火墙来限制外界进入你的电脑及里面的信息。防火墙是做什么的? 防火墙对你的计算机或网站提供保护，像盾牌一样屏蔽外界的恶意软件或不必要的网络流量的攻击。防火墙可以设置成阻止来自某些特定区域的数据，同时允许其他相关的和必要的数据通过。这些对于依靠有线上网或DSL调制解调器上网的“一直在线”型网络用户来说，特别值得推荐。哪种类型的防火墙是最好的? 防火墙有两种形式：硬件型(外围)和软件型(内部)。虽然它们各自都有其优点和缺点，决定使用防火墙比决定采用何种类型防火墙来说重要的多。硬件防火墙- 通常称为网络防火墙，这些外围设备的位置处在你的计算机或网络与你的有线或DSL调制解调器之间。很多厂商和一些网络服务提供商(ISPs)提供叫做“路由器”的设备也包括防火墙功能。基于硬件的防火墙特别用于保护多台电脑，但是也为单独的一台电脑提供高度保护。如果你的防火墙后面只有一台电脑，或者你能确保网络中的其他电脑都随时进行补丁更新，因此免于受到病毒，蠕虫，或其他恶意代码的攻击，那么你就无需安装额外的软件防火墙进行保护。基于硬件的防火墙有其优点，有独立设备运行自己的操作系统，所以他们为防御攻击提供了额外的防线。他们的美中不足在于费用，不过现在已经有很多产品价格少于100美元(甚至有些不到50美元) 软件防

防火墙- 一些操作系统包含了内置防火墙.如果你的就是，那么可以考虑在已有外部防火墙的同时，增加一层内部防火墙的保护。如果你没有内置防火墙，你可以以相对小甚至零成本从当地计算机商店，软件供应商，或ISP获得一个防火墙软件。因为从网络上下载软件到未经保护的计算机上存在相关风险，因此最好从CD，DVD或软盘来安装防火墙软件。尽管只依赖于一个软件防火墙已能提供一些保护，但是要了解到防火墙与需要保护的信息同在一台计算机上，会削弱防火墙在恶意数据流进入电脑前将他们捕捉到的能力。怎样知道选择哪种配置? 大多数商用防火墙产品，无论是基于硬件或软件的防火墙，都配置为最能被广大用户接受的安全模式。由于每个防火墙都是不同的，你需要阅读和理解它的附带文件来确定它的默认设置是否能满足你的需要。你还可以从你的防火墙供应商或ISP(无论是技术支持还是网站)得到额外的帮助。此外，关于最新病毒和蠕虫的警报(比如US-CERT 的电脑安全警报)有时也包含你可执行在你防火墙上的设置信息。不幸的是，虽然正确设置防火墙可以有效阻止一些攻击，但是也不能对电脑安全产生虚假的幻觉。尽管防火墙提供相当的保护，它不能保证你的电脑不被攻击。特别是对那些由你来运行电脑中已被感染的程序文件的病毒，防火墙能够提供的保护只能很小或几乎没有，比如电子邮件传播的病毒。尽管如此，使用防火墙结合其他的保护措施(例如反病毒软件和其他安全使用电脑的方法)能够增强对攻击的阻挡。 100Test 下载频道开通，各类考试题目直接下载。详细请访问

www.100test.com