知识补漏：防火墙相关术语解释 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E7_9F_A5_E8_AF_86_E8_A1_A5_E6_c101_252822.htm 防火墙：英文名为“ FireWall ”，它是目前一种最重要的网络防护设备。从专业角度讲，防火墙是位于两个（或多个）网络间，实施网络之间访问控制的一组组件集合。 典型的防火墙具有以下三个方面的基本特性：（一）内部网络和外部网络之间的所有网络数据流都必须经过防火墙；（二）只有符合安全策略的数据流才能通过防火墙；（三）防火墙自身应具有非常强的抗攻击免疫力。 并发连接数：是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，这个参数的大小直接影响到防火墙所能支持的最大信息点数。 吞吐量：网络中的数据是由一个个数据包组成，防火墙对每个数据包的处理要耗费资源。吞吐量是指在不丢包的情况下单位时间内通过防火墙的数据包数量。吞吐量的大小主要由防火墙内网卡及程序算法的效率决定。 IDS：是英文“ Intrusion Detection Systems ”的缩写，意即“ 入侵检测系统 ”。专业上讲就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。 安全过滤带宽：是指防火墙在某种加密算法标准下，如DES（56位）或3DES（168位）下的整体过滤性能。它是相对于明文带宽提出的。一般来说，防火墙总的吞吐量越大，其对应的安全过滤带宽越高。 DDoS：是英文

“ distribution Denial of service ”的缩写，中文意思是“ 分布式拒绝服务攻击 ”。这种攻击方法使用与普通拒绝服务攻击同样的方法，但发起攻击的源是多个。通常，攻击者使用下载工具渗透无保护的主机，当获得该主机适当的访问权限后，攻击者在主机中安装软件的服务或进程（以下简称代理）。这些代理保持睡眠状态，直到从它们的主控端得到指令，主控端命令代理对指定的目标发起拒绝服务攻击。随着 Cable Modems、DSL和危害力极强的黑客工具的广泛传播使用，有越来越多的可以被访问的主机。分布式拒绝服务攻击是指主控端可以同时对一个目标发起几千个攻击。单个的拒绝服务攻击的威力也许对带宽较宽的站点没有影响，而分布于全球的几千个攻击将会产生致命的效果。