分布式拒绝服务(DDoS)是指不同位置的多个攻击者同时攻击一个或多个目标。或者攻击者控制不同位置的多台机器，并使用这些机器同时攻击受害者。由于攻击点分布在不同的地方，这种攻击称为分布式拒绝服务攻击，可以有多个攻击者。

分布式拒绝服务攻击可以同时攻击多台计算机，使攻击目标无法正常使用。分布式拒绝服务攻击多次出现，导致很多大型网站无法运行，不仅会影响用户的正常使用。同时造成的经济损失也非常巨大。

分布式拒绝服务攻击在攻击时可以伪造源IP地址，使得这种攻击在发生时非常隐蔽，检测起来也非常困难。因此，这种攻击也成为一种非常难以防范的攻击。

分布式拒绝服务攻击原理DDoS是基于DoS的拒绝服务攻击的一种特殊形式，是一种分布式协同的大规模攻击模式。。单一的DoS攻击通常是一对一的。它利用网络协议和操作系统的一些缺陷，采用欺骗和伪装策略进行网络攻击，使网站服务器充斥大量需要回复的信息，消耗网络带宽或系统资源。，导致网络或系统超负荷，停止提供正常的网络服务。与单个主机发起的DoS攻击相比，DDoS攻击是由数百台甚至数千台被入侵并安装了攻击程序的主机发起的群体行为。

一个完整的DDoS攻击系统由四部分组成：攻击者、主机、代理和目标。主终端和代理终端分别用于控制和实际发起攻击。主终端只发布命令，不参与实际攻击，代理终端发布DDoS的实际攻击包。。攻击者控制或部分控制主控端和代理端的计算机。在攻击过程中，他会用各种手段隐藏自己。一旦真正的攻击者向主控终端发送攻击命令，攻击者可以关闭或离开网络，主终端会向各个代理主机发出命令。这样攻击者就可以避免被跟踪。每个攻击代理主机都会向目标主机发送大量的服务请求包，这些包经过伪装，无法识别其来源。而且这些数据包请求的服务往往会消耗大量的系统资源，使得目标主机无法为用户提供正常的服务。甚至导致系统崩溃。