DDOS 应用层拒绝服务攻击

网络层DDOS发生在TCP三次握手中，攻击者伪造大量的虚假IP，向服务器发起请求，服务器接受请求后，返回SYN和ACK。但虚拟的ip不能完成第三次握手，服务器会重试三到五次，并且等待一段时间。 服务器需要不断的处理这些无用的请求，导致服务器无法处理正常的请求。

应用层拒绝服务攻击

CC攻击 challenge collapasar

攻击原理：就是对一些消耗资源比较大的应用页面不断发起正常的请求，应用层拒绝服务攻击发生在三次握手之后，因此攻击需要真实的ip。

应用层拒绝服务攻击还可以通过以下方式完成，在黑客入侵了一个流量很大的网站后，通过篡改页面，将巨大的流量分流到目标网页。那么所有访问该页面的用户都将对目标页面，发起一次GET请求

最常见的针对应用层的DDOS攻击的防御措施 是在应用中针对每个客户端做一个请求频率的限制。但是已经有很多自动化变换ip cookie的工具，使得服务器无法识别客户端，自然也无法对请求频率加以限制。

验证法是互联网中最常见的事情之一，如果忽略对用户的体验，那么引入验证码这一手段能够有效阻止自动化的重放角色。