DDoS（Distributed Denial of Service，分布式拒绝服务）攻击的主要目的是让指定目标无法提供正常服务，甚至从互联网上消失。

1. **SYN Flood**

攻击：

SYN Flood是互联网上最经典的DDoS攻击方式之一，利用了TCP三次握手的缺陷，能够以较小代价使目标服务器无法响应，且难以追查。

攻击者伪装大量的IP地址给服务器发送SYN报文，由于伪造的IP地址几乎不可能存在，也就几乎没有设备会给服务器返回任何应答了。因此，服务器将会维持一个庞大的等待列表，不停地重试发送SYN+ACK报文，同时占用着大量的资源无法释放。更为关键的是，被攻击服务器的SYN\_RECV队列被恶意的数据包占满，不再接受新的SYN请求，合法用户无法完成三次握手建立起TCP连接。也就是说，这个服务器被SYN Flood拒绝服务了。

防御：

SYN Flood攻击大量消耗服务器的CPU、内存资源，并占满SYN等待队列。相应的，我们修改内核参数即可有效缓解。主要参数如下：

net.ipv4.tcp\_syncookies = 1  
net.ipv4.tcp\_max\_syn\_backlog = 8192  
net.ipv4.tcp\_synack\_retries = 2

分别为启用SYN Cookie、设置SYN最大队列长度以及设置SYN+ACK最大重试次数。

SYN Cookie的作用是缓解服务器资源压力。cp\_max\_syn\_backlog则是使用服务器的内存资源，换取更大的等待队列长度，让攻击数据包不至于占满所有连接而导致正常用户无法完成握手。net.ipv4.tcp\_synack\_retries是降低服务器SYN+ACK报文重试次数，尽快释放等待资源。

1. **DNS Query Flood**

攻击：作为互联网最基础、最核心的服务，DNS自然也是DDoS攻击的重要目标之一。DNS Query Flood就是攻击者操纵大量傀儡机器，对目标发起海量的域名查询请求。

防御：

1. 缓存
2. 重发：可以是直接丢弃DNS报文导致UDP层面的请求重发，可以是返回特殊响应强制要求客户端使用TCP协议重发DNS查询请求。
3. 白名单：对于授权域DNS的保护，设备会在业务正常时期提取收到的DNS域名列表和ISP DNS IP列表备用，在攻击时，非此列表的请求一律丢弃，大幅降低性能压力。对于域名，实行同样的域名白名单机制，非白名单中的域名解析请求，做丢弃处理。
4. **HTTP Flood（**Challenge Collapsar CC攻击**）**

攻击：

SYN Flood和DNS Query Flood都需要攻击者以root权限控制大批量的傀儡机。收集大量root权限的傀儡机很花费时间和精力，而且在攻击过程中傀儡机会由于流量异常被管理员发现，攻击者的资源快速损耗而补充缓慢，导致攻击强度明显降低而且不可长期持续。HTTP Flood攻击则不同，攻击者并不需要控制大批的傀儡机，取而代之的是通过端口扫描程序在互联网上寻找匿名的HTTP代理或者SOCKS代理，攻击者通过匿名代理对攻击目标发起HTTP请求。匿名代理是一种比较丰富的资源，花几天时间获取代理并不是难事，因此攻击容易发起而且可以长期高强度的持续。

另一方面，HTTP Flood攻击在HTTP层发起，极力模仿正常用户的网页请求行为，与网站业务紧密相关，安全厂商很难提供一套通用的且不影响用户体验的方案。在一个地方工作得很好的规则，换一个场景可能带来大量的误杀。

防御：

1. 缓存：尽量由设备的缓存直接返回结果来保护后端业务。大型的互联网企业，会有庞大的CDN节点缓存内容
2. IP频率统计：当高级攻击者穿透缓存时，清洗设备会截获HTTP请求做特殊处理。最简单的方法就是对源IP的HTTP请求频率做统计，高于一定频率的IP地址加入黑名单。
3. 特殊处理：HTTP Flood是由程序模拟HTTP请求，一般来说不会解析服务端返回数据，更不会解析JS之类代码。因此当清洗设备截获到HTTP请求时，返回一段特殊JavaScript代码，正常用户的浏览器会处理并正常跳转不影响使用，而攻击程序会攻击到空处。
4. **慢速连接攻击（**Slowloris**）**

攻击：

HTTP协议规定，HTTP Request以\r\n\r\n结尾表示客户端发送结束，服务端开始处理。攻击者在HTTP请求头中将Connection设置为Keep-Alive，要求Web Server保持TCP连接不要断开，随后缓慢地每隔几分钟发送一个key-value格式的数据到服务端，如a:b\r\n，导致服务端认为HTTP头部没有接收完成而一直等待。如果攻击者使用多线程或者傀儡机来做同样的操作，服务器的Web容器很快就被攻击者占满了TCP连接而不再接受新的请求。

防御：

1. 统计：统计每个TCP连接的时长并计算单位时间内通过的报文数量即可做精确识别。一个TCP连接中，HTTP报文太少和报文太多都是不正常的，过少可能是慢速连接攻击，过多可能是使用HTTP 1.1协议进行的HTTP Flood攻击，在一个TCP连接中发送多个HTTP请求。
2. 限制：限制HTTP头部传输的最大许可时间。超过指定时间HTTP Header还没有传输完成，直接判定源IP地址为慢速连接攻击，中断连接并加入黑名单。