分布式拒绝服务攻击

分布式拒绝[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序[通讯](http://baike.baidu.com/item/%E9%80%9A%E8%AE%AF" \t "http://baike.baidu.com/_blank)，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

## 定义

首先从一个比方来深入理解什么是DDOS。

一群恶霸试图让对面那家有着竞争关系的商铺无法正常营业，他们会采取什么手段呢？（只为举例，切勿模仿）恶霸们扮作普通客户一直拥挤在对手的商铺，赖着不走，真正的购物者却无法进入；或者总是和营业员有一搭没一搭的东扯西扯，让工作人员不能正常服务客户；也可以为商铺的经营者提供虚假信息，商铺的上上下下忙成一团之后却发现都是一场空，最终跑了真正的大客户，损失惨重。此外恶霸们完成这些坏事有时凭单干难以完成，需要叫上很多人一起。嗯，网络安全领域中DoS和DDoS攻击就遵循着这些思路。

在信息安全的三要素——“保密性”、“完整性”和“可用性”中，DoS（Denial of Service），即拒绝服务攻击，针对的目标正是“可用性”。该攻击方式利用目标系统网络服务功能缺陷或者直接消耗其系统资源，使得该目标系统无法提供正常的服务。

[DdoS](http://baike.baidu.com/item/DdoS" \t "http://baike.baidu.com/_blank)的攻击方式有很多种，最基本的[DoS攻击](http://baike.baidu.com/item/DoS%E6%94%BB%E5%87%BB" \t "http://baike.baidu.com/_blank)就是利用合理的[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。单一的DoS攻击一般是采用一对一方式的，当攻击目标[CPU](http://baike.baidu.com/item/CPU" \t "http://baike.baidu.com/_blank)速度低、内存小或者网络带宽小等等各项指标不高的性能，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了[千兆](http://baike.baidu.com/item/%E5%8D%83%E5%85%86" \t "http://baike.baidu.com/_blank)级别的网络，这使得DoS攻击的困难程度加大了-目标对恶意攻击包的"消化能力"加强了不少。这时候分布式的拒绝[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)攻击手段（DDoS）就应运而生了。DDoS就是利用更多的[傀儡机](http://baike.baidu.com/item/%E5%82%80%E5%84%A1%E6%9C%BA" \t "http://baike.baidu.com/_blank)（[肉鸡](http://baike.baidu.com/item/%E8%82%89%E9%B8%A1" \t "http://baike.baidu.com/_blank)）来发起进攻，以比从前更大的规模来进攻受害者

## 攻击方式

[DDoS攻击](http://baike.baidu.com/item/DDoS%E6%94%BB%E5%87%BB" \t "http://baike.baidu.com/_blank)通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。 这种攻击方式可分为以下几种：

通过使网络过载来干扰甚至阻断正常的网络通讯；

通过向[服务器](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "http://baike.baidu.com/_blank)提交大量请求，使服务器超负荷；

阻断某一用户访问[服务器](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "http://baike.baidu.com/_blank)；

阻断某[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)与特定系统或个人的[通讯](http://baike.baidu.com/item/%E9%80%9A%E8%AE%AF" \t "http://baike.baidu.com/_blank)。

IP Spoofing

IP欺骗攻击是一种[黑客](http://baike.baidu.com/item/%E9%BB%91%E5%AE%A2" \t "http://baike.baidu.com/_blank)通过向[服务端](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E7%AB%AF" \t "http://baike.baidu.com/_blank)发送虚假的包以欺骗[服务器](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "http://baike.baidu.com/_blank)的做法。具体说，就是将包中的源[IP地址](http://baike.baidu.com/item/IP%E5%9C%B0%E5%9D%80" \t "http://baike.baidu.com/_blank)设置为不存在或不合法的值。[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)器一旦接受到该包便会返回接受请求包，但实际上这个包永远返回不到来源处的计算机。这种做法使[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)器必需开启自己的监听端口不断等待，也就浪费了系统各方面的资源。

LAND attack

这种攻击方式与SYN floods类似，不过在[LAND attack](http://baike.baidu.com/item/LAND attack" \t "http://baike.baidu.com/_blank)攻击包中的源地址和目标地址都是攻击对象的IP。这种攻击会导致被攻击的机器死循环，最终耗尽资源而[死机](http://baike.baidu.com/item/%E6%AD%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)。

ICMP floods

[ICMP](http://baike.baidu.com/item/ICMP" \t "http://baike.baidu.com/_blank)floods是通过向未良好设置的[路由器](http://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8" \t "http://baike.baidu.com/_blank)发送广播信息占用系统资源的做法。

Application

与前面叙说的攻击方式不同，Application level floods主要是针对应用软件层的，也就是高于OSI的。它同样是以大量消耗系统资源为目的，通过向IIS这样的网络[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)程序提出无节制的资源申请来迫害正常的网络服务。

## 攻击现象

被攻击[主机](http://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)上有大量等待的TCP连接；

网络中充斥着大量的无用的[数据包](http://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85" \t "http://baike.baidu.com/_blank)；

源地址为假 制造高流量无用数据，造成[网络拥塞](http://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%8B%A5%E5%A1%9E" \t "http://baike.baidu.com/_blank)，使受害[主机](http://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)无法正常和外界[通讯](http://baike.baidu.com/item/%E9%80%9A%E8%AE%AF" \t "http://baike.baidu.com/_blank)；

利用受害[主机](http://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)提供的[传输协议](http://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE" \t "http://baike.baidu.com/_blank)上的缺陷反复高速的发出特定的[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)请求，使主机无法处理所有正常请求；

严重时会造成系统[死机](http://baike.baidu.com/item/%E6%AD%BB%E6%9C%BA" \t "http://baike.baidu.com/_blank)。

## 攻击特点

分布式拒绝服务攻击采取的攻击手段就是分布式的，在攻击的模式改变了传统的点对点的攻击模式，使攻击方式出现了没有规律的情况，而且在进行攻击的时候，通常使用的也是常见的协议和服务，这样只是从协议和服务的类型上是很难对攻击进行区分的。在进行攻击的时候，攻击数据包都是经过伪装的，在源IP 地址上也是进行伪造的，这样就很难对攻击进行地址的确定，在查找方面也是很难的。这样就导致了分布式拒绝服务攻击在检验方法上是很难做到的。

## 攻击特性

对分布式攻击进行必要的分析，就可以得到这种攻击的特性。分布式拒绝服务在进行攻击的时候，要对攻击目标的流量地址进行集中，然后在攻击的时候不会出现拥塞控制。在进行攻击的时候会选择使用随机的端口来进行攻击，会通过数千端口对攻击的目标发送大量的数据包，使用固定的端口进行攻击的时候，会向同一个端口发送大量的数据包。

## 防范

### 主机设置

所有的主机平台都有抵御DoS的设置，总结一下，基本的有几种：

**关闭不必要的**[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)

**限制同时打开的Syn半连接数目**

**缩短Syn半连接的time out 时间**

**及时更新**[系统补丁](http://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%A1%A5%E4%B8%81" \t "http://baike.baidu.com/_blank)

### 网络设置

网络设备可以从[防火墙](http://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "http://baike.baidu.com/_blank)与[路由器](http://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8" \t "http://baike.baidu.com/_blank)上考虑。这两个设备是到外界的接口设备，在进行防DDoS设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

**1.**[防火墙](http://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "http://baike.baidu.com/_blank)

禁止对主机的非开放[服务](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1" \t "http://baike.baidu.com/_blank)的访问 限制同时打开的SYN最大连接数 限制特定IP地址的访问 启用[防火墙](http://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "http://baike.baidu.com/_blank)的防DDoS的属性 严格限制对外开放的服务器的向外访问 第五项主要是防止自己的[服务器](http://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "http://baike.baidu.com/_blank)被当做工具去害人。

**2.**[路由器](http://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8" \t "http://baike.baidu.com/_blank)

设置SYN[数据包](http://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85" \t "http://baike.baidu.com/_blank)流量速率 升级版本过低的ISO 为[路由器](http://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8" \t "http://baike.baidu.com/_blank)建立log server

## 攻击手段

当前主要有三种流行的 DDOS:

**1、SYN/ACK Flood 攻击：**  
　　这种攻击方法是经典最有效的 DDOS 方法， 可通杀各种系统的网络服务， 主要是通过向  
　　受害主机发送大量伪造源 IP 和源端口的 SYN 或 ACK 包，导致主机的缓存资源被耗尽或忙  
　　于发送回应包而造成拒绝服务， 由于源都是伪造的故追踪起来比较困难， 缺点是实施起来有  
　　一定难度， 需要高带宽的僵尸主机支持。 少量的这种攻击会导致主机服务器无法访问， 但却  
　　可以 Ping 的通， 在服务器上用 Netstat -na 命令会观察到存在大量的 SYN\_RECEIVED 状态，  
　　大量的这种攻击会导致 Ping 失败、TCP/IP 栈失效，并会出现系统凝固现象，即不响应键盘  
　　和鼠标。普通防火墙大多无法抵御此种攻击。  
　　**2、TCP 全连接攻击：**  
　　这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过  
　　滤 T earDrop、Land 等 DOS 攻击的能力，但对于正常的 TCP 连接是放过的，殊不知很多网  
　　络服务程序（如：IIS、Apache 等 W eb 服务器）能接受的 TCP 连接数是有限的，一旦有大  
　　量的 TCP 连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问，TCP 全连接攻  
　　击就是通过许多僵尸主机不断地与受害服务器建立大量的 TCP 连接，直到服务器的内存等  
　　资源被耗尽而被拖跨， 从而造成拒绝服务， 这种攻击的特点是可绕过一般防火墙的防护而达  
　　到攻击目的，缺点是需要找很多僵尸主机，并且由于僵尸主机的 IP 是暴露的，因此容易被  
　　追踪。  
　　**3、刷 Script 脚本攻击：**  
　　这种攻击主要是针对存在 ASP、JSP、PHP、CGI 等脚本程序，并调用 MSSQLServer、  
　　MySQLServer、Oracle 等数据库的网站系统而设计的，特征是和服务器建立正常的 TCP 连  
　　接， 并不断的向脚本程序提交查询、 列表等大量耗费数据库资源的调用， 一般来说， 提交一  
　　个 GET 或 POST 指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此  
　　请求却可能要从上万条记录中去查出某个记录， 这种处理过程对资源的耗费是很大的， 常见  
　　的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却是轻而易举  
　　的， 因此攻击者只需通过 Proxy 代理向主机服务器大量递交查询指令， 只需数分钟就会把服  
　　务器资源消耗掉而导致拒绝服务，常见的现象就是网站慢如蜗牛、ASP 程序失效、PHP 连  
　　接数据库失败、数据库主程序占用 CPU 偏高。这种攻击的特点是可以完全绕过普通的防火  
　　墙防护， 轻松找一些 Proxy 代理就可实施攻击， 缺点是对付只有静态页面的网站效果会大打  
　　折扣，并且有些 Proxy 会暴露攻击者的 IP 地址。  
　　怎么抵御 DDOS  
　　仅仅依靠某种系统或产品防住 DDOS 是不现实的， 可以肯定的是， 完全杜绝 DDOS  
　　是不可能的，但通过适当的措施抵御 90%的 DDOS 攻击是可以做到的，基于攻击和防御都  
　　有成本开销的缘故，若通过适当的办法增强了抵御 DDOS 的能力，也就意味着加大了攻击  
　　者的攻击成本，那么绝大多数攻击者将无法继续下去而放弃，也就相当于成功的抵御了  
　　DDOS 攻击。

## 防御基础

总体来说，对DoS和DDoS的防范主要从下面几个方面考虑：

尽可能对系统加载最新补丁，并采取有效的合规性配置，降低漏洞利用风险；

采取合适的安全域划分，配置防火墙、入侵检测和防范系统，减缓攻击。

采用分布式组网、负载均衡、提升系统容量等可靠性措施，增强总体服务能力。

可参考措施如下：

**1、采用高性能的网络设备引**

首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、 口碑好的产品。 再就是假如和网络提供商有特殊关系或协议的话就更好了，当大量攻击发生的时候请他们在网络接点处做一下流量限制来对抗某些种类的DDOS 攻击是非常有效的。

**2、尽量避免 NAT 的使用**

无论是路由器还是硬件防护墙设备要尽量避免采用网络地址转换 NAT 的使用， 因为采用此技术会较大降低网络通信能力，其实原因很简单，因为 NA T 需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多 CPU 的时间，但有些时候必须使用 NA T，那就没有好办法了。

**3、充足的网络带宽保证**

网络带宽直接决定了能抗受攻击的能力， 假若仅仅有 10M 带宽的话， 无论采取什么措施都很难对抗当今的 SYNFlood 攻击， 至少要选择 100M 的共享带宽，最好的当然是挂在1000M 的主干上了。但需要注意的是，主机上的网卡是 1000M 的并不意味着它的网络带宽就是千兆的， 若把它接在 100M 的交换机上， 它的实际带宽不会超过 100M， 再就是接在 100M的带宽上也不等于就有了百兆的带宽， 因为网络服务商很可能会在交换机上限制实际带宽为10M，这点一定要搞清楚。

**4、升级主机服务器硬件**

在有网络带宽保证的前提下，请尽量提升硬件配置，要有效对抗每秒 10 万个 SYN 攻击包，服务器的配置至少应该为：P4 2.4G/DDR512M/SCSI-HD，起关键作用的主要是 CPU 和内存， 若有志强双 CPU 的话就用它吧， 内存一定要选择 DDR 的高速内存， 硬盘要尽量选择SCSI 的，别只贪 IDE 价格不贵量还足的便宜，否则会付出高昂的性能代价，再就是网卡一定要选用 3COM 或 Intel 等名牌的，若是 Realtek 的还是用在自己的 PC 上吧。

**5、把网站做成静态页面**

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，至少到为止关于 HTML 的溢出还没出现，新浪、搜狐、网易等门户网站主要都是静态页面， 若你非需要动态脚本调用， 那就把它弄到另外一台单独主机去，免的遭受攻击时连累主服务器， 当然， 适当放一些不做数据库调用脚本还是可以的， 此外，最好在需要调用数据库的脚本中拒绝使用代理的访问， 因为经验表明使用代理访问你网站的80%属于恶意行为。