

# 防御CC攻击的4个方法和常见的CC攻击的方式

|      |                         |
|------|-------------------------|
| 产品名称 | 防御CC攻击的4个方法和常见的CC攻击的方式  |
| 公司名称 | 广州数据猫网络科技有限公司           |
| 价格   | .00/个                   |
| 规格参数 |                         |
| 公司地址 | 广州市天河区灵英东路3号            |
| 联系电话 | 17701938714 15625004753 |

## 产品详情

防护CC攻击找【152-1719-5017黄小姐】CC攻击防御、CC攻击防护、防御CC、WEB防护、WEF防护、入侵防御等为各类型攻击的防御

CC攻击：

CC攻击是DDOS（分布式拒绝服务）的一种，相比其它的DDOS攻击CC似乎更有技术含量一些。他们之间的原理都是一样的，即发送大量的请求数据来导致服务器拒绝服务，是一种连接攻击。

CC，全称Challenge Collapsar，意为“挑战黑洞”，其前身名为Fatboy攻击，是利用不断对网站发送连接请求致使形成拒绝服务的目的。

CC攻击常见的方式：

- 1、单主机虚拟多IP地址攻击：攻击者利用一台主机虚构出多个IP地址向目标服务器指定页面发送大量请求，当服务器来不及处理这些访问请求时，将导致该页面不能响应，正常的访问也将被拒绝。
- 2、代理服务器攻击：攻击者通过攻击主机发送访问请求给代理服务器。然后攻击主机可以立刻断开与代理服务器的连接，并马上发送下一次的访问请求，由于代理服务器接受访问请求指令后一定会对应用服务器的指定页面资源进行访问。所以攻击主机不必像直接访问应用服务器那样维持访问的连接，因此采用这种方攻击效率将会大大提高。

3、僵尸网络攻击：攻击者通过僵尸网络向服务器发起大量请求,受害主机收到的请求来自大量分散的地址,没有任何攻击者的IP地址信息,这一攻击方法高度模拟了众多用户正常访问应用服务器的过程，因此具有很强的隐蔽性。

这种攻击你见不到真实源IP，见不到特别大的异常流量，但造成服务器无法进行正常连接。醉让站长们忧虑的是这种攻击技术含量低，利用更换IP代理工具和一些IP代理一个初、中级的电脑水平的用户就能够实施攻击。那么我们怎么防护呢？

CC攻击防御方法：

CC攻击可以模拟正常用户和采用真实IP地址进行访问，因此隐蔽性较强。CC攻击常用的有效的防御方法如下：

1.选择可靠的高防服务器，提升服务器硬件和网络带宽资源：高性能服务器硬件能力和充足的网络带宽资源可以提升系统对CC攻击的承载能力

2.网站页面静态化：网站页面静态化可以较大程度的减少系统资源消耗，从而达到提高抗系统抗攻击能力；

3.IP屏蔽限制：辨别攻击者的源IP，针对CC攻击的源IP，可以在IIS中设置屏蔽该IP，限制其访问，达到防范IIS攻击的目的；

4.部署高防CDN：接入高防CDN，隐藏服务器源IP，自动识别攻击流量，清洗后将正常访客流量回源到源服务器IP上，保障业务安全；