

防御ddos的常用方法

产品名称	防御ddos的常用方法
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	机房:佛山/江苏等 租赁周期:年/月 套餐:200G/300G等
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

Ddos防御系统需要了解联系梁经理（199-2742-9680微电同号）帮你解决，Ddos防御专业防护、Ddos防攻击、Ddos套餐内防不住退款、Ddos防攻击、Ddos流量防护、Ddos流量防攻击！

什么是DDoS攻击？

DDoS攻击的zui简单目标是通过流量压倒您的服务器，这就是它的全部内容。如果你在Facebook上有10,000个朋友并且要求他们在特定时间尽可能多地访问一个网站，那么你将负责基本的拒绝服务攻击尝试。不同DDoS类型之间的所有变化都是使用的技术和目标网络基础设施的部分。

网站受到DDoS的表现

1.服务器CPU被大量占用

DDoS攻击其实是一种恶意性的资源占用攻击，攻击者利用肉鸡或者攻击软件对目标服务器发送大量的无效请求，导致服务器的资源被大量的占用，因而正常的进程没有得到有效的处理，这样网站就会出现打开缓慢的情况。如果服务器某段时期能突然出现CPU占用率过高，那么就可能是网站受到CC攻击影响。

2.带宽被大量占用

占用带宽资源通常是DDoS攻击的一个主要手段，毕竟对很多小型企业或者个人网站来说，带宽的资源可以说非常有限，网络的带宽被大量无效数据给占据时，正常流量数据请求很很难被服务器进行处理。如果服务器上行带宽占用率达到90%以上时，那么你的网站通常出现被DDoS攻击的可能。

3服务器连接不到，网站也打不开

如果网站服务器被大量DDoS攻击时，有可能会造成服务器蓝屏或者死机，这时就意味着服务器已经连接不上了，网站出现连接错误的情况。当然出现这种请求时我们zui好是确认一下服务器是否是硬件故障等所导致出现的问题，否者在进行服务器连接时就要做好相关的防御首段。

4.域名ping不出IP

可能这种情况站长们可能会比较少考虑到，这其实也是DDoS攻击的一种表现，只是攻击着所针对的攻击目标是网站的DNS域名服务器。在出现这种攻击时，ping服务器的IP是正常联通的，但是网站就是不能正常打开，并且在ping域名时会出现无法正常ping通的情况。

怎样去防御ddos攻击好？

1、保证服务器系统的安全

首先要确保服务器软件没有任何漏洞，防止攻击者入侵。确保服务器采用zui新系统，并打上安全补丁。在服务器上删除未使用的服务，关闭未使用的端口。对于服务器上运行的网站，确保其打了zui新的补丁，没有安全漏洞。

2、隐藏服务器的真实IP地址

不要把域名直接解析到服务器的真实IP地址，不能让服务器真实IP泄漏，服务器前端加CDN中转（免费的CDN一般能防止5G左右的DDOS），如果资金充裕的话，可以购买高防的盾机，用于隐藏服务器真实IP，域名解析使用CDN的IP，所有解析的子域名都使用CDN的IP地址。此外，服务器上部署的其他域名也不能使用真实IP解析，全部都使用CDN来解析。

总之，只要服务器的真实IP不泄露，5G以下小流量DDOS的预防花不了多少钱，免费的CDN就可以应付得了。如果攻击流量超过10G，那么免费的CDN可能就顶不住了，需要购买一个高防的盾机来应付了，而服务器的真实IP同样需要隐藏。

本文部分摘自网络，如有不便，请及时联系删除