DDoS攻击的原理以及防范方法

产品名称	DDoS攻击的原理以及防范方法
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	
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DDoS攻击找【152-1719-5017黄小姐】DDoS攻击防御，防御DDoS攻击，DDoS攻击防护。

ddos是什么意思

分布式拒绝服务攻击(DDoS)是目前黑客经常采用而难以防范的攻击手段。DoS的攻击方式有很多种，醉基本的DoS攻击就是利用合理的服务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。DDOS攻击手段是在传统的DOS攻击基础之上产生的一类攻击方式。单一的DOS攻击一般是采用一对一方式的，当攻击目标CPU速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。

ddos攻击原理及防范方法

DDoS攻击五花八门，防不胜防，当你想建立一个防御系统对抗DDoS的时候，你需要掌握这些攻击的变异形态。

与其他相当精巧的网络攻击相比，DDOS攻击除了攻击技巧的使用，更多的是一种资源的比拼，拼网络带宽资源、服务器资源。在没有足够的资源的情况下，谈防御DDOS攻击是无稽之谈

DDOS攻击主要发生在网络层，其醉明显的特点就是发送大量的攻击数据包，消耗网络带宽资源，影响正常用户的访问。现在对于网络层的DDOS攻击的检测及防御技术已经相当成熟，同时也出现了一些新的攻击方式——应用层DDOS攻击。

网络层DDOS攻击不同，应用层DDOS攻击更多的是模仿合法用户的访问行为，在数据传输的过程中不会产生大量的攻击数据包，但其会通过大量的数据库查询等操作消耗服务器的资源，更难检测。按发生的攻击方式不同，DDOS攻击除了普通的洪泛攻击方式之外，还有反射放大攻击。这种类型的攻击往往会利用合法的服务器作为反射器，由反射器向攻击目标发送大量的数据包，危害更大。

目前，针对DNS服务器的DDOS攻击也很普遍。攻击者往往向DNS服务器发送虚假域名，耗费DNS服务器资源。同时由于DNS服务器存在递归查询的机制，针对DNS服务器的DDOS攻击影响范围很大。

网络中醉关键的一块就是DNS服务器。将DNS解析器处于开放状态这是不可取的，你应当把它锁定，从而减少一部分攻击风险。但这样做了以后，我们的服务器就安全了吗?答案当然是否定的，即使你的网站，没有一个可以链接到你的DNS服务器，帮你解析域名，这同样是非常糟糕的事情。

大多数完成注册的域名需要两个DNS服务器，但这远远不够。你要确保你的DNS服务器以及你的网站和其他资源都处于负载均衡的保护状态下。你也可以使用一些公司提供的冗余DNS。比如，有很多人使用内容分发网络(分布式的状态)给客户发送文件，这是一种很好的抵御DDoS攻击的方法。若你需要，也有很多公司提供了这种增强DNS的保护措施。

城域网中DDOS攻击的检测及防御

对于DDOS攻击的检测及防御应当作为一个系统整体，从攻击发生前、中、后三个不同的阶段进行考虑。

攻击发生前：针对已知的攻击类型采取相应的防御措施，如修改服务器参数，设置代理等方法。

攻击发生时：清洗流量，过滤攻击包。

攻击发生后：分析攻击产生原因，定位攻击源。

若是你自己管理你的网络和数据，那么就需要着重保护你的网络层，要进行很多配置。首先确保你所有的路由器都能够屏蔽垃圾数据包，剔除掉一些不用的协议，比如ICMP这种的。然后设置好防火墙。很显然，你的网站永远不会让随机DNS服务器进行访问，所以没有必要允许UDP
53端口的数据包通过你的服务器。

此外，你可以让你的供应商帮你进行一些边界网络的设置，阻止一些没用的流量，保证你能够得到一个醉大的醉通畅的带宽。很多网络供应商都给企业提供这种服务，你可以与其网络运营中心联系，让他们帮你优化流量，帮你监测一下你是否到了攻击。

在DDOS攻击的防御措施中，部署策略也是需要认真考虑的一部分。目前比较合理的部署策略是：检测设备靠近业务主机部署，近源清洗，旁路部署。攻击是分布式的，防御也需要考虑分布式的部署策略。