DDOS高防IP如何防御攻击？

产品名称	DDOS高防IP如何防御攻击？
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

防御DDOS攻击【微电152-1719-5017黄小姐】DDOS防御流量攻击，DDOS防CC流量攻击，专业防御DDOS攻击，防御DDOS攻击，防御CC攻击，DDOS防御，CC防御，DDOS防御CC攻击。

关于DDos攻击的常见方法

1.SYN Flood：利用TCP协议的原理，这种攻击方法是经典醉有效的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。TCP通道在建立以前，需要三次握手：

a.客户端发送一个包含SYN标志的TCP报文，同步报文指明客户端所需要的端口号和TCP连接的初始序列号

b.服务器收到SYN报文之后，返回一个SYN+ACK报文，表示客户端请求被接受，TCP初始序列号加1

c.客户端也返回一个确认报文ACK给服务器，同样TCP序列号加1

d.如果服务器端没有收到客户端的确认报文ACK，则处于等待状态，将该客户IP加入等待队列，然后轮训发送SYN+ACK报文

所以攻击者可以通过伪造大量的TCP握手请求，耗尽服务器端的资源。

2.HTTP Flood：针对系统的每个Web页面，或者资源，或者Rest API，用大量肉鸡，发送大量http request。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，典型的以小博大的攻击方法。缺点是对付只有静态页面的网站效果会大打折扣。

3.慢速攻击：Http协议中规定，HttpRequest以\r\n\r\n结尾来表示客户端发送结束。攻击者打开一个Http 1.

1的连接，将Connection设置为Keep-Alive，保持和服务器的TCP长连接。然后始终不发送\r\n\r\n，每隔几分钟写入一些无意义的数据流，拖死机器。

4.P2P攻击：每当网络上出现一个热门事件，比如XX门，精心制作一个种子，里面包含正确的文件下载，同时也包括攻击目标服务器的IP。这样，当很多人下载的时候，会无意中发起对目标服务器的TCP连接。

DDOS攻击现象判定方法

1.SYN类攻击判断：A.CPU占用很高；B.网络连接状态：netstat – na,若观察到大量的SYN_RECEIVED的连接状态；C.网线插上后，服务器立即凝固无法操作，拔出后有时可以恢复，有时候需要重新启动机器才可恢复。

2.CC类攻击判断：A.网站出现service unavailable提示；B.CPU占用率很高；C.网络连接状态：netstat – na,若观察到大量的ESTABLISHED的连接状态单个IP高达几十条甚至上百条；D.用户无法访问网站页面或打开过程非常缓慢,软重启后短期内恢复正常,几分钟后又无法访问。

3.UDP类攻击判断：A.观察网卡状况每秒接受大量的数据包；B.网络状态：netstat – na TCP信息正常。

4.TCP洪水攻击判断：A.CPU占用很高；B.netstat – na,若观察到大量的ESTABLISHED的连接状态单个IP高达几十条甚至上百条

DDoS攻击如何防御？

1、采用高性能的服务器，CPU处理能力更强；

2、开通更高的网络带宽，带宽决定抗攻击的能力；

3、把网站做成静态页面或者伪静态；

4、启用SYN攻击保护；

5、关闭不必要的服务，限制同时打开的Syn半连接数目；

6、开通Anti-DDoS流量清洗，DDoS高防服务；

7、安装专业防CC攻击的Web应用防火墙；

8、HTTP恶意请求直接拦截；

9、部署CDN，用户就近访问，提高速度。

如何区分DDoS攻击还是CC攻击：

查看用户受到攻击的情况：如果只配置了4层转发，一般攻击是DDoS的。控制台登录查看对应防护流量信息，ddos防护有攻击流量的波动，且在清洗，在CC防护中没有相关的波动。

如果只配置了7层转发，一般攻击是CC攻击。控制台登录查看对应防护流量信息，DDoS防护有攻击流量的波动，且在清洗，在CC防护中有相关的波动。

以上就是关于DDoS攻击的方法以及DDoS攻击的防御，希望能帮到大家，当出现这种攻击的时候也不要

担心，现在很多服务商都能提供高防服务器，我们数据猫公司针对互联网的DDOS大流量攻击提供的网络安全解决方案，防护能力可达400G以上，提供单线、双线、多线等线路选择，让您的业务不再畏惧DDOS攻击的挑战，同时拥有极速的访问体验。