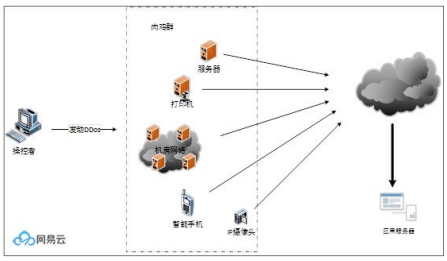
什么是 DDoS 攻击?

网易云社区 关注
2018.11.28 11:02:01 字数 2,214 阅读 7,490

欢迎访问网易云社区，了解更多网易技术产品运营经验。

全称Distributed Denial of Service，中文意思为"分布式拒绝服务"，就是利用大量合法的分布式服务器对目标发送请求，从而导致正常合法用户无法获得服务。通俗点讲就是利用网络节点资源如：IDC服务器、个人PC、手机、智能设备、打印机、摄像头等对目标发起大量攻击请求，从而导致服务器拥塞而无法对外提供正常服务，只能宣布game over，详细描述如下图所示：



DDoS攻击示意图

2、黑客为什么选择DDoS

不同于其他恶意篡改数据或劫持类攻击，DDoS简单粗暴，可以达到直接摧毁目标的目的。另外，相对其他攻击手段DDoS的技术要求和发动攻击的成本很低，只需要购买部分服务器权限或控制一批肉鸡即可，而且攻击相应速度很快，攻击效果可视。另一方面，DDoS具有攻击易防守难的特征，服务提供商为了保证正常客户的需求需要耗费大量的资源才能和攻击发起方进行对抗。这些特点使得DDoS成为黑客们手中的一把很好使的利剑，而且所向霹雳。

从另一个方面看，DDoS虽然可以侵蚀带宽或资源，迫使服务中断，但这远远不是黑客的正真目的。所谓没有买卖就没有杀害，DDoS只是黑客手中的一枚核武器，他们的目的要么是敲诈勒索、要么是商业竞争、要么是要表达政治立场。在这种黑色利益的驱使下，越来越多的人参与到这个行业并对攻击手段进行改进升级，致使DDoS在互联网行业愈演愈烈，并成为全球范围内无法攻克的一个顽疾。

3、DDoS的攻击方式

一种服务需要面向大众就需要提供用户访问接口，这些接口恰恰就给了黑客有可乘之机，如：可以利用TCP/IP协议握手缺陷消耗服务端的链接资源，可以利用UDP协议无状态的机制伪造大量的UDP数据包阻塞通信信道.....可以说，互联网的世界自诞生之日起就不缺乏被DDoS利用的攻击点，从TCP/IP协议机制到CC、DNS、NTP反射类攻击，更有甚者利用各种应用漏洞发起更高级更精确的攻击。

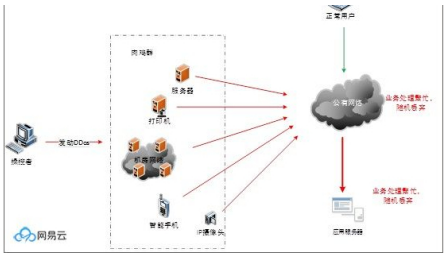
从DDoS的危害性和攻击行为来看，我们可以将DDoS攻击方式分为以下几类：

a）资源消耗类攻击

资源消耗类是比较典型的DDoS攻击，最具代表性的包括：Syn Flood、Ack Flood、UDP Flood。这类攻击的目标很简单，就是通过大量请求消耗正常的带宽和协议栈处理资源的能力，从而达到服务端无法正常工作的目的。

b）服务消耗性攻击

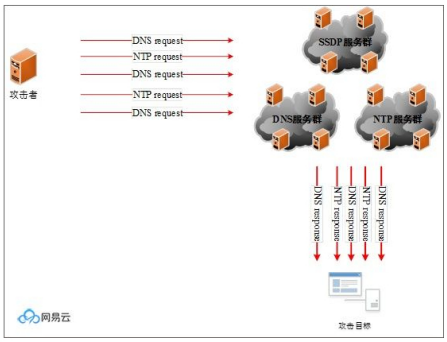
相比资源消耗类攻击，服务消耗类攻击不需要太大的流量，它主要是针对服务的特点进行精确定点打击，如web的CC，数据服务的检索，文件服务的下载等。这类攻击往往不是为了拥塞流量通道或协议处理通道，它们是让服务端始终处理高消耗型的业务的忙碌状态，进而无法对正常业务进行响应，详细示意图如下：



服务消耗类攻击

c）反射类攻击

反射攻击也叫放大攻击，该类攻击以UDP协议为主，一般请求回应的流量远远大于请求本身流量的大小。攻击者通过流量被放大的特点以较小的流量带宽就可以制造出大规模的流量源，从而对目标发起攻击。反射类攻击严格意义上来说不算是攻击的一种，它只是利用某些服务的业务特征来实现用更小的代价发动Flood攻击，详细示意图如下：



反射类攻击

d）混合型攻击

混合型攻击是结合上述几种攻击类型，并在攻击过程中进行探测选择最佳的攻击方式。混合型攻击往往伴随这资源消耗和服务消耗两种攻击类型特征。

4、DDoS防护困难

一方面，在过去十几年中，网络基础设施核心部件从未改变，这使得一些已经发现和被利用的漏洞以及一些成成熟的攻击工具生命周期很长，即使放到今天也依然有效。另一方面，互联网七层模型应用的迅猛发展，使得DDoS的攻击目标多元化，从web到DNS，从三层网络到七层应用，从协议栈到应用App，层出不穷的新产品也给了黑客更多的机会和突破点。再者DDoS的防护是一个技术和成本不对等的工程，往往一个业务的DDoS防御系统建设成本要比业务本身的成本或收益更加庞大，这使得很多创业公司或小型互联网公司不愿意做更多的投入。

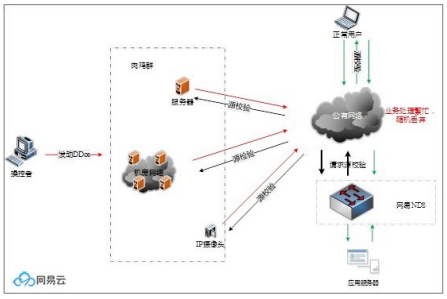
5、DDoS防护手段

DDoS的防护系统本质上是一个基于资源较量和规则过滤的智能化系统，主要的防御手段和策略包括：

a）资源隔离

资源隔离可以看作是用空间换时间的一种防护手段，这在防护系统拥有无比强大的带宽和流量处理能

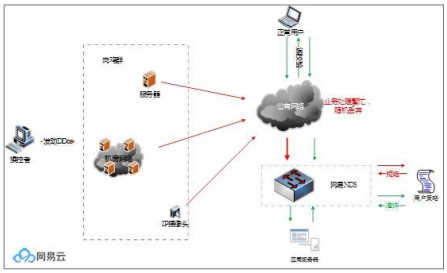
资源隔离可以看作是用户服务的一堵防护盾，这套防护系统拥有无比强大的数据和流量处理能力，为用户过滤异常的流量和请求。如：针对Syn Flood，防护盾会响应Syn Cookie或Syn Reset认证，通过对数据源的认证，过滤伪造源数据包或发功攻击的攻击，保护服务端不受恶意连接的侵蚀。资源隔离系统主要针对ISO模型的第三层和第四层进行防护。资源隔离示意图如下：



资源隔离示意图

b）用户规则

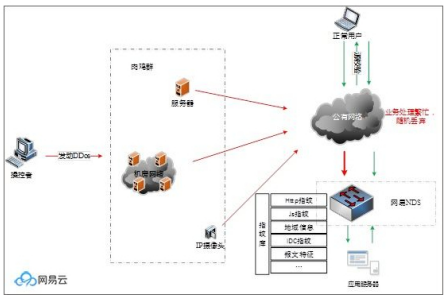
从服务的角度来说DDoS防护本质上是一场以用户为主体依赖抗D防护系统与黑客进行较量的战争，在整个数据对抗的过程中服务提供者往往具有绝对的主动权，用户可以基于抗D系统特定的规则，如：流量类型、请求频率、数据包特征、正常业务之间的延时间隔等。基于这些规则用户可以在满足正常服务本身的前提下更好地对抗七层类的DDoS，并减少服务端的资源开销。详细示意图如下：



用户规则清洗

c）大数据智能分析

黑客为了构造大量的数据流，往往需要通过特定的工具来构造请求数据，这些数据包不具有正常用户的一些行为和特征。为了对抗这种攻击，可以基于对海量数据进行分析，进而对合法用户进行模型化，并利用这些指纹特征，如：Http模型特征、数据来源、请求源等，有效地对请求源进行白名单过滤，从而实现对DDoS流量的精确清洗。



指纹过滤清洗

d）资源对抗

资源对抗也叫"死扛"，即通过大量服务器和带宽资源的堆砌达到从容应对DDoS流量的效果

网易云DDoS 高防拥有1T 超大防护带宽，为您提供超强的 DDoS 攻击保障服务，点击可免费试用。

以上文章来自网易云社区的博文《理解DDoS防护本质：基于资源较量和规则过滤的智能化系统》。

相关文章：
【推荐】大公司怎么做Android代码混淆的?
【推荐】细嚼慢咽 Mongoose 5
【推荐】四步走查智能硬件异常Case

0人点赞 > 日记本 ···

"小礼物走一走，来简书关注我"

赞赏支持

还没有人赞赏，支持一下

网易云社区 网易云社区是网易云旗下，由网易实践者社区、网易资深产品技术和... 关注
总资产28 (约2.54元) 共写了172.1W字 获得812个赞 共597个粉丝

写下你的评论...

全部评论 0 只看作者 按时间倒序 按时间正序

被以下专题收入，发现更多相似内容

DDoS防御系列

推荐阅读 更多精彩内容 >

什么是 DDoS 攻击?
欢迎访问网易云社区，了解更多网易技术产品运营经验。 全称Distributed Denial of Service...
yijian2595 阅读 39 评论 0 赞 0

漫画告诉你什么是 DDoS 攻击?
如今大流量网络攻击正逐渐呈现增长趋势，前不久锤子科技的发布会以及9月12日苹果官网宕机的案例就印证了这一点。那什么...
grain先森 阅读 1,586 评论 4 赞 40

2017年Q1全球DDoS攻击情况洞察
1. DDoS简介： 1.1 DdoS定义： DDOS是什么？分布式拒绝服务(DDoS:Distributed D...
木木是个乖宝宝 阅读 2,535 评论 2 赞 8

115.DDos攻击及预防
参考http://blog.csdn.net/huwei2003/article/details/45476743...
鱼仔_1625 阅读 791 评论 0 赞 5

读《毛姆短篇小说选》随想随记
读《毛姆短篇小说选》随想随记 《女佣》 书中被毛姆称之为宝贝的，是一个女佣。 那个女佣家政事...
玉米面糊糊 阅读 358 评论 0 赞 0