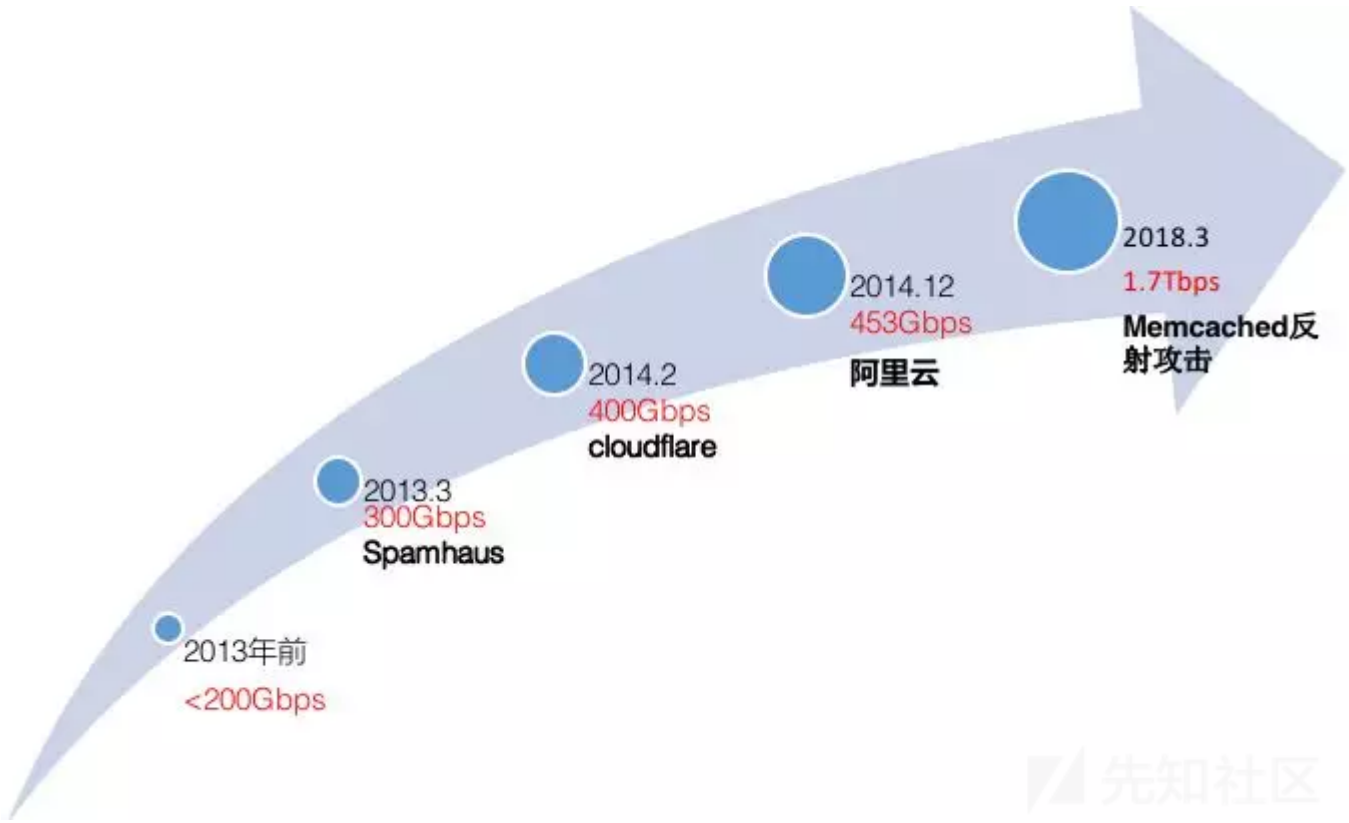
DDoS攻防：一场古老战争的"新发展"

阿里云安全技术 / 2018-10-26 08:05:00 / 浏览数 2724 技术文章 技术文章 顶(0) 踩(0)

---

1. DDoS趋势的一些变化

从今年3月份起，世界上最大的DDoS攻击记录到了1.7
Tbps，是一个普通家庭带宽出口的数十万倍，几乎可以横扫互联网，作为一个生存了20年之久的古老攻击形式，我们看到了今年来DDoS攻击量成指数级攀升，不仅没有出现



1.1 DDoS攻击的成本究竟有多高

美国云安全技术服务公司Armor发布的一份报告揭示了暗网上针对各种网络犯罪相关服务实施的价格标准。该报告是通过搜罗数个知名的暗网市场数据总结出来的。据报告显

WordPress Exploit	$100
Password Stealer	$50
Android Malware Loader	$1,500
Western Union Hacking Bug For World Wide Transfer	$300
DDoS Attacks	Week long attack $500 - $1,200
ATM Skimmers: Wincor, Slimm, NCR, Diebold	$700 - $1,500

数据来源：freebuf

另外，从搜索引擎上也可以搜到很多类似的攻击平台，DDoS攻击即服务，黑客跑的一点也不慢。

1.2 DDoS防御为什么这么贵

众所周知，防御海量的DDoS攻击，就必须要有海量的防御带宽，我们经常看到很多的客户提问说，主机上看到的恶意DDoS的IP是否可以用安全组或者软件防火墙封禁掉，

DDoS防御的主要成本是带宽、机房资源、服务器和清洗设备，这些都属于重资产资源，目前业界几种产品形态分别存在于运营商、云厂商、CDN厂商或者是IDC机房中，但

2 上云后的DDoS防御最佳实践

依据防御能力的不同，阿里云上有不同的产品形态可以供用户选择，在企业上云的不同阶段，面临的威胁不同，也可以选用不同的防御产品来构建自身的安全体系，如下是阿

2.1 DDoS基础防护

云产品默认自带的防御能力，针对海量客户提供500M-5G的免费抗D能力，加入安全信誉联盟之后，可以累积信誉值，获得比5G更高的能力（限次）。

2.2 DDoS防护包

提供比5G更高的增值防御能力，用户可以不改变任何配置，直接提升云产品的防御能力，部署简单方便。

2.3 DDoS高防IP（BGP多线）

针对海量DDoS攻击的场景，需要把流量引入大流量清洗中心清洗，清洗完之后送回用户的主机，相较与业界产品，阿里云用户可以享受到专线回源，独享海量防御带宽的优

2.4 游戏盾

针对攻击的重灾区游戏行业推出的端到端到无上限防御方案，防御DDoS攻击，CC攻击，游戏连接性攻击等各种复杂攻击，提供按照业务规模收费的成长性服务机制。

3 探索抗D服务的几个发展方向

3.1 不设上限防御服务

如今，一般的云厂商都具备了上T的防御能力，运营商也在逐步开放一些能力，防御方的实力大大增强，我们已经观察到了国外有厂商开始提供这种“unlimited”的服务，尽量

3.2 贴近业务，更具备成长性

遭受DDoS攻击的企业，一般还是以中小企业为主，目前DDoS防御的手段多以攻击流量的大小来进行收费。但是，1.7T的攻击出来之后，一般的企业基本上无法付费防住这

3.3 更快更稳的网络质量

抗D服务是一种应急类的安全产品，在出现攻击的时候，需要用最快的反应时间来防御住攻击，因此客户一般会常态化的将业务跑在高防机房里。高可用的网络质量也是一个

3.4 数据与可视化

另外一方面，随着DDoS攻击的不断发展，其攻击手段越来越复杂。在海量DDoS攻击发生的时候，完整的记录下攻击的详细日志，形成快速有效的实时分析数据，相比很多

4 对于DDoS终局的一些思考

这几年，我们发现无论是攻击手段的翻新还是防御厂商的增多，整个市场似乎出现了非常火热的现象，这其实跟整个互联网环境的变化息息相关。诸多防御厂商的涌入带来的

就任何一种攻击而言，没有攻击就没有防御。我们相信，只要互联网还存在，DDoS攻击就不会消失。当5T、10T的攻击来临的时候，也许只有所有的厂商联合起来，才能真

这一切，还只是刚刚开始。

上一篇：Mac恶意软件拦截加密web流量注入广告 下一篇：区块链安全—分析P2P网络攻击及密...

1. 0 条回复
   - 动动手指，沙发就是你的了！