腾讯云大禹分布式防御

产品白皮书

[2015.11.25]

[V1.0]

腾讯云

目录

1

1 互联网蓬勃发展，这是最好的时代

1.1 中国互联网业正在高速发展

根据中国互联网协会《中国互联网站发展状况及其安全报告（2015）》和 CNNIC《第 35 次中国互联网络发展状况统计报告》披露的数据。近年来，我国互联网市场规模和用户体量高速增长，截至 2014 年 12 月底，网站总量保持规模化发展，为 364.7 万个，网站使用的独立域名为 481.2 万余个，互联网接入服务商达 1068 家，网民规模达 6.49 亿，手机网民规模达 5.57 亿，互联网普及率达到 47.9%，中国已经成为全球最大的互联网市场。

1.2 万众创新，互联网创业正当时

在 2015 年 3 月 6 日中国总理李克强的政府工作报告中，正式提出了"互联网+"的概念，并制定国家级"互联网+"行动计划以推动经济进一步发展。万众创新、大众创业的时代已经来临，大批优秀人才投入到互联网创业的大潮中，一大批新型互联网企业如雨后春笋般兴起，渗透餐饮、医疗、教育等社会经济、生活的方方面面，改变着人们生活的方式，提升国民的生活品质。这是一个最好的时代。

2 攻击横行，这也是糟糕的时代

2.1 DDoS 攻击事件频发

在互联网产业飞速发展的同时，网络中 DDoS 攻击等各类恶意攻击行为也在不断增多。以域名系统为例，2014 年针对我国域名系统的流量规模达 1Gbps 以上的拒绝服务攻击事件日均约 187 起，约为 2013 年的 3 倍。根据业界相关机构的监测，珠三角等经济发达地区，为 DDoS 攻击的重灾区，游戏、视频等新兴行业也成为 DDoS 攻击的高发地带。DDoS 攻击已成

为敲诈勒索、恶意竞争的手段，在利益的驱逐下，DDoS 攻击有愈演愈烈之势。

2.2 针对重要网站的域名解析篡改事件频发

2014 年发生了多起国内政府网站、重要媒体或企事业单位网站的域名解析被篡改的事件。2014 年 1 月 21 日，出现全国 DNS 被污染事件，导致中国出现大范围网络访问异常故障。

不断涌现的 DDoS 攻击等各类恶意行为，已经严重阻碍中国互联网产业的正常发展，这是一个最好的时代，但也是一个糟糕的时代。面对如此严峻的挑战，互联网企业该如何应对？

3 大禹产品概述

3.1 大禹，DDoS 防护专家

腾讯云大禹分布式防御产品（Dayu Distributed Defense）是腾讯云安全团队多年来自研安全技术积累的成果。大禹分布式防御产品（后称：大禹产品）基于腾讯遍布全国的防护节点和先进的 DDoS 防护算法，可为网站、APP、游戏等丰富业务场景的开发商们提供专业的 DDoS 防护服务。

3.2 分而治之，大禹核心理念

面对汹涌的大流量的 DDoS 攻击，依托腾讯遍布全国的防护网络，通过灵活的调度算法，将攻击流量分散调度到就近的防护节点进行清洗，是腾讯云对 DDoS 攻击的应对之道。“分而治之”，是大禹产品的核心理念。

腾讯云安全团队在全国搭建了众多高强度的攻击防护点。每个攻击防护点均独立部署，和其他腾讯自营业务进行完全隔离，并且为后续的防护能力升级提前进行了网络规划。当前系统中的攻击防护点具备攻击防护影响的最小化，以及防护能力升级的便捷化。

腾讯云安全团队针对 DDoS 攻击的流量特点自研了一套高效流量调度算法，借助腾讯云移动加速服务的全网流量调度能力，实现了攻击发生时的就近最优调度，保证开发商业务的高可用性。

3.3 大禹产品架构

大禹产品主要由以下三个部分组成：智能调度系统、攻击防护节点、宙斯盾系统。

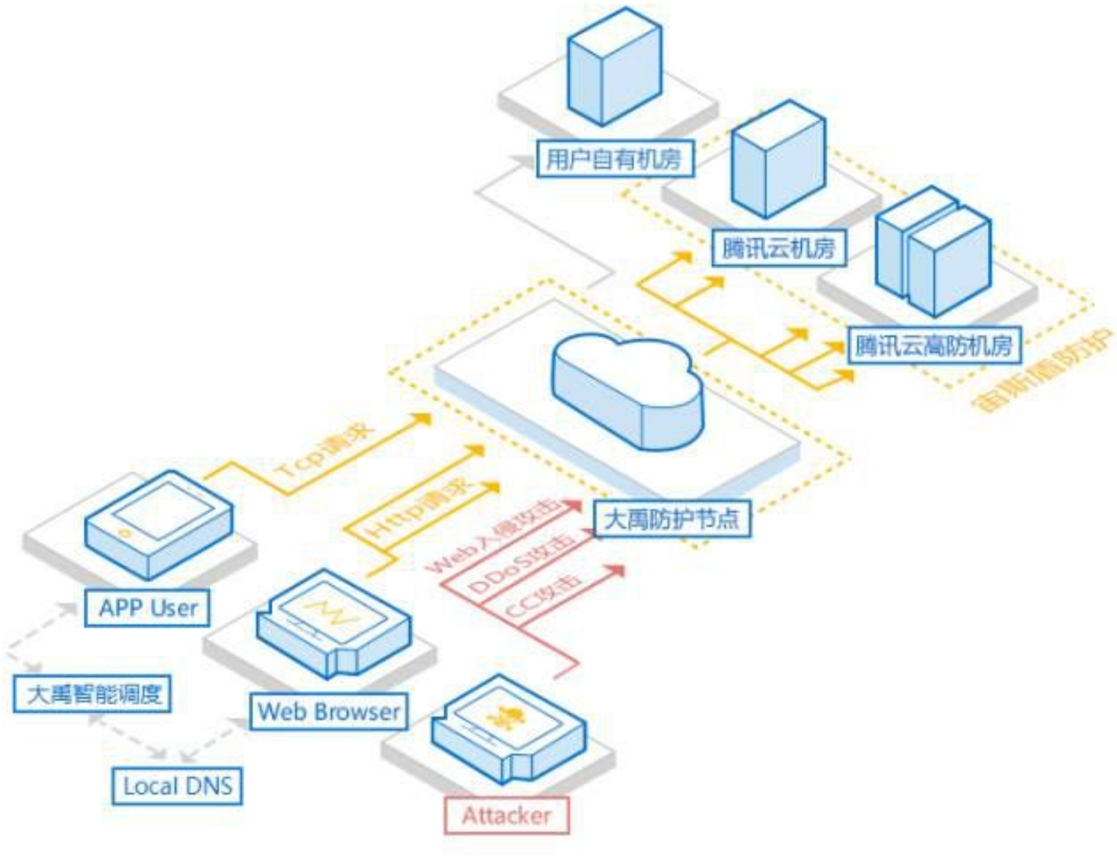

图 3- 1 大禹产品网络架构图

3.3.1 智能调度系统

a）域名解析：为接入大禹系统的域名分配防护域名，可隐藏客户的源站 IP。当客户接入大禹系统后，用户访问客户域名时，流量会跳转至大禹为该客户分配的防护域名，此时智能调度系统会对该域名进行动态解析，将流量引流至相应的攻击防护节点。

b）网络监控：智能调度系统会对流经各个防护节点的流量，以及各个防护节点到客户源站的回源率等网络质量指标进行实时监控。

c）流量调度：当检测到有大流量 DDoS 攻击或者 CC 攻击，智能调度系统会将流量动态调度到新增的防护节点或者腾讯云高防专区，保障客户业务的正常。

3.3.2 攻击防护节点

对访问流量中的攻击流量进行过滤，并将正常流量转发到客户源站，如果客户的源站在自有机房，则转发至客户自有机房，若客户源站在腾讯云机房，则转发流量至腾讯云机房。

3.3.3 宙斯盾系统

宙斯盾系统，是腾讯的通用 DDoS 防护系统，具有超强的 DDoS 检测清洗能力，在腾讯云高防专区进行部署，可以对超大流量的 DDoS 攻击进行防护。

3.4 大禹适用场景

3.4.1 网站

大禹产品支持基于 TCP，HTTP 和 HTTPS 协议的网站类业务。可为网站提供 DDoS 防护、流量加速、域名安全认证、网站漏洞防护等一系列服务。

3.4.2 移动 APP

大禹产品支持 iOS 和安卓系统上基于 TCP，HTTP 协议的移动端业务。

3.4.3 游戏

大禹产品支持各类主流游戏开发框架，例如 cocos2d-x， unity3D 等。

4 大禹为网站提供全方位的防护

4.1 DDoS 和 CC 防护抵御流量攻击

大禹产品可对各种主流 DDoS 攻击提供四到七层的防护，可对 CC，ISYN Flood、ICMP Flood 等各类 TCP Flood、UDP Flood 攻击进行防护。

2015 年上半年，腾讯云安全经受住了最严峻的 DDoS 攻击考验，有数千台主机遭受外部黑客 1 万多次 DDoS 攻击。峰值月份受到 DDoS 攻击次数达到 2600 多次。最高月份防护峰值接近 300Gbps。

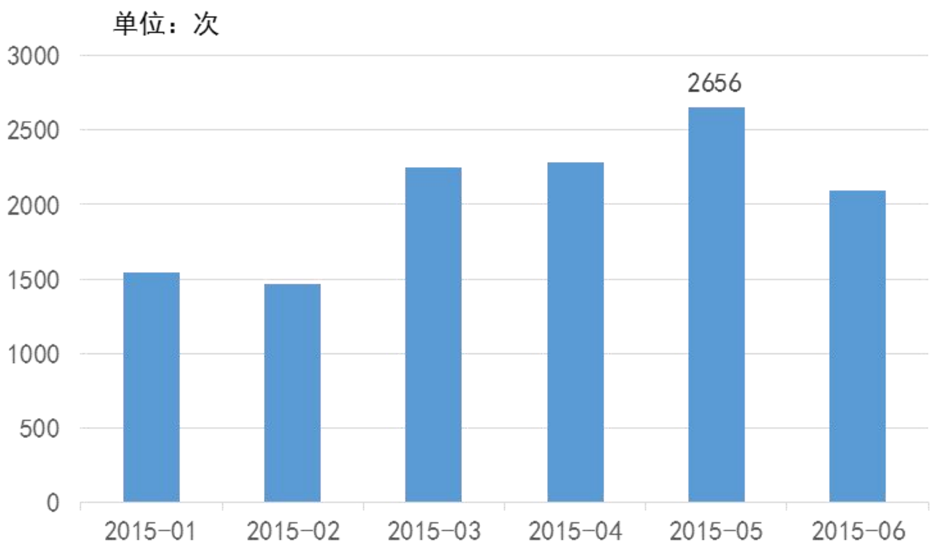

图 4- 1 腾讯云 2015H1 遭受 DDoS 攻击趋势

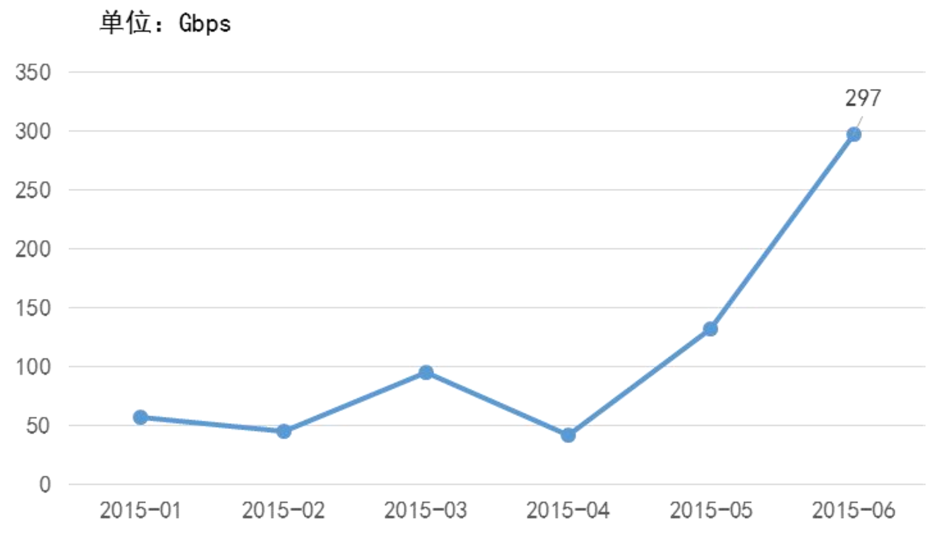

图 4- 2 腾讯云 2015H1 遭受 DDoS 攻击流量峰值趋势

针对 CC 攻击，大禹产品提供了针对 QPS 和访问频率的灵活防护策略，并将防护策略开放给客户。客户可根据实际业务需要，对特定的域名开启 CC 防护，并设置基于 QPS 和用户访问频率的防护策略，有效对抗 CC 攻击。

4.2 WAF 强化网站安全

大禹产品集成了腾讯自研 WAF 产品，可为客户的 Web 应用提供实时防护，可为客户提供以下功能：

a) 漏洞攻击防护:目前可拦截常见的 web 漏洞攻击，例如 SQL 注入、XSS 跨站、获取敏感信息、利用开源组件漏洞的攻击等常见的攻击行为。

b) 虚拟补丁:可提供 0Day，NDay 漏洞防护。当发现有未公开的 0Day 漏洞，或者刚公开但未修复的 NDay 漏洞被利用时，WAF 可以在发现漏洞到用户修复漏洞这段空档期对漏洞增加虚拟补丁，抵挡黑客的攻击，防护网站安全。

腾讯云大禹 WAF 具有如下两个特点：

a) 实时防护：可实时阻断黑客通过 web 漏洞试图入侵服务器、危害用户等恶意行为；可以实时屏蔽恶意扫描程序爬虫，为您的系统节省带宽和资源。

b) 零成本开通:网站安全防护无需配置 DNS 指向及其他网络配置，一键开通，不影响业务的正常运作。

4.3 DNS 劫持检测保障业务通达

DNS 劫持是一种通过改变指定域名在运营商侧 Local DNS 配置的解析地址，将该域名的解析结果重定向到劫持 IP 的行为。为了快速发现针对业务域名的 DNS 劫持，腾讯云采取了分布式探测和集中分析防护相结合的架构模型。通过在全国部署 400+个探测指针，周期性地向本地的 Local DNS 发送域名解析请求，并对响应结果进行集中汇总和分析匹配，从而快速、准确、全面的发现域名劫持行为,保障客户的业务通达。

4.4 安全认证彰显网站实力

腾讯云可为大禹产品客户提供安全认证服务，通过认证的客户户将将在腾讯各渠道获得专属腾讯云认证展示，让您的业务获得腾讯亿万用户的认可，具体如下：

a) QQ 对话框安全链接认证展示：

图 4- 3 QQ 对话框安全认证展示

b) 网站认证展示：

图 4- 4 网站认证展示

5 大禹产品典型案例

5.1 大禹为土巴兔保驾护航

土巴兔是中国家装 O2O 行业的领军企业，在互联网+时代业务发展迅猛，用户和业务成交量迅速不断提升。在业务发展的同时，受到了来自黑产团队的滋扰，一度深受 DDoS 攻击，影响业务发展。对与初创企业来说，为了应对 DDoS 的挑战，去不断扩带机房出口带宽和自建一套攻防体系，是成本巨大的和难以做到的。在了解腾讯云大禹产品后，土巴兔迅速选择接入大禹产品，由大禹为其阻挡各类恶意攻击。通过使用大禹产品，土巴兔以最低的成本获得了网站的安全稳定，从而可以更专注地致力于其公司业务的发展。

5.2 大禹助力锤子手机发布会

2015 年 8 月 25 日晚,锤子科技举办坚果手机发布会，其官网同步直播并开展抢购活动。发布会即将开始时，锤子科技官网遭 DDoS 攻击，网络直播中断，发布会现场紧急暂停，200 万用户在线等直播。危急之际，锤子科技于 20:05 紧急联系腾讯云安全大禹团队，大禹团队立即启动互联网应急救援预案，做配置、接域名、洗流量、业务恢复，一气呵成，在大禹系统的强力保障下，锤子官网各项业务一一恢复正常，20:17，直播恢复，发布会召开，22:30，坚果手机在线预售，22:39，手机售罄。

6 大禹产品的关键优势

6.1 超大的防护带宽

依托于遍布全国的 100+防护节点，大禹产品总共拥有 4T 的防御带宽，可为客户抵御超大流量的攻击。

6.2 访问加速能力

大禹产品的防护节点是基于腾讯云移动加速服务的加速点和静态加速的节点升级而成，因此大禹的客户，除享受 DDoS 防护服务外，还可以通过大禹实现业务访问加速。

6.3 快速的接入

客户接入大禹产品，无需对其源站或机房进行改动，只需在腾讯云开通大禹产品服务，开通后服务后，腾讯云会为客户生成一个大禹防护域名。客户再到其 DNS 服务提供商处，将其防护域名 cname 为大禹防护域名，即可完成大禹产品的接入。整个接入过程，最快可在几分钟内完成。当攻击发生时，可及时响应，保障业务的稳定。

产品介绍地址：http://www.qcloud.com/product/ddd.html

产品开通地址：https://console.qcloud.com/dayu/vip