SECURITY NSFOCUS

2015H1 绿盟科技 DDoS 威胁报告

2015 H1 NSFOCUS DDoS THREAT REPORT

目录

执行摘要

2015 年上半年报告中，绿盟科技发现 DDoS 攻击存在两极分化的态势，大流量攻击不断增长（>100G 的攻击有 33 起）并开始走向云端，小流量攻击（1 分钟以下 42.74%）变身脉冲及慢速攻击，主要针对行业业务特性。在此背景下，攻击流量呈现混合化，并以 UDP 混合流量为主（72%）。

面对如此恶劣的 DDoS 攻击态势，主管机构、运营商、行业组织、厂商及用户都在不断开展 DDoS 治理及缓解工作，在解决方案方面，除了本地清洗、云清洗方案之外，更出现了分层清洗、信誉云及近源清洗多种方案及实践。

于此同时，基于 SDN 的攻击模式及缓解技术，更让笔者眼前一亮，由此也预测这些演变将与云计算及大数据一起，催生 DDoS 防护向下一代 DDoS 防护及 APT 时代迈进。

特别声明

本次报告中涉及的所有数据，来源于绿盟科技的自身产品、网络监测和合作伙伴的提供。所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在报告中。

如果您需要了解更多信息，请联系：

扫描二维码，在线看报告

前言

多年来，绿盟科技致力于帮助客户实现业务的安全顺畅运行。每天，绿盟科技的防护产品和监测系统会发现数以千计的 DDoS（分布式拒绝服务）攻击危害客户安全。为了快速反馈 DDoS 攻击的相关信息，绿盟科技发布《2015 H1 DDoS 威胁报告》。本报告为 2015 年上半年报告，用于快速跟踪及反馈 DDoS 威胁发展态势。如果您需要获取全年报告《2015 DDoS 威胁报告》，请跳转到该章节，了解相关信息。

DDoS 攻击态势

> Because of the closed context of the original ARPANET and NSFNet, noconsideration was given to denial-of-service attacks in the ori ginalInternet Architecture. As a result, almost all Internet services are vulnerable to denial-of-service attacks of sufficient scale.
>
> ---RFC 4732

观点 1：大流量攻击呈现增长趋势

国外带宽及互联网用户发展态势

在美国，美国联邦通信委员会（FCC）CC 对宽带重新定义：下行速度从 4Mbps 调整至 25Mbps，上行速度从 1Mbps 调整至 3Mbps。全球的互联网用户 2008-2012 共 4 年的年平均增长率高达 12%，2013 互联网用户数比例已经超过人口的 37.96%，预期在 2015 年用户数量可以超过 30 亿。

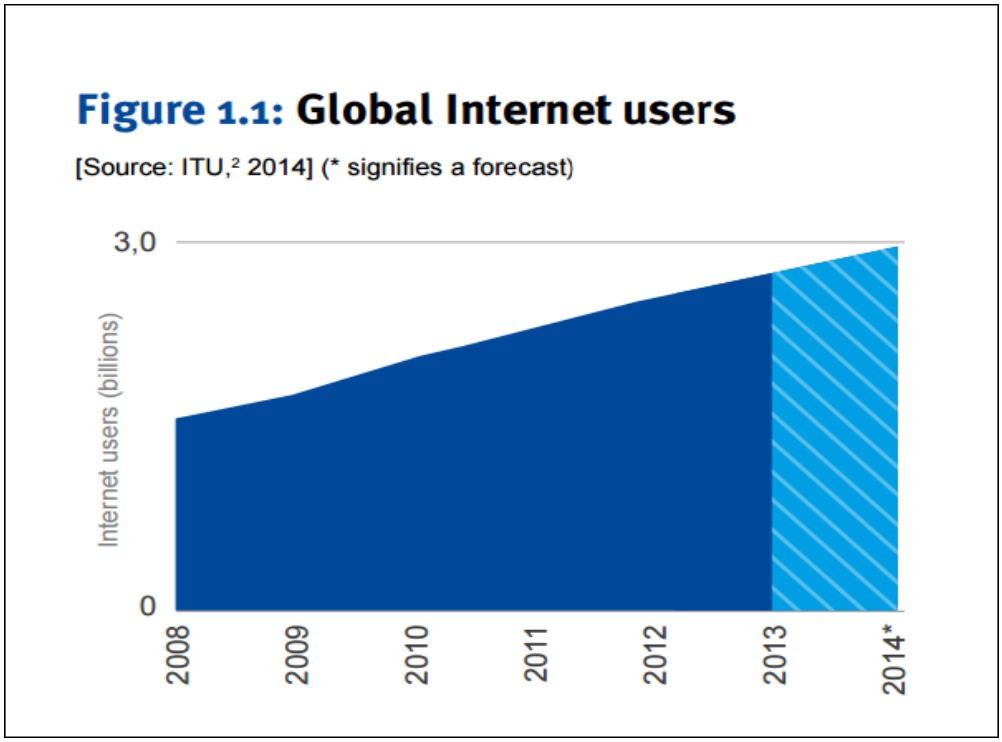


图 1.1　全球互联网用户增长趋势

随着带宽增加，每个连接的速度也在相应提升，根据 Internet Society 预测 2013-2018 年期间的增幅将达到 35%左右，流量显著提升，从中也可以看到平均每个连接的每月总流量也在持续升高。

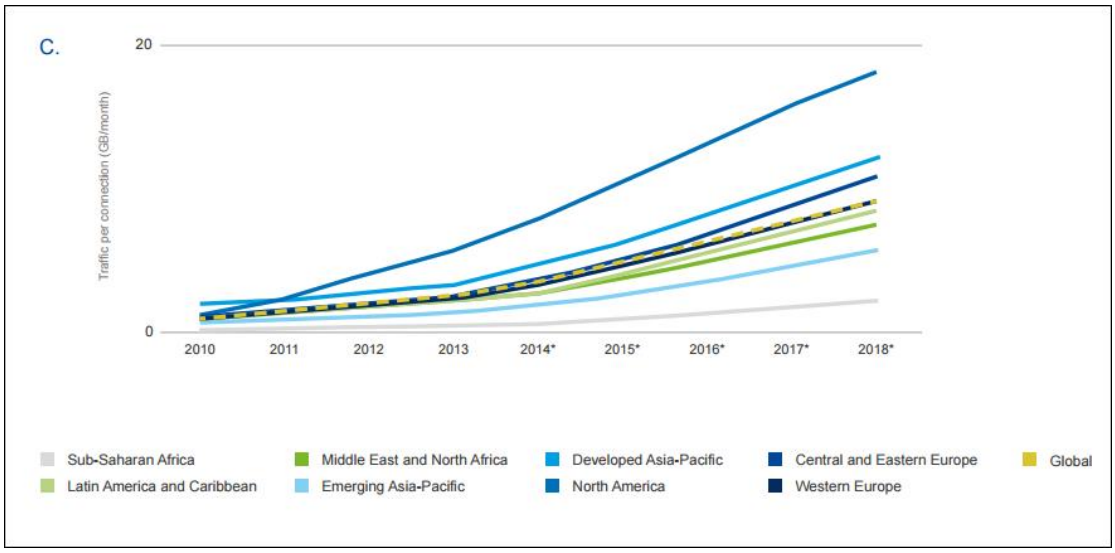


图 1.2　每连接速度增长趋势

中国出口带宽及互联网用户发展态势

十二五以来，随着“宽带中国”战略实施方案的推进，城市和农村家庭宽带接入能力逐步达到 20 兆比特每秒（Mbps）和 4Mbps，部分发达城市达到 100Mbps，宽带首次成为国家战略性公共基础设施。根据 CNNIC 的统计，中国国际出口带宽呈现非常快速的增长趋势。与此同时，中国的网民规模也在大幅度提升，5 年来平均增长幅度达到 7.2%，2014 年接近 6.5 亿。

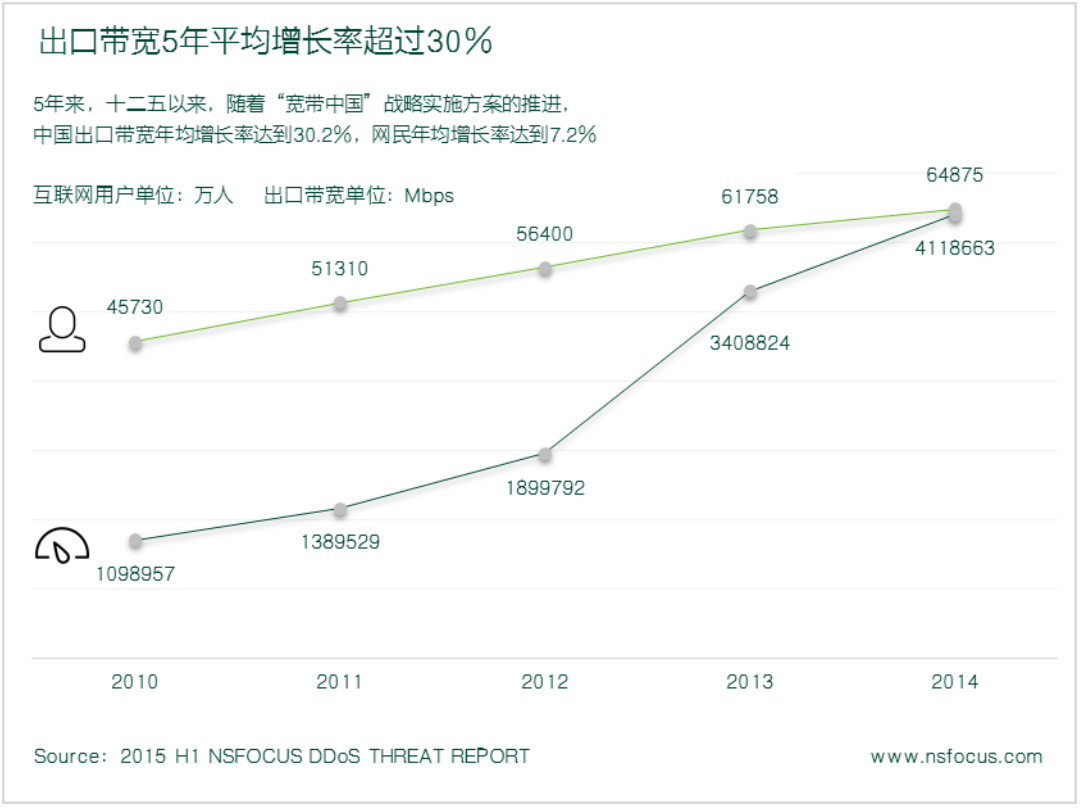


图 1.3　出口带宽增长幅度

宽带标准被调高和联网用户（设备）增多，在方便用户使用的同时，也为大流量 DDoS 攻击的出现创造了条件，加之设备厂商和消费者在安全意识方面需要提升，这方面的因素也助长了 DDoS 放大式攻击的发生，这些方面都直接导致了 DDoS 风险的增高。

本报告数据显示，在 2015 年大流量 DDoS 攻击仍旧在持续增加。2015 年上半年，至少出现 33 起流量超过 100G 的攻击，集中在 6 个相对独立的 IP 上。从全国范围分布上看，排名前五的城市包括上海、成都、东莞、济南、天津。

图 1.4　100G 以上被攻击区域分布

另外，从多年来为运营商服务的数据来看，也可以看到在 2015 年上半年的 DDoS 攻击中，百 G 以上的攻击频次明显增大。以某运营商为例，2015 年受 100G 以上流量攻击的 IP 数增长到 1675 个，攻击的次数增长到 3729 次，照此计算 100G 以上的攻击总量已经超过 300T。这个趋势相比 2014 年 IP 数量有所增长，单 IP 受到 100G 以上流量攻击的次数也明显上升。而 100G 以下的攻击总量要远远超过这个数量。

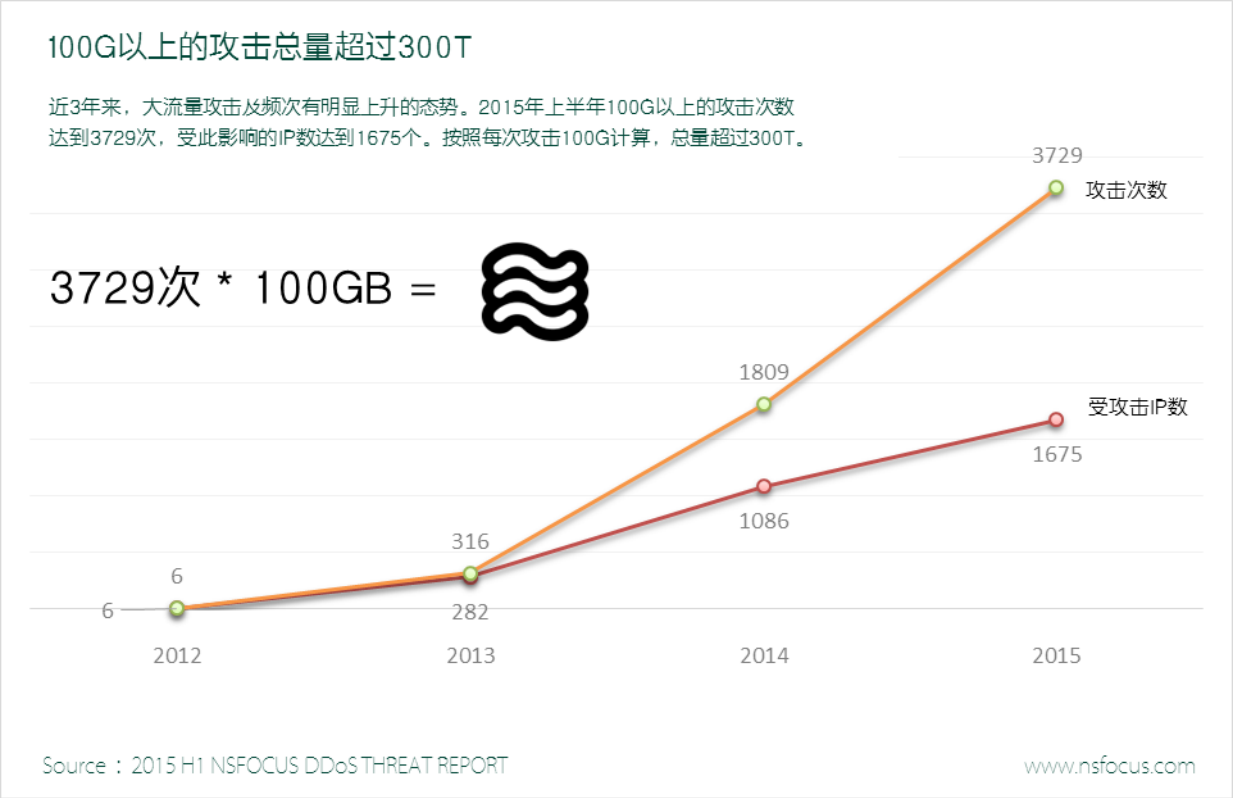


图 1.5　100G 以上攻击流量历年增长趋势

事件：历史上的 DDoS

纵观过去的 5 年间，DDoS 大流量攻击事件数不胜数，这里仅列出比较有代表性的几次事件，从这些事件中可以看到大流量攻击逐步抬升的态势。

- 2013 年 3 月 26 日　　欧洲反垃圾邮件组织 Spamhaus 受到 300G+的 DDoS 攻击
- 2014 年 2 月 11 日　　CloudFlare 透漏其客户遭受 400G 的 NTP Flood 攻击，刷新历史 DDoS 攻击的流量峰值外，使得 NTP Flood 攻击备受业界关注。
- 2014 年 12 月 20 日　　阿里云发布声明称其遭受攻击峰值流量 453G 的攻击
- 2015 年 1 月　　国外某安全厂商发现了一次大型 DDoS 攻击，334Gbps 的垃圾数据流攻击了一家亚洲网络运营商的数据中心，事件的发生时间在 2015 年一月至三月之间。

这一趋势在 2014 年的报告中已经呈现出来[①]，DDoS 攻击峰值流量逐年上升，这一方面是由于攻击技术的不断发展，另一方面也是由于网络带宽等可利用资源显著增加。这一趋势通过历年的 DDoS 事件来看，不会有大的变化。

计算器：动手算 DDoS 损失

这些 DDoS 的攻击将会给业务带来多少损失？这里我们提供一个计算器，通过几个常规项的计算，让大家可以更为直观的感受 DDoS 攻击将会给业务带来的影响。

① 2014 绿盟科技 DDoS 威胁报告，http://www.nsfocus.com.cn/upload/contents/2015/03/20150304131640_45210.pdf

业务营收及成本统计

统计项	金额(万元)
业务每月营收	4000
每年带宽租用费	50
固定资产投入	800
每月研发、运维人员投入费用	150
每月机房托管费用(托管机房选填)	100
每月机房维护费用(自建机房选填)	0

DDoS 攻击带来的损失统计（一个小时）

统计项	金额(万元)
营收损失	5.56
带宽租用费损失	0.01
固定资产成本损失	0.03
人员投入费用损失	0.21
机房托管费用损失	0.14
机房维护费用损失	0.00
小计	5.94

样例数据仅供参考
读者可以自行修改上面表格中的数值
右边就可以自动计算出损失情况

业务遭受 DDoS 攻击时间统计(每月)

统计项	统计值
业务每月遭受 DDoS 攻击次数(次)	2
业务每次 DDoS 攻击时长(小时)	2
业务每月遭受 DDoS 攻击总时长(小时)	4.00

DDoS 攻击带来的经济损失合计（一个月）

统计项	金额（万元）
合计	23.76

观点 2：大流量攻击走向云端

在 DDoS 大流量攻击兴起的同时，为了抵御风险免受其害，许多用户将其业务向云端迁移，云计算技术的诸多优点使得云服务得以广泛应用。中国信息通信研究院的报告[①]显示，我国公共云服务市场规模大概在 72 亿元左右，比去年增长 47.5%。中国私有云市场规模也在不断扩张，2014 年国内私有云市场规模大概在 246 亿人民币左右，增长速度将近 30%。

云服务的增多在为用户带来了便利的同时，也在安全方面也带来了两个方面的变化，1 客户端轻量化，客户端原本的计算任务，大幅度向云端转移，云端的流量会越来越大，这将会被大流量 DDoS 攻击所利用；2 环境复杂化，随着业务环境虚拟化，从业务更加灵活多变到运维管理，其中不断产生新的不确定性，都可能为新的 DDoS 攻击形式创造机会。这些可能的攻击形式，下面做简要的描述。

攻击模式及路径

云计算及云服务多种多样，但从基础架构的角度来说，业界比较公认的理论将其分为 3 层基础架构。IJANA 从这 3 层基础架构进行分析，给出了给出了云架构下可能面临的攻击手法，同时给出了云中的 DDoS 攻击场景。传统的安全防护手段依然能起到一定的防护效果，但不能防护同层基础架构中虚拟机之间的东西向攻击。虽然市场上已经有（国外的）虚拟化防火墙，但部署较少，且相关技术有待完善。

① 《中国公共云服务发展调查报告（2015 年）》

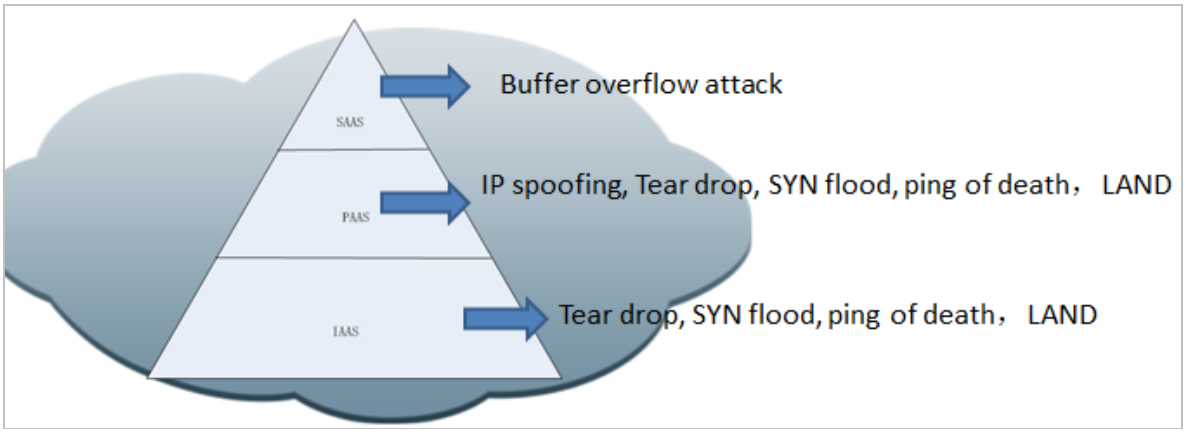


图 1.6　云基础架构

另外，从攻击路径来说，一般情况下按照攻击者所处的位置，可以大致分为三种攻击路径，1 从公有云发起的攻击；2 从私有云发起的攻击；3 从云外部发起的攻击，这三种攻击路径按照攻击目标的不同进行叠加，至少会产生 6 种攻击路径（见下图）。

在企业私有云场景中，需要考虑的不仅仅是来自外部②的攻击，也需要防御内部的攻击，这里的关键在于云是否有配置对内部流量的清洗，内部的流量是否经过清洗检测设备，也就是①类型的攻击需要进行防御，另外，对于内部向外的攻击③也可能存在。

在公有云的场景中，对于③④这样的攻击类型较为困难，因为云资源动态分配和动态拓扑，可以有效的进行流量负载平衡，且云服务商的流量清洗机制可以有效缓解这种攻击类型，这也就是很多的业务都愿意迁往云端的原因。但有一类攻击类型虽然在目前阶段很少看到，但较为隐蔽，后续随着云端服务的竞争，很容易出现这种攻击形式。比如下图中的⑤。这种攻击形式，攻击者可能从相同的物理网络甚至同一物理机上发起攻击，此时流量将在本地虚拟交换机或者 Hypervisor 上处理，并不会经过外部的流量检测及 DDoS 防护设备。这种风险成为现在已知的云端 DDoS 风险。

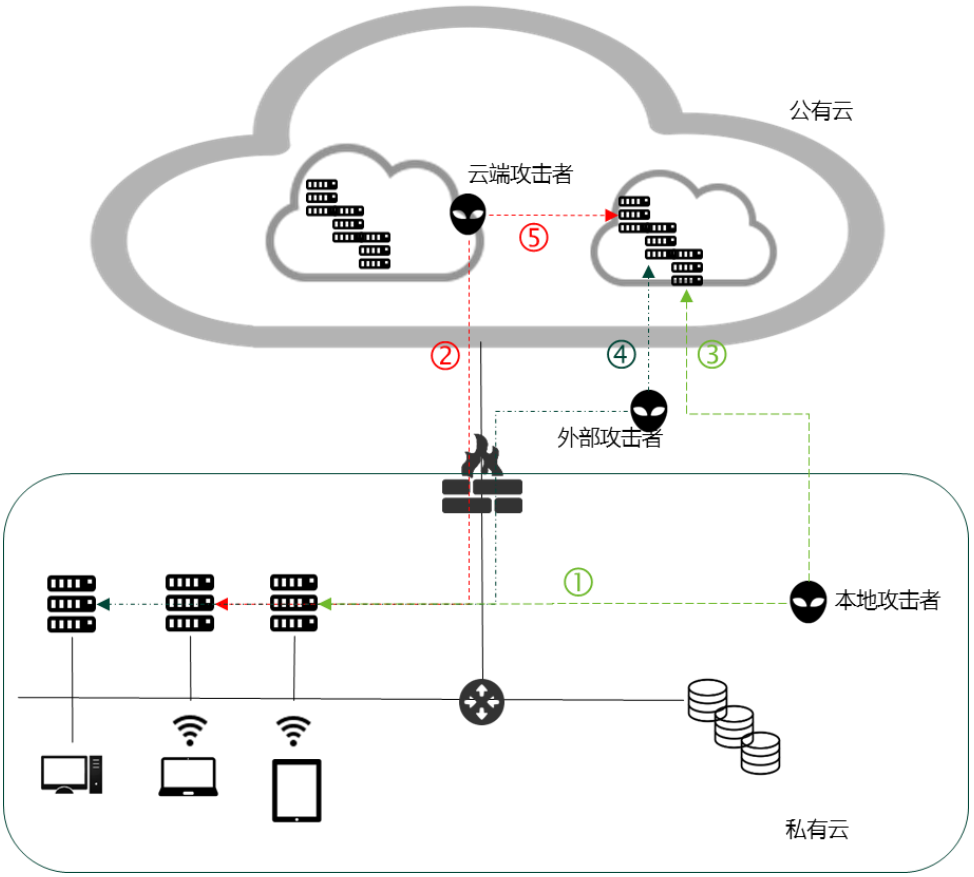


图 1.7　云攻击模式及路径

SDN 控制器成风险

在云计算体系架构中有一项关键性技术 SDN，它为网络的计算资源和存储资源的动态分配提供了易管理的机制，业界已经有厂商利用 SDN 技术实现 DDoS 防护的案例，但恰恰是这一点使其成为云内的安全薄弱环节。

在下面这张图中，我们将上图的攻击形式⑤进行微观放大，以便呈现这种涉及 SDN 控制器的云内 DDoS 攻击形式。在这个微观呈现中，至少会有两种可能发生的攻击形式。1 SDN 控制器被 DDoS 攻击后，造成数据调度的混乱，使其管理的网络大面积受到影响乃至瘫痪；2 SDN 控制器为了保持自己可用，将所有数据流导向被攻击的虚拟主机，最终造成虚拟主机被攻击直至瘫痪。

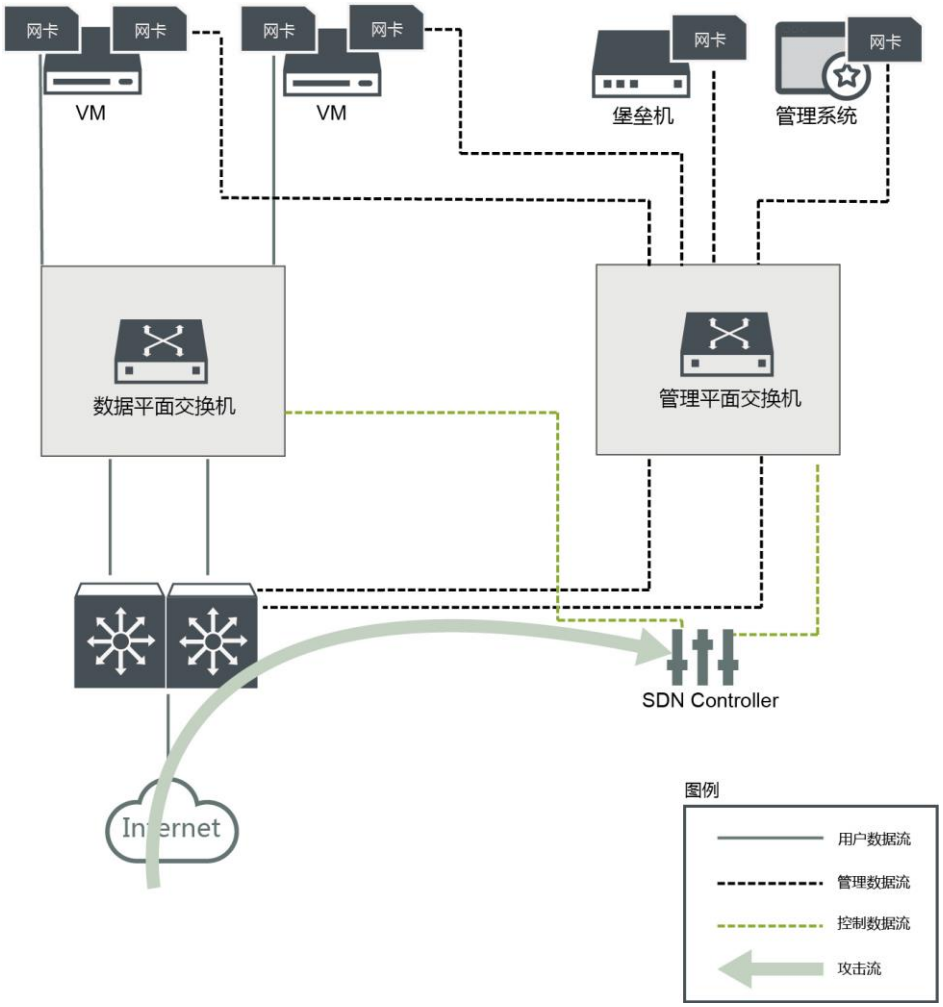


图 1.8　SDN 控制器被攻击风险

观点 3：大流量攻击在游戏行业中加剧

大流量攻击在影响着各个行业，在近几年的分析中，绿盟科技的技术专家观测到游戏行业遭受大流量攻击的情况在逐年增加，在 2014 年的报告中，我们将这种现象称之为“行业潮流性”[①]，即攻击者不仅会预估收益选择攻击目标，更能够根据行业业务特性演变攻击形式。

① 绿盟科技 2014 H1DDoS 威胁报告，http://www.nsfocus.com.cn/upload/contents/2015/03/20150304135825_91376.pdf

2015 年上半年的数据显示，游戏行业仍然是 DDoS 攻击的重点对象之一。游戏行业用户基数大、用户类型多、在线维护难度大的特点，也使得游戏行业成为极易受到攻击的目标行业。由于很多游戏基于私有协议开发，传统 DDoS 防御手段在没有贴合业务特性的情况下，防御 DDoS 攻击常常面临较大困难。

以某大型互联网企业为例，在其多项业务中，在线游戏仍然是 DDoS 主要的攻击对象（74.7%），DNS 服务及 Web 服务分别为 15.1%及 9.7%。通过对各项服务的展开分析可以看到，除了游戏业务以外，Web 服务及其他服务中 UDP 攻击的比例也不在少数。

而 UDP 攻击中尤以反射型攻击较为常见，这一现象延续了我们在 2014 年报告[①]中预测，“从防护角度看反射式 DDoS 攻击易于检测与缓解，这是因为攻击数据包的源端口相对固定；然而从攻击角度看，这种 DDoS 攻击方式具有隐匿攻击者真实身份、攻击者无需组建僵尸网络、对攻击者的网络带宽要求小等优势。在 2014 年下半年，基于 SSDP 协议 DDoS 反射式攻击次数显著上升。预计这种高效、低成本的 DDoS 攻击形式，在 2015 年还将持续出现。

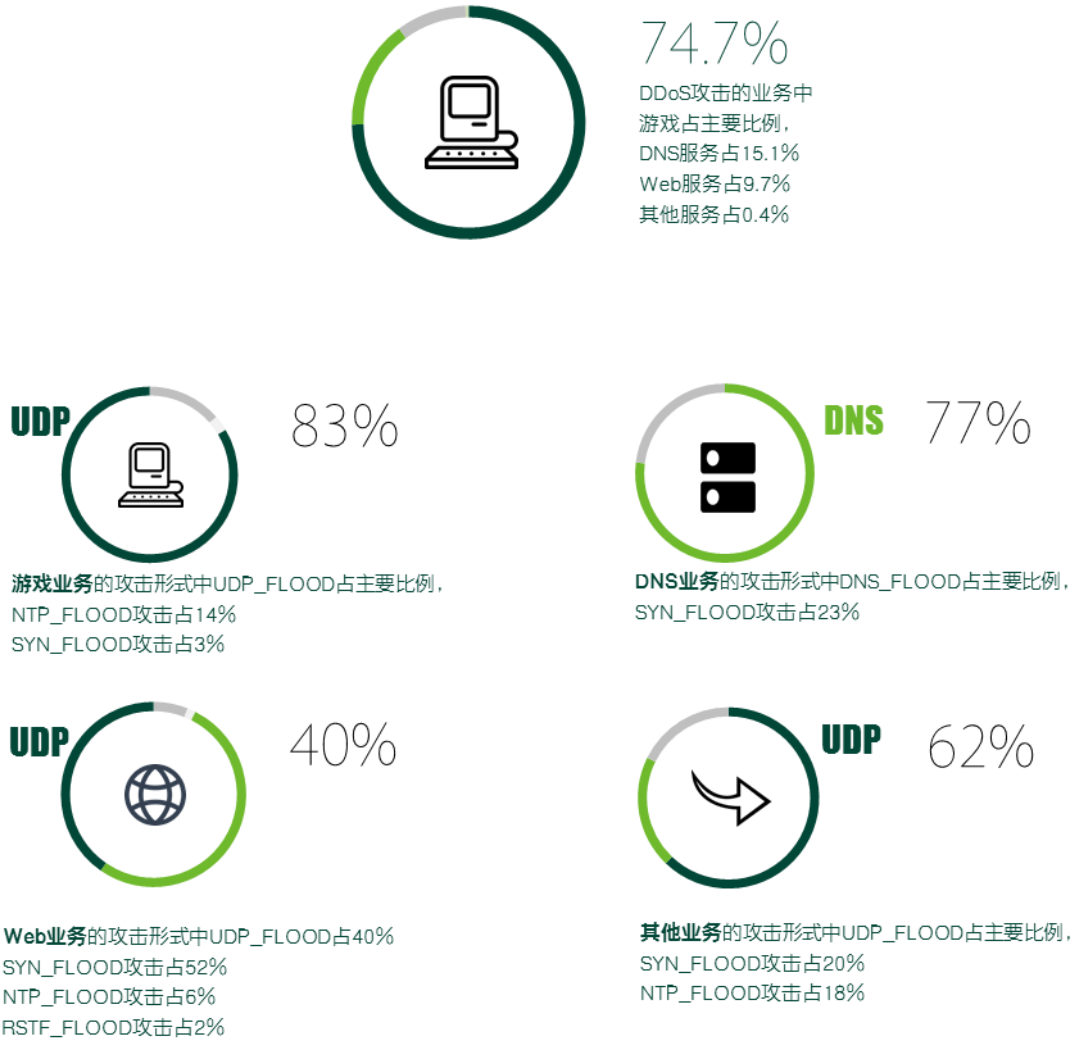


图 1.9　大流量攻击中频繁出现 UDP

① 2014 绿盟科技 DDoS 威胁报告，http://www.nsfocus.com.cn/upload/contents/2015/03/20150304131640_45210.pdf

观点 4：小流量“快”攻击 变身脉冲攻击

虽然大流量攻击乃至云端攻击会越来越多的出现，但这并不意味着小流量攻击就消失了。相反，在一些行业中，小流量攻击有着特殊的目的，与大流量（百 G 以上）及超大流量（500G 或 更高）相比，1 这些攻击因为其流量小，不会引起业界的关注，2 这些小流量隐藏在大流量其中，难以辨识；3 有些攻击时长小到防护设备难以捕获，很难完整呈现其攻击过程，这些特点决定了小流量攻击不仅不会被攻击者抛弃。2015 年上半年，0-30 分钟时长的攻击环比上涨 4.52%，1 分钟以下的攻击占总量的 42.74%。

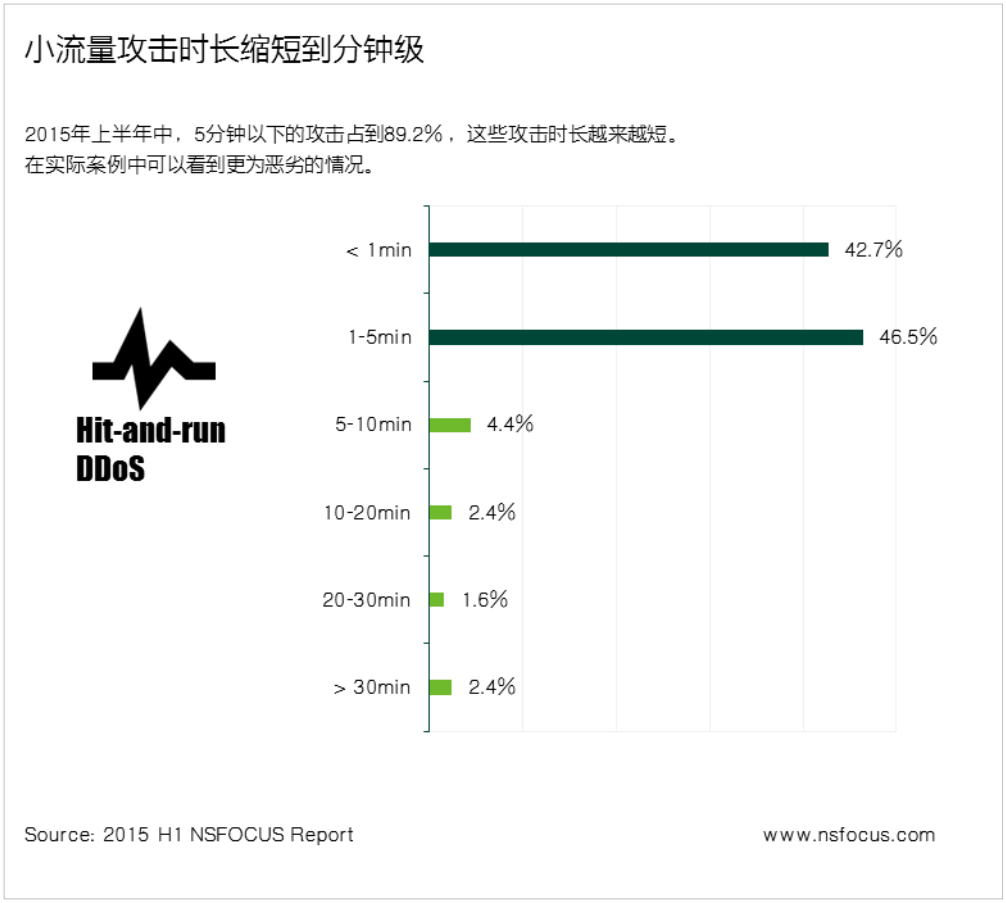


图 1.10　短时攻击占据大比例

将这些短时攻击组合起来看，往往每轮次总的攻击时间也很短。数据统计显示，5 分钟以下的攻击已经有 46%的比例，接近总量的半数。这里借用一张流量分析图展示其中的一个片段，绿盟科技的技术专家将这种短时长“闪电战”的攻击形式，归类为 DDoS 脉冲攻击（Hit-and-run DDoS[Φ]）。

Φ Hit-and-run DDoS , https://en.wikipedia.org/wiki/Hit-and-run_DDoS

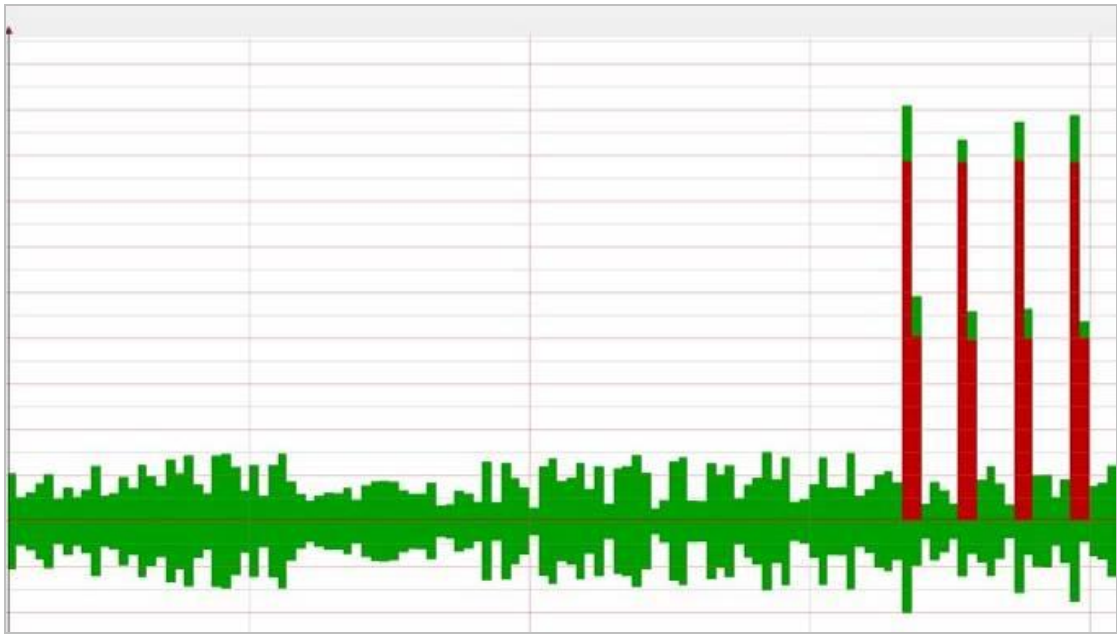


图 1.11　脉冲攻击的片段

在这些脉冲攻击的背后，实际情况是怎样的，在下面的两个实际案例中可以有一个初步的了解。

事件：游戏行业中的脉冲攻击

国内某游戏网吧

这个案例是国内某个大型网吧中捕获到的 DDoS 脉冲攻击，攻击类型为 UDP Flood。在众多捕获数据中，其持续的时间相对较短，峰值相对明显。其业务正常情况下的流量大约在几十 Mbps 左右，瞬间攻击流量却达到了 Gbps 的量级，但攻击总时长仅持续了 5 分钟。这种 DDoS 脉冲攻击流可以瞬间占满带宽，对业务影响非常明显。下图是绿盟科技应急响应团队在云端进行清洗时检测到的攻击流量状况图表。

攻击类型	攻击次数	过滤流量 (bits)	过滤流量 (packets)	过滤流量占比
SYN-Flood	0	0	0	0%
ACK-Flood	0	0	0	0%
UDP-Flood	1611	29061.4G	9.7G	99.0%
ICMP-Flood	52	58.1G	61.7M	0%
Conn-Flood	0	0	0	0%
Stream-Flood	9	95.4G	35.4M	0%
Others	0	0	0	0%

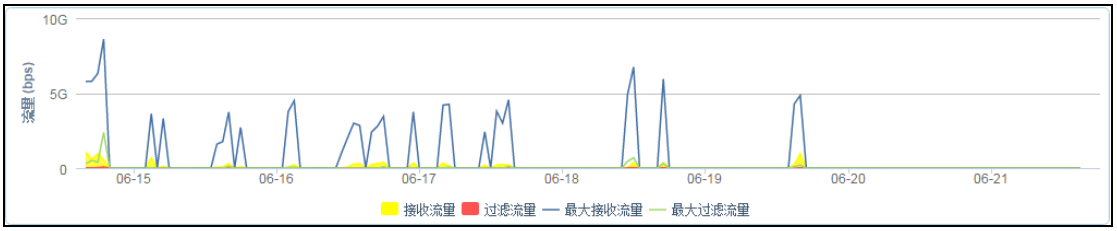


图 1.12　国内 DDoS 脉冲攻击案例

国外某游戏运营商

这个案例是国外某个游戏运营商捕获到的数据，其攻击手法更为高级，DDoS 脉冲攻击特征更为隐蔽。攻击时间仅持续 30 秒左右，瞬间流量峰值达到 899.7Mbps。由于诸多条件的限制，绿盟科技应急响应团队快速进行应对，未能进一步跟踪及捕获其完整的攻击过程。一般情况下，国外同行业游戏运营商中，单用户的流量在几 Kbps 到几十 Kbps 量级不等，以用户规模计算，80%游戏厂商的业务流量在百 Mbps 到几十 Gbps 之间，可以看到在这个案例中，接近 Gbps 攻击流量频繁攻击，对业务已经产生了明显的影响。

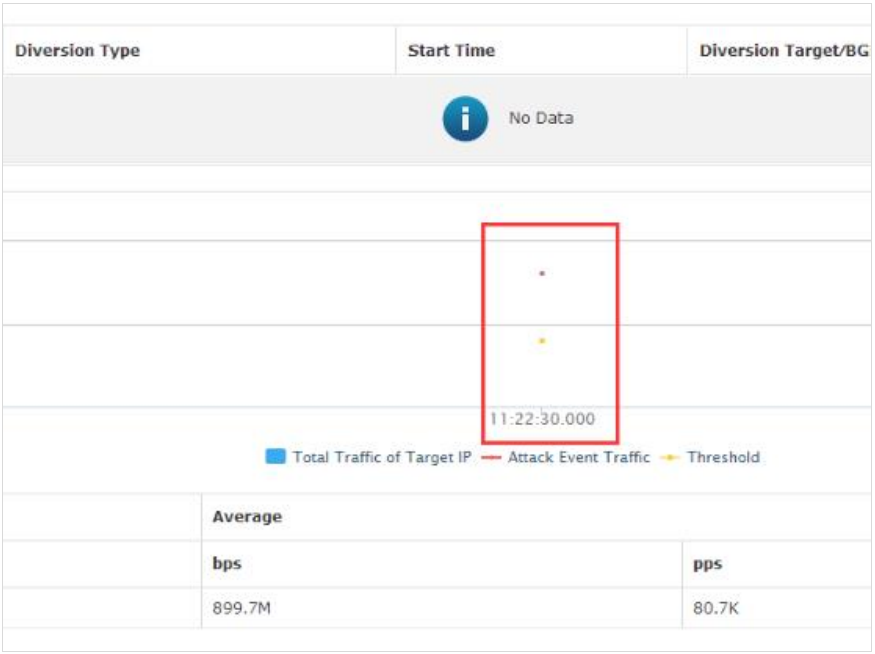


图 1.13　国外 DDoS 脉冲攻击案例

观点 5：小流量“慢”攻击业务逻辑

在众多小流量攻击案例中，针对业务逻辑设计问题的慢速攻击也具有代表性。不同于游戏领域的小而快，这种攻击类型的小流量慢速攻击由于间隔时间较长，从协议、流量、逻辑上来看也没有明显异常，但是却针对协议的弱点或者应用逻辑上的弱点，故意延长通信的时间、占用连接的资源、增加服务器的处理过程，进行资源消耗，使目标的 CPU 资源、内存资源、连接池等耗尽，最终产生拒绝服务。

事件：P2P 在线交易平台

在这个案例中，客户反馈晚上 8 点多开始无法打开页面。经过绿盟科技应急响应团队分析，发现了大量的 HTTP 请求，请求页面为网站首页，但其攻击流量比较小，单次会话时间也较短，设备难以追踪及拦截。但就是这样的攻击，使其数据库性能达到上限，最终因为数据库查询没有返回结果而无法返回用户请求，导致无法打开页面。

在后续的分析中发现，其 web 首页有一个部分是动态显示的内容，每一次请求后，都会查询一次数据库，动态返回交易信息，但由于查询机制不够完善，导致延时较长，攻击者显然仔细跟踪了这个查询过程，找到了这个业务逻辑设计上的问题。

类似这种针对业务逻辑设计问题的攻击，还有一些行业的案例，比如撞库攻击，通过不断发起小而慢的登录请求，最终让系统过载，无法响应用户登录请求。

观点 6：攻击手段 APT 化

在上面的分析中我们可以看到，DDoS 攻击者为了达到目的，会结合多个方面的因素实施不同形式的攻击，攻击手段不断翻新，甚至呈现出“APT”的特色。这些在多个案例中反复出现的要素包括环境、业务、时间、流量、设备，也可以称之为 DDoS 攻击 5 元组。

攻击业务多样化

DDoS 多年难以治理，有一方面原因就是因为业务形态的多样性。随着业务形态的不断发展及演变，结构及业务流程越来越复杂，攻击者无时无刻不在反复跟踪分析这些业务特点及可能存在的问题，而攻击形式也随之而变。

攻击流量多样化

在 2015 年上半年数据显示，在 DDoS 攻击中，攻击者往往混合使用多种攻击手段和多种类型的攻击源。UDP 混合流量占主要比重，达到 72%。这些流量组合正如前面的分析所展示的那样，并非无的放矢，而是跟随业务的特性发生的变化。

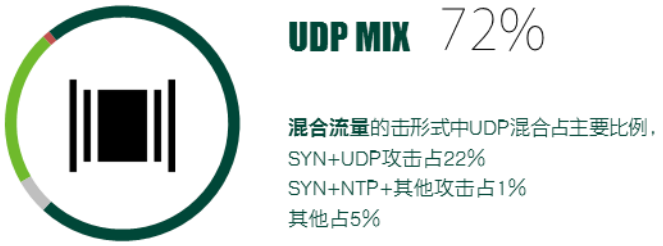


图 1.14　UDP 混合流量占据大比例

攻击设备多样化

如今，用户连接互联网的设备越来越多样化，在终端方面，已经不再局限于 PC，更多的设备也包括平板电脑、手机、电视等智能终端；同时，反射放大式攻击，让业界清晰的认识到，DDoS 可利用的设备也不再局限于终端，更多的设备也包括路由器、打印机、摄像头、扫描仪等智能设备。

在 2014 年的报告中，我们统计了全球的这些可能被利用的智能设备超过 80 万，在 6 月份的数据中，我们统计了全球 SSDP 协议设备的分布状况（如下图），显然一情况并未得到大的改观，这也是基于 SSDP 协议的放大攻击仍旧肆虐的原因。在此我们呼吁这些设备的厂商尽快发布相关补丁 or 升级相关固件，最终用户也需要随时关注升级信息，尽快升级及采用对应的防护措施，不要被利用，成为“攻击者”！同时，在智能设备增加、混合流量攻击模式下，传统的业务场景和思路可能需要考虑新的模式和新的应用场景。

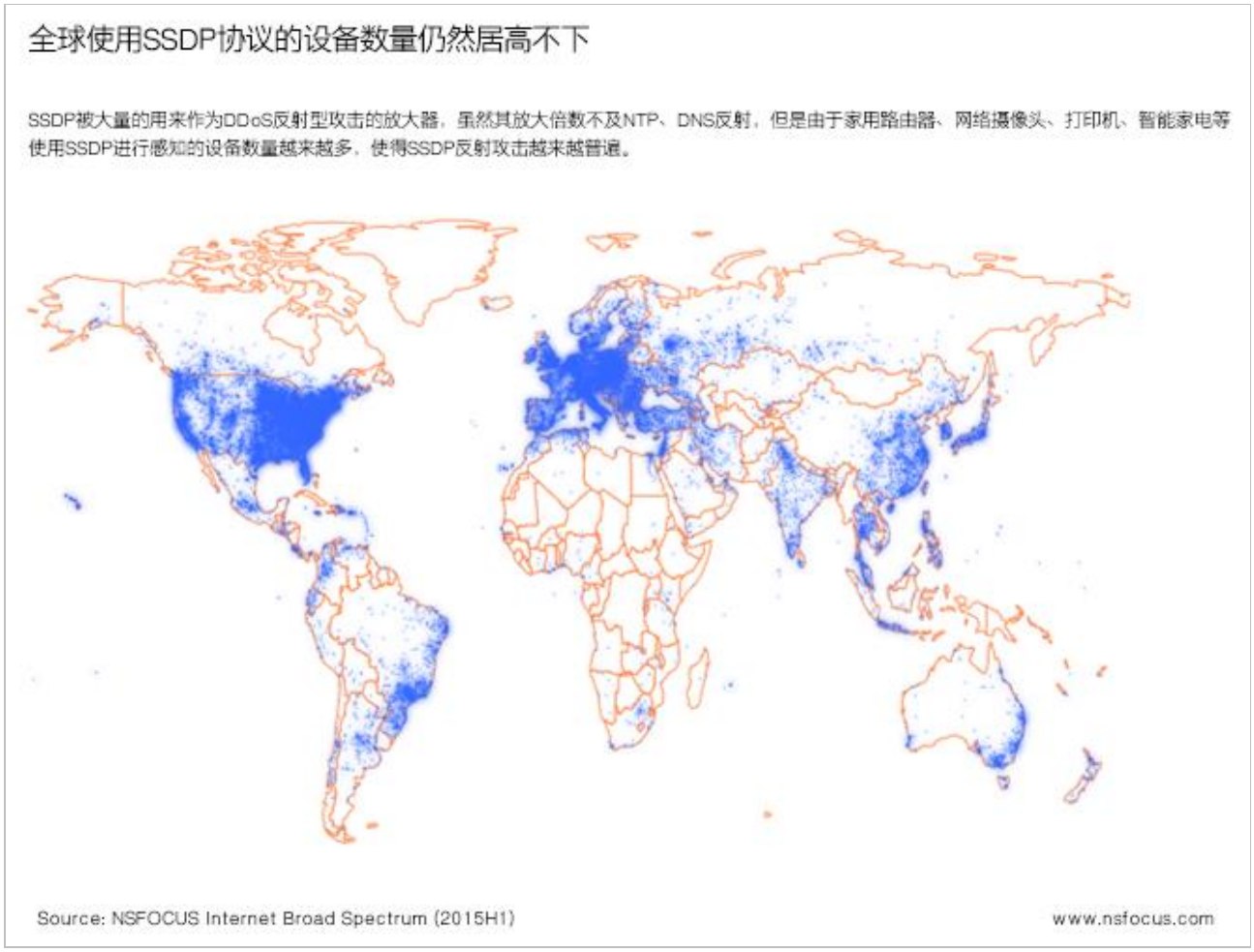


图 1.15　全球 SSDP 分布情况

在这些智能设备中，手机等相关移动终端的大量接入及快速增长，势必造成互联网环境的改变，而且它们缺乏受普遍遵循的规范和标准，很多传统的防护算法面临挑战。这种情况下，手机等移动终端被利用，成为攻击者或者被攻击者，只是一个时间或者时机的问题，防护厂商如何提供更有效的算法是当前行业需要解决的难题。

事件：智能路由器成为僵尸温床

智能路由器设计上普遍存在安全性问题，在初始化配置、安全防护方面并未引起设备厂商足够的重视，这使得大量的智能路由器在网路上成为攻击者利用的工具，也使得攻击的成本和难度大幅的下降，下面通过展示上半年智能路由器漏洞事件中，影响较大的几个事件，从直观上印证其被 DDoS 攻击者利用后的危害。

智能路由器安全事件

漏洞名称	漏洞简述	时间*
CVE-2015-0554	ADB Pirelli 家庭路由器存在信息泄露漏洞，该漏洞可以使得黑客控制设备成为肉鸡	2015-01-05 公开漏洞细节
CVE-2015-1187	D-Link 设备存在命令注入漏洞，同时认证机制存在严重缺陷，攻击者可以远程获取设备 root 权限，并获得设备的完整控制权	2015-01
system_mgr.cgi wizard_mgr.cgi login_mgr.cgi 组件漏洞	D-link 存储设备存在默认账户和空密码，存在后门程序	2015-01-20
CVE-2015-3036	NetUSB 组件漏洞，该组件在大量物联网设备和路由设备中使用，触发条件非常简单	2015-02-01
ZynOS 固件漏洞	该固件被多个路由器厂商使用，使用该漏洞可劫持用户流量，可以进入设备管理界面进行更多的配置操作	2015-01-27
webproc.cgi 组件漏洞	利用该漏洞进行目录遍历并获取配置文件，可以得到管理员密码，并且由于路由器密码的算法很弱，黑客可以较为容易的获取路由器的配置权限，进行流量劫持	2015-03-18
POODLE 漏洞	100000 多台澳大利亚家用路由器受到影响	2015-04-01
PIN 弱算法	Belkin 设备密码可以被破解	2015-04-10
CVE-2014-8361	miniigd SOAP 服务存在漏洞，该漏洞存在于 RLT81xx 芯片中，该芯片广泛适用于各大路由器厂商，影响范围较广，黑客可以利用漏洞进行远程代码执行操作	2015-04-29

* 这里的时间严格意义上来讲不是发布时间，而是该漏洞成为事件被关注的时间

从这些事件统计中我们发现，有的设备漏洞不仅被发现一次，而且最早的漏洞在两年前就已经报给厂商，但是厂商历经两年都未曾修补这些漏洞，厂商对安全的忽视对安全来说是非常大的安全隐患，应该加强这一块的监管和规范。不难发现，智能设备大量连入传统互联网必然造成 DDoS 安全隐患。主要原因：

- 大量设备存在默认端口和默认登录凭证，安全性能极低。路由器等设备在设计的时候对安全性考虑十分薄弱，因此大量路由器暴露在中间人攻击、劫持和远程利用的风险之下。为 DDoS 提供了潜在的带宽资源。
- 路由器功能越来越多，计算能力越来越强。路由器一方面提供了更多的功能，可以方便管理和智能化操作，另一方面却也使得黑客可以使用被入侵的路由器当做肉鸡，进行更复杂的操作。在一些研究中，安全人员发现有的路由器僵尸网络具有自我复制扩张的特点，正是利用了路由器提供的一些智能化的功能。
- 智能设备与传统设备通过网络互连，安全性能缺乏考虑。智能设备本身在设计生产过程中就存在非常多的安全隐患，加之智能设备的多样性造成管理上的困难。这有可能使得传统的防护措施失效，这样的环境下，可能会成为被动的攻击者或者受害者。
- 设备数量大。智能设备数量大，性能也渐渐提高，这使得攻击者可以在很小的成本下就可以获得很多的互联资源。攻击者获取到大量肉鸡的成本和难度越来越低，著名的 Lizard Stresser 就是依赖大量家庭路由器形成僵尸网络，甚至该工具还被商业化提供服务。

DDoS 防护现状

正如前面提到的，传统互联网架构是非控制性的网络架构，因此，从技术角度来说，DDoS 不可能完全杜绝，只能最大程度的“缓解”。作为防护方，我们应该思考的怎样从传统的动态防御、限速、行为分析方式，转变为态势感知和大数据分析相结合的模式，形成防护的闭环。同时，在 DDoS 攻击已经发生的情况下，通常会采取各种方式减少 DDoS 攻击造成的影响，从而保障其服务的可用性。

而另一方面，DDoS 涉及到业务的方方面面，从主管机构、行业机构、社会组织、安全厂商到用户，单独哪一方面也很难实现，而且攻击者形成的地下产业链已经很成熟，这就需要有一个协同机制的建立，能够阻止正在发生或者可能发生的 DDoS 攻击，抑制其攻击规模，消除安全隐患，我们称之为“治理”。

下面从 DDoS 治理及 DDoS 缓解两个方面，来说明 DDoS 防护的现状及未来发展方向。

治理：主管机构打造平台

2015 年 7 月 31 日，由工业和信息化部指导，国家互联网应急中心（CNCERT）牵头组织开展了《互联网网络安全威胁治理行动》签约仪式，绿盟科技受邀参加。来自中国移动、中国联通、中国电信、百度及腾讯等 47 家发起单位，在仪式上共同签署了行动承诺书。

据 CNCERT 抽样监测显示，2015 年 1-5 月，1GB 以上的 DDoS 攻击事件日均 1300 起，1GB 以上 DDoS 攻击事件 26903 万余起，日均 1793 起，较 2014 年均有小幅度增长。在这种态势下，CNCERT 动员行业内相关单位，从加强监测入手，通过密切配合、积极处理、曝光攻击者黑名单等措施，有效防范和治理 DDoS 及更多威胁互联网网络安全的行为。

治理：运营商治理大流量

随着 DDoS 攻击流量的增加，大流量防护的问题日益凸显出来。在云端，骨干运营商已经开始结合抗 DDoS 服务，开发相应的安全运营平台，以开展相应的安全增值服务。同时，从治理的角度来看，行业多数运营商已经部署了大量的安全设备，随着自身对安全运营的重视，开始加强安全能力的建设，防护系统平台化呈现流行趋势，同时携手行业相关单位，一起做好应急响应及大网抗击 DDoS 的工作方案。

治理：行业组织标准欠缺

目前国内在 DDoS 防护方面，存在一些行业组织的雏形，但一方面还缺少响应的标准，另一方面在针对性及健壮性方面还有待提升。

缓解：厂商提升技术能力

在本地，对 DDoS 攻击的防护产品/技术已经比较成熟，单台设备的处理能力越来越高，已经可以处理数十 G 的攻击。虽然，DDoS 的攻击形式多种多样，但就其攻击形式的类别而言主要有 4 种，攻击网络带宽资源、攻击系统资源、攻击应用资源及混合式攻击。这些方面，各厂商的技术专家都在不断分析和改进，以常见的 CC 防御而言，绿盟科技的技术专家总结了至少 5 种常见的算法，对比了各自的局限和优势如下：

CC 防御技术对比

CC 防护算法	验证码位置	算法兼容性说明	防护优势	防护劣势
0-Tag 验证	http 头部的 Tag 字段	兼容性好	自动验证	无法防护肉鸡攻击
1-HttpCookie 验证	http 头部的 cookie 字段	兼容性好	自动验证	无法防护肉鸡攻击
2-URL 验证	url 字段	兼容性好，部分网站不处理携带新参数的 url 请求	自动验证	无法防护肉鸡攻击
3-ASCII 图片验证	图形验证码	兼容性好	较有效防护肉鸡	需人工参与验证
4-BMP 图片验证	图形验证码	兼容性好	较有效防护肉鸡	需人工参与验证
5-动态脚本防护	网页内容里的 js 脚本里	兼容性一般，部分客户端杀毒软件会报病毒	自动	无法防护肉鸡攻击

当然，除了当前行为验证为主的算法防护外，各种过滤技术都应该采用越灵活越好，比如基于 5 元组和数据包任意负载的灵活过滤技术。这里的五元组是指，源 IP 地址、源端口、目的 IP 地址、目的端口和传输层协议。针对五元组的过滤能够针对 IP 范围、IP 地理位置、端口、协议进行更灵活的限定和过滤。目前最常用的方法是目的端限速和源端限速，但是针对特定的攻击需要更加灵活的过滤技术。以 UDP 协议为例，如果针对其中常见的数据段提供解析，并添加对应的过滤规则，这样便能更方便的进行模式匹配，为过滤操作提供方便。

16 位端口号	16 位目的端口号
16 位 UDP 长度	16 位 UDP 检验和
数据（如果有）	

未来 DDoS 防护技术发展将会至少包括 3 个方面：

- 特征+行为。传统针对特征的扫描和防护，越来越难以应对未知攻击形式，而后者将会更多的利用虚拟环境及动态跟踪的方法，一方面以避免攻击者对于攻击环境的侦测，另一方面跟踪其攻击行为提高识别率；
- 过滤手段高级化。包括基于威胁环境和正常业务环境的过滤技术，比如云端威胁 IP 信誉库，云端威胁指纹库，基于业务正常环境的“白”的过滤技术，如地理位置，业务端口，时间段等。
- 智能化防御技术。为了降低安全运营的复杂性，应该增加建模、自学习、自动化技术，比如自学习用户业务环境，生成正常业务基线参数；感知设备攻击效果而自动化轮换防御算法等。

缓解：用户加固特定业务

在业务方面，只有用户自己才最了解自己的业务特性，如同攻击者一样，针对业务的薄弱环节进行加固，将在 DDoS 防护上起到事半功倍的效果。但限于组织内部等因素，可能用户自己实施缓解措施及制定加固方案存在一定的困难及风险，其原因在于：1 需要考虑业务系统的可用性；2 需要考虑整体实施方案制定；3 需要尽可能降低加固动作对业务环境的二次伤害。这就需要企业自身、漏洞相关厂商、安全厂商一起协作才能形成快速、安全、有效的行动方案，避免业务系统在获得安全加固之前遭受攻击。

以游戏业务防护为例，这里主要指基于私有协议的游戏。因为此类游戏使用了私有协议，导致清洗设备无法解码报文内容，无法进行进行类似 HTTP 302 跳转的验证动作。如果游戏还是基于 UDP 协议的，那么初级的反向探测等手法统统失效，给防御带来很大的困难。为解决这个防护问题，2012 年绿盟科技产品团队与某客户共同研发了水印防护算法，以保障其游戏业务的正常运行。截至目前该算法一直使用良好。

水印算法的主要原理是，游戏客户端在生成报文的时候，根据事先协商好的标准生成“水印”，并插入到游戏的报文中，黑洞 ADS 在收到游戏报文时，也采用同样的方法计算、验证水印的正确性，从而完成清洗的动作。同时，黑洞 ADS 提供了开放的 API 接口，用户可实时修改水印的生成方法，以防范水印被突破。水印算法的防护思想也同样可使用在手机 APP 的 DDoS 防御中。

这里要指出，水印算法有前提条件，也就是需要业务方配合完成水印的开发，对业务有一定的开销，但这个开销对于 DDoS 的缓解是值得的。

如下列举其他几种常见的业务场景及防护思路，但就像上面提到的游戏业务加固方案一样，实际业务中，用户往往会面临更为复杂的业务环境及处理细节，这里就不展开详述了。

常见业务场景及防护思路

业务场景	业务特点	常见攻击	防护思路
HTTP 业务防护	• 基于 HTTP 协议的业务。主要是 B/S 架构的 web 系统，比如企业门户网站、政府网站、证券公司网站、银行网银网站等。 • 目前也有许多 C/S 架构的系统也基于 HTTP 协议，比如手机或者 PC 终端的网上银行、证券交易系统等。	CC SYN Flood ACK Flood Connection Flood	• 使用探测包验证源 IP 的真假性。 • 使用 HTTP302 跳转、JS、图片等人机识别技术验证客户端行文 • 限制源 IP 的连接数。 • 基于大数据的异常行为识别、信誉过滤。 • 也会遇到攻击者使用 UDP 大流量攻击 HTTP 业务的情况，防护者可直接封禁此类非业务流量。 • 在网络边界直接封禁常见的反射攻击（该策略对其他业务场景也适用）。
网吧 业务防护	• 网吧的流量主要是下行流量，且网吧基本不对外提供服务 • 流量成分以 ACK、UDP 为主，报文的源端口大部分为知名业务端口。	UDP Flood ACK Flood	• 因网吧基本不对外提供业务，因而非常适合使用业务封禁策略，比如可封禁 SYN 80。 • UDP 源限速。 • 游戏是大部分网吧的主营业务，为保证在 DDoS 防御过程中游戏不掉线，可采用自学习策略提升用户体验。
DNS 业务防护	• DNS 业务通常使用 UDP 报文来承载，但其协议上也支持 TCP。 • 对于运营商的递归 DNS 服务器来说，查询源主要是用户终端。 • 对于企业的权威 DNS 服务器而言，查询源主要是运营商的递归服务器。	DNS Query Flood DNS Response Flood	• UDP 转 TCP 防护思路，用来验证源 IP 的真假，但实际效果不佳 • 域名学习思路，基于域名信誉的防御。 • GEOIP 防御思路，如运营商的递归 DNS 只对本地用户提供访问 • 白名单思路，如企业的权威 DNS 只对运营商的 DNS 开放，但需要防范白名单被突破的情况（可结合使用 TTL 等技术）
游戏 业务防护	• 游戏业务对网络质量敏感。 • 很多游戏使用私有协议，造成了 DDoS 防御的困难	各种 Flood	• 依然可使用反向探测等技术验证源 IP 的真假，过滤掉较为初级的攻击。 • 使用自学习策略提升游戏用户体验。 • 直接封禁非游戏业务端口的报文。 • 使用水印防护算法。客户端在发送数据报文时，可在报文中插入一个“水印”，防护设备基于此“水印”进行识别和过滤。

防护：DDoS 防护生态环境

未来 DDoS 防护，不再是单个硬件产品形态能解决的问题，从技术上需要一个防御体系，就像攻击态势中提到的那样，有大流量的方面，有小流量的方面。小流量应用性攻击在本地防御更为有效，大流量方面更适合在外部进行，而介乎于两者之间的部分，将部分 IDC 或云中心会建立自己的本地清洗中心。同时，伴随智能化、前瞻性理念在 DDoS 防护领域的应用，将会出现更

多的 DDoS 防护增值服务的出现，这些多维度、多形式的防护形式，将需要信誉等联动机制的出现，才能在整体防护效能上趋于合理。

另外，从服务上来说，对抗 DDoS 攻击是一个涉及行业多层面的问题，在有的环节，有效性和投入并不对等，这就需要主管机构、运营商、标准组织、安全厂商及最终用户共同协作，打造 DDoS 防护生态环境（DDoS Prevention Eco System），才能最终有效抑制这种攻击，我们期待未来这方面会看到更多更好的体系诞生。

DDoS 解决方案及实践

在现有的攻防态势和网络环境下，可以看到防护方面临的主要挑战：

- 攻防环境越来越复杂，防护技术越来越体系化；
- 缺少威胁信息，对威胁源的感知和预测不足；
- 传统方案难以应对针对急速变化的攻击形式 ；
- 清洗性能和清洗成本的平衡

针对这些挑战，业界出现了几种 DDoS 解决方案，为了方便大家对这些方案的特点有一个整体把握，下面就这些方案进行简要比对。

DDoS 清洗技术方案对比

No.	清洗技术	描述	优点	缺点	适合的客户场景
1	本地清洗	在本地业务侧部署专业抗 DDoS 设备或内置专业抗 DDoS 模块的其他安全设备	快速、及时；更适合小流量、应用型、业务型、慢速等攻击类型的防御	受本地带宽限制，无法防御大流量攻击；需要购买设备，投入专业的运维人员	对自身业务的安全要求具有较强可控性和快速响应的客户，如金融、政府等客户
2	云清洗	来自客户业务外部的云清洗中心提供的清洗服务。防护包括三个过程：将流量牵引至云清洗中心，清洗，流量回注至客户网络。	大流量攻击的防御；无需购买设备，按需购买服务；无需投入大量资金建设专业安全运营团队	涉及云端流量牵引及和客户的反复沟通等环节，响应速度不及本地端快速，尤其是采用 DNS 进行临时牵引的情况。	适合所有客户。尤其中小企业，选择合适的云清洗服务可降低整体投入，提升安全能力。对于大客户可有效对本地清洗的方式进行补充。
3	分层清洗	将本地清洗和云清洗结合，云端负责处理大流量攻击，本地设备处理小流量、应用型攻击。	结合了本地清洗和云清洗的优点，对各类攻击的防护覆盖全面。如果能实现上、下层系统的智能联动，还可有效提升防护效率。	方案投入成本高。	适合对业务延时、运维自主可控、防护等各方面都有较高要求，并有较强的经济投入能力的客户，如银行、证券，在线游戏服务商。
4	信誉云	通过安全大数据分析建立对攻击相关的僵尸主机 IP、攻击报文特征、行为特征模式的实时跟踪，形成信誉云。和本地清洗设备或云清洗系统结合实施。	可有效辅助防御复杂和未知攻击，提升防御效率，并可实现主动防御策略。	需要建立一套广泛的数据采集、大数据分析模型、反馈和应用机制的复杂系统。辅助手段。	对购买了本地清洗设备的客户进行部署。云端清洗中心的部署对客户不可见。
5	近源清洗	采用多个分布式云清洗中心协同清洗，各清洗中心对距离最近的攻击源进行清洗。	避免攻击汇聚到目的侧后规模过大，加大目的侧清洗压力。有效缓解海量攻击对沿途运营商链路的占用。	方案复杂，涉及的技术环节多，响应速度和实际效果有待验证。	方案对客户不可见。

下面就这些方案进行展开描述。

本地清洗

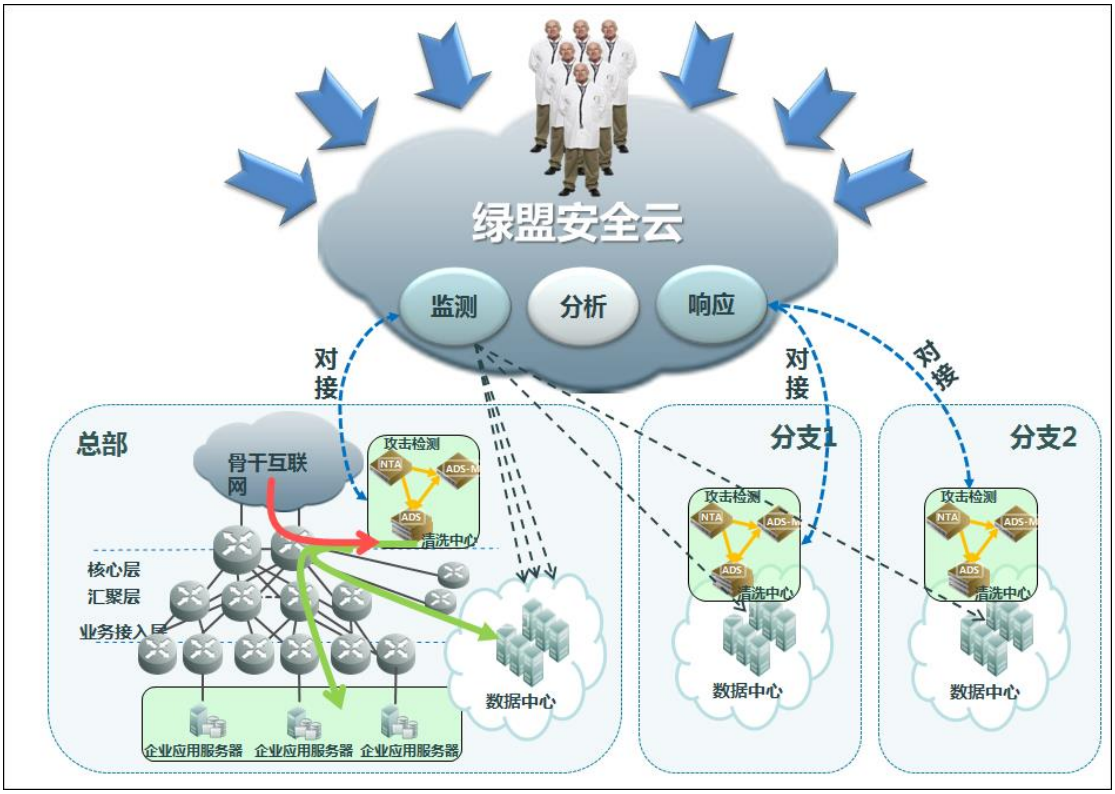
本地清洗方案是最为常见的清洗方案，通常在客户端（CPE）进行部署，一般会以旁路、串联部署的方式进行。大型企业通常采用这种方式，其优点在于自主可控，灵活性强。但是，这种方案需要本地化的维护，对人员要求较高，需要较高的运维成本，而且清洗性能受到本地端设备性能的限制，而高性能的设备又带来了设备及相关成本的增加。

云清洗方案

面对成本的考量，有些中小企业及组织考虑使用云端清洗的方案，除了成本之外，优点是直接可见的，得益于云计算的灵活性，业务及 DDoS 防护都可以交由云端进行，让设备和人员得以解放，去进行本地细粒度的维护，从而让企业将有更多的精力去关注自身的业务发展。在现阶段，云运维和云清洗的方案无疑是较为合理的选择。

云运维服务

云端运维服务关注于传统的 DDoS 防护运维的三个难题，1、难以实现对 DDoS 攻击 24 小时监控；2、难以迅速、有效地识别 DDoS 攻击并抑制危害；3、DDoS 攻击手段和类型复杂多变难以防护，而在线防护解决方案可以实现将客户本地设备与安全云对接和同步，由远程安全专家团队协助企业实现对 DDoS 攻击全天候监视、响应、防护服务。以绿盟科技云安全服务完整全面的提供了 DDoS 防护服务，加强了设备的额可维护性能。



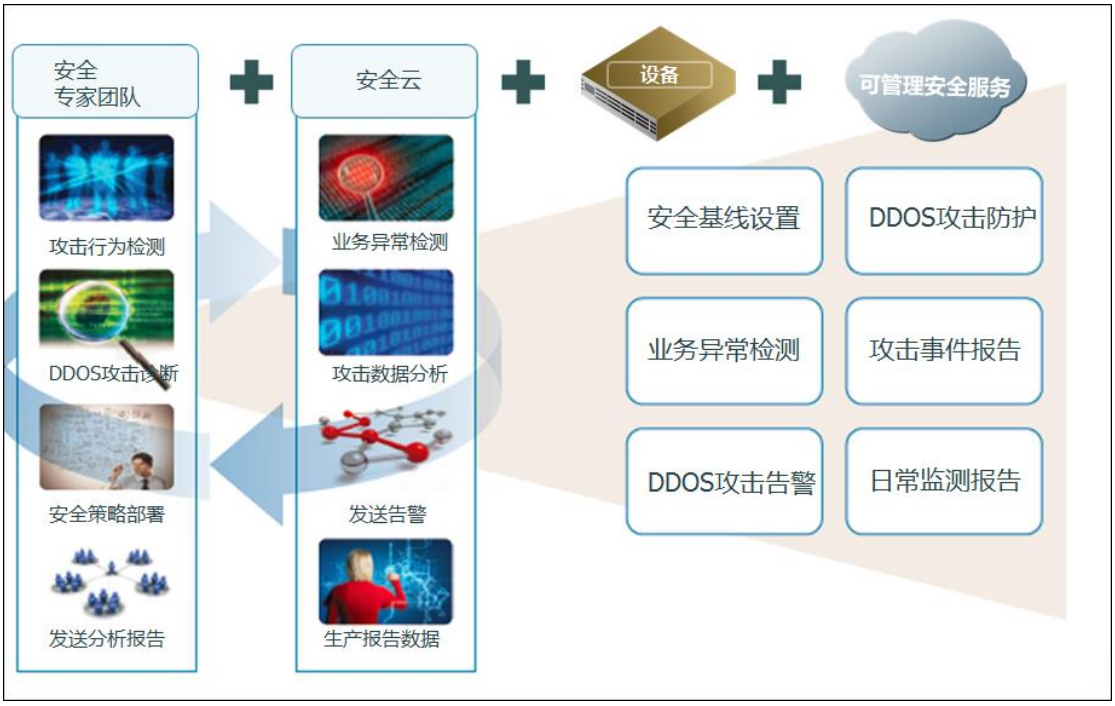


图 1.16　绿盟科技云运维服务

云清洗服务

另一种常见的云端 DDoS 防护服务是云清洗服务，该服务通过分布式的清洗中心进行流量负载均衡，通过安全云的方式向用户提供清洗服务，可以有效降低设备成本。这样的部署模式可以有几个优势：1、集中最专业的设备和人员，提供全面服务和超大的清洗容量。这种方案整合了优势资源，能够合理的分配利用资源，实现了资源的最大化利用，能够高效的进行 DDoS 防护；2、零运维，由于整个 DDoS 防护设备在云端部署，不需要本地投入另外的运维成本；3、零设备采购。云清洗作为一种服务销售给客户，客户免去了繁琐的运维和操作，直接享受服务带来的价值。

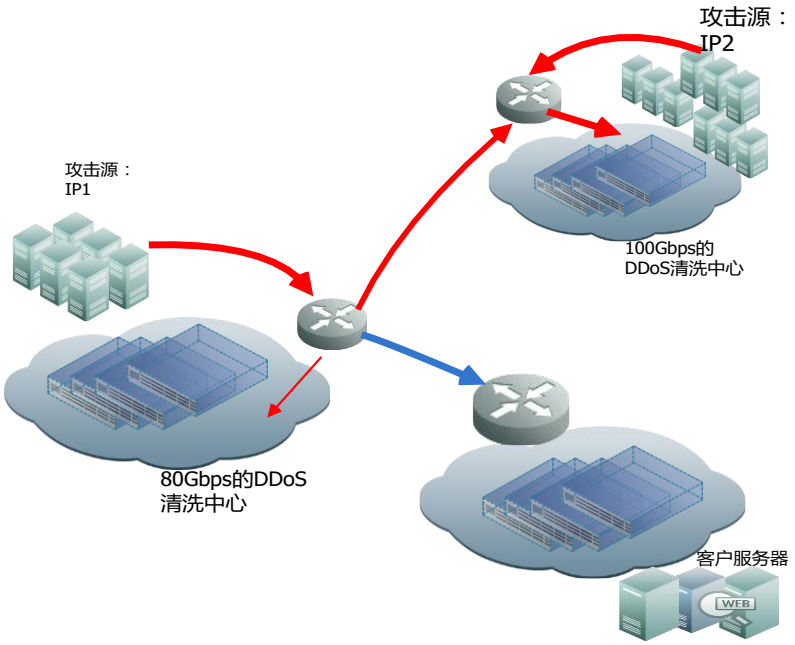


图 1.17　云清洗服务架构

SDN

在 DDoS 流量清洗的技术中，还有一类新秀，基于 SDN 的流量牵引。它有两方面优势，1、SDN 天生的灵活性使其可以做做到网络流量的快速调整，一起配合可以实现高效的网络管理，尤其是在与安全设备结合的同时，可以实现快速组成服务链的优点；2、SDN 控制器对全局网络流量具有很好的可视性，所以可以快速检测到流量异常，对于流量型的攻击，检测代价小，效果也不错。事中同时可以利用 SDN 控制器快速牵引流量到清洗中心进行防护，事后调整路由快捷方便，但正如攻击态势中提到的那样，这项技术投入实际运用需要时间，在此之前其自身也很容易成为 DDoS 的攻击目标。

分层清洗

正是看到了上面两种方式的优缺点，业界根据分层防护的思想提出了 DDoS 分层清洗的方案。这种方案融合了本地清洗和云端清洗的优势，从设备性能，综合成本的角度考虑，在业务前端部署专业抗 DDoS 设备或具备 Anti-DDoS 技术模块的设备，如 WAF。远端的清洗设备适合进行大流量粗粒度的过滤，客户端的设备可以根据用户的业务特点制定更加细化和有针对性的过滤。以绿盟科技的方案为例，上层采用绿盟方案构建的云清洗中心可以和下层绿盟的低端 ADS 和 WAF 设备互相交互信令和防护状态，协商防护主体，实现智能协同防护。

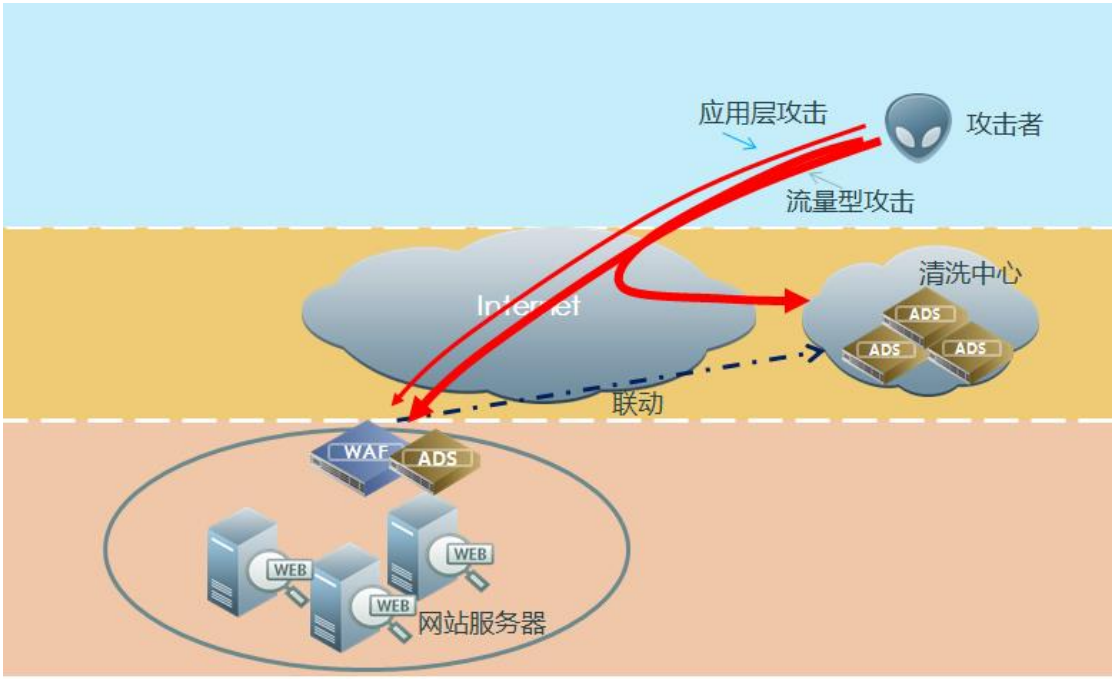


图 1.18　分层清洗模型

建立信誉云

攻击检测设备之间实现信息共享，提供 IP 信誉库，实现威胁情报共享，可以形成多方联动的响应机制，一方受到攻击，多方同时进行防御措施更新，可以有效的提高检测效率和防护效果，在现有的设备条件下可以提升防御性能，进行更有效更快速的响应。

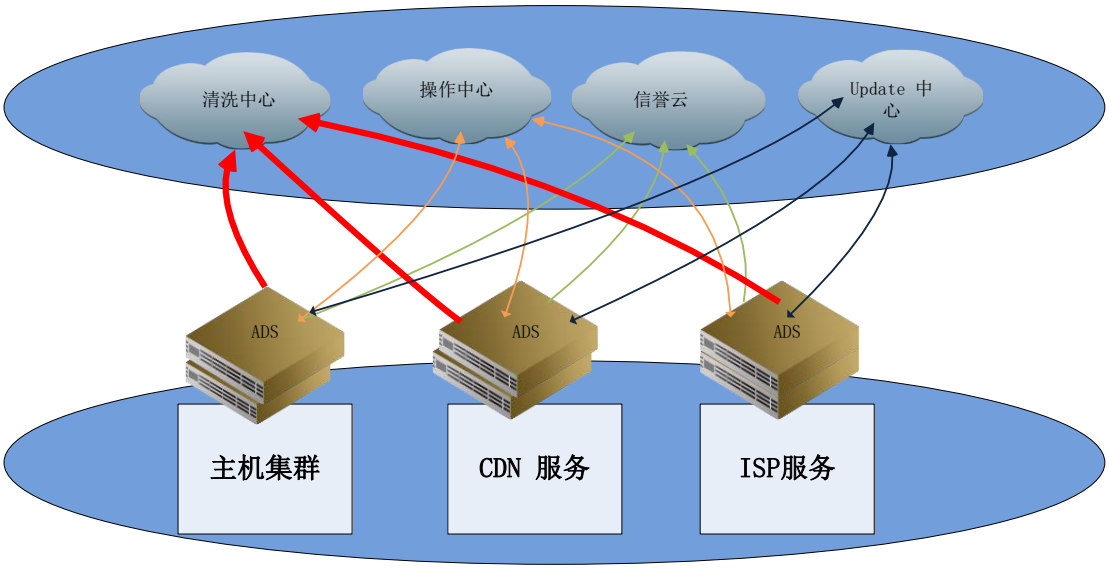


图 1.19　信誉云模型

近源清洗

这种防护思路是在离攻击源最近的分布式清洗中心节点实施清洗，避免攻击汇聚后形成规模，进而对网络沿途链路和设备造成影响，也可以有效避免汇聚后的流量到了目的端，进而导致目的侧清洗压力加大。这种方案是将战线脱离家门口，进行战略防御思路。

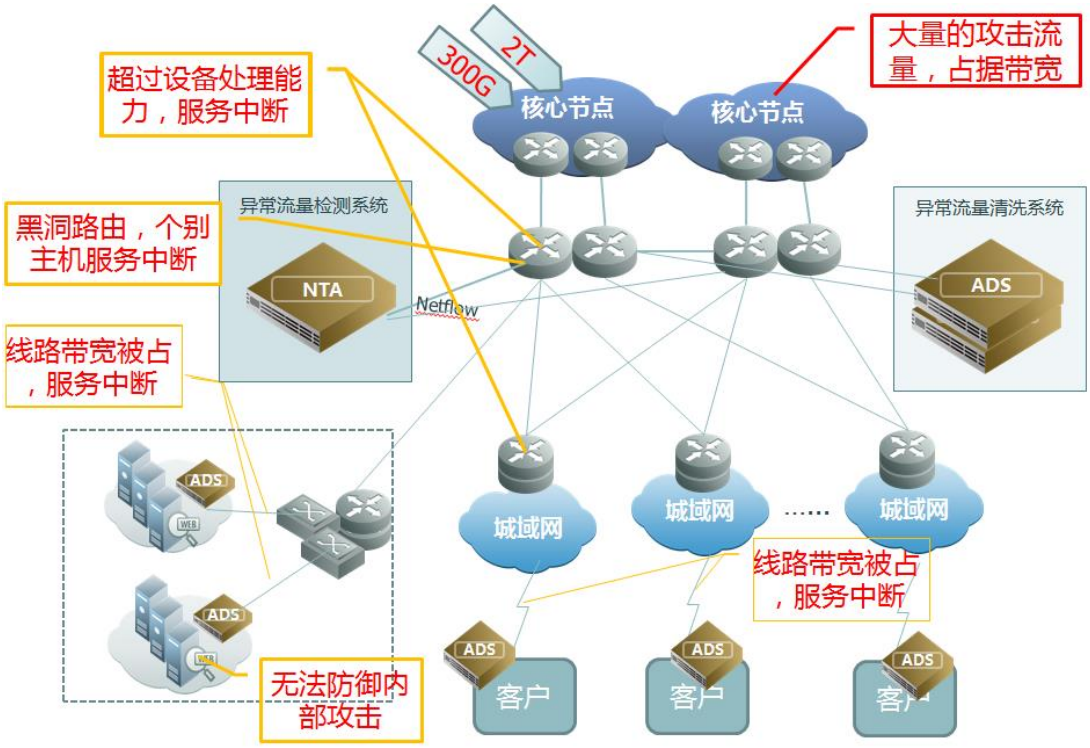
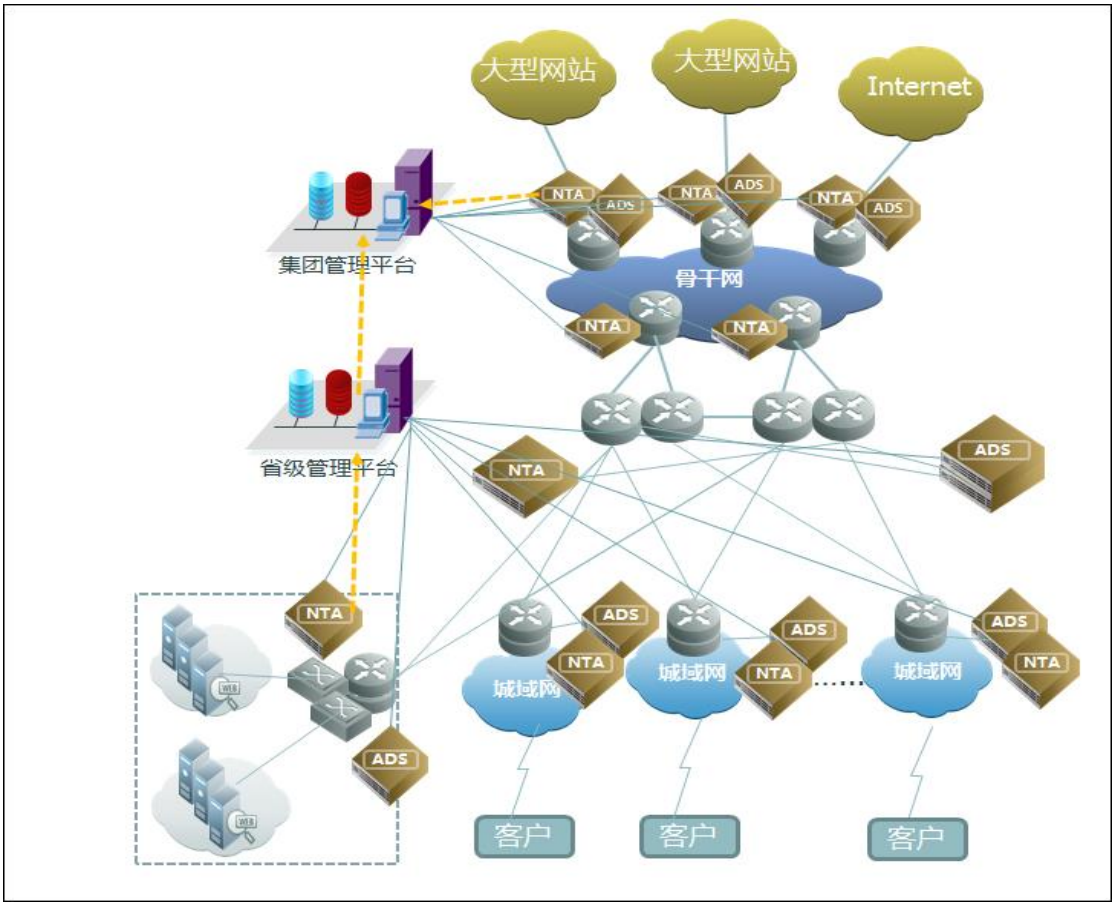


图 1.20　近源清洗模型

近源清洗技术带来的优势是明显可见的，1、DDoS 防护能力提升，全网得以在 DDoS 防护方面实现协同一体化，并有能力抵御 300G 以上攻击；2、干净的骨干网，由于清洗在源端进行，沿途的带宽消耗可以得到有效缓解，提升网络服务质量；3、集约化运营架构，全网异常流量得以集中检测、分布式清洗。4、安全增值服务，基于这个体系和架构，可以实现更多增值服务。

以绿盟科技近源清洗方案为例，下图是一个覆盖集团、省级及用户端的 3 级部署方案。在这个方案中，如果集团用户检测到攻击，会向省级管理平台通报 IP 地址及发出检测请求，省级平台根据该请求向下方的各级设备派发监测任务，省级管理平台负责搜集监测反馈，如果监测到攻击，下发指令让相应的近源设备开始进行清洗，清洗结束后省级平台向集团平台发送流量正常信息，清洗结束。这样，近源端设备和客户端设备形成了联动机制，有效防止大流量攻击对沿途带宽的占用及清洗不够彻底等问题。



但这种方案也有这它的不足，1、无法识别用户端网内攻击源，包括内部之间 or 由内往外的攻击（见观点 2）；2、对检测和防御设备的处理能力要求较大；3、用户端的流量异动可能随时被公告；4、面临多方信息共享及联动的困境。

结束语

在上面的分析中我们可以看到，2015 年上半年 DDoS 的攻击呈现两极分化形式，一类持续大流量攻击，尤其是针对高性能、高价值、大范围的攻击目标；另一类则呈现小而快、小而慢的形式，进入细分行业，主要是针对小流量及特殊业务目标；同时，我们也发现这两类攻击并非格格不入，而是伴随着环境、业务、时间、流量、设备的变化而组合演变，这些演变将与云计算及大数据一起，催生 DDoS 防护向下一代 DDoS 防护及 APT 时代迈进。

您还想看什么内容？

报告中有涉及客户的详细数据及信息已去除，如果您希望了解更多内容，可以联系报告作者。

同时，也欢迎您与我们分享您的见解，在这里先行致谢！

作者和贡献者

作者

陈颐欢，绿盟科技　　Email：chenyihuan@nsfocus.com

贡献者　（排名不分先后）

周忠，绿盟科技　　Email：zhouzhong@nsfocus.com

李国军，绿盟科技　　Email：liguojun@nsfocus.com

何坤，绿盟科技　　Email：hekun2@nsfocus.com

刘文懋，绿盟科技　　Email：Liuwenmao@nsfocus.com

王秀慧，绿盟科技　　Email：wangxiuhui@nsfocus.com

徐祖军，绿盟科技　　Email：xuzujun@nsfocus.com

刘炅，绿盟科技　　Email：liujiong@nsfocus.com

王洋，绿盟科技　　Email: wangyang2@nsfocus.com

DDoS 威胁报告

SECURITY

DDoS（分布式拒绝服务）作为网络安全威胁中的典型攻击手段，从诞生的那天起就从未停止，而网络安全威胁也正在变得日益复杂，各类攻击目标、手段就来源始终在不断的发生着变化，随之企业及各类组织需要不断关注这些发展趋势，以便能够理解与预测未来可能遭遇到的恶意攻击，进而让应对复杂变化所带来的挑战。

随着 DDoS 的攻击日益加剧，年度报告已经无法快速呈现其发展态势，故绿盟科技从 2012 年起，增发 DDoS 威胁报告半年报。本次报告即为 2015 上上半年的 DDoS 威胁报告，在年底前后绿盟科技威胁响应中心将会发布《2015 DDoS 威胁报告》，即 2015 年度安全报告。《2015 DDoS 威胁报告》，帮助大家：

- 持续了解及掌握 DDoS 威胁发展态势
- 在遭遇到攻击后，可以快速理解及检测可能的伤害程度
- 不断强化网络安全意识，完善解决方案

关注 DDoS 威胁报告

如果您希望与我们一起持续关注这个项目，请关注：

- DDoS 威胁报告：
- http://www.nsfocus.com.cn/research/report.html
- 绿盟科技官方微博：
- http://weibo.com/nsfocus
- 绿盟科技官方微信：
- 搜索公众号 绿盟科技

扫描二维码，在线看报告

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS