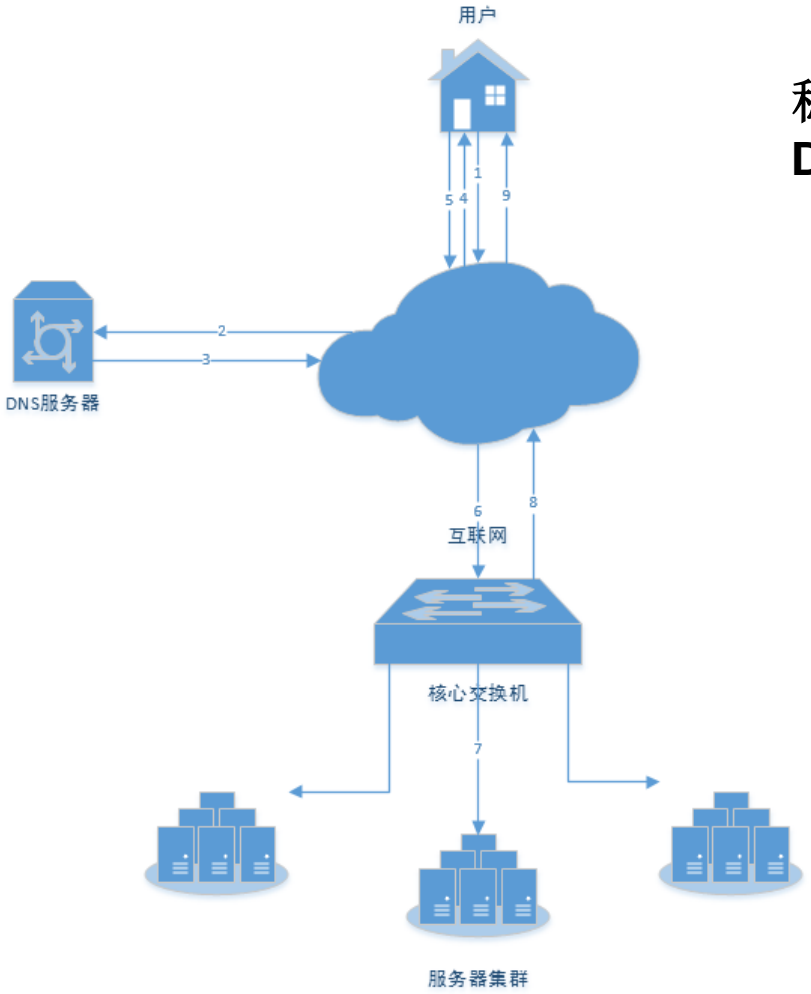
基于CDN平台的DDOS攻击防护

百度云安全部 吴昊挺

wuhaoting@baidu.com

百度云加速网络攻击防御负责人

用户是怎么获取服务的？



稳定服务的三要素：
DNS、进出口带宽、服务器集群

DDoS攻击是什么？

DDoS Distributed Denial of Service 分布式拒绝服务

- **系统漏洞型攻击**

利用操作系统、TCP/IP协议、应用程序等缺陷，构造某种特殊的数据包，是系统停止对正常用户的访问请求或使操作系统、应用程序崩溃；

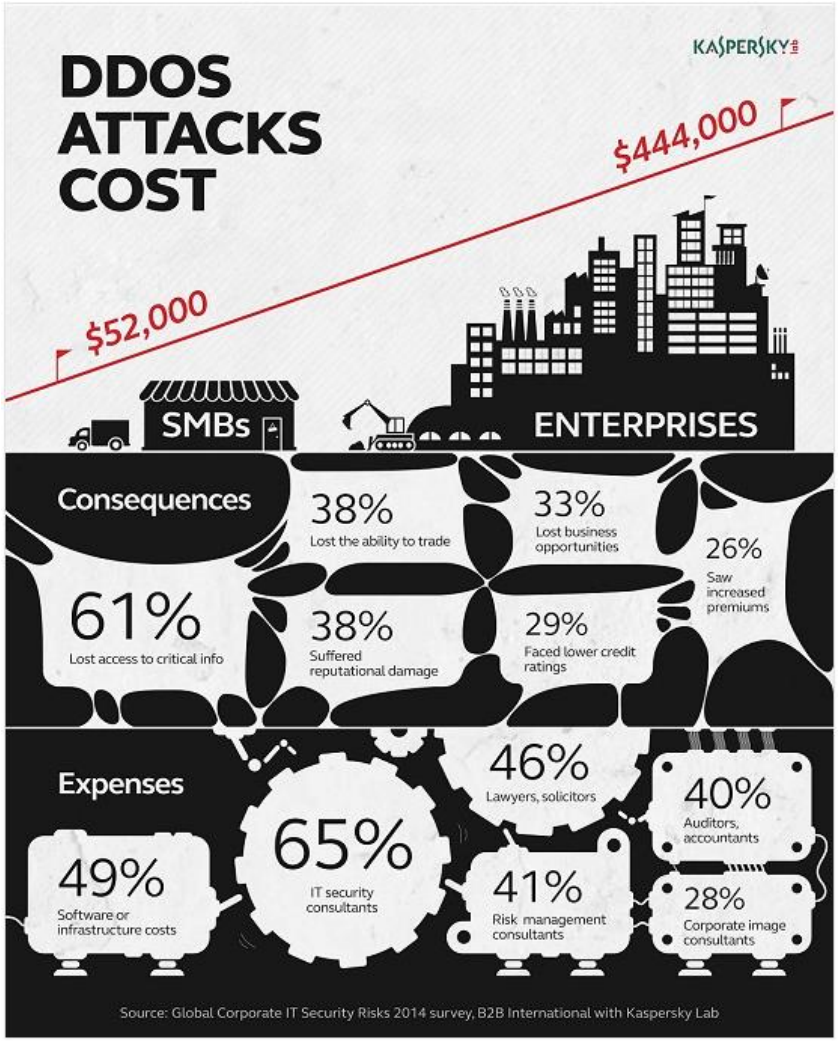
- **大流量型攻击**

攻击者利用比被攻击网络更大的带宽，生成大量发向被攻击网络的数据包，从而耗尽被攻击网络的有效带宽或被攻击系统的处理能力，是攻击目标瘫痪；

- **大流量+应用型+混合型攻击**

基于大流量模型，通过对协议特征、源IP、应用层数据内容等利用来实现对攻击目标的复杂隐蔽性攻击；

DDoS攻击的危害



一个单一的DDoS（分布式拒绝服务）对公司的在线资源的攻击可能会造成相当大的损失，平均的数字根据公司规模的不同，大概从52，000美元到美国444，000美元不等。

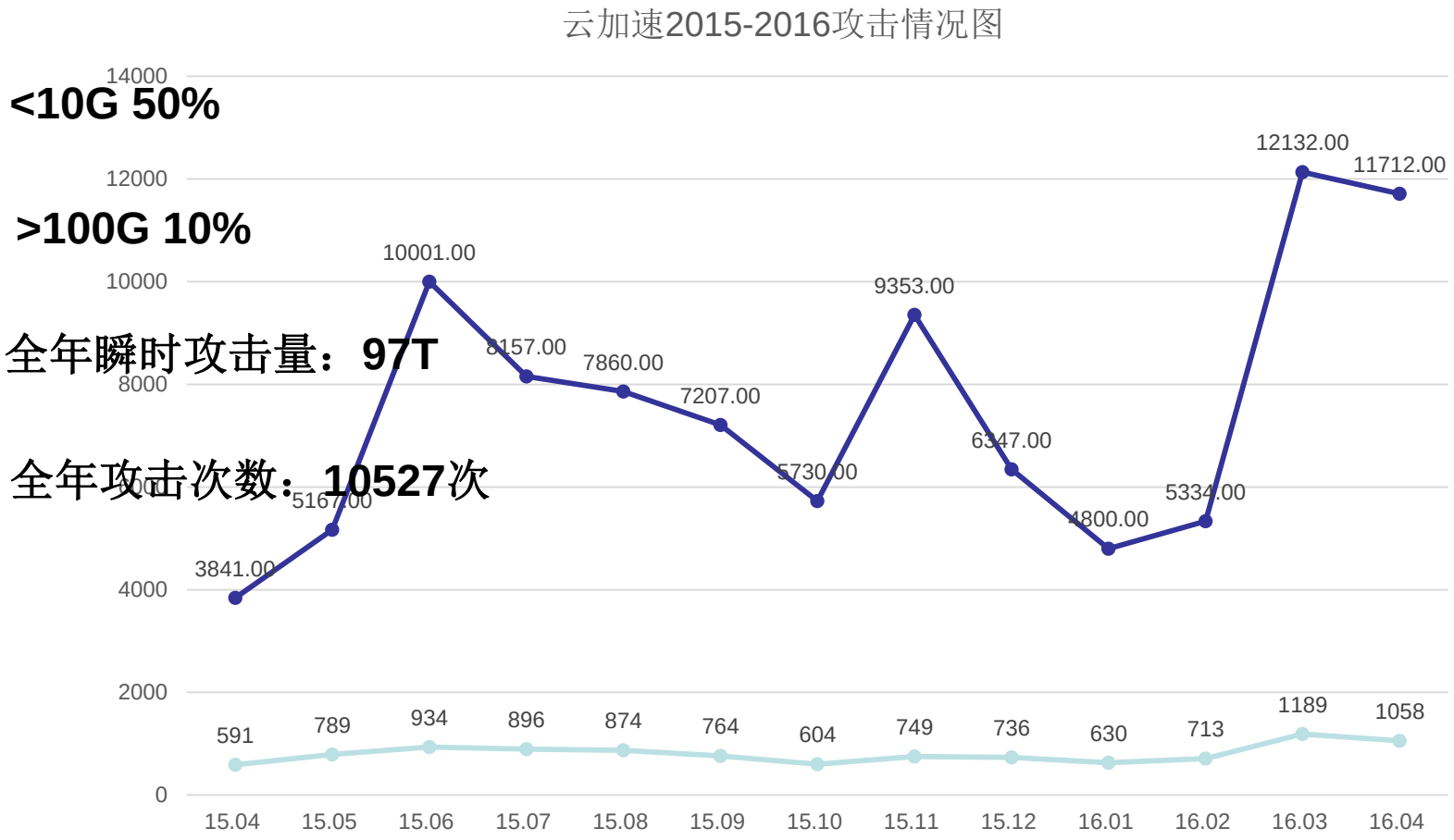
DDoS攻击造成61%的公司无法访问其关键业务信息，38%公司无法访问其关键业务，33%的受害者因此有商业合同或者合同上的损失

遭遇攻击后65%的公司会向IT安全专家咨询，49%的公司会支付资金来修改他们的IT基础设施，46%的受害者不得不咨询律师服务，还有41%的公司会投资保险业务

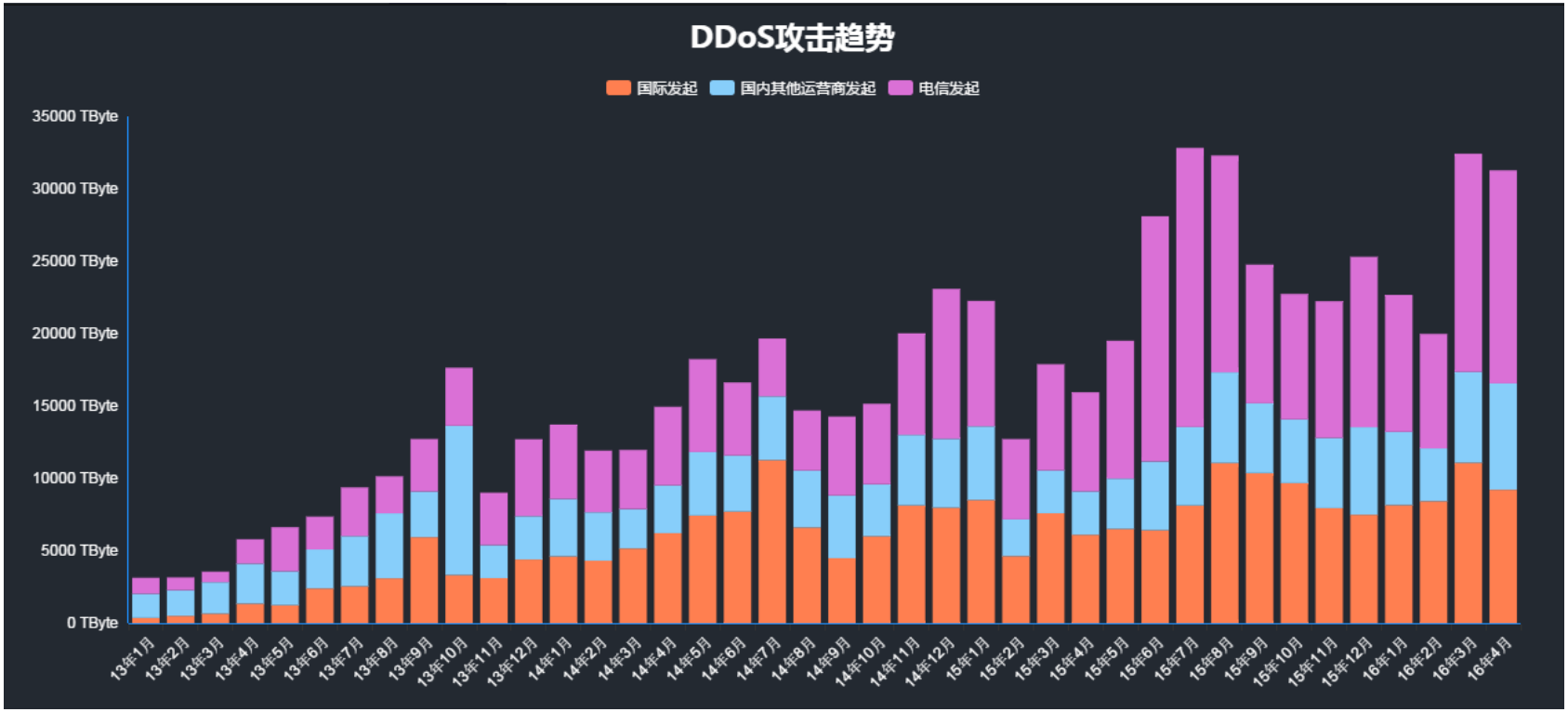
大纲

- DDoS攻击趋势
- DDoS攻击防护思考
- CDN是什么？
- 云加速DDoS防护方案
- Q&A

攻击规模呈增长趋势


云加速2015-2016攻击情况图
<10G 50%
>100G 10%
全年瞬时攻击量：97T
全年攻击次数：10527次
14000
12000
10000
8000
6000
4000
2000
0
3841.00
5167.00
10001.00
8157.00
7860.00
7207.00
5730.00
9353.00
6347.00
4800.00
5334.00
12132.00
11712.00
591
789
934
896
874
764
604
749
736
630
713
1189
1058
15.04
15.05
15.06
15.07
15.08
15.09
15.10
15.11
15.12
16.01
16.02
16.03
16.04

流量越来越大



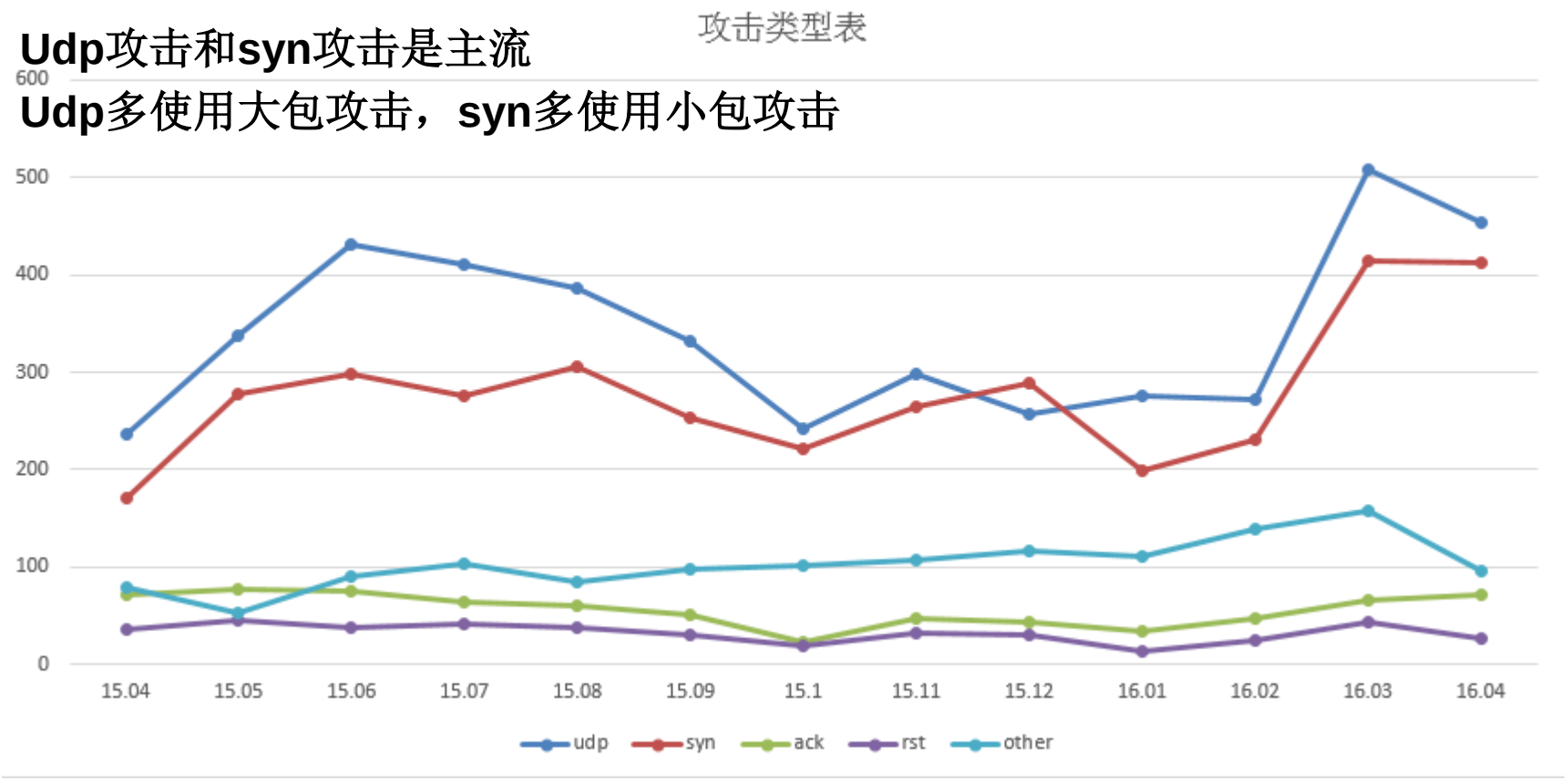
来自电信云堤

Baidu 百度

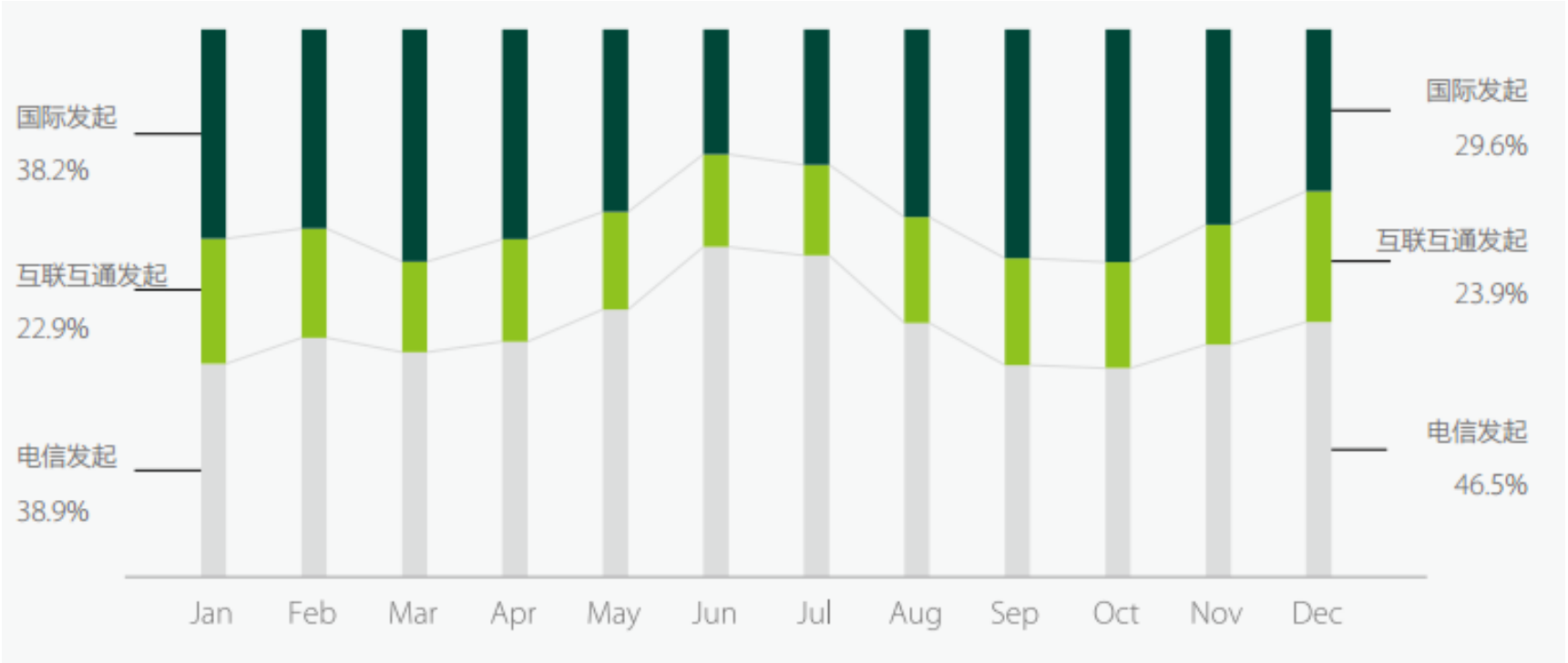
攻击的类型

Udp攻击和syn攻击是主流

Udp多使用大包攻击，syn多使用小包攻击



攻击的来源



来自电信云堤

大纲

- DDoS攻击趋势
- DDoS攻击防护思考
- CDN是什么？
- 云加速DDoS防护方案
- Q&A

如何防御DDOS攻击

加个防火墙吧？

上台高性能的ADS吧？

再加几G带宽吧？

Baidu 百度

我们能做些什么？

1、程序层面：

安全的编码和架构设计；

页面静态化，减少CPU消耗；

针对可能被用户刷的一些CGI或是WEB页面，**加上频率限制和验证码**；

2、主机和系统层面：

充分利用服务器的功能、比如开启服务器的syn cookie防护小流量syn flood;

使用主机防火墙丢弃一些恶意IP，如linux的iptables，配合脚本进行分析实现简单ddos防护或是连接耗尽防护

3、网络设备层面：

使用交换机/路由器ACL，过滤掉服务器不需要的流量，例如针对WEB服务器的UDP/ICMP流量；

启用具有防DDOS功能的防火墙或专业的硬件ADS设备；

4、网络环境层面：

多线出口；

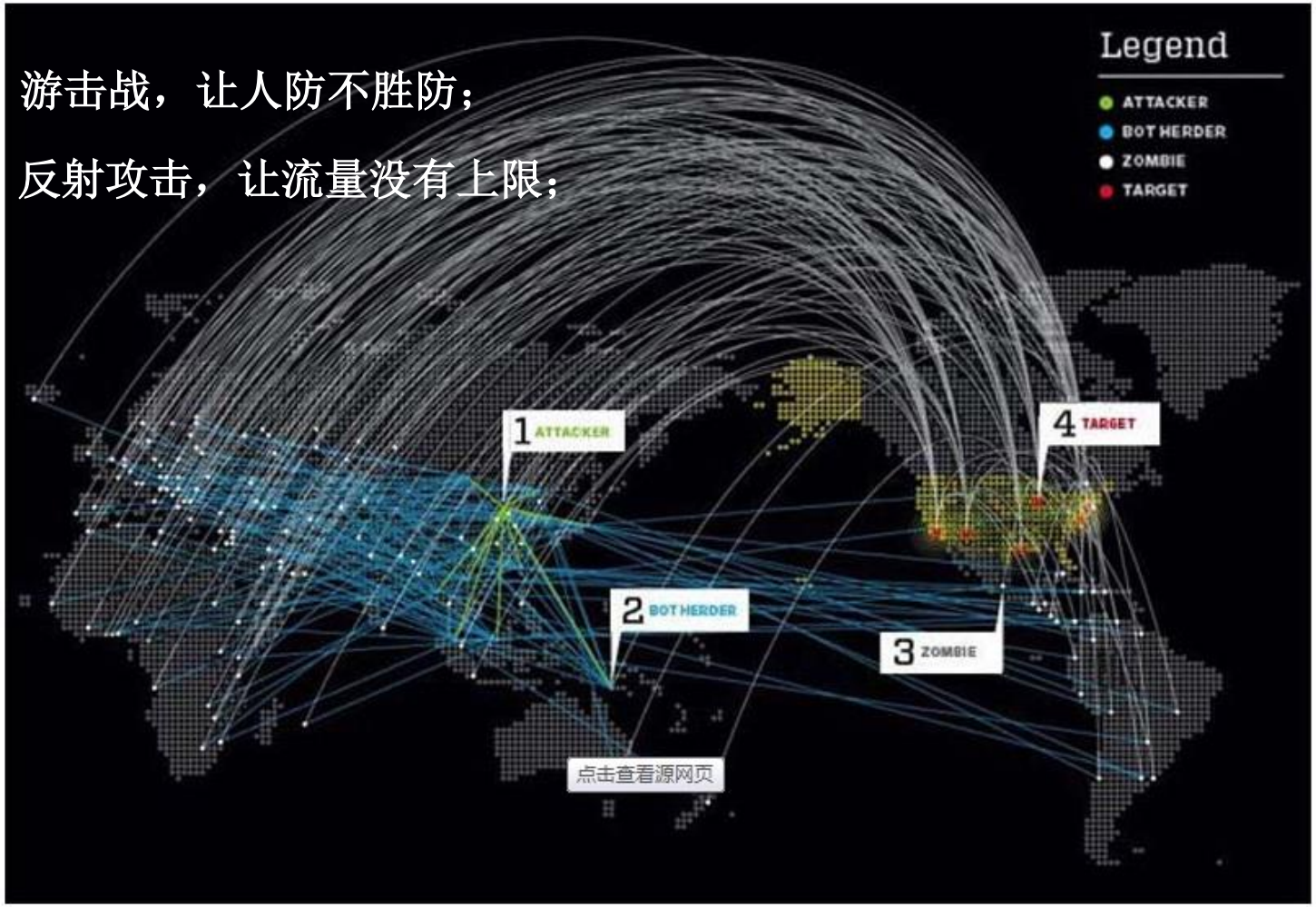
足够的带宽；

Baidu 百度

为什么服务还是不正常？

游击战，让人防不胜防；

反射攻击，让流量没有上限；



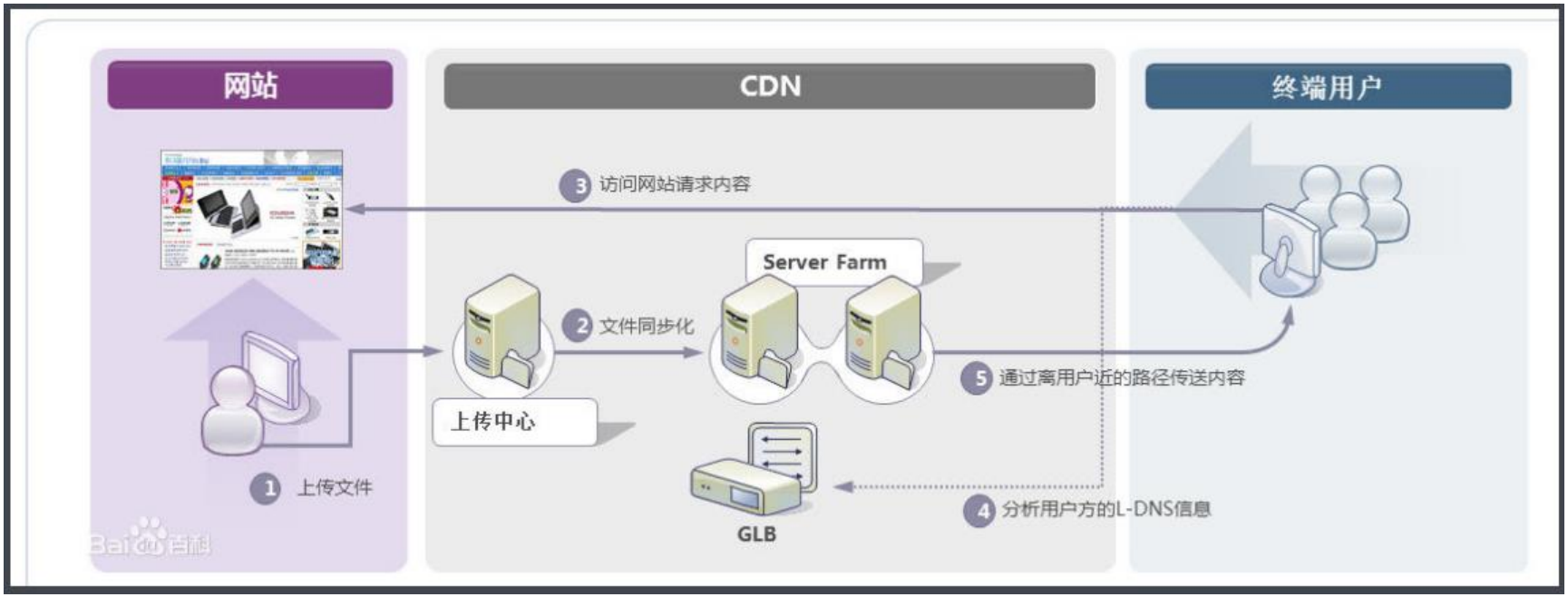
大纲

- DDoS攻击趋势
- DDoS攻击防护思考
- CDN是什么？
- 云加速DDoS防护方案
- Q&A

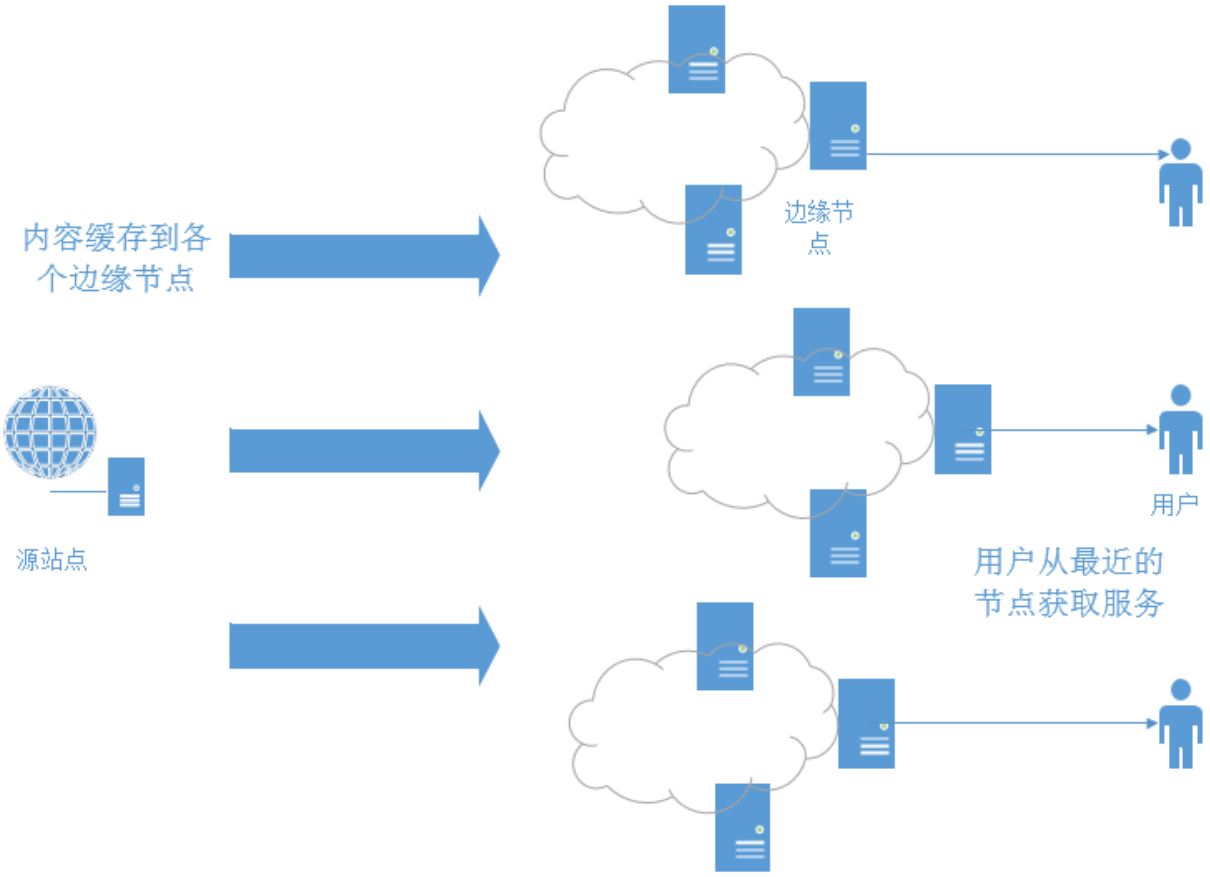
CDN是什么？

CDN的全称是Content Delivery Network，即内容分发网络。

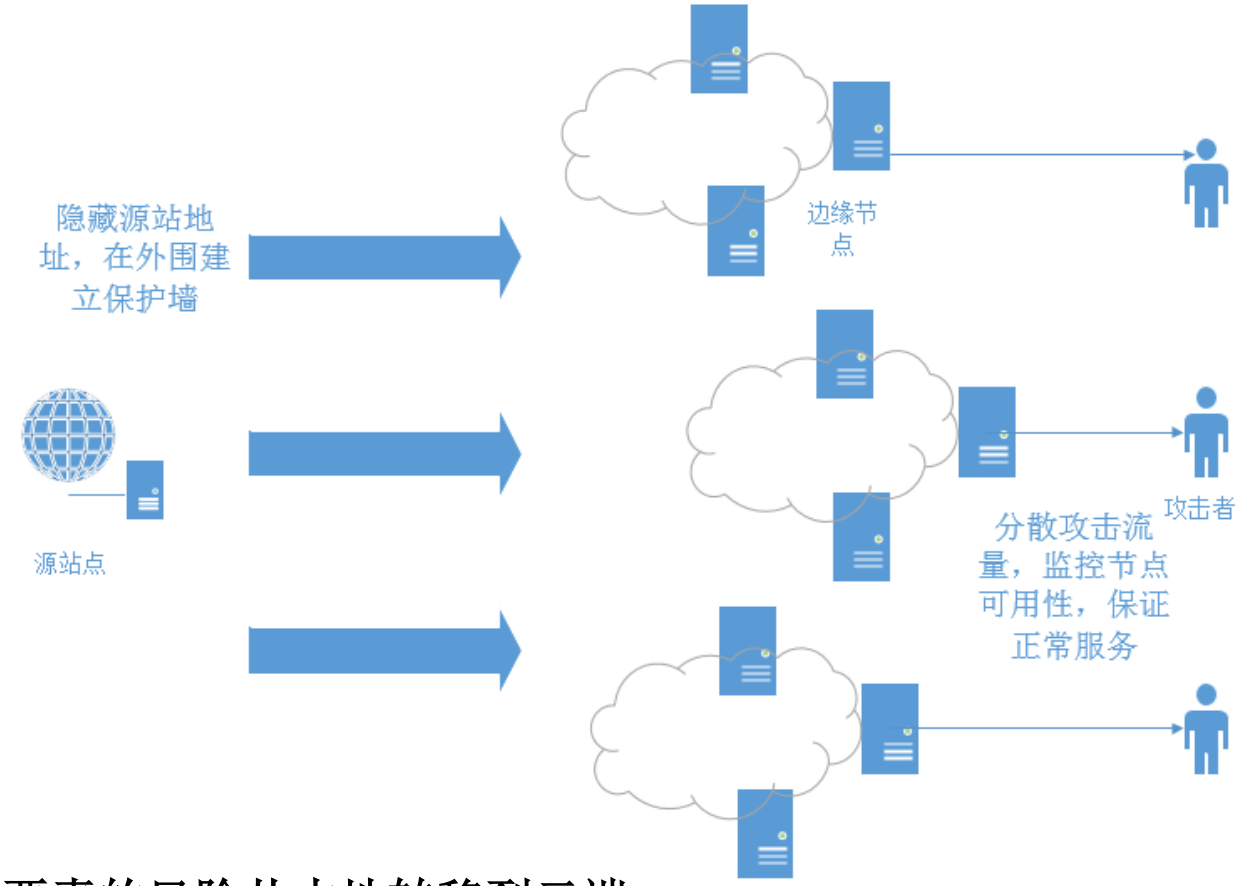
简单来说就是通过在网络各处放置节点服务器，让用户能够在离自己最近的地方访问服务，以此来提高访问速度和服务质量；



CDN的特性



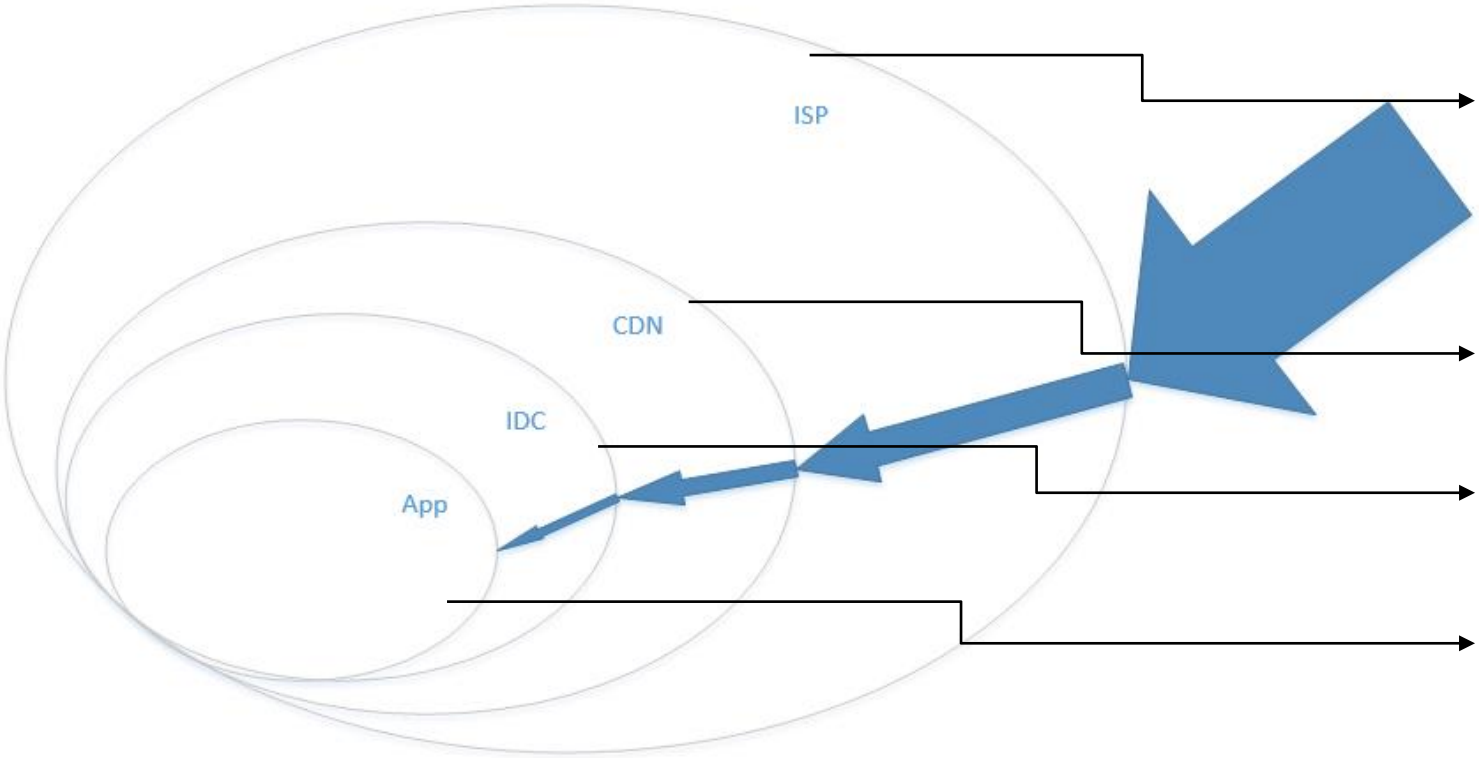
我们的思考



稳定性三要素的风险从本地转移到云端

Baidu 百度

DDoS层级防护



近源清洗，ISP、云服务商对攻击发起地的流量监控和清洗

云端清洗，利用cdn冗余带宽清洗攻击

IDC内清洗，配置专业防护设备

App进行精细化防护

使用云端CDN进行DDOS防御的三大优点

1、平时加速，战时防御

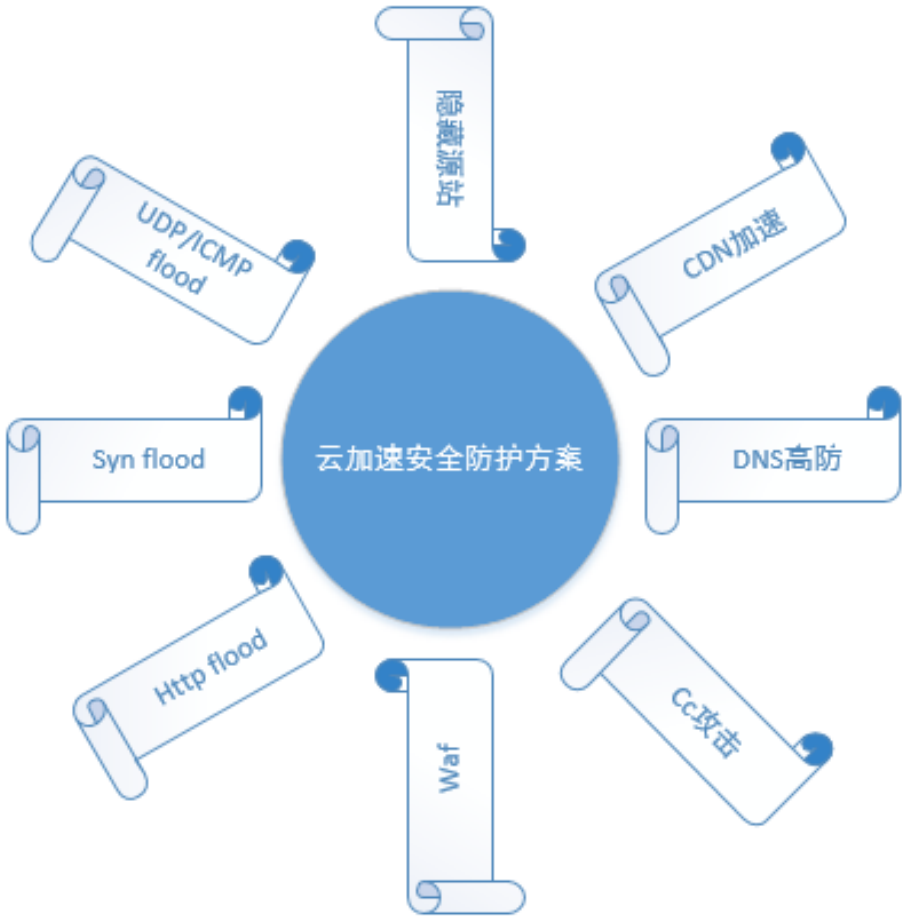
2、冗余带宽和资源

3、专业的运维团队

大纲

- DDoS攻击趋势
- DDoS攻击防护思考
- CDN是什么？
- 云加速DDoS防护方案
- Q&A

云加速的功能



1、CDN加速，利用智能调度和缓存，让用户能够就近服务，优化服务质量

2、隐藏源站，将攻击目标引至CDN节点，屏蔽源站的安全漏洞，阻挡恶意流量攻击

Baidu 百度

安全防护需要什么？

多点防御如何统筹？

混合型攻击如何防御？

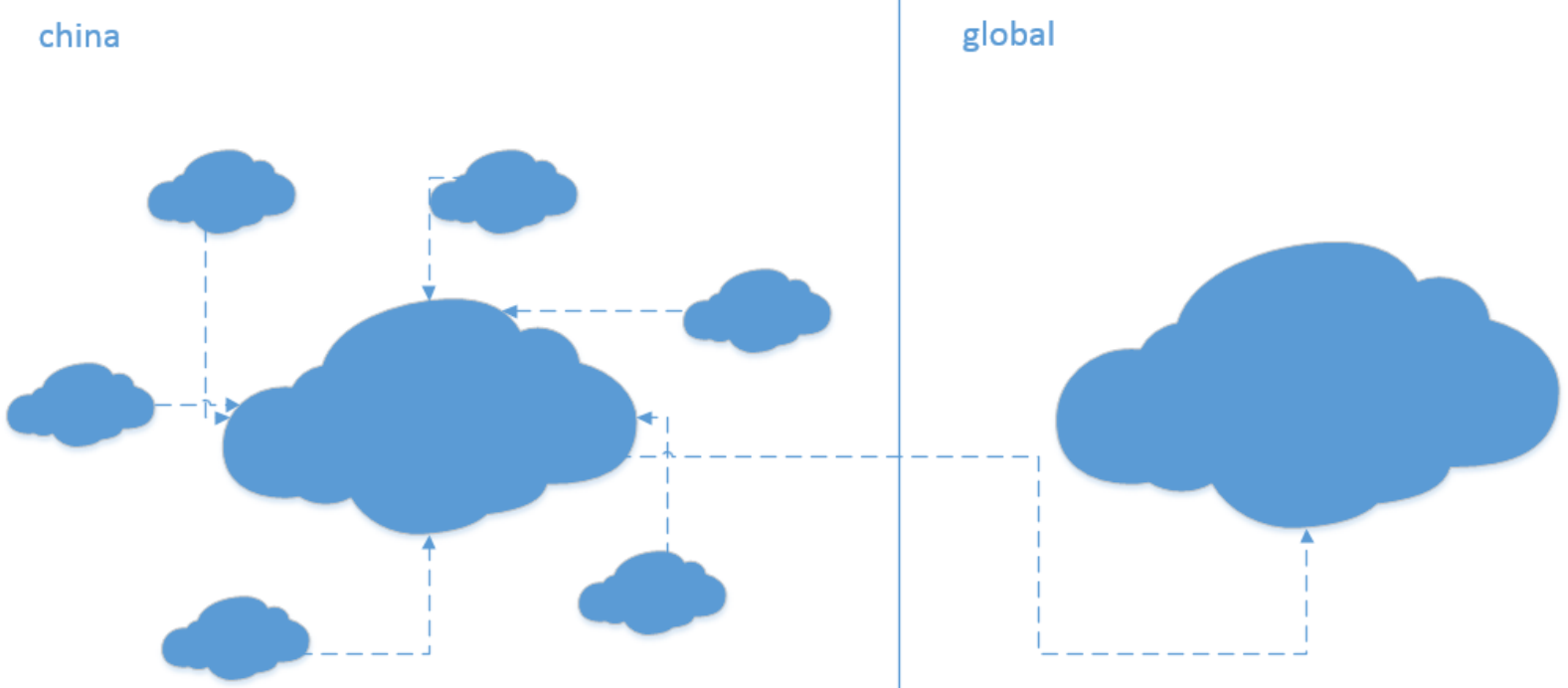
攻击点分散如何解决？

服务站点多怎么办？

Cdn防御ddos需要的不是一个防护设备，需要的是一个防御体系！

分散的网络环境

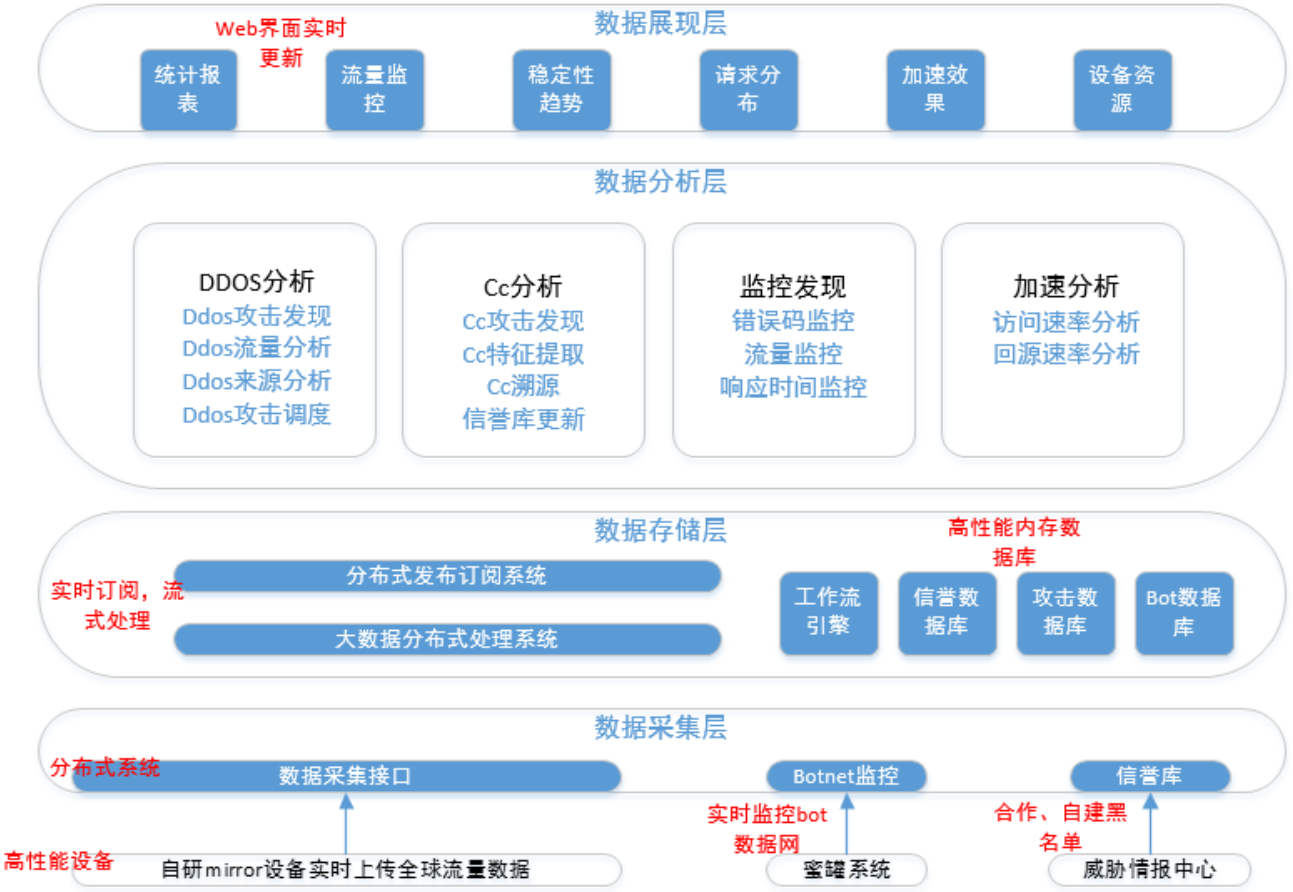
风险均摊，鸡蛋不能放一个篮子里；



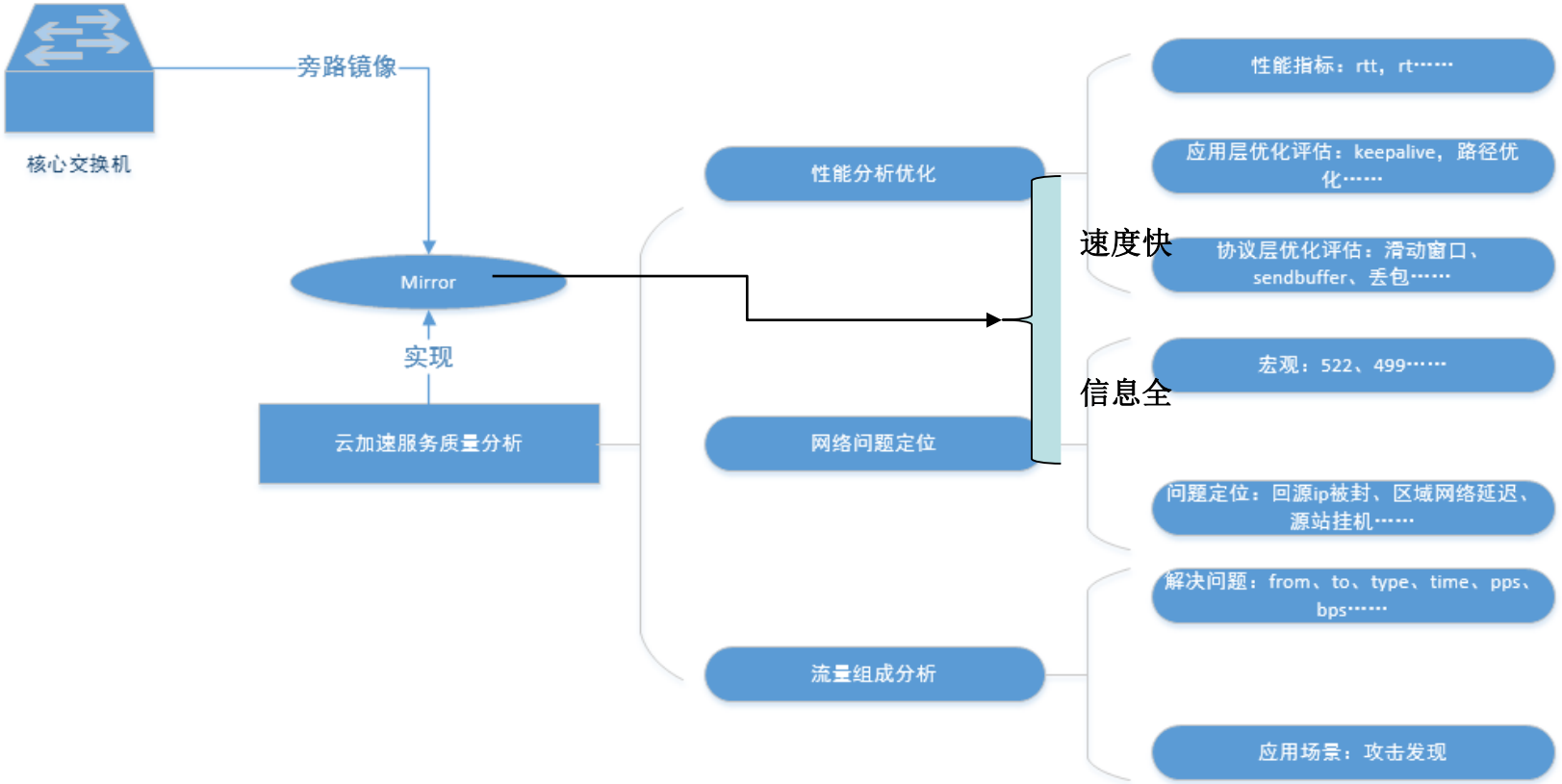
通用节点满足日常需求、高防节点负责流量对抗；

Global节点作为最后的防线；

统一的决策系统

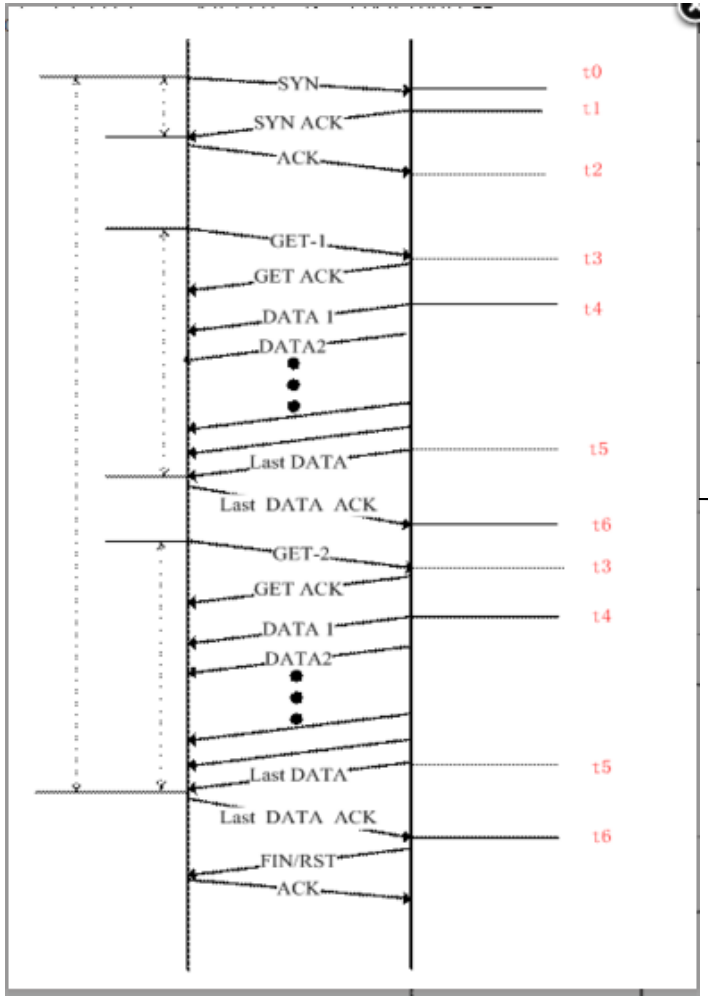

数据展现层
Web界面实时更新
统计报表
流量监控
稳定性趋势
请求分布
加速效果
设备资源
数据分析层
DDOS分析
Ddos攻击发现
Ddos流量分析
Ddos来源分析
Ddos攻击调度
Cc分析
Cc攻击发现
Cc特征提取
Cc溯源
信誉库更新
监控发现
错误码监控
流量监控
响应时间监控
加速分析
访问速率分析
回源速率分析
数据存储层
高性能内存数据库
实时订阅，流式处理
分布式发布订阅系统
大数据分布式处理系统
工作流引擎
信誉数据库
攻击数据库
Bot数据库
数据采集层
分布式系统
数据采集接口
Botnet监控
信誉库
实时监控bot数据网
合作、自建黑名单
高性能设备
自研mirror设备实时上传全球流量数据
蜜罐系统
威胁情报中心

全能的监控设备


旁路镜像
核心交换机
Mirror
实现
云加速服务质量分析
性能分析优化
网络问题定位
流量组成分析
速度快
信息全
性能指标：rtt，rt……
应用层优化评估：keepalive，路径优化……
协议层优化评估：滑动窗口、sendbuffer、丢包……
宏观：522、499……
问题定位：回源ip被封、区域网络延迟、源站挂机……
解决问题：from、to、type、time、pps、bps……
应用场景：攻击发现

丰富的分析内容

Tcpflow+



Tcpflow信息—指导性能调优

三层流量统计—发现ddos攻击

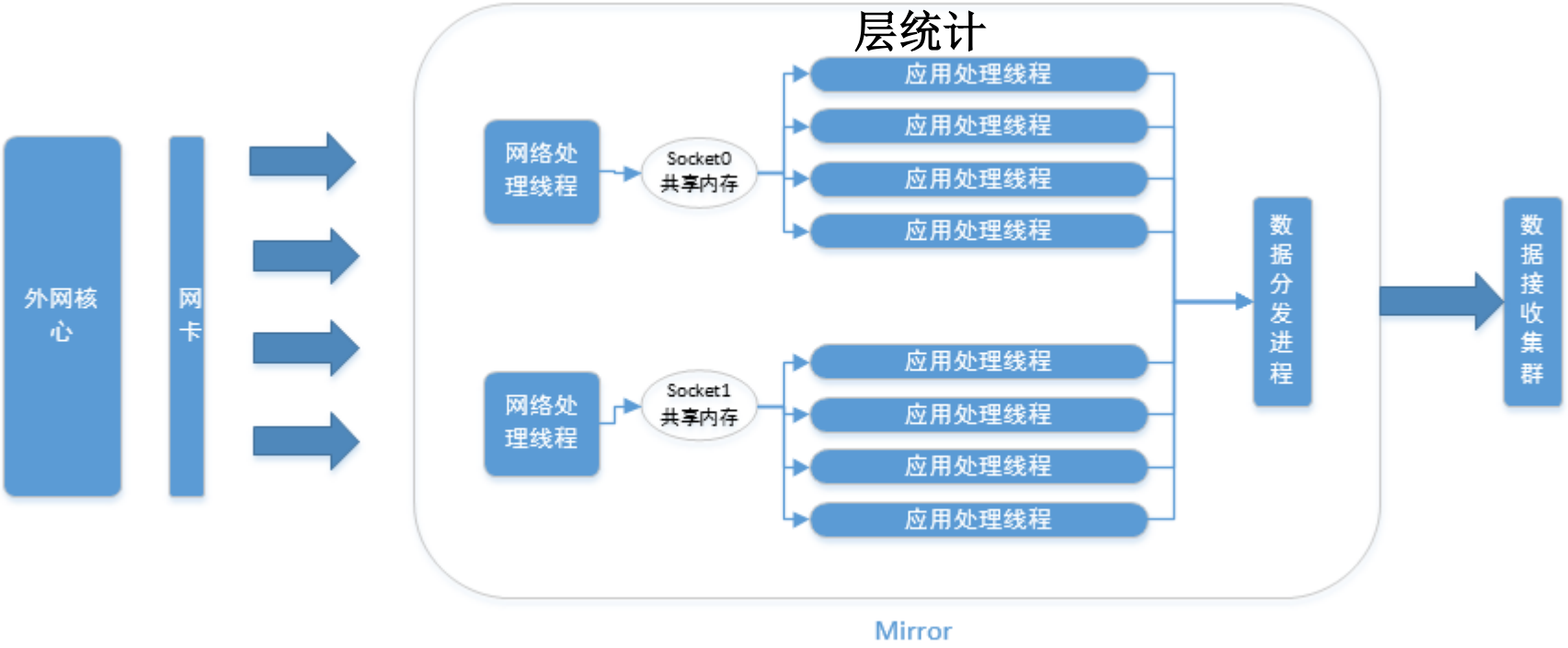
服务站点访问信息统计—保障源站存活

访问者特征统计—发现cc攻击

高性能的数据监控

DPDK + NUMA

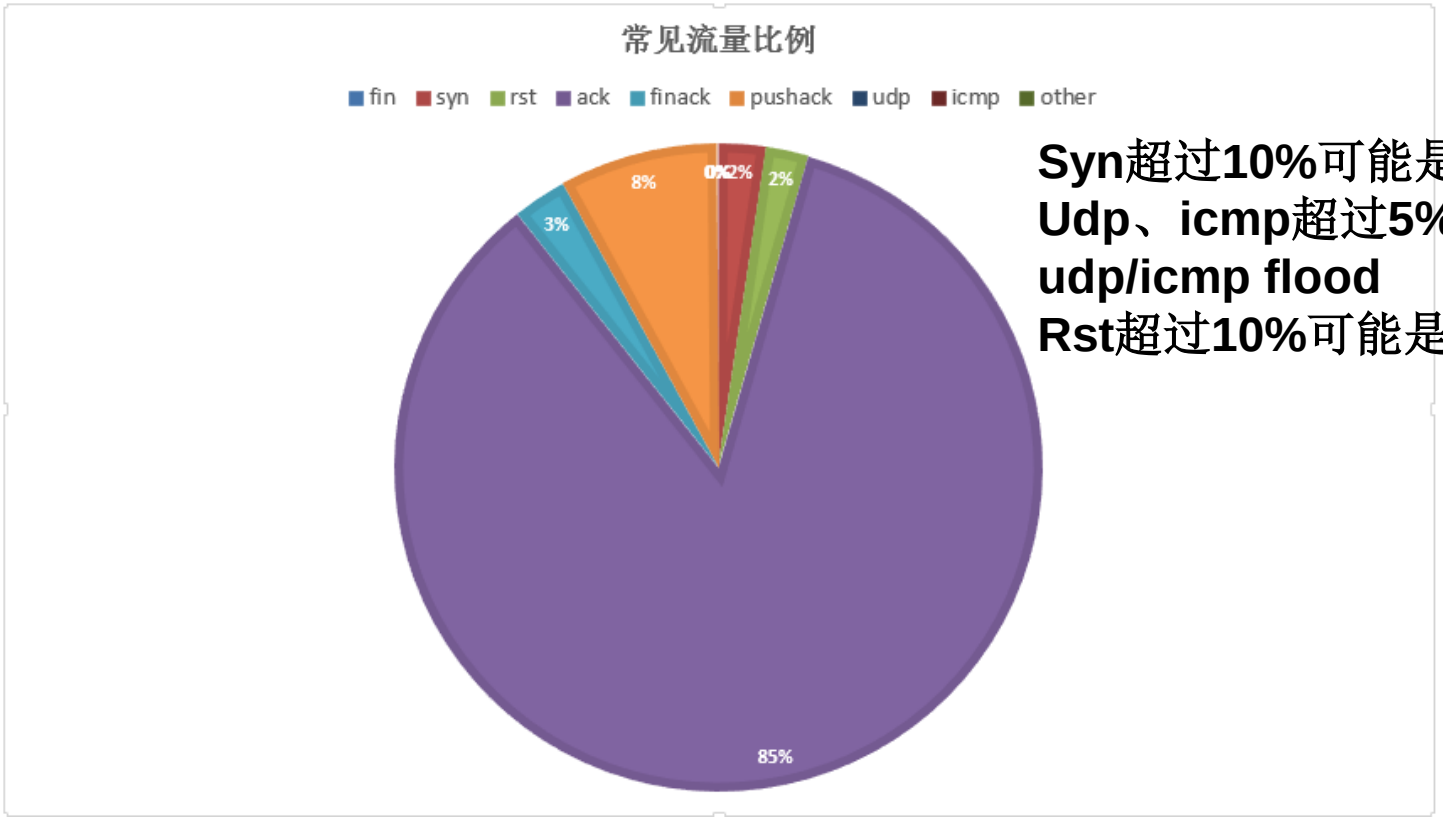
快慢通道解耦合，应用层处理不影响3层统计



单机2800wpps+500kcps+200kqps

Baidu 百度

准确的四层攻击发现策略



Syn超过10%可能是syn flood
Udp、icmp超过5%可能是udp/icmp flood
Rst超过10%可能是ack flood

传统的DNS调度

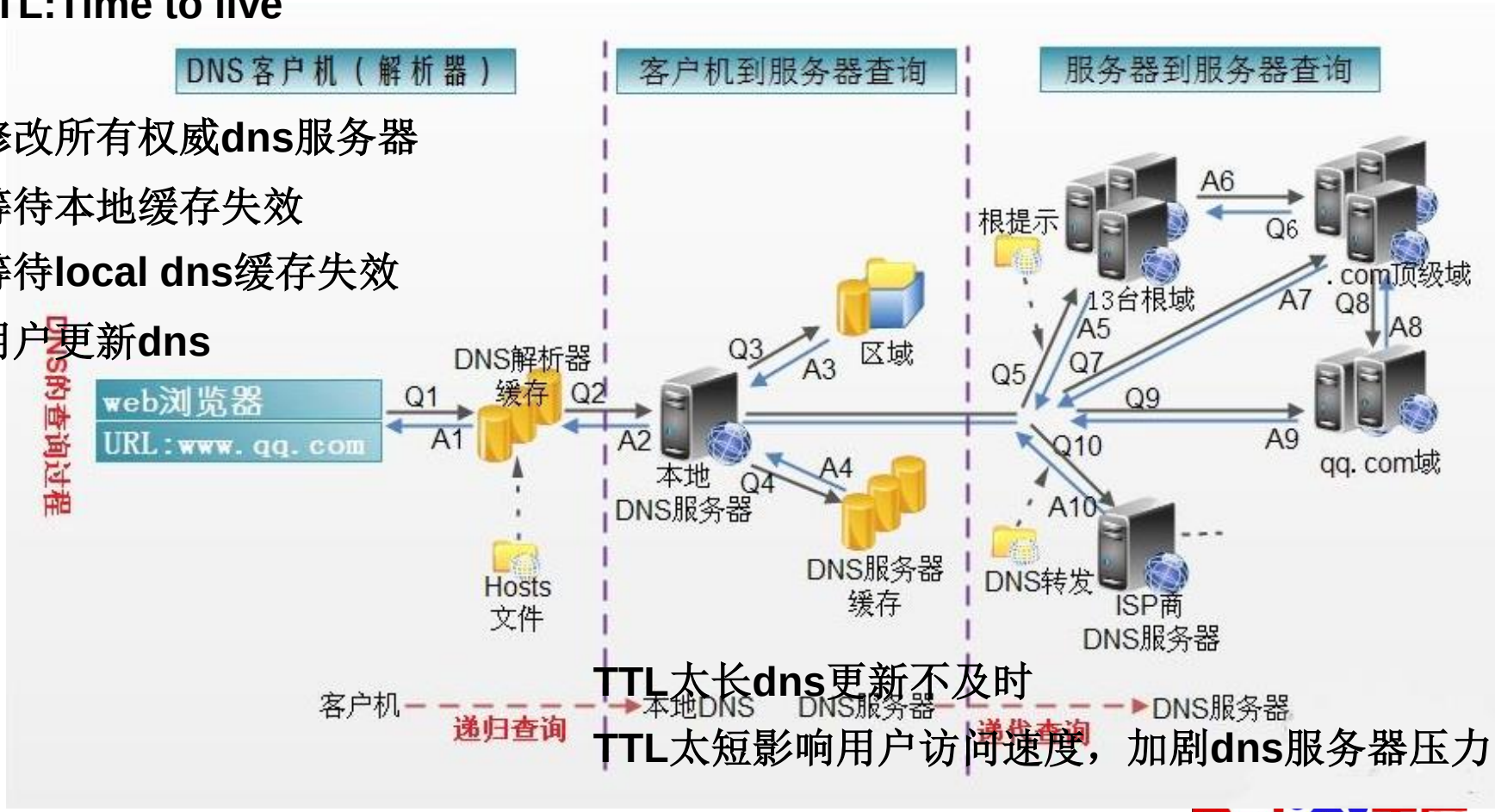
TTL:Time to live

修改所有权威dns服务器

等待本地缓存失效

等待local dns缓存失效

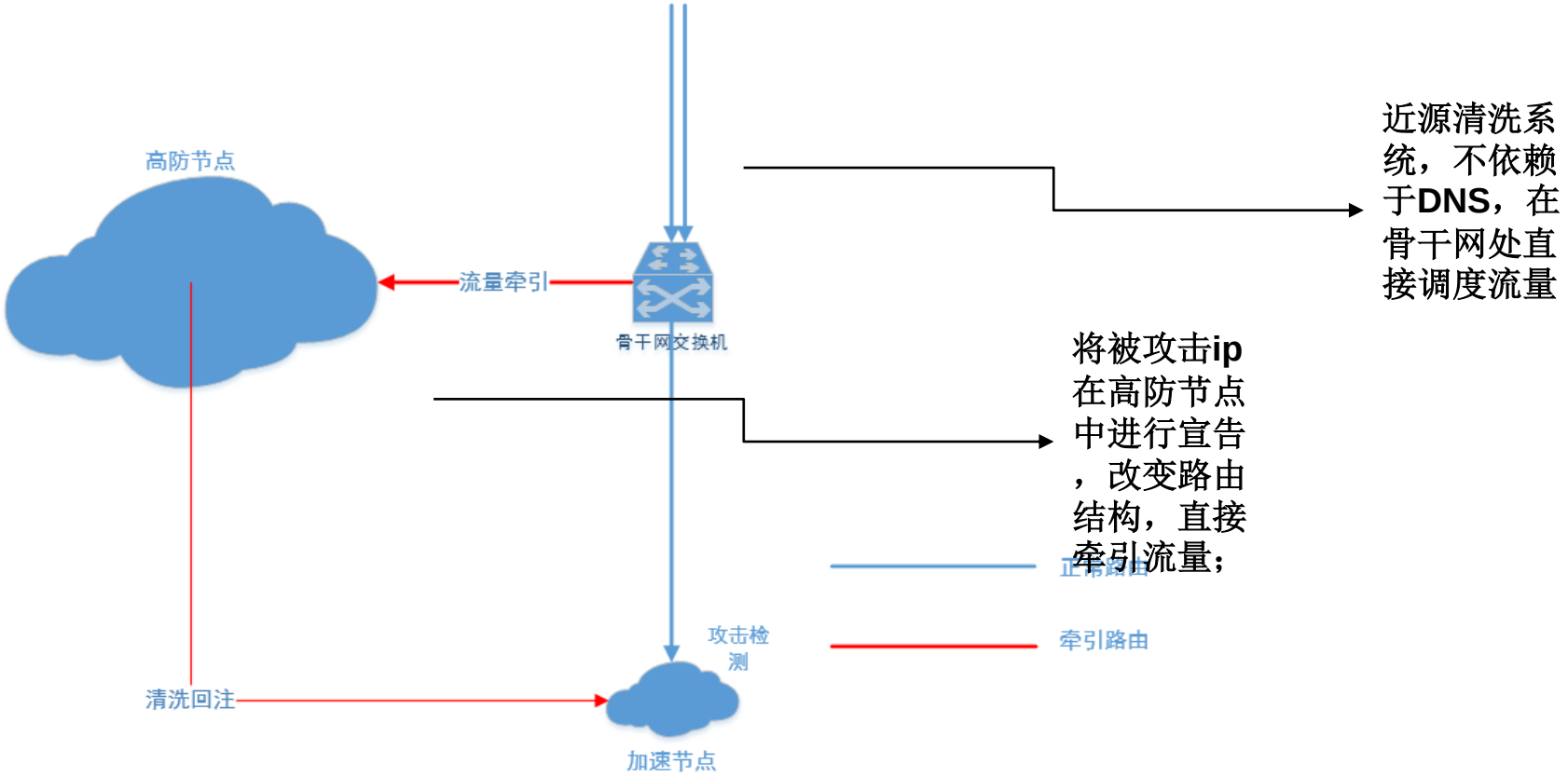
用户更新dns



TTL太长dns更新不及时

TTL太短影响用户访问速度，加剧dns服务器压力

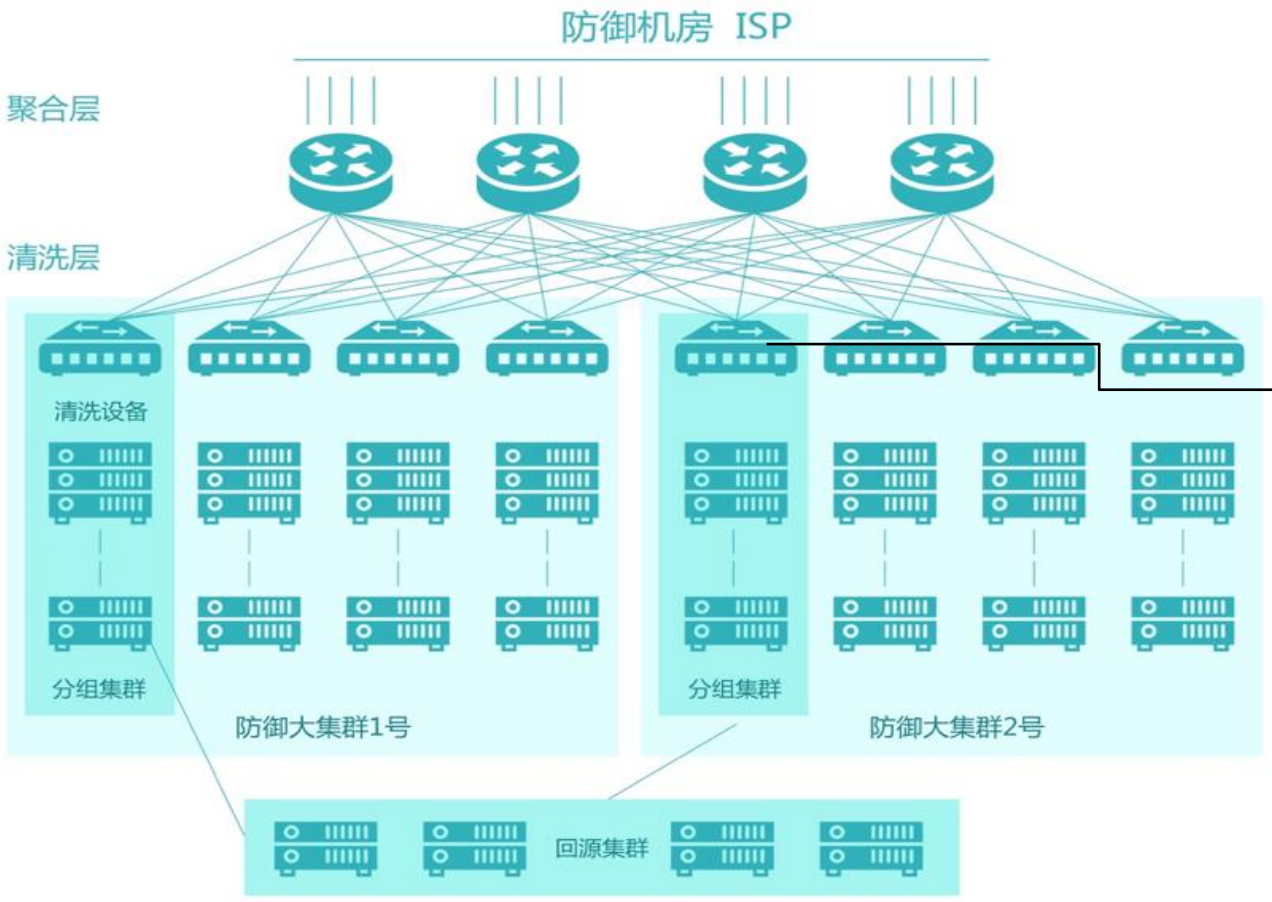
无损的调度方法


高防节点
流量牵引
骨干网交换机
近源清洗系统，不依赖于DNS，在骨干网处直接调度流量
将被攻击ip在高防节点中进行宣告，改变路由结构，直接牵引流量；
正常路由
牵引路由
攻击检测
清洗回注
加速节点

多样的防护策略

防御技术	描述	优点	缺点
Syn cookie/ Syn proxy	在syn包进入协议栈之前对来访syn包进行虚假回应，如果访问者完成正常的tcp握手再重新和保护主机进行tcp建连	防御效果好，对CS双方透明不会造成用户感知	消耗计算资源，需要强性能的机器，否则单机防护性能不高；消耗出口带宽；
Safe Reset	对所有的syn包均主动回应，探测包特意构造错误的字段，真实存在的IP地址会发送rst包给防护设备，然后发起第2次连接，从而建立TCP连接；	算法简单，不消耗资源，防护性能好	依赖协议栈特性，修改后的协议栈可能不会遵循，同时丢弃首个连接，造成用户体验差
Syn 重传	利用了TCP/IP协议的重传特性，来自某个源IP的第一个syn包到达时被直接丢弃并记录状态，在该源IP的第2个syn包到达时进行验证，然后放行	操作简单，消耗资源少，单机防护量大	依赖重传算法，理论上需要用户多等待3s的重传时间，且攻击器如果重发攻击包可绕过防护
智能算法	结合以上算法，将所有历史ip进行信誉分析，对不同信誉的ip使用不同的防护算法	对不同ip使用不同策略，积累历史防护经验，在计算资源和用户体验之间做到平衡	需要对实现上述所有防护策略，并针对业务设计最优策略，工期耗时长

智能防御集群



智能清洗集群，高效清洗流量

Cc防御的几个阶段

- **开始阶段**

Web服务器的瞬时链接数量急剧增多

访问Web服务器的IP数量急剧增多

- **定位阶段**

部分特征请求(IP、UA、referer)访问的频率非常快

部分特征访问请求(IP、UA、referer)的URL非常单一或者规律性非常明显

- **触发阶段**

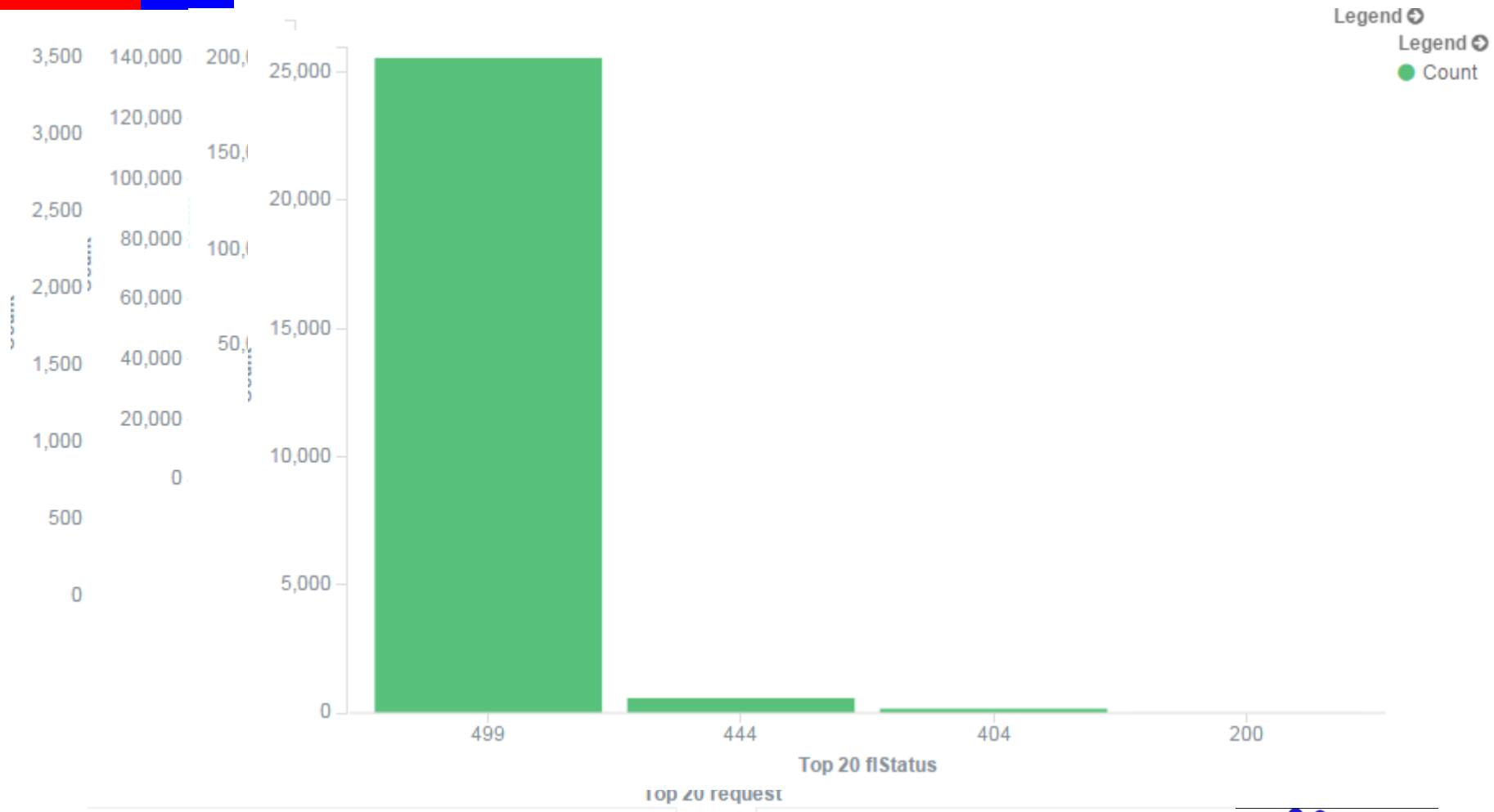
服务器的响应数和客户端的请求数比例开始变低

服务器响应速度开始变慢甚至停止服务

- **回顾阶段**

IP信誉积累

攻击的样例


Legend
Legend
Count
25,000
20,000
15,000
10,000
5,000
0
499
444
404
200
Top 20 flStatus
Top 20 request

Cc防御的手段和难点

- **CC攻击特征**
  - 攻击手段多样化
  - 绕过技术高，一些新的攻击不仅能绕过cookie，连js验证都能绕过
  - 模拟的更像正常访问

- **防御难度**
  - 突发的攻击容易导致源站死掉
  - 客户挑揚使用弹窗验证码的防御方式

- **业内防御**
  - Cookie, js验证 + 弹窗验证码
  - 只提清洗率，不提误拦截率
  - 存在突发流量透过导致源站宕机

Baidu 百度

创新的防御手段

- **创新的源站保护模式 -- 实现99%的清洗率**
  - 分多个不同优先级的队列管理请求
  - 能感知源站响应能力，适当放行请求量，保护源站

- **节点分析及放大能力 -- 实现0.1%的低误拦截率**
  - 自动分析可疑IP
  - 自动分析疑似被攻击的url
  - 筛选恶意IP，优先拦截
  - 辅助cookie，js验证放行误拦截，降低误拦截
  - 自动提取明显特征进行拦截，快速清洗
  - 通过缓存及自动内容放大响应内容，拦截前有充分的分析机会
  - 结合节点带宽资源，适当实现网络层拦截，保护节点可用性

Baidu 百度

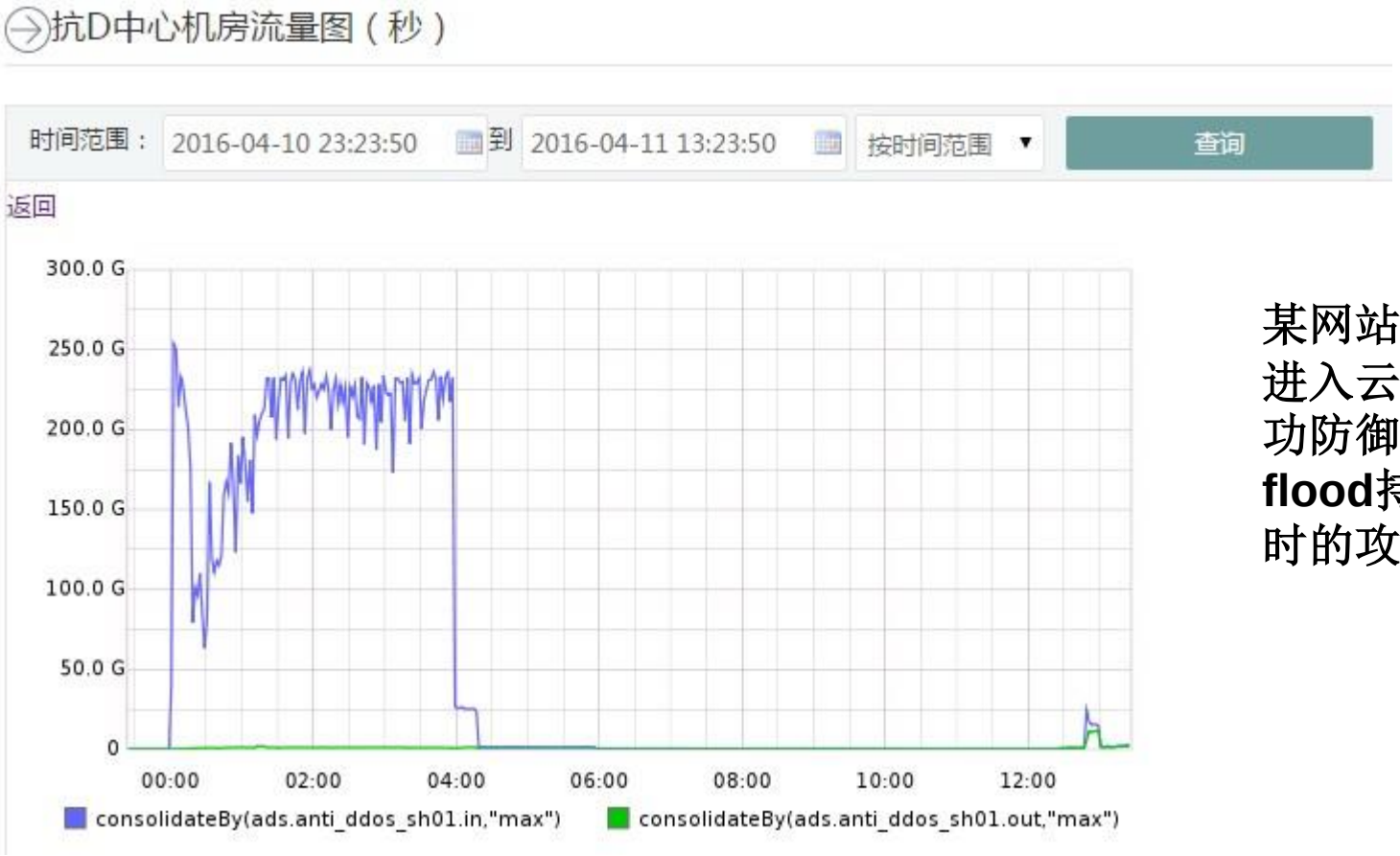
攻击案例

序号	日期	峰值时间	峰值带宽(Gbps)	被攻击域名
1	2015年6月19日	18:34:36	190.79	未知
2	2015年6月20日	23:47:10	213.20	未知
3	2015年7月15日	16:49:33	233.40	0571scg.com
4	2015年7月16日	14:32:45	205.11	douwan28.com
5	2015年7月16日	14:36:30	225.41	hycjyy.com
6	2015年7月16日	15:21:11	247.98	douwan288.com
7	2015年7月27日	11:11:14	227.83	jinchengsy.com
8	2015年8月2日	10:17:52	222.80	dshxtc.com
9	2015年8月6日	11:45:43	197.99	myb520.com
10	2015年8月7日	12:00:37	186.99	myb520.com
11	2015年8月7日	12:17:42	210.69	tfboys.com

击实

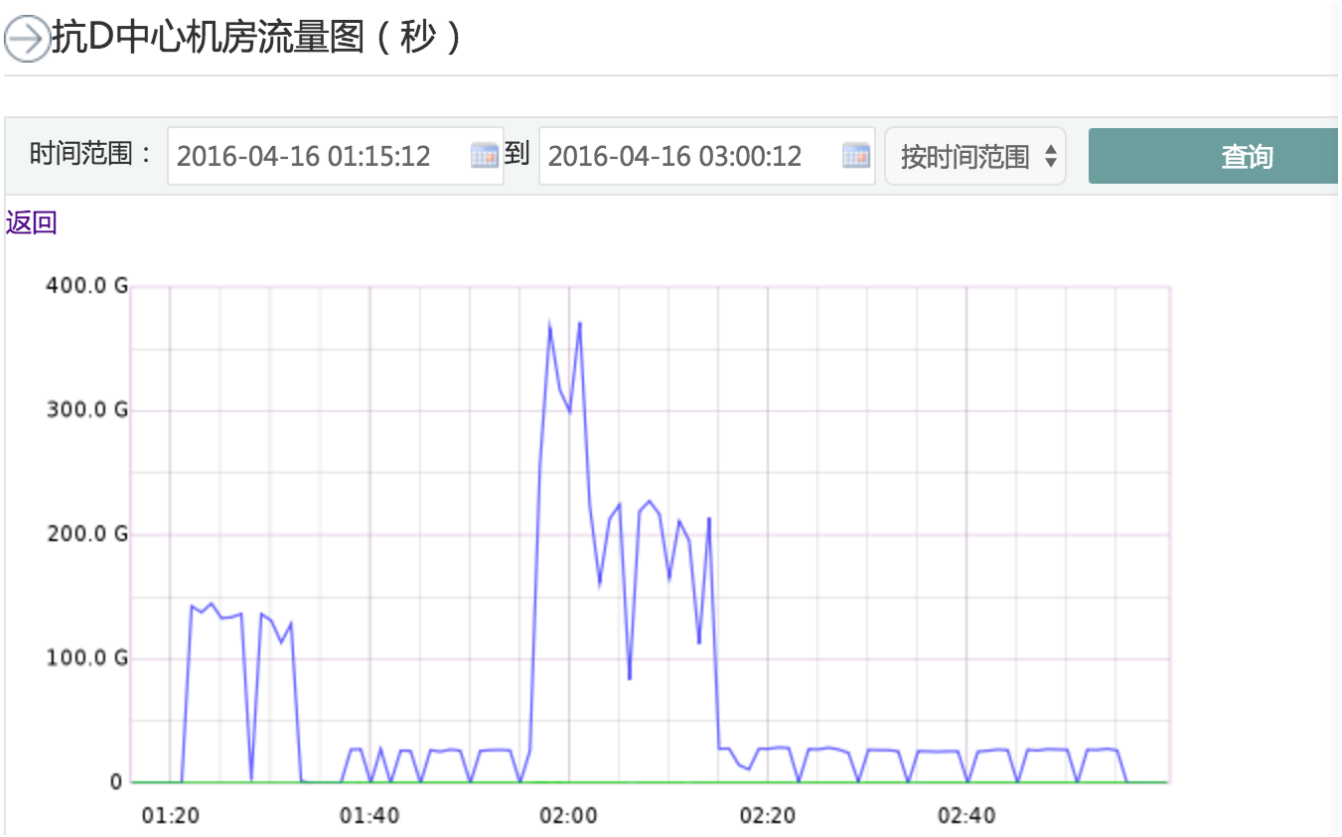
高防机房的一天

攻击案例



某网站4月10日进入云加速，成功防御200Gsyn flood持续4个小时的攻击

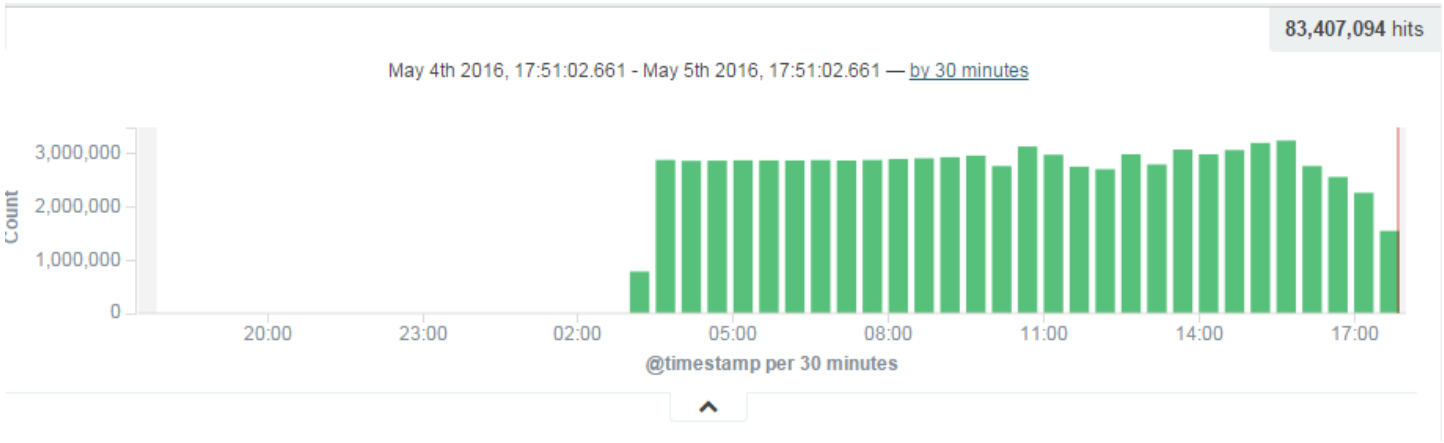
攻击案例



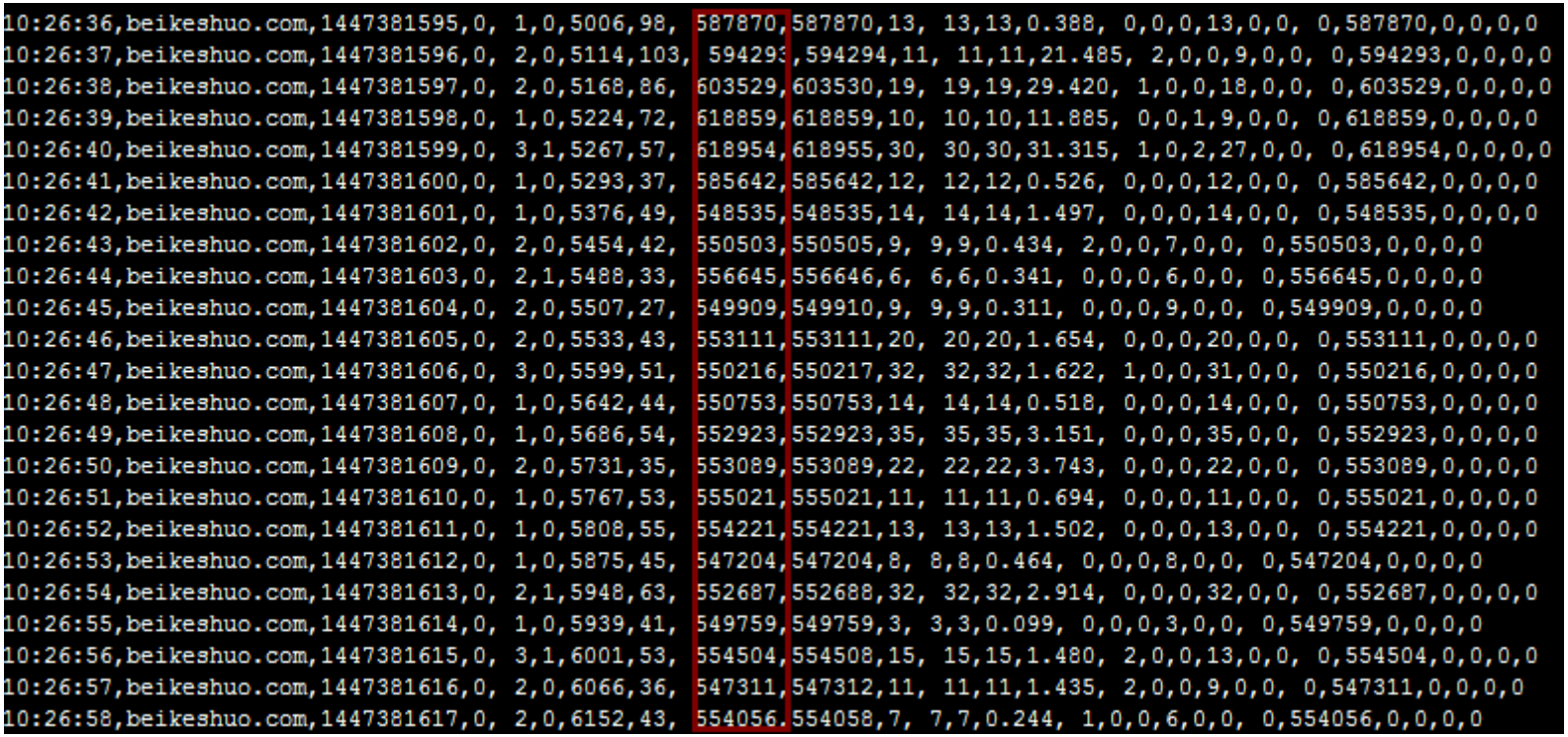
某网站4月16日进入云加速，成功防御最高380G攻击

攻击案例

某网站5月5日进入云加速，成功防御8000万+的cc攻击



攻击案例



```
10:26:36,beikeshuo.com,1447381595,0, 1,0,5006,98, 587870,587870,13, 13,13,0.388, 0,0,0,13,0,0, 0,587870,0,0,0,0
10:26:37,beikeshuo.com,1447381596,0, 2,0,5114,103, 594293,594294,11, 11,11,21.485, 2,0,0,9,0,0, 0,594293,0,0,0,0
10:26:38,beikeshuo.com,1447381597,0, 2,0,5168,86, 603529,603530,19, 19,19,29.420, 1,0,0,18,0,0, 0,603529,0,0,0,0
10:26:39,beikeshuo.com,1447381598,0, 1,0,5224,72, 618859,618859,10, 10,10,11.885, 0,0,1,9,0,0, 0,618859,0,0,0,0
10:26:40,beikeshuo.com,1447381599,0, 3,1,5267,57, 618954,618955,30, 30,30,31.315, 1,0,2,27,0,0, 0,618954,0,0,0,0
10:26:41,beikeshuo.com,1447381600,0, 1,0,5293,37, 585642,585642,12, 12,12,0.526, 0,0,0,12,0,0, 0,585642,0,0,0,0
10:26:42,beikeshuo.com,1447381601,0, 1,0,5376,49, 548535,548535,14, 14,14,1.497, 0,0,0,14,0,0, 0,548535,0,0,0,0
10:26:43,beikeshuo.com,1447381602,0, 2,0,5454,42, 550503,550505,9, 9,9,0.434, 2,0,0,7,0,0, 0,550503,0,0,0,0
10:26:44,beikeshuo.com,1447381603,0, 2,1,5488,33, 556645,556646,6, 6,6,0.341, 0,0,0,6,0,0, 0,556645,0,0,0,0
10:26:45,beikeshuo.com,1447381604,0, 2,0,5507,27, 549909,549910,9, 9,9,0.311, 0,0,0,9,0,0, 0,549909,0,0,0,0
10:26:46,beikeshuo.com,1447381605,0, 2,0,5533,43, 553111,553111,20, 20,20,1.654, 0,0,0,20,0,0, 0,553111,0,0,0,0
10:26:47,beikeshuo.com,1447381606,0, 3,0,5599,51, 550216,550217,32, 32,32,1.622, 1,0,0,31,0,0, 0,550216,0,0,0,0
10:26:48,beikeshuo.com,1447381607,0, 1,0,5642,44, 550753,550753,14, 14,14,0.518, 0,0,0,14,0,0, 0,550753,0,0,0,0
10:26:49,beikeshuo.com,1447381608,0, 1,0,5686,54, 552923,552923,35, 35,35,3.151, 0,0,0,35,0,0, 0,552923,0,0,0,0
10:26:50,beikeshuo.com,1447381609,0, 2,0,5731,35, 553089,553089,22, 22,22,3.743, 0,0,0,22,0,0, 0,553089,0,0,0,0
10:26:51,beikeshuo.com,1447381610,0, 1,0,5767,53, 555021,555021,11, 11,11,0.694, 0,0,0,11,0,0, 0,555021,0,0,0,0
10:26:52,beikeshuo.com,1447381611,0, 1,0,5808,55, 554221,554221,13, 13,13,1.502, 0,0,0,13,0,0, 0,554221,0,0,0,0
10:26:53,beikeshuo.com,1447381612,0, 1,0,5875,45, 547204,547204,8, 8,8,0.464, 0,0,0,8,0,0, 0,547204,0,0,0,0
10:26:54,beikeshuo.com,1447381613,0, 2,1,5948,63, 552687,552688,32, 32,32,2.914, 0,0,0,32,0,0, 0,552687,0,0,0,0
10:26:55,beikeshuo.com,1447381614,0, 1,0,5939,41, 549759,549759,3, 3,3,0.099, 0,0,0,3,0,0, 0,549759,0,0,0,0
10:26:56,beikeshuo.com,1447381615,0, 3,1,6001,53, 554504,554508,15, 15,15,1.480, 2,0,0,13,0,0, 0,554504,0,0,0,0
10:26:57,beikeshuo.com,1447381616,0, 2,0,6066,36, 547311,547312,11, 11,11,1.435, 2,0,0,9,0,0, 0,547311,0,0,0,0
10:26:58,beikeshuo.com,1447381617,0, 2,0,6152,43, 554056,554058,7, 7,7,0.244, 1,0,0,6,0,0, 0,554056,0,0,0,0
```

瞬时攻击**550kqps**

尾声

小结：

DDOS攻击的本质是：利用木桶原理，寻找利用系统应用的瓶颈；阻塞和耗尽；当前问题：用户的带宽或资源小于攻击的规模，噪声访问带宽成为木桶的短板；

一般中小型公司可以尝试解决小流量型ddos，但不建议自行解决大流量DDoS攻击问题；

Cdn防御方案可以有效的隐藏源站，并提供冗余带宽和资源对原有的单一节点进行有力的补充；

专业安全cdn厂商拥有成熟的防御体系和庞大的资源集群能够有效的帮助用户对抗攻击；

Q & A

谢　谢！