云端DDoS攻击防护

百度商业产品部 吴昊挺

wuhaoting@baidu.com

关于我

吴昊挺

百度高级安全工程师

工作内容:

安全相关的后台架构研究

分布式拒绝服务攻击

基于访问数据进行攻击行为分析

微信：754538539

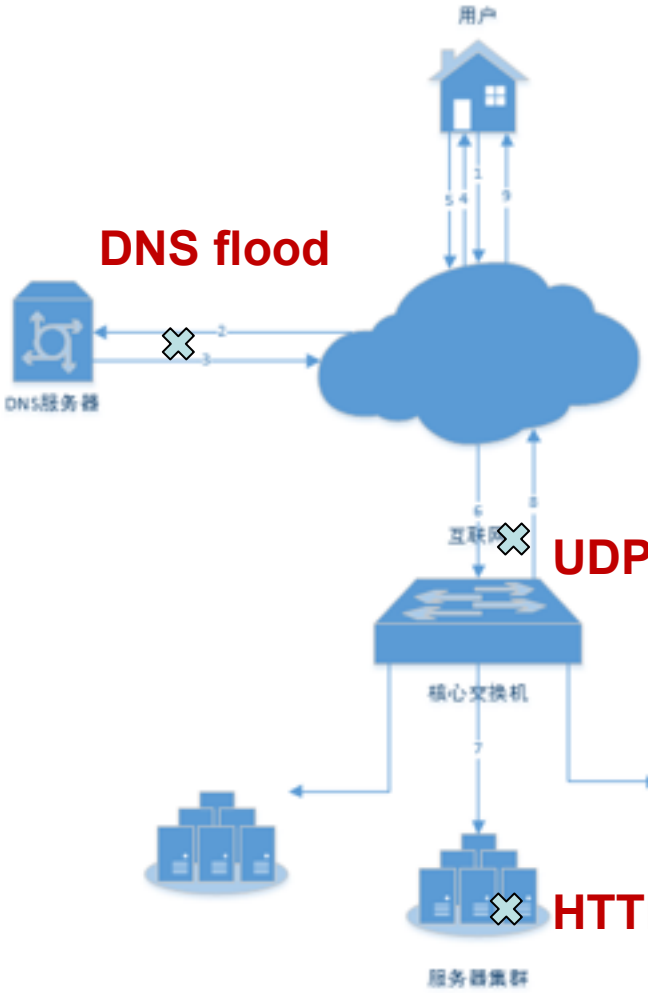
大纲

- DDoS攻击简介
- 传统的攻击防护
- 基于云的攻击防护
- 云加速的攻击防护方案

DDoS攻击是什么？

DDoS Distributed Denial of Service 分布式拒绝服务

DDoS对网站访问的影响



UDP flood、ICMP flood

HTTP flood、SYN flood

大纲

- DDoS攻击简介
- 传统的攻击防护
- 基于云的攻击防护
- 云加速的攻击防护方案

如何防御DDoS攻击

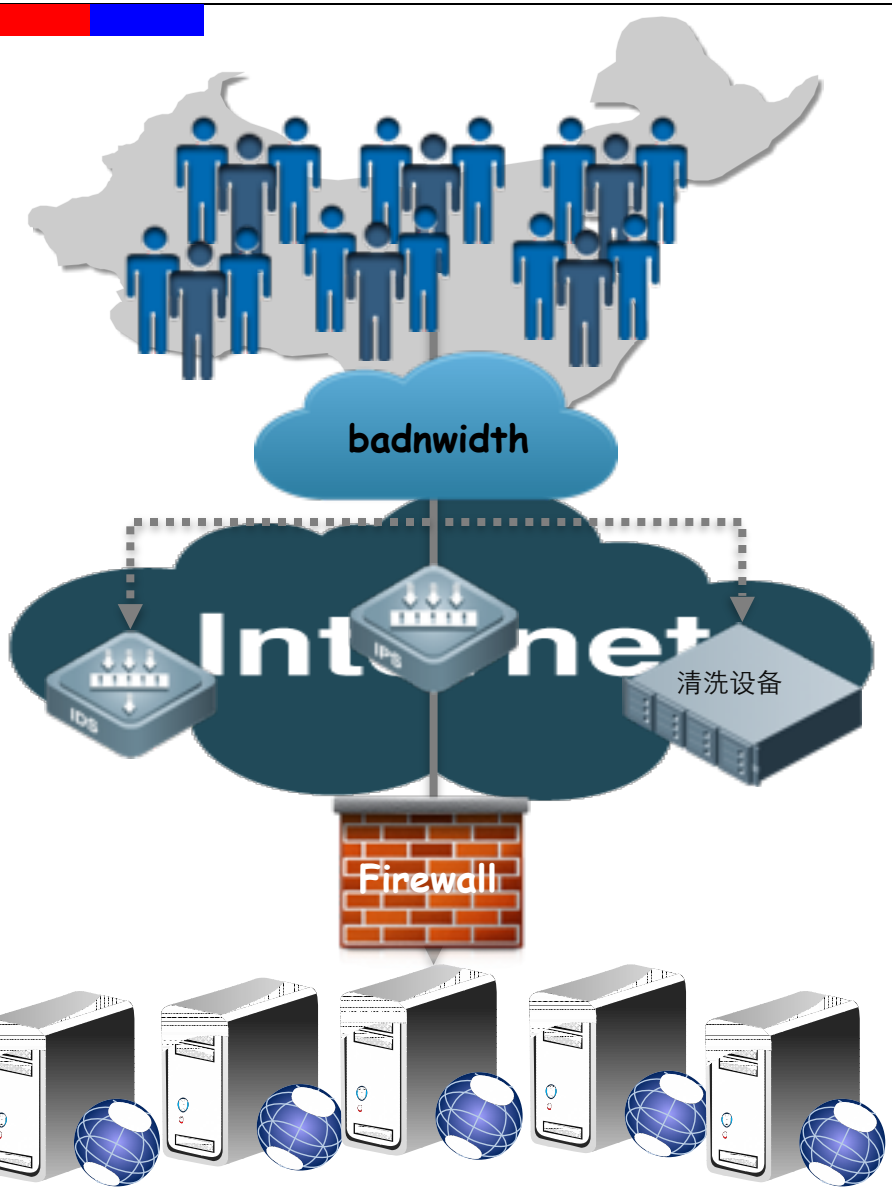
加几台服务器?

加个防火墙?

上台高性能的抗DDoS设备?

再加几G带宽?

传统的防护方案



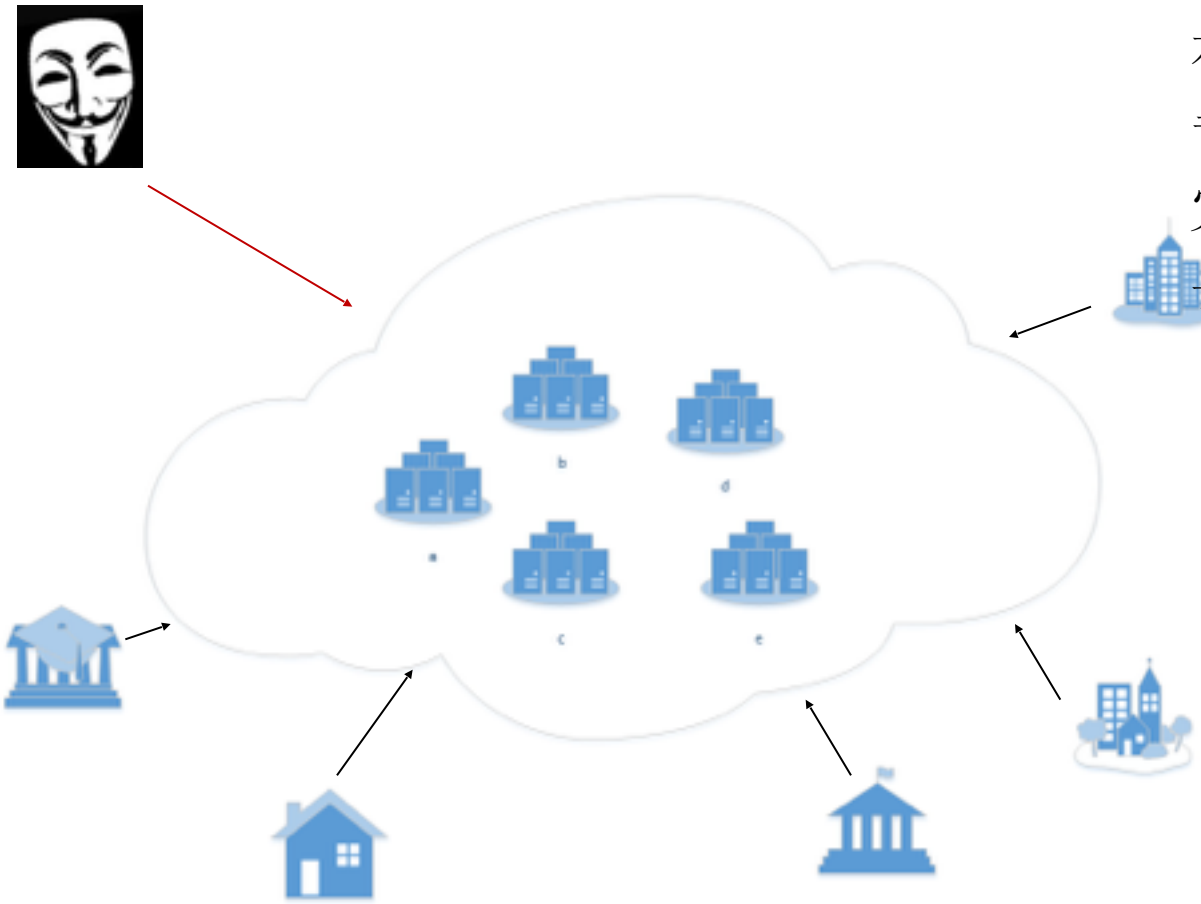
我靠，为什么还是不稳定，不安全！！！

①设备多，可能面临各种问题，需要专业人员维护
②带宽不够，防护设备规则没更新，攻击DNS更没辙
总之啥都需要钱

大纲

- DDoS攻击简介
- 传统的攻击防护
- 基于云的攻击防护
- 云加速的攻击防护方案

云端服务的优势



本地防御->云端防御

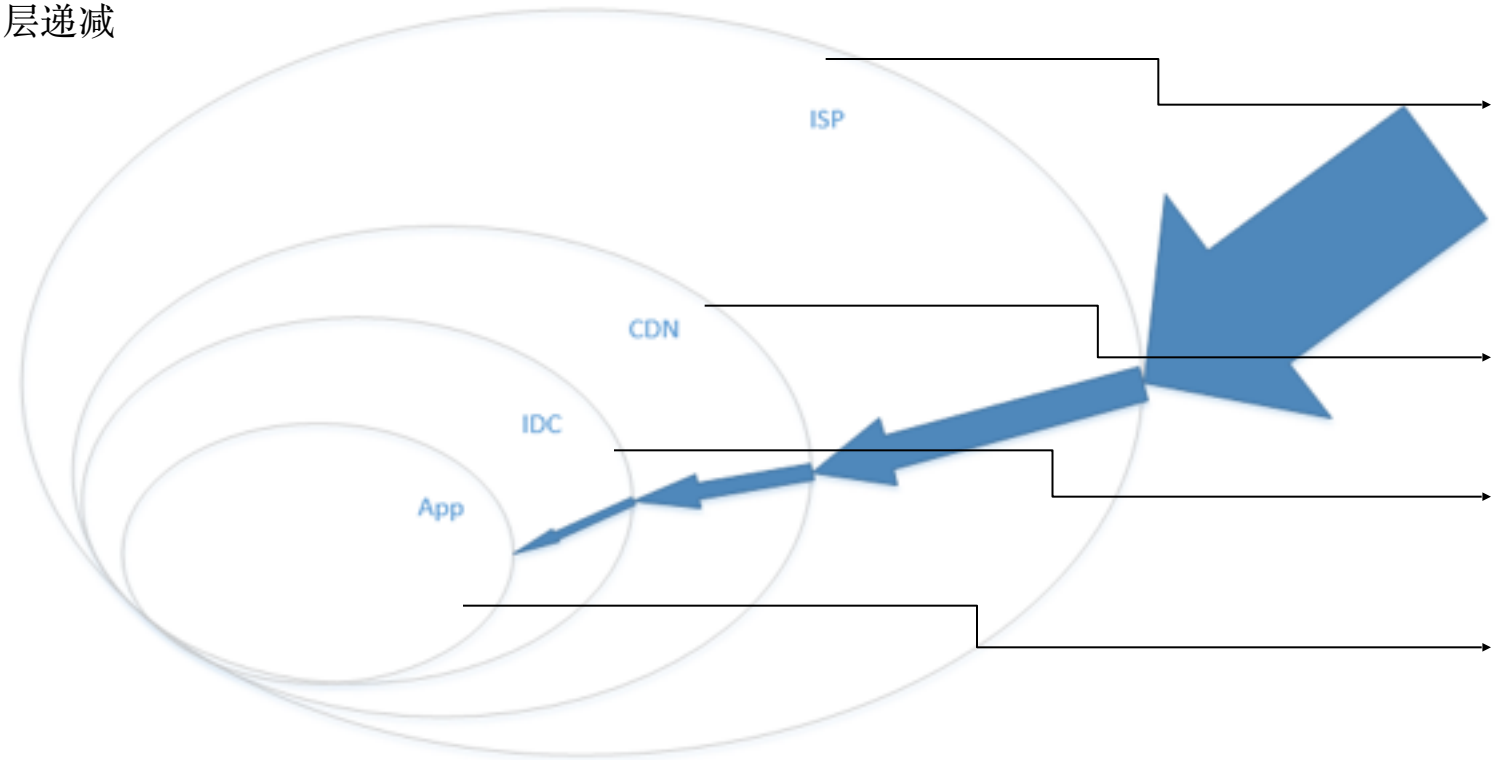
专人维护->托管

冗余采购->弹性收费

长期演进->直接上线

DDoS层级防护

攻击流量层层递减



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，利用云服务商的冗余带宽清洗攻击

IDC内清洗，配置专业防护设备

App进行精细化防护

Baidu 百度

大纲

- DDoS攻击简介
- 传统的攻击防护
- 基于云的攻击防护
- 云加速的攻击防护方案

云端防护的难点

攻击目标多、流量大?

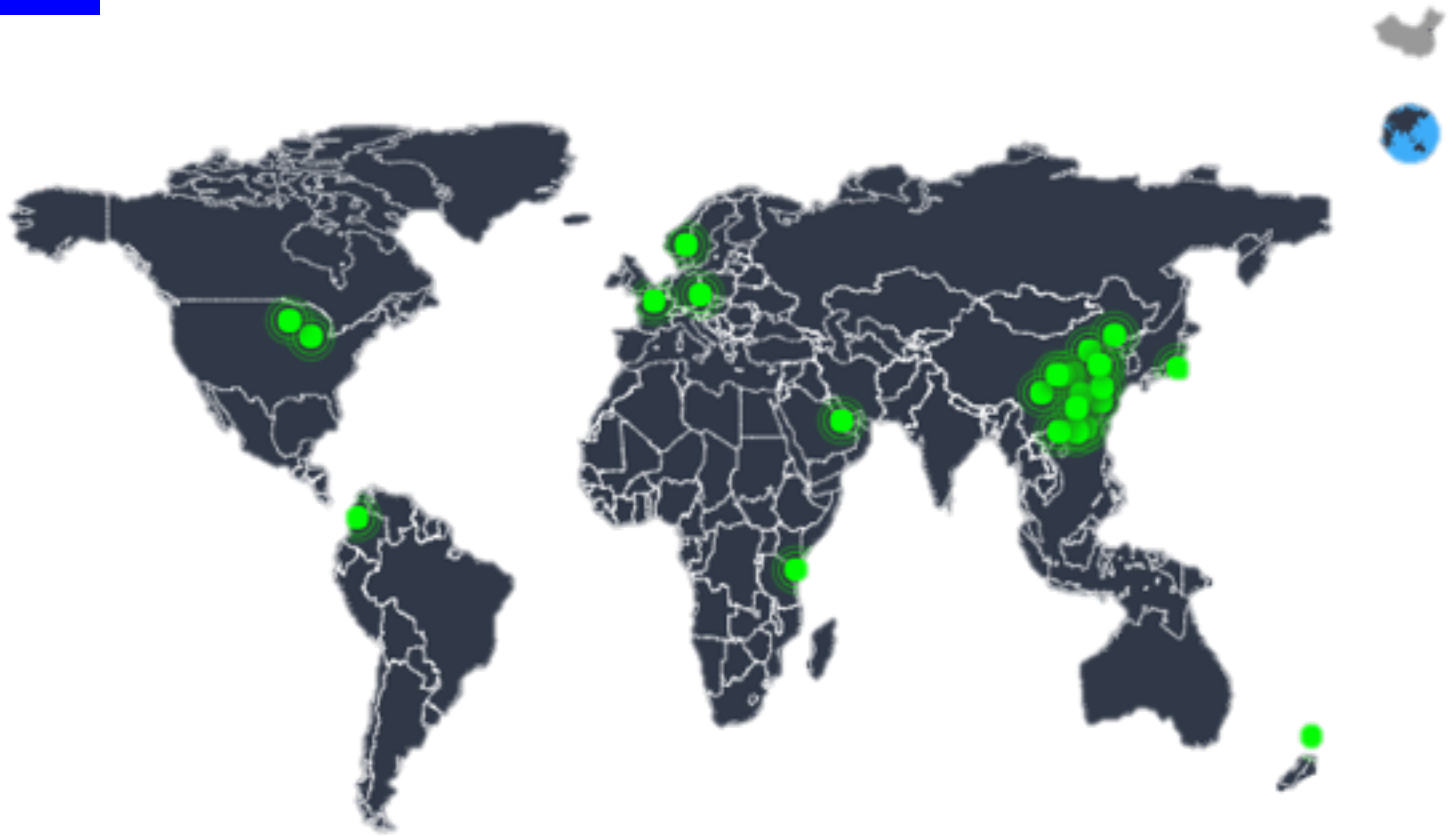
攻击点分散?

混合型攻击难发现?

流量迁移不及时?

自主防御都很困难，怎么做云防护?

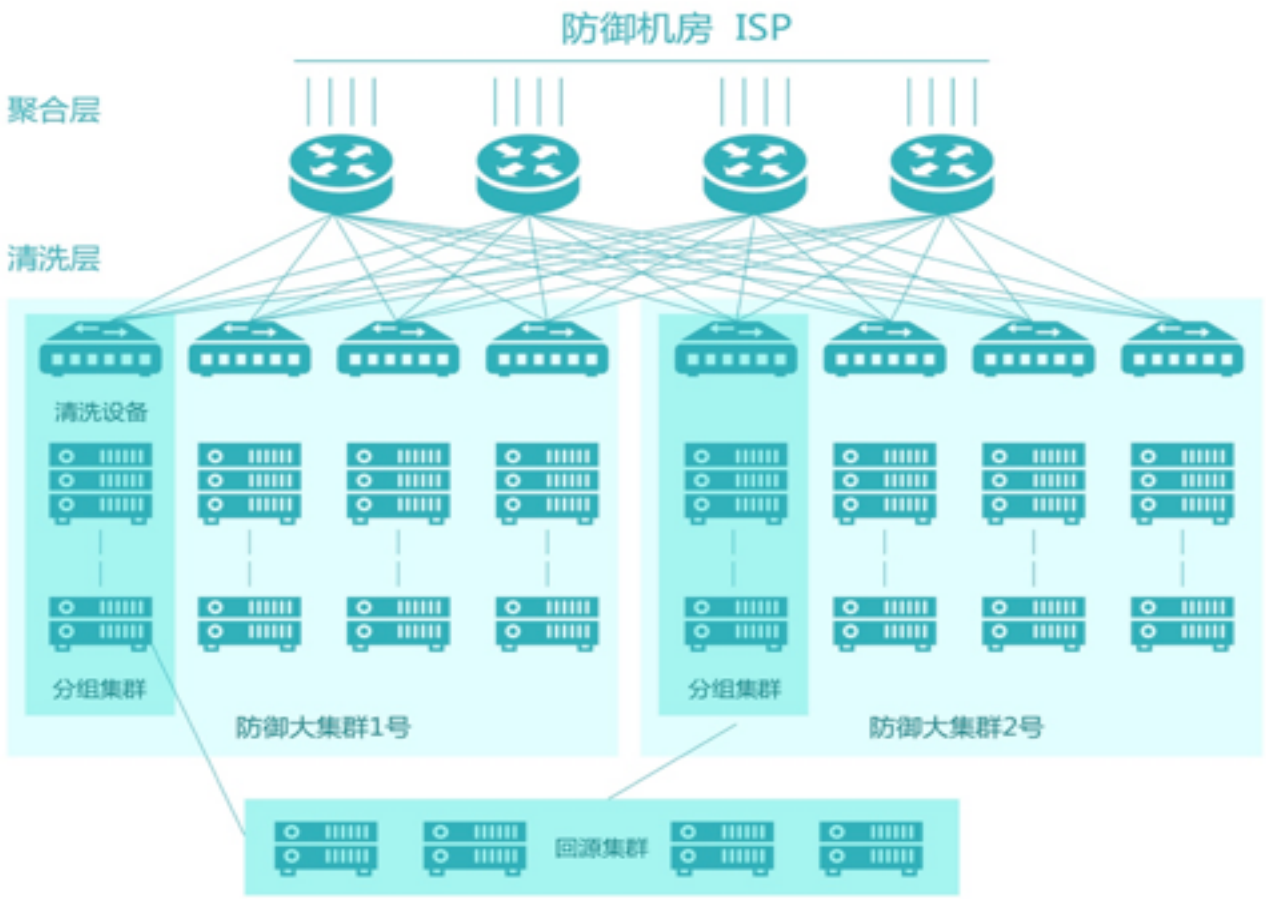
攻击目标多、流量大--机房建设



全球自建网络节点保障加速能力，重点地区加大带宽，对抗流量攻击；

云上用户越多，云服务商能力越强；

混合攻击防御--智能防御集群

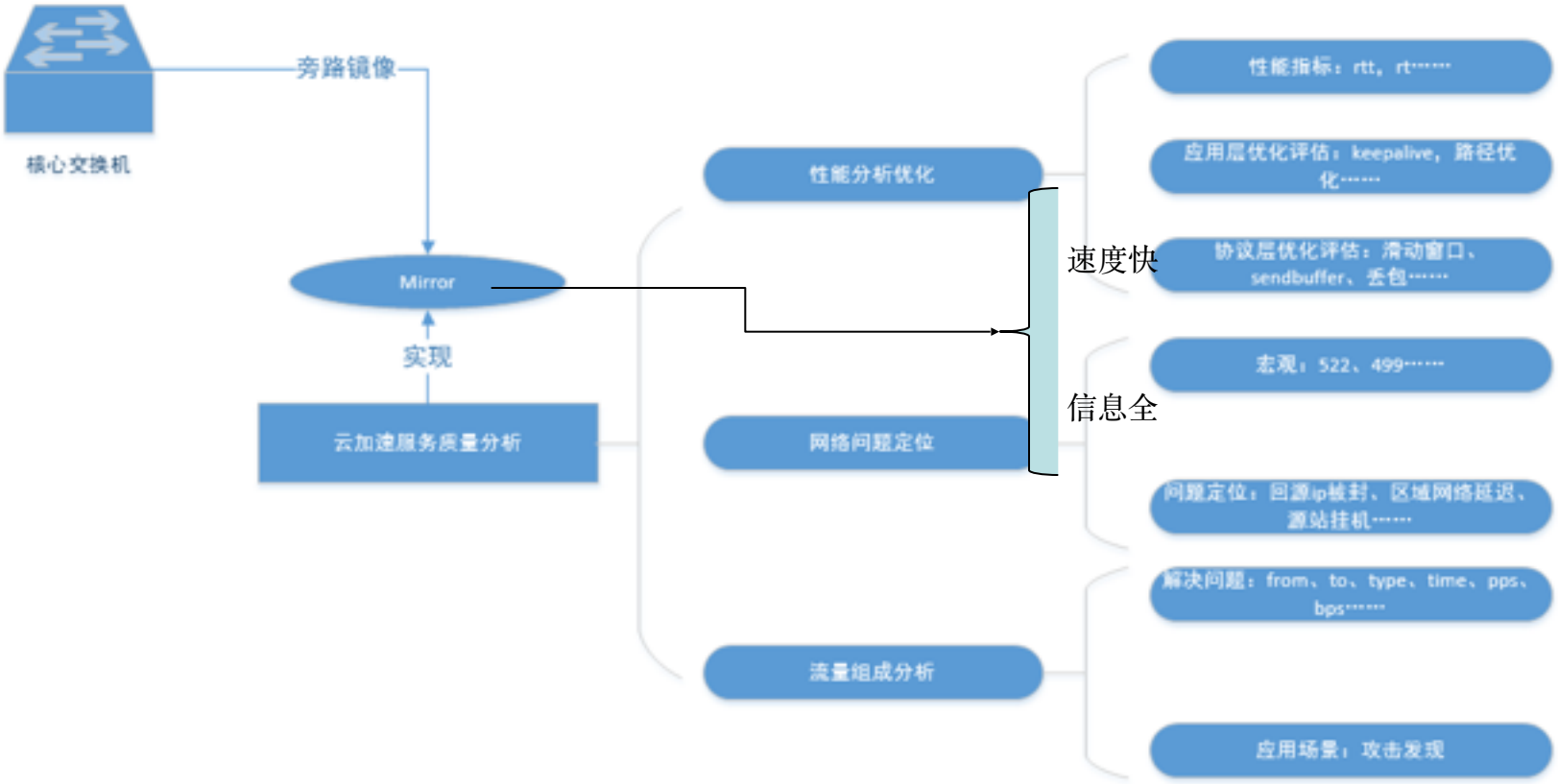


重点防御设备全自研，满足业务定制需求

深入定制**7**层代理软件**nginx**，优化加速效果及防御效果

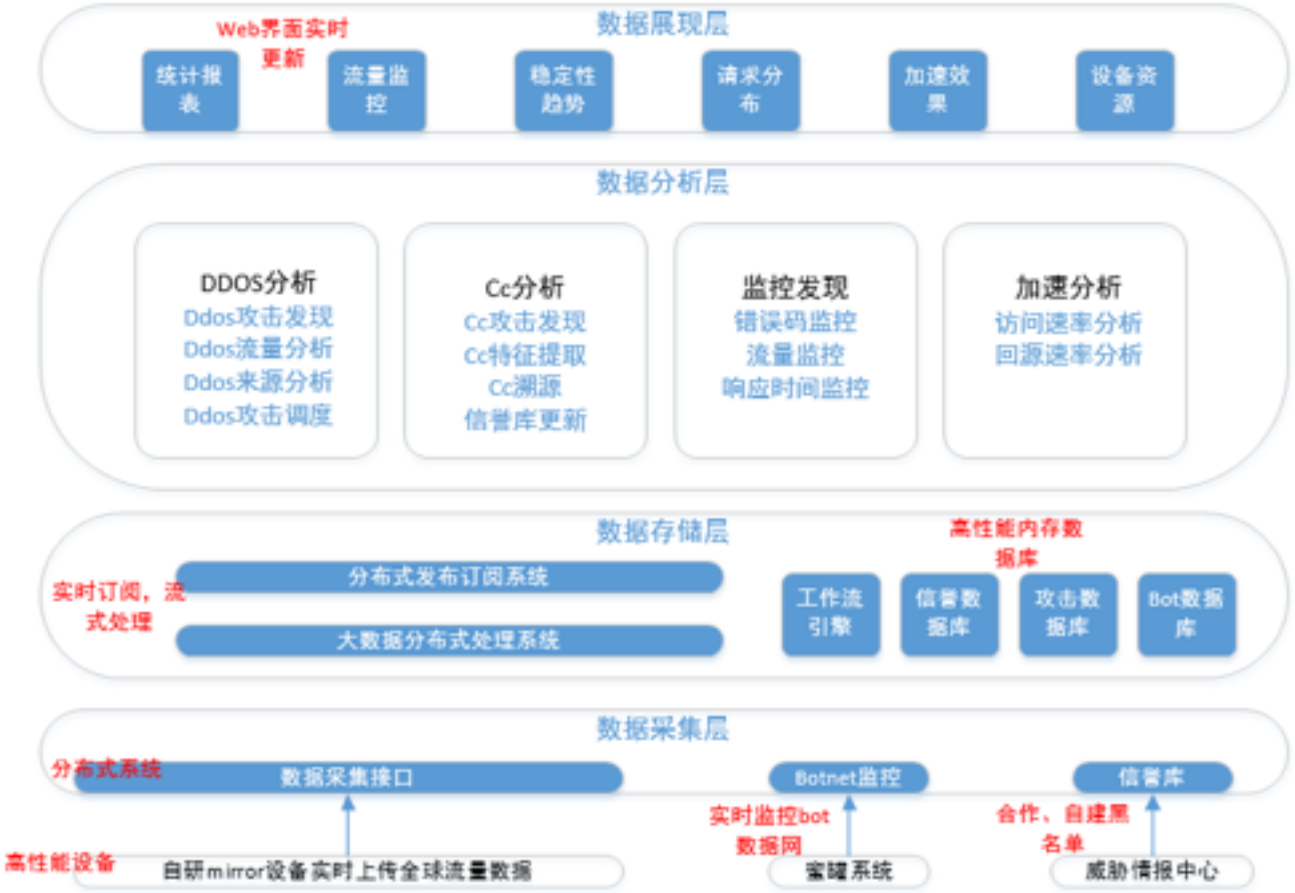
Baidu 百度

攻击点分散--实时监控



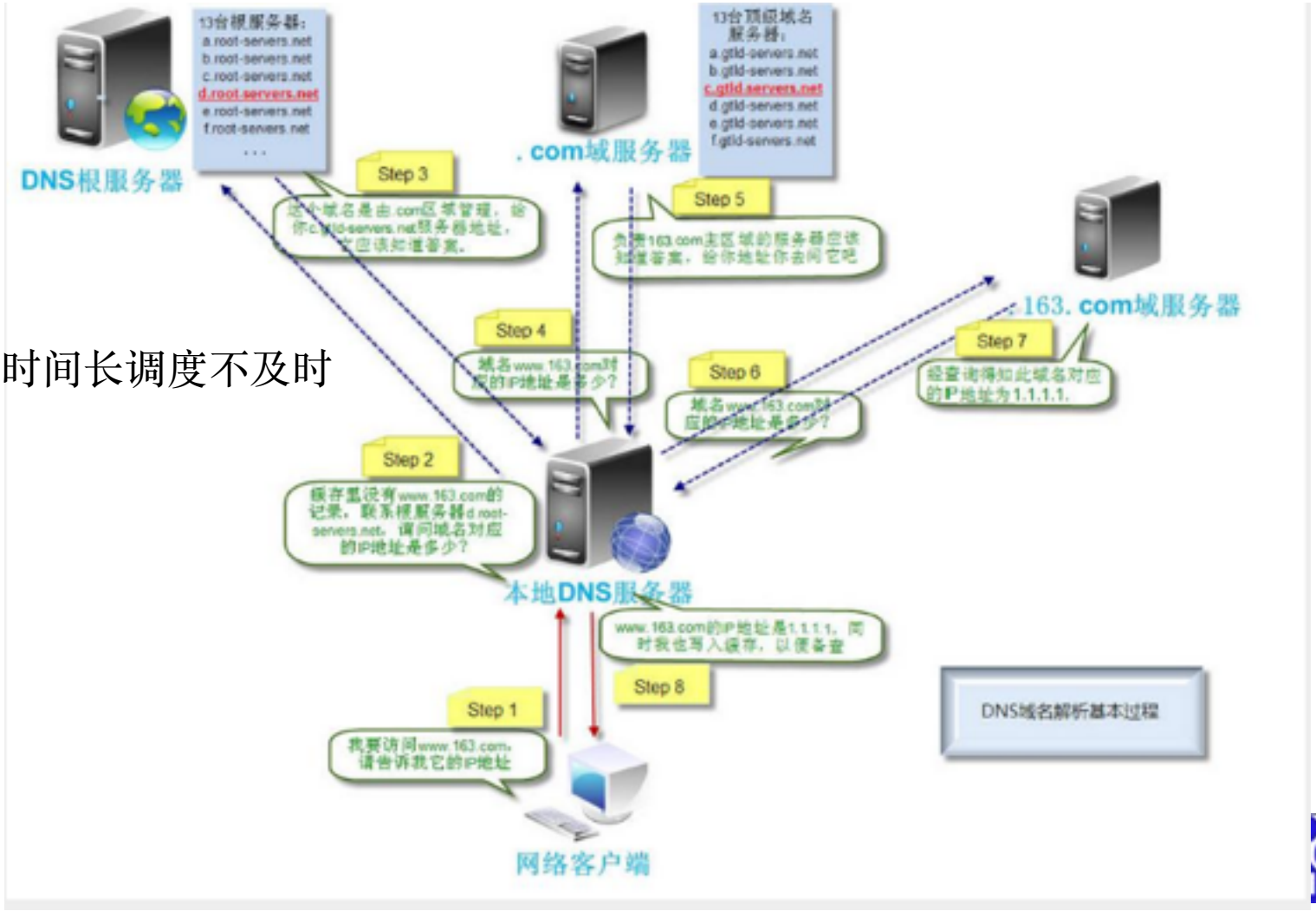
全流量监控替代传统的流量采样；

攻击点分散--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

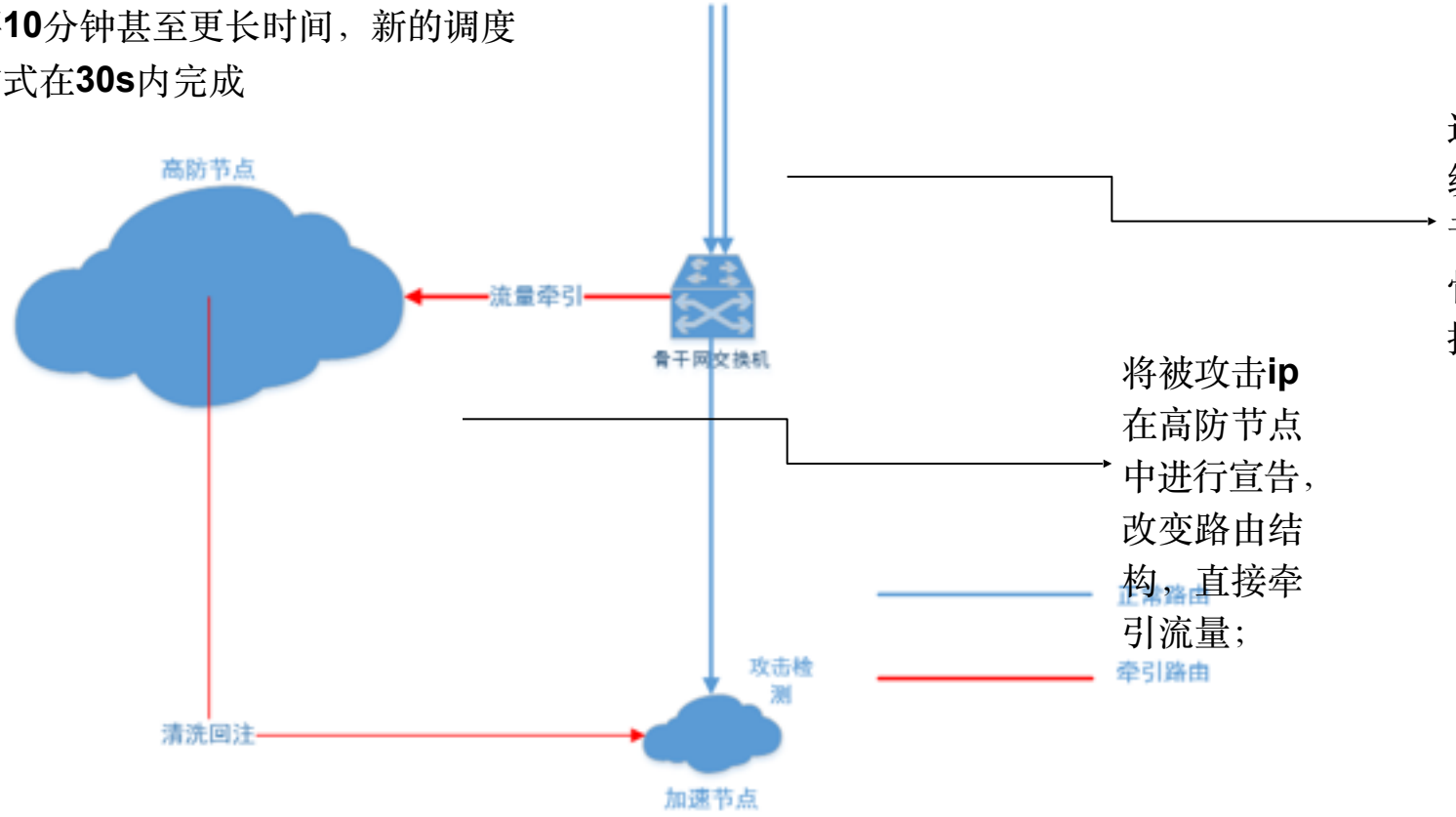
调度不及时--dns调度

缓存时间长调度不及时



调度不及时--路由调度

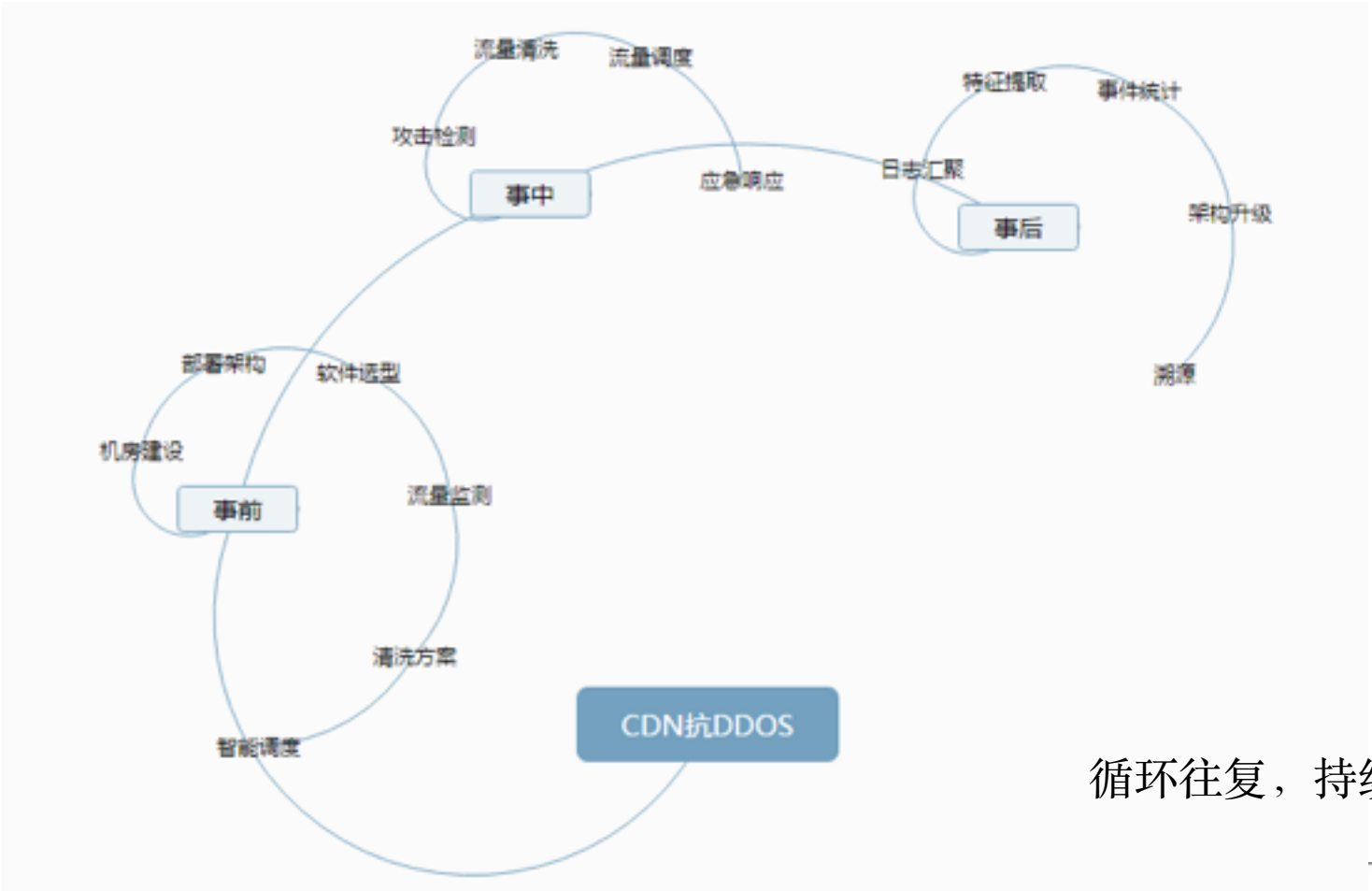
传统的基于**dns**调度流量的方式需要**10**分钟甚至更长时间，新的调度方式在**30s**内完成



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；

攻击防护体系

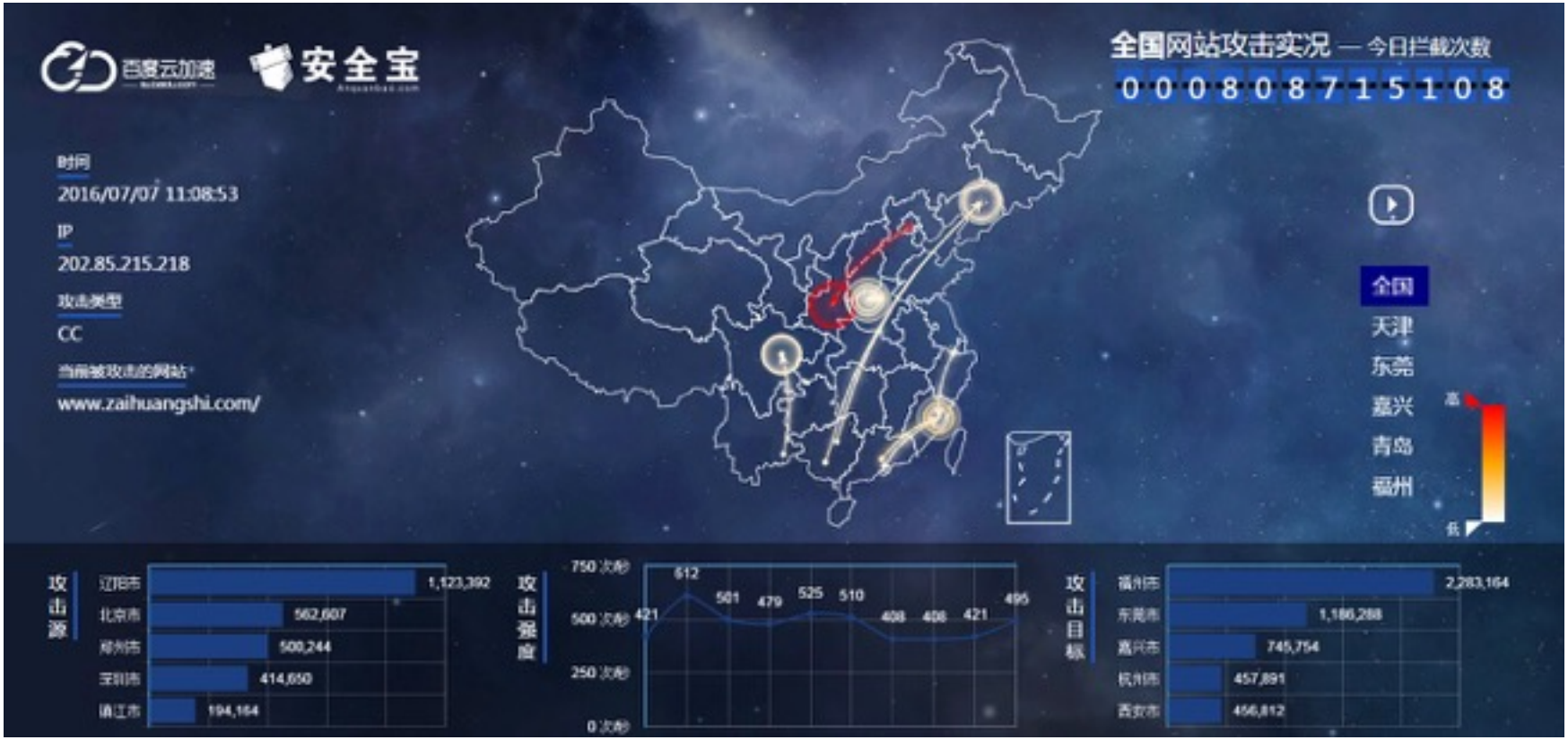


循环往复，持续进化；

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	[redacted]
2	2015年6月20日	23:47:10	213.20	[redacted]
3	2015年7月15日	16:49:33	233.40	[redacted].com
4	2015年7月16日	14:32:45	205.11	[redacted].com
5	2015年7月16日	14:36:30	225.41	[redacted].com
6	2015年7月16日	15:21:11	247.98	[redacted].com
7	2015年7月27日	11:11:14	227.83	[redacted].com
8	2015年8月2日	10:17:52	222.80	[redacted].com
9	2015年8月6日	11:45:43	197.99	[redacted].com
10	2015年8月7日	12:00:37	186.99	[redacted].com
11	2015年8月7日	12:17:42	210.69	[redacted].com

攻击案例


百度云加速
安全宝
全国网站攻击实况 — 今日拦截次数
0 0 0 8 0 8 7 1 5 1 0 8
时间
2016/07/07 11:08:53
IP
202.85.215.218
攻击类型
CC
当前被攻击的网站
www.zaihuangshi.com/
全国
天津
东莞
嘉兴
青岛
福州
高
低
攻击源
辽阳市 1,123,392
北京市 562,607
郑州市 500,244
宝鸡市 414,650
镇江市 194,164
攻击强度
750 次/秒
500 次/秒
250 次/秒
0 次/秒
421 612 501 479 525 510 408 408 421 495
攻击目标
福州市 2,283,164
东莞市 1,186,288
嘉兴市 745,754
杭州市 457,891
西安市 456,812

END

谢　谢!