演讲标题： DDoS攻击下的DNS

演讲人：张鹏

中国互联网络信息中心（CNNIC）高级产品经理

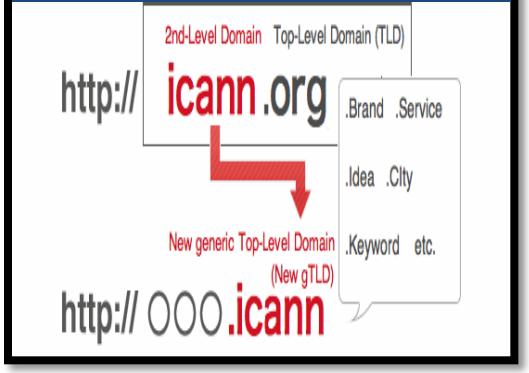
日期：2014.9

DNS

All IP/IPv6

基于IP的应用和IPv6极大扩展了DNS的**覆盖范围**

New gTLD



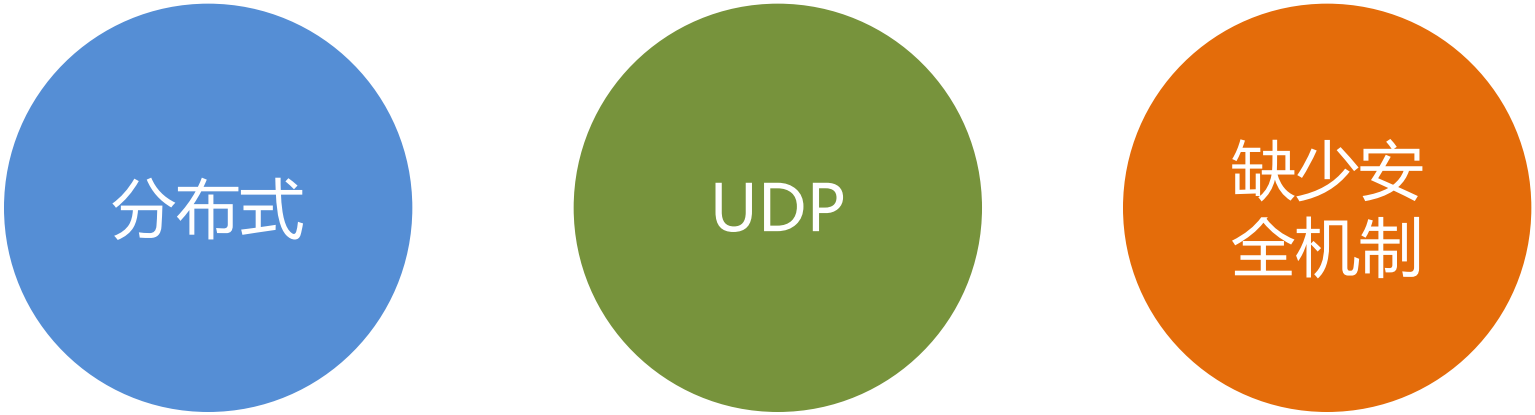
NewG推动域名成百倍增长DNS的**解析量倍增**

移动互联网

移动互联网日益丰富的应用成倍扩展了DNS的**应用范围**

互联网发展对DNS的依赖日益增加

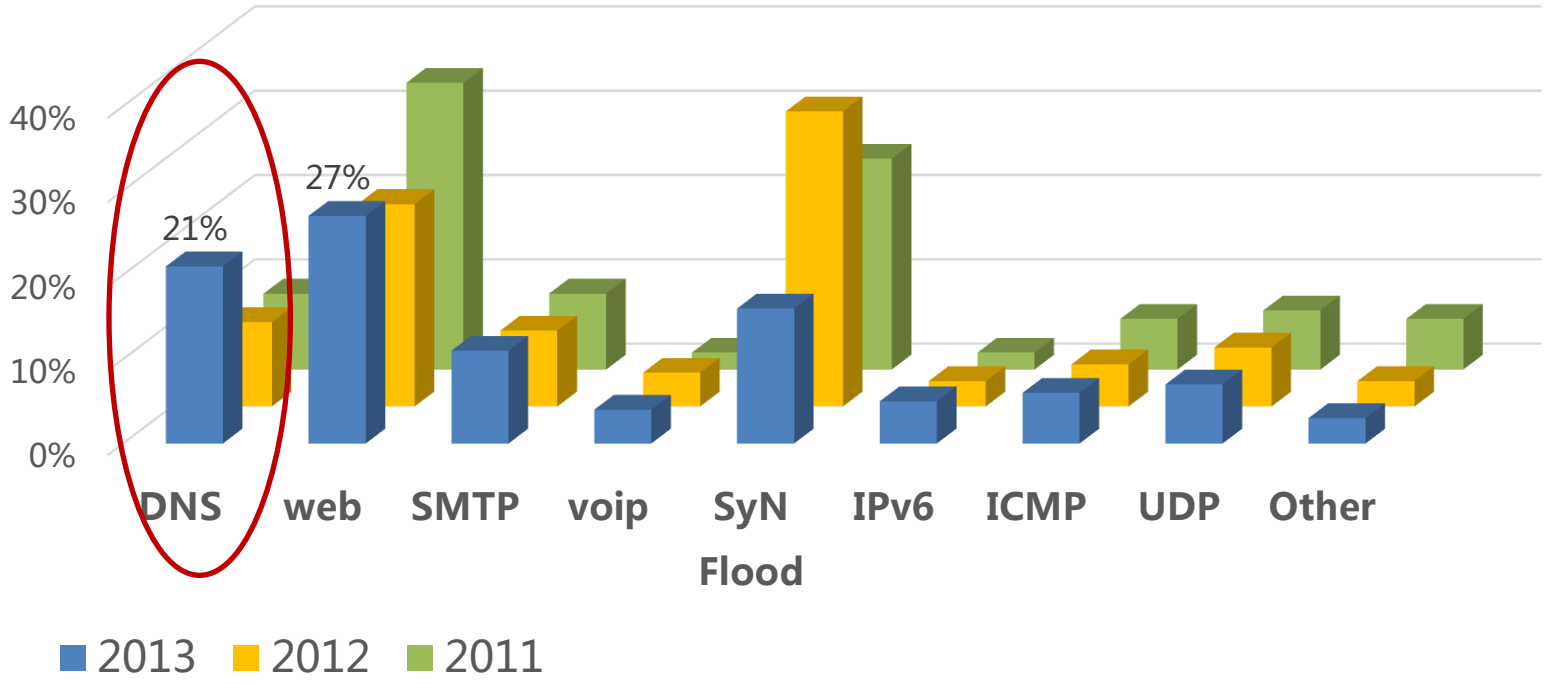
DNS的特点



DDoS攻击

DDoS攻击逐渐成为主要攻击方式

DNS成为攻击的主要类型



Radware global Application & network security report

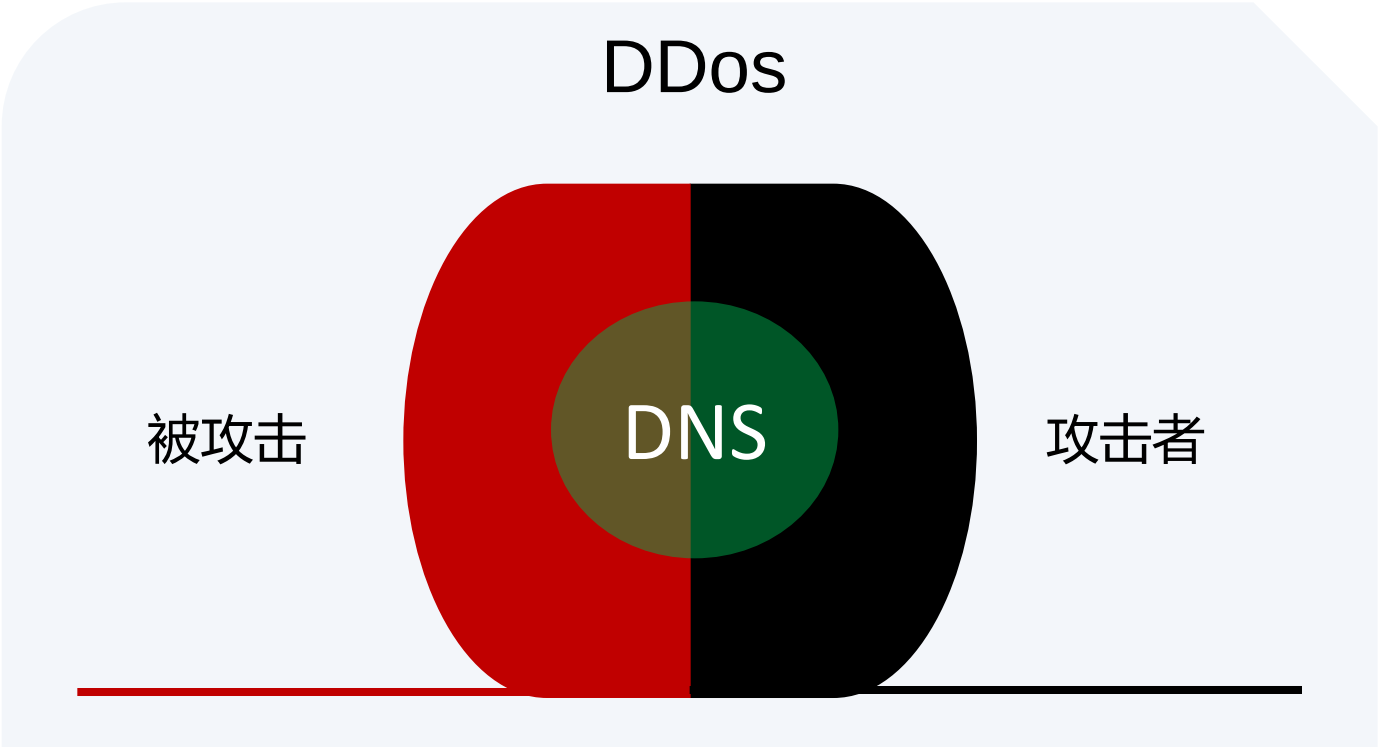
为什么是DNS？

1 基础设施

2 流量放大

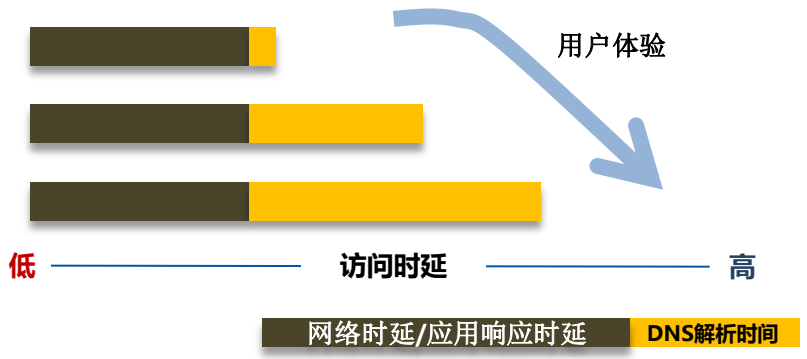
3 匿名

DDoS攻击中的DNS



DNS对互联网的影响

DNS解析时间的影响



•**DNS解析时长增加**会明显降低互联网用户体验。

DNS故障的影响

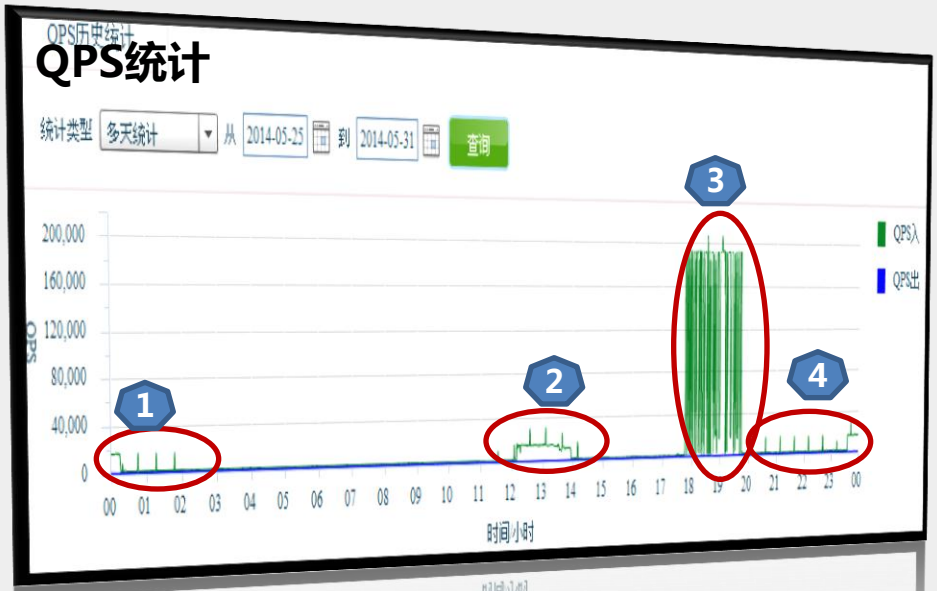
时间	受攻击目标	结果	影响范围	影响方式
2002.10	DNS根服务器	根服务器不可用	全球	全球互联网中断数小时
2006.09	新网DNS	DNS 宕机	中国	大于200,000网站无法访问
2009.05	Dnspod	DNS性能下降	中国	5省断网 23省网络变慢
2012.08	ATNT	DNS不可用	美国	百万商业用户网站无法访问
2012.09	GoDaddy	DNS不可用	美国	几百万网站无法访问

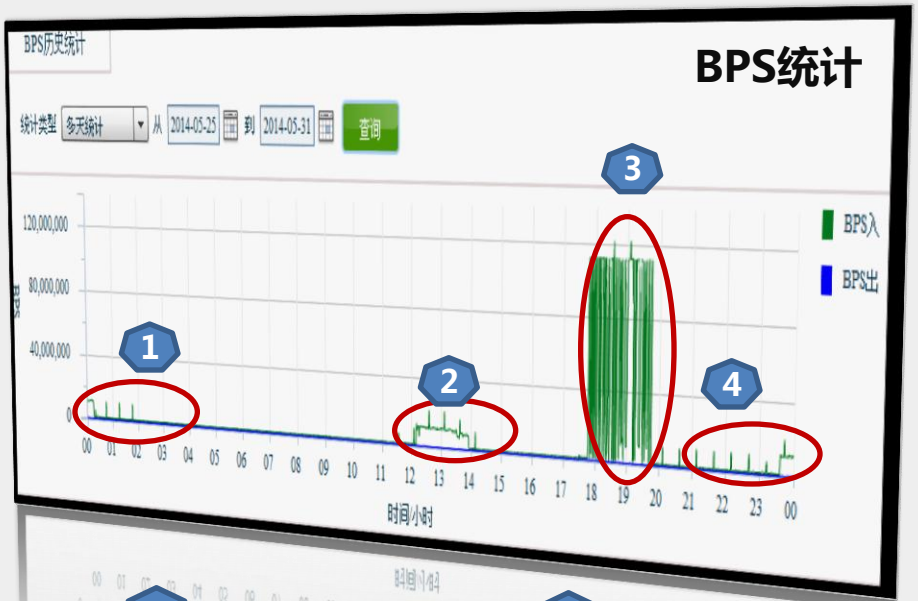
•DNS故障**易于感知影响范围大**

DNS遭受频繁的攻击

正常解析： 400QPS，400Kbps

2014.5.25 ~ 2014.5.31 按时间段统计的DNS流量状态





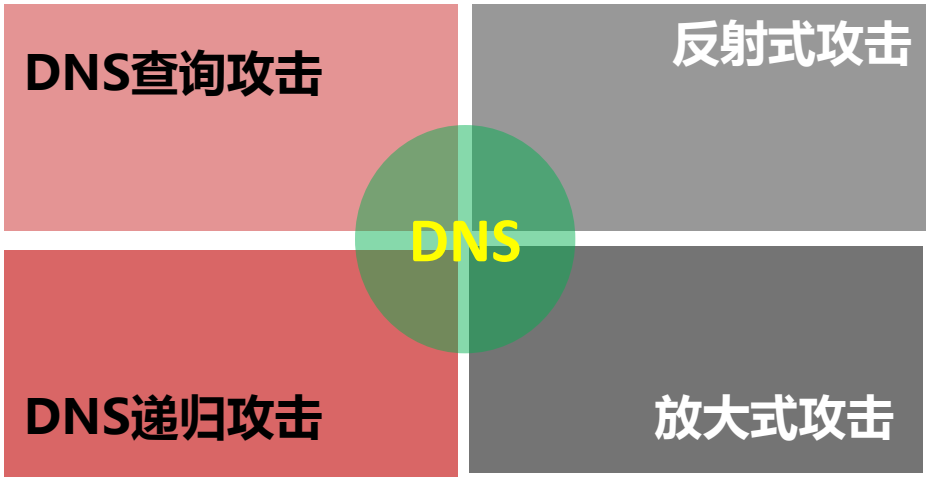
1 时间：5.26/5.29
75Mbps，10万QPS

2 时间：5.30
71M， 11.1万QPS

3 时间：5.31
779Mbps，133.2万QPS

4 时间：5.28
81Mbps，11.1万QPS

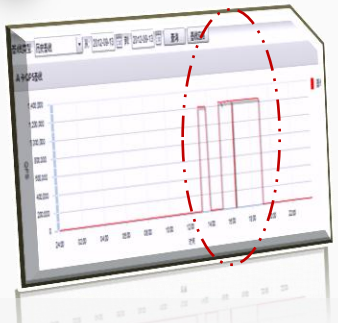
针对DNS的DDoS攻击



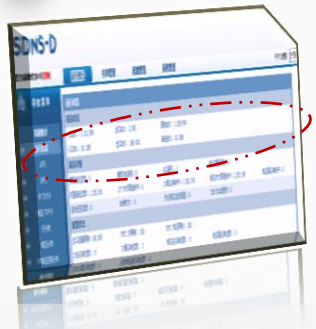
DNS抵御DDoS

使用**专用**DDoS防护设备提高DNS的安全性

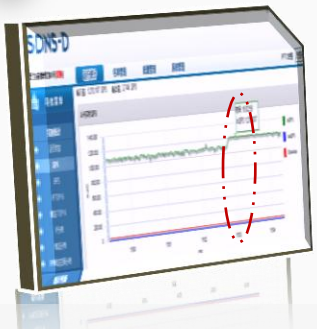
1 识别攻击



2 准确清洗



3 正常服务

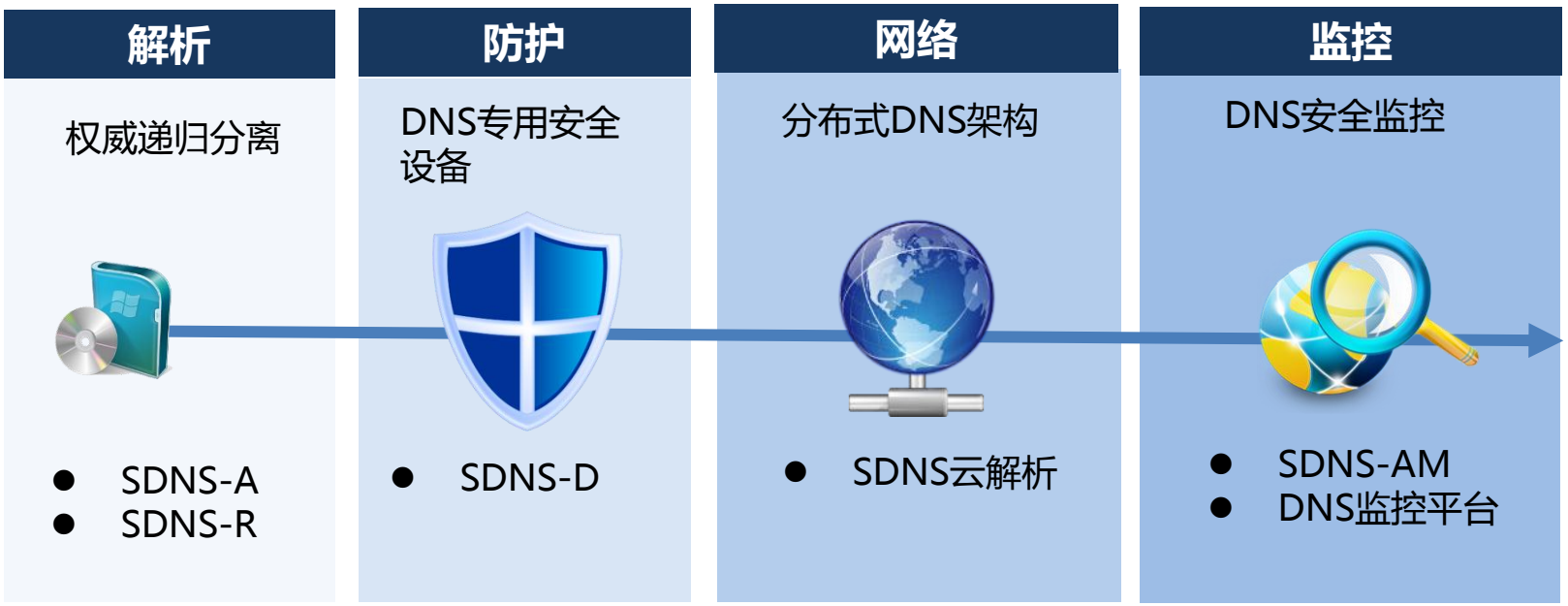


1212.6Kqps(输入) > **1209.9Kqps** (清洗) > **2.7Kqps** (正常请求)

聚焦**DNS** | 抵御**DDoS** | 专用**硬件** | **自动**学习**准确**清洗

构建全方位的DNS体系

CNNIC的SDNS解决方案全方位提高DNS系统的安全性



Thanks!