

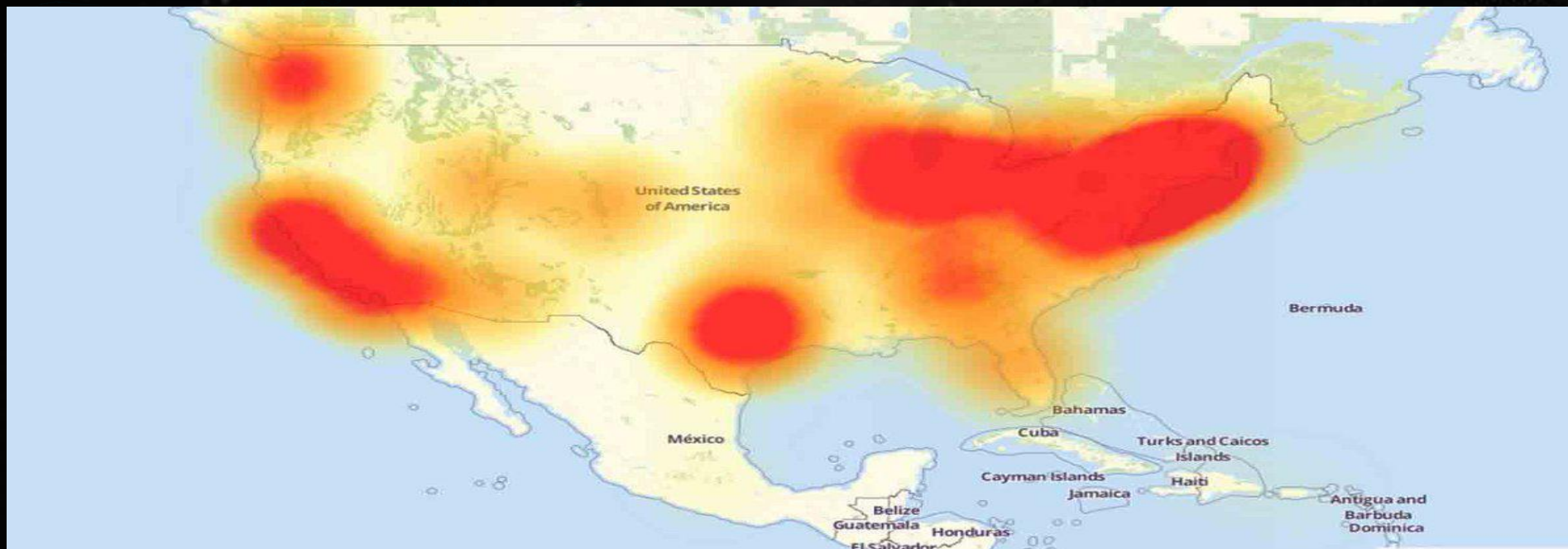
REEBUF

2017深圳站

FREETALK

基于Ai学习的DNS防御

- 美国遭遇史上最严重DNS DDoS攻击  
—— DNS安全再次引发关注



2016年10月，美国最主要的 DNS 服务商 Dyn 遭遇大规模 DDoS 攻击，导致 Twitter、Spotify、Netflix、AirBnb、CNN、华尔街日报等数百家网站无法访问。媒体将此次攻击称作是“史上最严重 DDoS 攻击”。值得注意的是，此次网络攻击中，黑客利用了大量的物联网设备。

物联网设备的问题在于，它们常常无法安装安全软件。“你不能在婴儿监控器上安装防火墙，因为它没有足够的存储空间。”



## Dns攻击从未远离

# FREETALK

### 2017 深圳站

09年5月19日

游戏私服私斗打挂dnspod，殃及暴风影音域名解析，进一步殃及电信运营商本地DNS服务器，从而爆发六省大规模断网事故

11年9月5日

微软、宏碁、沃达丰和UPS在内的众多知名网站都遭遇了DNS劫持

13年8月25日

cn域dns受到DDoS攻击而导致所有cn域名无法解析

15年11月30日

13个根服务器大都受到了攻击，攻击者对根服务器发起了针对两个特定域名的数十亿次无效查询请求

2010年1月12日

baidu.com的NS记录被伊朗网军（Iranian Cyber Army）劫持，然后导致www.baidu.com无法访问

12年2月16日

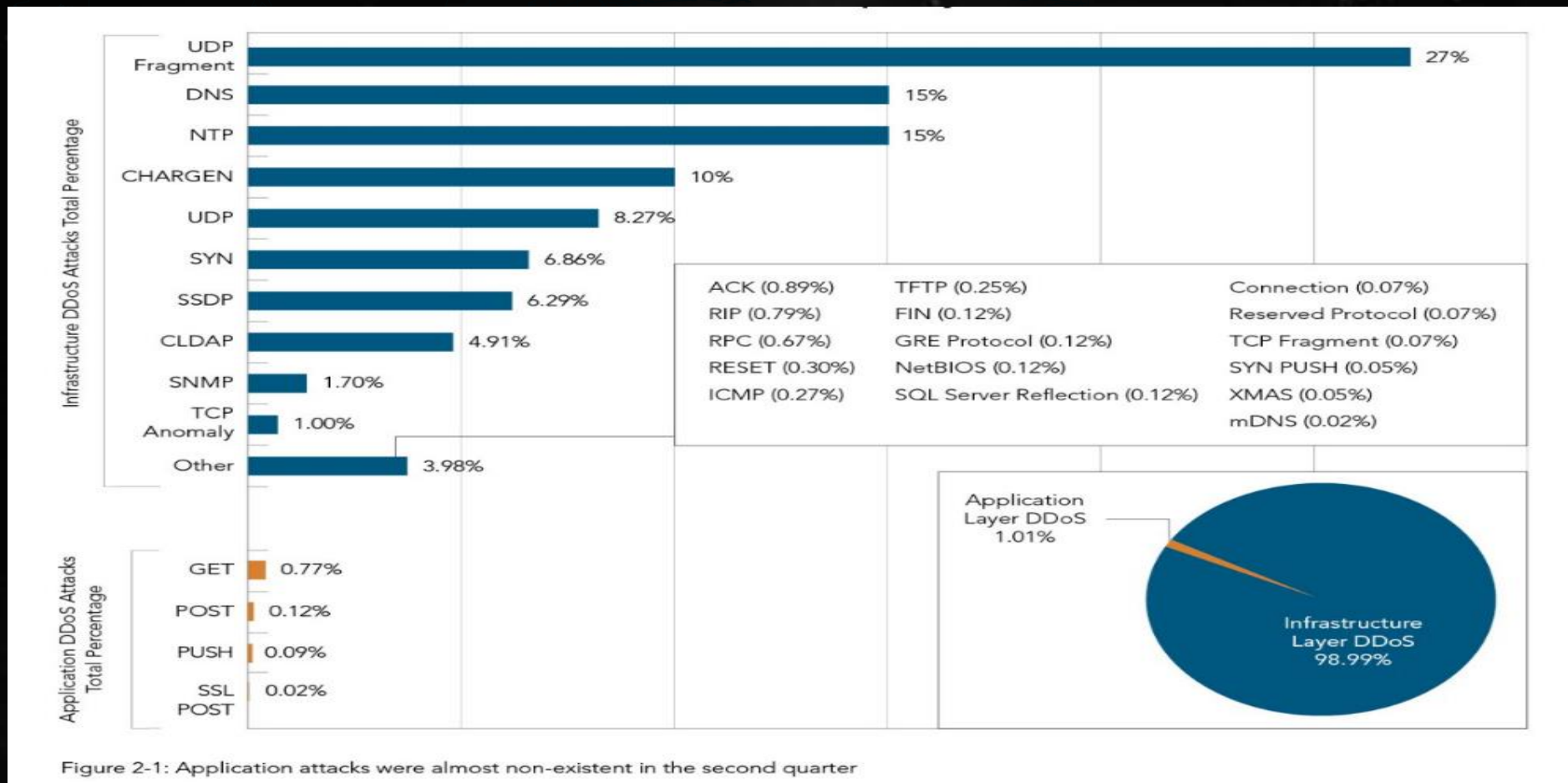
匿名者（Anonymous）对外宣称，将在3月31日攻击DNS的13个根服务器，以达到让全球互联网瘫痪的目的

14年1月21日

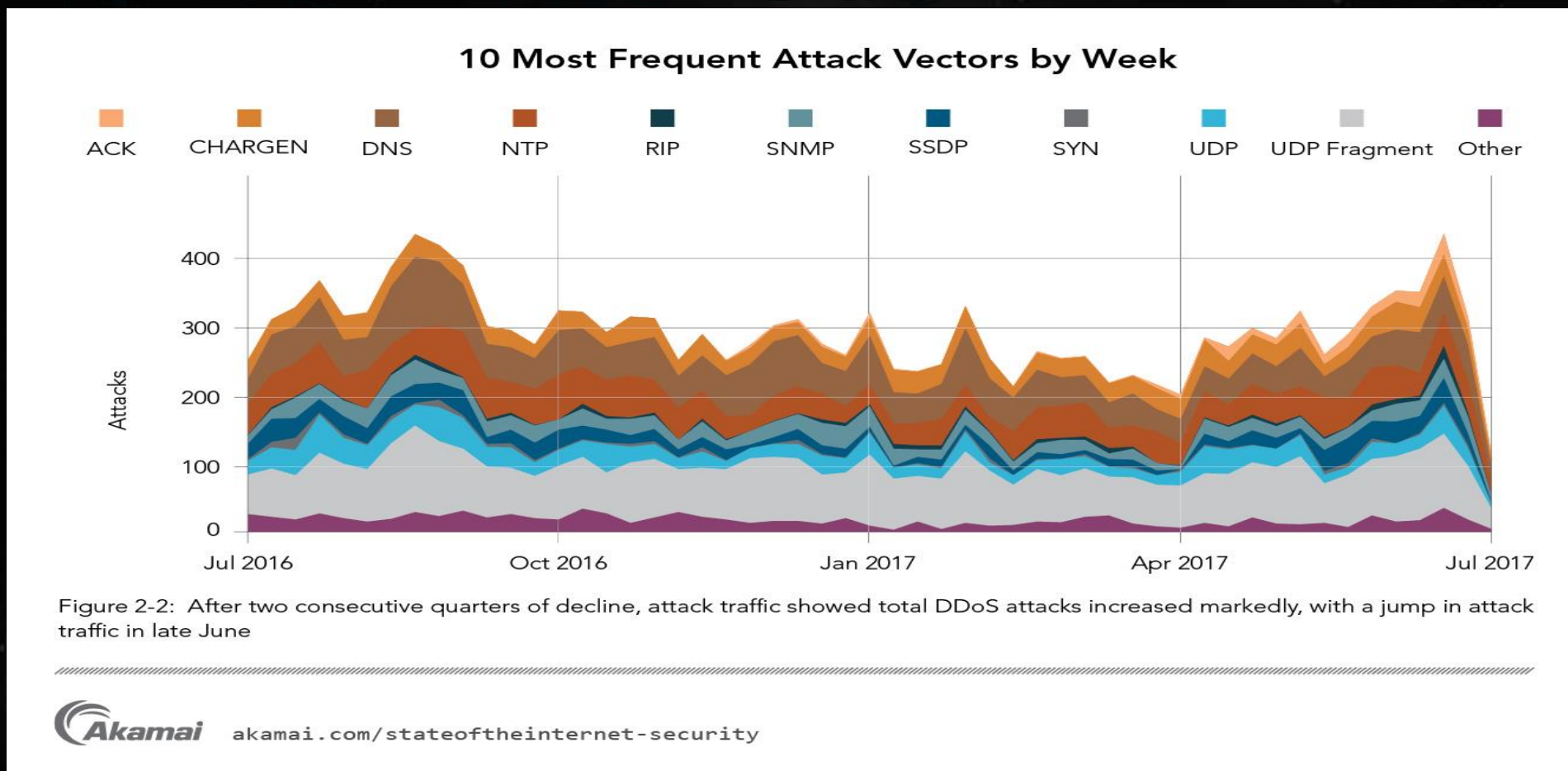
迄今为止，大陆境内发生的最为严重的DNS故障，所有通用顶级域（com/net/org）遭到DNS污染

15年12月14日

土耳其国家域遭攻击。黑客组织匿名者（Anonymous）宣布自己是40Gbps DDoS的网络攻击发起人，并表示该攻击跟反ISIS行动相关



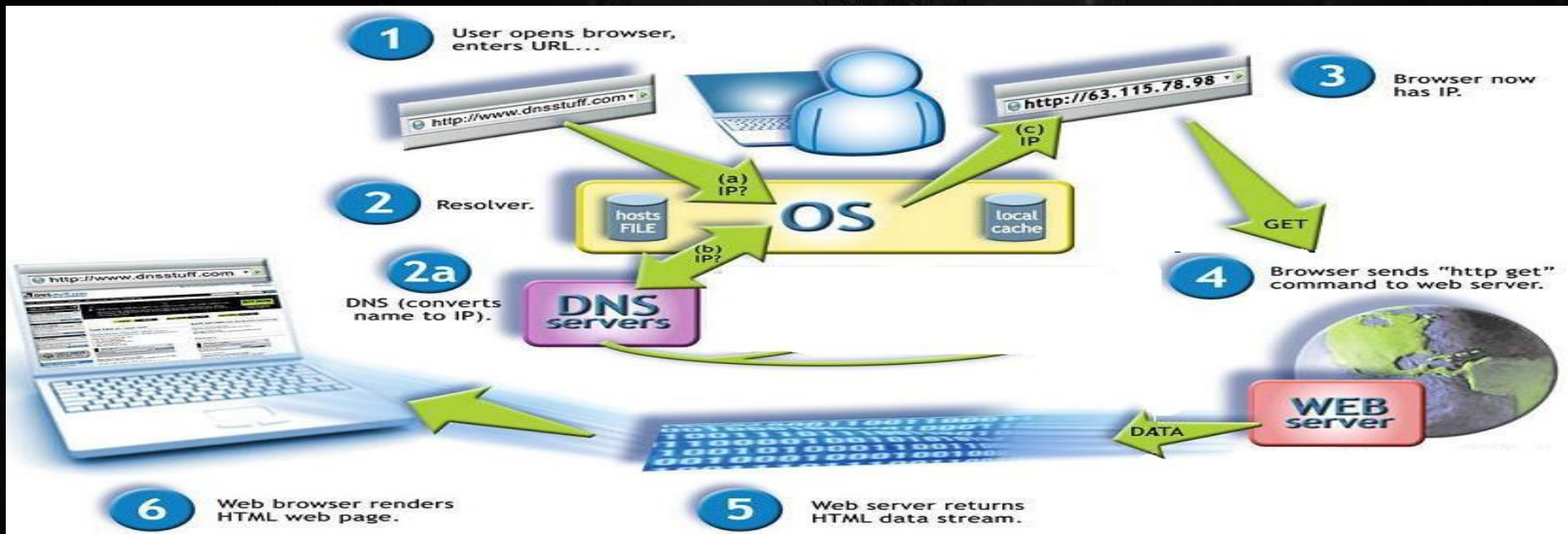




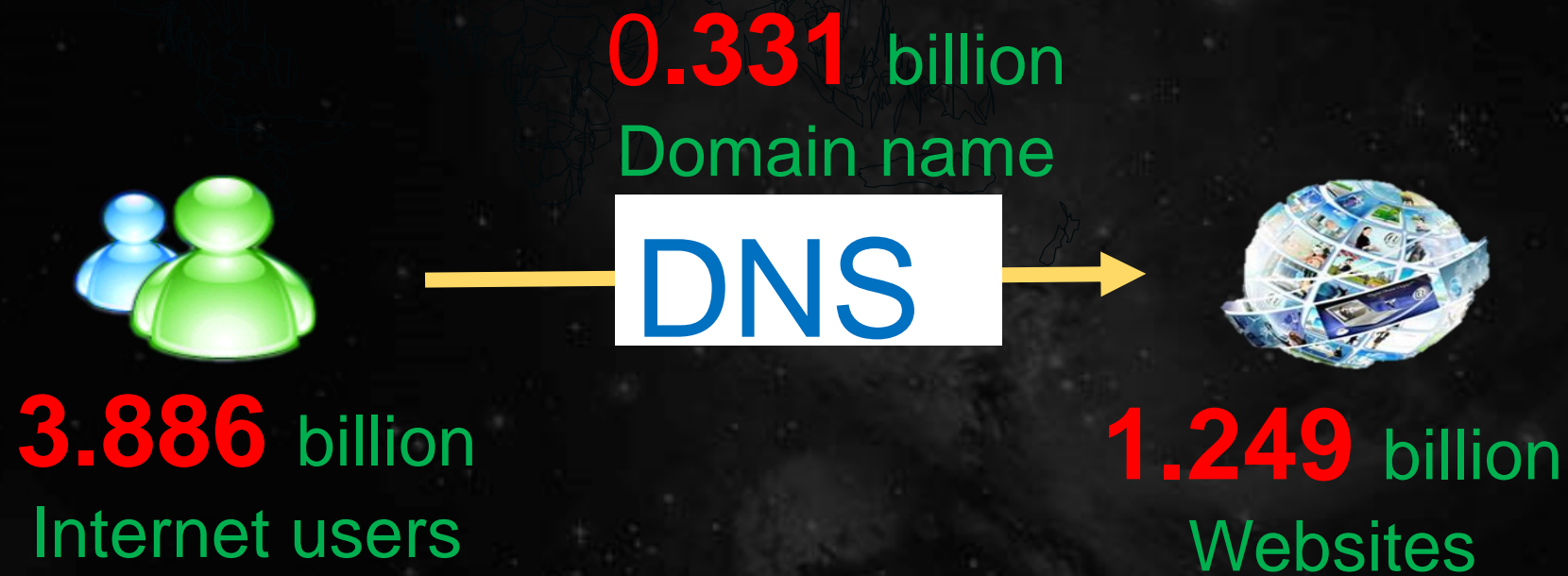
## ● DNS (域名系统) —— 维基百科定义

2017 深圳站

网域名称系统（[英文](#)：Domain Name System，[缩写](#)：DNS）是[互联网](#)的一项服务。它作为将[域名](#)和[IP地址](#)相互[映射](#)的一个[分布式数据库](#)，能够使人更方便地访问[互联网](#)。DNS使用[TCP](#)和[UDP端口53](#)。DNS查询有两种方式：递归和迭代。DNS客户端使用的DNS服务器一般都是递归服务器，它负责全权处理客户端的DNS查询请求，直到返回最终结果。而DNS服务器之间一般采用迭代查询方式。



- DNS (域名系统) —— 互联网框架



## ● DNS体系架构的特点

### 开放性

1

- 1) 是[互联网](#)的一项基本服务
- 2) 通常采用UDP协议使用53端口
- 3) 服务提供者对请求者无限制

### 高效性

2

- 1) 通常采用UDP协议使用53端口
- 2) 通常没有任何认证
- 3) 一个报文即可完成服务

### 分布性

3

- 1) 架构是一个[分布式数据库](#)
- 2) 通常需要cache服务器提供
- 3) 采用递归和迭代的方式查询



### ● DNS请求和响应报文

Num	Source Address	Dest Address	Summary
1	145.145.145.145	146.146.146.146	DNS: Standard query A www.ddos.com
2	146.146.146.146	145.145.145.145	DNS: Standard query response
3	145.145.145.145	146.146.146.146	DNS: Standard query A www.ddos.com
4	146.146.146.146	145.145.145.145	DNS: Standard query response A 146.146.146.146

Frame 4 (121 bytes on wire, 121 bytes captured)

Ethernet II, Src: 00:22:a1:00:98:44, Dst: 00:26:5a:06:64:2b

Internet Protocol, Src Addr: 146.146.146.146 (146.146.146.146), Dst Addr: 145.145.145.145 (145.145.145.145)

User Datagram Protocol, Src Port: domain (53), Dst Port: 1238 (1238)

Domain Name System (response)

Transaction ID: 0x0007

Flags: 0x8580 (Standard query response, No error)

1... .. = Response: Message is a response → QR=1, 回应报文

.000 0... .. = Opcode: Standard query (0)

... 1... .. = Authoritative: Server is an authority for domain

... 0... .. = Truncated: Message is not truncated

... 1... .. = Recursion desired: Do query recursively

... 1... .. = Recursion available: Server can do recursive queries

... 0... .. = Z: reserved (0)

... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server

... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 1

Queries

www.ddos.com: type A, class IN

Name: www.ddos.com

Type: A (Host address)

Class: IN (0x0001)

Answers → 回答

www.ddos.com: type A, class IN, addr 146.146.146.146

Name: www.ddos.com

Type: A (Host address) → 查询类型

Class: IN (0x0001)

Time to live: 1 hour → TTL

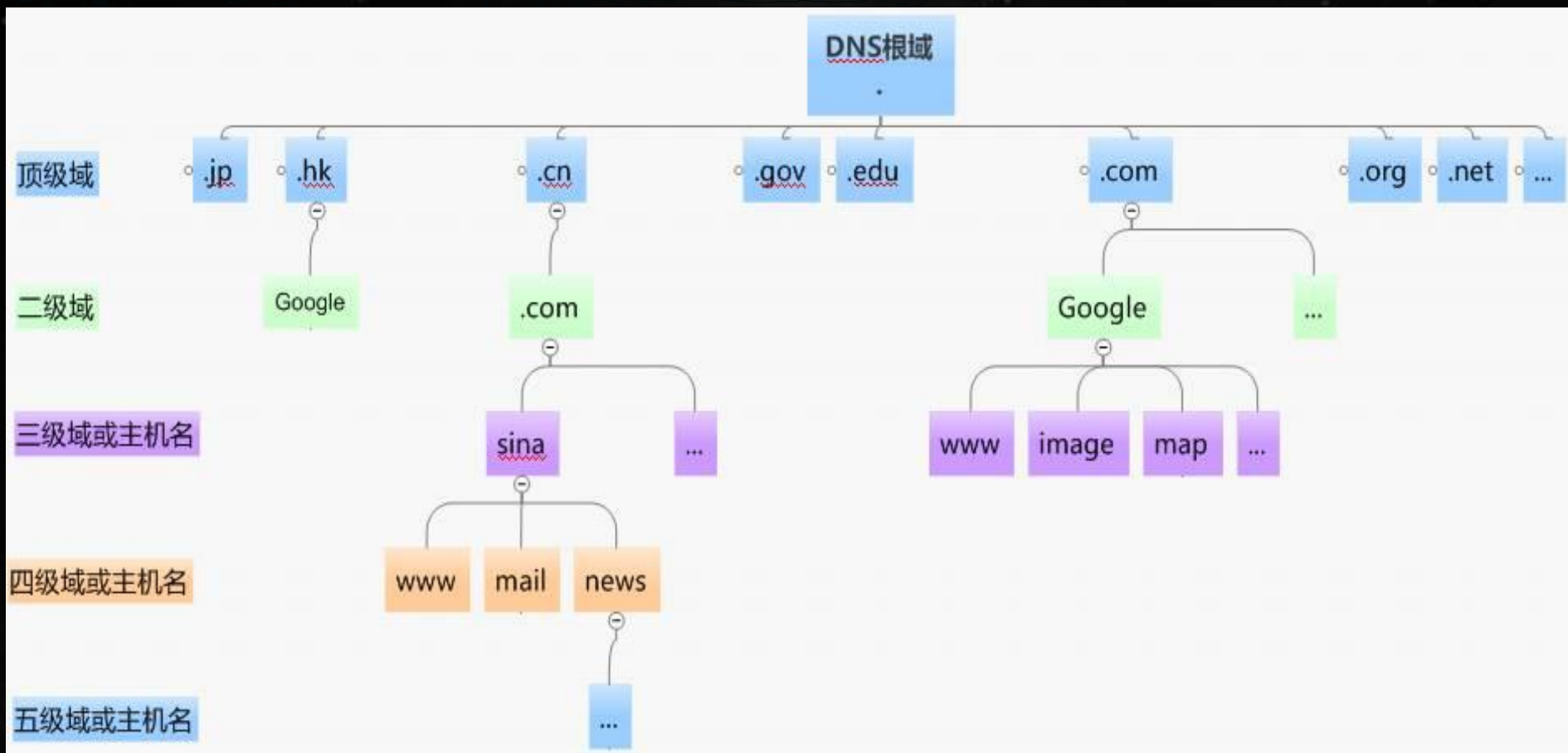
Data length: 4

Addr: 146.146.146.146 → 域名对应的IP地址

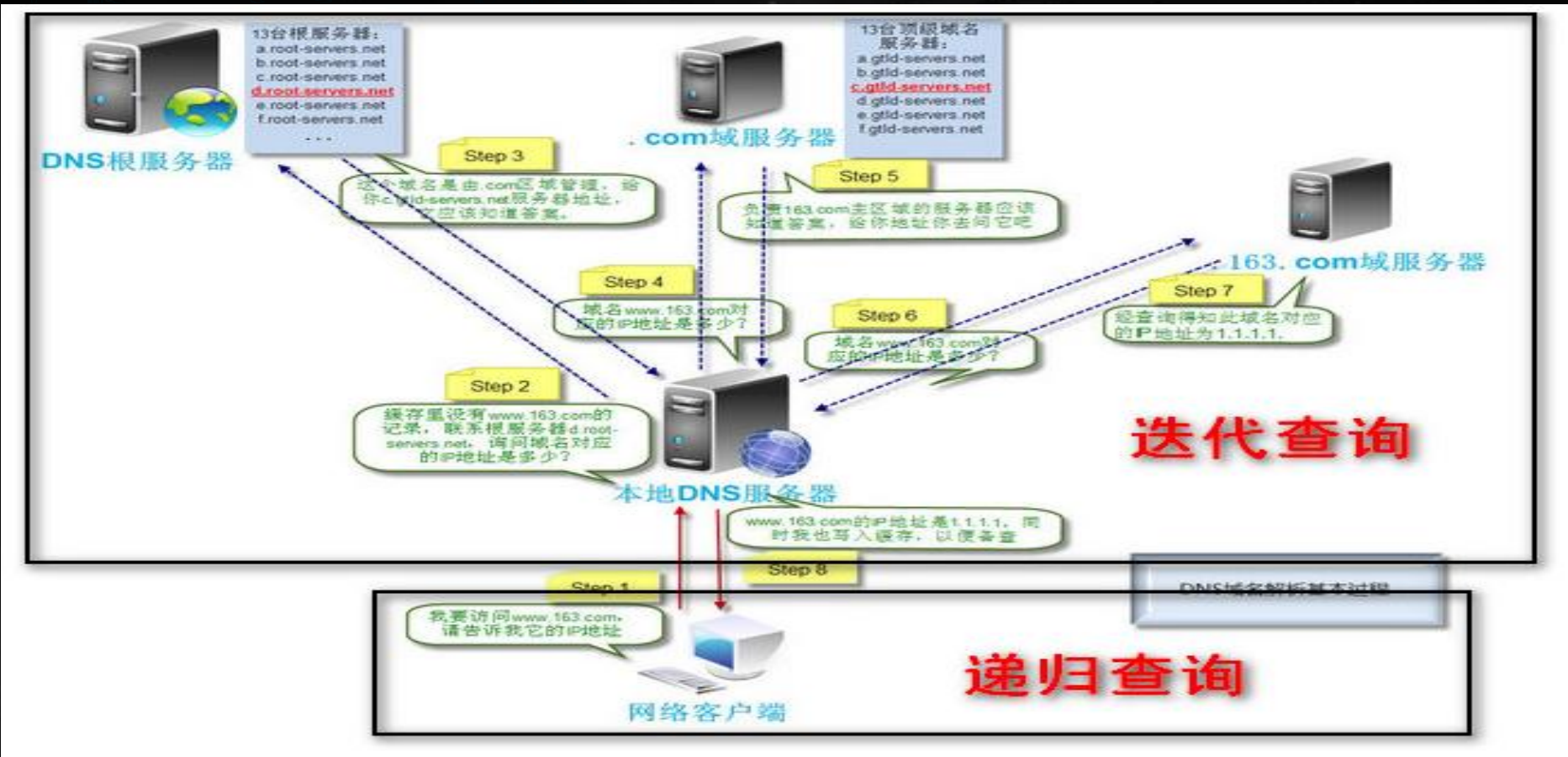
Authoritative nameservers → 授权

Additional records → 额外信息

# ● DNS树型分布式数据库架构



## ● DNS查询过程



## ● DNS体系架构的攻击



01

DNS查询攻击

02

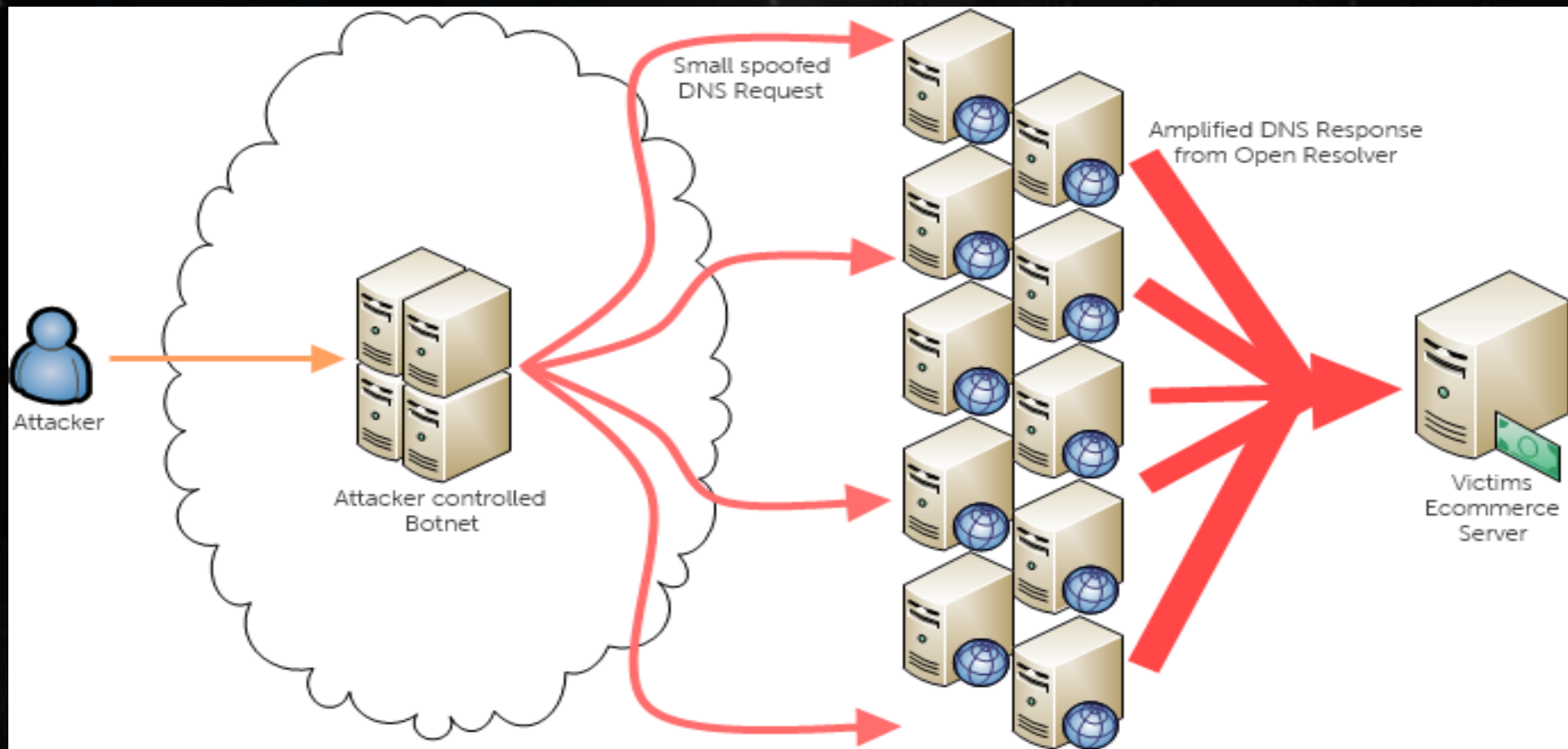
DNS反射攻击

03

DNS污染



- DNS查询/反射攻击



# ● DNS污染

# FREETALK

2017深圳站



# 13大根服务器

FREETALK

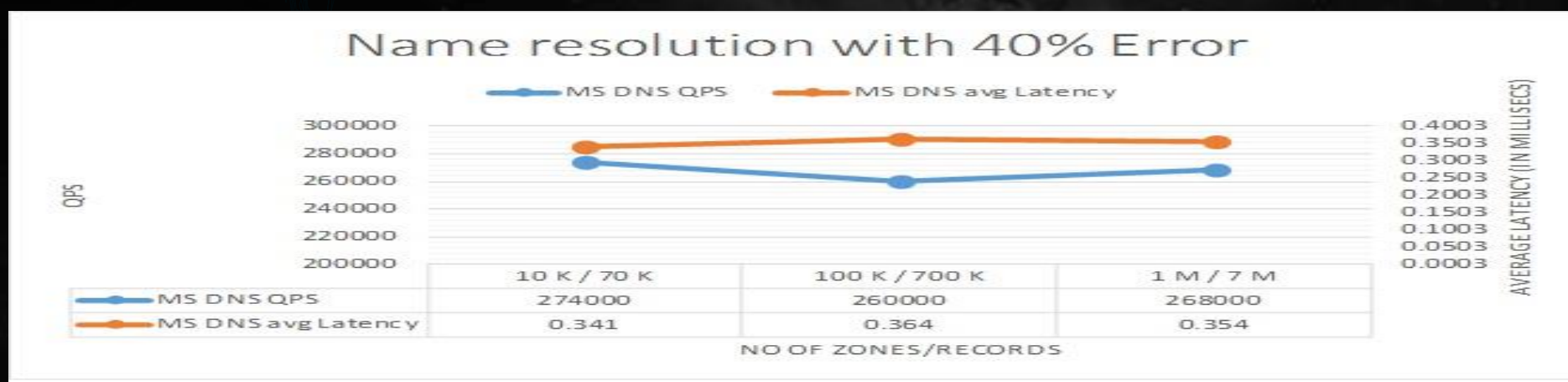
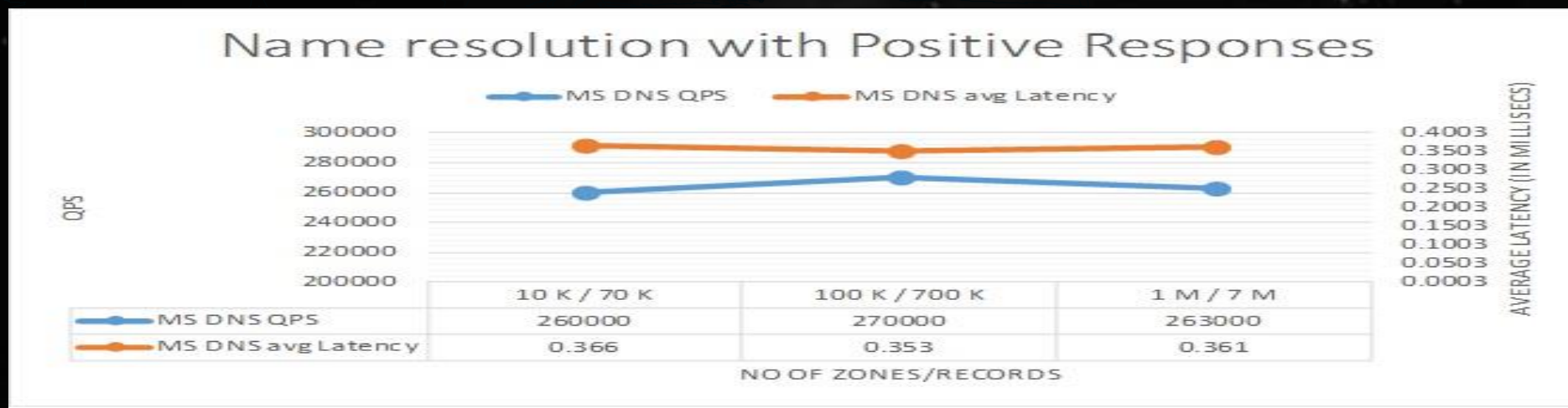
2017深圳站

字母	IPv4地址	IPv6地址	自治系统编号 (AS-number) [2]	旧名称	运作单位	设置地点 #数量 (全球性/地区性) [3]	软件
<b>A</b>	198.41.0.4	2001:503:ba3e::2:30	AS19836, [2][note 1] AS36619, AS36620, AS36622, AS36625, AS36631, AS64820[note 2][4]	ns.internic.net	VeriSign	以任播技术设置于多处 5/0	BIND
<b>B</b>	192.228.79.201 ( 2004年1月起生效, 旧IP地址为 128.9.0.107 ) [5]	2001:500:84::b	(none), [2] AS4[6]	ns1.isi.edu	南加州大学信息学研究所	美国加州马里纳戴尔雷伊 0/1	BIND
<b>C</b>	192.33.4.12	2001:500:2::c	AS2149[2][7]	c.psi.net	Cogent Communications	以任播技术设置于多处 8/0	BIND
<b>D</b>	199.7.91.13 ( 2013年起生效, 旧IP地址为128.8.10.90 ) [8]	2001:500:2d::d	AS27[2][9]	terp.umd.edu	美国马里兰大学学院市分校	以任播技术设置于多处 50/67	BIND
<b>E</b>	192.203.230.10	2001:500:a8::e	AS297[2][10][11], AS42[10]	ns.nasa.gov	美国国家航空航天局	以任播技术设置于多处 1/11	BIND
<b>F</b>	192.5.5.241	2001:500:2f::f	AS3557, [2][12] AS1280, AS30132[12]	ns.isc.org	互联网系统协会	以任播技术设置于多处 57/0	BIND g[13]
<b>G</b>	192.112.36.4	2001:500:12::d0d	AS5927[2][14]	ns.nic.ddn.mil	美国国防部国防信息系统局	以任播技术设置于多处 6/0	BIND
<b>H</b>	198.97.190.53 ( 2015年12月起生效, 旧IP地址为 128.63.2.53 ) [15]	2001:500:1::53 ( 2015年12月起生效, 旧IP地址为 2001:500:1::803f235 ) [16]	AS13[2][17]	aos.arl.army.mil	美国国防部陆军研究所	美国马兰州阿伯丁 ( Aberdeen ) 2/0	NSD
<b>I</b>	192.36.148.17	2001:500:9f::42	AS29216[2][18]	nic.nordu.net	瑞典Netnod ( 曾经是 Autonomica ) [19]	以任播技术设置于多处 41/0	BIND
<b>J</b>	192.58.128.30 ( 2002年11月起生效, 旧IP地址为 198.41.0.10 )	2001:503:c27::2:30	AS26415, [2][20] AS36626, AS36628, AS36632[20]		VeriSign	以任播技术设置于多处 61/13	BIND
<b>K</b>	193.0.14.129	2001:7fd::1	AS25152[2][21][22]		荷兰RIPE NCC	以任播技术设置于多处 5/12	NSD[23]
<b>L</b>	199.7.83.42 ( 2007年11月起生效, 旧IP地址为 198.32.64.12 ) [24]	2001:500:3::42	AS20144[2][25][26]		ICANN	以任播技术设置于多处 157/0	NSD[27]
<b>M</b>	202.12.27.33	2001:dc3::35	AS7500[2][28][29]		日本WIDE Project	以任播技术设置于多处 6/1	BIND

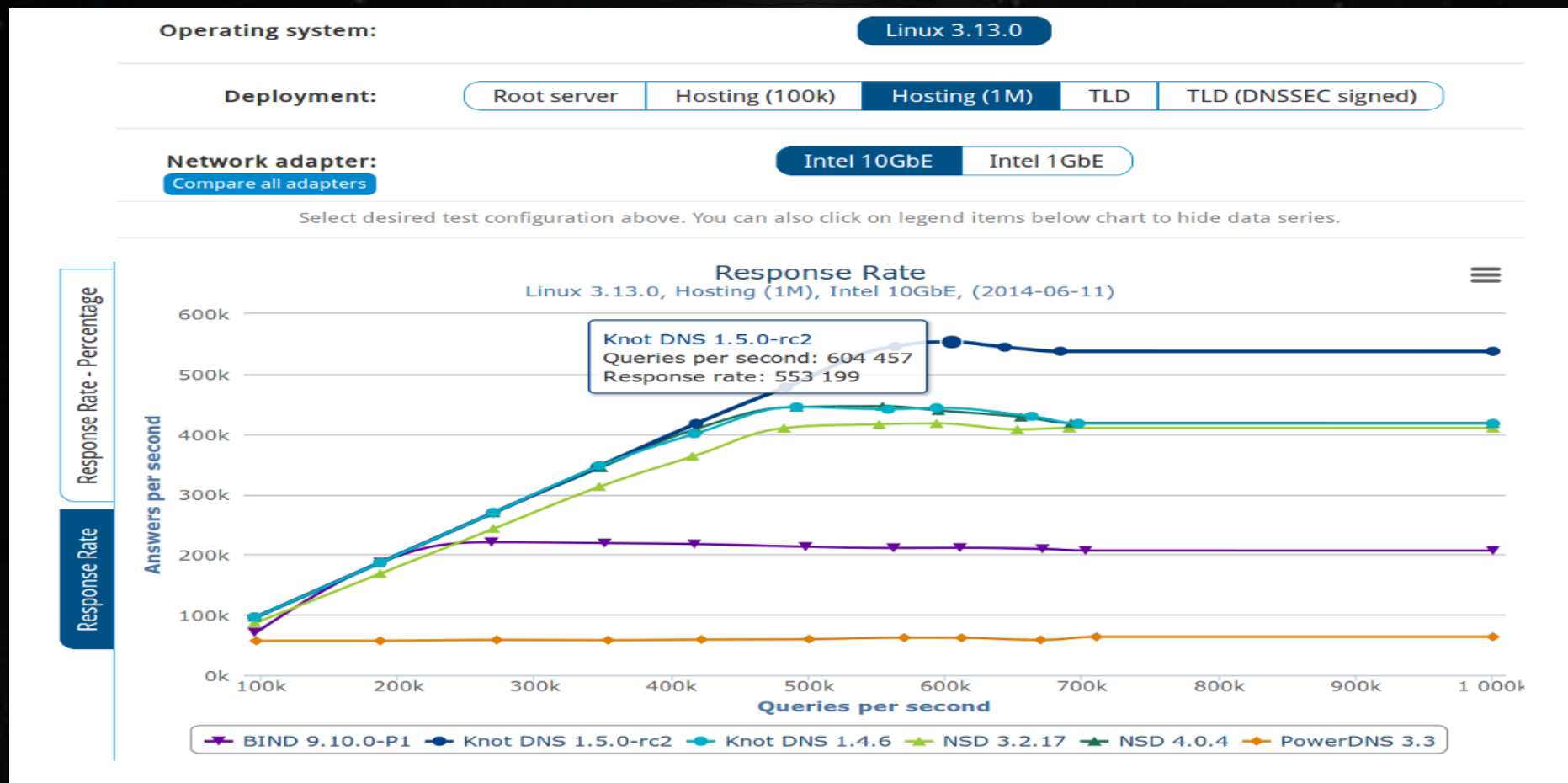
# ● DNS性能——QPS windows server 2012

# FREETALK

2017深圳站







- DNS性能和攻击能力不成正比(2014年报告)

2017 深圳站

## DNS Flood DDoS Attack Hit Video Gaming Industry with 90 Million Requests per Second

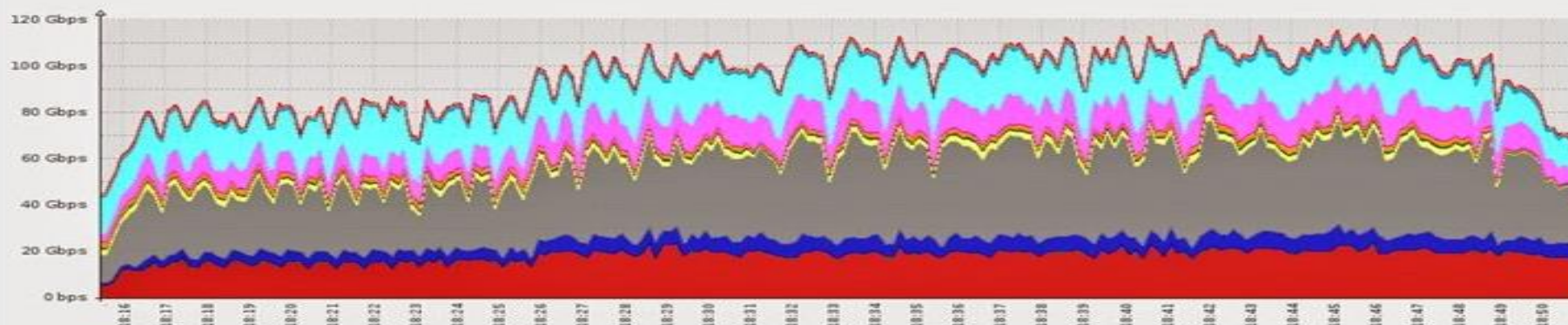
Monday, June 23, 2014 Mohit Kumar

发送图片到手机



# DNS Flood DDoS Attack

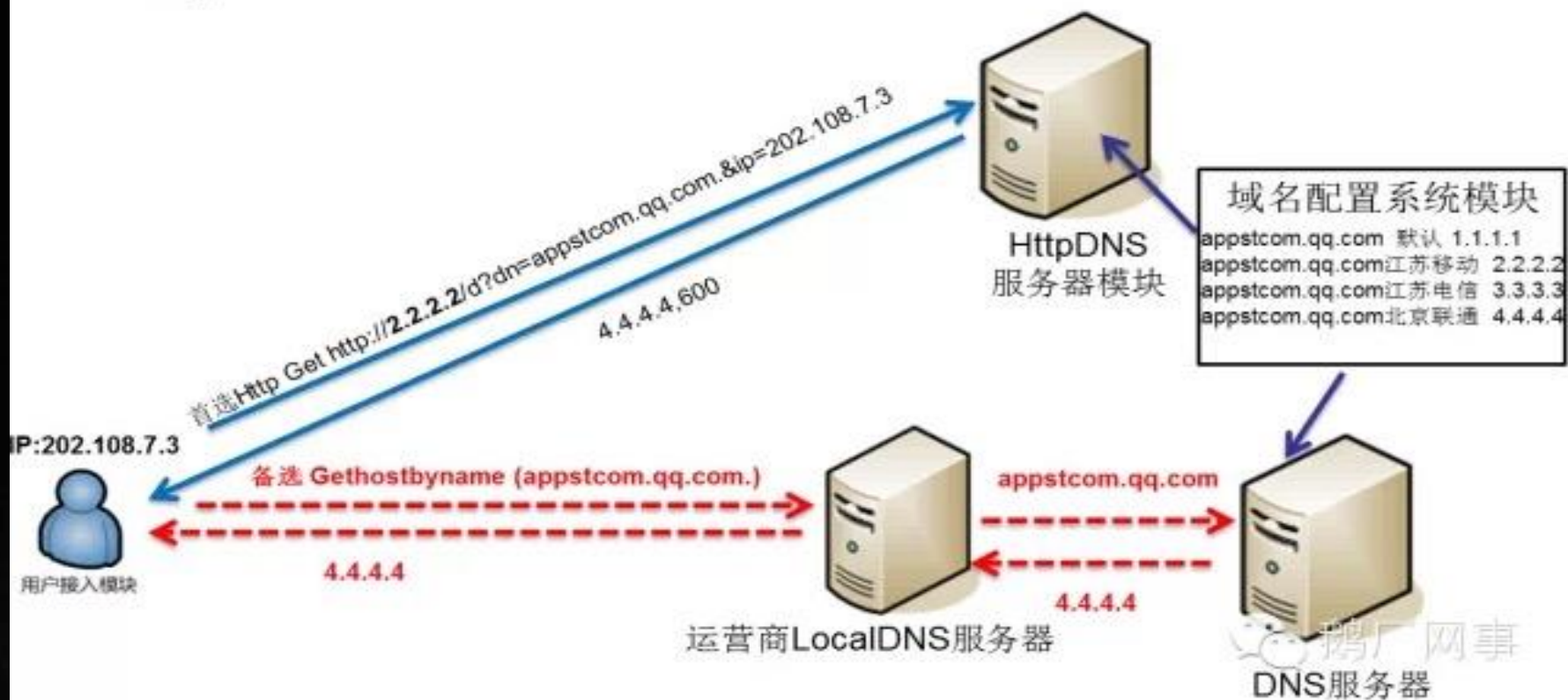
*90 Million requests/sec (Above 110 Gbps)*



The Hacker News  
Security in a serious way

## ● 目前解决方案——httpdns

## HttpDNS基本原理





- 目前解决方案——public dns

## WHAT IS PUBLIC DNS?

A free DNS resolution service that respects your privacy



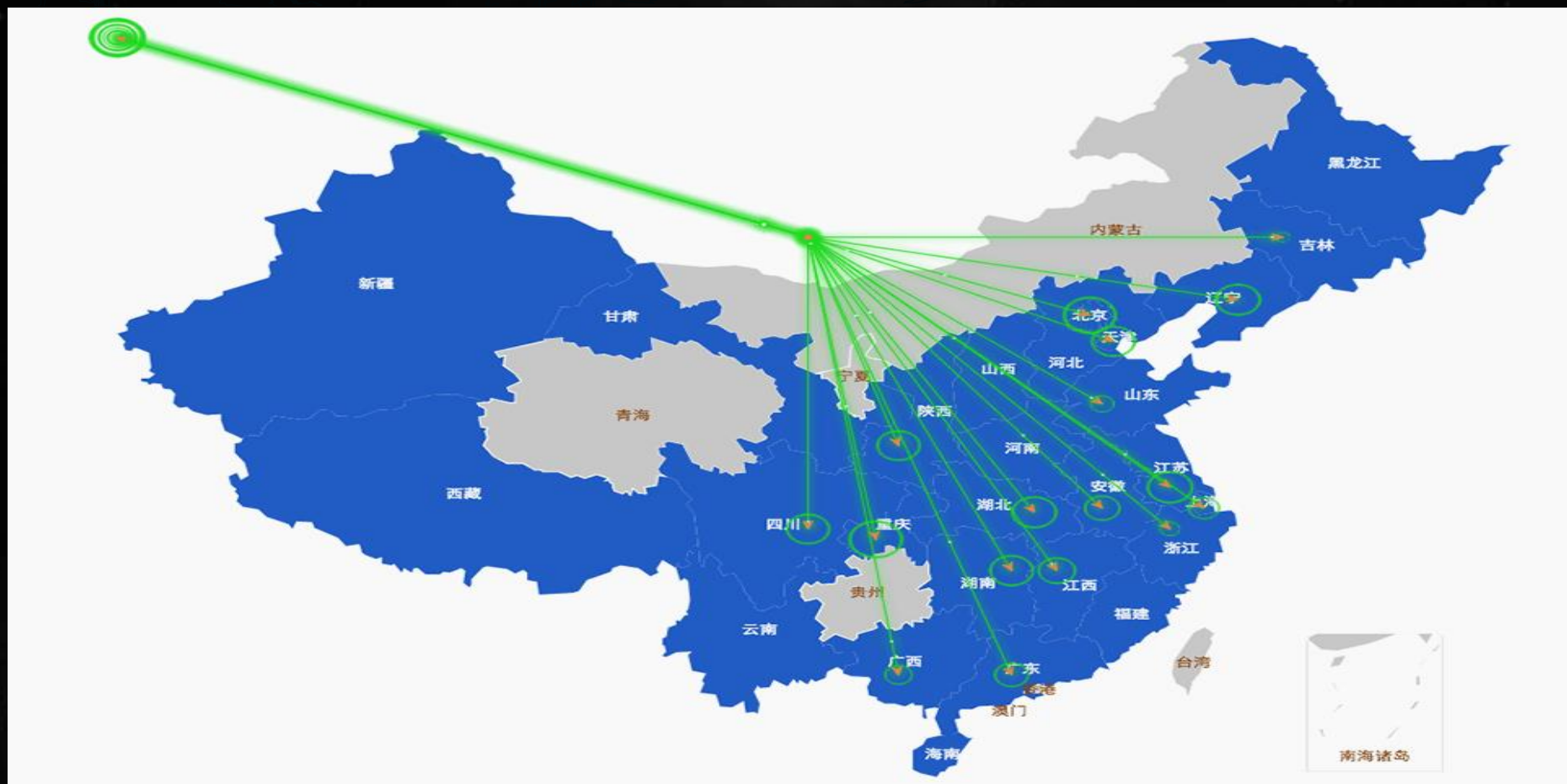
Verisign Public

2

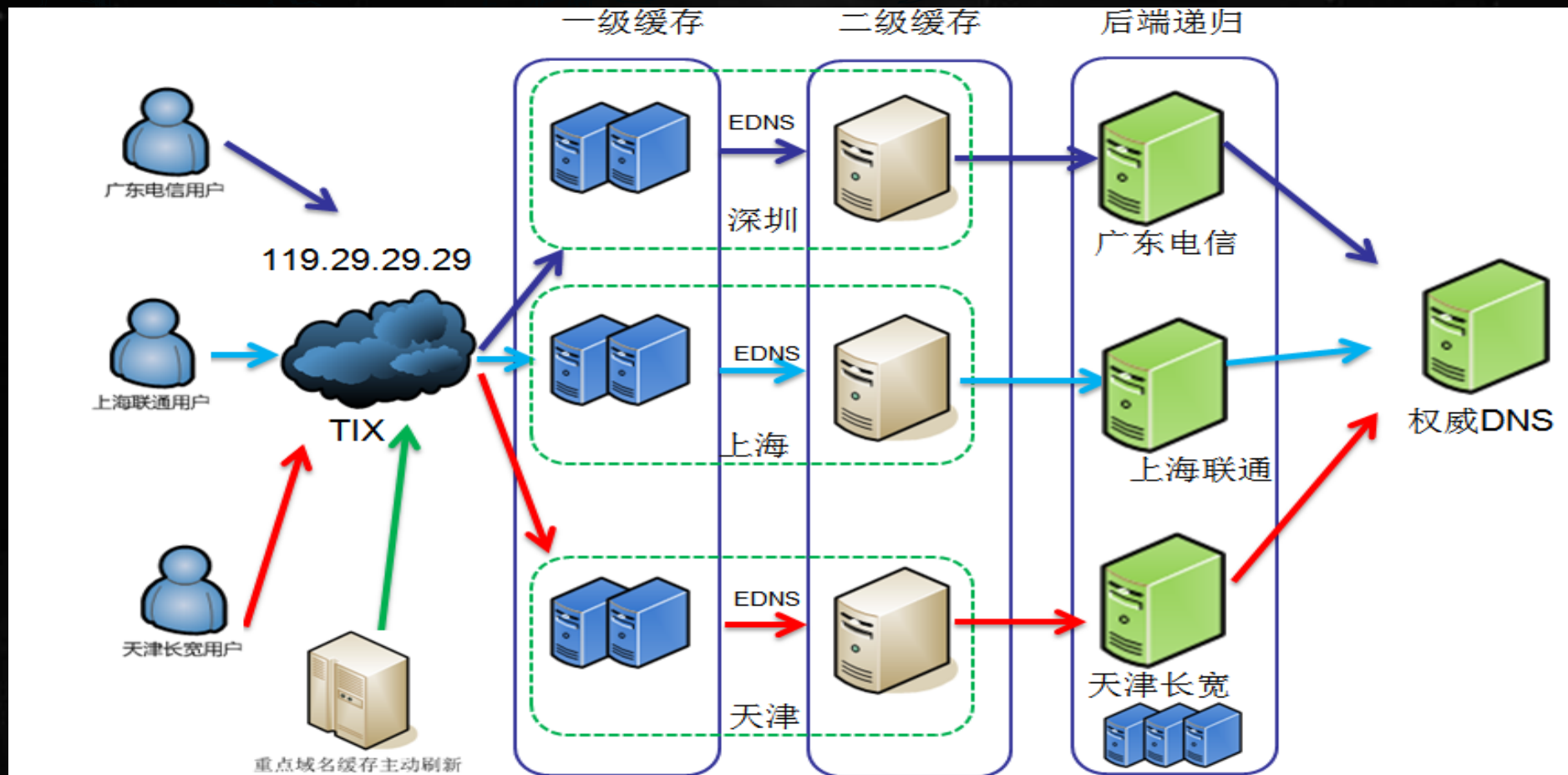


# ● 目前解决方案——public dns 分布示意图

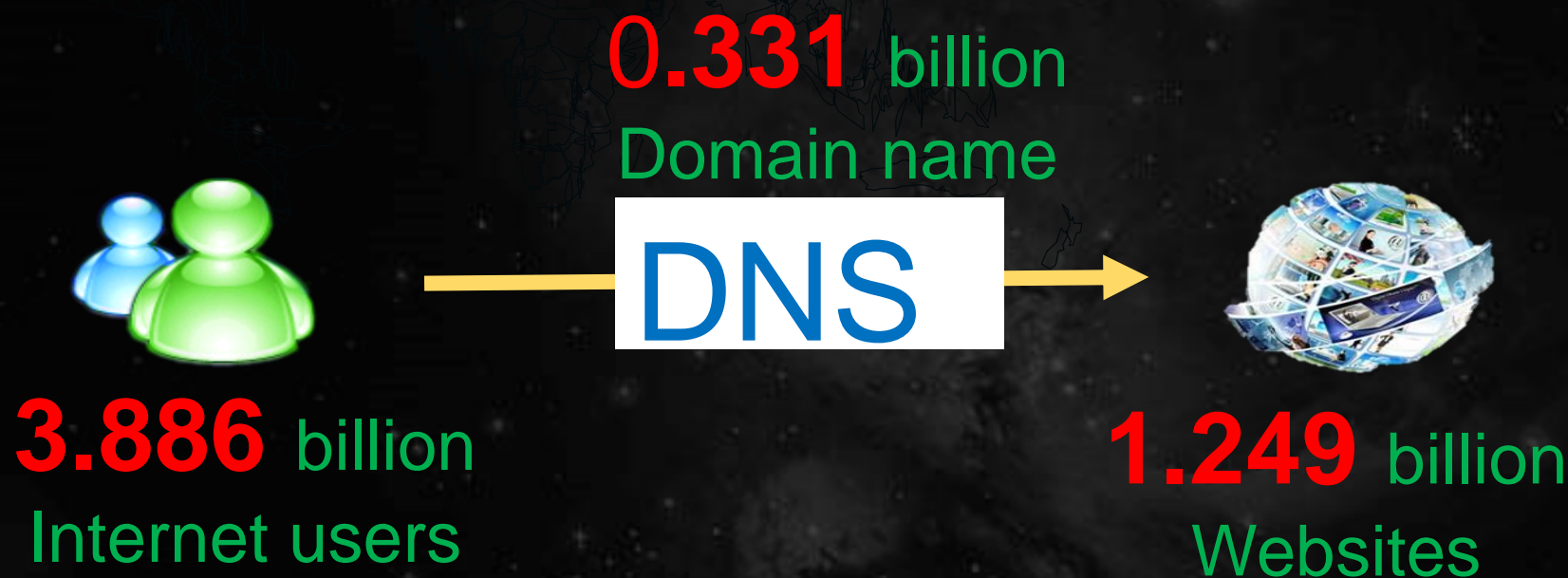
2017深圳站



## ● 目前解决方案——智能 dns 示意图



- DNS (域名系统) —— 互联网框架回顾



## 我们的解决方案——基于机器学习的全新架构





● 当前其他厂家性能——业界最佳17M QPS



安全高

高达1100万次/秒的解析性能，拥有500G强大的DNS攻击防护能力，是大数据时代最可靠的网站安全专家。


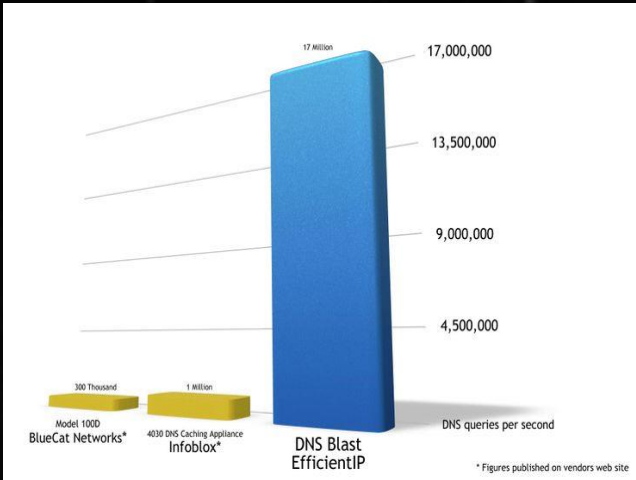


千万级解析性能，快速省时

自主研发高性能DNS内核  
单机处理性能是传统解析服务的200倍



转发性能	抵抗攻击性能
80 万 QPS	120 万 QPS



Security module  
wired deal with attack

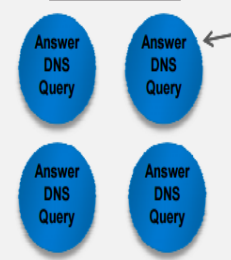
Resolve module  
up to 10,000,000QPS

Management module

queries/second  
BIG-IP 1600: ~300k qps  
BIG-IP 3900: ~600k qps  
BIG-IP 8900: ~1.5 Million

VIPRION  
Up to 6 million qps!

DNS Express in TMOS



© F5 Networks, Inc.

# 我们的解决方案——攻防严重不对等导致大量资源浪费

随机生成域名测试，单台攻击发包能力1.2亿 QPS  
目前防御最高能力国内0.11亿/海外0.17亿QPS

攻防能力不对等

正异常不对等

正常流量不到防御能力的百分之一

攻防  
不对等

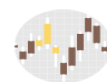
想要DNS解析安全稳定，选择我们，选择放心



日解析量  
**1000+** 亿次  
平均每秒115万次查询响应



域名总量  
**2000+** 万个  
千万域名选择帝恩思的解析服务



防御峰值  
**2+** 亿QPS  
真实防御案例，传统DNS千万攻击已被打垮

### 我们的解决方案——基于客户的AI学习和预测



## ● 我们的解决方案——基于热点的AI学习和预测

**应用热点**  
新闻、体育、股票、搜索、  
汽车、公司、教育、游戏、  
医疗

**临时热点**  
体育赛事  
突发新闻等  
当前流行高热度内容

**区域热点**

不同地区、类型的客户热点  
物联网相关热点  
服务器应用热点

**行为/时间热点**

早、午、晚  
工作时间、休息时间  
工作日、休息日



## ● 基于AI的智能DNS主动防御

AI  
DNS

单设备60G+的带宽0.72亿QPS能力

多层次，分布式部署的综合防御网络

基于AI学习的属性数据库

基于AI预测的多层次判据

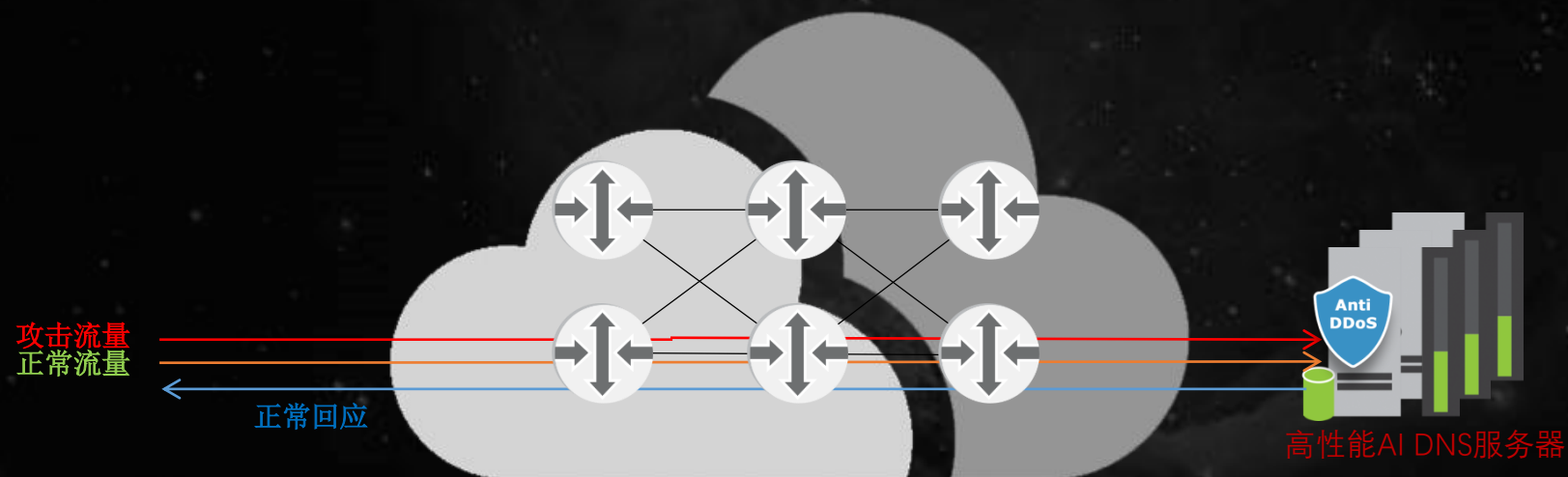
基于体验优先的预编译多维算法



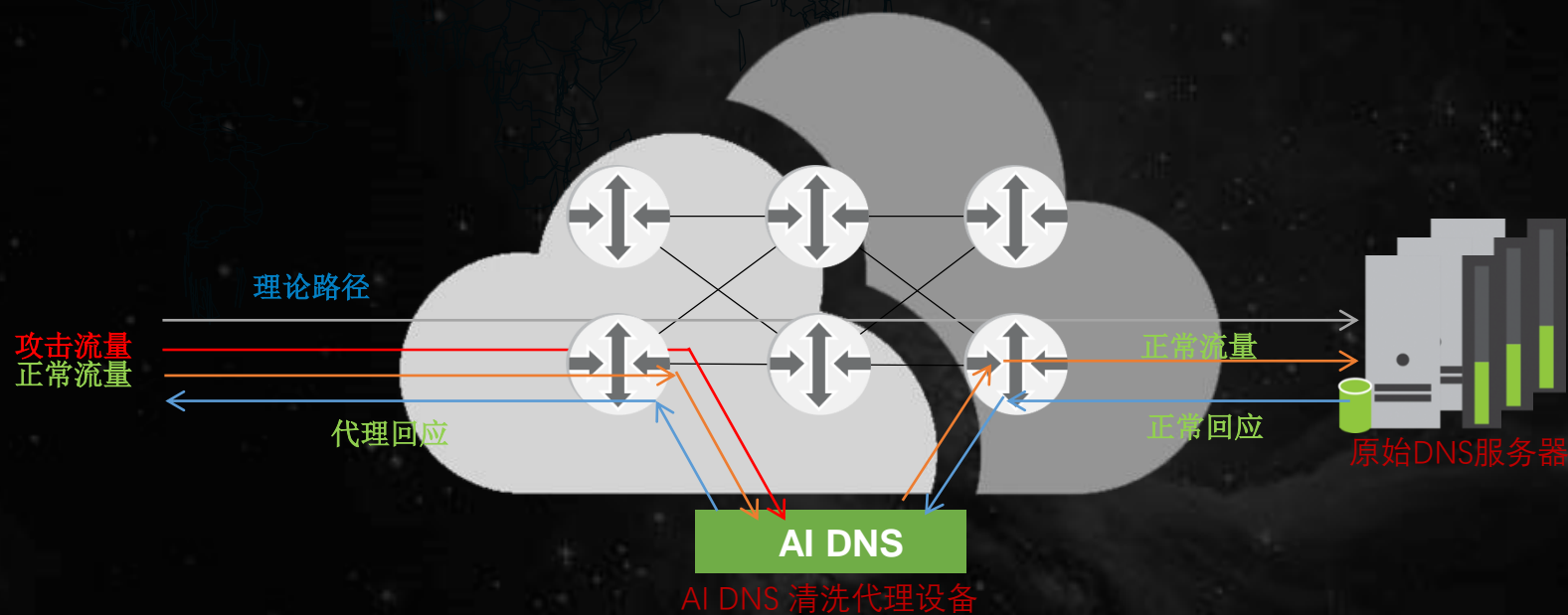
- DNS DDos Server – 服务器模式

# FREETALK

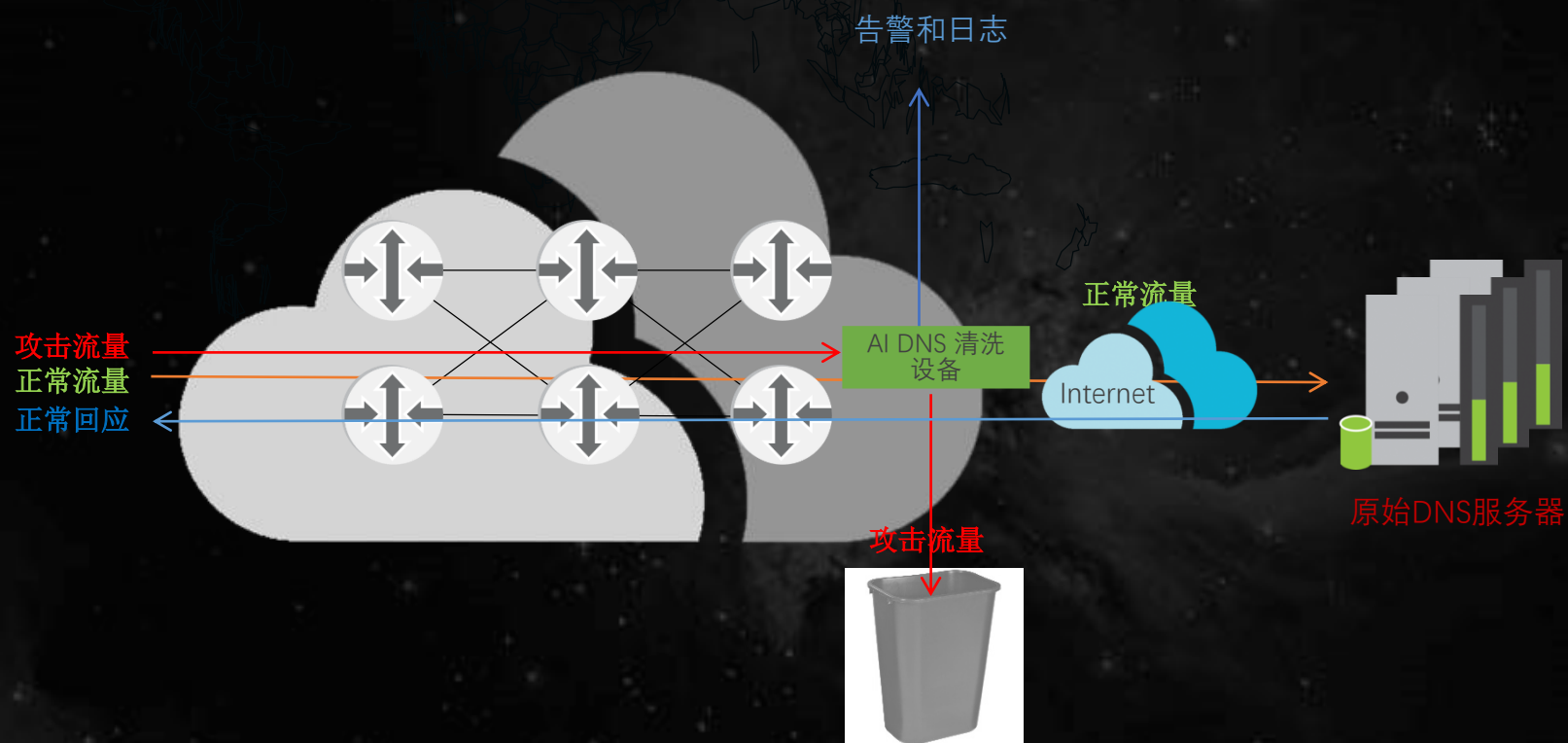
2017 深圳站



- DNS DDos Proxy – 代理模式



- DNS DDos Defense – 防护模式





## ● 基于新一代AI DNS系统的其他应用

### 01 安全应用

僵尸网络, C&C中心监控  
基于AI DNS的Ddos防御

### 02 AI流量管理

基于AI的智能流量管理  
基于应用压力的均衡  
基于计划维护的流量均衡  
基于用户等级/策略的流量均衡

### 03 商业应用

热门应用的预测  
有害爬虫、无害爬虫的分析

### 04 热点预测

基于客户行为的热点预测  
基于应用趋势的热点预测  
基于商业行为的热点预测  
商业行为真实性报告

