DNS Security Threats and Solutions

Prof. Xiaodong Lee

Dec. 10, 2014

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

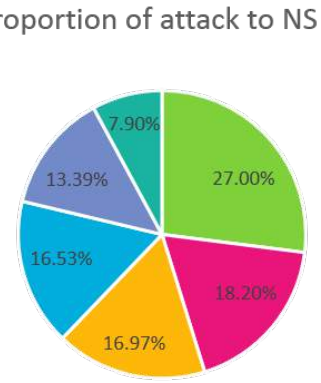
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Content

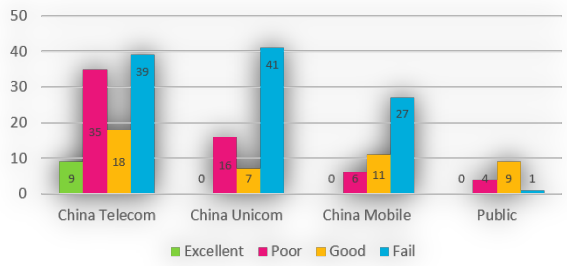
“825” case study

1.1 “825” review

- Process:
  - 2013.8.25 00:06, .CN suffered massive denial of service attack, attack traffic is several hundred times of daily traffic.
  - Attacked domain name is random name ending with rfinfo.cn .
  - The resolution service is partly influenced by bandwidth congestion.
  - The attack ended at 8.26 07:40, lasted nearly 8 hours.
- Disposal Strategy:
  - Traffic cleaning with anti-attack equipment
  - Emergency bandwidth capacity expansion
  - Increased TTL temporarily
  - NS transfer



Fail rate of recursive server



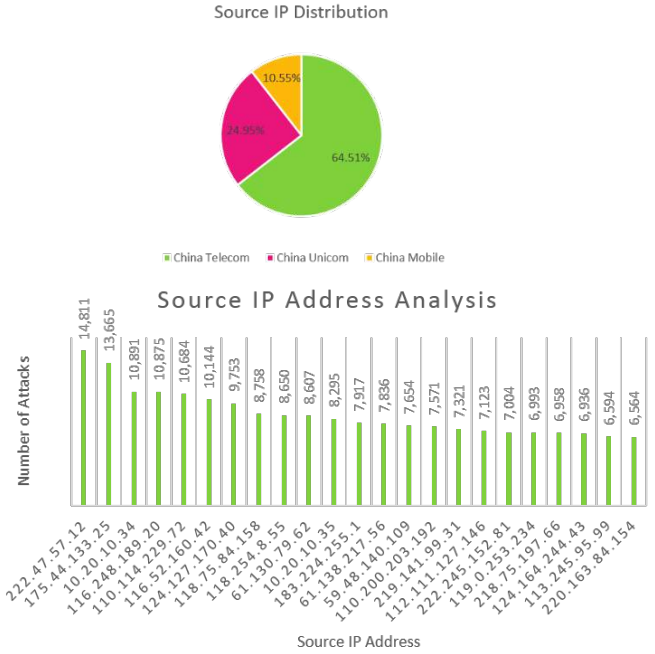
Success rate of recursive server (by ISP)

“825” case study

1.2 “825” analysis

- Attack type is DDoS from controlled clients and source IP is dispersed

Attack traffic



- Attack characteristics are obvious

#ab^c.rfinfo.cn
+r%h.rfinfo.cn
%t&k.rfinfo.cn

- Attack aimed to a game website, not .CN

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Content

2.1 DDoS attacks occupy mainstream

- Mostly attack came from controlled clients
- Attack traffic increased significantly
- Source IP is dispersed

① June
- 4th: 153Kqps

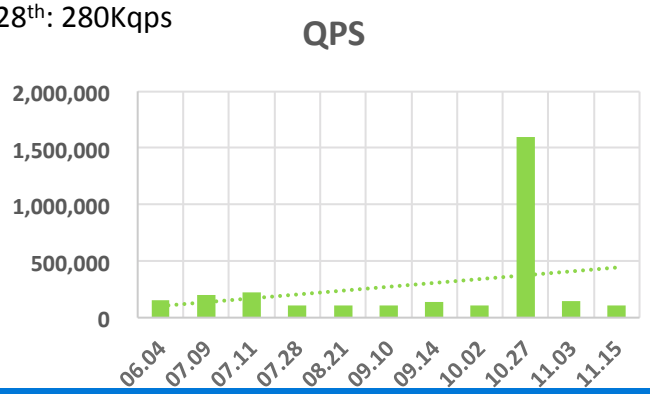
③ July
- 9th: 200Kqps
- 11th: 226Kqps
- 28th: 280Kqps

① August
- 21st: 110Kqps

② September
- 10th: 106Kqps
- 14th: 140Kqps

② October
- 2nd: 104Kqps
- **27th: 1.6Mqps**

② November
- 3rd: 160Kqps
- 15th: 104Kqps



2014.6-2014.11

Total: 64

Peak QPS > 100,000: 11

Average per Month: 2

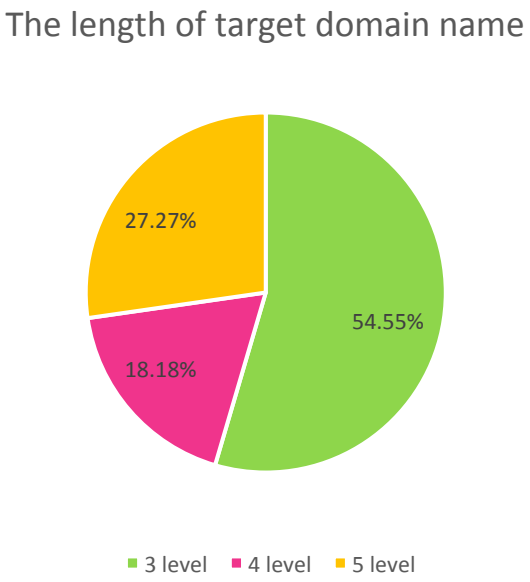
Max Peak QPS: 1.6 Million

27th, Oct. 2014

2.2 Attack characteristics are obvious

- Mostly attack random.fixed-domain.cn
- Mostly attack 3rd and below level domain name

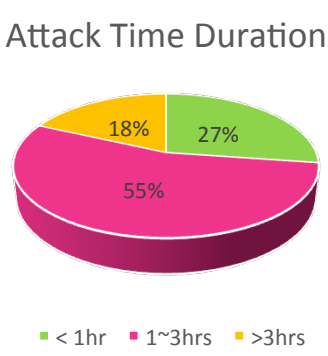
2 types of attacks		
Fake Prefix	xxx.domain.cn	63
Fake Suffix	domain.cnxxx	1

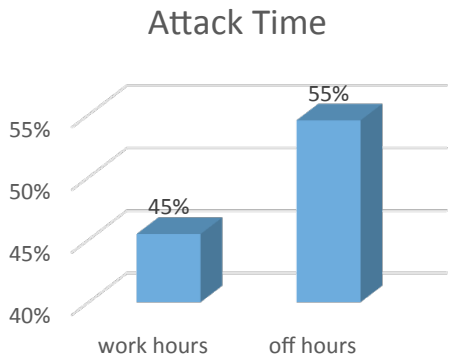


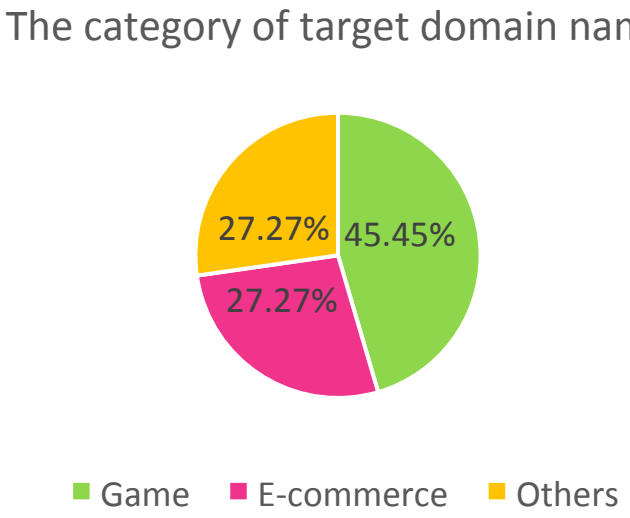
2.3 Accidental injury - Not aim to, but actually affected .CN

- Mostly attack Game, E-commerce site and so on

Attacked Domain Applications' Types		
Games Site	E-commerce Site	Lottery Site
Gambling Site	Bitcoin Site	Navigate Site







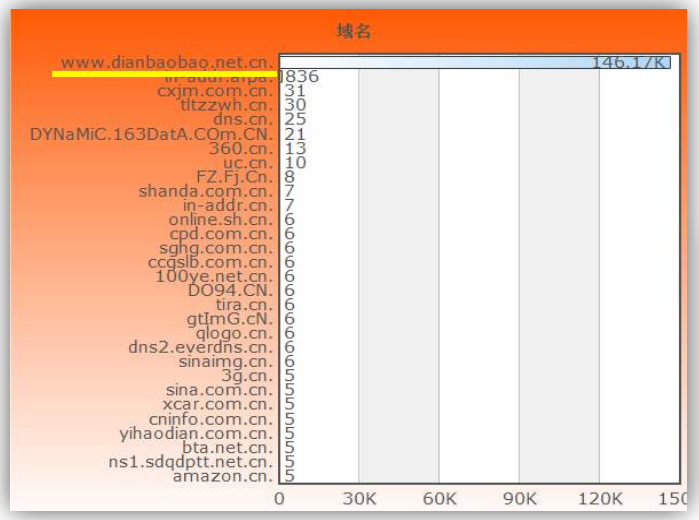
2.4 Analysis of typical attack case-2014.10.27

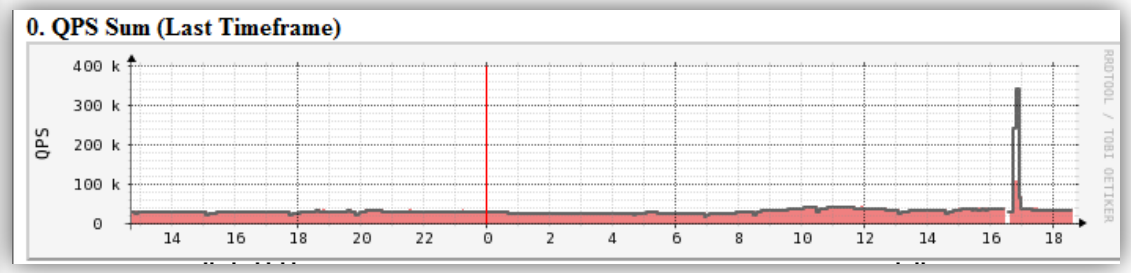
- DDoS: 1.6 Million QPS
- Charasteristic: xxx.dianbaobao.net.cn
- Aim to: E-commerce Site

Analysis for the location of the source attack IP in typical sites

IP	Location	IP	Location
202.100.93.154	P.R.C.	66.249.66.0	U.S.
211.137.44.0	P.R.C.	23.29.72.126	U.S.
202.104.3.87	P.R.C.	208.67.219.0	U.S.
61.140.11.0	P.R.C.	23.29.72.105	U.S.
218.107.56.67	P.R.C.	163.10.42.221	AR
74.118.193.0	U.S.	92.187.121.0	FRA
67.23.166.152	U.S.		

QNAME Rank in one typical .CN site

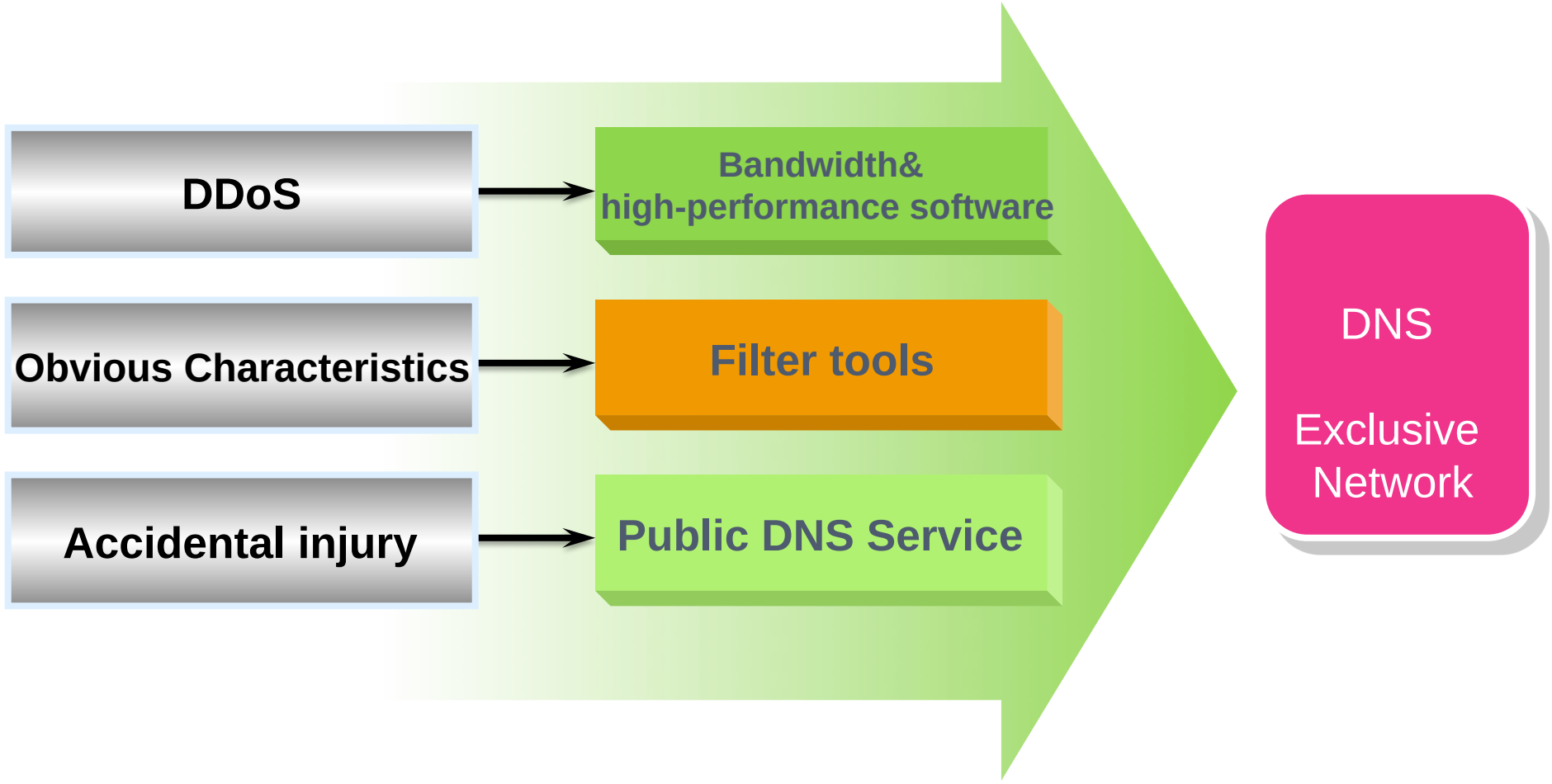




中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

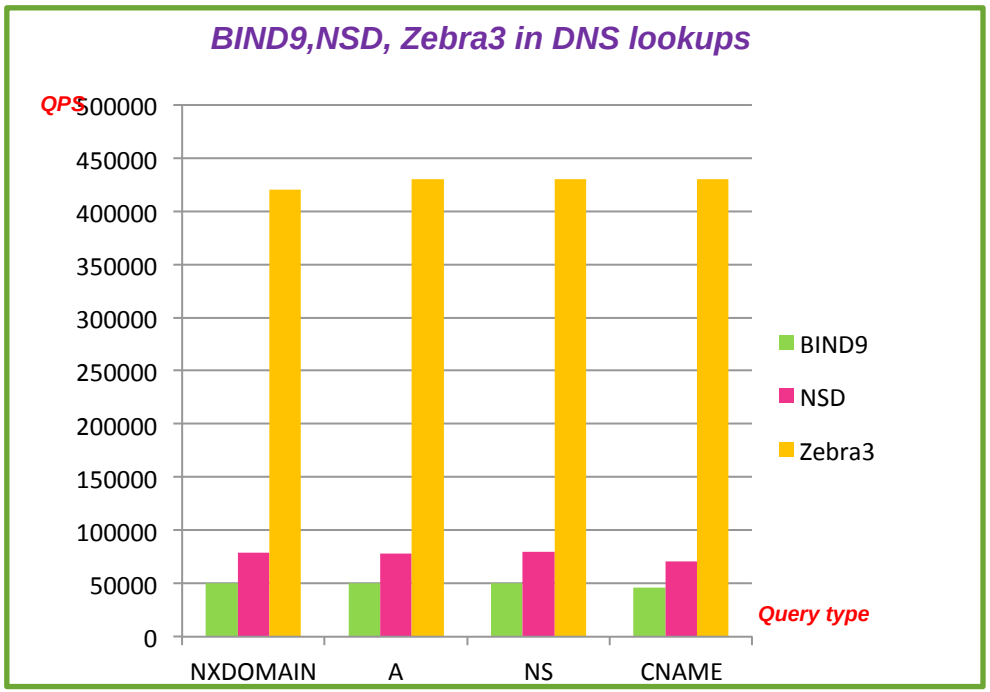
Content

3.1 Overview


DDoS
Bandwidth&
high-performance software
Obvious Characteristics
Filter tools
Accidental injury
Public DNS Service
DNS
Exclusive
Network

3.2 Anti-DDoS

- Bandwidth expansion
- High-performance DNS Software



SDNS-A (Zebra 3):

- an authoritative name server
- developed by CNNIC
- support DNS/DNSSEC lookups, zone transfer and so on

DNS query performance

- Zebra3 outperforms BIND9 up to about 10 times in QPS
- Zebra3 almost have the same performance in different lookups

3.3 Filter tools

SDNS-D

CNNIC *Anti-attack device*

Using FPGA to improve the performance

- Monitor the DNS query
- Block the DDOS attack query
- Emergency Cache
- Gigabit wire-speed one port

DNS-prime

Using 10G ethernet

10G wire-speed one port

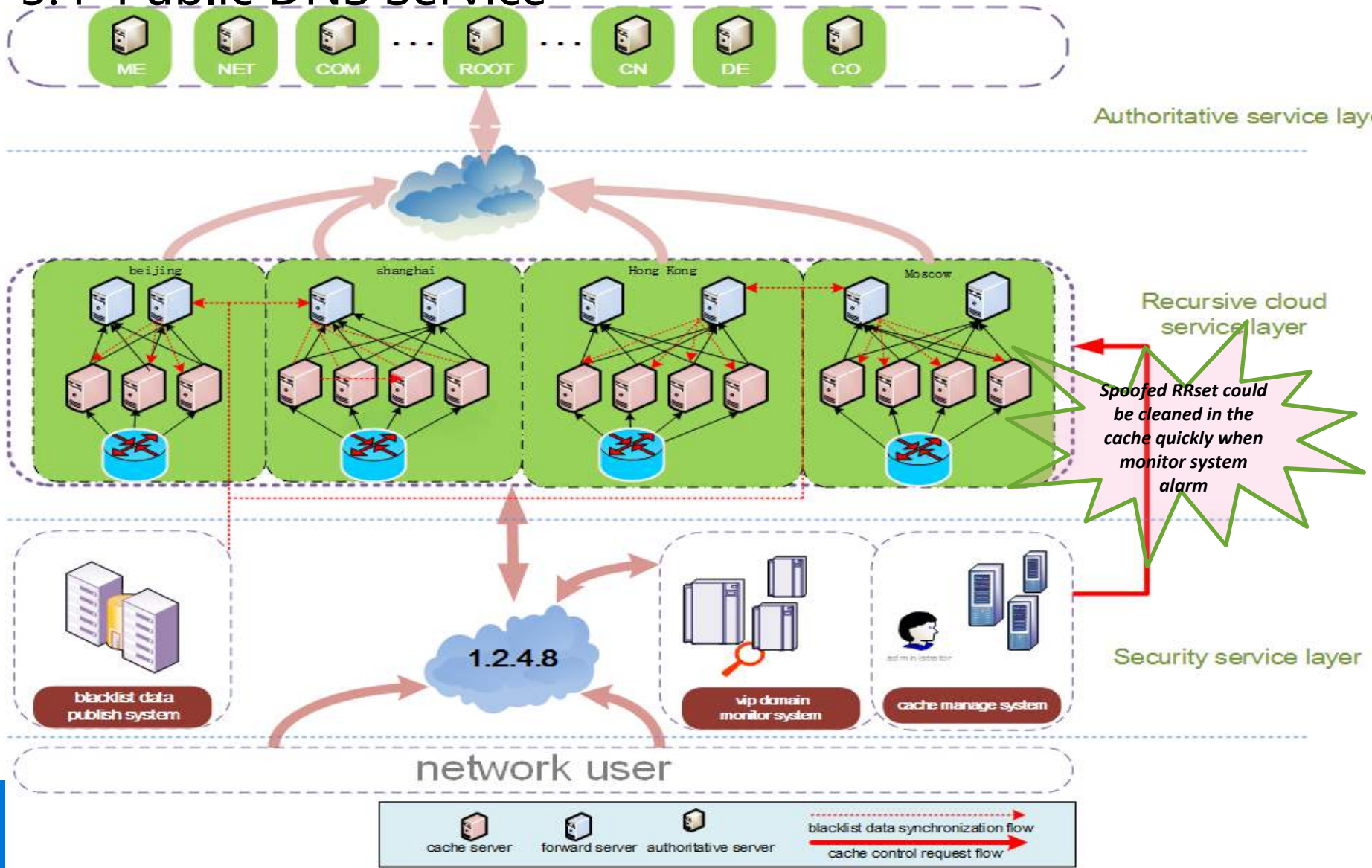
- 10 Gigabit wire-speed one port
- Using Zone-transfer protocol to build domain white list
- Traffic control for every IP and Domain
- Deep packet inspection

ZoomDNS

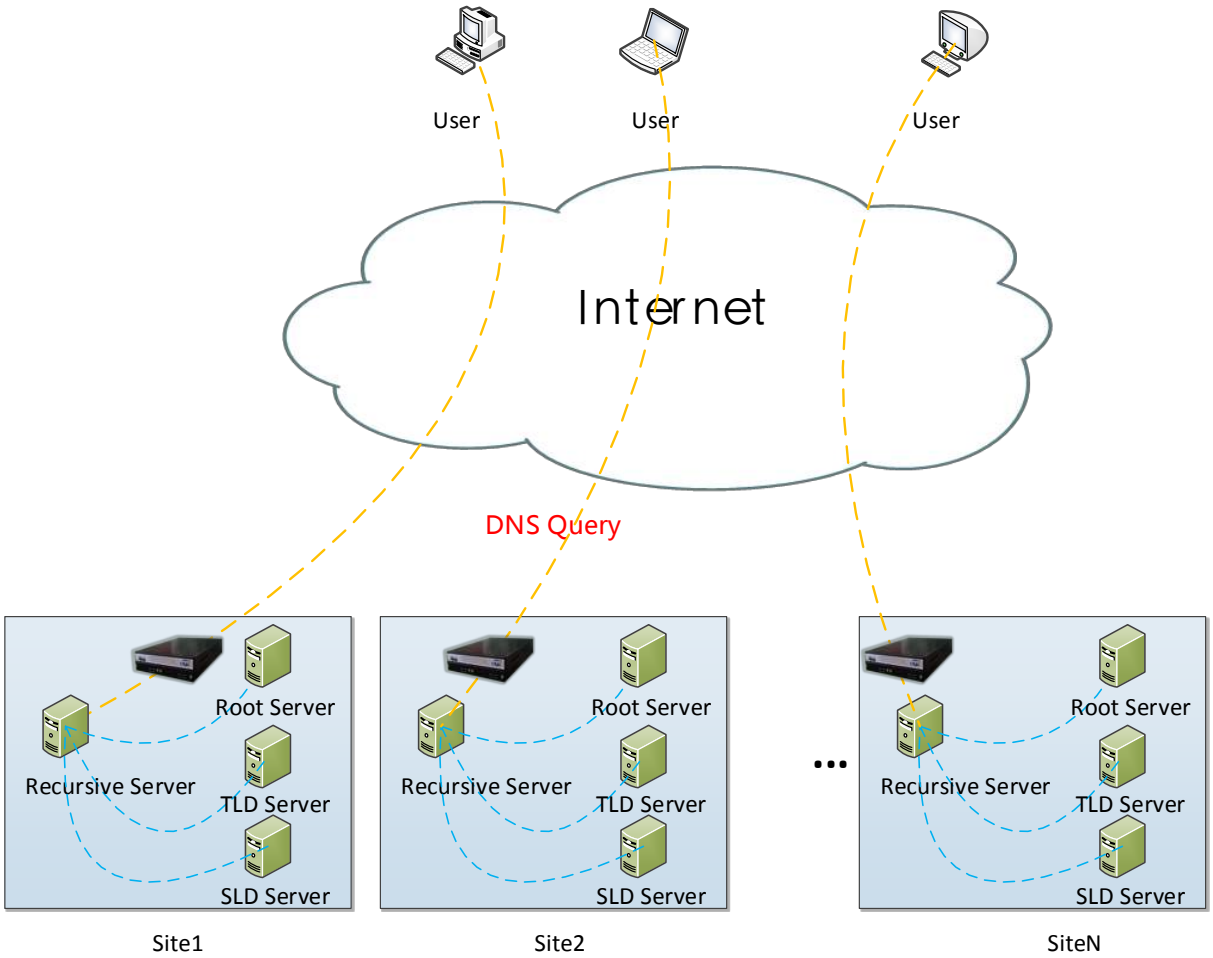

```
[root@localhost server]# zoomdns-client show status

ZOOM STATUS INFO -
+ speed-up yes
+ QpS  700000/s

FILTER STATUS INFO -
+ the number of black list items
     -ipv4 :  234 -ipv6 : 12 -domain name : 1000
+ black list ipv4        dropped : 89756
+ black list ipv6        dropped : 45678
+ black list domain name dropped : 2345566
```

- Lightweight solution
- Deep packet inspection
- Blacklist of domain suffixes
- Gigabit wire-speed
- Speed up the DNS performance

3.4 Public DNS Service



3.5 DNS Exclusive Network



中国信息社会重要的基础设施建设者、运行者和管理者

北京市海淀区中关村南四街四号中科院软件园　　邮编: 100190

www.cnnic.cn