Infoblox
NEXT LEVEL NETWORKING

DNS Security: Threats and Solutions

Cricket Liu, Chief DNS Architect

Outline

- Threat: Distributed Denial of Service and DNS
- Solutions: Monitoring DNS Traffic, Anycast and Response Rate Limiting
- ~~Threat: Cache Poisoning~~
- ~~Solutions: Query Port Randomization and DNSSEC~~
- Threat: Malware Propagation, Command and Control
- Solution: Response Policy Zones
- Threat: DNS Tunneling
- Solution: Advanced DNS Protection

DDoS and DNS

- DDoS attacks are twice the threat to DNS
  - DDoS attacks *target* name servers
  - DDoS attacks *use* name servers

DDoS Attacks Target Name Servers

- Authoritative name servers are obviously a critical resource
  - Without them, your customers can't get to your web site, send you email
- Authoritative name servers are easy to find

```
dig ns company.example.
```

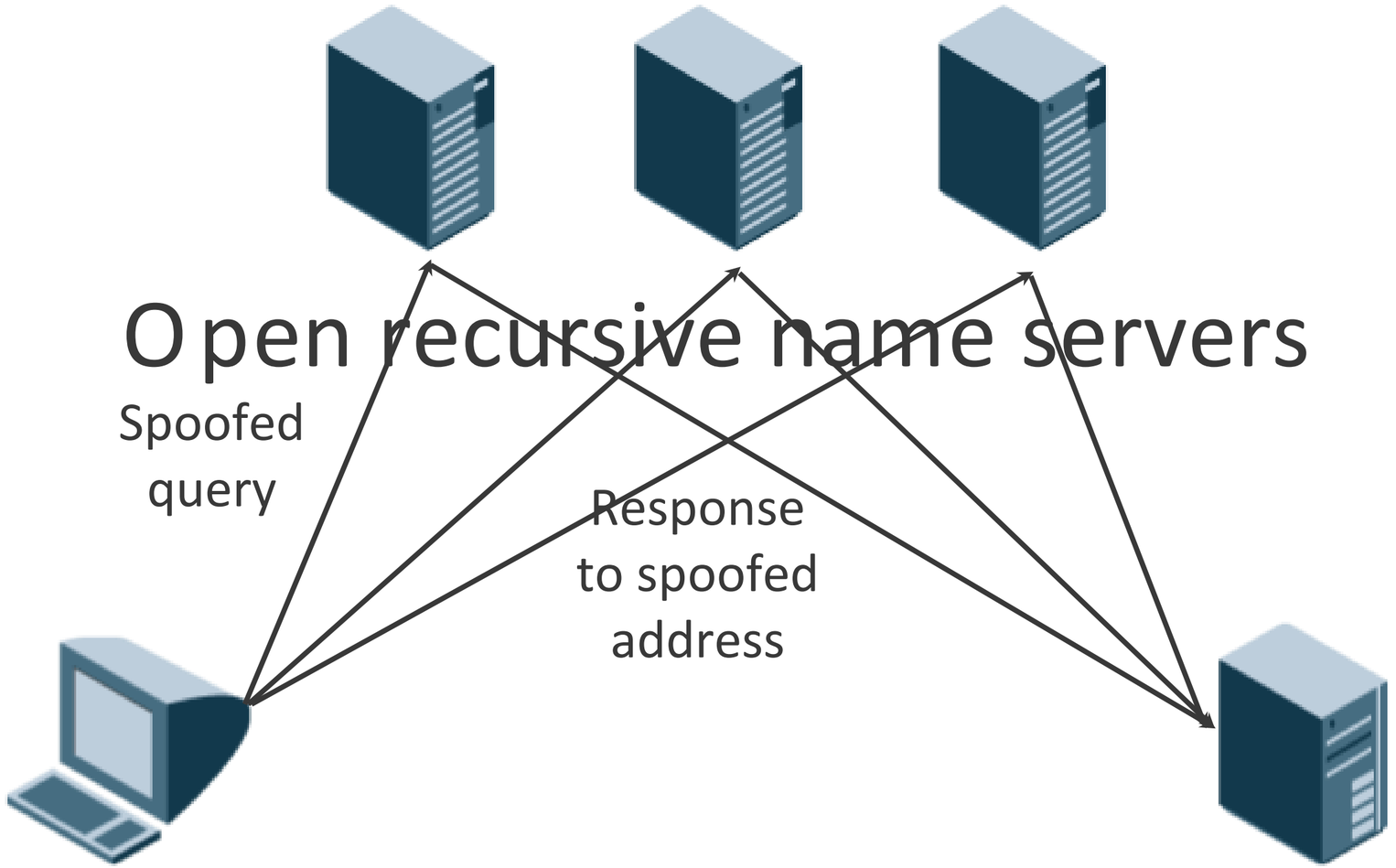
- "…big increase in proportion of attacks targeting DNS in Q2" – Arbor Networks
  - Up from 8% to 13.3%
- 2016 DDoS attack against Dyn: 1.2 Tbps

And DDoS Attacks Use Name Servers

- Why?
  - Because name servers make surprisingly good amplifiers

This one goes to eleven…

DDoS Illustrated



Amplification: They Go Past Eleven…

```
$ dig @sfba.sns-pb.isc.org. any isc.org. +norec +dnssec

; <<>> DiG 9.9.1-P1 <<>> @sfba.sns-pb.isc.org. any isc.org. +norec +dnssec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34036
;; flags: qr aa; QUERY: 1, ANSWER: 26, AUTHORITY: 0, ADDITIONAL: 15

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org.                IN      ANY

;; ANSWER SECTION:
isc.org.    7200    IN    SOA      ns-int.isc.org. hostmaster.isc.org. 2013090300 7200 3600 24796800 3600
isc.org.    7200    IN    RRSIG    SOA 5 2 7200 20131002233248 20130902233248 50012 isc.org. hUfqnG5gKbygAeVRHjP5As31lsheMKNPD7g9MJlWZTrmD2de6Z/eCwUX kQxRT5TV0lFWjtGFuA0a4svbCZ1qHS9d/rhWc7IMziu2u+L9tbho+c4j szvGAJ9kYvalNbgpmkHdm+wmOHWmiY3cYKcl5Ps8gs5N0Q1JdkaCARPF HQs=
isc.org.    7200    IN    NS       sfba.sns-pb.isc.org.
isc.org.    7200    IN    NS       ns.isc.afilias-nst.info.
isc.org.    7200    IN    NS       ams.sns-pb.isc.org.
isc.org.    7200    IN    NS       ord.sns-pb.isc.org.
isc.org.    7200    IN    RRSIG    NS 5 2 7200 20131002233248 20130902233248 50012 isc.org. ...
isc.org.    60      IN    A        149.20...
isc.org.    60      IN    RRSIG    ...
isc.org.    7200    IN    MX       ... mx.pao1.isc.org.
isc.org.    7200    IN    RRSIG    MX 5 2 7200 20131002233248 20130902233248 50012 isc.org. ...
isc.org.    7200    IN    TXT      "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
isc.org.    7200    IN    TXT      "$Id: isc.org,v 1.1845 2013-08-16 16:16:50 dmahoney Exp $"
isc.org.    7200    IN    RRSIG    TXT 5 2 7200 20131002233248 20130902233248 50012 isc.org. J0UV7iIvQn7Pzu/itUN1JH4hLg8bjQo/73kBef/T/yzx/P8t6VX+MYDC ysyXNigSi1JPoWfYt7qu6eXcALQEwJ/Z156Rebefjls4R18wr+BttzWF lCb+zJ7K7o4meckc7ZQr12glAXjij09dr9omYoObWo6/lH76S6N3Er4i xdg=
isc.org.    60      IN    AAAA     2001:4f8:0:2::69
isc.org.    60      IN    RRSIG    AAAA 5 2 60 20131002233248 20130902233248 50012 isc.org. OBWafw6hmgueTvaL06Q3zzpKODW3OIWKxHr3Z30mag1vJW5ECwlkK3xI lPr4A1Rg6SZiJp78yewBWkDB0436cY1uCJ0yzsk9YWlLW/5hScy1ueaH s2tfymZD7UdOh0FuLs05gunsxK2Of3DCG3Zh3cD4FMnu8ju1CuLD2+dU W1U=
isc.org.    7200    IN    NAPTR    20 0 "S" "SIP+D2U" "" _sip._udp.isc.org.
isc.org.    7200    IN    RRSIG    NAPTR 5 2 7200 20131002233248 20130902233248 50012 isc.org. s9cuc6O0e2kgBNffd6dyJyJH1Zm5Wd0pRO1q5aKMc7UsiKFUI7Ml7Q8N VzTqwM/zWh2VzvtV/w1O3IHuSiXBN9k51Loy4WGHJSDcXs865PWjHJwJ jRqfz1bE+LsW/aZD2Ud/iGyhCoQPeZIOcqB6plB+kelf3mGR0bHkdjV+ Zw4=
isc.org.    3600    IN    NSEC     _adsp._domainkey.isc.org. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY SPF
isc.org.    3600    IN    RRSIG    NSEC 5 2 3600 20131002233248 20130902233248 50012 isc.org. K3/RL0nn54FkFvcPnaecG26JjQVCZL1g41zB02YssxZnE/3lX9X4O8uk DrONRd...EeMq51YUy8NBljWAlPOIRYD0lWUMrXuSNHMyGIFwHFIZqNrN CuQUl+24oPQXi3/wWX0TGH5XW9XF2IB+Dc1zdP/5qRHiKCjAnYDNE384 PAQ=
isc.org.    7200    IN    DNSKEY   257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t... 47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SDmsn2e...
isc.org.    7200    IN    DNSKEY   256 3 5 BQEAAAABwuHz9Cem0BJ0JQTO7C/a3M...
isc.org.    7200    IN    RRSIG    DNSKEY 5 2 7200 20131002230127 20130902230127 12892 isc.org. ... Az+B9J8xVz5GGMb8FStEXMYauE9r8Z5G4ZzRZUv619lXYH+Uhha5QUfq IcVYvtOt+QLlwdWV4Kt3fp3m6KveBAnliorPSjOd40PfWZD3CQ4GqVIc EyYai55bKN1hV...
isc.org.    7200    IN    RRSIG    DNSKEY 5 2 7200 20131002230127 20130902230127 50012 isc.org. HFc6EpppK8DieQnYccCLEMuP3uhCFENhY9pwbqcwYh9fVOMMeEim/XSy QIk9FsVGZnXw2SgC946gSXnTkLdaogwibOZLq2oJ0UGbsF2+4SreLIx0 nv6EyJh1...
isc.org.    7200    IN    SPF      "v=spf1 a mx ip4:204.152.184.0/21 ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
isc.org.    7200    IN    RRSIG    SPF 5 2 7200 20131002233248 20130902233248 50012 isc.org. enxTFXMYwtZW9rmS2eZ0svQwlaRJn3whFCblQ2mpqjtT3BxuqpGcvlbC jwjLxNhn89x2Y2//pkN1EPvgwr2yd7lIBoLV9X/VnGCH/sBlNaRtckk2 SE75cuH2L7jkR1D...

;; ADDITIONAL SECTION:
ams.sns-pb.isc.org.    7200    IN    A        199.6.1.30
ams.sns-pb.isc.org.    7200    IN    AAAA     2001:500:60::30
ord.sns-pb.isc.org.    7200    IN    A        199.6.0.30
ord.sns-pb.isc.org.    7200    IN    AAAA     2001:500:71::30
sfba.sns-pb.isc.org.   7200    IN    A        149.20...
sfba.sns-pb.isc.org.   7200    IN    AAAA     2001:4f8:0...
mx.pao1.isc.org.       3600    IN    A        149.20.64.53
mx.pao1.isc.org.       3600    IN    AAAA     2001:4f8:0:2::2b
asterisk.isc.org.      300     IN    A        149.20.32.15
ams.sns-pb.isc.org.    7200    IN    RRSIG    A 5 4 7200 2013100... 50012 isc.org. EyCDO...
ams.sns-pb.isc.org.    7200    IN    RRSIG    AAAA 5 4 7200 20131002233248 20130902233248 50012 isc.org. RFpmtA/CAZOExrl8Pc6tDW38Eoc/xXxtu...534xllKoM77zhGLx6vLRR wiH3Ny1gW++hyj6b6LMDVbBEm7vAMVxrOQVYM5fWtYCF/cN4IHVlti33 /Hgiuk2SSdsZEgeAu57FgxgZIMaO...
ord.sns-pb.isc.org.    7200    IN    RRSIG    A 5 4 7200 20131002233248 20130902233248 50012 isc.org. ...
ord.sns-pb.isc.org.    7200    IN    RRSIG    AAAA 5 4 7200 20131002233248 20130902233248 50012 isc.org. H5eByfYUHm4c8V12auNIl1QhQL4UA9MV9w1wQPJiU/Rtxbfvvrl3rlVj uIUP6v4R5NVO3lad7bsNPb9xMou1qOC5FL9fn0MVFqU+qCwQ7GIRxyA6 fQaFKBNrOL6iiVbC6LbE+2uZPR...
sfba.sns-pb.isc.org.   7200    IN    RRSIG    A 5 4 7200 20131002233248 20130902233248 50012 isc.org. sr0nh5ZbxmbnGaduo4ri1tHpPR4+D0Mf4WpEjzu21+iEBkgc3M1XdYCT gCpd8JRCEcz+glu8wXQI5+29mUrK3QwPCIWJNx/AKol7TbIPxrYoKCiv pZv7yTwO2bC1SGfcNXZAm5UuKU0jl7jel...

;; Query time: 35 msec
;; SERVER: 2001:4f8:0:2::19#53(2001:4f8:0:2::19)
;; WHEN: Wed Sep  4 11:14:01 2013
;; MSG SIZE  rcvd: 4077
```

Query for isc.org/ANY

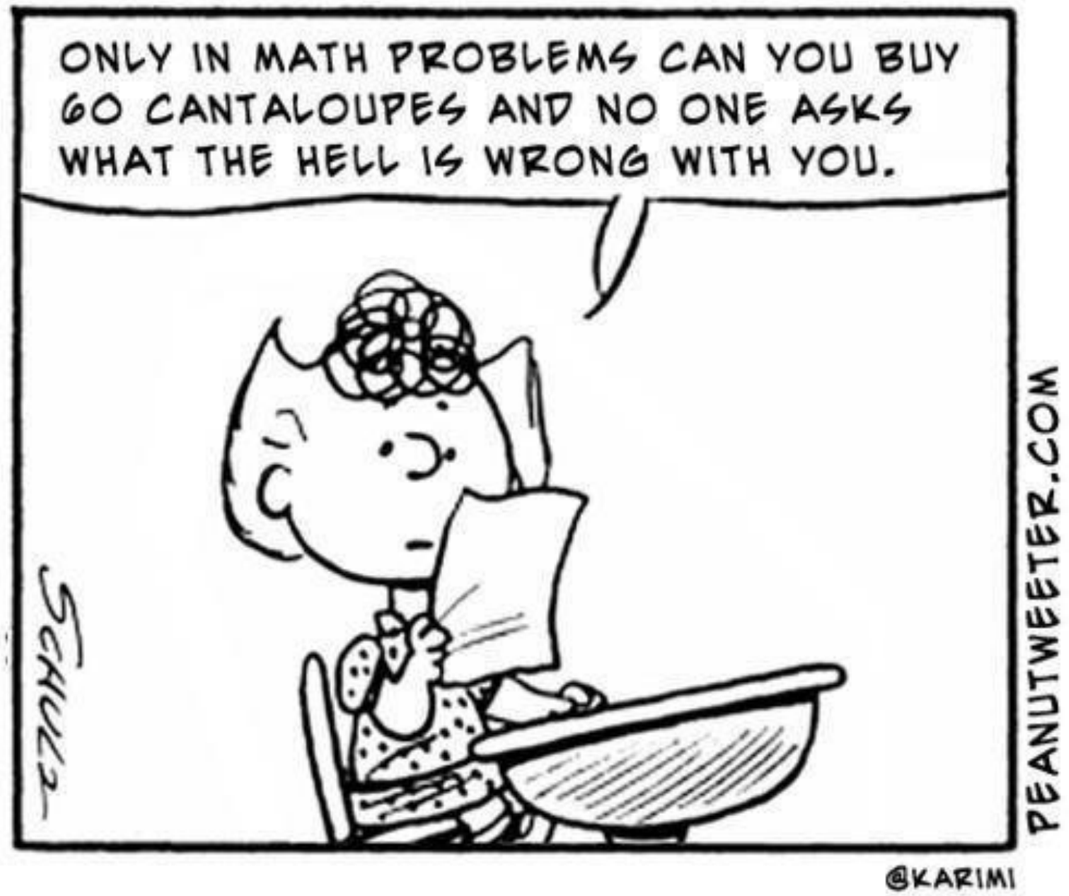
44 bytes sent, 4077 bytes received

~93x amplification!

 |

A Little Math

- Say each bot has a measly 1 Mbps connection to the Internet
  - It can send 1Mbps/44B =~ 2909 qps
  - That generates 2909 pps * 4077B =~ 93 Mbps
- So 11 bots > 1 Gbps



Case Study: The Mirai Botnet's DDoS Attack on Dyn's Name Servers

Mirai Botnet

- Consists of compromised "Internet of Things" (IoT) devices
  - IP CCTV cameras
  - Digital video recorders
- Previously used in a DDoS attack against *krebsonsecurity.com*
  - Peaked at 620 Gbps
  - Used GRE traffic

Case Study: The Mirai Botnet's DDoS Attack on Dyn's Name Servers

Impact

- Hurled traffic at Dyn's name servers
  - Said to peak at **1.2 Tbps**
  - Unclear whether it was junk traffic (e.g., SYN, GRE) or legitimate DNS queries
  - Name servers rendered unresponsive
- High-profile Dyn customers impacted
  - Read: the Web

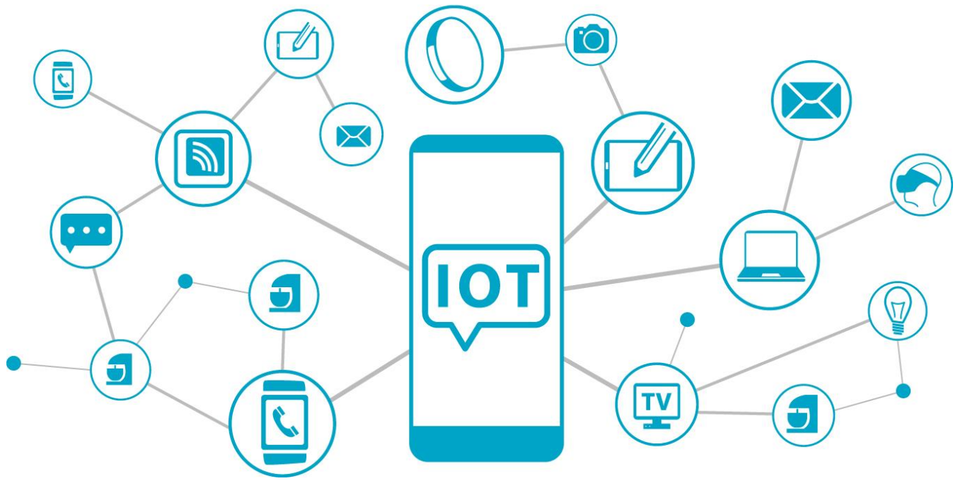
How Did It Happen?

- Mirai botnet estimated to include ~1.5 million IoT devices
- Many IoT devices in the botnet ship with a default password
  - In some cases, the default password cannot be changed easily, or at all
- Mirai source code was released publicly in early October

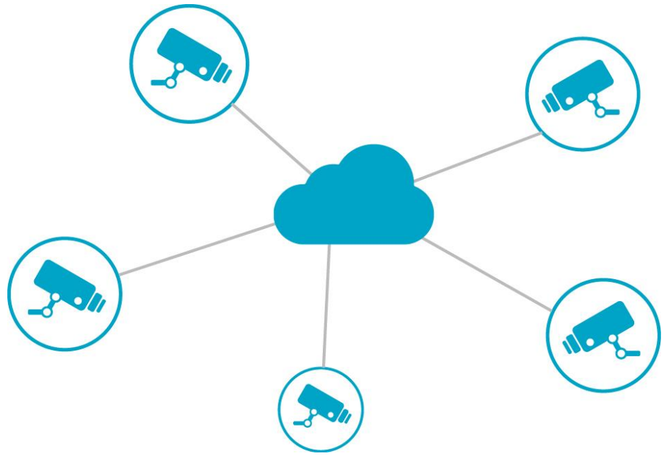
 |

IoT Devices: Easy to Build a Big, Powerful Botnet

- IoT devices are cheap & plentiful
  - Because they're cheap, manufacturers skimp on security



- Some require high bandwidth
  - Such as IP CCTV cameras
- Some must be accessible over the Internet
  - Such as IP CCTV cameras
  - And are therefore easily targeted

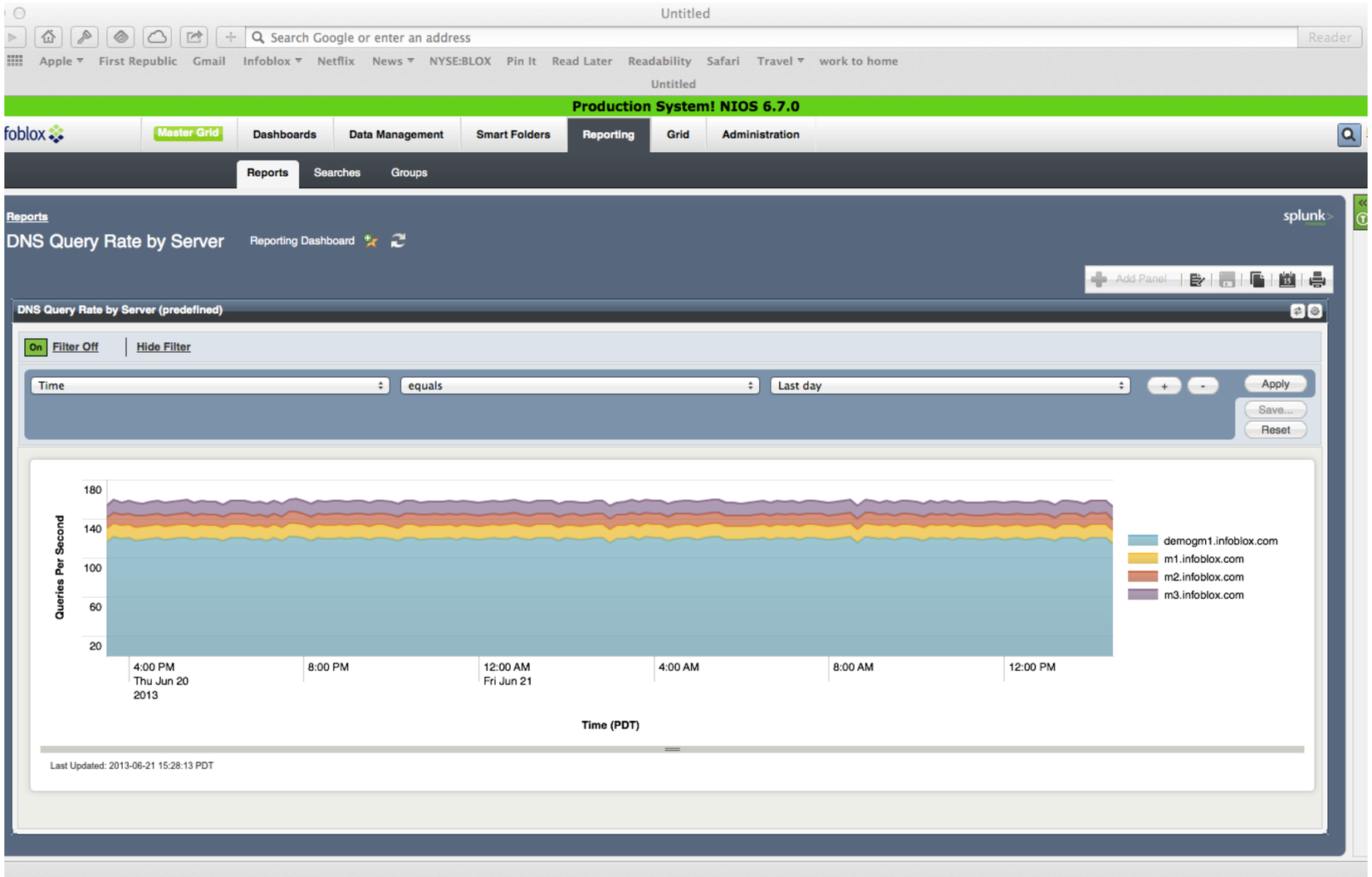


 |

Solution: Monitoring DNS Traffic

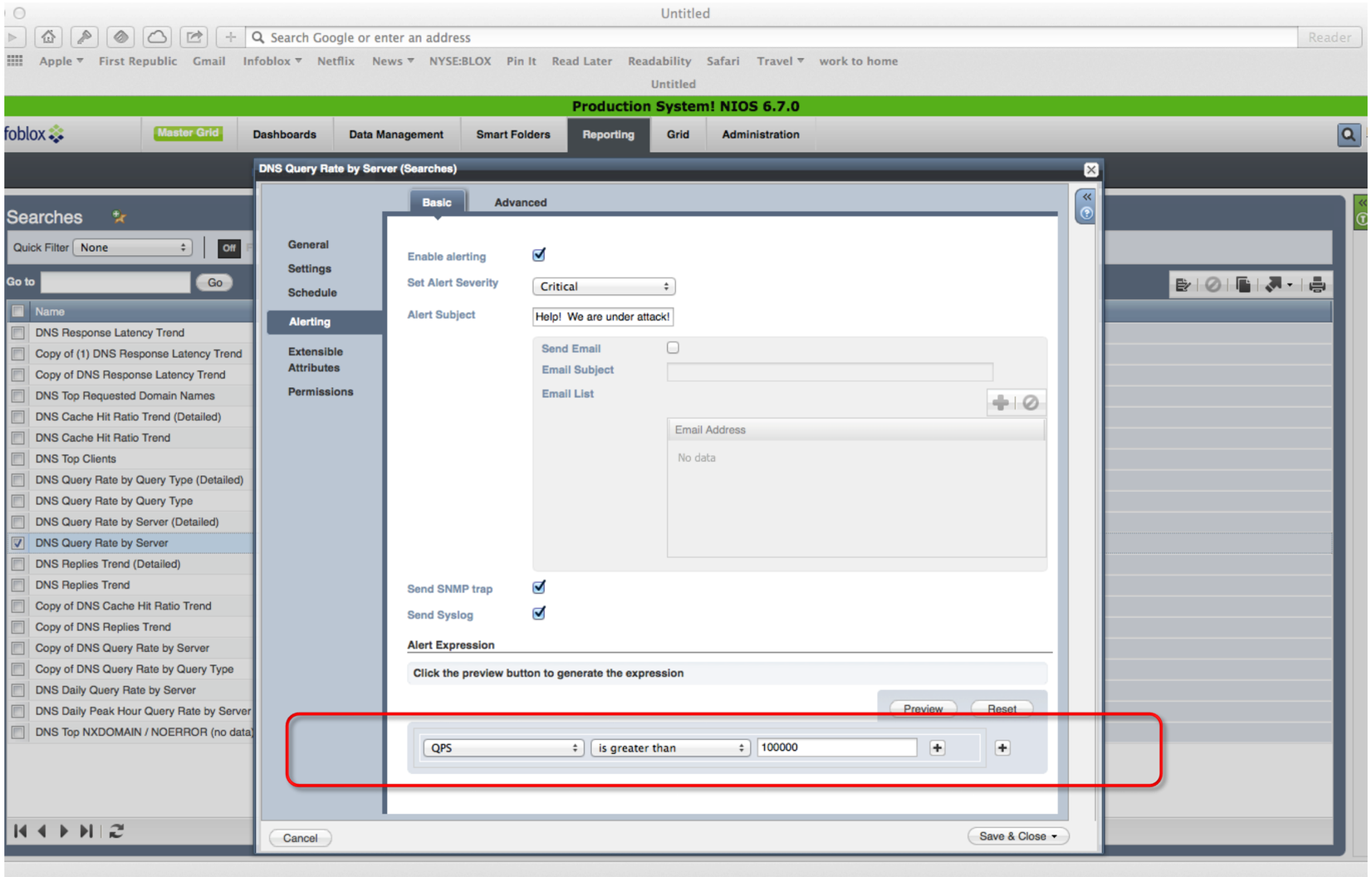
- Monitor traffic to your name servers, including
  - Aggregate query rate
  - Top queriers

Monitoring Aggregate Query Rate



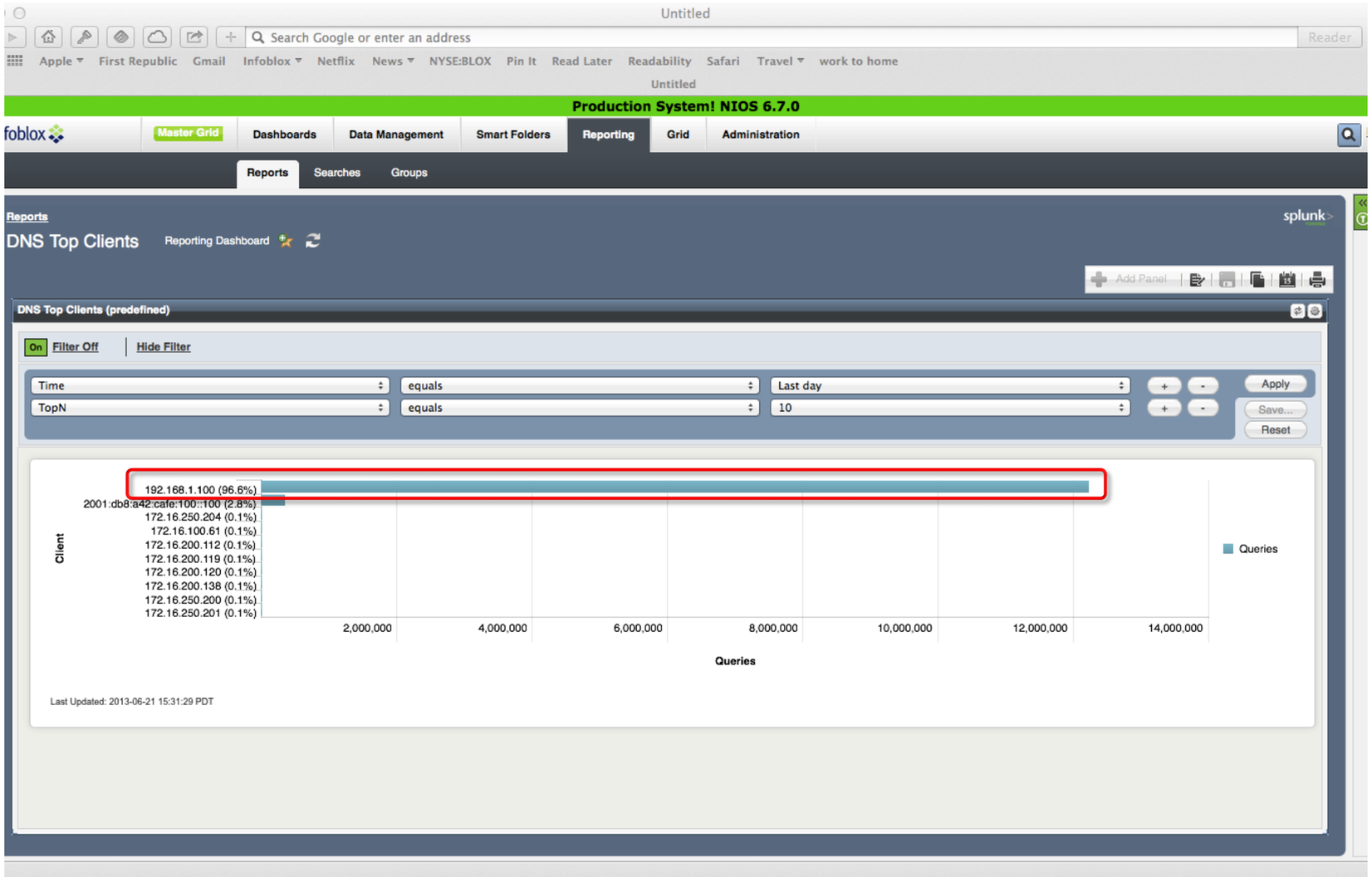
 |

Setting an Alert on Aggregate Query Rate



 |

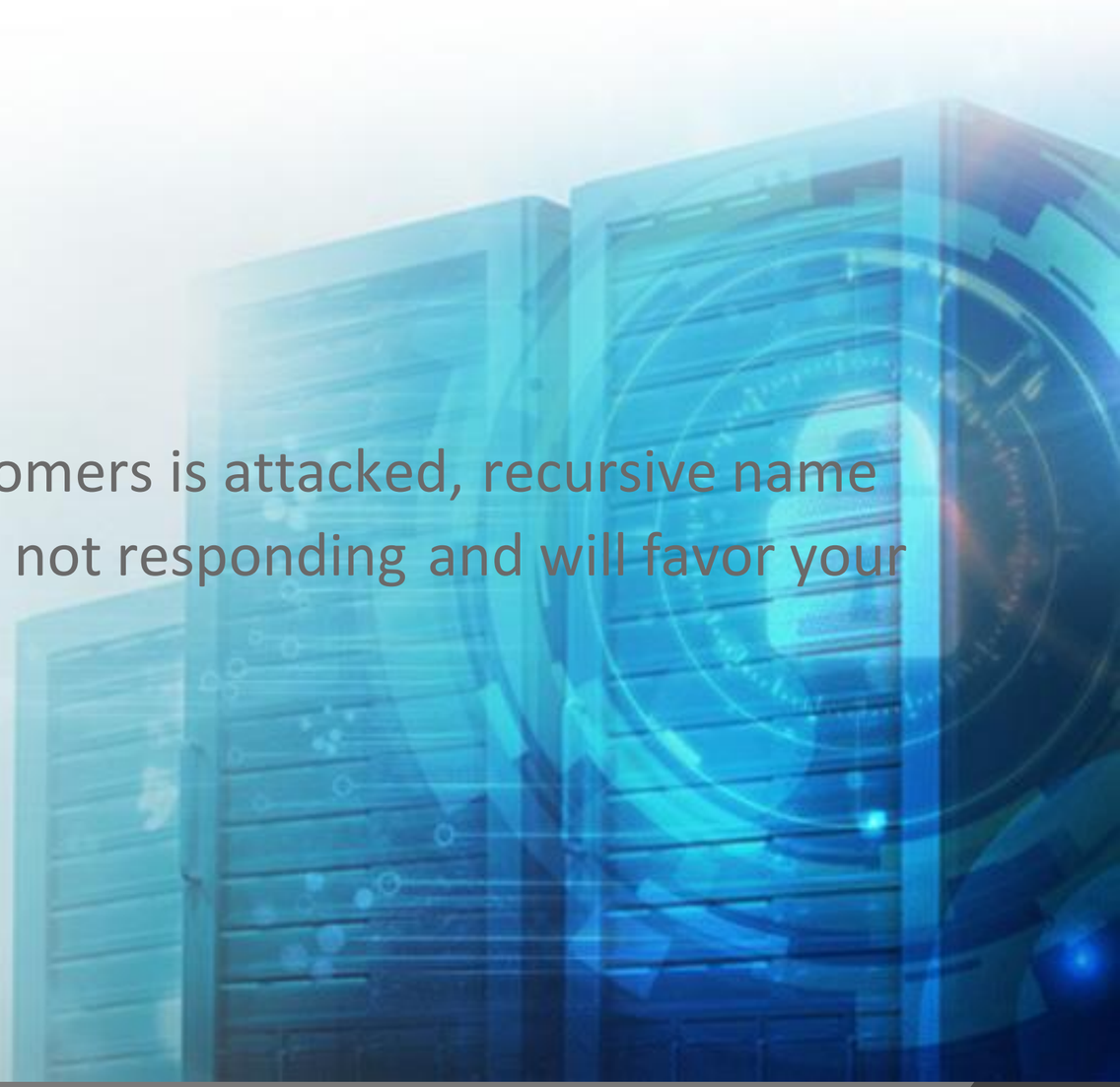
Monitoring Top Clients



 |

Solution: Authoritative Diversity

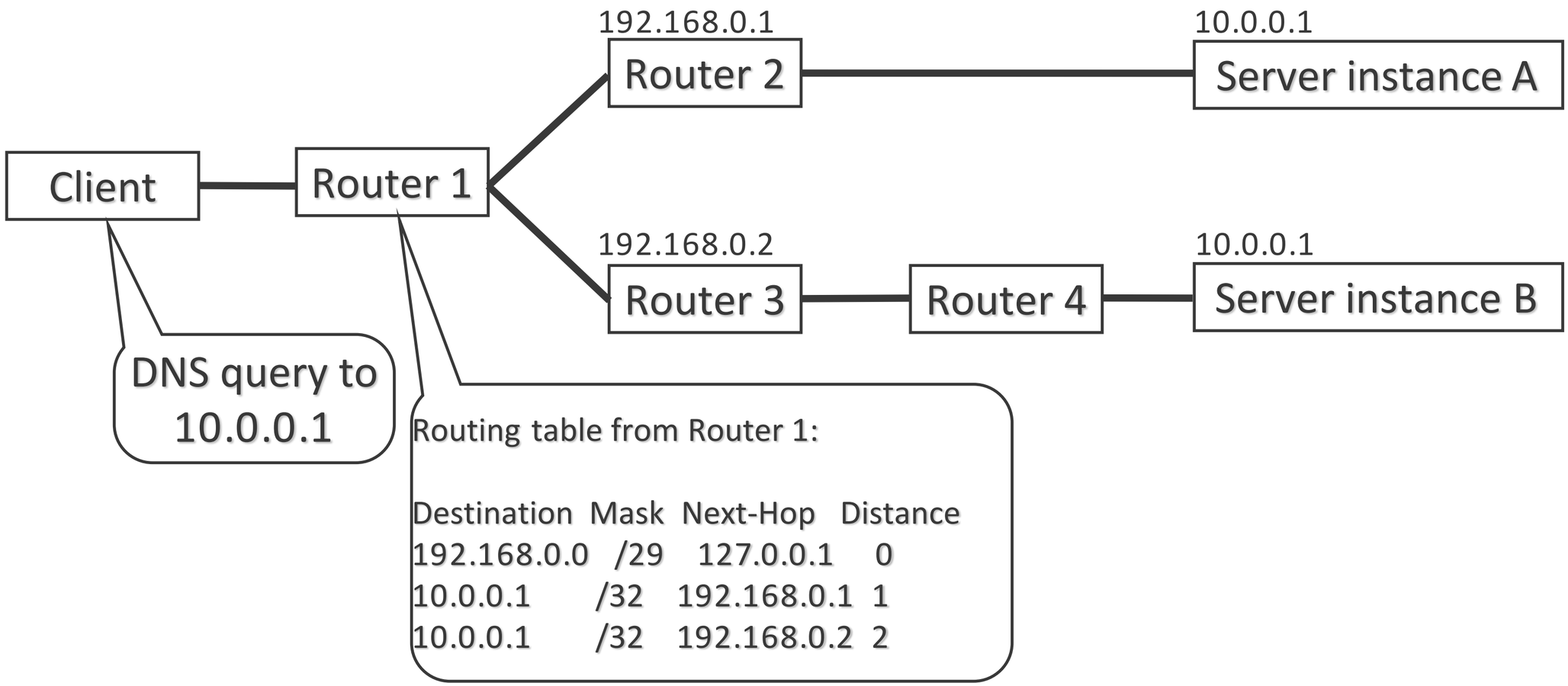
- Use a mixed set of authoritative name servers
  - On-premises name servers
  - Hosted name servers
  - If your DNS hosting provider or one of its customers is attacked, recursive name servers on the Internet will notice that they're not responding and will favor your on-premises name servers
- But beware proprietary features!
  - For example, load balancing



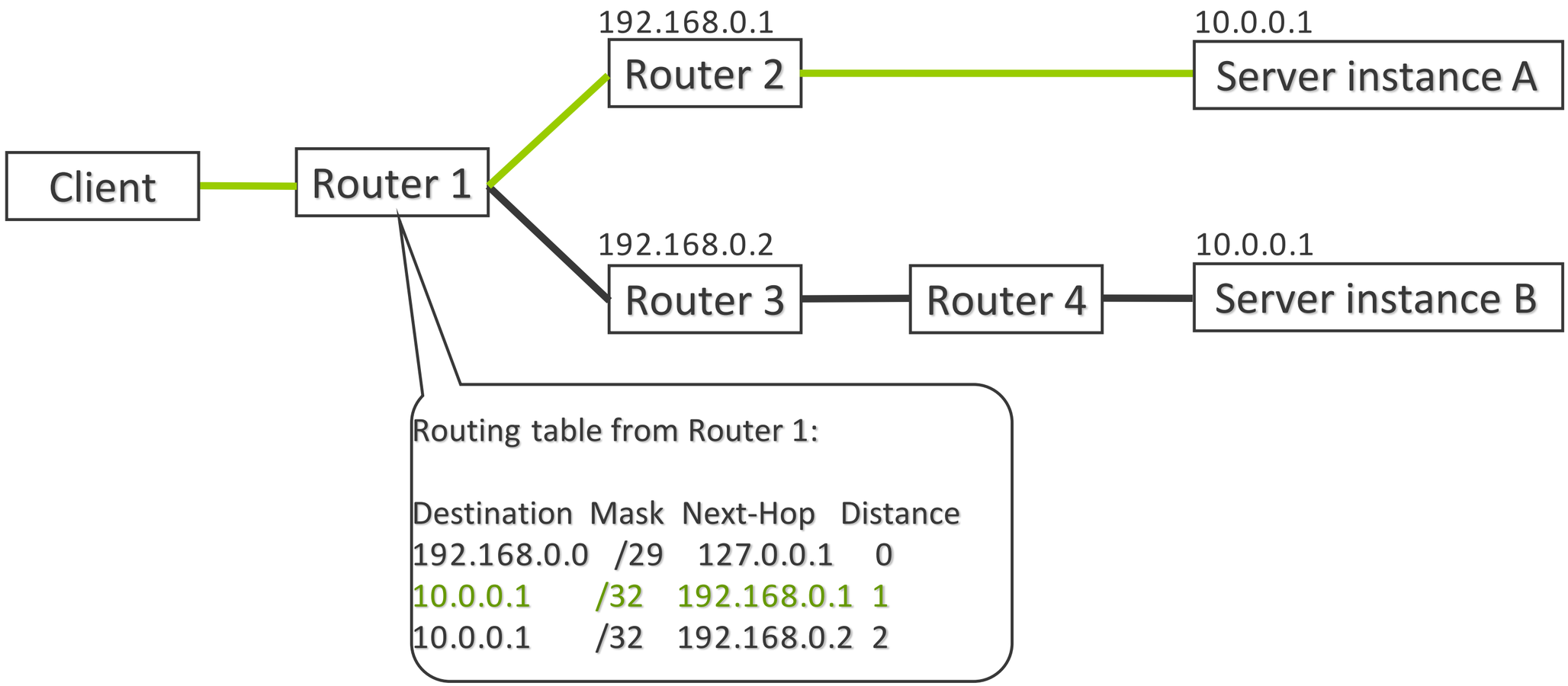
Solution: Anycast

- Anycast allows multiple, distributed name servers to share a single virtual IP address
- Each name server advertises a route to that address to its neighbors
- Queries sent to that address are routed to the closest name server instance

Anycast in Action



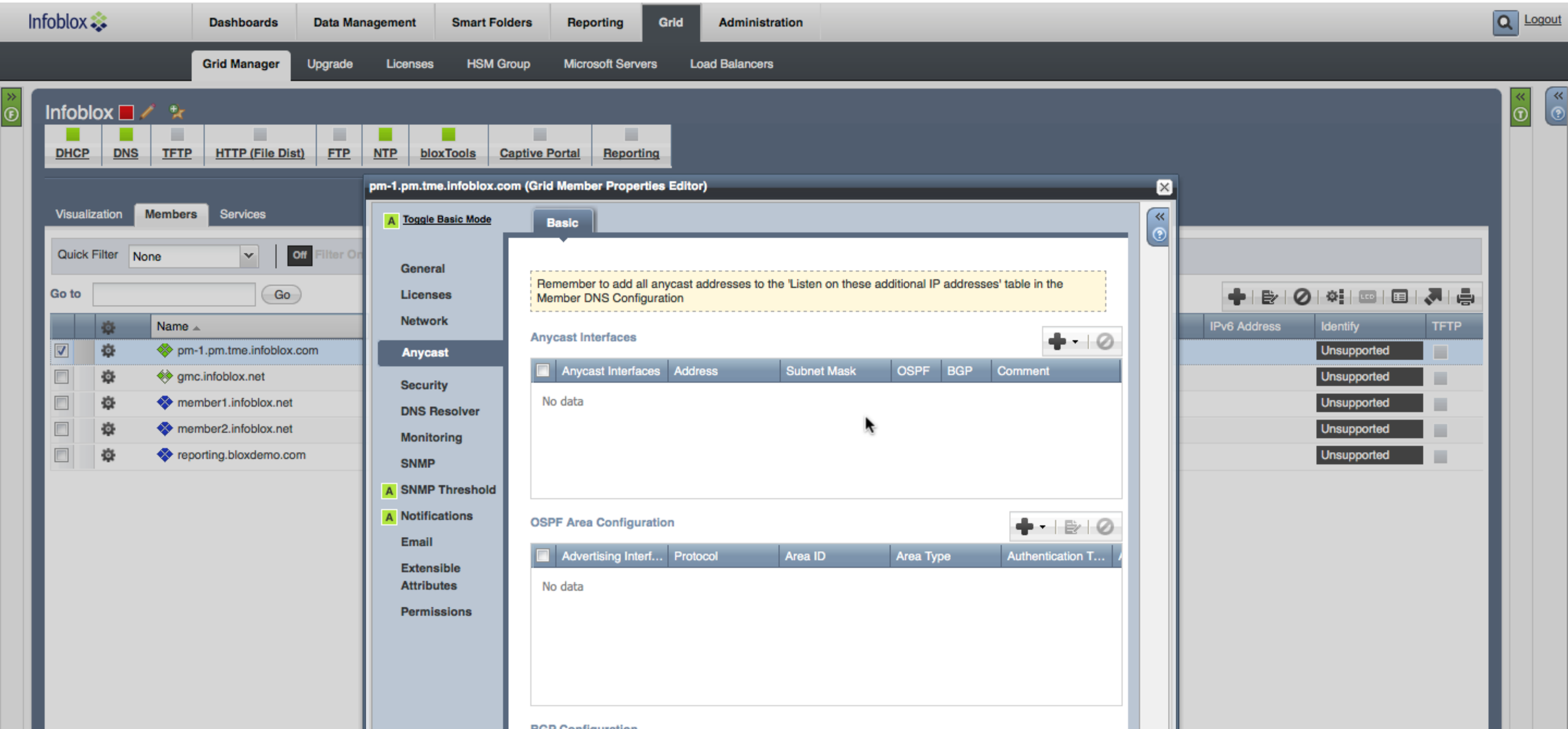
Anycast in Action



How Does Anycast Address DDoS?

- From any one location on the Internet, you can only see (and hence attack) a single member of an anycast group at once
- If you succeed in taking out that replica, routing will shift traffic to another
  - The first replica will probably recover
  - It's like Whac-A-Mole

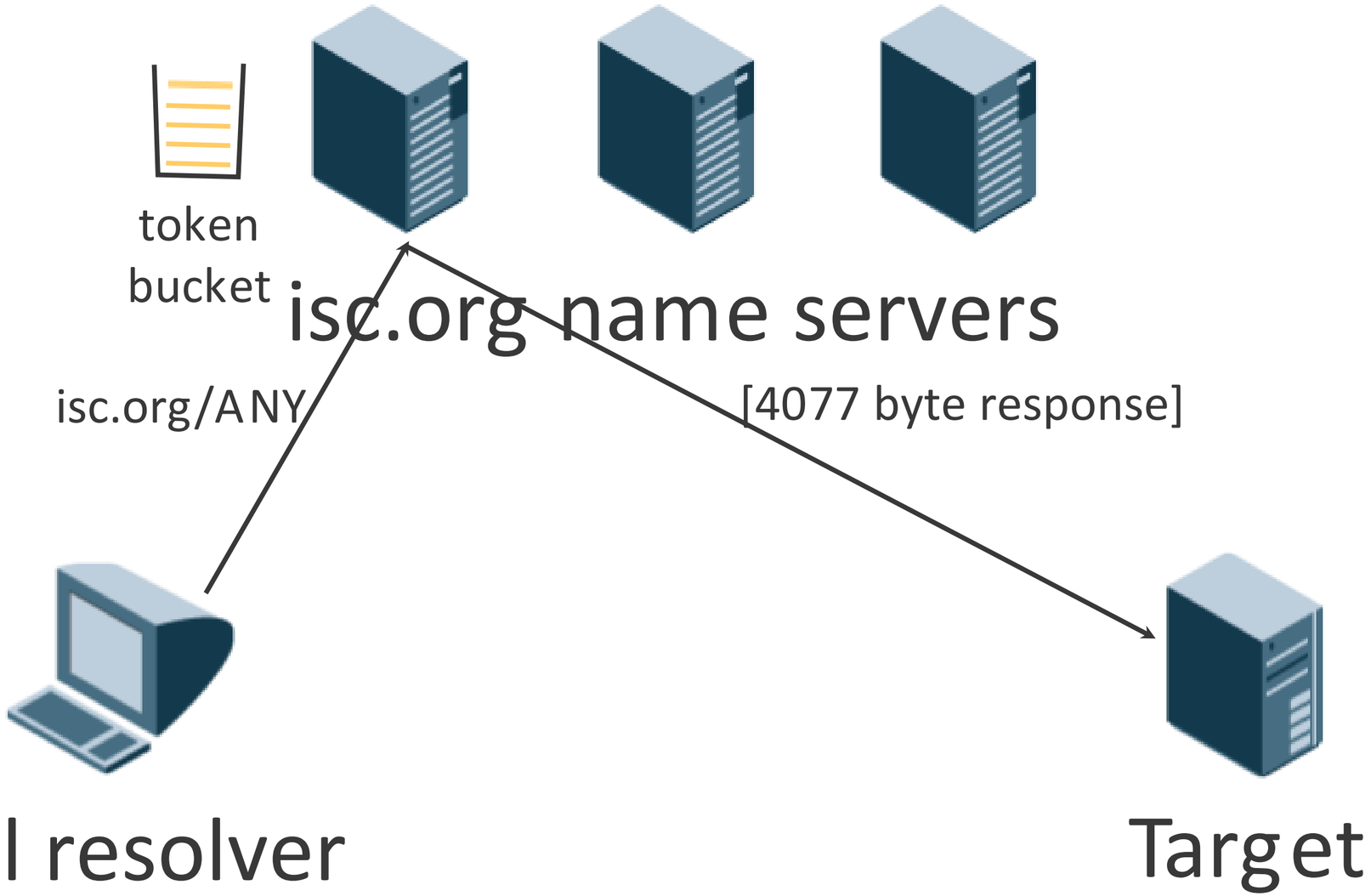
Anycast Made Easy



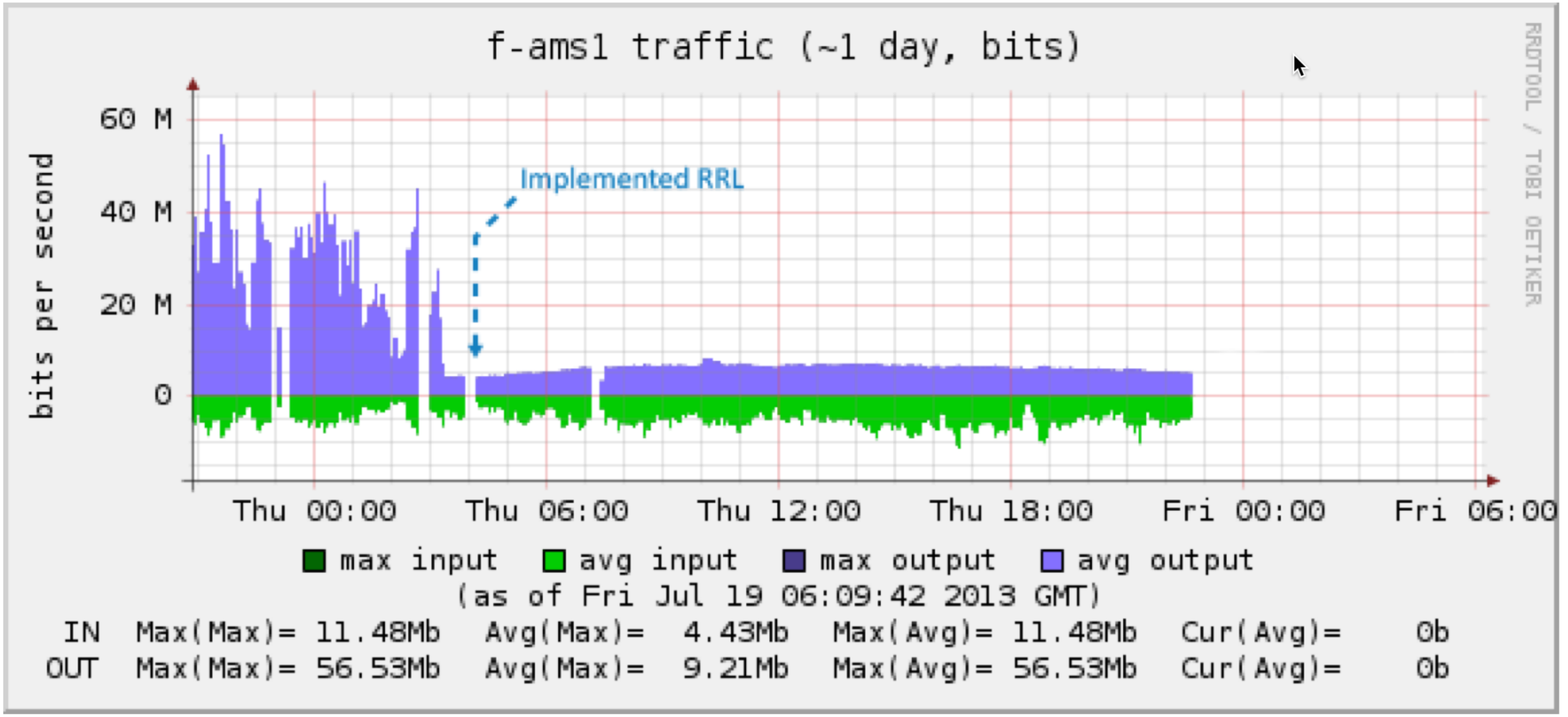
Solution: Response Rate Limiting

- Originally a patch to BIND 9 by Paul Vixie and Vernon Schryver
  - Now included in BIND 9, other name servers
- Applies to authoritative name servers used in DDoS attacks against others
- Prevents these name servers from sending the same response to the same client too frequently

How RRL Works



ISC F-Root


f-ams1 traffic (~1 day, bits)
bits per second
60 M
40 M
20 M
0
Implemented RRL
Thu 00:00
Thu 06:00
Thu 12:00
Thu 18:00
Fri 00:00
Fri 06:00
max input
avg input
max output
avg output
(as of Fri Jul 19 06:09:42 2013 GMT)
IN Max(Max)= 11.48Mb Avg(Max)= 4.43Mb Max(Avg)= 11.48Mb Cur(Avg)= 0b
OUT Max(Max)= 56.53Mb Avg(Max)= 9.21Mb Max(Avg)= 56.53Mb Cur(Avg)= 0b
RRDTOOL / TOBI OETIKER

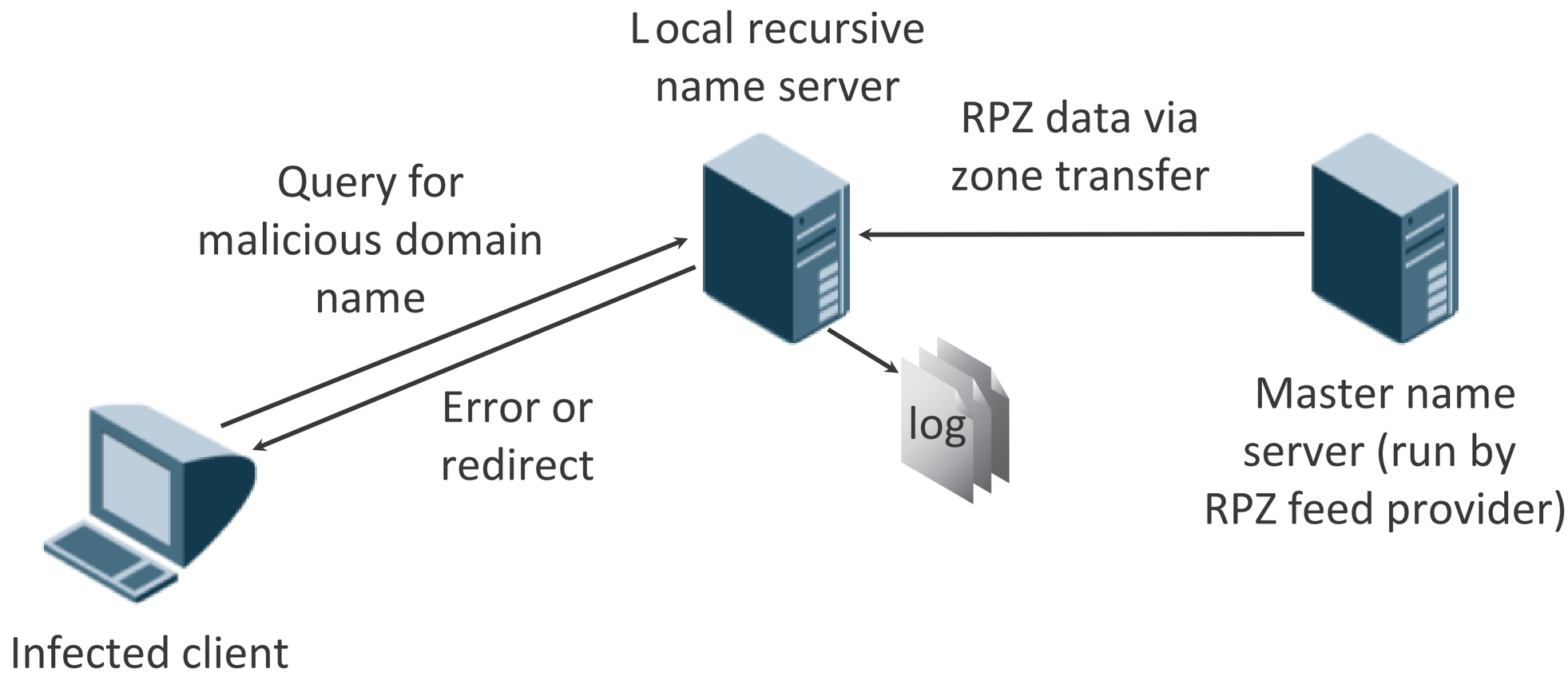
Threat: Malware *Uses* DNS

- Malware infects clients when they visit malicious web sites, whose names are resolved using DNS
- Malware then uses DNS to evade detection
  - Resolving compiled-in lists of domain names until it finds an active command-and-control server
  - Resolving domain names synthesized by a domain generation algorithm until it finds an active command-and-control server
- Malware can then use DNS as a covert communications channel
  - As a bidirectional command-and-control channel
  - As a channel to download new malicious code
  - As a channel to exfiltrate valuable data

Solution: Response Policy Zones

- Many organizations on the Internet track malicious activity
  - They know which web sites are malicious
  - They know which domain names malware look up to rendezvous with command-and-control servers
- Response Policy Zones are funny-looking zones that embed rules instead of records
  - The rules say, “If someone looks up a record for this [malicious] domain name, or that points to this [malicious] IP address, do this.”
  - This is generally “return an error” or “return the address of this walled garden” instead

How Response Policy Zones Work



Case Study: WanaCrypt0r

- Background
  - Also called WannaCry and WannaCrypt
  - SMB vulnerability stolen from NSA by ShadowBrokers
  - Microsoft issues patch MS17-010 on March 14
  - WanaCrypt0r worm released May 12
  - Major effects on Telefonica and Britain's NHS

Case Study: WanaCrypt0r

- The Worm
  - Initial infection vector unknown
  - Spreads using SMB vulnerability and exploiting previously backdoored computers
  - Checks for web server at *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*
    - Initially, "kill switch" domain name did not exist on the Internet
  - Connects to a command-and-control server via TOR
  - Similarities between the code and previous malware implicates Lazarus Group
  - Lazarus attacked Sony after the release of *The Interview*

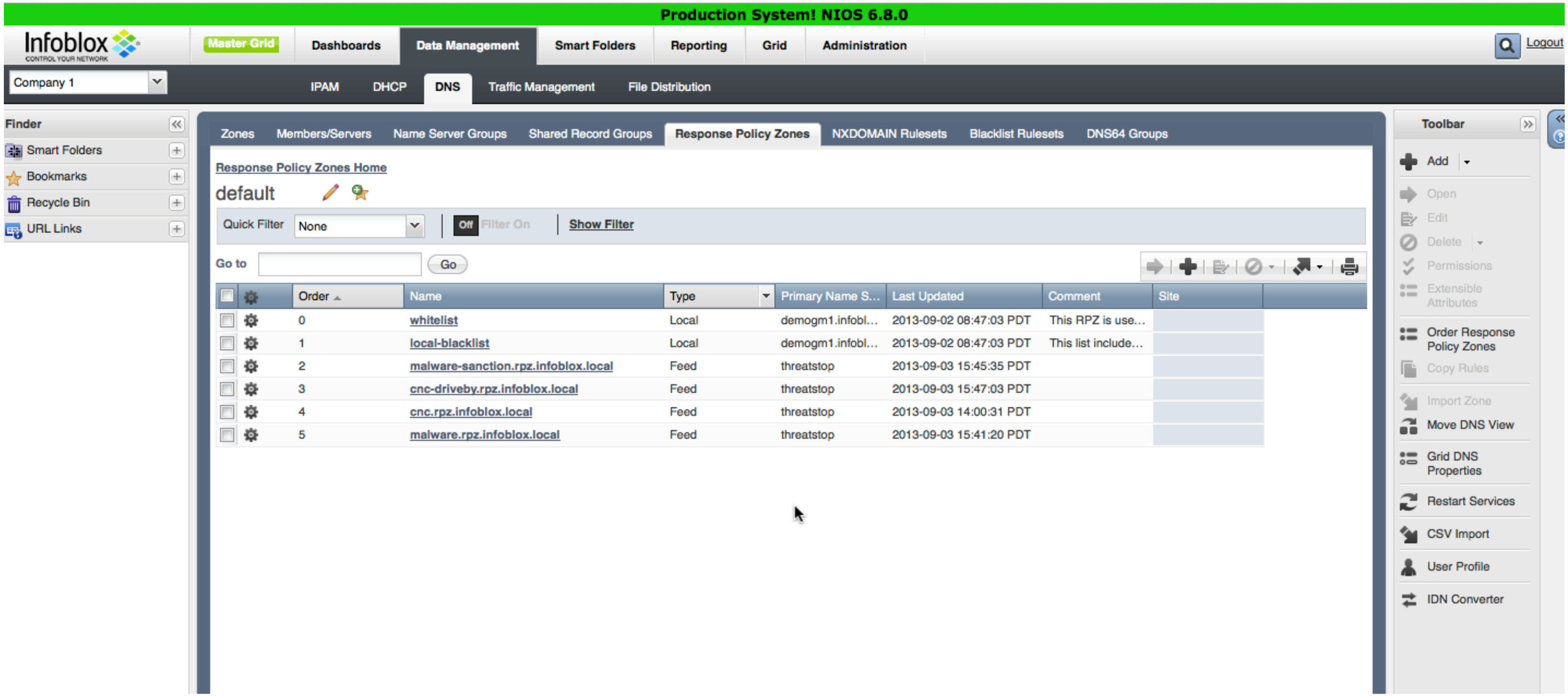
Case Study: WanaCrypt0r

- Detection and mitigation using DNS
  - Initially, "kill switch" domain name did not exist on the Internet
    - @MalwareTechBlog (yay!) noticed queries to this domain name and registered it
    - WanaCrypt0r stopped encrypting
  - Query logging
    - Quickly identify internal infected hosts
  - Response Policy Zones
    - Set up internal web server just to log access
    - Answer queries for kill switch domain name with internal web server's IP address
    - Quickly identify and neuter internal infected hosts

Where Do I Get One of These Newfangled RPZ Feeds?

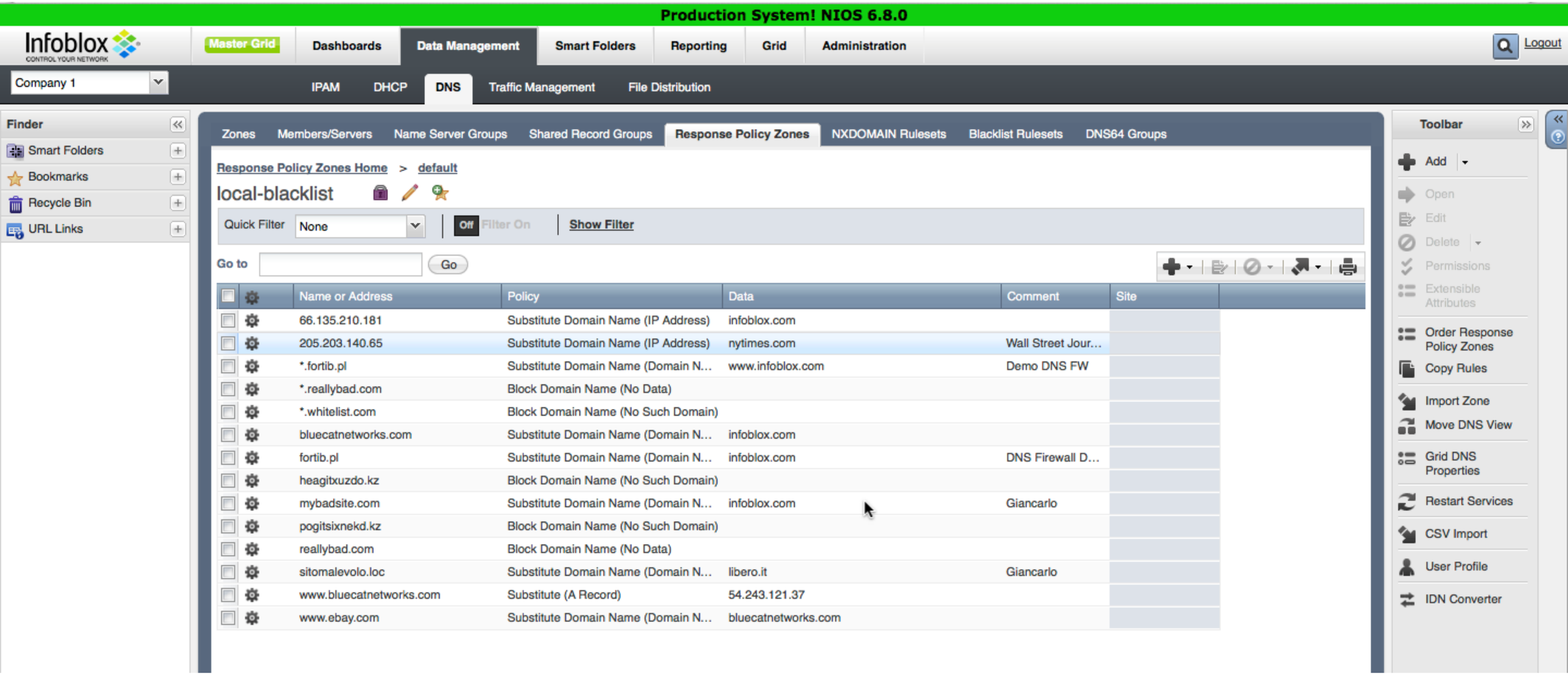
- From Infoblox!
- From a provider such as Spamhaus or SURBL
- From a commercial provider such as Farsight Security

Managing Response Policy Zones



 |

Managing Response Policy Zones (continued)

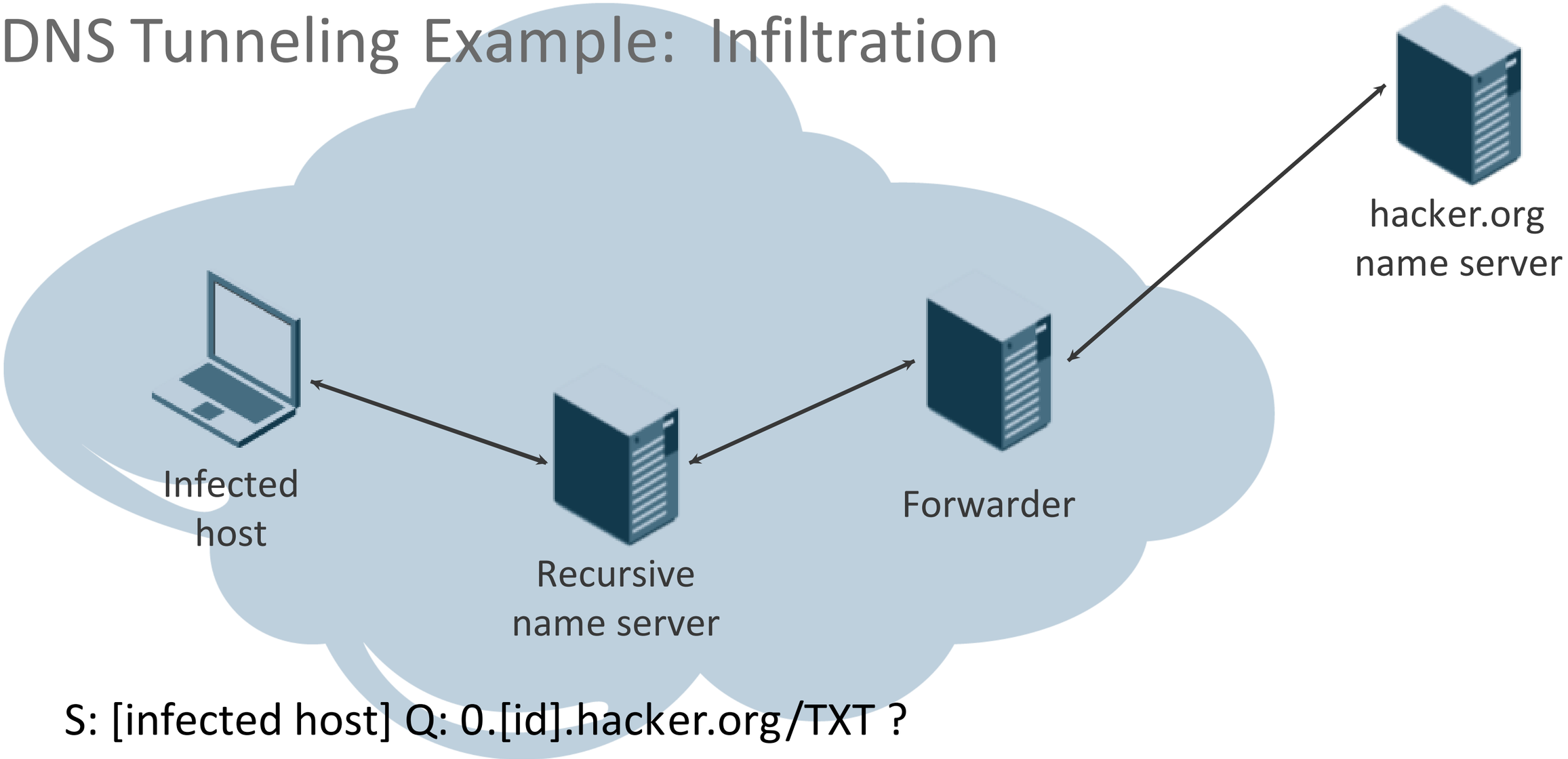


 |

Threat: DNS Tunneling

- Tunneling data surreptitiously into or out of a network using DNS as a vector
  - This is often effective because
    - DNS is generally allowed into and out of an organization (e.g., you can look up Internet domain names from inside the network)
    - DNS queries and responses are usually poorly monitored
  - Can be used
    - As a command and control channel for a botnet
    - To download new code to existing malware
    - To exfiltrate data from the internal network to a drop server

DNS Tunneling Example: Infiltration



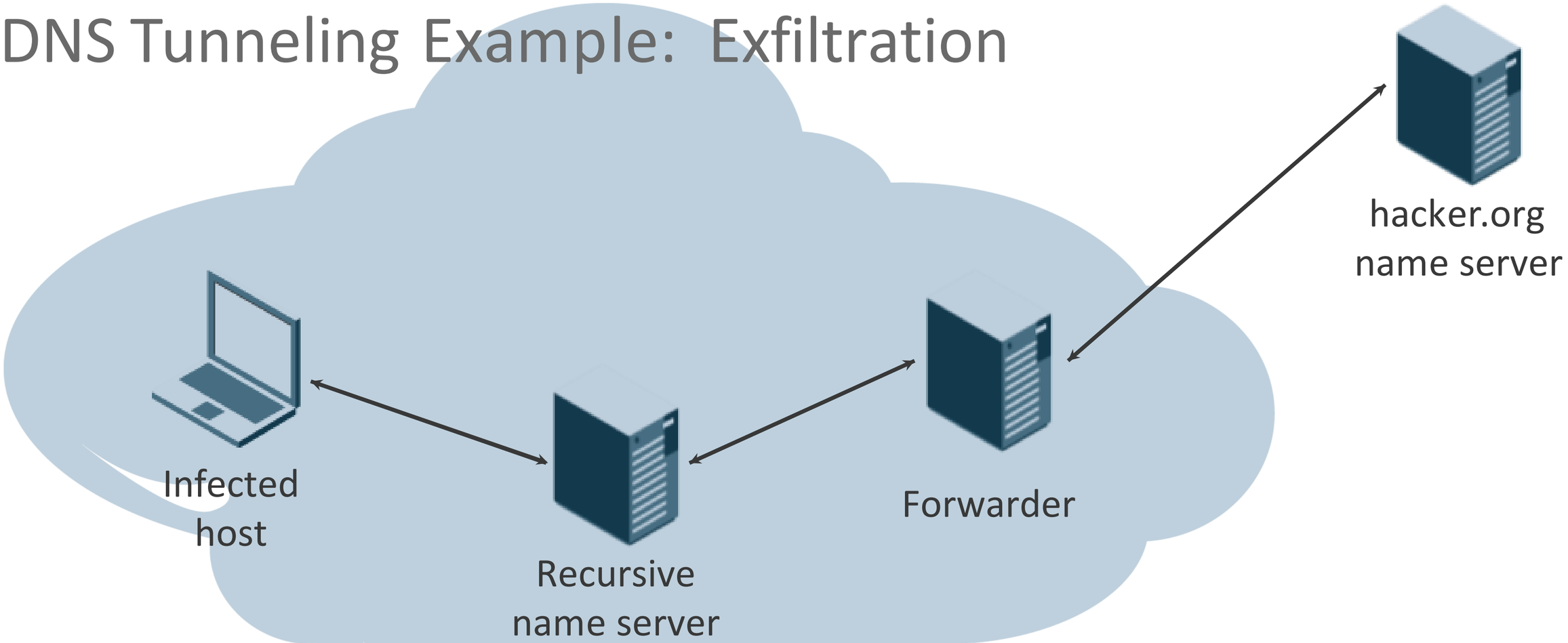
S: [infected host] Q: 0.[id].hacker.org/TXT ?

D: [infected host] A: 0.[id].hacker.org TXT “0.[base-64-encoded data]”

0.[id].hacker.org TXT “1.[base-64-encoded data]”

...

DNS Tunneling Example: Exfiltration



S: [infected host] Q: 0.[base-32-encoded data].[id].hacker.org/A ?

D: [infected host] A: NXDOMAIN

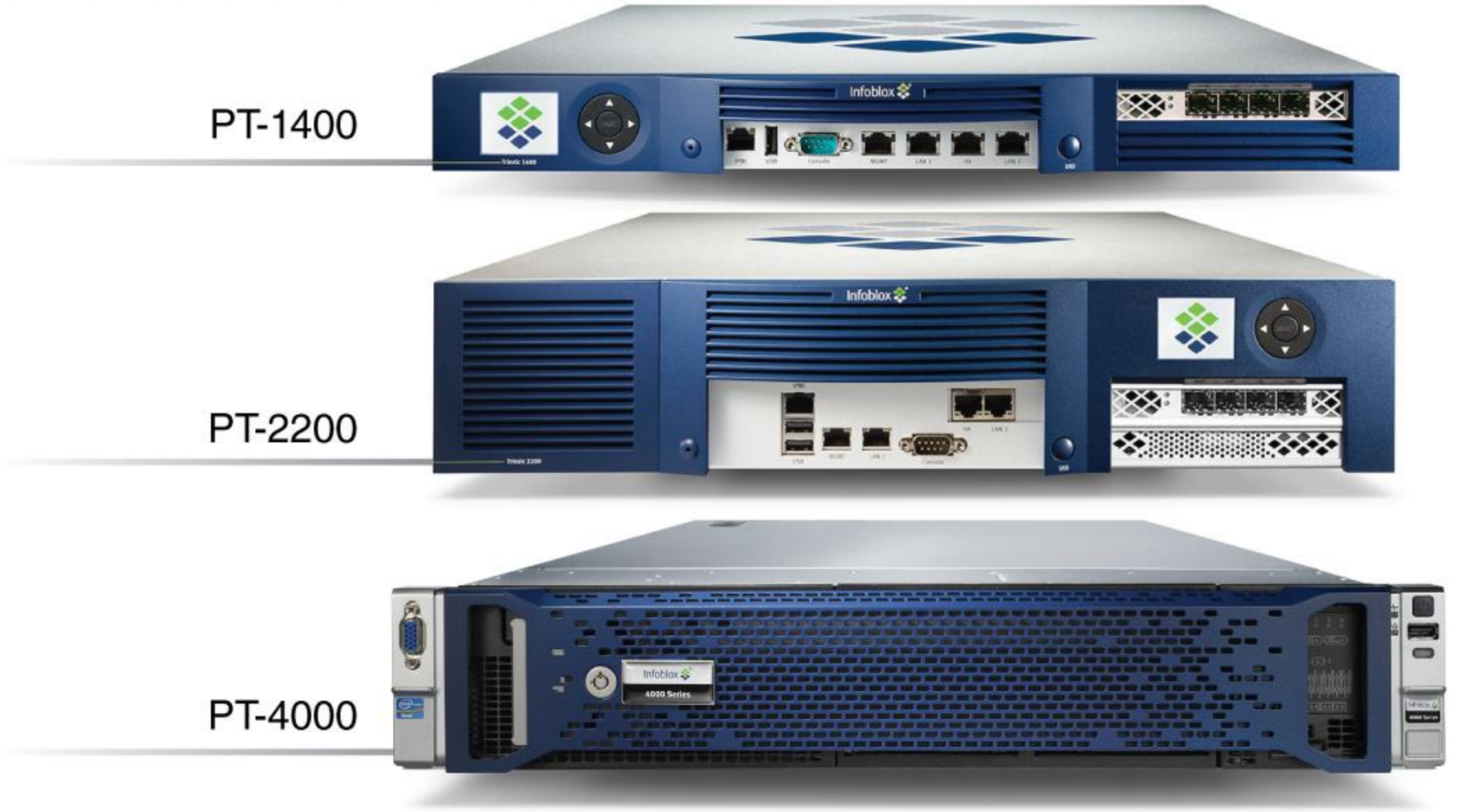
S: [infected host] Q: 1.[base-32-encoded data].[id].hacker.org/A ?

D: [infected host] A: NXDOMAIN

Sound Complicated to Implement?

- OzymanDNS: http://dankaminsky.com/2004/07/29/51/
- Iodine: http://code.kryo.se/iodine
- Dns2tcp: http://www.hsc.fr/ressources/outils/dns2tcp
- NSTX: http://savannah.nongnu.org/projects/nstx
- Squeeza: http://www.sensepost.com
- Heyoka: http://heyoka.sourceforge.net

Infoblox Advanced Appliances

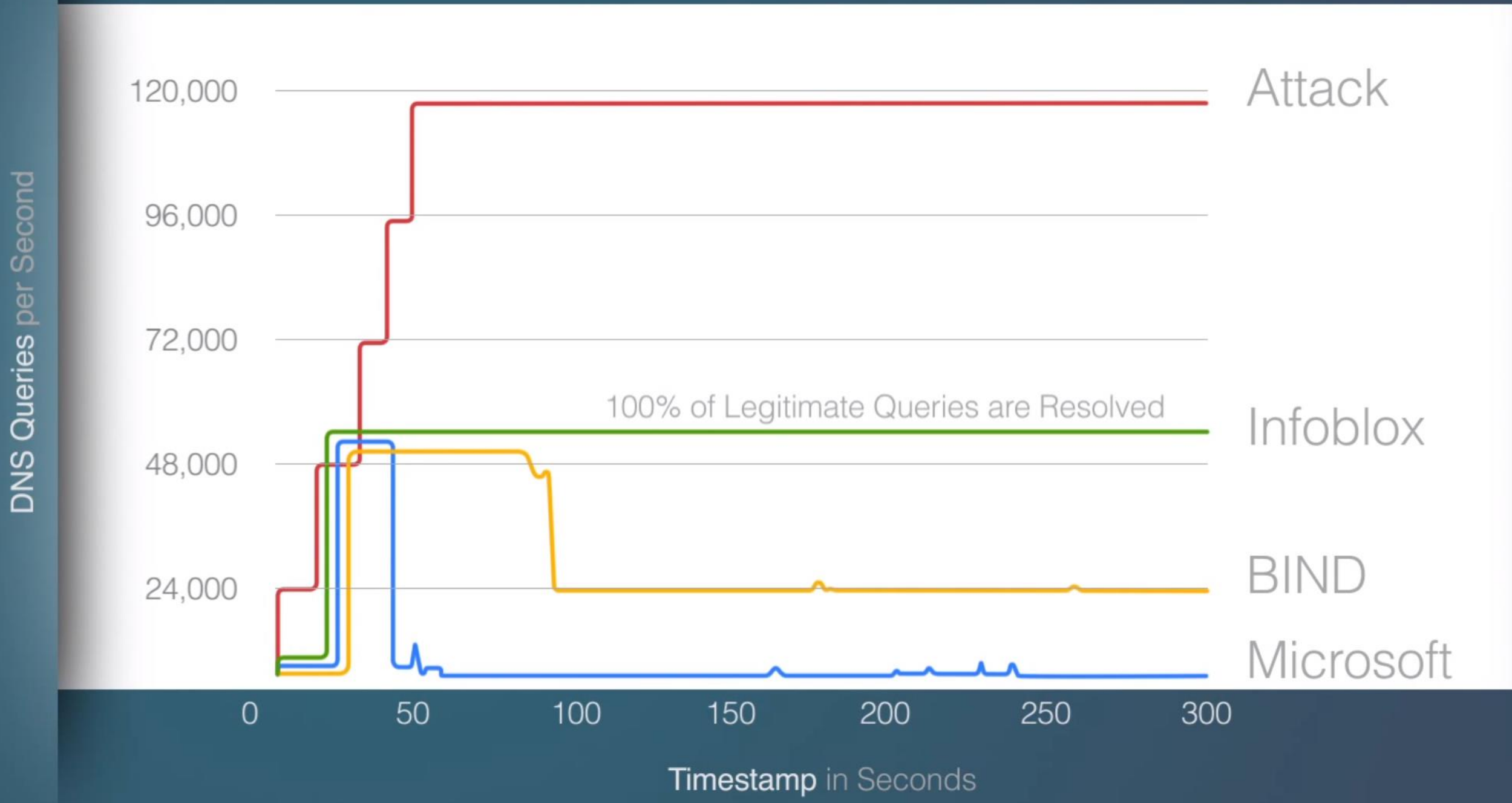


Advanced Appliances include next-generation programmable processors for deep packet inspection

Infoblox Advanced Appliances

- Infoblox Advanced Appliances use heuristics to detect, report and thwart DNS tunneling
  - "Hmm, that's a lot of queries for TXT records."
  - "Those are interesting-looking domain names you're looking up."
- They also help combat
  - Cache poisoning
  - DDoS attacks
  - Malformed DNS messages
- And they're updated automatically to respond to new threats

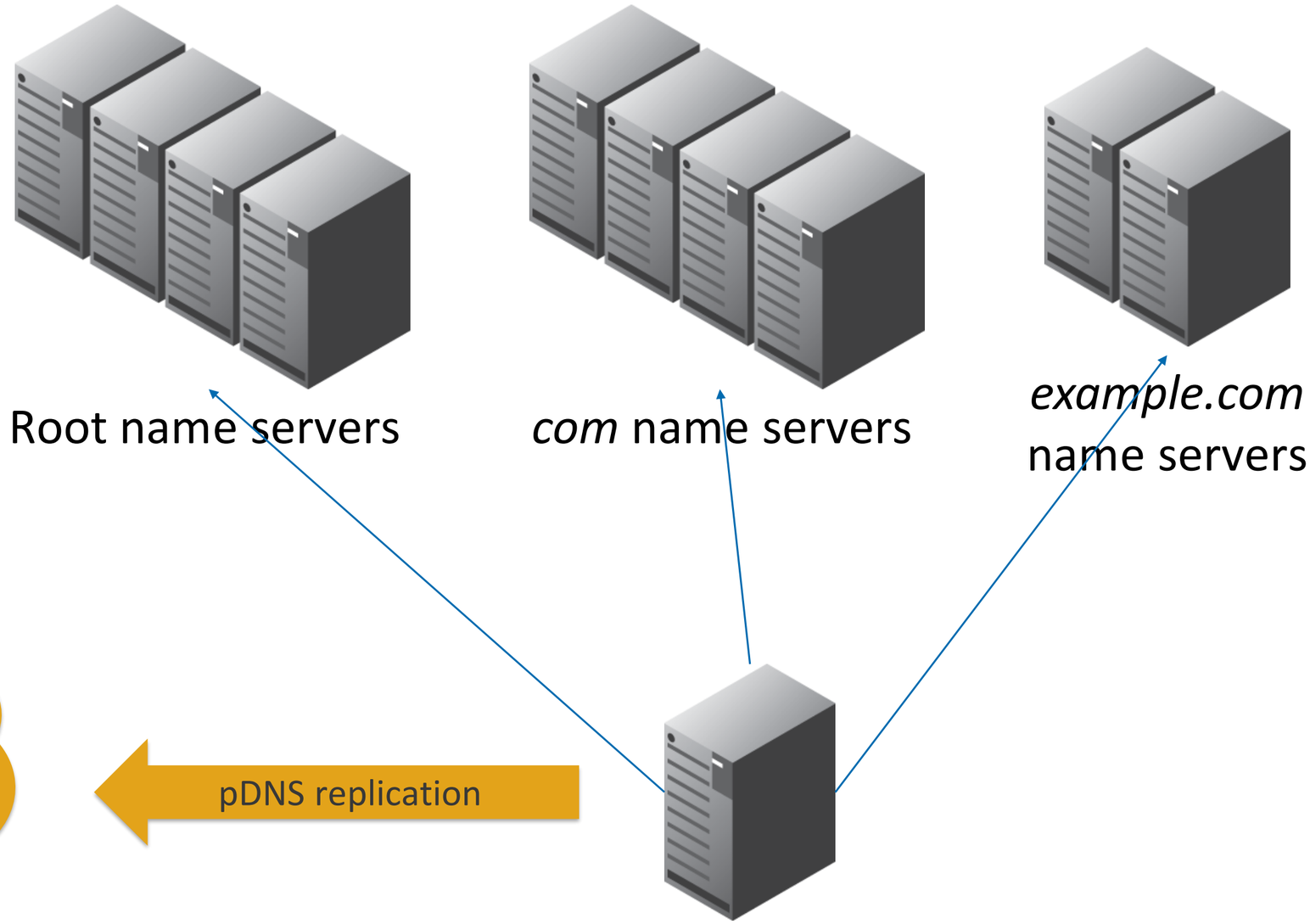
DNS Attack


DNS Queries per Second
120,000
96,000
72,000
48,000
24,000
100% of Legitimate Queries are Resolved
Attack
Infoblox
BIND
Microsoft
0
50
100
150
200
250
300
Timestamp in Seconds

Analytics in the Cloud

- There's a limit to an individual name server's ability to detect malicious activity
  - Limited visibility into DNS traffic (i.e., only *some* of *one* organization's traffic)
  - Limited time window (i.e., only current DNS traffic plus a cache of a few hours)
- To do a better job, we need to
  - Aggregate traffic and
  - Store it longer

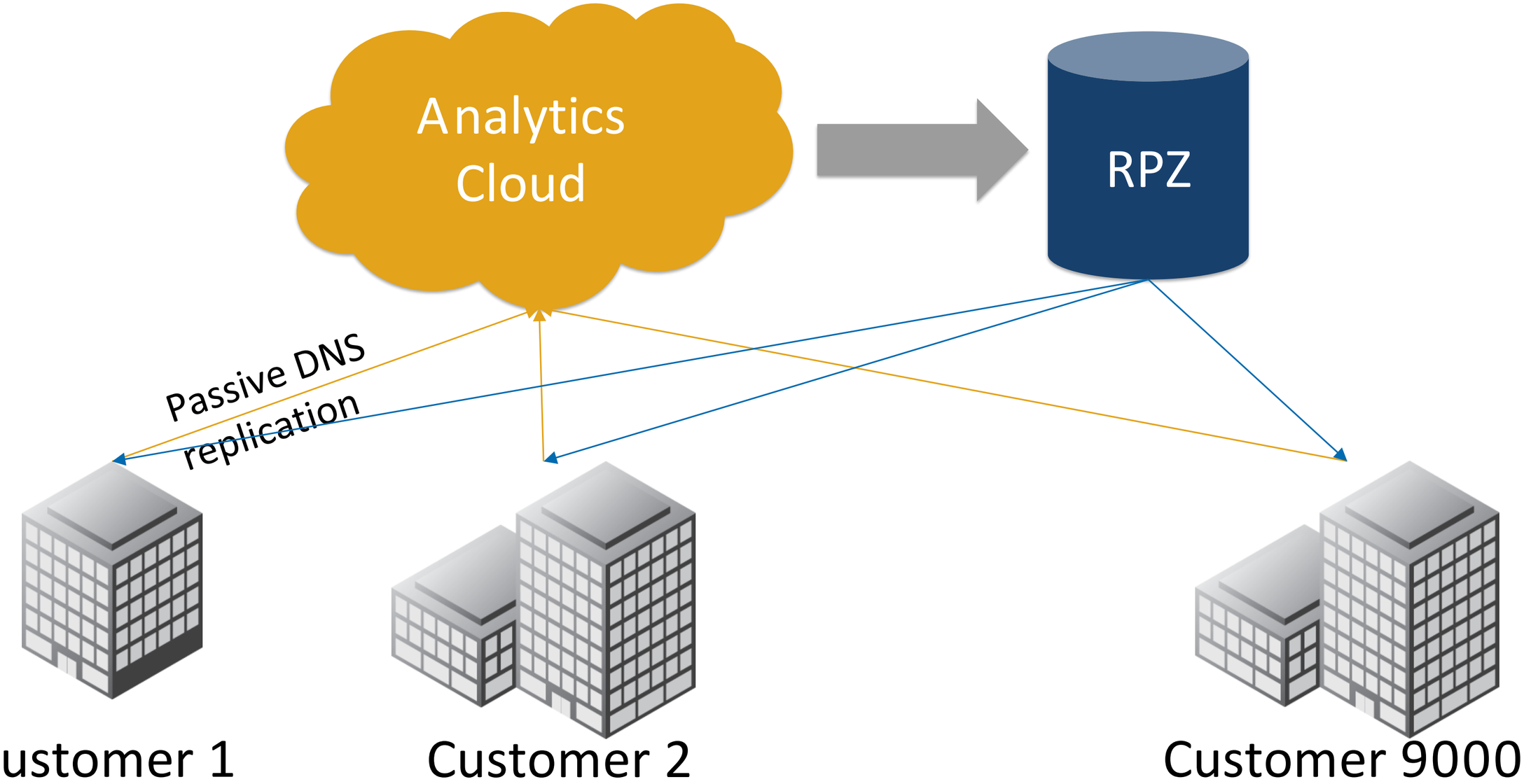
Passive DNS



What Can Analytics Do?

- Identify fast-fluxing and similar techniques
- Identify tunneling, *even previously unknown*
- Identify Domain-Generation Algorithms (DGAs), *even previously unknown*
- Identify suspicious resolution patterns, e.g., east-west resolution
- Identify potential unauthorized access to cloud-based services
- Identify cache poisoning of your domain names in others' caches
- Identify tradename infringement and phishing
- Provide *herd immunity*

Closing the Loop



Here Comes the Cavalry!

- Anycast
- Response Rate Limiting
- The DNS Security Extensions
- Response Policy Zones
- Advanced DNS Protection


Thank You
Vinaka
köszönöm
Asante
Shukria
Kiitos
Maake
Dhanyavadagalu
감사합니다
Kam Sah Hammida
Manana
Dankon
Matondo
Dank Je
Dankscheen
спасибо
Mauruuru
Biyan
Terima Kasih
Taiku
Blagodaram
Ngiyabonga
Dziekuje
Chokrane
Diolch i Chi
Tack
Grazie
Juspaxar
Arigato
Mochchakkeram
நன்றி
Bedankt
Dakujem
Gracias
Khap
Paldies
Tingki
Ua Tsaug Rau Koj
धन्यवाद
cảm ơn bạn
Gratias Tibi
Grazas
Obrigado
Děkuji
Nirringrazzjak
Di Ou Mèsi
Kia Ora
Kop Khun
ありがとう
Suksama
Rahmat
Nuwun
Hvala
Djiere Dieuf
Matur
Welalin
Misaotra
Danke
Merci
Go Raibh Maith Agat
Eskerrik Asko
Salamat
ขอขอบคุณคุณ
Najis Tuke