



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



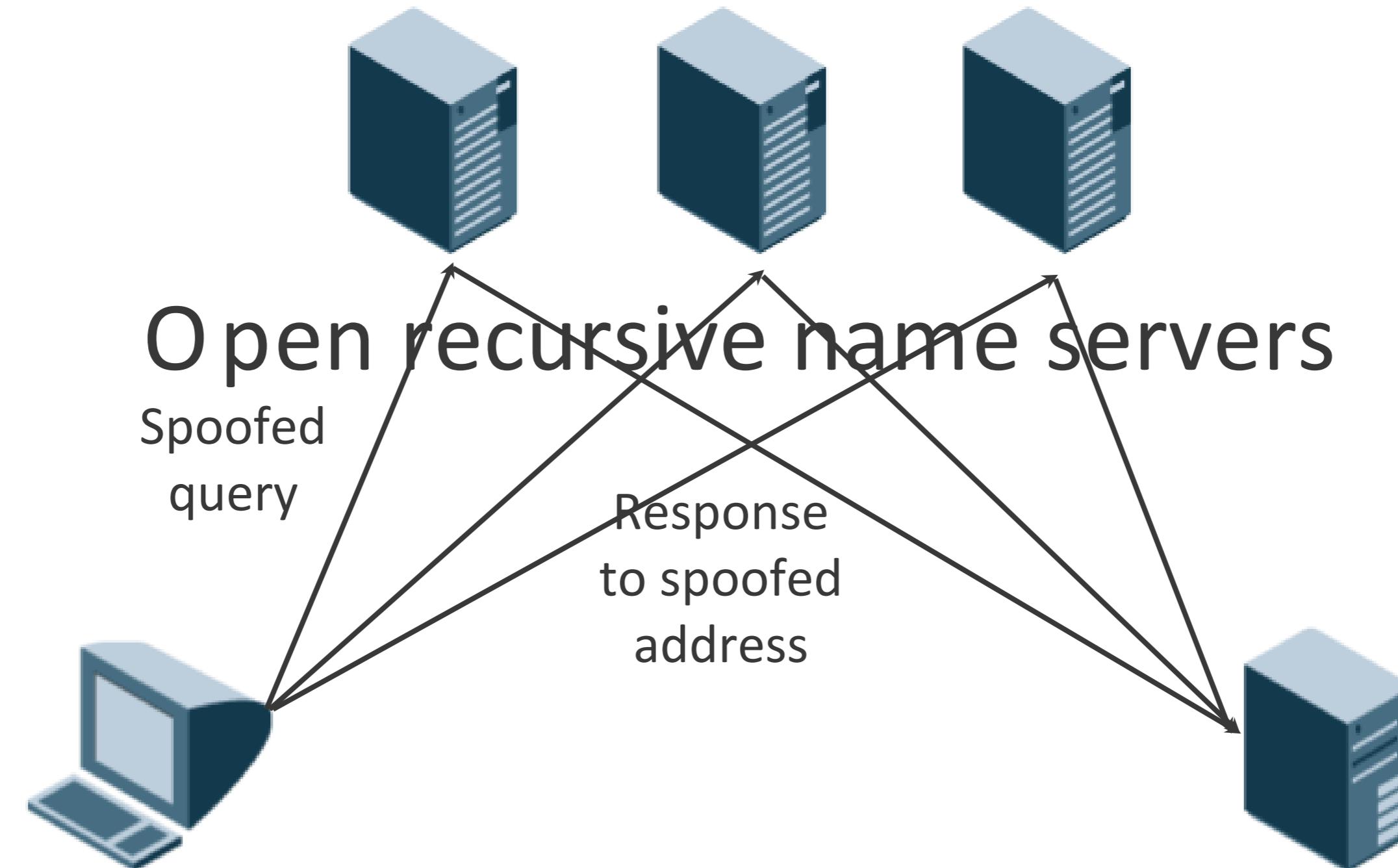
And DDoS Attacks Use Name Servers

- 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. +nored +dnssec
```

```
; <>> DiG 9.9.1-P1 <>> @sfba.sns-pb.isc.org. any isc.org. +nored +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
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 20130902233248 20130902233248 50012 isc.org. Fdfb5ND2XUlnk/nPcPOaNBCK617LdrhC/dqdS+TMtBjKMmJNJB101D8fOnckBzlwNK1JLP25znMNByMekctR2r7O2Xm9mT+su4ff8r1pMcUphpsq73V6NjlbgA3LT6zf4gWyFdos60Ma/Bsq26SmpECQFNA Rpl=
isc.org.	60	IN	A 149.20.4.63
isc.org.	60	IN	RRSIG A 149.20.4.63 20130902233248 50012 isc.org. CkSVvzLktJG2PX1QssxyUYNpALjb06NMW0BC5vcuQY21N20J1XIf/wGo9Gv720u/K6rGPXgWmk/6t0T8ukt9u3xMaMxBg2ZApEg6r3zngu9vQ71/xcK+5Ok7gI8L18hBTi+vpCAKY q6A=
isc.org.	7200	IN	MX mx.pao1.isc.org.
isc.org.	7200	IN	RRSIG MX M 7200 20130902233248 20130902233248 50012 isc.org. iLi/ebGauXv4Vht5yglYXchh2WNE37wICVU6YKkqDuV2h5Twy2Tmdqj4pqVOjDF/A7zzRPkewibTM8h5yDENFLAsSij2mXBsgFGtDGSV9IUtryFkVMrDlj9gcLKT1EZpyxwQH2y2XCT5BhA bQA=
isc.org.	7200	IN	TXT "v=spf1 a mx ip4:204.152.180.0/16 ip4:149.20.0.0/16 ip6:2001:04f8:0:32 ip6:2001:04f8::32 ip6:2001:500:0:65/128 ~all"
isc.org.	7200	IN	TXT "S: isc.org.v 1.1845 2013-08-16 16:16:50 dmahoney Exp \$"
isc.org.	7200	IN	RRSIG TXT 5 2 7200 20130902233248 50012 isc.org. J0UV7ilvQn7Pzu/itUN1JH4hLg8bjQo/73kBef/T/yzx/P8t6VX+MYDC ysyXNigSi1JPoWfy7qu6eXcALQEwj/Z156Rebefjls4R18wr+BttzWF ICb+z7k/o4meckc7ZQr12gIAxij09dr9omYoObWo6/IH76S6N3Er4i xdg=
isc.org.	60	IN	AAAA 2001:4f8:0:2::69
isc.org.	60	IN	RRSIG AAAA 5 2 60 20130902233248 50012 isc.org. OBWafw6hmqueTval06Q3zpKODW3OIWKxHr3Z30mag1vJW5Ecwlk3x1lPr4A1Rg6SZlp78yewBWLDB0436cY1uCJ0yzsk9YWILW/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 20130902233248 50012 isc.org. s9cuc600e2kgBNffd6dyJyH1Zm5Wd0pRO1q5aKMc7UsiKFUI7MI7Q8N VzTqwM/zWh2VztV/w103IHuSiXB9Nk51Loy4WG HJSdcXs865PWjHJw jRqfz1bE+LsW/aZD2Ud/iGyhCoQPeZIOcqB6pIB+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 20130902233248 20130902233248 50012 isc.org. K3/RL0nn54FkFvcPnaecG26JjqVCZL1g41zB02YssZnE/3IX9X4O8uk DrONRdrEeMq51YUy8NBijWAPOIRYD0IWUMrXuSNHMyGIFwHFIZqNrN CuQUI+24oPQXi3/wWX0TG H5XW9XF2B+Dc1zDp/5qRHicKjAnYDNE384 PAQ=
isc.org.	7200	IN	DNSKEY 257 3 5 BEAAA0hHQDRhQbtphgq2wQupeQ5tDmoxMvCgXyGrhbA2zh7yf8ZcW6hd3nXG/1Q6Krbpdet3YXLA5/kA+u50WIL8Z1R6KTbsYVMf/Qx5RinbPClw+vT+U8eXEJmO20jiS1ULgqy3
47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNiMcwsB8/2+2E63/zzRQz Bkj0Brn/9Bexjpi3sRhZatEsXn3dT47R09Uix5Wcjt+xzqZ7+ysL KOOeds39Z7SDmsn2eFktQpv6LXegCw-w-jw3oA8IVfzef/rzezbvNsOQaEFT	IN	DNSKEY 256 3 BQEAAABwuHz9Cem0BJ0JQTO7C/a3M6hMaJp7VH XTrACw6eQLruKoZLzJnqf1OMmtBfh/hbImCft207n3MfqeytvPnY7dWghYw4sVfH7VVEGm958o9nf79532Qeklxh x8pXWdeAaRU=	
isc.org.	7200	IN	RRSIG 256 3 BQEAAABwuHz9Cem0BJ0JQTO7C/a3M6hMaJp7VH XTrACw6eQLruKoZLzJnqf1OMmtBfh/hbImCft207n3MfqeytvPnY7dWghYw4sVfH7VVEGm958o9nf79532Qeklxh x8pXWdeAaRU=
isc.org.	7200	IN	DNSKEY 5 2 7200 20130902230127 20130902230127 50012 isc.org. ioYlytf4vAhxkxdz6U/fuQCa2f2XVUxjxkxo4845vLVsre5GkG1Wyn4FeWLOUVWm5HElb/hK2QEResp0csAwTnll7W8fM65aS7pIO9JZ QWMvkPxQjsTYzEP1P2GA8NVGRUhz17RMLLSFgAJS9aEl7xK0fMwsd9U4
Az+B9J8xz5GGMb8FStEXMYauE9r8z5G4z2RZUv619IXYH+Uhh5QUfq IcVYvtOt+QLlwdWV4Kt3fp3m6KveBAnliorPSjOd40PfwZD3CQ4GqVlc EyYai55bKn1hVFRhL8MqjwU491f7pzC6cLjXqvjBe+Eo	IN	RRSIG DNSKEY 5 2 7200 20130902230127 20130902230127 50012 isc.org. Hfc6Eppk8DieQnYccCLEMuP3uhCFENhY9pwbcwYh9fOMMeEim/XSyQlk9FsVGZnXw2SgC946gSXnTkLdaogwibOZLq2o0UG bsF2+4SreLlx0 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 ip6:2001:500:65/128 ~all"
isc.org.	7200	IN	RRSIG SPF 5 2 7200 20130902233248 50012 isc.org. enxTFXMYwtZW9rms2eZ0svQwlaRjn3whFcblQ2mpqjtT3BxuqpGcvlbC jwjLxNhn89x2Y2//pkN1EPvgwr2yd7lBoLV9X/VnGCH/sBInaRtckk2 SE75cuH2LjkR1D
;; 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 149.20.4.3
sfba.sns-pb.isc.org.	7200	IN	AAAA 2001:4f8:0:1::1
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 20130902233248 50012 isc.org. EyCDOBQmQqQelS_Fsk6kFT0YO13Xhizj077K8ec3+Zd7u61nSEH1R73nXOSwZ+YXV1Qo02TbeQtap2B9xDajTR4kEWg6PtneOKG
ams.sns-pb.isc.org.	7200	IN	RRSIG AAAA 5 4 7200 20130902233248 50012 isc.org. RFpmrCAZOExrl8Pc6tDW38Eoc/xxtud634xllKoM77zhGLx6vLRR wiH3Ny1gW++hyj6b6LMDVbBEm7vAMVxrOQVYMFwTycf/cN4IHVlt33/Hgiuk2SSdsZEgeaU57FgxgZIMaO
ord.sns-pb.isc.org.	7200	IN	RRSIG A 5 4 7200 20130902233248 50012 isc.org. N/ZYnIB9X5ungJF+TaCj0nN5K8FLCwRwMb3cJ9DRU4nvJFJ018LP a1nBjQwQKCIrYsfqPW1/ku09djvKEyU3W7jsdkE89Ep/4QX9M4jt+w921FQO+e9SNPimQojjCE5fbRYfls7KX0V79
ord.sns-pb.isc.org.	7200	IN	RRSIG AAAA 5 4 7200 20130902233248 50012 isc.org. H5eByfYUHm4c8V12auNll1QhQL4UA9MV9w1wQPjU/Rtxbfvrl3rlj ulUP6v4R5NvO3lad7bsNpb9xMou1qOC5FL9fn0MVFgU+qCwQ7GIRxyA6fQaFKBNrO L6iivbC6LbE+2uZPR
sfba.sns-pb.isc.org.	7200	IN	RRSIG A 5 4 7200 20130902233248 50012 isc.org. sr0nh5ZbxmbnG aduo4ri1tHpPR4+D0Mf4WpEjzu21+iEBkgc3M1XdyCT gCpd8JRCEcz+glu8wXQI+29mUrK3QwPCIWJNx/AKol7TbIPxrYoKciv pZv7yTwO2bC1SGfcNXZAm5UuKU0j7je

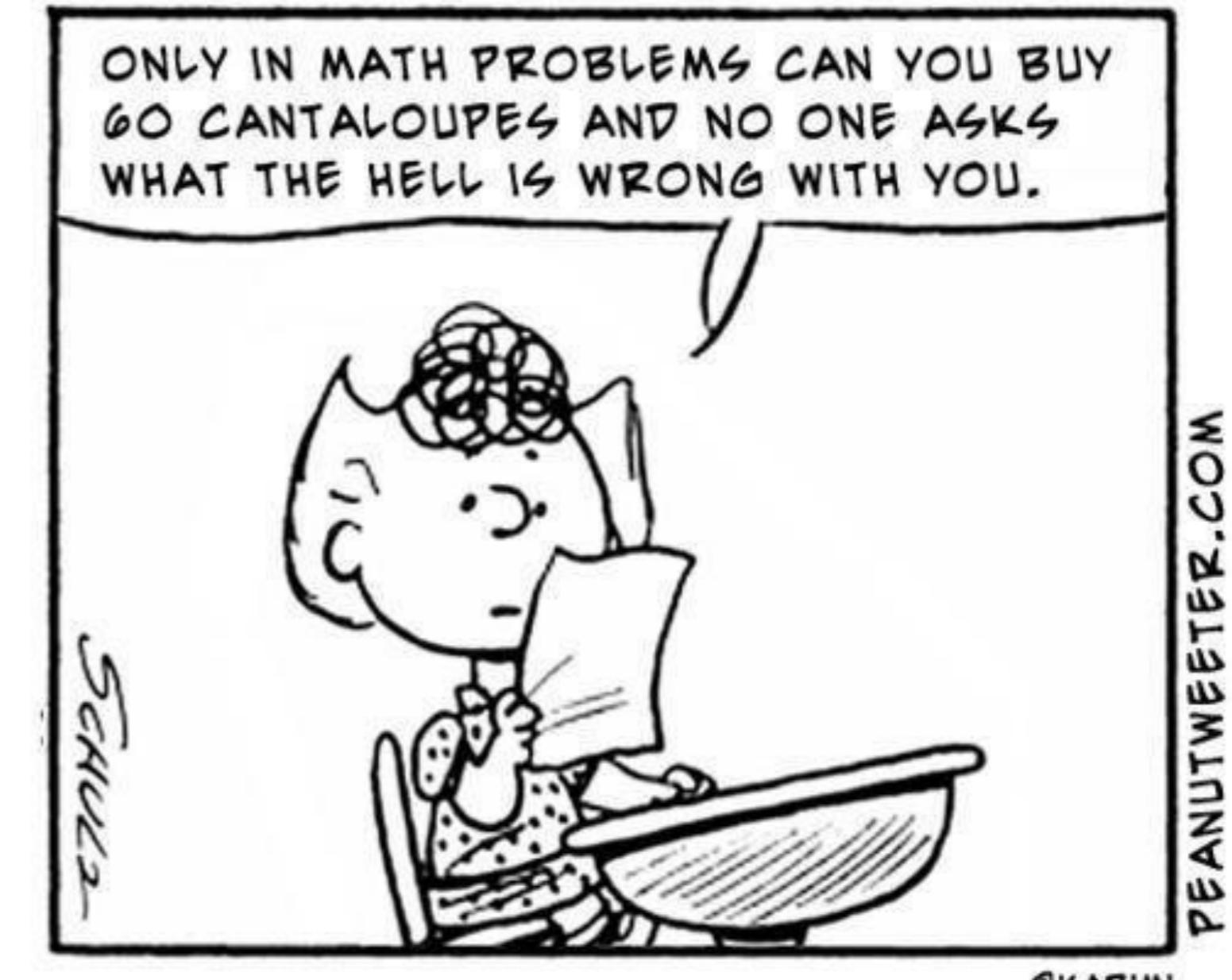
44 bytes sent, 4077 bytes received

~93x amplification!



A Little Math

- Say each bot has a measly 1 Mbps connection to the Internet
 - It can send $1\text{Mbps}/44\text{B} = \sim 2909$ qps
 - That generates $2909 \text{ pps} * 4077\text{B} = \sim 93 \text{ Mbps}$
- 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



NETFLIX



The New York Times



tumblr.



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

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

 **Anna-senpai** 8
L33t Member



Preface
Greetz everybody,

When I first go in DDoS Industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it However, I know every skid and their mama, it's their wet dream to have something besides qbot.

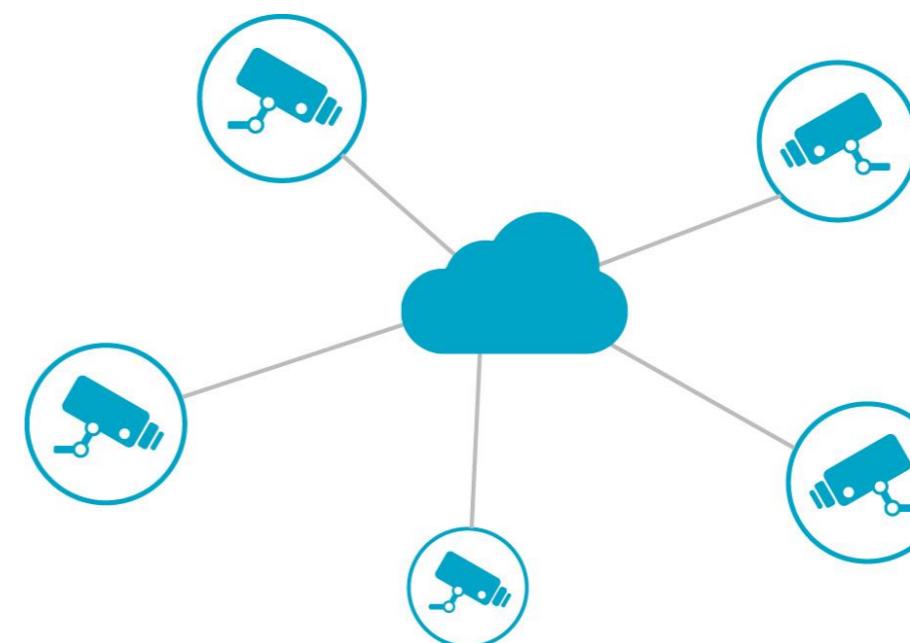
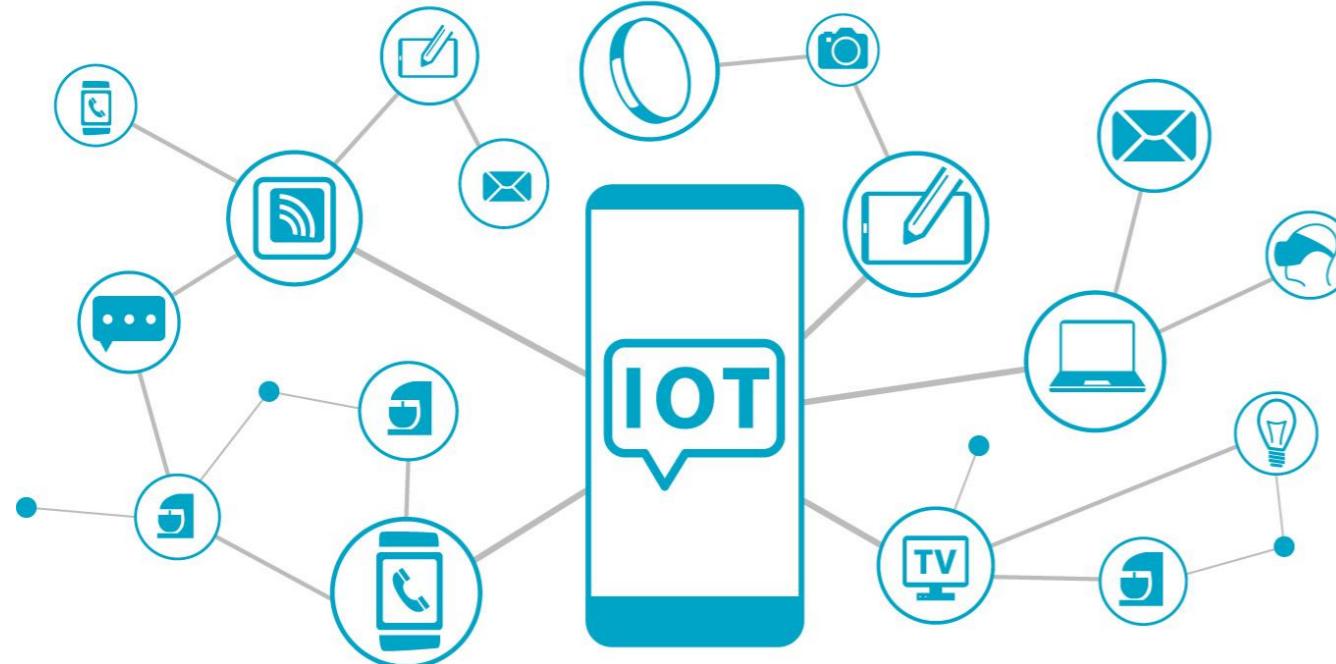
So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.



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

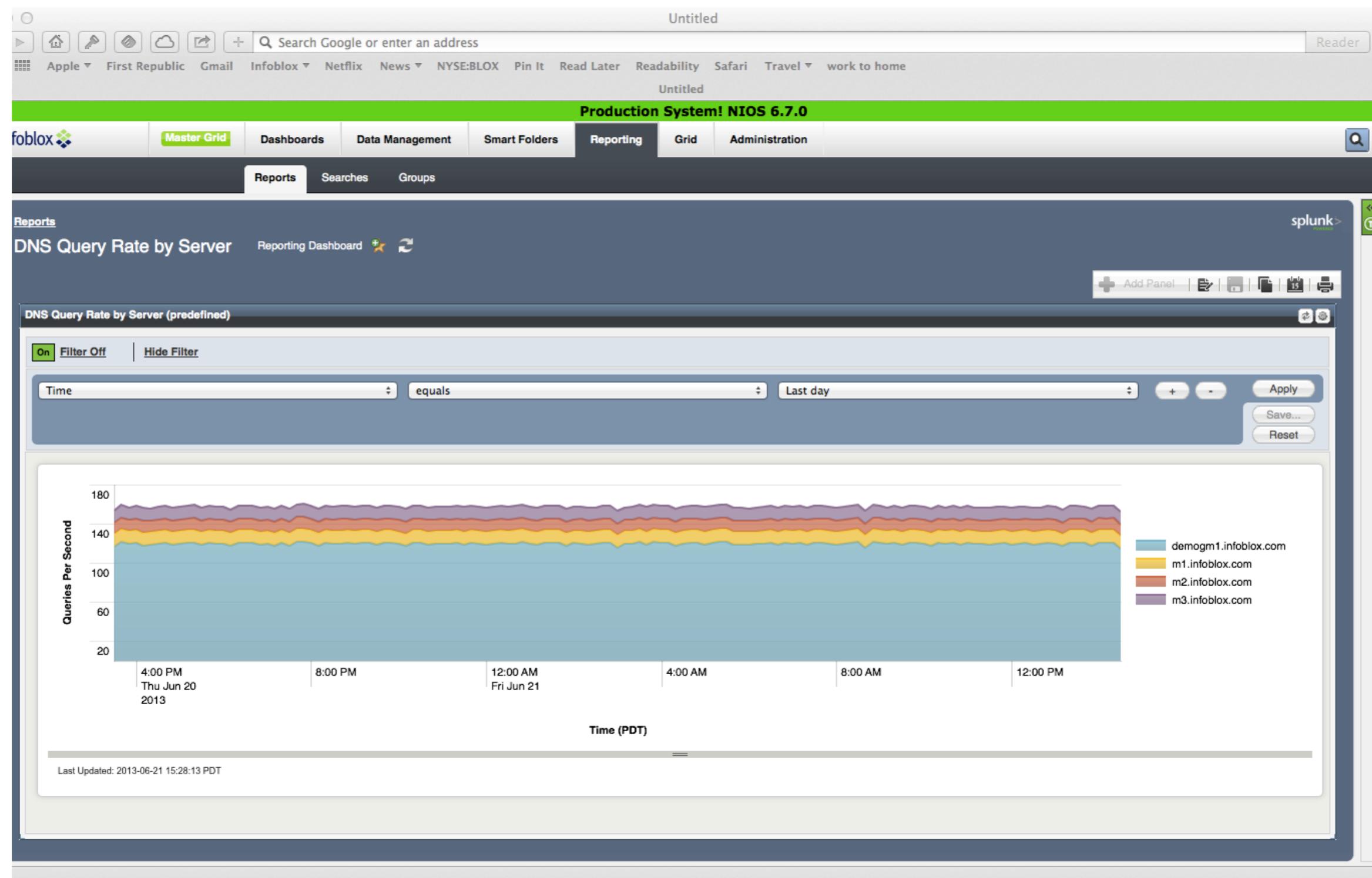


Solution: Monitoring DNS Traffic

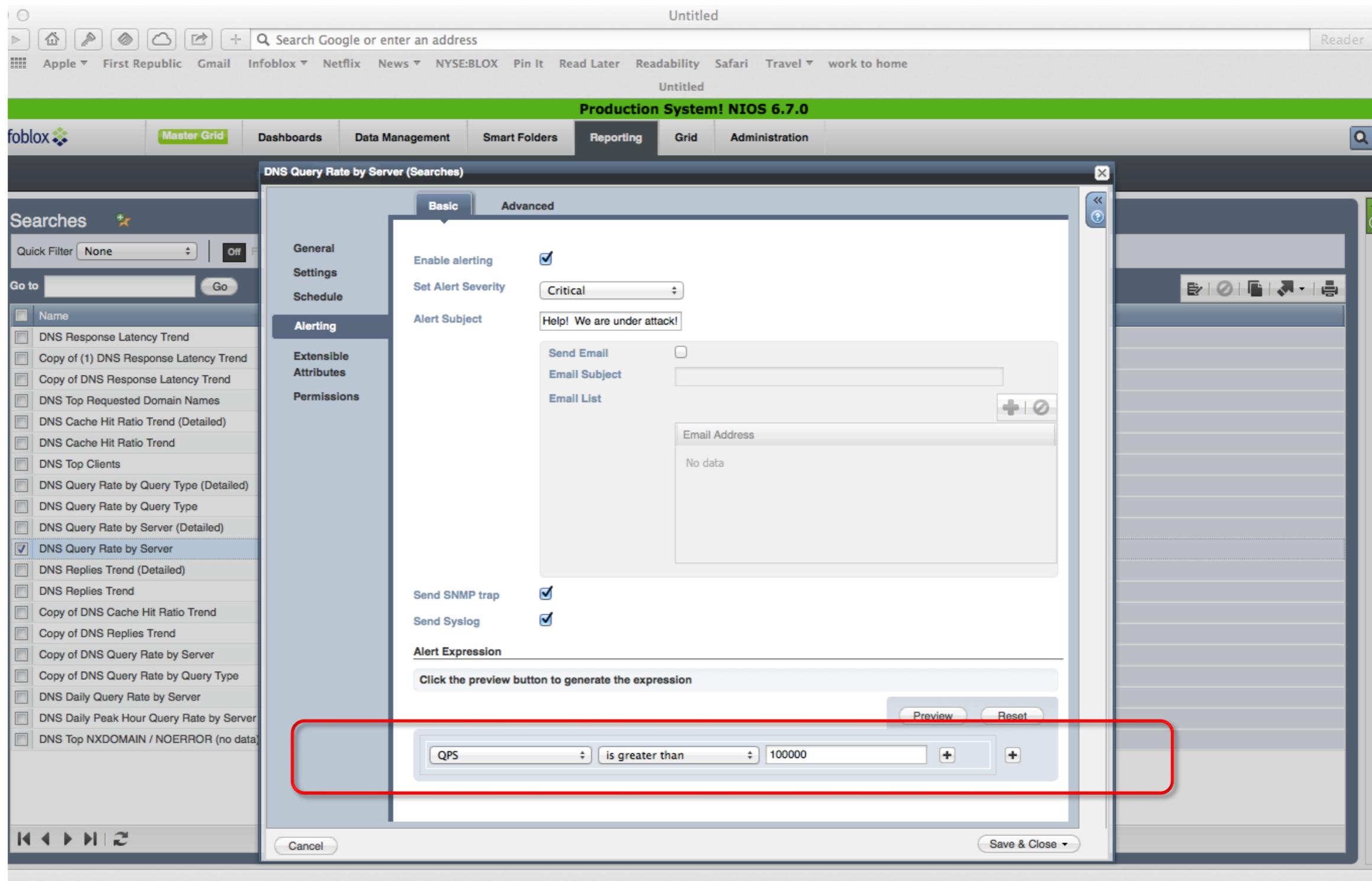
- Monitor traffic to your name servers, including
 - Aggregate query rate
 - Top queriers



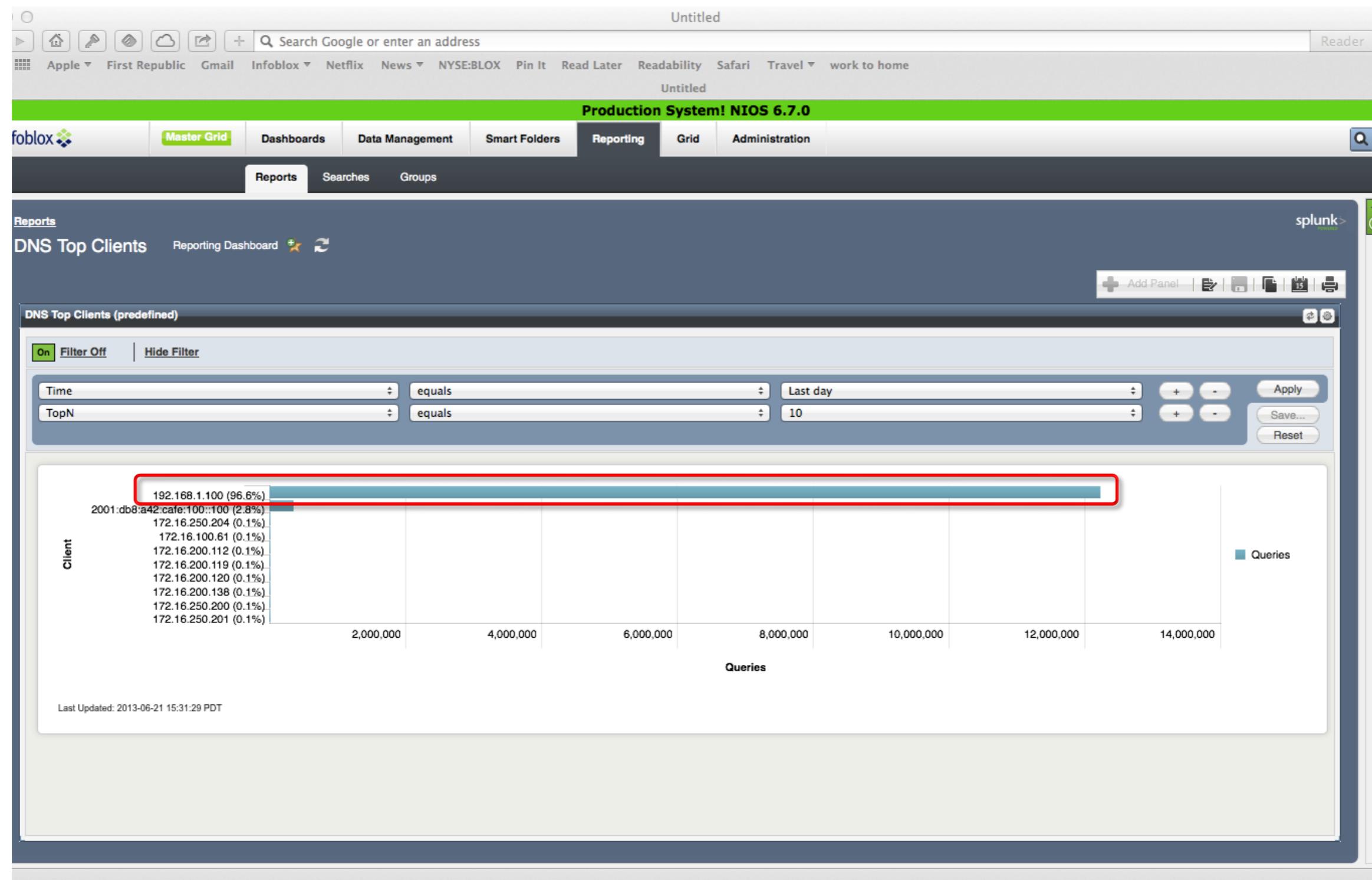
Monitoring Aggregate Query Rate



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

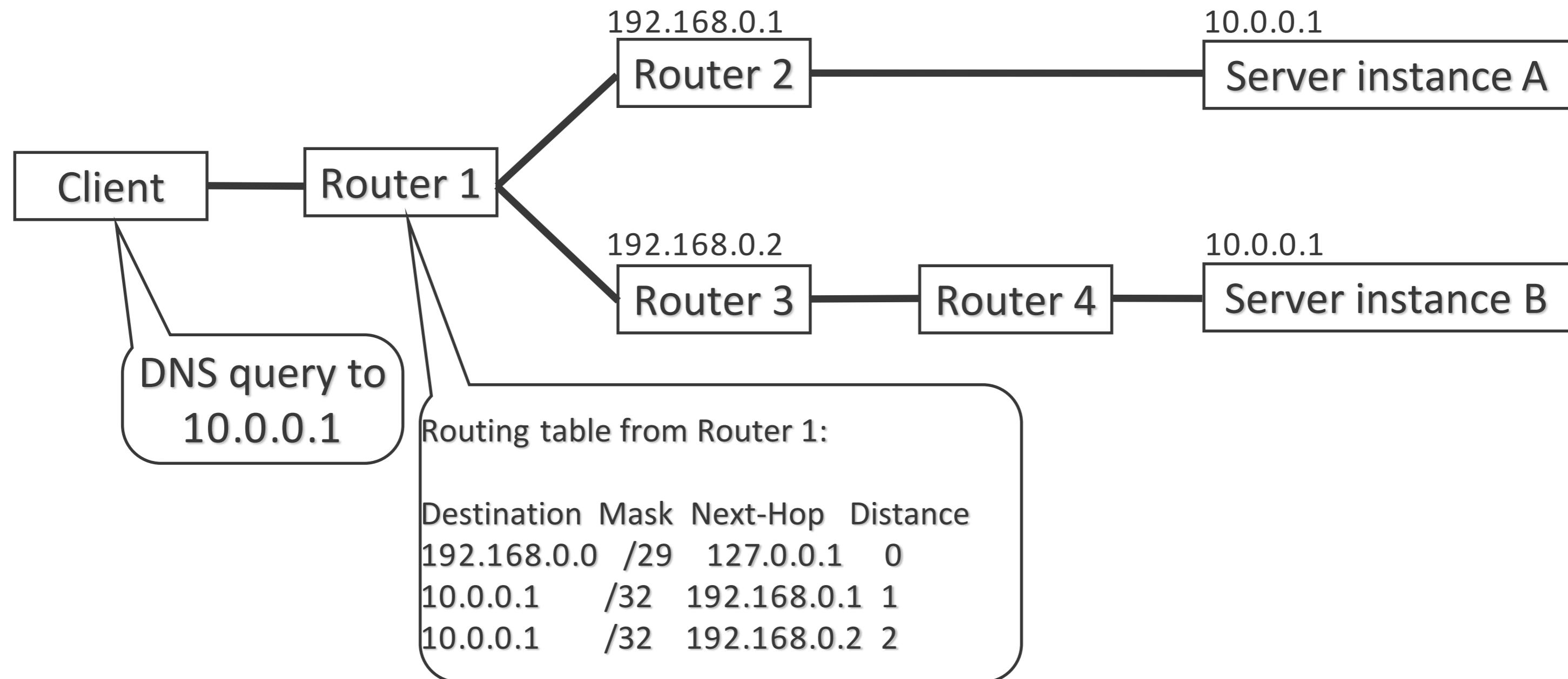


Solution: Anycast

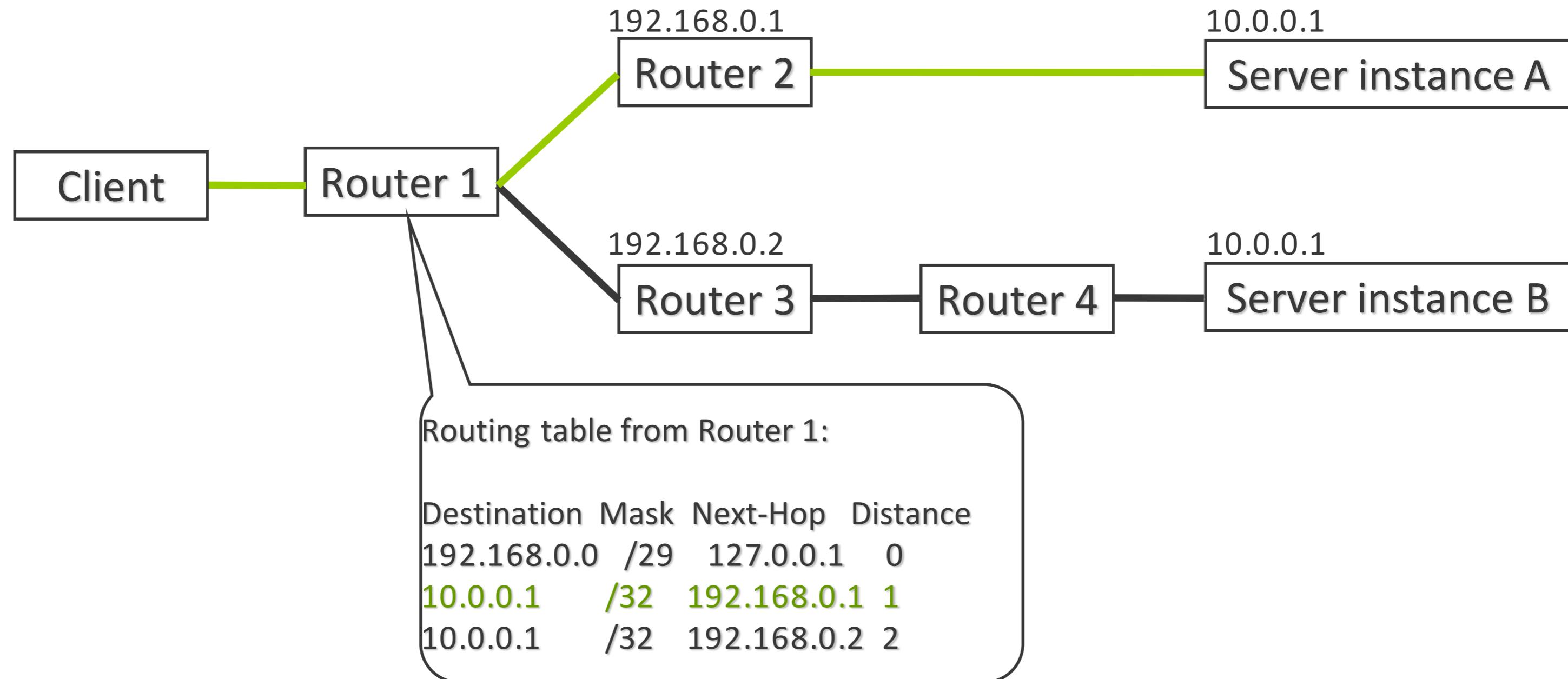
- Anycast allows multiple, distributed name servers to share a single virtual IP address
- Each name server advertises a route to that address to its neighbors
- Queries sent to that address are routed to the closest name server instance



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

The screenshot shows the Infoblox Grid Manager interface. The top navigation bar includes links for Dashboards, Data Management, Smart Folders, Reporting, Grid, Administration, Grid Manager (selected), Upgrade, Licenses, HSM Group, Microsoft Servers, and Load Balancers. The main header has tabs for DHCP, DNS, TFTP, HTTP (File Dist), FTP, NTP, bloxTools, Captive Portal, and Reporting. The main content area displays the 'pm-1.pm.tme.infoblox.com (Grid Member Properties Editor)' dialog.

The dialog has tabs for General, Licenses, Network, Anycast (selected), Security, DNS Resolver, Monitoring, SNMP, SNMP Threshold, Notifications, Email, Extensible Attributes, and Permissions. The Anycast tab contains a note: "Remember to add all anycast addresses to the 'Listen on these additional IP addresses' table in the Member DNS Configuration". Below this is a table for Anycast Interfaces:

	Anycast Interfaces	Address	Subnet Mask	OSPF	BGP	Comment
No data						

Below the Anycast tab is the OSPF Area Configuration section:

	Advertising Interf...	Protocol	Area ID	Area Type	Authentication T...
No data					

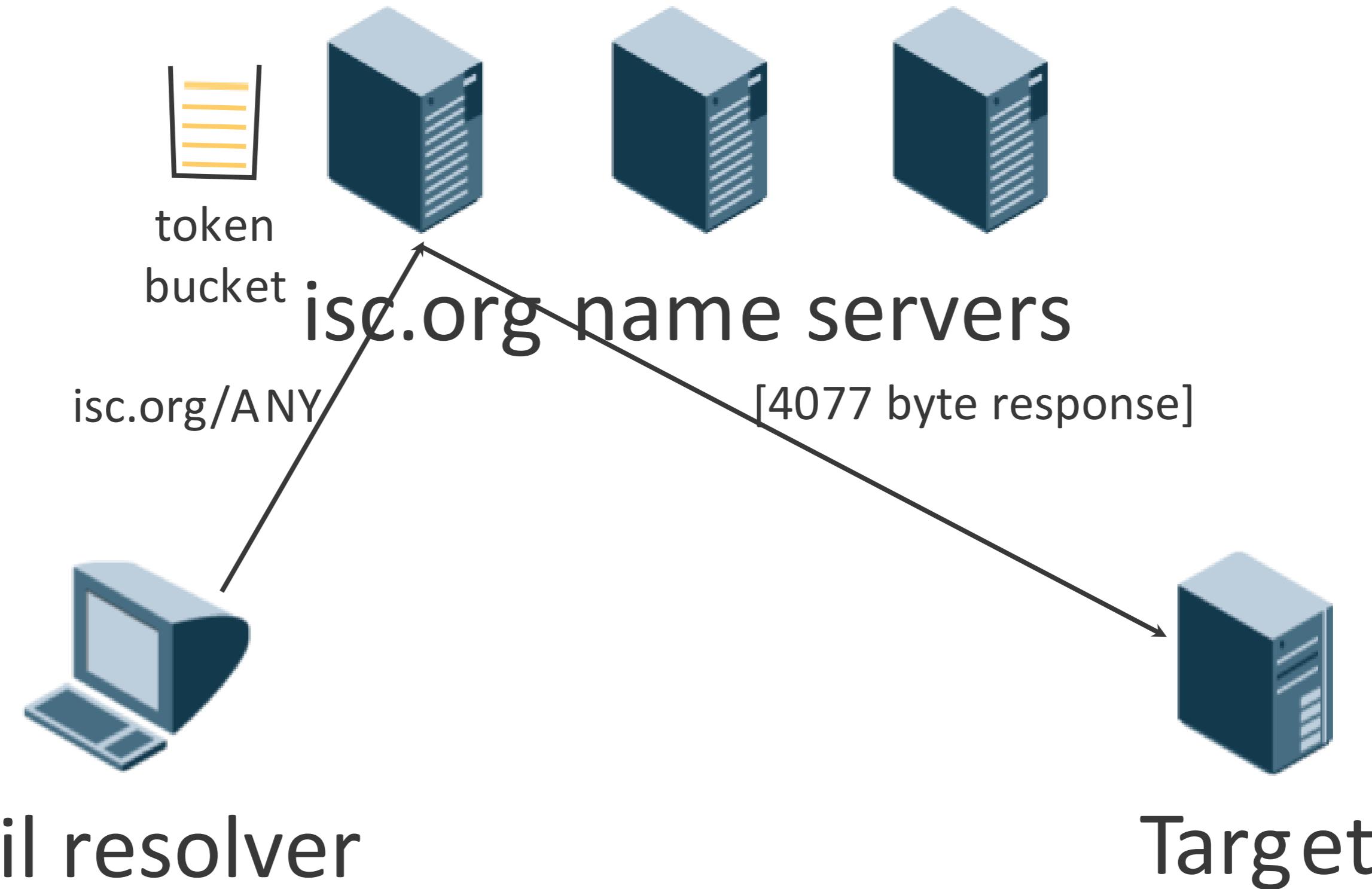
On the right side of the interface, there is a sidebar with icons for IPv6 Address, Identify, and TFTP. The Identify and TFTP columns show the status as "Unsupported" for all entries.

Solution: Response Rate Limiting

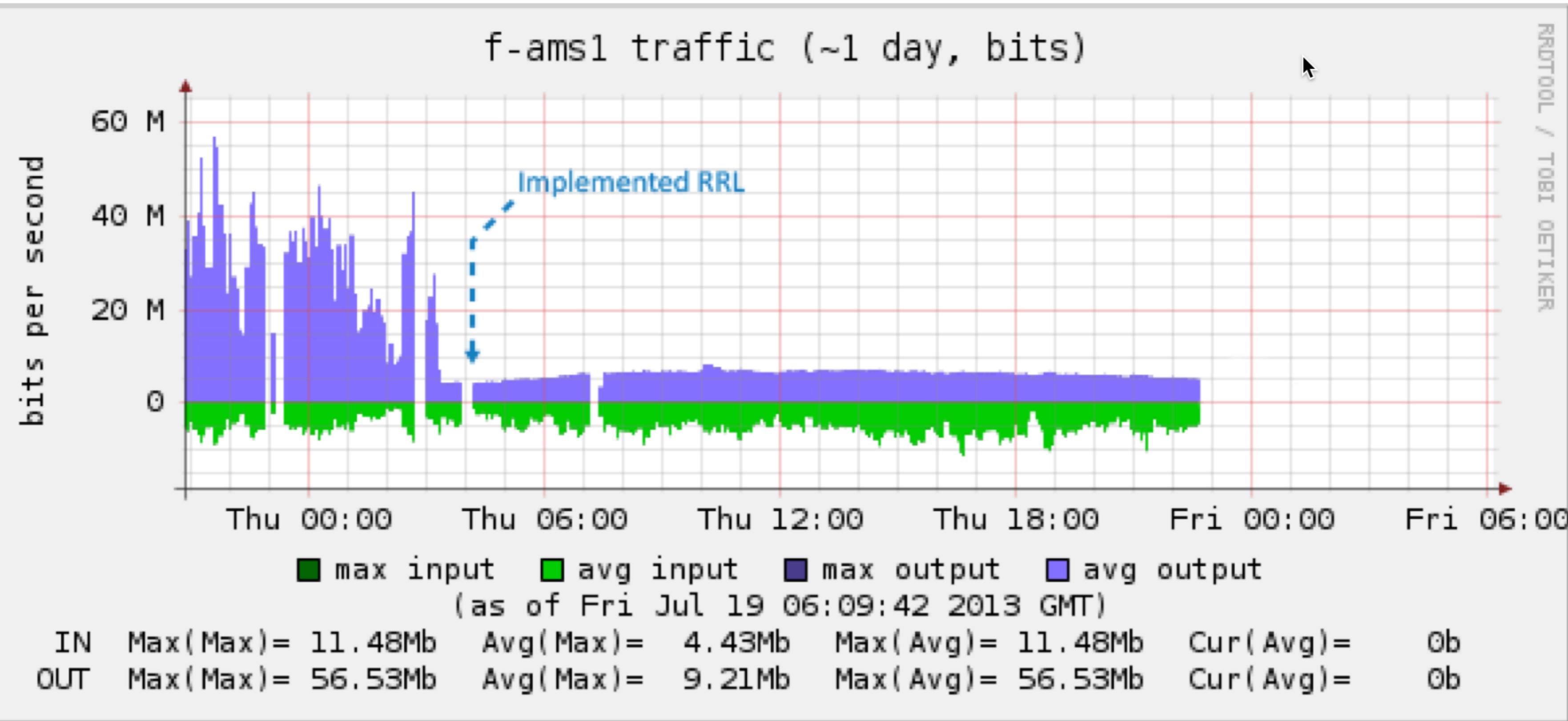
- Originally a patch to BIND 9 by Paul Vixie and Vernon Schryver
 - Now included in BIND 9, other name servers
- Applies to authoritative name servers used in DDoS attacks against others
- Prevents these name servers from sending the same response to the same client too frequently



How RRL Works



ISC F-Root



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

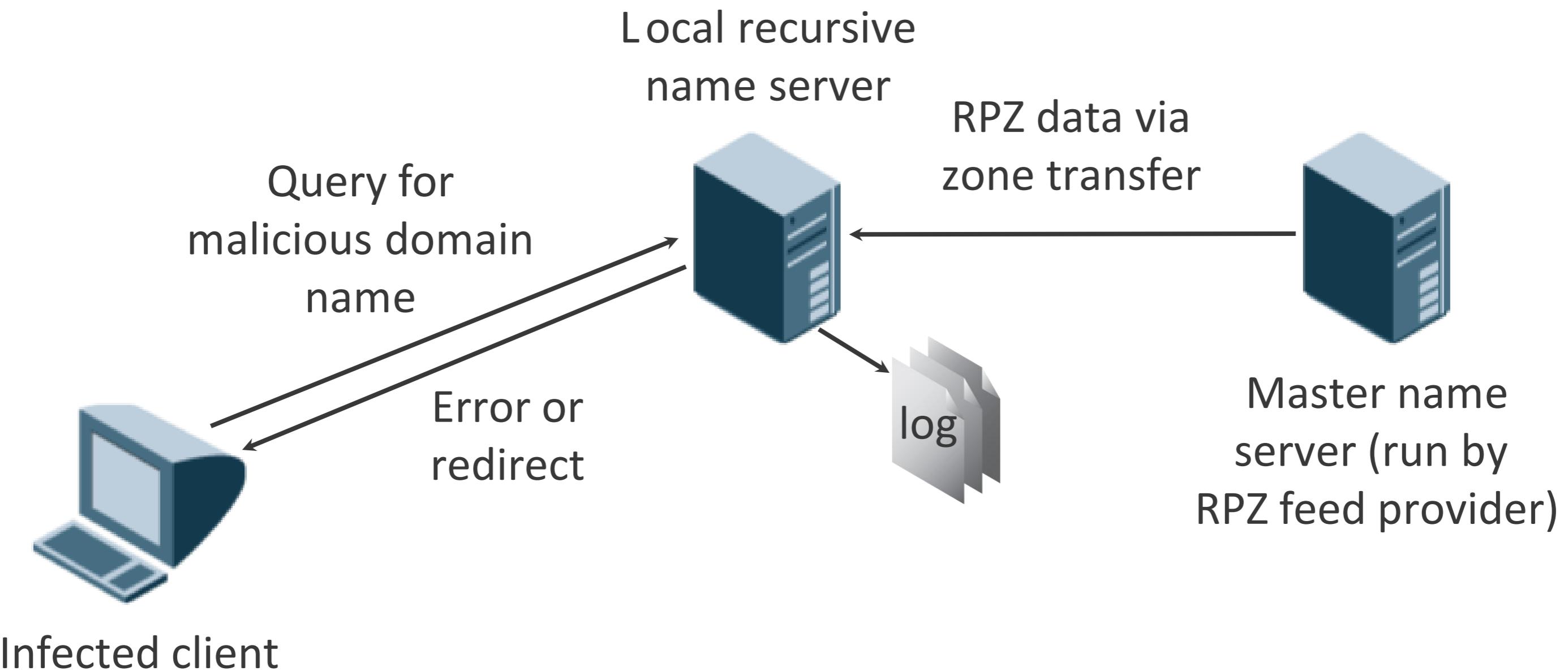


Solution: Response Policy Zones

- 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: WanaCryptOr

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



Case Study: WanaCryptOr

- The Worm
 - Initial infection vector unknown
 - Spreads using SMB vulnerability and exploiting previously backdoored computers
 - Checks for web server at *iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.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: WanaCryptOr

- 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
 - WanaCryptOr 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

Production System! NIOS 6.8.0

Infoblox CONTROL YOUR NETWORK

Master Grid Dashboards Data Management Smart Folders Reporting Grid Administration

Company 1 IPAM DHCP DNS Traffic Management File Distribution

Finder Smart Folders Bookmarks Recycle Bin URL Links

Toolbar Add Open Edit Delete Permissions Extensible Attributes Order Response Policy Zones Copy Rules Import Zone Move DNS View Grid DNS Properties Restart Services CSV Import User Profile IDN Converter

Zones Members/Servers Name Server Groups Shared Record Groups Response Policy Zones NXDOMAIN Rulesets Blacklist Rulesets DNS64 Groups

Response Policy Zones Home default

Quick Filter None Off Filter On Show Filter

Go to Go

	Order ▲	Name	Type	Primary Name S...	Last Updated	Comment	Site	
	0	whitelist	Local	demogm1.infobl...	2013-09-02 08:47:03 PDT	This RPZ is use...		
	1	local-blacklist	Local	demogm1.infobl...	2013-09-02 08:47:03 PDT	This list include...		
	2	malware-sanction.rpz.infoblox.local	Feed	threatstop	2013-09-03 15:45:35 PDT			
	3	cnc-driveby.rpz.infoblox.local	Feed	threatstop	2013-09-03 15:47:03 PDT			
	4	cnc.rpz.infoblox.local	Feed	threatstop	2013-09-03 14:00:31 PDT			
	5	malware.rpz.infoblox.local	Feed	threatstop	2013-09-03 15:41:20 PDT			

Managing Response Policy Zones (continued)

Production System! NIOS 6.8.0

Infoblox CONTROL YOUR NETWORK Master Grid Dashboards Data Management Smart Folders Reporting Grid Administration Company 1 IPAM DHCP DNS Traffic Management File Distribution

Finder Smart Folders Bookmarks Recycle Bin URL Links

Zones Members/Servers Name Server Groups Shared Record Groups Response Policy Zones NXDOMAIN Rulesets Blacklist Rulesets DNS64 Groups

Response Policy Zones Home > default local-blacklist

Quick Filter None Off Filter On Show Filter

Go to Go

	Name or Address	Policy	Data	Comment	Site
	66.135.210.181	Substitute Domain Name (IP Address)	infoblox.com		
	205.203.140.65	Substitute Domain Name (IP Address)	nytimes.com	Wall Street Jour...	
	*.fortib.pl	Substitute Domain Name (Domain N...	www.infoblox.com	Demo DNS FW	
	*.reallybad.com	Block Domain Name (No Data)			
	*.whitelist.com	Block Domain Name (No Such Domain)			
	bluecatnetworks.com	Substitute Domain Name (Domain N...	infoblox.com		
	fortib.pl	Substitute Domain Name (Domain N...	infoblox.com	DNS Firewall D...	
	heagitkuzdo.kz	Block Domain Name (No Such Domain)			
	mybadsite.com	Substitute Domain Name (Domain N...	infoblox.com	Giancarlo	
	pogitsixnekd.kz	Block Domain Name (No Such Domain)			
	reallybad.com	Block Domain Name (No Data)			
	sitomalevolo.loc	Substitute Domain Name (Domain N...	libero.it	Giancarlo	
	www.bluecatnetworks.com	Substitute (A Record)	54.243.121.37		
	www.ebay.com	Substitute Domain Name (Domain N...	bluecatnetworks.com		

Toolbar Add Open Edit Delete Permissions Extensible Attributes Order Response Policy Zones Copy Rules Import Zone Move DNS View Grid DNS Properties Restart Services CSV Import User Profile IDN Converter

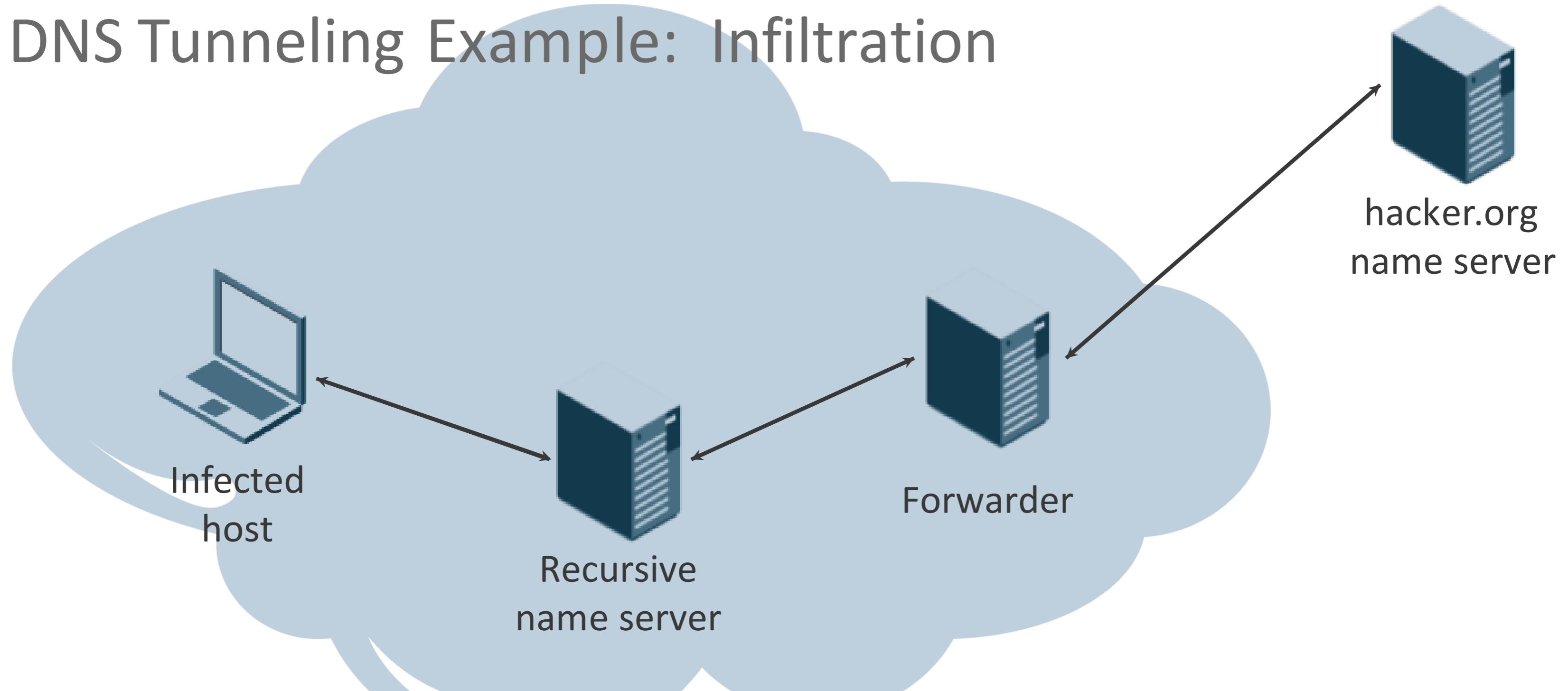


Threat: DNS Tunneling

- 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



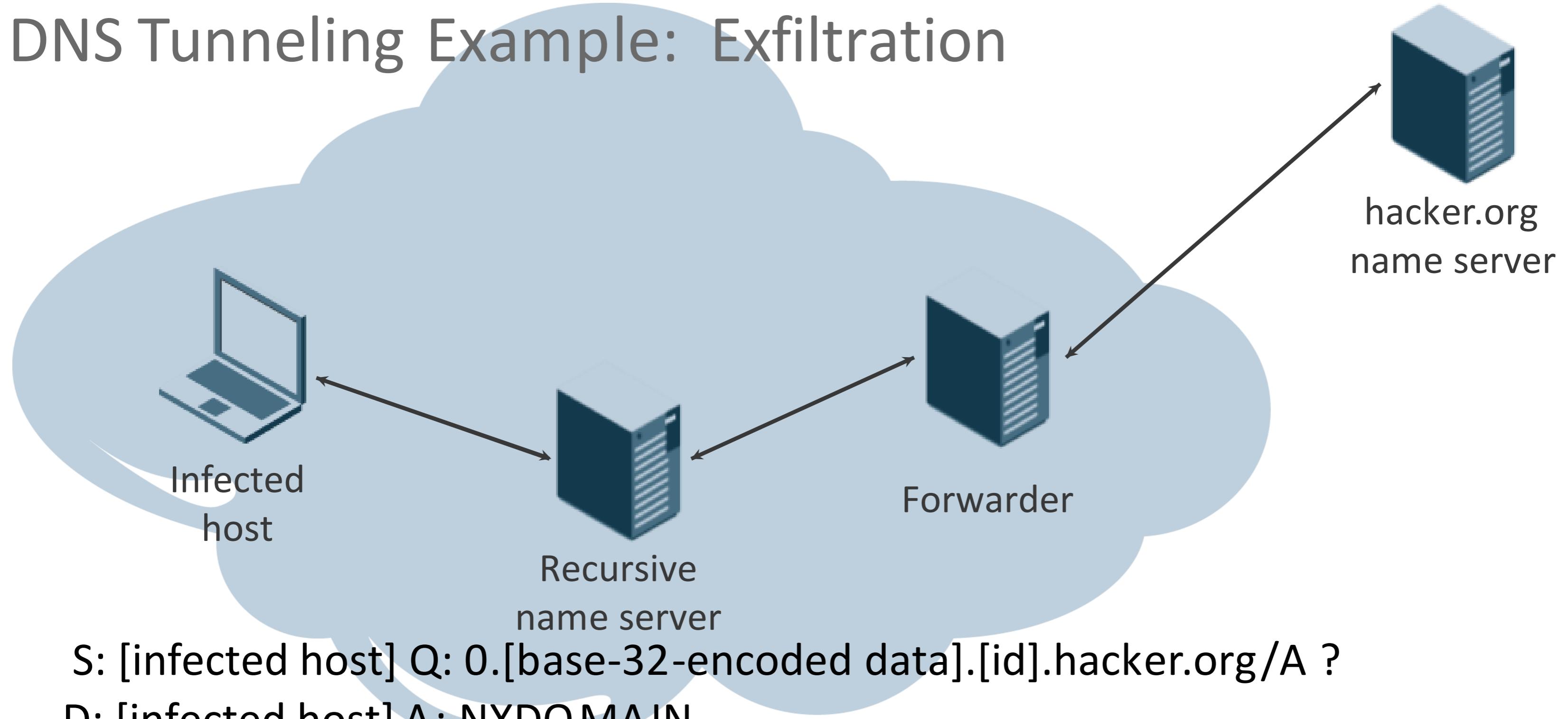
DNS Tunneling Example: Infiltration



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/ouils/dns2tcp>
- NSTX: <http://savannah.nongnu.org/projects/nstx>
- Squeezza: <http://www.sensepost.com>
- Heyoka: <http://heyoka.sourceforge.net>



Infoblox Advanced Appliances

PT-1400



PT-2200



PT-4000



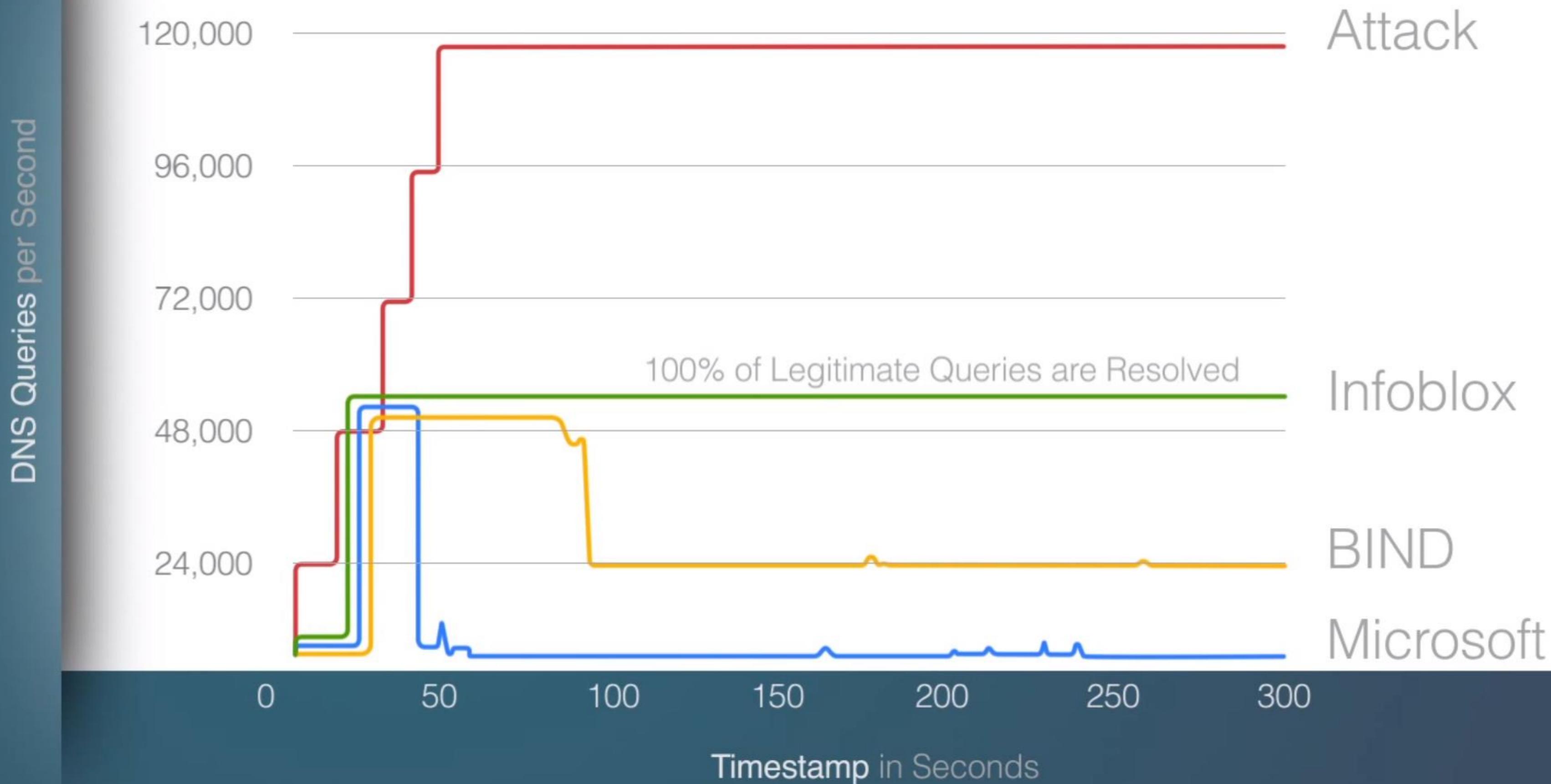
Advanced Appliances include next-generation programmable processors for deep packet inspection

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

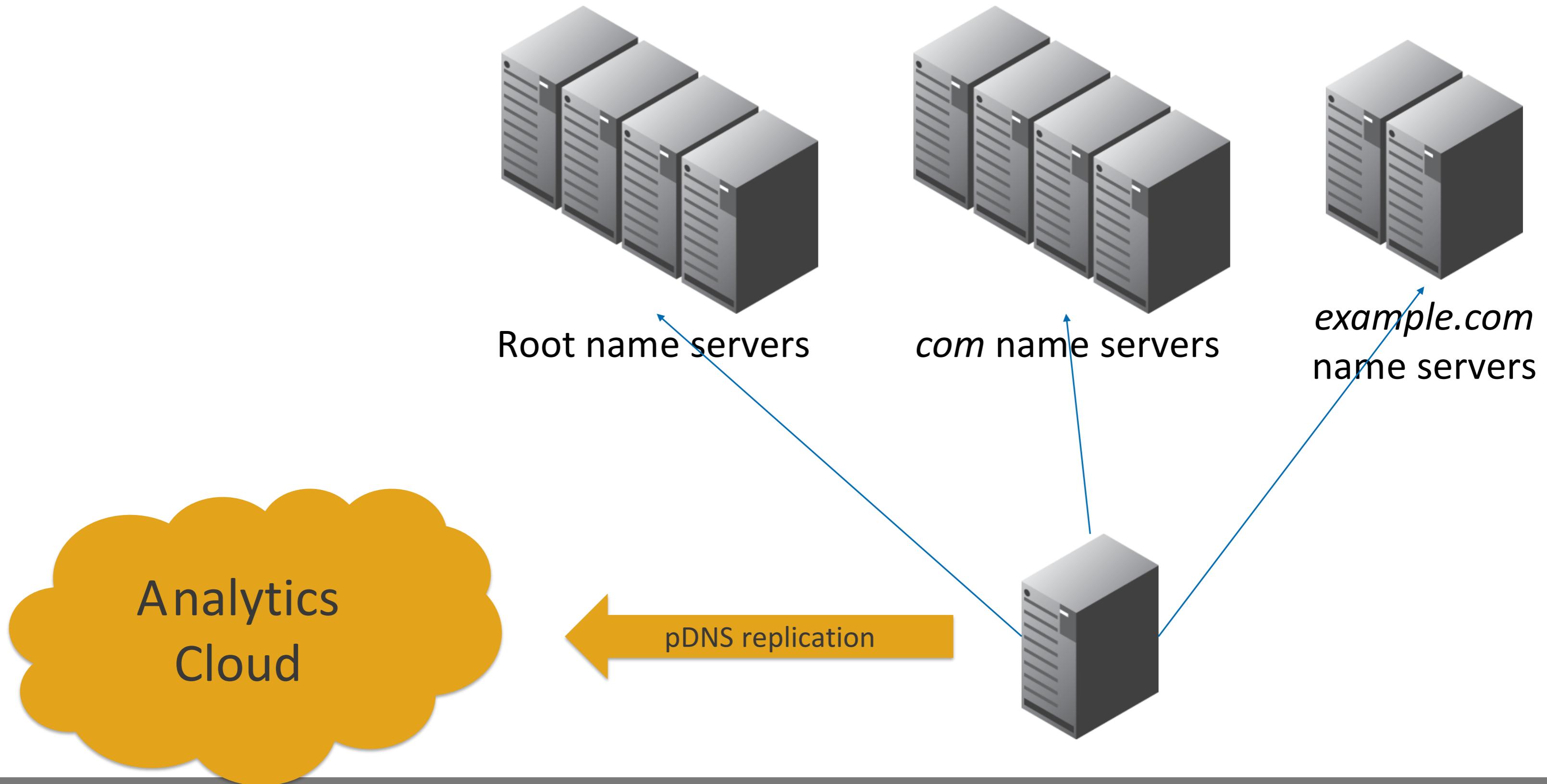


Analytics in the Cloud

- 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

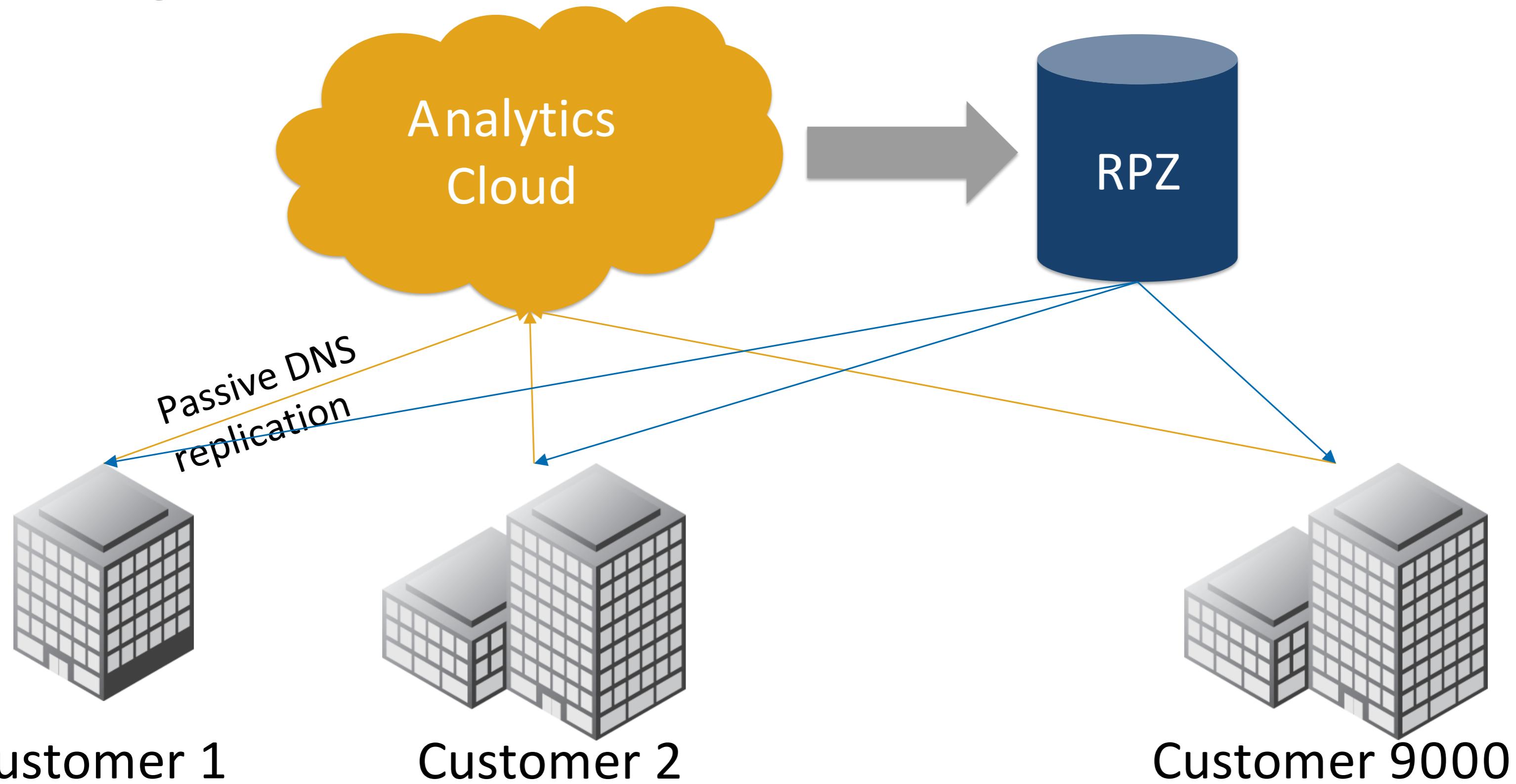


What Can Analytics Do?

- 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

A large central text "Thank You" is composed of various international words for "thank you" in different languages, including English, Spanish, French, German, Italian, Portuguese, Dutch, Swedish, Danish, Norwegian, Polish, Czech, Latvian, Lithuanian, Hungarian, Welsh, Breton, Maltese, Chinese, Korean, Japanese, and others.

The surrounding text includes:

- Vinaka (Fiji)
- Dankscheen (Croatian)
- Cпасибо (Russian)
- köszönöm (Hungarian)
- 감사합니다 (Korean)
- Dank Je (Burmese)
- Blagodaram (Swahili)
- Ngiyabonga (Xhosa)
- Dziekuje (Polish)
- Juspaxar (Maltese)
- ଧେନ୍ତି (Oriya)
- Ua Tsaug Rau Koj (Lao)
- Rahmat (Arabic)
- Matur Nuwun (Burmese)
- Suksama (Indonesian)
- Misaotra (Burmese)
- XBAJIA (Chinese)
- 謝謝 (Chinese)
- Bedankt (Dutch)
- Dákuijem (Latvian)
- Nirringrazzjak (Lithuanian)
- Děkuji (Czech)
- Gracias (Spanish)
- Grazas (Latvian)
- �ন্যবাদ (Bengali)
- Di Ou Mesi (Welsh)
- Hvala (Croatian)
- Welalin (Breton)
- Di. Danke (German)
- Merçi (French)
- Salamat (Filipino)
- Go Raibh Maith Agat (Irish)
- ຂອບຄຸນ (Khmer)
- Najis Tuke (Malay)
- Asante (Swahili)
- Shukria (Arabic)
- Maake (Somali)
- Mauruuru (Somali)
- Biyan (Somali)
- Chokrane (Somali)
- Arigato (Japanese)
- Gracias (Spanish)
- Mochchakkeram (Malay)
- Tack (Swedish)
- Terima Kasih (Indonesian)
- Diolchi (Welsh)
- Grazie (Italian)
- Tingki (Malay)
- Gratias Tibi (Latin)
- Obrigado (Portuguese)
- Kia Ora (Māori)
- Kop Khun (Lao)
- Dieuf (French)
- Eskerrik Asko (Basque)
- Dieuf (French)
- Matongo (Swahili)
- Matondo (Swahili)
- Chu (Swahili)
- Matondo (Swahili)