BLOX FEST

Infoblox

Robert Nagy

CEO – DeepDive Networking
rob@deepdivenetworking.com
www.deepdivenetworking.com

Topics Covered

- Architecture
- DNS Anycast
- DNSSEC Validation

DNS Architecture

DNS Architecture

Overview

- Where did DNS start
  - The original base design assumptions for the DNS were that it must:
    - Provide at least all of the same information as HOSTS.TXT
    - Allow the database to be maintained in a distributed manner
    - Have no obvious size limits for names, name components, data associated with a name, etc.
    - Interoperate across the DARPA Internet and in as many other environments as possible
    - Provide tolerable performance
- What is missing?

Security

DNS Architecture

Goals of today's DNS

Efficiency

Must handle the needs of the other Applications

Security

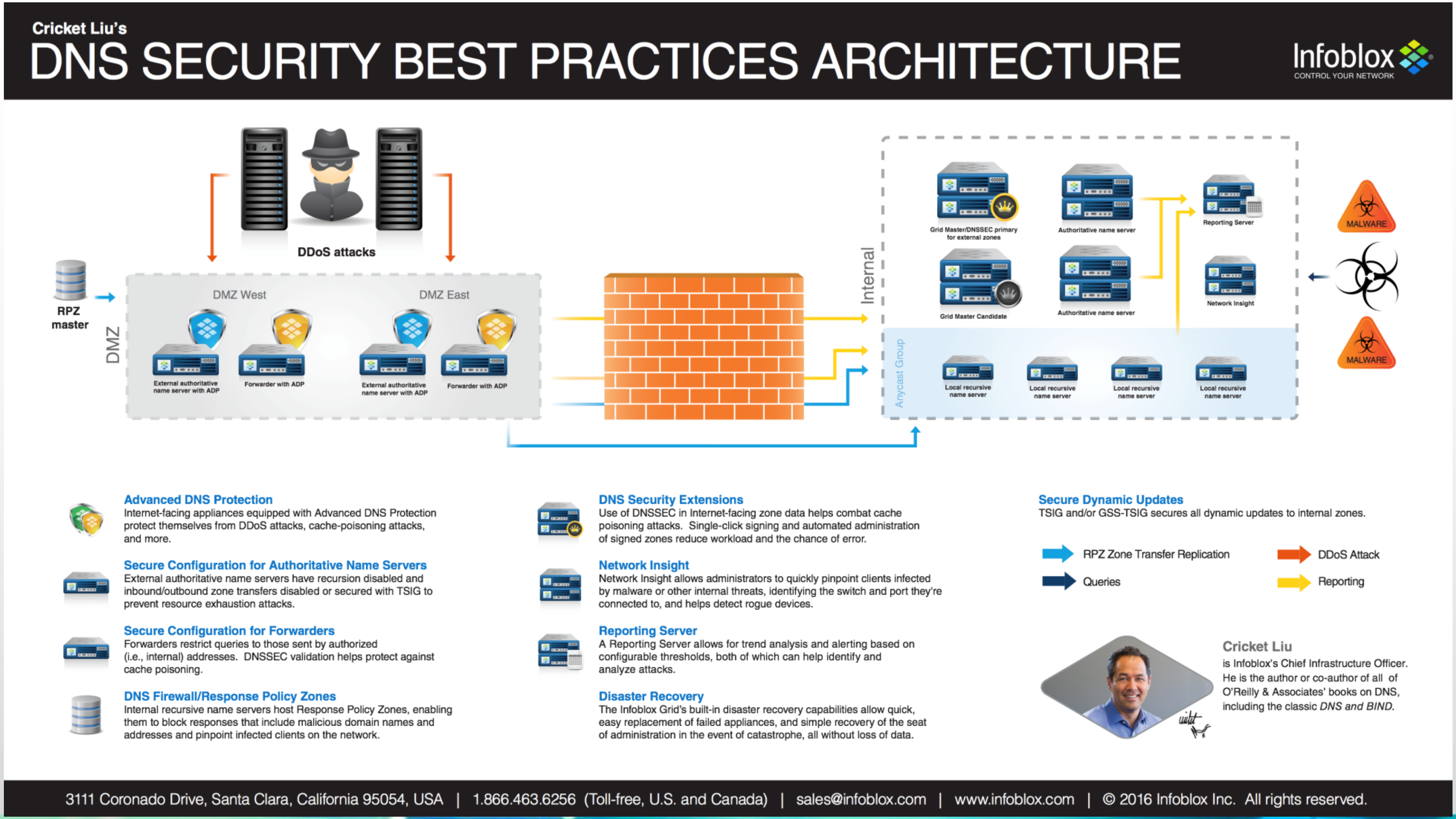
DNS must be a part of the solution

Scalability

Growth rates must be addressable

DNS Architecture

Architecture best-practices



Cricket Liu's

DNS SECURITY BEST PRACTICES ARCHITECTURE

Infoblox

CONTROL YOUR NETWORK

DDoS attacks
RPZ master
DMZ
DMZ West
DMZ East
External authoritative name server with ADP
Forwarder with ADP
External authoritative name server with ADP
Forwarder with ADP
Internal
Grid Master/DNSSEC primary for external zones
Authoritative name server
Reporting Server
Grid Master Candidate
Authoritative name server
Network Insight
Anycast Group
Local recursive name server
Local recursive name server
Local recursive name server
Local recursive name server
MALWARE
MALWARE

Advanced DNS Protection
Internet-facing appliances equipped with Advanced DNS Protection protect themselves from DDoS attacks, cache-poisoning attacks, and more.

Secure Configuration for Authoritative Name Servers
External authoritative name servers have recursion disabled and inbound/outbound zone transfers disabled or secured with TSIG to prevent resource exhaustion attacks.

Secure Configuration for Forwarders
Forwarders restrict queries to those sent by authorized (i.e., internal) addresses. DNSSEC validation helps protect against cache poisoning.

DNS Firewall/Response Policy Zones
Internal recursive name servers host Response Policy Zones, enabling them to block responses that include malicious domain names and addresses and pinpoint infected clients on the network.

DNS Security Extensions
Use of DNSSEC in Internet-facing zone data helps combat cache poisoning attacks. Single-click signing and automated administration of signed zones reduce workload and the chance of error.

Network Insight
Network Insight allows administrators to quickly pinpoint clients infected by malware or other internal threats, identifying the switch and port they're connected to, and helps detect rogue devices.

Reporting Server
A Reporting Server allows for trend analysis and alerting based on configurable thresholds, both of which can help identify and analyze attacks.

Disaster Recovery
The Infoblox Grid's built-in disaster recovery capabilities allow quick, easy replacement of failed appliances, and simple recovery of the seat of administration in the event of catastrophe, all without loss of data.

Secure Dynamic Updates
TSIG and/or GSS-TSIG secures all dynamic updates to internal zones.

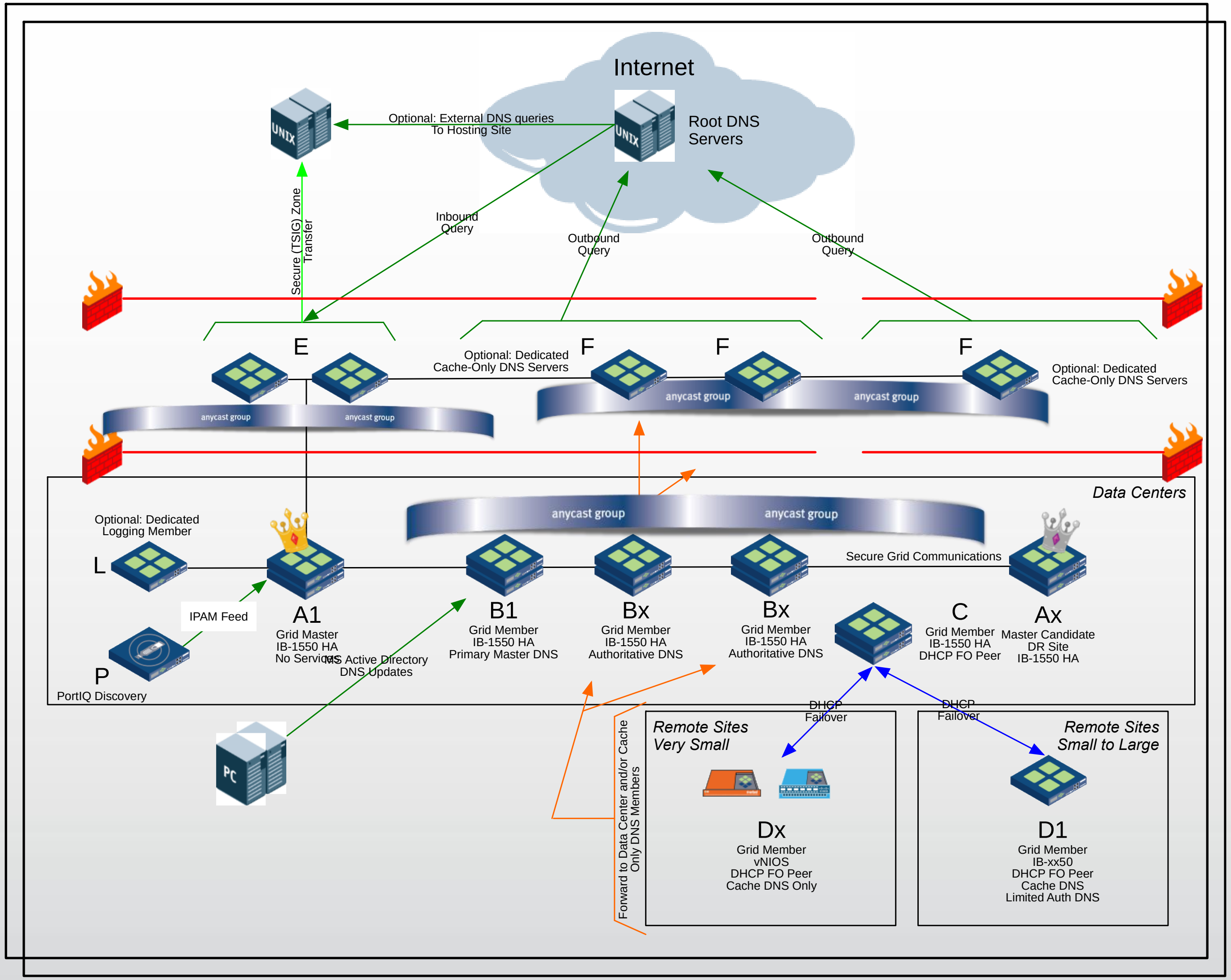
→ RPZ Zone Transfer Replication
→ DDoS Attack
→ Queries
→ Reporting

Cricket Liu
is Infoblox's Chief Infrastructure Officer. He is the author or co-author of all of O'Reilly & Associates' books on DNS, including the classic *DNS and BIND.*

3111 Coronado Drive, Santa Clara, California 95054, USA | 1.866.463.6256 (Toll-free, U.S. and Canada) | sales@infoblox.com | www.infoblox.com | © 2016 Infoblox Inc. All rights reserved.

DNS Architecture

Design goals



Internet

UNIX

Root DNS Servers

UNIX

Optional: External DNS queries
To Hosting Site

Secure (TSIG) Zone Transfer

Inbound Query

Outbound Query

Outbound Query

E

anycast group

anycast group

Optional: Dedicated
Cache-Only DNS Servers

F

F

F

anycast group

anycast group

Optional: Dedicated
Cache-Only DNS Servers

Data Centers

anycast group

anycast group

Optional: Dedicated
Logging Member

L

IPAM Feed

P

PortIQ Discovery

A1
Grid Master
IB-1550 HA
No Services

MS Active Directory
DNS Updates

B1
Grid Member
IB-1550 HA
Primary Master DNS

Bx
Grid Member
IB-1550 HA
Authoritative DNS

Bx
Grid Member
IB-1550 HA
Authoritative DNS

Secure Grid Communications

C
Grid Member
IB-1550 HA
DHCP FO Peer

Ax
Master Candidate
DR Site
IB-1550 HA

PC

DHCP Failover

DHCP Failover

Forward to Data Center and/or Cache
Only DNS Members

Remote Sites
Very Small

Dx
Grid Member
vNIOS
DHCP FO Peer
Cache DNS Only

Remote Sites
Small to Large

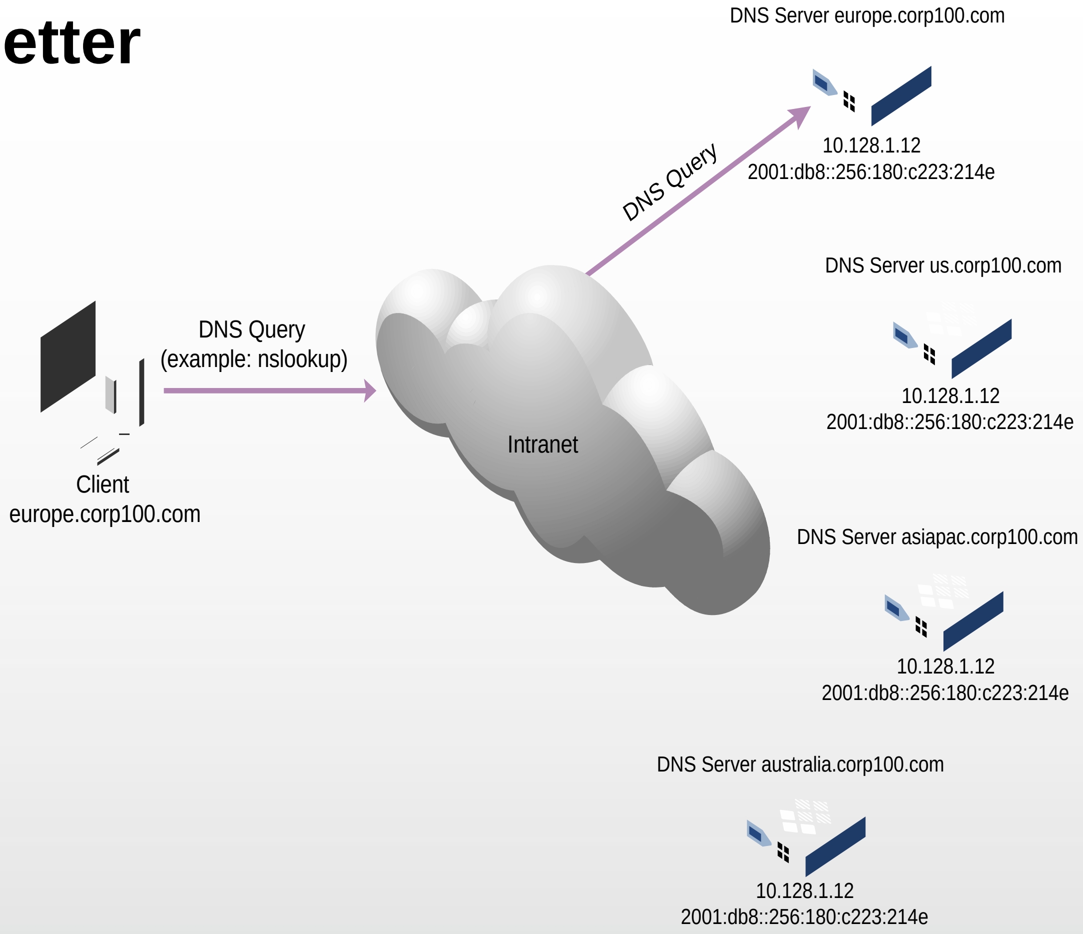
D1
Grid Member
IB-xx50
DHCP FO Peer
Cache DNS
Limited Auth DNS

Anycast

DNS Anycast

Overview – If one is good, more is better

- Nodes share a single IP address
- Routing allows clients to connect to the “nearest” node
- DNS Servers advertise this IP as a route when DNS is available

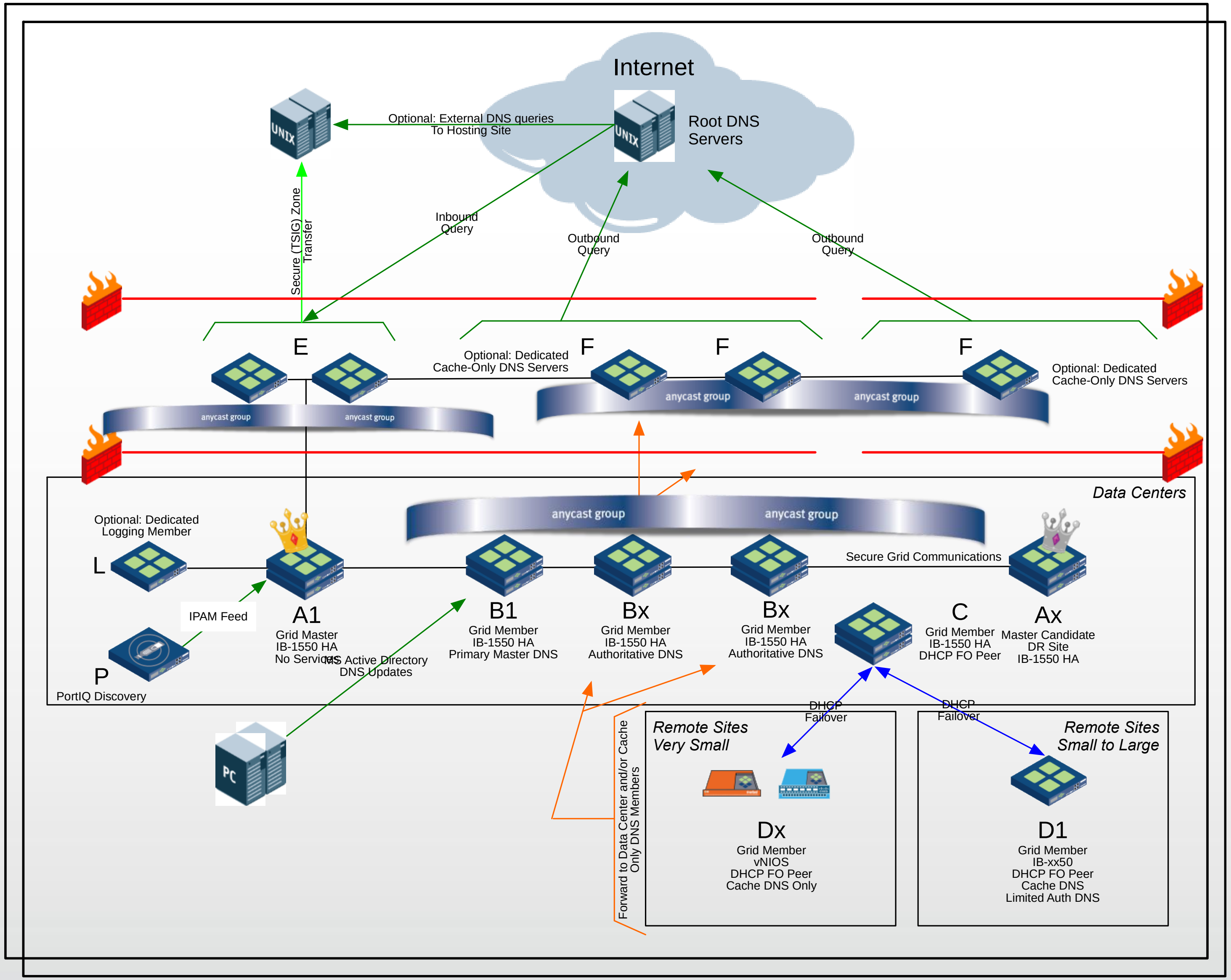

DNS Server europe.corp100.com
10.128.1.12
2001:db8::256:180:c223:214e
DNS Query
DNS Server us.corp100.com
10.128.1.12
2001:db8::256:180:c223:214e
DNS Query
(example: nslookup)
Client
europe.corp100.com
Intranet
DNS Server asiapac.corp100.com
10.128.1.12
2001:db8::256:180:c223:214e
DNS Server australia.corp100.com
10.128.1.12
2001:db8::256:180:c223:214e

DNS Anycast

Where to use it

Everywhere!

- Authoritative
  - Internal
  - External
- Recursive/Caching



Anycast

Considerations

- Routing protocols in use
- Network complexity
- DNS team’s access to routing information
- Troubleshooting

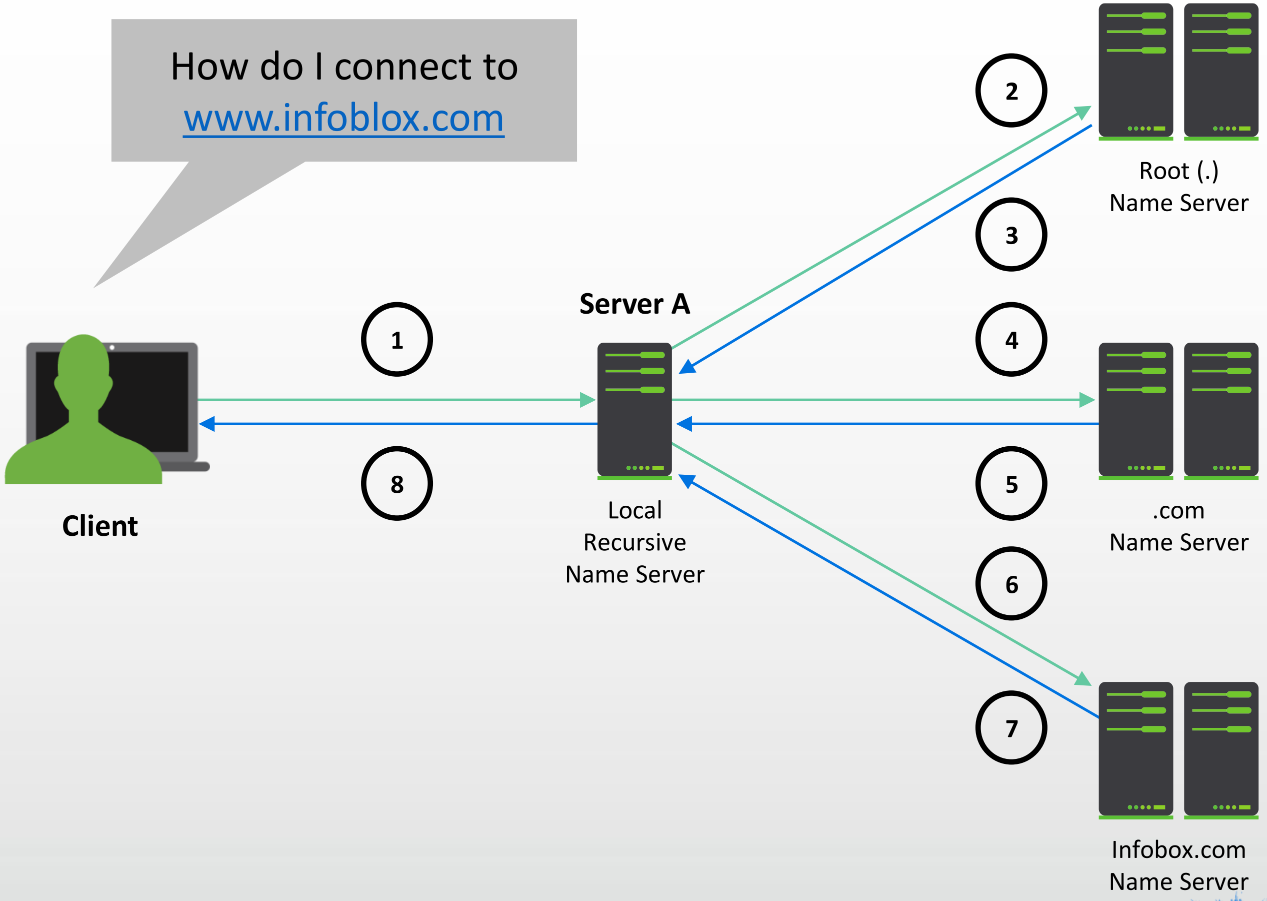
DNSSEC

DNSSEC

Traditional DNS walkthrough

Client queries for www.infoblox.com

1. **Client** queries it's locally configured DNS **Server A**
2. **Server A** Queries Root
3. **Root name servers** replies with NS and A records for .com (delegation)
4. **Server A** queries .com Name Servers
5. **.com name servers** reply with NS and A records for infoblox.com (delegation)
6. **Server A** queries **Infoblox Name Servers**
7. **Infoblox Name Servers** replies with A Record for www.infoblox.com
8. **Server A** caches the answer and returns the record to the Client

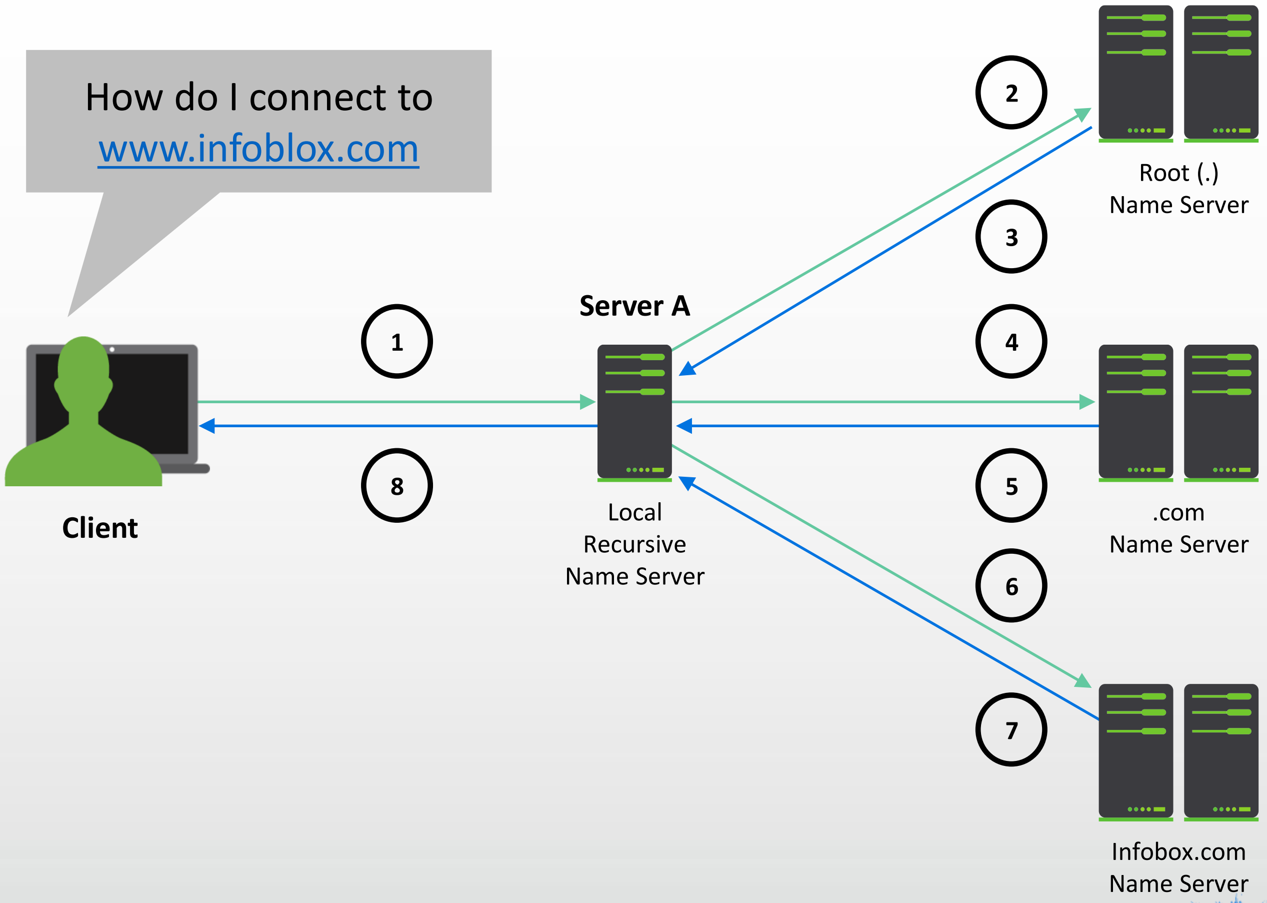


DNSSEC

DNSSEC validation walkthrough

Client queries for www.infoblox.com

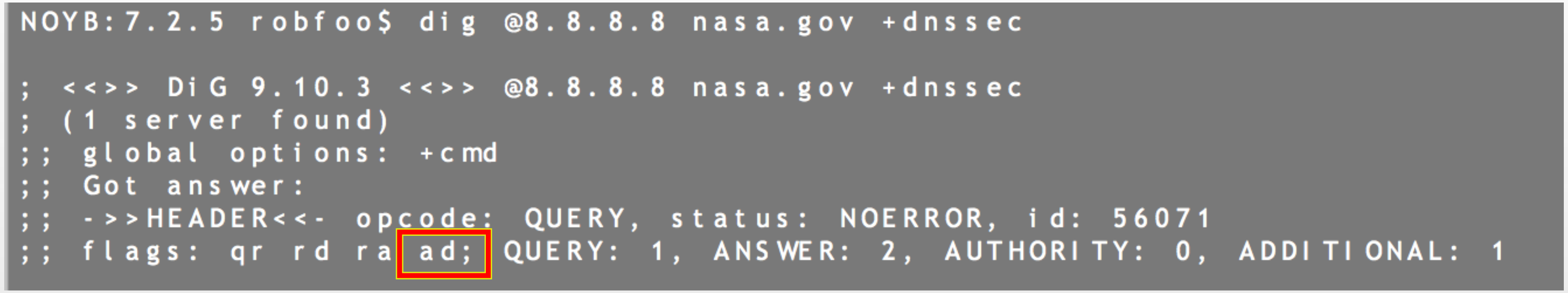
- Steps 1-7 happen as before.
- In **2**, **4** and **6** each time the recursive server queries it adds a DO bit to indicate it would like DNSSEC info
- Each response in **3**, **5** and **7** includes DNSSEC records including;
  - DNSKEY, DS and RRSIG
- Once **Server A** receives an answer it begins the validation



DNSSEC

Validation is in use today

- Google 8.8.8.8
- Comcast
- Neustar DNS Advantage
- …



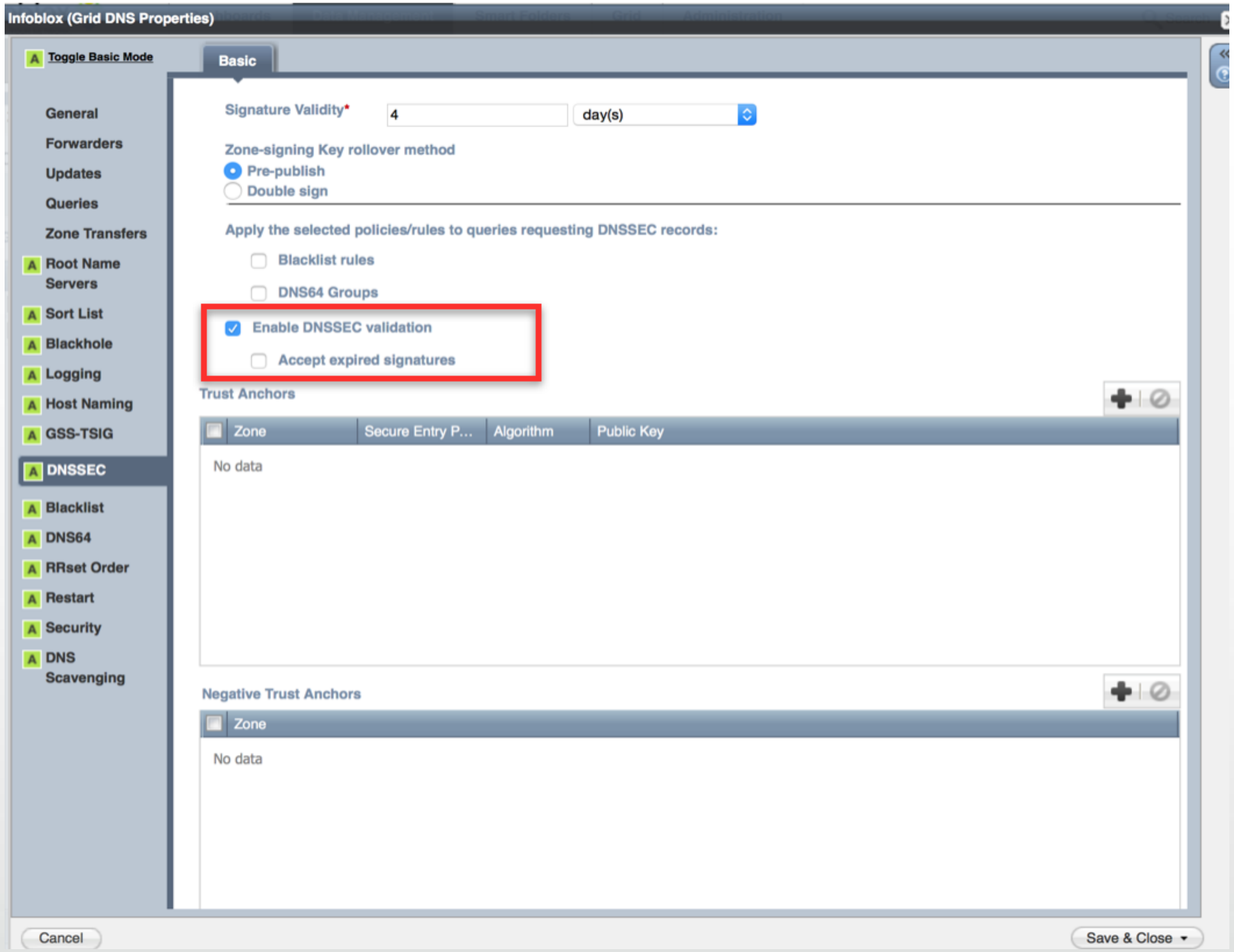
```
NOYB:7.2.5 robfoo$ dig @8.8.8.8 nasa.gov +dnssec

; <<>> DiG 9.10.3 <<>> @8.8.8.8 nasa.gov +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56071
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

- ad flag: Shows we have Authenticated Data

DNSSEC

Enabling validation



Signature Validity* 4 day(s)

Zone-signing Key rollover method

● Pre-publish

○ Double sign

Apply the selected policies/rules to queries requesting DNSSEC records:

□ Blacklist rules

□ DNS64 Groups

☑ Enable DNSSEC validation

□ Accept expired signatures

Trust Anchors

□	Zone	Secure Entry P...	Algorithm	Public Key
	No data			

Negative Trust Anchors

□	Zone
	No data

Questions?