RIPE DNS Resolver Recommendations

Shane Kerr <shane.kerr@ibm.com>

OARC 42 ● 2024-02-09

History

- Public DNS resolvers were getting popular
- All based outside of EU (mostly US)
- Worrying for EU
- EU created an RFP for EU public DNS resolver
- RIPE decided to encourage more resolvers
  - Not one more big centralized public resolver

Current Draft: Example 1

Packet Fragmentation Avoidance

Servers should be configured to avoid fragmentation.

For: ALL DNS resolver operators.

Packet fragmentation can cause issues with DNS over UDP, especially over IPv6. These issues can be minimized by choosing implementations that set IP options to avoid this, and by taking care with EDNS0 message sizes.

Recommendations are available in draft-ietf-dnsop-avoid-fragmentation.

Current Draft: Example 2

Transparency

DNS resolvers usually provide transparency reports once a year. The reports inform the public about disclosure of user information and removal of content required by law enforcement and other government agencies.

Transparency reports should (to the extent that the law allows) indicate which government agencies and law enforcement agencies request access on what basis.

It should also be clear from the transparency reports what kind of data has been requested and if content removal and content blocking have been requested. Categories of data include: Content Data, Basic Subscriber Data, Other Non-Content Data and Content Blocking.

Current Draft Topics [1/4]

- Who is it for?
  - Resolver operators
  - Users/operators choosing a resolver operator
- What is it not?
  - A checklist
  - Something that can be used for certification

Current Draft Topics [2/4]

- System & Network Hardening
  - Cloud vs. bare metal
  - Picking DNS software
- Network Considerations
  - IPv4/IPv6, addressing
  - Anycast
  - Filtering, (D)DoS
  - RPKI
- Capacity Planning
- System, network
- Resilience/Diversity
- Security
- Certifications

Current Draft Topics [3/4]

- DNSSEC
- UDP+TCP
- Fragmentation
- DoT/DoH/DoQ
  - DDR
- QNAME minimization

- NSEC caching
- Local root
- DNS cookies
- TTL limits
- Pre-fetch
- ECS

- Extended DNS errors
- Negative TA
- DNS error reporting
- TA reporting

Current Draft Topics [4/4]

- Privacy & anonymity
- Logging
- Filtering & blocking
  - Legal blocking
  - RPZ
  - Opt-in/Opt-out
- Transparency
- Standards
- Human rights considerations

Current Feedback [1/2]

- Convince people to run resolvers
  - Add a section on *WHY*
- Include HA section
- Make each recommendation measurable
  - Ideally externally and automatically
- Fix RFC number for Aggressive NSEC caching

Current Feedback [2/2]

- Use memorable IP addresses
- Don’t require aggressive NSEC caching
- Don’t encourage DNS cookies
- Omit RPZ

Next Steps

- Review feedback within task force
  - Abort, Retry, Ignore?
- Publish RIPE document
- 🍾🥂
- Decide what to ***do*** with the document

References

Message with current draft:
https://www.ripe.net/ripe/mail/archives/dns-wg/2023-November/004124.html

Working space of task force:
https://github.com/DNS-Resolver-BCP-TF/Resolver-Recommendations