KINDNS

An Initiative to Promote DNS Operational Best Practices

Fahd Batayneh
Stakeholder Engagement Sr. Manager – Middle East, ICANN

ICANN

What Is It?

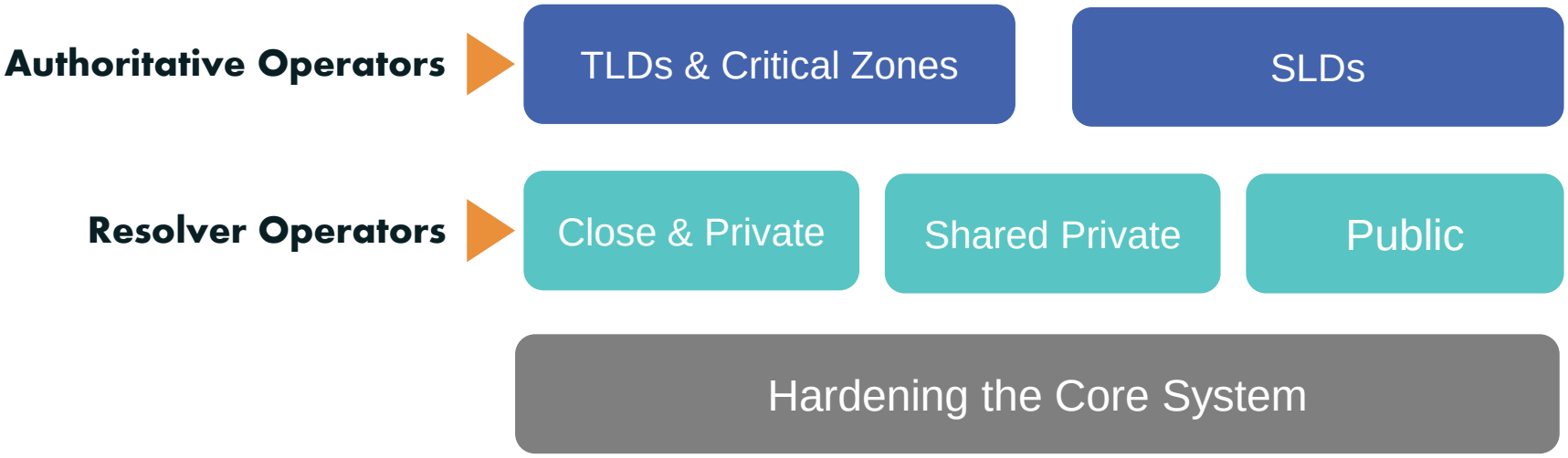
KINDNS

Knowledge-sharing and **I**nstantiating **N**orms for **D**NS (Domain Name System) and **N**aming **S**ecurity

An initiative to produce something simple to refer to that can **help a wide variety of DNS operators**, from small to large, to follow both the **evolution** of the DNS protocol and the **best practices** that the industry identifies for better security and more effective DNS operations.

*….. is pronounced "**kindness**"*

Targeted Operators



- Each category has 6-8 practices that we will encourage operators to implement. See www.kindns.org, for more details
- By joining KINDNS, DNS operators are voluntarily committing to **adhere** to these identified practices and act as "**goodwill ambassadors**" within the community.

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Authoritative DNS Operators of SLDs

KINDNS

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed & Private Resolver Operators

KINDNS

Private resolvers are not publicly accessible and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks

Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list **(**ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from a diversified Infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Shared Private Resolver Operators

KINDNS

Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. **For pr**ivacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Hardening the Core

In addition to implementing best practices for DNS security and for DNS availability and resilience, all operators must pay careful attention to practices for hardening the platforms their DNS services use.

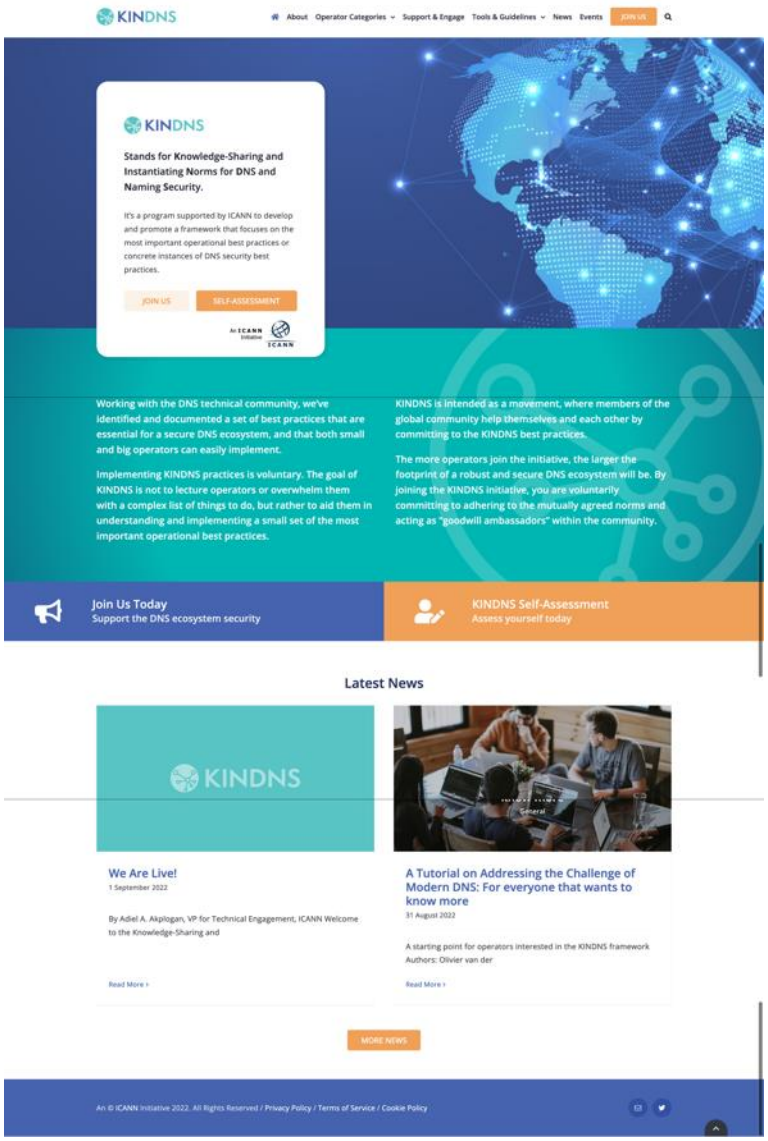
Core Hardening

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices

Self-Assessment & Enrollment

1. Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.
    - Self-Assessment is anonymous, and reports can be downloaded directly from the web site.
2. Operators can participate in one or multiple categories covered by KINDNS.
3. Beyond participating as Operator, organizations can also soon participate as sponsors.

Self Assessment Reports and Website



Selecting Best Current Practices (BCPs)

KINDNS

- How do we identify them ?
  - Draw from own operational experience
  - Ask operators (NOG lists, communities)
  - Review RFCs and other standards
    https://powerdns.org/dns-camel/
  - Shortlist based on relevance, ease of implementation, and how widespread the adoption is
- Ask operators to review the selection (kindns-discuss)
- Debate and justify choices

Engaging the community

Operators must agree on the selected BCPs

kindns-discuss list launched in 2021

- Encouraged operators from all backgrounds to join
- When in doubt, we asked community for advice on what they consider to be a BCP or not
- Some things were debated – is DNSSEC validation a **MUST** nowadays ? (We think so ☺)
- Some practices weren't implemented widely enough, or too complicated (not low hanging fruit) for small operators
  - e.g. Anycast

Engaging the community

KINDNS

- Others were still points of debate, like DoH
  - Increases privacy for end-users
  - But has an impact on visibility into client traffic:
    - Tracking malware infected clients by detecting known C&C FQDNs & DNS lookups to known abusive/problematic domain names (IOCs) becomes more difficult.

Current Focus: Phase 2

- Launching the **enrollment management** tool
- Continue to **engage with operators** to get them on board:
  - *Direct 1:1 Engagements*
  - *Workshops & webinars to raise awareness on KINDNS practices as part of our overall DNS ecosystem security awareness program*.
- **Translating** the website and the tools into other languages *(starting with the self-assessment and enrollment tools)*.
- Working with the community **to define indicators that can help measure** elements of the global DNS operation that are impacted by KINDNS practices' implementation (more on this later)
- **Evolving the Self-assessment** tool to be able to assess all or part of how operators implement the practices.
- Continue to encourage operators and partners to **contribute and improve** the practices of framework.

Discussion points:

1. **Adding Response Rate Limiting (RRL)** to Authoritative Servers' practice
   - ccTLD and critical Zone Operators
   - Other SLDs too?

2. **Addressing 'Split' responsibilities** for Authoritative servers' operation:
   - Zone file content is controlled by a third party. i.e Root server operators and the root zone itself.

3. **Access reliability:** Reachability over IPv6, RPKI for the prefix used for the DNS servers.

4. **Review team**: Volunteers from the community to work with staff to help with assessing participating candidates or other aspect of KINDNS practice evolution.

Discussion points:

5. Metrics

- What indicators are there that can help measure the impact of the adoption of KINDNS on global DNS operations ?
  - Could we measure the before and after ?
  - Increased resiliency, diversity
    - Look at NSset for instance
  - Some internal hardening procedures don't have directly measurable indicators
  - If there's a decrease in outages for a given set of domains / NSes, can that be attributed to KINDNS uptake ?
- Privacy improvements
  - DoH don't translate to more operational stability

Some external additional tools

- Zonemaster: https://zonemaster.net/
  - a program that tests a DNS zone configuration with different sanity checks configured in an engine and provides a zone health report.
- DNSviz: https://dnsviz.net/
  - provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and lists configuration errors detected by the tool.
- SuperTool: https://mxtoolbox.com/SuperTool.aspx
  - An integrated tool that can perform several kind of diagnostics on a domain name, IP address or host name. Documentation available at https://mxtoolbox.com/restapi.aspx
- Intodns: https://intodns.com/
  - checks the health and configuration and provides DNS report and mail servers report.
- There are others …

How to Stay Informed and Contribute

Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Wiki page	https://community.icann.org/display/KINDNS *Where you can still find all the working documents.*
Mailing list	kindns-discuss@icann.org

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: kindns-info@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg