Hot off the Queue: RFC 9704 *Validated Split Horizon DNS*

Tiru Reddy, Dan Wing, Kevin Smith, **Ben Schwartz**

OARC 44, 2025 Feb 7

Split Horizon DNS - *It's Bigger on the Inside*

- Internal-only domains like "wiki.internal.corp.example"
  - From the outside: **NXDOMAIN**
  - From the inside: **10.x.y.z**
- Special view domains like "www.corp.example"
  - From the outside: **2001:db8:...**
  - From the inside: **CNAME www-beta.corp.example**

But what if the clients don't use the network resolver?

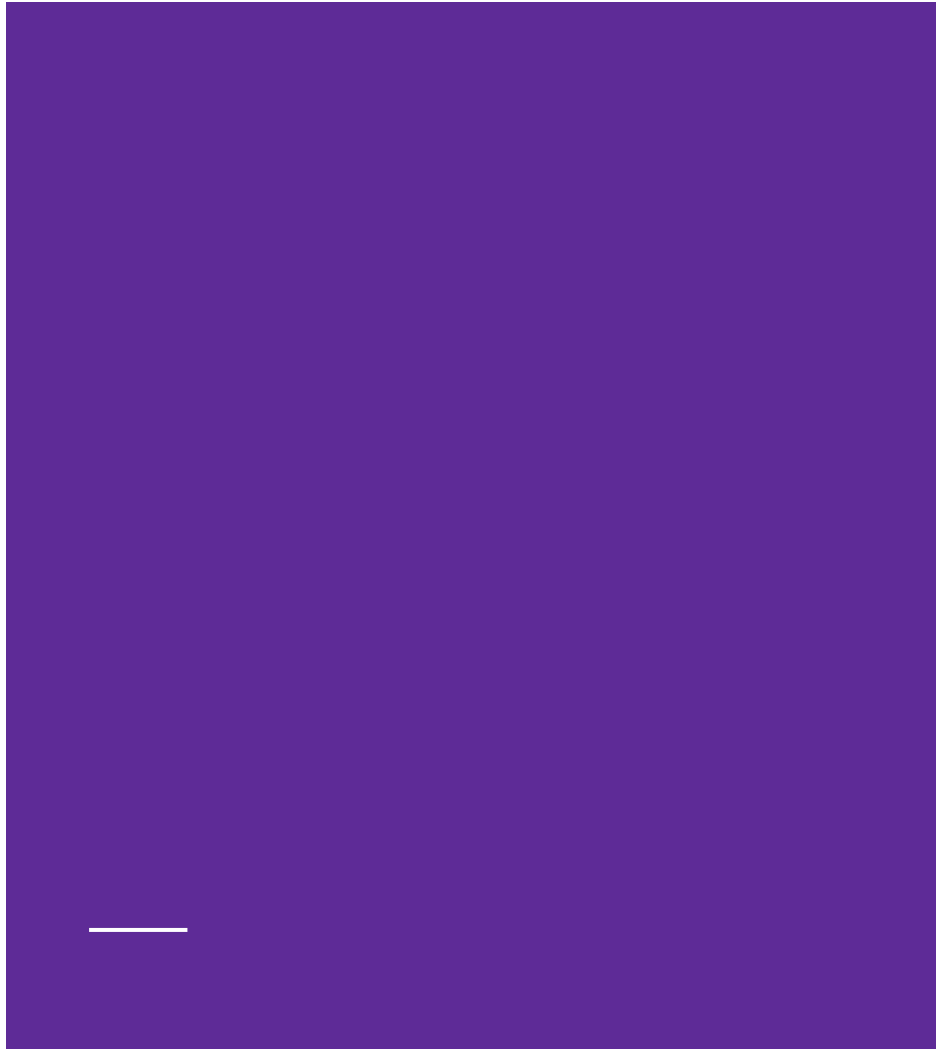
Clients increasingly distrust the local network

- DNS server override (/etc/resolv.conf)
- Validating stubs (option in iOS 16+)
- Encrypted DNS settings in OSes and Browsers (e.g. Firefox DoH)
- Third-Party VPN Apps
- Hyperscale Platform Proxies (e.g. iCloud Private Relay)

These are all incompatible with Split Horizon DNS.

Split Horizon DNS is indistinguishable from DNS hijacking

to a client who doesn't already trust the local network.



How do you make Split-Horizon DNS work with these clients?

How do you make Split-Horizon DNS work with these clients?

YOU DON'T

How do you make Split-Horizon DNS work with these clients?

~~YOU DON'T~~

RFC 9704

RFC 9704 in One Slide

- Network→Client:
  - Welcome! Your local DNS server is dns-atl.corp.example at 10.x.y.z and supports DoT" (DNR)
  - This DNS server claims to have an authorized split view for "internal" in the "corp.example" zone, provable with SHA-384 and the salt "12345". (RFC 9704 Authorization Claim)
- Client→corp.example
  - "corp.example, do you authorize a split view claim by dns-atl.corp.example?"
  - dns:**dns-atl.corp.example._splitdns-challenge.corp.example**?type=**TXT**
    - Must be resolved in a "tamper-proof" fashion
  - "token=${SHA-384(\x05**12345**\x08**internal**\x00}"
- Client→10.x.y.z
  - "Prove that you are dns-atl.corp.example" (DNS over TLS)
- Client directs queries for "wiki.internal.corp.example" to dns-atl.corp.example.

0

Number of known implementations of RFC 9704

2+

Independent parties who have to implement before anything useful happens.

With RFC 9704, Split Horizon DNS doesn't require a leap of faith.

But actually getting it implemented might require a miracle.

1

Weeks since publication of RFC 9704