Establishing Local DNS Authority in Split-Horizon Environments

draft-ietf-add-split-horizon-authority-00

IETF 114

July 2022

Tiru Reddy (Akamai)

Dan Wing (Citrix)

Kevin Smith (Vodafone)

Ben Schwartz (Google)

Update Summary

- New terms *Split-Horizon DNS* and *Validated Split-Horizon*
- Updated Scope section
- Use of pre-configured external resolver and DNSSEC
- Not leaking internal domains to external resolvers

Terminology

Split-Horizon DNS:

The DNS service provided by a resolver that also acts as an authoritative server for some names, providing resolution results that are meaningfully different from those in the Global DNS. (See "Split DNS" in Section 6 of [RFC8499].)

Terminology

Validated Split-Horizon

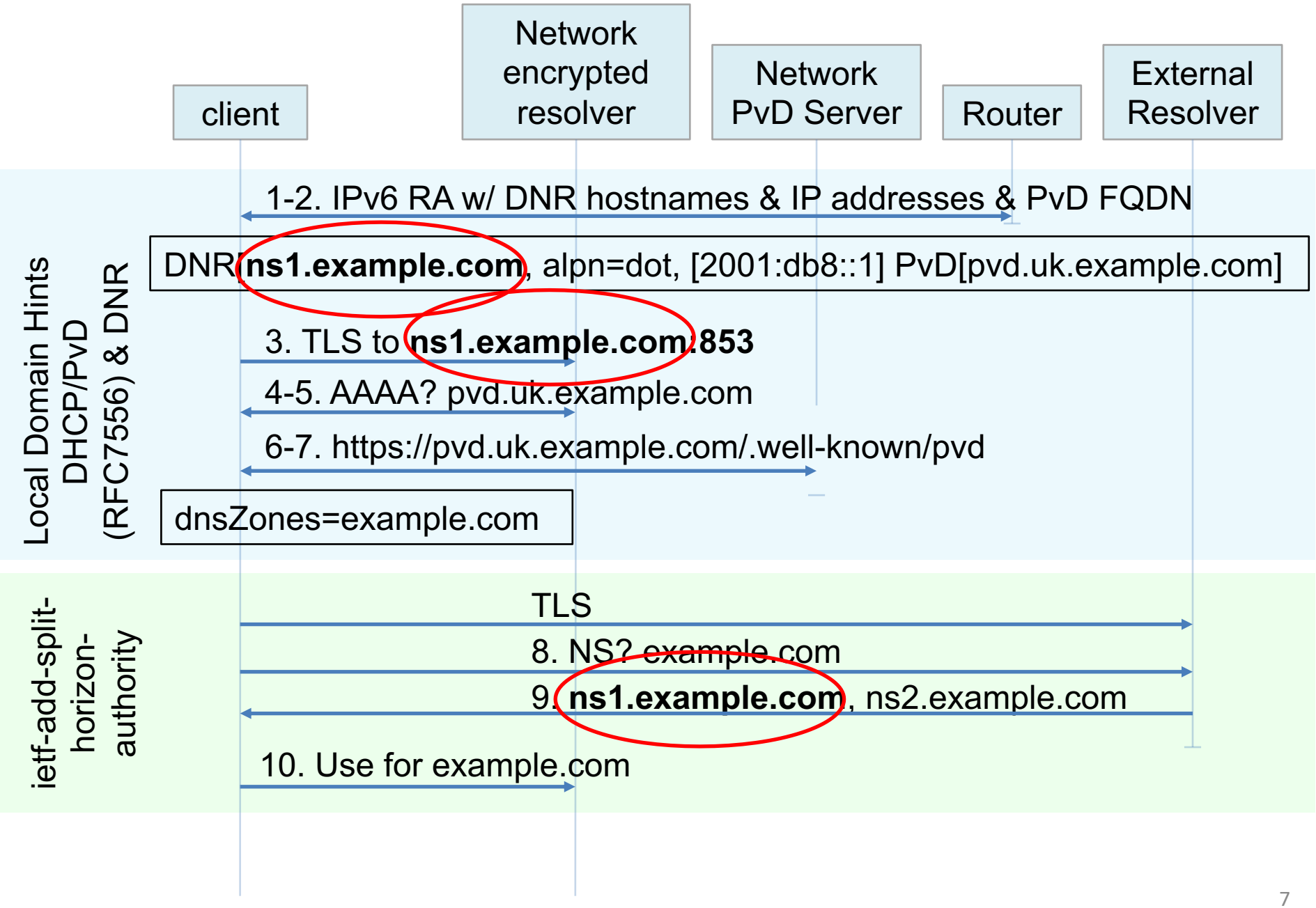
A split horizon configuration for some name is considered "validated" if the client has confirmed that a parent of that name has authorized this resolver to serve its own responses for that name. Such authorization generally extends to the entire subtree of names below the authorization point.

Scope

- Domain owner to create or authorize a split-horizon view of their domain.
  - DNS filtering is not enabled by this protocol.
- Applicable to any type of network offering split-horizon DNS configuration.
- No prior configuration on the endpoint that a local domain hint was indeed authorized by the domain.

Validate authority over local domain hints

- The draft's protocol requires:
  - External resolver agreement on zone ownership, or
  - DNSSEC validation


client
Network encrypted resolver
Network PvD Server
Router
External Resolver
Local Domain Hints DHCP/PvD (RFC7556) & DNR
1-2. IPv6 RA w/ DNR hostnames & IP addresses & PvD FQDN
DNR[ns1.example.com, alpn=dot, [2001:db8::1] PvD[pvd.uk.example.com]
3. TLS to ns1.example.com:853
4-5. AAAA? pvd.uk.example.com
6-7. https://pvd.uk.example.com/.well-known/pvd
dnsZones=example.com
ietf-add-split-horizon-authority
TLS
8. NS? example.com
9. ns1.example.com, ns2.example.com
10. Use for example.com

Use of Pre-configured Resolver

- "tamperproof" because any actor who could modify the NS response could already modify all of the user's other DNS responses.
- The clients MUST NOT relax the acceptance rules they would otherwise apply when using this resolver.
  - Client would continue to check the AD bit or validate RRSIGs locally using the resolver.
  - Conditional DNSSEC validation for NS query even if disabled for other DNS queries.

Not leaking internal domains

- The internal domains can be kept in a child zone of the local domain hints advertised by the network.
- Example:
  - Local domain hint = internal.example.com
  - Network-provided resolver = ns1.internal.example.com
  - Internal domain names = {private1.internal.example.com, private2.internal.example.com}.

draft-ietf-add-split-horizon-authority-00

- Comments and suggestions are welcome