Split-Horizon DNS Configuration

draft-reddy-add-enterprise-split-dns-04

IETF 111

July 2021

T. Reddy (McAfee)

D.Wing (Citrix)

Agenda

- Draft updates from 02 to 04 to address comments from WG
- Issues & Next Steps

Quick recap

- Discover local names (Similar to split DNS configuration in IKEv2 for RFC8598)
    - private-only
    - public but different version.

Update to Scope

- **Split-DNS configuration is applicable to any network** (e.g., Enterprise, ISP, Mobile network etc.).
  - Provisioning Domain (PvD) Key to provide the domains.
  - RFC8801: Discovery of explicit PvD and additional information using Web PvD (HTTP-over-TLS)

Proof of Authority

- NS Query of the domain using an encrypted public resolver or to a local resolver whose response is validated using DNSSEC
  - Public resolver: NXDOMAIN for private domains

- NS RRset matches, or is a subdomain of, any one of the ADN of the discovered network-designated encrypted DNS resolvers
  - Establish secure connection to authenticate the network-designated resolver and to resolve the domains in PvD

- NS RRset match fails, network is not authoritative
- The client does not have to perform validation for domains reserved for special purpose (".home.arpa“).

Discovery of Network block policy

- **Policy expression** (not “policy prescription”)
  - PvD Keys
    - NetworkDNSOnly
    - ErrorNetworkDNSOnly (Human-friendly description)
  - Scope restricted to Enterprise networks
    - User has explicitly overridden local DNS settings for a specific network
    - DNS client may not use Do53 to resolve the non-network-designated resolver (no EDE)

- **Retain or Remove the network policy from the draft**
- **If removed, WG interest to peruse.**

draft-reddy-add-enterprise-split-dns-04

- Comments and suggestions are welcome
- Consider for WG adoption