Split-Horizon DNS Configuration in Enterprise Networks

draft-reddy-add-enterprise-split-dns-01

IETF 110

March 2021

T. Reddy (McAfee)
D.Wing (Citrix)

Agenda

- Goals & Scope
- Proposed Mechanism
- Issues & Next Steps

Goals

- Discover local names (Similar to split DNS configuration in IKEv2 for RFC8598)
- Discover if the Enterprise network offers a split DNS configuration

Scope

- Client can authenticate the identity of the network (or has pre-existing relationship with the network).
  - The user has authorized the client to override local DNS settings for a specific network.
  - BYOD devices joining Enterprise network without any MDM and configuration profile (e.g., using EAP-pwd, EAP-PSK).

Mechanism

- Provisioning Domains (PvDs) provide network configuration information to access network including
  - **DNS resolution**
- RFC8801: Discovery of explicit PvD and additional information using Web PvD (HTTP-over-TLS).
  - **PvD Keys to provide the domains**
    - **private-only or**
    - **public but different version.**

Web PVD example

```
{
        "identifier": "cafe.example.com.",
        "expires": "2020-05-23T06:00:00Z",
        "prefixes": ["2001:db8:1::/48", "2001:db8:4::/48"],
        "SplitDNSAllowed": True,
         "dnsZones:": [{
             "name": "city.other.test",
             "private-only": true
         },{
             "name": "example.com",
             "private-only": false
         }]
 }
```

Zones do not exist in Global DNS (Issue#1)

- NSEC3 or NSEC used to validate domains do not exist in Global DNS

- What happens if public resolver is not reachable ?
  - Top well-known domains and TLDs stored locally (it is not a full-proof solution).
  - RFC8598: ***IKE clients MAY want to require whitelisted domains for Top-Level Domains (TLDs) and Second-Level Domains (SLDs) to further prevent malicious DNS redirections for well-known domains. This prevents users from unknowingly giving DNS queries to third parties***.

Prove network is authoritative of the public domain (Issue#2)

- Different version of the public domain in the network
- Proof of authority
  - NS Query of the public domain
  - NS RRset matches the ADN of discovered network-provided resolver (DNR)
  - Establish secure connection to authenticate the network-provided resolver to resolve the domains in PvD

draft-reddy-add-enterprise-split-dns-01

- Comments and suggestions are welcome
- Consider for WG adoption