IETF 96 IPSECME SPLIT-DNS

draft-pauly-ipsecme-split-dns-01

Tommy Pauly
Paul Wouters

INTERNAL_DOMAIN CP

- When in split tunnel mode, we need split-DNS functionality
- Client and Server need to agree on a list of domain names that live across the VPN

```
CP(CFG_REQUEST) =
    INTERNAL_IP4_ADDRESS()
    INTERNAL_IP4_DNS()
    INTERNAL_DNS_DOMAIN(example.com)
    INTERNAL_DNS_DOMAIN(other.com)

  CP(CFG_REPLY) =
    INTERNAL_IP4_ADDRESS(198.51.100.234)
    INTERNAL_IP4_DNS(198.51.100.2)
    INTERNAL_IP4_DNS(198.51.100.4)
    INTERNAL_DNS_DOMAIN(example.com)
    INTERNAL_DNS_DOMAIN(city.other.com)
```

- The IP's of the nameserver MUST be within the range of the traffic selectors negotiated
- Nameserver reconfiguration MUST be done after the CHILD SA covering the DNS IP's are available

INTERNAL_DNSSEC_TA CP

- If internal DNS domain is signed with a private trust anchor, client needs to obtain and configure this domain's private trust anchor.

- Server can send CP payload with DNSKEY RRtype
  - In DNS presentation format (not DNS wire format)
  - We would like to use DS instead of DNSKEY
    - Seems resolvers can/will deal with fetching DNSKEY insecurely and confirm the DS record obtained from CP.

INTERNAL_DNSSEC_TA CP

```
CP(CFG_REQUEST) =
   INTERNAL_IP4_ADDRESS()
   INTERNAL_IP4_DNS()
   INTERNAL_DNS_DOMAIN()

 CP(CFG_REPLY) =
   INTERNAL_IP4_ADDRESS(198.51.100.234)
   INTERNAL_IP4_DNS(198.51.100.2)
   INTERNAL_IP4_DNS(198.51.100.4)
   INTERNAL_DNS_DOMAIN(example.com)
   INTERNAL_DNSSEC_TA(example.com IN DS 1321 8 2 XXXXXXXX)
   INTERNAL_DNS_DOMAIN(city.other.com)
```

Moving forward

- We have interop between Apple and Libreswan for INTERNAL_DOMAIN

- What do want?
  - Working Group adoption
  - Early Code Point
- When do we want it?
  - now!
- DNSKEY or DS records?
  - We would like to switch to DS records