IKEv2 Configuration for Encrypted DNS

draft-btw-add-ipsecme-ike-01

Mohamed Boucadair (Orange)
Tirumaleswar Reddy (McAfee, Inc.)
Dan Wing (Citrix Systems, Inc.)
Valery Smyslov (ELVIS-PLUS)

November 2020, IETF#109
Status

• Presented at IETF#108
• Comments raised so far:
  – Complexity induced by muxing the attributes (mask bit)
  – Check if there are DoQ specifics
  – Supply DoH URI Template
• Fixed in 01: See next slide
• There are trade-offs
Changes from -00

• New Attribute format for Encrypted DNS
  – separate attribute types for each Encrypted DNS type (DoT, DoH, DoQ) and for IP version
    • ENCDNS_IP4_DOT, ENCDNS_IP6_DOT
    • ENCDNS_IP4_DOH, ENCDNS_IP6_DOH
    • ENCDNS_IP4_DOQ, ENCDNS_IP6_DOQ
  – port number is added
    • Triggered by a check with the authors of DoQ to assess if they have specific configuration data to be returned to DoQ clients
  – “scope” bit is removed
Separate Attribute Types

• We assume all types of Encrypted DNS are equivalent, so the client can be configured with any of them
  – with this approach the client includes all attributes for Encrypted DNS types it supports and the server returns back one (or few) of them with the DNS server(s) details
  – each attribute can contain several IP addresses of resolvers
Port Number

• Support for customizing port number for DNS servers is added
  – Port number is the same for all IP-addresses in a single attribute
  – if DNS servers have different port numbers, then separate attributes of the same type should be returned
Scope

• “Scope” bit is removed
  – DNS server selected by the client outside of the VPN tunnel is out of scope of this draft
# Attribute Format

```
+----------------+-------------------+-------------------+
|                | Attribute Type     | Length             |
|                | Port Number        | RESERVED           |
|                | Num Addresses      |                   |
+----------------+-------------------+-------------------+
| ~               | IP Addresses       | ~                 |
+----------------+-------------------+-------------------+
| ~               | DNS Authentication Domain Name | ~     |
+----------------+-------------------+-------------------+
```

DoH Specifics

- DoH servers may support more than one URI Template
- The DoH server may also host several DoH services (e.g., no-filtering, blocking adult content)
  - These services can be discovered as templates
- The client uses a well-known URI "resinfo" to discover these templates:
  ```
  https://doh.example.com/.well-known/resinfo
  ```
  Authentication Domain Name To be assigned by IANA
- Discovering the well-known URI is out of scope of this draft and is discussed in Section 5 of draft-btw-add-home
- Draft will use whatever mechanism(s) are finalized by the ADD WG for URI template discovery
Next Steps

• Comments?
• Questions?
• Consider WG adoption

Thank you