IKEv2 Configuration for Encrypted DNS

`draft-btw-add-ipsecme-ike`

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

July 2020, IETF#108

Agenda

- Context
- A Sample Use Case
- IKE Configuration Attribute for Encrypted DNS
- Next Steps

Problem Description

- Several schemes to encrypt DNS have been specified
  - DNS over TLS (RFC 7858)
  - DNS over DTLS (RFC 8094)
  - DNS over HTTPS (RFC 8484)
- …And others are being specified:
  - DNS over QUIC (draft-ietf-dprive-dnsoquic)
- ***How to securely provision clients to use Encrypted DNS? This use can be within or outside the IPsec tunnel***

A Sample Use Case: DNS Offload

- VPN service providers can offer publicly accessible Encrypted DNS
  - the split-tunnel VPN configuration allows the client to access the DoH/DoT servers hosted by the VPN provider ***without traversing the tunnel***

A Sample Use Case: Protecting Internal DNS Traffic

- DoH/DoT ensures DNS traffic is ***not susceptible to internal attacks***
  - see draft-arkko-farrell-arch-model-t-03#section-3.2.1
- encrypted DNS can benefit to Roaming Enterprise users to ***enhance privacy***
  - With DoH/DoT the visibility of DNS traffic is limited to only the parties authorized to act on the traffic (“Zero Trust Architecture”)

Using IKE to Configure Encrypted DNS on Clients

- New configuration attribute `INTERNAL_ENC_DNS` is defined to convey encrypted DNS information to clients:
  - Encrypted DNS type (e.g., DoH/DoT)
  - Scope of encrypted DNS use
  - One or more encrypted DNS server IPv6 addresses
    - For IPv4 addresses are encoded using IPv4-mapped IPv6 address format defined in RFC4291
  - Fully qualified authentication domain name

- The `INTERNAL_ENC_DNS` attributes are exchanged in `IKE_AUTH` exchange along with other configuration attributes

Attribute Format

Scope bit
0: Outside the tunnel
1: Within the tunnel

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-----------------------------+-------------------------------+
|R|         Attribute Type      |            Length             |
+-+-------------+---------------+-------------------------------+
|S|Enc DNS Type | Num addresses |                               |
+-+-------------+---------------+                               +
|                          IPv6 Addresses                       ~
|                               +-------------------------------+
~                               |                               |
+-------------------------------+                               |
|                                                               |
~                  DNS Authentication Domain Name               ~
|                                                               |
+---------------------------------------------------------------+
```

1: DoT
2: DoH
…

Interaction with Split DNS IKE Extension

- RFC 8598 *Split DNS Configuration for the Internet Key Exchange Protocol Version 2 (IKEv2)* requires `INTERNAL_IP*_DNS` attribute(s) to be present when `INTERNAL_DNS_DOMAIN` is included

- It is **no more needed** if `INTERNAL_ENC_DNS` attribute is present

Next Steps

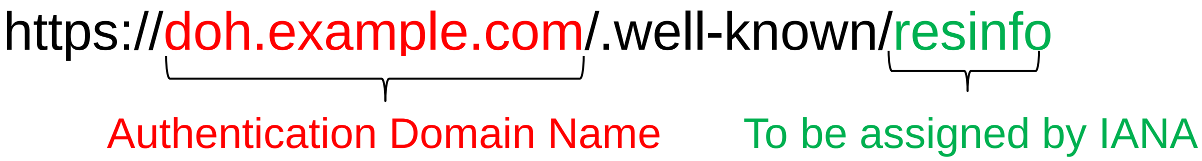
- Comments?
- Questions?
- Suggestions for progressing the document?

Thank you

Backup Slides

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 draft-btw-add-rfc8484-clarification