ADD
Internet-Draft
Intended status: Standards Track
Expires: October 9, 2020

M. Boucadair
Orange
T. Reddy
McAfee
D. Wing
Citrix
V. Smyslov
ELVIS-PLUS

April 7, 2020

Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS
draft-btw-add-ipsecme-ike-00

Abstract

This document specifies a new Internet Key Exchange Protocol Version 2 (IKEv2) Configuration Payload Attribute Type for encrypted DNS such as DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 9, 2020.

Table of Contents

1. Introduction

This document specifies encrypted DNS configuration for an IKE initiator, particularly the Authentication Domain Name (ADN, defined in [RFC8310]) of DNS-over-HTTPS (DoH) [RFC8484] or DNS-over-TLS (DoT) [RFC7858] server using Internet Key Exchange Protocol Version 2 (IKEv2) [RFC7296].

Particularly, this document introduces a new IKEv2 Configuration Payload Attribute Types (Section 4) for the support of encrypted DNS servers (e.g., DoT, DoH).

Sample use cases are discussed in Section 3. The Configuration Payload Attribute Type defined in Section 4 is not specific to these deployments, but can be used in other deployment contexts.

Note that, for many years, typical designs has often considered that the DNS server was usually located inside the protected domain, but could theoretically be located outside of it. With DoH or DoT, the latter option becomes plausible.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [RFC8499] and [I-D.ietf-dnsop-terminology-ter].

Also, this document makes use of the terms defined in [RFC7296]. In particular, readers should be familiar with "initiator" and "responder" terms used in that document.

Do53 refers to unencrypted DNS.

'DoH/DoT' refers to DNS-over-HTTPS and/or DNS-over-TLS.

3. Sample Deployment Scenarios

3.1. Roaming Enterprise Users

In this Enterprise scenario (Section 1.1.3 of [RFC7296]), a roaming user connects to the Enterprise network through an IPsec tunnel. The split-tunnel Virtual Private Network (VPN) configuration allows the endpoint to access hosts that resides in the Enterprise network [RFC8598] using that tunnel; other traffic not destined to the Enterprise does not traverse the tunnel. In contrast, a non-split-tunnel VPN configuration causes all traffic to traverse the tunnel into the enterprise.

For both split- and non-split-tunnel configurations, the use of DoT/DoH instead of Do53 provides privacy and integrity protection along the entire path (rather than just to the VPN termination device) and can communicate the DoT/DoH server policies.

For split-tunnel VPN configurations, the endpoint uses the Enterprise-provided DoT/DoH server to resolve internal-only domain names.

For non-split-tunnel VPN configurations, the endpoint uses the Enterprise-provided DoT/DoH server to resolve both internal and external domain names.

Enterprise networks are susceptible to internal and external attacks. To minimize that risk all enterprise traffic is encrypted (Section 2.1 of [I-D.arkko-farrell-arch-model-t]).

3.2. VPN Service Provider

Legacy VPN service providers usually preserve end-users' data confidentiality by sending all communication traffic through an encrypted tunnel. A VPN service provider can also provide guarantees about the security of the VPN network by filtering malware and phishing domains.

Browsers and OSes support DoH/DoT; VPN providers may no longer expect DNS clients to fallback to Do53 just because it is a closed network.

The DoT/DoH server hosted by the VPN service provider can be securely discovered by the endpoint using the IKEv2 Configuration Payload Attribute Type.

3.3. DNS Offload

VPN service providers typically allow split-tunnel VPN configuration in which users can choose applications that can be excluded from the tunnel. For example, users may exclude applications that restrict VPN access.

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

The DoT/DoH server hosted by the VPN service provider can be securely discovered by the endpoint using the IKEv2 Configuration Payload Attribute Type.

4. INTERNAL_ENC_DNS Attribute

The INTERNAL_ENC_DNS IKEv2 Configuration Payload Attribute Type is used to configure an encrypted DNS server. The format of this attribute is shown in Figure 1.

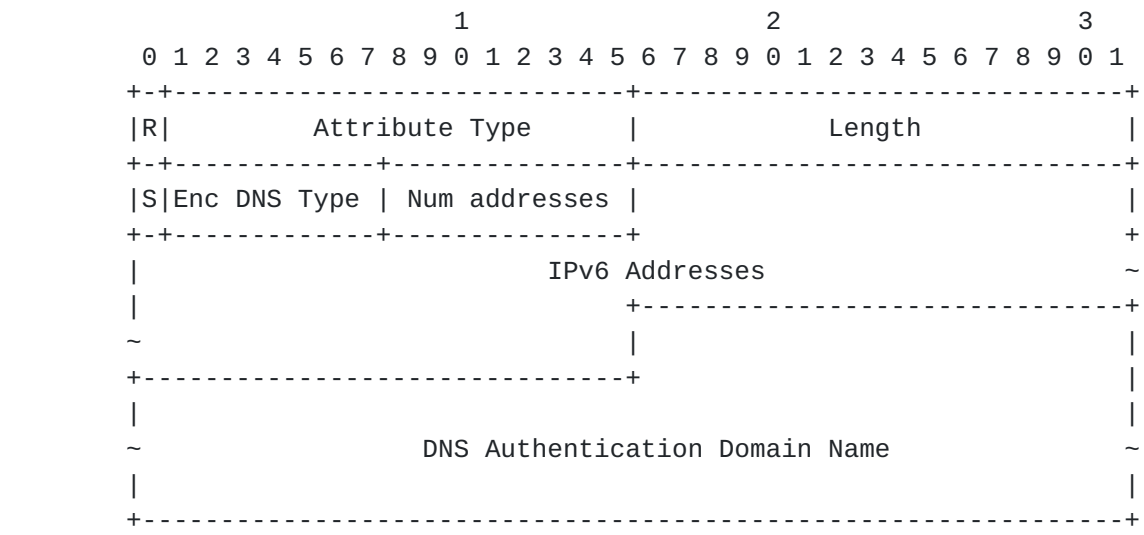

Figure 1: INTERNAL_ENC_DNS Attribute Format

The fields of the attribute shown in Figure 1 are as follows:

- R: Reserved bit; refer to Section 3.15.1 of [RFC7296].

- Attribute Type: MUST be set to TBA (Section 8.1).

- Length: Length of the data in octets. It MUST be set to 1 if the Configuration payload has types CFG_REQUEST or CFG_ACK or to (2 + Length of the ADN + N * 16) if the Configuration payload has types CFG_REPLY or CFG_SET; N being the number of included IP addresses ('Num addresses').

- S: Scope bit. This bit controls whether the DNS queries are sent within the tunnel or outside. If set, this bit instructs the initiator to send encrypted DNS queries outside the tunnel. If the bit is unset, the queries are sent inside the tunnel. The default value of this bit is "0".

- Encrypted DNS Type: Indicates the type of the encrypted DNS server conveyed in this attribute. The following values are defined:

  0: Reserved

  1: DoT

  2: DoH

  See Section 8.2 for future assignment considerations.

- Num addresses: If Length > 1, it indicates the number of enclosed IP addresses.

- IPv6 Address(es): One or more IPv6 addresses to be used to reach the encrypted DNS identified by the name in the DNS Authentication Domain Name.

  IPv4 addresses MUST be encoded using the IPv4-Mapped IPv6 Address format defined in [RFC4291].

- Authentication Domain Name: A fully qualified domain name of the DoT (or DoH) server following the syntax defined in [RFC5890]. The name MUST NOT contain any terminators (e.g., NULL, CR).

  An example of valid ADN for DoH server is "doh1.example.com".

5. URI Template

DoH servers may support more than one URI Template [RFC8484]. The following sub-sections discuss some candidate solutions for a DoH client to retrieve the list of supported templates by a DoH server. Also, if the resolver hosts several DoH services (e.g., no-filtering, blocking adult content, blocking malware), these services can be discovered as templates.

This section will be updated to reflect the outcome of the discussion in [I-D.btw-add-home].

How a DoH client makes use of the configured DoH services is out of the scope of this document.

6. IKEv2 Protocol Exchange

This section describes how an initiator can be configured with an encrypted DNS server (e.g., DoH, DoT) using IKEv2.

Initiators indicate the support of an encrypted DNS in the CFG_REQUEST payloads by including INTERNAL_ENC_DNS attribute, while responders supply the encrypted DNS configuration in the CFG_REPLY payloads. Concretely:

If the initiator supports encrypted DNS, it includes one or more INTERNAL_ENC_DNS attributes in the CFG_REQUEST with the "Encrypted DNS Type" set to the requested encrypted DNS type (Section 4). For each supported encrypted DNS type the initiator MUST include exactly one INTERNAL_ENC_DNS attribute with the Length field set to 1.

If an INTERNAL_ENC_DNS attribute is included in the CFG_REQUEST, the INTERNAL_ENC_DNS attribute MUST NOT include an ADN and list of IP addresses.

For each INTERNAL_ENC_DNS attribute from the CFG_REQUEST, if the responder supports the corresponding encrypted DNS type, then it MAY send back an INTERNAL_ENC_DNS attribute in the CFG_REPLY with this encrypted DNS type and an appropriate list of IP addresses and ADN. The list of IP addresses MUST NOT be empty.

If the CFG_REQUEST includes an INTERNAL_ENC_DNS attribute but the CFG_REPLY does not include an INTERNAL_ENC_DNS, this is an indication that requested encrypted DNS type(s) is not supported by the responder.

The behavior of the responder if it receives both INTERNAL_ENC_DNS and INTERNAL_IP6_DNS (or INTERNAL_IP4_DNS) attributes is policy-based and deployment-specific. However, it is RECOMMENDED that if the responder includes at least one INTERNAL_ENC_DNS attribute in the reply, it should not include any of INTERNAL_IP4_DNS/ INTERNAL_IP6_DNS attributes.

The DNS client establishes a DoH/DoT session with the address(es) conveyed in INTERNAL_ENC_DNS and uses the mechanism discussed in Section 8 of [RFC8310] to authenticate the DNS server certificate using the authentication domain name conveyed in INTERNAL_ENC_DNS.

If the IPsec connection is a split-tunnel configuration and the initiator negotiated INTERNAL_DNS_DOMAIN as per [RFC8598], the DNS client MUST resolve the internal names using INTERNAL_ENC_DNS DNS servers.

Note: [RFC8598] requires INTERNAL_IP6_DNS (or INTERNAL_IP4_DNS) attribute to be mandatory present when INTERNAL_DNS_DOMAIN is included. This specification relaxes that constraint in the presence of INTERNAL_ENC_DNS attribute.

7. Security Considerations

This document adheres to the security considerations defined in [RFC7296]. In particular, this document does not alter the trust on the DNS configuration provided by a responder.

Networks are susceptible to internal attacks as discussed in Section 3.2 of [I-D.arkko-farrell-arch-model-t]. Hosting DoH/DoT server even in case of split-VPN configuration minimizes the attack vector (e.g., a compromised network device cannot monitor/modify DNS

traffic). This specification describes a mechanism to restrict access to the DNS messages to only the parties that need to know.

In most deployment scenarios, the initiator expects that it is using the DoH/DoT server hosted by a specific organization or enterprise. The DNS client can validate the signatory (i.e., cryptographically attested by the organization hosting the DoH/DoT server) using, for example, [I-D.reddy-add-server-policy-selection], and the user can review human-readable privacy policy information of the DNS server and assess whether the DNS server performs DNS-based content filtering. This helps to protect from a compromised IKE server advertising a malicious DoH/DoT server.

The initiator may trust the DoH/DoT servers supplied by means of IKEv2 from a trusted responder more than the locally provided DNS servers, especially in the case of connecting to unknown or untrusted networks (e.g., coffee shops or hotel networks). In addition, the initiator may prefer IKEv2-supplied DoH/DoT servers if they provide additional features (e.g., malware filtering) compared to the pre-configured DNS servers and meets the privacy preserving data policy requirements of the user.

If the DoH/DoT server that was discovered by means of IKEv2 does not meet the privacy preserving data policy and filtering requirements of the user, the user can instruct the DNS client to take appropriate actions. For example, the action can be to use the local DoH/DoT server only to access internal-only DNS names and use another DNS server (that addresses his/her expectations) for public domains. Such actions and their handling is out of scope.

If IKEv2 is being negotiated with an anonymous or unknown endpoint (such as for Opportunistic Security [RFC7435]), the initiator MUST NOT use INTERNAL_ENC_DNS servers unless it is pre-configured in the OS or the browser.

This specification does not extend the scope of accepting DNSSEC trust anchors beyond the usage guidelines defined in Section 6 of [RFC8598].

8. IANA Considerations

8.1. Configuration Payload Attribute Type

This document requests IANA to assign the following new IKEv2 Configuration Payload Attribute Types from the "IKEv2 Configuration Payload Attribute Types" namespace available at https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-21.

Value	Attribute Type	Multi-Valued	Length	Reference
TBA	INTERNAL_ENC_DNS	YES	1 or more	RFC XXXX

8.2. Encrypted DNS Types

This document requests IANA to create a new registry called "Encrypted DNS Types" under "Internet Key Exchange Version 2 (IKEv2) Parameters" available at https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-21. The initial values of the registry is as follows:

Value	Description	Reference
0	Reserved	RFC XXXX
1	DNS-over-TLS (DoT)	RFC XXXX
2	DNS-over-HTTPs (DoH)	RFC XXXX

New values are assigned on a First Come, First Served (FCFS) basis (Section 4.4 of [RFC8126]).

9. Acknowledgements

Many thanks to Yoav Nir, Christian Jacquenet, Paul Wouters, and Tommy Pauly for the review and comments.

Yoav and Paul suggested the use of one single attribute carrying both the name and an IP address instead of depending on the existing INTERNAL_IP6_DNS and INTERNAL_IP4_DNS attributes.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

10.2. Informative References

[I-D.arkko-farrell-arch-model-t]
Arkko, J. and S. Farrell, "Challenges and Changes in the Internet Threat Model", draft-arkko-farrell-arch-model-t-03 (work in progress), March 2020.

[I-D.btw-add-home]
Boucadair, M., Reddy.K, T., Wing, D., and N. Cook, "DNS-over-HTTPS and DNS-over-TLS Server Discovery and Deployment Considerations for Home and Mobile Networks", draft-btw-add-home-04 (work in progress), March 2020.

[I-D.ietf-dnsop-terminology-ter]
Hoffman, P., "Terminology for DNS Transports and Location", draft-ietf-dnsop-terminology-ter-01 (work in progress), February 2020.

[I-D.reddy-add-server-policy-selection]
Reddy.K, T., Wing, D., Richardson, M., and M. Boucadair, "DNS Server Selection: DNS Server Information with Assertion Token", draft-reddy-add-server-policy-selection-00 (work in progress), March 2020.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8598] Pauly, T. and P. Wouters, "Split DNS Configuration for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8598, DOI 10.17487/RFC8598, May 2019, <https://www.rfc-editor.org/info/rfc8598>.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: TirumaleswarReddy_Konda@McAfee.com

Dan Wing
Citrix Systems, Inc.
USA

Email: dwing-ietf@fuggles.com

Valery Smyslov
ELVIS-PLUS
RU

Email: svan@elvis.ru