

Network  
Internet-Draft  
Intended status: Standards Track  
Expires: July 26, 2018

T. Pauly  
Apple Inc.  
P. Wouters  
Red Hat  
January 22, 2018

## **Split DNS Configuration for IKEv2 draft-ietf-ipsecme-split-dns-04**

### Abstract

This document defines two Configuration Payload Attribute Types for the IKEv2 protocol that add support for private DNS domains. These domains should be resolved using DNS servers reachable through an IPsec connection, while leaving all other DNS resolution unchanged. This approach of resolving a subset of domains using non-public DNS servers is referred to as "Split DNS".

### 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 <http://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 July 26, 2018.

### Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4](#).e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">2</a>
<a href="#">1.1.</a>	<a href="#">Requirements Language . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Background . . . . .</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Protocol Exchange . . . . .</a>	<a href="#">3</a>
<a href="#">3.1.</a>	<a href="#">Configuration Request . . . . .</a>	<a href="#">4</a>
<a href="#">3.2.</a>	<a href="#">Configuration Reply . . . . .</a>	<a href="#">4</a>
<a href="#">3.3.</a>	<a href="#">Mapping DNS Servers to Domains . . . . .</a>	<a href="#">5</a>
<a href="#">3.4.</a>	<a href="#">Example Exchanges . . . . .</a>	<a href="#">5</a>
<a href="#">3.4.1.</a>	<a href="#">Simple Case . . . . .</a>	<a href="#">5</a>
<a href="#">3.4.2.</a>	<a href="#">Requesting Domains and DNSSEC trust anchors . . . . .</a>	<a href="#">6</a>
<a href="#">4.</a>	<a href="#">Payload Formats . . . . .</a>	<a href="#">6</a>
<a href="#">4.1.</a>	<a href="#">INTERNAL_DNS_DOMAIN Configuration Attribute Type . . . . .</a>	<a href="#">6</a>
<a href="#">4.2.</a>	<a href="#">INTERNAL_DNSSEC_TA Configuration Attribute . . . . .</a>	<a href="#">7</a>
<a href="#">5.</a>	<a href="#">Split DNS Usage Guidelines . . . . .</a>	<a href="#">7</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">9</a>
<a href="#">7.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">9</a>
<a href="#">8.</a>	<a href="#">References . . . . .</a>	<a href="#">10</a>
<a href="#">8.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">10</a>
<a href="#">8.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">10</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">11</a>

## [1.](#) Introduction

Split DNS is a common configuration for secure tunnels, such as Virtual Private Networks in which host machines private to an organization can only be resolved using internal DNS resolvers [[RFC2775](#)]. In such configurations, it is often desirable to only resolve hosts within a set of private domains using the tunnel, while letting resolutions for public hosts be handled by a device's default DNS configuration.

The Internet Key Exchange protocol version 2 [[RFC7296](#)] negotiates configuration parameters using Configuration Payload Attribute Types. This document defines two Configuration Payload Attribute Types that add support for trusted Split DNS domains.

The INTERNAL\_DNS\_DOMAIN attribute type is used to convey one or more DNS domains that should be resolved only using the provided DNS nameserver IP addresses, causing these requests to use the IPsec connection.

The INTERNAL\_DNSSEC\_TA attribute type is used to convey DNSSEC trust anchors for those domains.



When only a subset of traffic is routed into a private network using an IPsec SA, these Configuration Payload options can be used to define which private domains should be resolved through the IPsec connection without affecting the client's global DNS resolution.

For the purposes of this document, DNS resolution servers accessible through an IPsec connection will be referred to as "internal DNS servers", and other DNS servers will be referred to as "external DNS servers".

A client using these configuration payloads will be able to request and receive Split DNS configurations using the INTERNAL\_DNS\_DOMAIN and INTERNAL\_DNSSEC\_TA configuration attributes. The client device can use the internal DNS server(s) for any DNS queries within the assigned domains. DNS queries for other domains should be sent to regular external DNS server.

### **1.1. Requirements Language**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

## **2. Background**

Split DNS is a common configuration for enterprise VPN deployments, in which only one or a few private DNS domains are accessible and resolvable via an IPsec based VPN connection.

Other tunnel-establishment protocols already support the assignment of Split DNS domains. For example, there are proprietary extensions to IKEv1 that allow a server to assign Split DNS domains to a client. However, the IKEv2 standard does not include a method to configure this option. This document defines a standard way to negotiate this option for IKEv2.

## **3. Protocol Exchange**

In order to negotiate which domains are considered internal to an IKEv2 tunnel, initiators indicate support for Split DNS in their CFG\_REQUEST payloads, and responders assign internal domains (and DNSSEC trust anchors) in their CFG\_REPLY payloads. When Split DNS has been negotiated, the existing DNS server configuration attributes will be interpreted as internal DNS servers that can resolve hostnames within the internal domains.



### **3.1. Configuration Request**

To indicate support for Split DNS, an initiator includes one more INTERNAL\_DNS\_DOMAIN attributes as defined in [Section 4](#) as part of the CFG\_REQUEST payload. If an INTERNAL\_DNS\_DOMAIN attribute is included in the CFG\_REQUEST, the initiator SHOULD also include one or more INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS attributes in the CFG\_REQUEST.

The INTERNAL\_DNS\_DOMAIN attribute sent by the initiator is usually empty but MAY contain a suggested domain name.

The absence of INTERNAL\_DNS\_DOMAIN attributes in the CFG\_REQUEST payload indicates that the initiator does not support or is unwilling to accept Split DNS configuration.

To indicate support for DNSSEC, an initiator includes one or more INTERNAL\_DNSSEC\_TA attributes as defined in [Section 4](#) as part of the CFG\_REQUEST payload. If an INTERNAL\_DNSSEC\_TA attribute is included in the CFG\_REQUEST, the initiator SHOULD also include one or more INTERNAL\_DNS\_DOMAIN attributes in the CFG\_REQUEST.

An initiator MAY convey its current DNSSEC trust anchors for the domain specified in the INTERNAL\_DNS\_DOMAIN attribute. If it does not wish to convey this information, it MUST use a length of 0.

The absence of INTERNAL\_DNSSEC\_TA attributes in the CFG\_REQUEST payload indicates that the initiator does not support or is unwilling to accept DNSSEC trust anchor configuration.

### **3.2. Configuration Reply**

Responders MAY send one or more INTERNAL\_DNS\_DOMAIN attributes in their CFG\_REPLY payload. If an INTERNAL\_DNS\_DOMAIN attribute is included in the CFG\_REPLY, the responder MUST also include one or both of the INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS attributes in the CFG\_REPLY. These DNS server configurations are necessary to define which servers should receive queries for hostnames in internal domains. If the CFG\_REQUEST included an INTERNAL\_DNS\_DOMAIN attribute, but the CFG\_REPLY does not include an INTERNAL\_DNS\_DOMAIN attribute, the initiator should behave as if Split DNS configurations are not supported by the server.

Each INTERNAL\_DNS\_DOMAIN represents a domain that the DNS servers address listed in INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS can resolve.

If the CFG\_REQUEST included INTERNAL\_DNS\_DOMAIN attributes with non-zero lengths, the content MAY be ignored or be interpreted as a suggestion by the responder.



For each DNS domain specified in an INTERNAL\_DNS\_DOMAIN attribute, one or more INTERNAL\_DNSSEC\_TA attributes MAY be included by the responder. This attribute lists the corresponding internal DNSSEC trust anchor in the DNS presentation format of a DS record as specified in [RFC4034]. The INTERNAL\_DNSSEC\_TA attribute MUST immediately follow the INTERNAL\_DNS\_DOMAIN attribute that it applies to.

### **3.3. Mapping DNS Servers to Domains**

All DNS servers provided in the CFG\_REPLY MUST support resolving hostnames within all INTERNAL\_DNS\_DOMAIN domains. In other words, the INTERNAL\_DNS\_DOMAIN attributes in a CFG\_REPLY payload form a single list of Split DNS domains that applies to the entire list of INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS attributes.

### **3.4. Example Exchanges**

#### **3.4.1. Simple Case**

In this example exchange, the initiator requests INTERNAL\_IP4\_DNS and INTERNAL\_DNS\_DOMAIN attributes in the CFG\_REQUEST, but does not specify any value for either. This indicates that it supports Split DNS, but has no preference for which DNS requests should be routed through the tunnel.

The responder replies with two DNS server addresses, and two internal domains, "example.com" and "city.other.com".

Any subsequent DNS queries from the initiator for domains such as "www.example.com" should use 198.51.100.2 or 198.51.100.4 to resolve.

```
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_DNS_DOMAIN(city.other.com)
```





### 3.4.2. Requesting Domains and DNSSEC trust anchors

In this example exchange, the initiator requests INTERNAL\_IP4\_DNS, INTERNAL\_DNS\_DOMAIN and INTERNAL\_DNSSEC\_TA attributes in the CFG\_REQUEST

Any subsequent DNS queries from the initiator for domains such as "www.example.com" or "city.other.com" would be DNSSEC validated using the DNSSEC trust anchor received in the CFG\_REPLY

In this example, the initiator has no existing DNSSEC trust anchors would the requested domain. the "example.com" dommain has DNSSEC trust anchors that are returned, while the "other.com" domain has no DNSSEC trust anchors

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

```
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(43547,8,1,B6225AB2CC613E0DCA7962BDC2342EA4F1B56083)
INTERNAL_DNSSEC_TA(31406,8,2,F78CF3344F72137235098ECBBD08947C2C90....)
INTERNAL_DNS_DOMAIN(city.other.com)
```

## 4. Payload Formats

#### 4.1. INTERNAL\_DNS\_DOMAIN Configuration Attribute Type

```

      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           |
+--+-----+-----+-----+-----+-----+-----+-----+-----+
|
~           Domain Name in DNS presentation format           ~
|
+-----+-----+-----+-----+-----+-----+-----+-----+

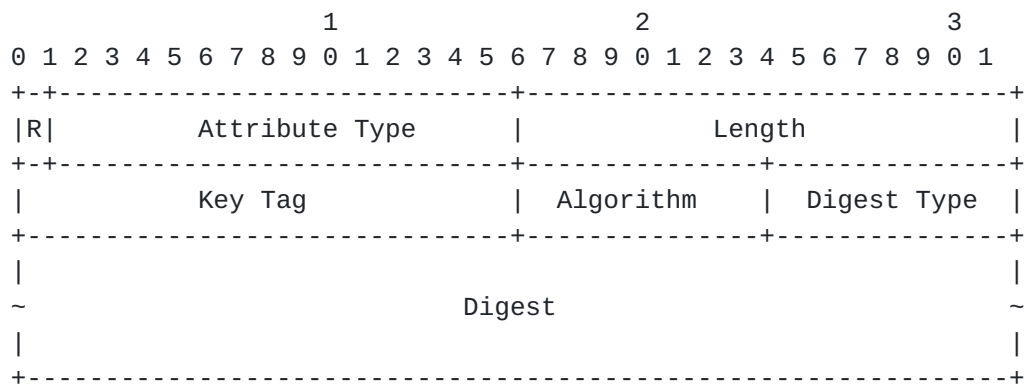
```

- o Reserved (1 bit) - Defined in IKEv2 RFC [[RFC7296](#)].
- o Attribute Type (15 bits) 25 - INTERNAL\_DNS\_DOMAIN.



- o Length (2 octets, unsigned integer) - Length of domain name.
- o Domain Name (0 or more octets) - A Fully Qualified Domain Name used for Split DNS rules, such as example.com, in DNS presentation format and optionally using IDNA [[RFC5890](#)] for Internationalized Domain Names. Implementors need to be careful that this value is not null-terminated.

#### **[4.2.](#) INTERNAL\_DNSSEC\_TA Configuration Attribute**



- o Reserved (1 bit) - Defined in IKEv2 RFC [[RFC7296](#)].
- o Attribute Type (15 bits) [TBD IANA] - INTERNAL\_DNSSEC\_TA.
- o Length (2 octets, unsigned integer) - Length of DNSSEC Trust Anchor data.
- o Key Tag value (0 or 2 octets, unsigned integer) - Key Tag as specified in [[RFC4034](#)] [Section 5.1](#)
- o Algorithm (0 or 1 octet) - DNSKEY algorithm value from the IANA DNS Security Algorithm Numbers Registry
- o DS algorithm (0 or 1 octet) - DS algorithm value from the IANA Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms Registry
- o Digest (0 or more octets) - The DNSKEY digest as specified in [[RFC4034](#)] [Section 5.1](#) in presentation format.

### **[5.](#) Split DNS Usage Guidelines**

If a CFG\_REPLY payload contains no INTERNAL\_DNS\_DOMAIN attributes, the client MAY use the provided INTERNAL\_IP4\_DNS or INTERNAL\_IP6\_DNS servers as the default DNS server(s) for all queries.



If a client is configured by local policy to only accept a limited number of INTERNAL\_DNS\_DOMAIN values, the client MUST ignore any other INTERNAL\_DNS\_DOMAIN values.

For each INTERNAL\_DNS\_DOMAIN entry in a CFG\_REPLY payload that is not prohibited by local policy, the client MUST use the provided INTERNAL\_IP4\_DNS or INTERNAL\_IP6\_DNS DNS servers as the only resolvers for the listed domains and its sub-domains and it MUST NOT attempt to resolve the provided DNS domains using its external DNS servers.

If the initiator host is configured to block DNS answers containing IP addresses from special IP address ranges such as those of [RFC1918](#), the initiator SHOULD allow the DNS domains listed in the INTERNAL\_DNS\_DOMAIN attributes to contain those Special IP addresses.

If a CFG\_REPLY contains one or more INTERNAL\_DNS\_DOMAIN attributes and its local policy does not forbid these values, the client MUST configure its DNS resolver to resolve those domains and all their subdomains using only the DNS resolver(s) listed in that CFG\_REPLY message. If those resolvers fail, those names MUST NOT be resolved using any other DNS resolvers. Other domain names SHOULD be resolved using some other external DNS resolver(s), configured independently from IKE. Queries for these other domains MAY be sent to the internal DNS resolver(s) listed in that CFG\_REPLY message, but have no guarantee of being answered. For example, if the INTERNAL\_DNS\_DOMAIN attribute specifies "example.com", then "example.com", "www.example.com" and "mail.eng.example.com" MUST be resolved using the internal DNS resolver(s), but "anotherexample.com" and "ample.com" SHOULD NOT be resolved using the internal resolver and SHOULD use the system's external DNS resolver(s).

When an IKE SA is terminated, the DNS forwarding must be unconfigured. The DNS forwarding itself MUST be deleted. All cached data of the INTERNAL\_DNS\_DOMAIN provided DNS domains MUST be flushed. This includes negative cache entries. Obtained DNSSEC trust anchors MUST be removed from the list of trust anchors. The outstanding DNS request queue MUST be cleared.

INTERNAL\_DNS\_DOMAIN and INTERNAL\_DNSSEC\_TA attributes SHOULD only be used on split tunnel configurations where only a subset of traffic is routed into a private remote network using the IPsec connection. If all traffic is routed over the IPsec connection, the existing global INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS can be used without creating specific DNS exemptions.



## 6. Security Considerations

The use of Split DNS configurations assigned by an IKEv2 responder is predicated on the trust established during IKE SA authentication. However, if IKEv2 is being negotiated with an anonymous or unknown endpoint (such as for Opportunistic Security [[RFC7435](#)]), the initiator MUST ignore Split DNS configurations assigned by the responder.

If a host connected to an authenticated IKE peer is connecting to another IKE peer that attempts to claim the same domain via the INTERNAL\_DNS\_DOMAIN attribute, the IKE connection should only process the DNS information if the two connections are part of the same logical entity. Otherwise, the client should refuse the DNS information and potentially warn the enduser.

INTERNAL\_DNSSEC\_TA payloads MUST immediately follow an INTERNAL\_DNS\_DOMAIN payload. As the INTERNAL\_DNSSEC\_TA format itself does not contain the domain name, it relies on the preceding INTERNAL\_DNS\_DOMAIN to provide the domain for which it specifies the trust anchor.

If the initiator is using DNSSEC validation for a domain in its public DNS view, and it requests and receives an INTERNAL\_DNS\_DOMAIN attribute without an INTERNAL\_DNSSEC\_TA, it will need to reconfigure its DNS resolver to allow for an insecure delegation. It SHOULD NOT accept insecure delegations for domains that are DNSSEC signed in the public DNS view, for which it has not explicitly requested such delegation by specifying the domain specifically using a INTERNAL\_DNS\_DOMAIN(domain) request.

A domain that is served via INTERNAL\_DNS\_DOMAIN should pay close attention to their use of indirect reference RRtypes such as CNAME, DNAME, MX or SRV records so that resolving works as intended when all, some or none of the IPsec connections are established.

The content of INTERNAL\_DNS\_DOMAIN and INTERNAL\_DNSSEC\_TA may be passed to another (DNS) program for processing. As with any network input, the content should be considered untrusted and handled accordingly.

## 7. IANA Considerations

This document defines two new IKEv2 Configuration Payload Attribute Types, which are allocated from the "IKEv2 Configuration Payload Attribute Types" namespace.





Value	Attribute Type	Multi-Valued	Length	Reference
-----	-----	-----	-----	-----
25	INTERNAL_DNS_DOMAIN	YES	0 or more	[this document]
[TBD]	INTERNAL_DNSSEC_TA	YES	0 or more	[this document]

Figure 1

## 8. References

### 8.1. Normative References

- [RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), DOI 10.17487/RFC1918, February 1996, <<https://www.rfc-editor.org/info/rfc1918>>.
- [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>>.
- [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", [RFC 4034](#), DOI 10.17487/RFC4034, March 2005, <<https://www.rfc-editor.org/info/rfc4034>>.
- [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>>.

### 8.2. Informative References

- [RFC2775] Carpenter, B., "Internet Transparency", [RFC 2775](#), DOI 10.17487/RFC2775, February 2000, <<https://www.rfc-editor.org/info/rfc2775>>.
- [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>>.



Authors' Addresses

Tommy Pauly  
Apple Inc.  
1 Infinite Loop  
Cupertino, California 95014  
US

Email: [tpauly@apple.com](mailto:tpauly@apple.com)

Paul Wouters  
Red Hat

Email: [pwouters@redhat.com](mailto:pwouters@redhat.com)

