

Network  
Internet-Draft  
Intended status: Standards Track  
Expires: November 28, 2016

T. Pauly  
Apple Inc.  
P. Wouters  
Red Hat  
May 27, 2016

Split-DNS Configuration for IKEv2  
draft-pauly-ipsecme-split-dns-01

## Abstract

This document defines two Configuration Payload Attribute Types for the IKEv2 protocol that define sets of private DNS domains which should be resolved by DNS servers reachable through an IPsec connection, while leaving all other DNS resolution unchanged. The options define the set of DNS domains, DNS nameserver IP addresses and DNSSEC trust anchors to use for these DNS domains. This approach of resolving a subset of domains using an IPsec connection is referred to as "split-DNS". The information obtained via these attribute types can be used to reconfigure the local DNS resolution to use DNS forwarding for specific private domains.

## 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 November 28, 2016.

## Copyright Notice

Copyright (c) 2016 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="#">3</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="#">4</a>
<a href="#">3.4.</a>	<a href="#">Example Exchanges</a>	<a href="#">4</a>
<a href="#">3.4.1.</a>	<a href="#">Simple Case</a>	<a href="#">4</a>
<a href="#">3.4.2.</a>	<a href="#">Requesting Limited Domains</a>	<a href="#">5</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="#">6</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="#">8</a>
<a href="#">7.</a>	<a href="#">IANA Considerations</a>	<a href="#">9</a>
<a href="#">8.</a>	<a href="#">References</a>	<a href="#">9</a>
<a href="#">8.1.</a>	<a href="#">Normative References</a>	<a href="#">9</a>
<a href="#">8.2.</a>	<a href="#">Informative References</a>	<a href="#">10</a>
	<a href="#">Authors' Addresses</a>	<a href="#">10</a>

## [1.](#) Introduction

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, this Configuration Payload option 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 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, while routing other DNS queries to its 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

### [3.1.](#) Configuration Request

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

If the length of the INTERNAL\_DNS\_DOMAIN attribute is zero, then the initiator is requesting that the attribute be assigned without restricting the subdomains that it will accept.

If the length of the INTERNAL\_DNS\_DOMAIN is greater than zero, the value is a single DNS domain. The initiator is indicating that it will only allow this domain and any sub-domains within this domain to be resolved using the internal DNS servers. The list of INTERNAL\_DNS\_DOMAIN attributes in the CFG\_REQUEST defines the full set of domains the initiator is willing to resolve using the internal DNS servers.

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.

### [3.2.](#) Configuration Reply

Responders MAY send one or more INTERNAL\_DNS\_DOMAIN attributes in their CFG\_REPLY payload if the CFG\_REQUEST contained at least one INTERNAL\_DNS\_DOMAIN attribute. If the CFG\_REQUEST did not contain an INTERNAL\_DNS\_DOMAIN attribute, the responder MUST NOT include an INTERNAL\_DNS\_DOMAIN attribute in the CFG\_REPLY. If an INTERNAL\_DNS\_DOMAIN attribute is included in the CFG\_REPLY, the responder SHOULD also include one or both of the INTERNAL\_IP4\_DNS and INTERNAL\_IP6\_DNS attributes in its CFG\_REPLY. 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 CFG\_REPLY MUST NOT assign any domains in its INTERNAL\_DNS\_DOMAIN attributes that are not contained within the requested domains. The initiator SHOULD ignore any domains beyond its requested list.

For each DNS domain specified in an INTERNAL\_DNS\_DOMAIN attribute, an INTERNAL\_DNSSEC\_TA attribute may be included by the responder. This

attribute lists the corresponding DSSNEC trust anchor in the presentation format of a DS record as specified in [[RFC4034](#)].

### [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 its 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 one internal domain, "example.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)
```

#### [3.4.2.](#) Requesting Limited Domains

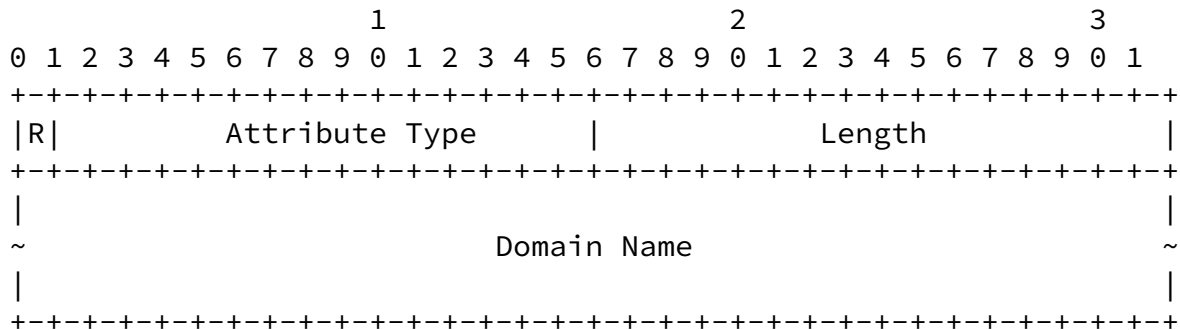
In this example exchange, the initiator requests INTERNAL\_IP4\_DNS and INTERNAL\_DNS\_DOMAIN attributes in its CFG\_REQUEST, specifically requesting only "example.com" and "other.com". The responder replies with two DNS server addresses, 198.51.100.2 and 198.51.100.4, and two domains, "example.com" and "city.other.com". Note that one of the domains in the CFG\_REPLY, "city.other.com", is a subset of the requested domain, "other.com". This indicates that hosts within "other.com" that are not within "city.other.com" should be resolved using an external DNS server. The CFG\_REPLY would not be allowed to respond with "com" or "example.net", however, since these were contained within the limited set of requested domains.

Any subsequent DNS queries from the initiator for domains such as "www.example.com" or "city.other.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(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)
```

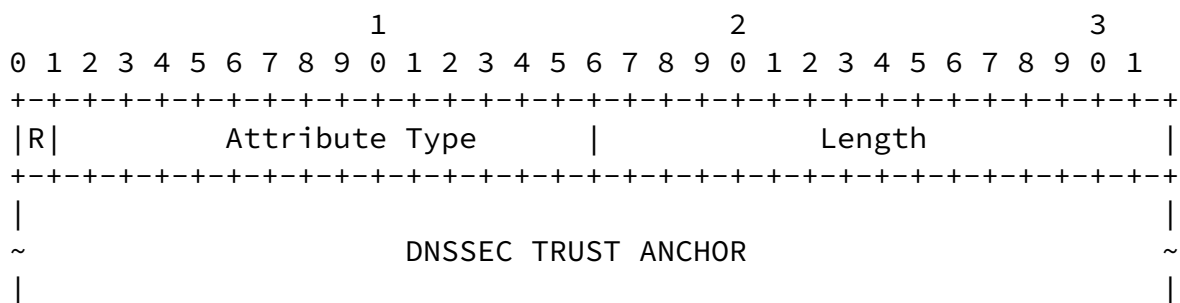
#### [4.](#) Payload Formats

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



- o Reserved (1 bit) - Defined in IKEv2 RFC [[RFC7296](#)].
- o Attribute Type (15 bits) [TBD IANA] - INTERNAL\_DNS\_DOMAIN.
- o Length (2 octets, unsigned integer) - Length of domain name.
- o Domain Name (0 or more octets) - A domain or subdomain used for split-DNS rules, such as example.com. This is a string of ASCII characters with labels separated by dots, with no trailing dot, using IDNA [[RFC5890](#)] for non-ASCII DNS domains. The value is NOT null-terminated.

#### 4.2. INTERNAL\_DNSSEC\_TA Configuration Attribute



[illegible]

## 5. Split-DNS Usage Guidelines

For each INTERNAL\_DNS\_DOMAIN entry in a CFG\_REPLY payload, the client SHOULD 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 SHOULD NOT attempt to resolve the provided DNS domains using its external DNS servers.

If a CFG\_REPLY contains one or more INTERNAL\_DNS\_DOMAIN attributes, the client SHOULD 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 SHOULD NOT be resolved using any other DNS resolvers. All other domain

Expires November 28, 2016



configured independently, and SHOULD NOT be sent to the internal DNS resolver(s) listed in that CFG\_REPLY message. 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" MUST be resolved using the system's external DNS resolver(s).

An initiator SHOULD ignore INTERNAL\_DNS\_DOMAIN attributes containing domains that are designated Special Use Domain Names in [[RFC6761](#)], such as "local", "localhost", "invalid", etc. Although it may explicitly wish to support some Special Use Domain Names.

When an IPsec connection 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 MAY be cleared.

A domain that is served via INTERNAL\_DNS\_DOMAIN MUST NOT have indirect references to DNS records that point to other split-DNS domains that are not served via INTERNAL\_DNS\_DOMAIN attributes. Indirect reference RRtypes include CNAME, DNAME, MX and SRV RR's.

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 be terminated.

If the IP address value of the received INTERNAL\_IP4\_DNS or INTERNAL\_IP6\_DNS attribute is not covered by the proposed IPsec connection, then the local DNS should not be reconfigured until a CREATE\_CHILD Exchange is received that covers these IP addresses.

INTERNAL\_DNSSEC\_TA directives MUST have an accompanying INTERNAL\_DNS\_DOMAIN directive. This prevents the insertion of rogue DNSSEC trust anchors for domains that have not been configured to use the IPsec connection.

## 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
[TBD]	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, <<http://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, <<http://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, <<http://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,

<<http://www.rfc-editor.org/info/rfc5890>>.

Pauly & Wouters

Expires November 28, 2016

[Page 9]

---

Internet-Draft

Split-DNS Configuration for IKEv2

May 2016

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

## 8.2. Informative References

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", [RFC 6761](http://www.rfc-editor.org/info/rfc6761), DOI 10.17487/RFC6761, February 2013, <<http://www.rfc-editor.org/info/rfc6761>>.

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

