IPSECME WG
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

A. Noble
S. Gundavelli
Cisco
J. Korhonen
F. Baboescu
Broadcom Corporation
B. Weis
Cisco

July 4, 2014

3GPP IMS Option for IKEv2

draft-gundavelli-ipsecme-3gpp-ims-options-02.txt

Abstract

This document defines two new configuration attributes for Internet Key Exchange Protocol version 2 (IKEv2). These attributes can be used for carrying the IPv4 and IPv6 address of the Proxy-Call Control and Service function (P-CSCF). When an IPSec gateway delivers these attributes to an IPsec client, it can obtain the IPv4 and/or IPv6 address of the P-CSCF server located in the home network.

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 January 5, 2015.

Copyright Notice

Table of Contents

1. Introduction

The Third Generation Partnership Project (3GPP) S2b reference point [TS23402], specified by the 3GPP system architecture defines a mechanism for allowing a mobile node (MN) attached in an untrusted non-3GPP IP Access Network to securely connect to the 3GPP home network and access IP services. In this scenario, the mobile node establishes an IPsec ESP tunnel [RFC4303] to the security gateway called evolved packet data gateway (ePDG) and which in turn establishes a Proxy Mobile IPv6 (PMIPv6) [RFC5213] or GPRS Tunneling Protocol (GTP) [TS23402] tunnel to the packet data gateway (PGW) [TS23402] where the mobile node's session is anchored.

The below figure shows the interworking option for non-3GPP access over an untrusted-access network. The mobile access gateway (MAG) and the local mobility anchor (LMA) functions are defined in [RFC5213]. The ePDG and PGW functions are defined in [TS23402]. IPSec ESP tunnel is between the MN and the ePDG and PMIP or GTP tunnel between the ePDG and the PGW.

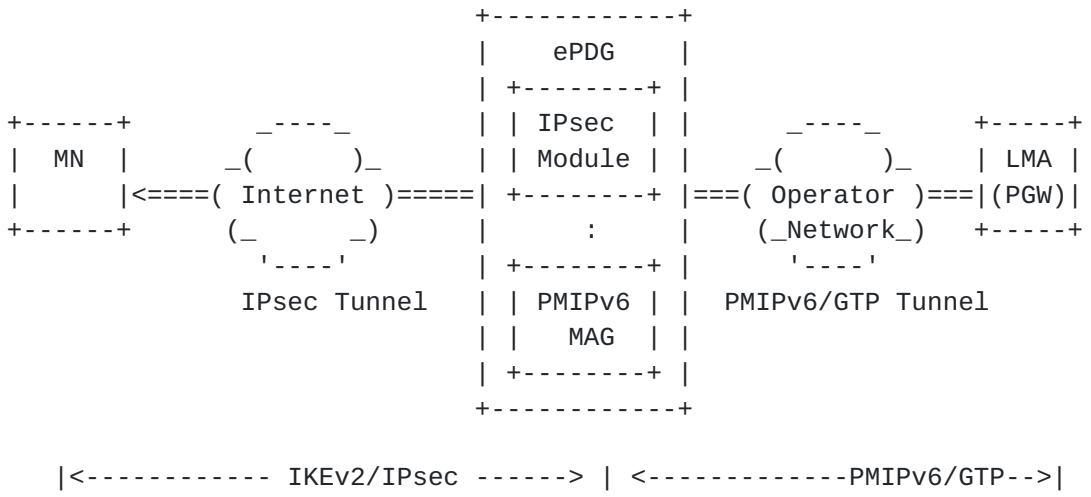

Figure 1: Exchange of IPv4 Traffic Offload Selectors

A mobile node in this scenario may potentially need to access the IP Multimedia Subsystem (IMS) services in the home network. Currently, there are no attributes in IKEv2 [RFC5996] that can be used for carrying these information elements. In the absence of these attributes the mobile node needs to be statically configured with this information and this is proving to be an operational challenge.

This specification therefore defines two new IKEv2 attributes

[RFC5996] that allows an IPsec gateway to provide the IPv4 and/or IPv6 address of the P-CSCF server. These attributes can be exchanged by IKEv2 peers as part of the configuration payload exchange. The attributes follow the configuration attribute format defined in Section 3.15.1 of [RFC5996].

2. Conventions and Terminology

2.1. Conventions

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].

2.2. Terminology

All the IKEv2 related terms used in this document are to be interpreted as defined in [RFC5996] and [RFC5739]. All the mobility related terms are to interpreted as defined in [RFC5213] and [RFC5844]. Additionally, this document uses the following terms:

Proxy-Call Session Control Function (P-CSCF)

The P-CSCF is the entry point to the 3GPP IMS (IP Multimedia Subsystem) domain and serves as the outbound proxy server for the mobile node. The mobile node attaches to the P-CSCF prior to performing IMS registrations and initiating SIP sessions.

Evolved Packet Data Gateway (ePDG)

Its is a security gateway defined by the 3GPP system architecture. The protocol interfaces it supports include IKEv2 [RFC5996].

3. P-CSCF_IP4_ADDRESS Configuration Attribute

The P-CSCF_IP4_ADDRESS configuration attribute is formatted as follows:

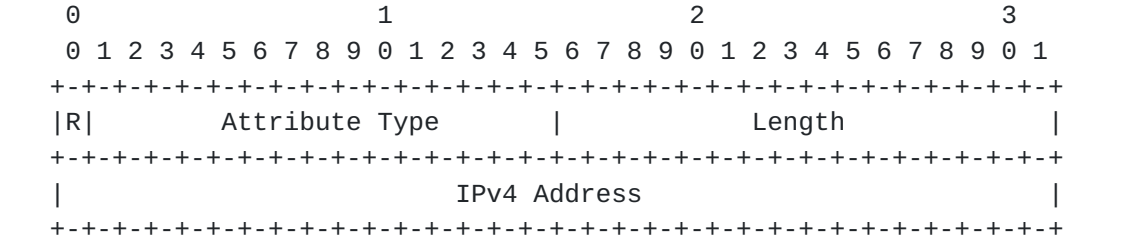

Figure 2: IPv4 Address of P-CSCF

Reserved (1 bit)
Refer to IKEv2 specification

Attribute Type (15 bits)
<IANA-1>

Length (2 octets)
Length of the IPv4 address field that follows. Possible values are (0) and (4). A value of (4) indicates the size of the 4-octet IPv4 address that follows. A value of (0) indicates that its a empty attribute with zero-length IPv4 address field, primarily used as a request indicator.

IPv4 Address (4 octets)
An IPv4 address of the P-CSCF server.

The P-CSCF_IP4_ADDRESS configuration attribute provides an IPv4 address of a P-CSCF server within the network. Multiple P-CSCF servers MAY be requested by including a single instance of an empty P-CSCF_IP4_ADDRESS attribute with zero-length IPv4 Address field. The responder MAY respond with zero or more P-CSCF_IP4_ADDRESS attributes, and there is no implied order in the response.

4. P-CSCF_IP6_ADDRESS Configuration Attribute

The P-CSCF_IP4_ADDRESS configuration attribute is formatted as follows:

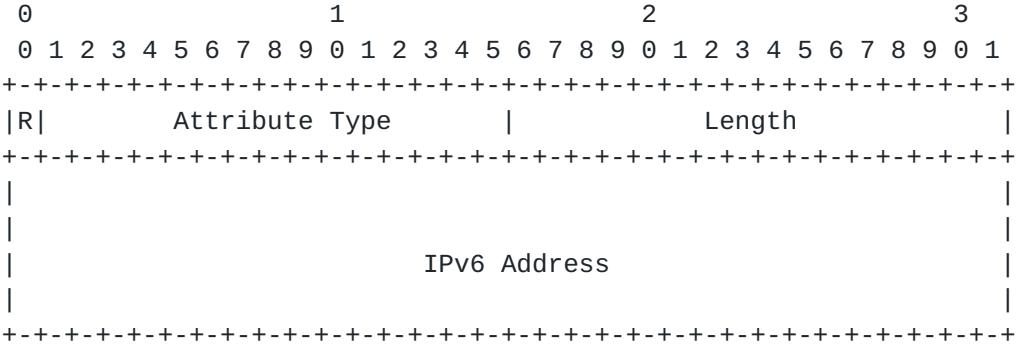

Figure 3: IPv6 Address of P-CSCF

Reserved (1 bit)
Refer to IKEv2 specification

Attribute Type (15 bits)
<IANA-1>

Length (2 octets)
Length of the IPv6 address field that follows. Possible values are (0) and (16). A value is (16) indicates the size of the 16-octet IPv6 address that follows. A value of (0) indicates that its a empty attribute with zero-length IPv6 address field, primarily used as a request indicator.

IPv6 Address (16 octets)
An IPv6 address of the P-CSCF server.

The P-CSCF_IP6_ADDRESS configuration attribute provides an IPv6 address of a P-CSCF server within the network. Multiple P-CSCF servers MAY be requested by including a single instance of an empty P-CSCF_IP6_ADDRESS attribute with zero-length IPv6 Address field. The responder MAY respond with zero or more P-CSCF_IP6_ADDRESS attributes, and there is no implied order in the response.

5. Example Scenario

The mobile node MAY request the IP address of an P-CSCF server as shown below.

```
         Client      Gateway
        --------    ---------

        HDR(IKE_SA_INIT), SAi1, KEi, Ni  -->

                 <--  HDR(IKE_SA_INIT), SAr1, KEr, Nr, [CERTREQ]

        HDR(IKE_AUTH),
        SK { IDi, CERT, [CERTREQ], AUTH, [IDr],
             CP(CFG_REQUEST) =
                { INTERNAL_IP4_ADDRESS(),
                  INTERNAL_IP4_DNS(),
                  P-CSCF_IP4_ADDRESS() }, SAi2,
             TSi = (0, 0-65535, 0.0.0.0-255.255.255.255),
             TSr = (0, 0-65535, 0.0.0.0-255.255.255.255) }  -->

               <--  HDR(IKE_AUTH),
                    SK { IDr, CERT, AUTH,
                         CP(CFG_REPLY) =
                            { INTERNAL_IP4_ADDRESS(192.0.2.234),
                              P-CSCF_IP4_ADDRESS(192.0.2.1),
                              P-CSCF_IP4_ADDRESS(192.0.2.4),
                              INTERNAL_IP4_DNS(198.51.100.33) },
                         SAr2,
                         TSi = (0, 0-65535, 192.0.2.234-192.0.2.234),
                         TSr = (0, 0-65535, 0.0.0.0-255.255.255.255) }
```

Figure 4: P-CSCF Attribute Exchange

6. IANA Considerations

This document requires the following two IANA actions.

- Action-1: This specification defines a new IKEv2 attribute for carrying the IPv4 address of P-CSCF server. This attribute is defined in Section 3. The Type value for this Attribute needs to be assigned from the IKEv2 Configuration Payload Attribute Types namespace defined in [RFC5996].

- Action-2: This specification defines a new IKEv2 attribute for carrying the IPv6 address of P-CSCF server. This attribute is defined in Section 4. The Type value for this Attribute needs to be assigned from the IKEv2 Configuration Payload Attribute Types namespace defined in [RFC5996].

7. Security Considerations

This document is an extension to IKEv2 [RFC5996] and therefore it inherits all the security properties of IKEv2.

The two new IKEv2 attributes defined in this specification are for carrying the IPv4 and IPv6 address of the P-CSCF server. These attributes can be exchanged by IKE peers as part of the configuration payload and the currently defined IKEv2 security framework provides the needed integrity and privacy protection for these attributes. Therefore this specification does not introduce any new security vulnerabilities.

8. Acknowledgements

The Authors would like to specially thank Tero Kivinen for the detailed reviews. Authors would also like to thank Vojislav Vucetic, Heather Sze, Sebastian Speicher and Maulik Vaidya for all the discussions related to this topic.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

9.2. Informative References

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5739] Eronen, P., Laganier, J., and C. Madson, "IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5739, February 2010.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2012.

Authors' Addresses

Aeneas Noble
Cisco
30 International Pl
TEWKSBURY, MASSACHUSETTS 95134
USA

Email: noblea@cisco.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Jouni Korhonen
Broadcom Corporation
Porkkalankatu 24
Helsinki FIN-00180
Finland

Email: jouni.nospam@gmail.com

Florin Baboescu
Broadcom Corporation
100 Mathilda Place
Sunnyvale, CA 94086
USA

Email: baboescu@broadcom.com>

Brian Weis
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: bew@cisco.com