Independent Submission
Request for Comments: 7651
Category: Informational
ISSN: 2070-1721

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

September 2015

3GPP IP Multimedia Subsystems (IMS) Option for the Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

This document defines two new configuration attributes for the Internet Key Exchange Protocol version 2 (IKEv2). These attributes can be used for carrying the IPv4 address and IPv6 address of the Proxy-Call Session Control Function (P-CSCF). When an IPsec gateway delivers these attributes to an IPsec client, the IPsec client can obtain the IPv4 and/or IPv6 address of the P-CSCF server located in the 3GPP network.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7651.

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 a 3GPP network and access IP services. In this scenario, the mobile node establishes an IPsec Encapsulating Security Payload (ESP) tunnel [RFC4303] to the security gateway called the Evolved Packet Data Gateway (ePDG) that in turn establishes a Proxy Mobile IPv6 (PMIPv6) [RFC5213] or GPRS Tunneling Protocol (GTP) [TS23402] tunnel to the Packet Data Network 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]. The IPsec ESP tunnel is used between the MN and the ePDG; either a PMIP or GTP tunnel is used between the ePDG and PGW.

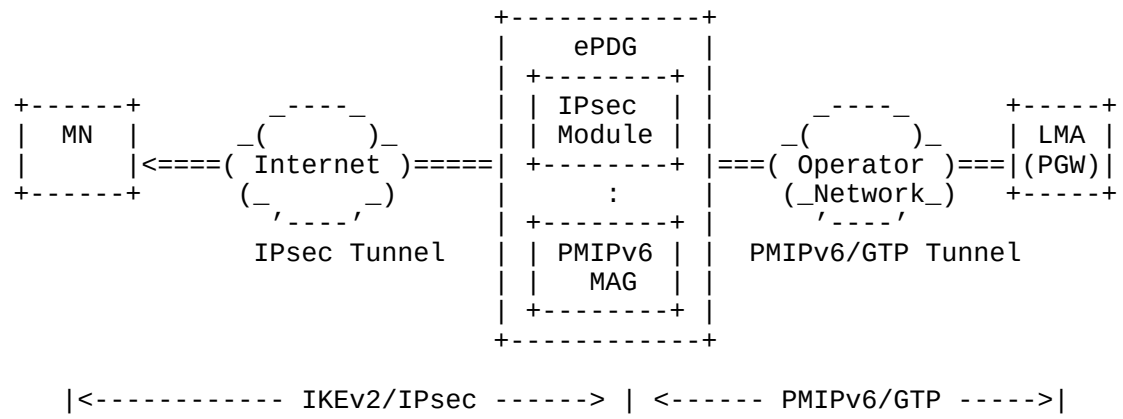

Figure 1: Exchange of IPv4 Traffic Offload Selectors

A mobile node in this scenario may potentially need to access the IP Multimedia Subsystem (IMS) services in the 3GPP network. The 3GPP IMS architecture is described in [TS23228] and [TS24229]. Currently, there are no attributes in IKEv2 [RFC7296] 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. Any other approaches for discovering these functions (such as using DNS or DHCP) would result in obtaining configuration from the access network and not from the home network. Given that the above referenced 3GPP interface is primarily for allowing the mobile node to connect to the 3GPP network through an untrusted access network, the access network may not have any relation with the home network provider and may be unable to deliver the mobile node’s home network configuration.

This specification therefore defines two new IKEv2 attributes [RFC7296] that allow 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 [RFC7296]. Furthermore, providing the P-CSCF server address(es) in IKEv2 as a standard attribute(s) enables clients to directly access IMS services behind a VPN gateway without going through the 3GPP-specific interfaces.

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 [RFC7296] and [RFC5739]. All the mobility-related terms are to be 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 and serves as the SIP outbound proxy for the mobile node. The mobile node performs SIP registration to 3GPP IMS and initiates SIP sessions via a P-CSCF.

Evolved Packet Data Gateway (ePDG)

This is a security gateway defined by the 3GPP system architecture. The protocol interfaces it supports include IKEv2 [RFC7296].

3. P_CSCF_IP4_ADDRESS Configuration Attribute

The P_CSCF_IP4_ADDRESS configuration attribute is formatted as follows:

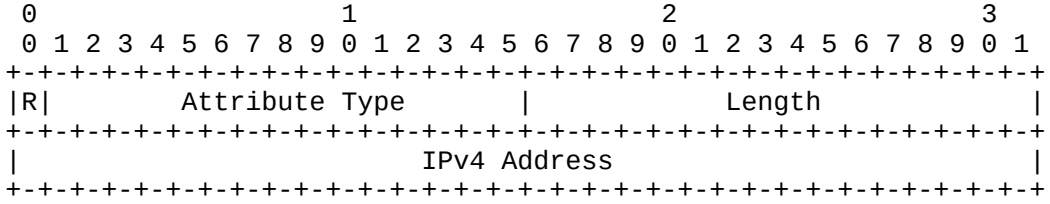

Figure 2: IPv4 Address of P-CSCF

Reserved (1 bit)
Refer to the IKEv2 specification [RFC7296]

Attribute Type (15 bits)
20

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 it's an empty attribute with a 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. If an instance of an empty P_CSCF_IP4_ADDRESS attribute with a zero-length IPv4 Address field is included by the mobile node, the responder MAY respond with zero, one, or more P_CSCF_IP4_ADDRESS attributes. If several P_CSCF_IP4_ADDRESS attributes are provided in one IKEv2 message, there is no implied order among the P_CSCF_IP4_ADDRESS attributes. However, a system architecture using this specification may be able to enforce some order at both the peers.

4. P_CSCF_IP6_ADDRESS Configuration Attribute

The P_CSCF_IP6_ADDRESS configuration attribute is formatted as follows:

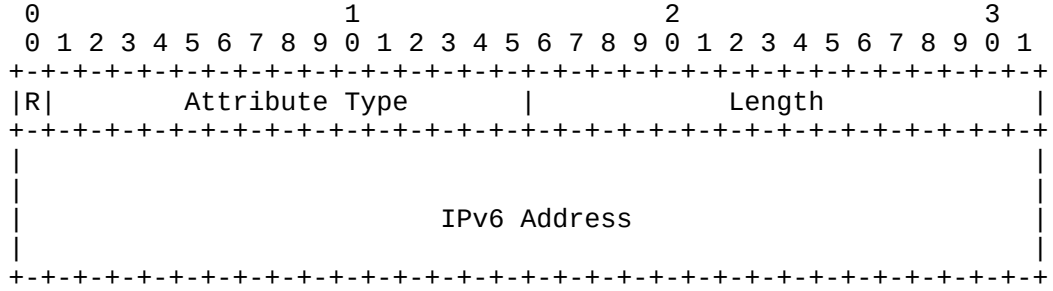

Figure 3: IPv6 Address of P-CSCF

Reserved (1 bit)
Refer to the IKEv2 specification [RFC7296]

Attribute Type (15 bits)
21

Length (2 octets)
Length of the IPv6 address field that follows. Possible values are (0) and (16). A value of (16) indicates the size of the 16-octet IPv6 address that follows. A value of (0) indicates that it's an empty attribute with a 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. If an instance of an empty P_CSCF_IP6_ADDRESS attribute with a zero-length IPv6 Address field is included by the mobile node, the responder MAY respond with zero, one, or more P_CSCF_IP6_ADDRESS attributes. If several P_CSCF_IP6_ADDRESS attributes are provided in one IKEv2 message, there is no implied order among the P_CSCF_IP6_ADDRESS attributes. However, a system architecture using this specification may be able to enforce some order at both the peers.

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

Per this document, the following IANA actions have been completed.

- Action 1: This specification defines a new IKEv2 attribute for carrying the IPv4 address of the P-CSCF server. This attribute is defined in Section 3. It has been assigned value 20 from the "IKEv2 Configuration Payload Attribute Types" namespace defined in [RFC7296].

- Action 2: This specification defines a new IKEv2 attribute for carrying the IPv6 address of the P-CSCF server. This attribute is defined in Section 4. It has been assigned value 21 from the "IKEv2 Configuration Payload Attribute Types" namespace defined in [RFC7296].

7. Security Considerations

This document is an extension to IKEv2 [RFC7296] 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. References

8.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[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, <http://www.rfc-editor.org/info/rfc7296>.

8.2. Informative References

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <http://www.rfc-editor.org/info/rfc5213>.

[RFC5739] Eronen, P., Laganier, J., and C. Madson, "IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5739, DOI 10.17487/RFC5739, February 2010, <http://www.rfc-editor.org/info/rfc5739>.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, DOI 10.17487/RFC5844, May 2010, <http://www.rfc-editor.org/info/rfc5844>.

[TS23228] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228, Version 13.3.0, June 2015.

[TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 3GPP TS 23.402, Version 13.2.0, June 2015.

[TS24229] 3GPP, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229, Version 13.2.1, June 2015.

Acknowledgements

The authors would like to specially thank Tero Kivinen for the detailed reviews. The authors would also like to thank Vojislav Vucetic, Heather Sze, Sebastian Speicher, Maulik Vaidya, Ivo Sedlacek, Pierrick Siete, and Hui Deng for all the discussions related to this topic.

Authors' Addresses

Aeneas Noble
Cisco
30 International Pl
Tewksbury, MA 95134
United States

Email: noblea@cisco.com

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

Email: sgundave@cisco.com

Jouni Korhonen
Broadcom Corporation
3151 Zanker Road
San Jose, CA 95134
United States

Email: jouni.nospam@gmail.com

Florin Baboescu
Broadcom Corporation
100 Mathilda Place
Sunnyvale, CA 94086
United States

Email: baboescu@broadcom.com

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

Email: bew@cisco.com