IPSECME
Internet-Draft
Intended status: Standards Track
Expires: August 18, 2013

D. Migault (Ed)
Francetelecom - Orange
K. Pentikousis
Huawei Technologies

February 14, 2013

IKEv2 Security Gateway Discovery
draft-mglt-ipsecme-security-gateway-discovery-00.txt

Abstract

Modern Virtual Private Network (VPN) services are typically deployed using several security gateways and are frequently accessed over a wireless network. There are several reasons for such a deployment ranging from enhancing system resilience to improving performance.

For example, in order to handle traffic efficiently and reduce the burden in the core network, the VPN service may be implemented in a distributed manner using multiple Security Gateways. A mobile VPN End User is attached to one of them using a WLAN interface and over time is likely to change its Security Gateway of attachment. In this case, in order to optimize the overall user Quality of Experience (QoE), a VPN End User should select the next most appropriate Security Gateway based on the characteristics of the available Security Gateways. This draft specifies how a VPN End User can securely collect information about Security Gateways in its network neighborhood in order to optimize its VPN experience.

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 August 18, 2013.

Copyright Notice

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Introduction

When a Virtual Private Network (VPN) client establishes a VPN connection with a distributed VPN infrastructure, care should be taken to choose the most appropriate Security Gateway. DNS may be considered as a selection mechanism to determine the first point of attachment to the distributed VPN infrastructure. However, as we explain later in this document, the information provided by DNS is limited and insufficient for this purpose. In effect, the VPN End User cannot rely on this information to optimize its point of attachment. Moreover, for the case of mobile nodes, such information cannot help in the case of multiple interface communication nor properly handle VPN mobility from one Security Gateway to another. This document addresses this problem by describing how a VPN End User can request from its Security Gateway information about other neighbor Security Gateways. Equipped with this knowledge the VPN End User can select the most appropriate Security Gateway.

The remainder of this document is organized as follows. Section 3 defines the terms and acronyms used in this document. Section 4 introduces scenarios that relate to Security Gateway selection. For each scenario, specific criteria are used by the VPN End User to select the most appropriate Security Gateway. Section 5 and Section 6 specify the Security Gateway Discovery Protocol introduced in this document, including defining the packet exchanges and the corresponding involved payloads, respectively.

3. Terminology

This section defines the terms and acronyms used in this document.

- VPN End User (EU): designates the entity that initiates a VPN connection with a Security Gateway. A VPN End User may be mobile and, as per this document, can change its VPN connection from one Security Gateway to another.

- Security Gateway: designates the network point of attachment for the VPN service. In this document, the VPN service can be provided by multiple Security Gateways. Each Security Gateway may be considered as a specific logical or physical network

entity.

- VPN service: designates the service provided to the End User. From the end-user point of view, in colloquial terms, this is what typical users consider as "establishing a VPN connection".

Throughout the document we assume that the user is not interested and, therefore, is not informed about which Security Gateway is chosen. We consider that mobility, both in terms of network point of attachment and the Security Gateway used for the VPN service, is handled inherently by the network and the user is not concerned about the actual operational details.

4. Motivation

This section motivates the technical solution advocated in this document by presenting three scenarios where the selection of the Security Gateway can significantly improve the Quality of Experience (QoE) of a VPN End User. For each scenario, we describe the information that the VPN End User needs in order to select the appropriate Security Gateway.

4.1. Multiple Interfaces

Multiple interfaces on the VPN End User or on the Security Gateway make possible path selection. If the VPN End User is able to perform path selection, it is likely to chose a Security Gateway that has multiple interfaces. Between multiple Security Gateways with multiple interfaces it may chose the one whose interfaces are attached to its preferred networks. This Security Gateway selection is particularly important since VPN End User can hardly split their VPN on two distinct Security Gateways.

Distributed VPN infrastructures are composed of multiple, independent Security Gateways. Currently, IPsec [RFC4301] does not have the mechanisms that enable "moving" a VPN connection from one Security Gateway to another Security Gateway. In practice, this means that moving the endpoint of a VPN connection from one Security Gateway to another requires a renegotiation establishment of a new VPN. This may also include new authentication for the VPN End User, likely with the need for user input in the process. On the other hand, MOBIKE [RFC4555] enables moving a VPN connection from one interface to another as long as they are attached to the same Security Gateway. Thus, we have two ways with different impact on the corresponding end user Quality of Experience (QoE), to move a VPN connection from one interface to another depending on whether these interfaces belong to the same node or not. As a result, a client implementing the MOBIKE

extension can perform interface management, and opt to be be attached to a Security Gateway with multiple interfaces.

Note that with IPsec [RFC4301], the signaling channel is defined by the IKE_SA while the user data is designated by the IPsec_SA. Unless specifically designed otherwise, these two channels are highly dependent on each other and MUST be hosted on the same host. More specifically, it is not possible for a VPN End User to have its IKE channel with one host and its IPsec_SA with a different, independent host.

Note also that MOBIKE enables a Security Gateway to inform a VPN End User about its available interfaces. However, these interfaces belongs to the Security Gateway the VPN End User is attached to, not another Security Gateway.

This document defines how a VPN End User can query a Security Gateway in a distributed VPN infrastructure whether other, neighboring Security Gateway have one or multiple interfaces. In this document we are concerned about the other Security Gateways so that the VPN End User can decide which Security Gateway it should be attached to next.

4.2. Closest Next Neighbor

With a large distributed VPN infrastructure like those serving xDSL broadband networks, a mobile VPN End User needs to define which Security Gateway it will be attached to next. The current Security Gateway can assist a VPN End User to avoid spending effort on Security Gateway discovery by providing this localization information. This is beneficial both in terms of network bandwidth and system resources.

Localization may be based on geo-localization data. Nevertheless, in many cases, the optimal Security Gateway for each particular VPN End User may not be the one that is closer in geographical terms, but the one with the best inter-Security Gateway bandwidth. In fact, in recent distributed mobility architectures, DSL boxes in a typical urban environment exchange information using their WLAN interface to avoid congesting the core network.

We argue that if Security Gateways can exchange information they can improve VPN client mobility and reduce traffic overhead. Such information may include, for instance, VPN client authentication credentials, IPsec counters, or packet redirection. Using this information-exchange protocol, the VPN End User has, for example, the advantage of moving to the DSL box with the best inter-Security-Gateway bandwidth.

4.3. Intra-Security Gateway Services

Although currently IPsec does not enable a VPN client to move from one Security Gateway to another one, proprietary protocols that enable such mobility from one Security Gateway to another do exist. This may, for example, involve exchange of IPsec counters. This information may help the VPN End User to properly chose the next Security Gateway it will be attached to. Standardizing the way this information is exchanged can benefit end users and network operators alike.

4.4. Why We Cannot Rely On DNS Only

DNS binds a FQDN to one or multiple IP addresses. In that sense, one may consider that DNS could be leveraged upon to provide information sufficient to determine the neighboring Security Gateways. Unfortunately, this is not the case because FQDN is an abstraction, and in our case, the FQDN most probably designates the name of the VPN service as a whole. Thus, DNS is used to bind the VPN service with specific interfaces, without specifying which Security Gateway they belong to. Since this information is not available, the VPN End User cannot select a specific Security Gateway, as two issues arise as we explain next.

First, DNS can provide a list of multiple interfaces available for a given service (i.e. FQDN), which enables a client to choose the most appropriate interface at the moment in time that it initiates a VPN service. Once connected to one of the Security Gateways, MOBIKE makes possible to convey to the VPN End User the available interfaces on the Security Gateway that the client is attached to. In principle, the VPN End User could then use the list of interfaces provided by DNS, correlate it with that received via MOBIKE and come to some conclusion with respect to Security Gateway availability. Besides the fact that this method is inexact science at best, it does not add much value in large deployments. Since each Security Gateway may have multiple interfaces, it has no clue if the remaining interfaces belong to a single Security Gateway or to multiple Security Gateways. This information cannot be provided by DNS. This motivates us to provide this information at the service layer, that is to say, for the VPN service, via IKEv2.

Second, DNS usually does not provide the complete list of all Security Gateway interfaces, but often just a subset of those available by the VPN service. For largely distributed applications, DNS provides a subset of available interfaces that are "close" to the resolving server. The problem with this is that DNS can hardly provide the "closest" server to the VPN End User. Firstly, defining the closest interface of the DNS query emitter remains difficult.

Secondly, it is impossible to consider the various interfaces of the VPN End User. Thirdly, the DNS query is usually sent by a resolving server, not by the VPN End User. Because of this indeterminacy, DNS may be more concerned about avoiding the worst answer, rather than looking for the best option. Thus, it may look for answers with a large diversity instead of focusing their answers to a given location. Among the proposed interfaces, the VPN End User may chose the most convenient interface according to its policy or its interfaces.

Note that [I-D.vandergaast-edns-client-ip] makes possible to avoid considering the resolving server location instead of the VPN client.

5. Security Gateway Discovery Protocol

In this document we assume that the VPN End User is already attached to a Security Gateway. The goal of this exchange is that the VPN End User can obtain information about other Security Gateways which are designated as neighbors.

The proposed Security Gateway Discovery Protocol (SGDP) employs a query / response exchange mechanism. Usually, the exchange is initiated by the VPN End User and the responder is the Security Gateway that the VPN End User is connected to. However, the protocol does not exclude that either of the peers initiates the exchange.

5.1. Sending a NEIGHBOR_INFORMATION Query

The initiator builds the NEIGHBOR_INFORMATION Notify Payload (described in Section 6.1) by setting the Question bit to 1 and providing the necessary Options. Notify Payloads have a Critical bit set.

The Option request Option (described in Section 6.2)makes possible to list the queried information about each neighboring Security Gateway. In this document, the Options that can be queried are:

- Interface Option: lists the interfaces associated to the neighboring Security Gateway.

- Geo-localization Option: provides geographic coordinates of the neighboring Security Gateway.

- Intra-Security Gateway Bandwidth Option: indicates how much bandwidth the current Security Gateway shares with the neighboring Security Gateway.

- Intra-Security Gateway Mobility Support Option: indicates if the current Security Gateway and the neighboring Security Gateway share a specific mobility protocol to ease moving the VPN connection from the current Security Gateway to the neighboring Security Gateway.

The Maximum Neighbor Option is intended to limit the size of the response and indicates how many neighboring Security Gateway SHOULD be considered. Finally, the Padding Payload format pads the overall Notify Payload to a length that is a multiple of 32 bits. Other Options may be added for future use.

5.2. Receiving NEIGHBOR_INFORMATION

A received NEIGHBOR_INFORMATION Notify Payload may be originating from a query by the initiator as described in Section 5.1. This case is detailed in Section 5.2.1, below. Alternatively, the incoming message may be a response to a query previously sent by the VPN connection peer, which is detailed in Section 5.2.2. The protocol also supports informative messages as detailed in Section 5.2.3. Finally, the received NEIGHBOR_INFORMATION Notify Payload may be an unwanted message.

Once a NEIGHBOR_INFORMATION Notify Payload is received, the responder checks whether the Critical bit is set to 1. If the Critical Bit is set and the Notify Payload is not supported by the responder then, following [RFC5996] section 2.5, setting the Critical bit to one forces the Responder to send back a UNSUPPORTED_CRITICAL_PAYLOAD Notify Payload if it does not understand the received Notify Payload.

If the Critical bit is set, and the receiver supports the NEIGHBOR_INFORMATION Notify Payload, the receiver checks the Question Bit. A set Question Bit means that the Notify Payload is a query as described in Section 5.1, and a response MUST formed and sent back to the initiator. This is described in Section 5.2.1. If the Question Bit is not set, then the Notify Payload corresponds to a response. If no corresponding query has been sent previously an INVALID_SYNTAX MUST be sent back and the rest of the Notify Payload MUST be ignored. Conversely, if a query has been sent, the receiver will process the response as per Section 5.2.2.

If the Critical bit is not set and the Notify Payload is not supported by the receiver, the Notify Payload MUST be ignored. However, this case is expected to only occur for informative NEIGHBOR_INFORMATION Notify Payload as described in Section 5.2.3.

If the Critical Bit is not set and the receiver supports the NEIGHBOR_INFORMATION Notify Payload, then the receiver examines the

Question Bit. If it is set, the message MUST be ignored. This is to avoid ambiguity in cases where the initiator does not know if it receives no response because there is no information or because the Notify Payload is not supported by the responder. If the Question Bit is not set, the Notify Payload corresponds to an informative NEIGHBOR_INFORMATION Notify Payload. This case is detailed in Section 5.2.3.

5.2.1. NEIGHBOR_INFORMATION Query Processing

For this section we assume that the Critical Bit and the Question Bit are set, the Notify Payload is properly formed and the receiver understands the NEIGHBOR_INFORMATION Notify Payload.

The responder checks if a Maximum Neighbor Option is in the query. If not present, the responder is allowed to provide as much Neighbor Payload information as deemed best. If the option is present, then the responder SHOULD check its internal policy and determine how many Neighbor Payload can be provided in the response. If the limit set by the internal policy is lower that what is requested by the initiator in the Maximum Neighbor Option, the responder MUST indicate it by providing a Maximum Neighbor Option that corresponds to the actual number of Neighbor Payloads.

The responder checks if a Option request Option is in the query. If not, the responder MAY use its default policy about the default Options to be returned. It MAY also return a void response. In any other case, the responder lists the queried Options. For each Neighbor, if the responder has the queried information, it MUST indicate it in the Neighbor Payload.

The Padding Option is used to properly format the response, and the response is sent to the initiator.

5.2.2. NEIGHBOR_INFORMATION Response Processing

This section assumes that the Critical Bit is set and the Question Bit is not set, the Notify Payload is properly formed and the receiver understands the NEIGHBOR_INFORMATION Notify Payload.

If a Maximum Neighbor Option is present, this means that only a subset of the available information has been sent. If no Maximum Neighbor Option has been sent in the query, the number received indicates an internal policy of the responder. On the other hand, if a Maximum Neighbor Option has been sent in the query, a number equal to the one specified in the query is expected. Other values indicate an internal policy of the responder.

5.2.3. Informative NEIGHBOR_INFORMATION

The VPN connection peer may provide informative NEIGHBOR_INFORMATION without being queried. This is the case when the Critical Bit and the Question Bit are not set, the Notify Payload is properly formed and the receiver understands the NEIGHBOR_INFORMATION Notify Payload.

6. Notify Payload Format

This section introduces the Notify Payload for the Security Gateway Discovery Protocol.

6.1. NEIGHBOR_INFORMATION Notify Payload

Fig. 1 illustrates the NEIGHBOR_INFORMATION Notify Payload packet format.

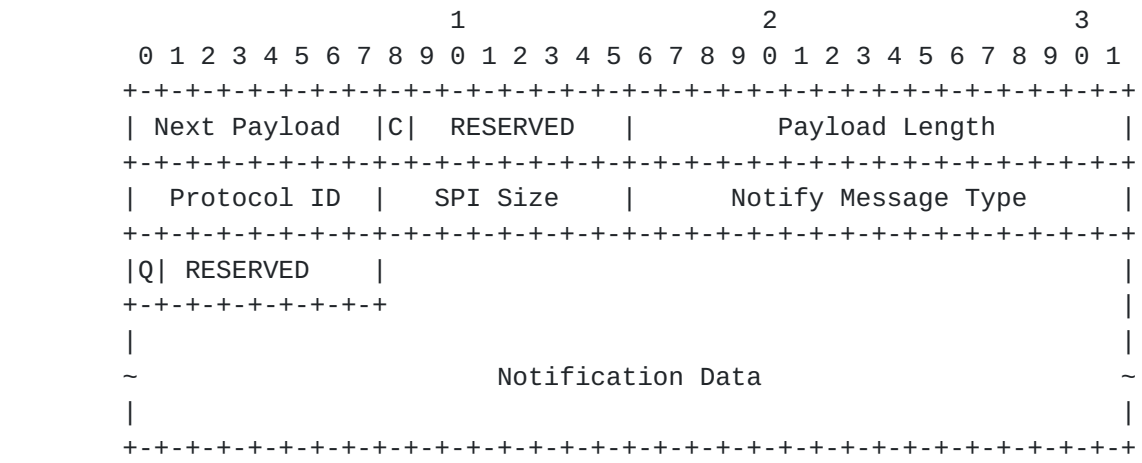

Figure 1: NEIGHBOR_INFORMATION Notify Payload

- Next Payload (1 octet): Indicates the type of payload that follows after the header.

- Critical Bit (1 bit): Indicates how the responder handles the Notify Payload. In this document the Critical Bit is not set only when an informative NEIGHBOR_INFORMATION is sent. Otherwise, the Critical bit is set to 1.

- RESERVED (7 bits): MUST be sen as zero; MUST be ignored on receipt.

- Payload Length (2 octet): Length in octets of the current payload, including the generic payload header.

- Protocol ID (1 octet): set to zero.

- SPI Size (1 octet): set to zero.

- Notify Message Type (2 octets): Specifies the type of notification message NEIGHBOR_INFORMATION_QUERY

- Question Bit (1 bit): set to one by the initiator and set to zero by the responder.

- RESERVED (7 bits): set to zero.

- Notification Data (variable length): When the Notify Payload is sent by the initiator, the Notification data is composed of Parameters.

6.2. Initiator Options: O-REQUEST

This section provides the parameters that comprise the Notification Data of the initiator.

The Option Request Payload defines the Options requested for each neighbor. In other words, it is expected in the response that each Neighbor Payload (NEIGHBOR) Section 6.3.1 is filled with these Options.

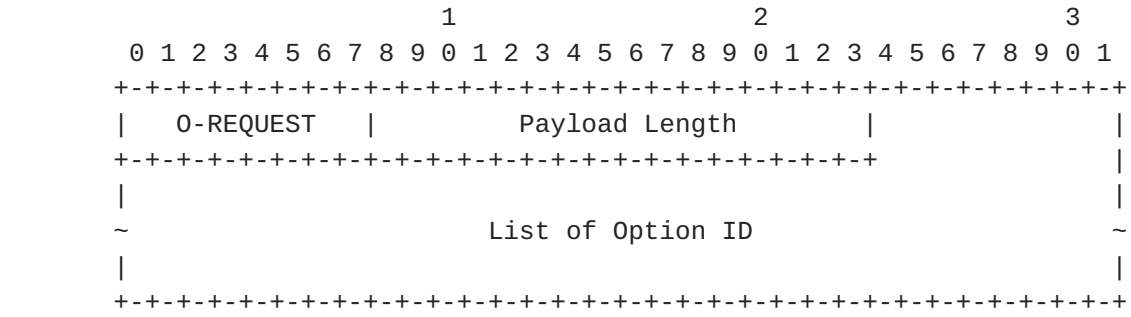

Figure 2: Option Request Option: O-REQUEST

- Option-ID (1 octet): O-REQUEST

- Payload Length (2 octet): Payload Length expressed in octet and includes the Option-ID and Payload Length fields' length. The Payload may not be a multiple of 32 bytes.

- List of Option ID (variable length): List of the Option that are expected for each NEIGHBOR Payload.

6.3. Responder Options

6.3.1. Neighbor: NEIGHBOR

The Neighbor Payload contains information about a neighbor Security Gateway. The number of Neighbor Payloads is defined by the Maximum Neighbors Payload, or if not specified by the responder. If the number of Neighbor Payloads is defined by the responder, the responder MUST add the Maximum Neighbors Payload.

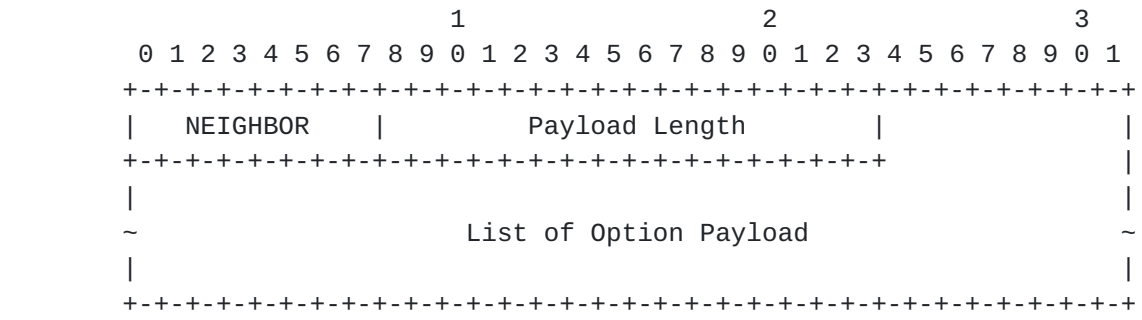

Figure 3: Neighbor: NEIGHBOR

- Option-ID (1 octet): NEIGHBOR

- Payload Length (2 octet): Payload Length expressed in octets, including the Option-ID and Payload Length fields' length. The Payload may not be a multiple of 32 bytes.

- List of Option Payload (variable length): List of the Option Payload requested by the initiator.

6.3.2. Interface Option: O_INTERFACE

The Interface Option provides the IP addresses of the Neighbor.

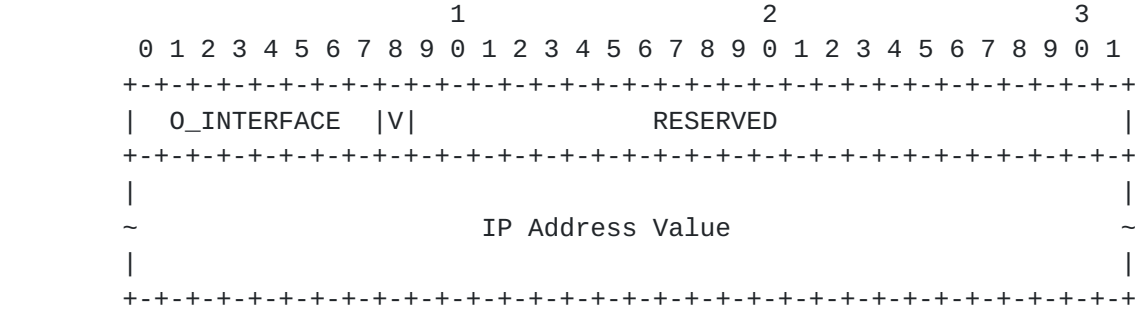

Figure 4: Interface Option: O_INTERFACE

- Option-ID (1 octet): O_INTERFACE

- Version Bit (1 bit): The Version Bit indicates if the IP address is an IPv4 or an IPv6 IP address. The Version Bit is set to 1 for an IPv4 address.

- RESERVED (23 bits): Set to Zero.

- IP Address Value (4 or 16 octets): The IP address value. An IPv4 address is 4 octet long and an IPv6 address is 16 octets long.

6.3.3. Geo-localization Option: O_GEOLOC

The Geo-localization Option provides Geographic coordinates of the Neighbor.

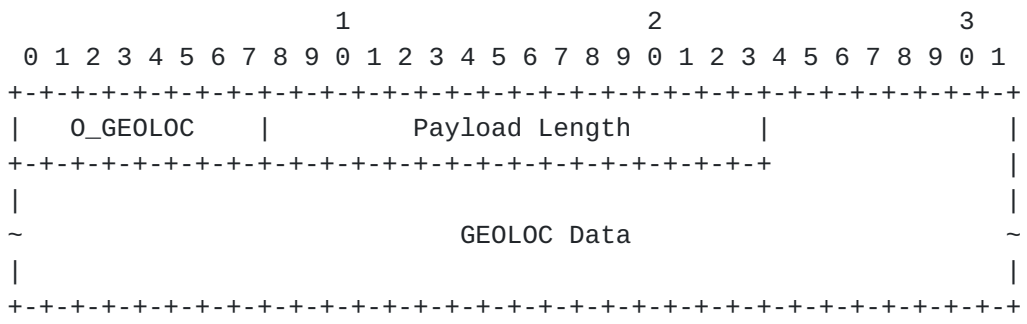

Figure 5: Geo-localization Option: O_GEOLOC

- Option-ID (1 octet): O_GEOLOC

- Payload Length (2 octet): Payload Length expressed in octets including the Option-ID and Payload Length fields' length. The Payload may not be a multiple of 32 bytes.

- GEOLOC Data (variable length): GEOLOC Data as defined in [RFC1876].

6.3.4. Intra-Security Gateway Bandwidth Option: O_ISG-BW

The Intra-Security Gateway Bandwidth Option characterizes the link between the responder and the Neighbor.

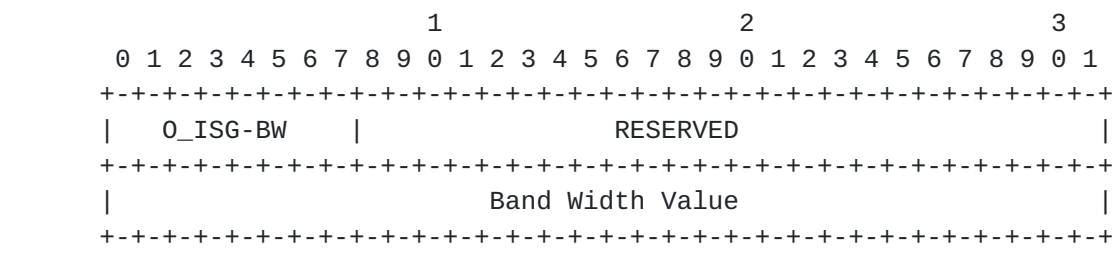

Figure 6: Intra-Security Gateway Bandwidth Option: O_ISG-BW

- Option-ID (1 octet): O_ISG-BW

- RESERVED (3 octets): Set to Zero.

- Band Width Value (4 octets): Specifies the bandwidth in octets per second.

6.3.5. Intra-Security Gateway Mobility Support Option: O_ISG-MOB

The Intra-Security Gateway Mobility Option defines if there are any mechanisms that support VPN mobility from the responder to the Neighbor.

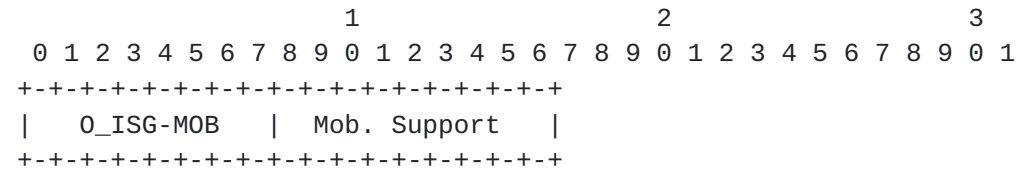

Figure 7: Intra-Security Gateway Mobility Support Option: O_ISG-MOB

- Option-ID (1 octet): O_ISG-MOB

- Mobility Support (1 octet): Specifies how VPN mobility is supported from the responder to the Neighbor.

Currently the following values are provided for Mobility Support:

- UNSUPPORTED_MOBILITY: 0

- IPSEC_CONTEXT_TRANSFERED: 1

6.4. General Options

This section describes two options that can be used by both the initiator and the responder.

6.4.1. Padding Payload: PADDING

The Padding Payload is used to make the NEIGHBOR_INFORMATION Notify Payload length a multiple of 32 bits.

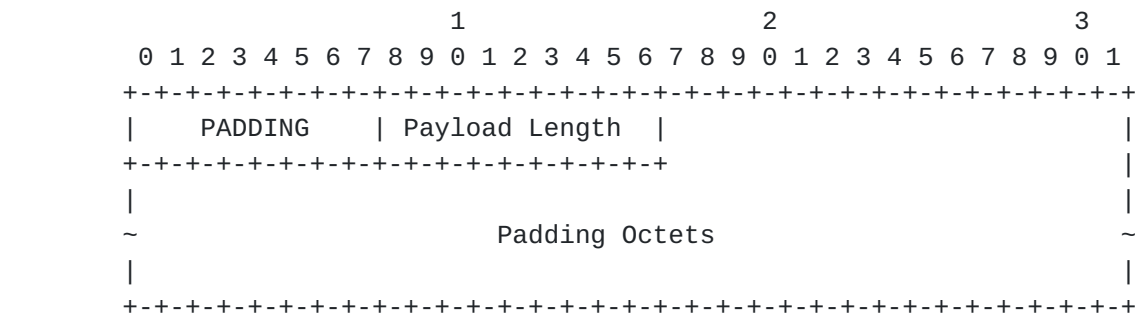

Figure 8: Padding Payload: PADDING

- Option-ID (1 octet): PADDING

- Payload Length (1 octet): Payload Length expressed in octet and includes the Option-ID and Payload Length fields' length. In case one need 2 octet padding, the Payload Length is set to 2. If there is only a need for a 1 octet padding, then 4 additional padding octets must be added and the Payload Length is set to 5.

- Padding Octets (variable length): These Octets are for padding and MUST NOT be interpreted.

6.4.2. Maximum Neighbors Payload: MAX-NEIGHBOR

The Maximum Neighbors Payload sets the maximum number of Neighbor the VPN End User wants information about. This Option is of fixed size.

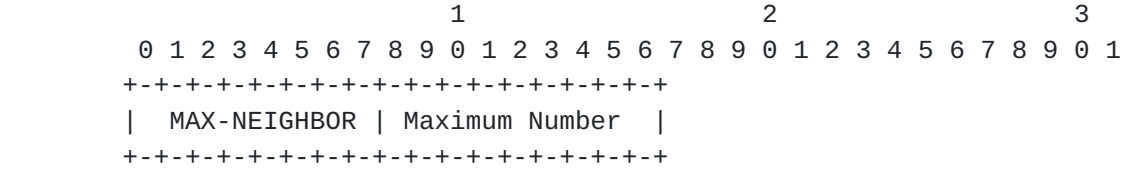

Figure 9: Maximum Neighbors Payload: MAX-NEIGHBOR

- Option-ID (1 octet): MAX-NEIGHBOR

- Maximum Number (1 octet): Specifies the maximum number of NEIGHBOR Payload the response carries.

7. IANA Considerations

The new fields and number are the following:

IKEv2 Notify Message Types - Status Types

NEIGHBOR_INFORMATION

Security Gateway Discovery Attributes

O-REQUEST
PADDING
MAX-NEIGHBOR
NEIGHBOR

Neighbor Options

O_INTERFACE
O_GEOLOC
O_ISG-BW
O_ISG-MOB

O_ISG-MOB Attributes

UNSUPPORTED_MOBILITY
IPSEC_CONTEXT_TRANSFERED

8. Security Considerations

The exchange described in this document is protected by the IKEv2 channel. Then, the only concern may be the information that a Security Gateway provides to the VPN End User. We do not see how the provided information can be used against the Security Gateway. Furthermore, the VPN End User has already been authenticated by IKEv2 prior to being able to obtain such information.

9. Acknowledgments

TBD

10. References

10.1. Normative References

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

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

10.2. Informative References

[I-D.vandergaast-edns-client-ip] Contavalli, C., Gaast, W., Leach, S., and D. Rodden, "Client IP information in DNS requests", draft-vandergaast-edns-client-ip-01 (work in progress), May 2010.

[RFC1876] Davis, C., Vixie, P., Goodwin, T., and I. Dickinson, "A Means for Expressing Location Information in the Domain Name System", RFC 1876, January 1996.

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

-00: First version published.

Authors' Addresses

Daniel Migault
Francetelecom - Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com

Kostas Pentikousis
Huawei Technologies
Carnotstrasse 4
10587 Berlin
Germany

Email: k.pentikousis@huawei.com