

MIF Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2013

D. Migault
Francetelecom - Orange
C. Williams
MCSR Labs
November 3, 2012

IPsec Multiple Interfaces Problem Statement
draft-mglt-mif-security-requirements-03.txt

Abstract

IKEv2 is the protocol used to set up and negotiate Security Associations between nodes. IKEv2 has not been designed for nodes with multiple interfaces.

This document is focused on IKEv2 ability to set up IPsec protected communications between nodes with multiple interfaces. This document states the problems and provides requirements for IKEv2 to ease IPsec for multiple interface communication.

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 May 7, 2013.

Copyright Notice

Copyright (c) 2012 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

Internet-Draft

IPsec MIF Problem Statement

November 2012

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

1.	Requirements notation	4
2.	Introduction	4
3.	Use Case 1: VPN with Multiple Interfaces	5
3.1.	Initial MIF IPsec Configuration	6
3.1.1.	Description	6
3.1.2.	Problem Statement	6
3.1.3.	Requirements	8
3.2.	Mobility	8
3.2.1.	Description	8
3.2.2.	Problem Statement	9
3.2.3.	Requirements	11
3.3.	Multihoming	12
3.3.1.	Description	12
3.3.2.	Problem Statement	13
3.3.3.	Requirements	13
3.4.	Adding an Interface	14
3.4.1.	Description	14
3.4.2.	Problem Statement	17
3.4.3.	Requirements	18
3.5.	Deleting an Interface	18
3.5.1.	Description	18
3.5.2.	Problem Statement	18
3.5.3.	Requirements	18
4.	Use Case 2: MIF applications and IPsec Tunnel mode	19
5.	Use Case 3: MIF aware applications with Transport mode	20
5.1.	Initial MIF IPsec Configuration	21
5.1.1.	Description	21
5.1.2.	Problem Statement	21
5.1.3.	Requirements	21
5.2.	Mobility	22
5.2.1.	Description	22
5.2.2.	Problem Statement	23
5.2.3.	Requirements	24
5.3.	Multihoming	24
5.3.1.	Description	24

5.3.2.	Problem Statement	24
5.3.3.	Requirements	25
5.4.	Adding an Interface	25
5.5.	Delete an Interface	25
6.	Security Considerations	25

7.	IANA Considerations	25
8.	Acknowledgment	25
9.	References	26
9.1.	Normative References	26
9.2.	Informational References	26
	Authors' Addresses	26

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

IPsec protocol suite [[RFC4301](#)], [[RFC5996](#)] is mainly used to:

- Extend a trusted domain over an untrusted network: This typically corresponds to the Virtual Private Network (VPN) use case. A Security Gateway is a trusted entry point to a trusted network. The end user is connected to an untrusted network and tunnels its traffic to the Security Gateway in a encrypted tunnel using the IPsec tunnel mode. The Security Gateway decapsulates the traffic and forwards it on the trusted network. Once the traffic is in the trusted network it is usually not encrypted anymore. In other words, the traffic is protected from the end user terminal to the Security Gateway, that it to say over the untrusted network.
- Provide end-to-end security: With end-to-end security, the traffic is protected from the source - or the end user in our case - to the destination. The traffic does not require to be tunneled, and any segments of the network between the end user and the destination is considered as untrusted. With end-to-end security, one does not require encapsulation, and the IPsec transport mode can be used.

Currently most devices have multiple interfaces. Mobile phones have most of the time a Wireless LAN (WLAN) and a Radio Access Network (RAN) interface. Laptop can easily have Ethernet / WLAN / RAN with WiMAX interfaces. Furthermore, USB dongle can be plugged to provide additional RAN and WLAN interfaces. Regular PCs, Servers, or CPEs have multiple Ethernet interfaces, with additional WLAN interfaces.

Protocols like SCTP [[RFC4960](#)] or MOBIKE [[RFC4555](#)] have been designed to use these multiple interfaces for multihoming. Only a single interface is used at a time. The interface used to carry the IP datagrams is called the Primary interface and other interfaces are called Secondary or Alternate interfaces. Alternate interfaces are only expected to be used in case the Primary interface fails.

However, multihoming does not enable the simultaneous use of multiple interfaces which can provide a better use of the available bandwidth. MPTCP [[RFC6182](#)] has been designed for that purpose, and SCTP [[RFC4960](#)] can also be used for it. Raiciu and al. [[Raiciu](#)] showed how using multiple paths improve the performances and robustness of

data centers compared to TCP. Furthermore, a communication may be connected simultaneously to different networks with different technologies and takes advantage of their different characteristics. This is typically the case of Offload when ISPs are offloading their RAN communications to a WLAN network. Motivations for offloading is that RAN cannot support all mobile traffic [[Cisco](#)]. As a result, with a RAN and a WLAN interface, Mobile phones and ISPs may balance the communications between an unreliable WLAN with economical bandwidth and always connected RAN with expensive bandwidth.

The document focuses on how applications and services protected with IPsec can also take advantage of multiple interfaces. The traditional VPN application with multiple interfaces is the first use case we consider. However, with the offload usage, ISPs are offloading unprotected communications, services from a trusted network - like the RAN - to an untrusted and unreliable network - like the WLAN. This means that the ISP must protect the communications related to these services and applications while being offloaded. IPsec appears to be one way to secure communications transparently to the application.

They are two ways to secure the communications with IPsec. One way

is to tunnel the communication to a Security Gateway. The other is to provide end to end security. The document will consider both ways.

[Section 3](#) considers the specific case of VPN with multiple interfaces. [Section 4](#) extends the previous use case by considering the general case of IPsec protected communications using the Tunnel mode. Finally [Section 5](#) considers the case of IPsec protected communications with the Transport mode. For each case, the document details different scenarios that take advantage of multiple interfaces. Then it positions IKEv2 toward each of these scenarios and points out requirements

3. Use Case 1: VPN with Multiple Interfaces

This section describes the VPN scenario with connectivity described in figure 1, the End User (EU) has multiple interfaces and figure 1 represents 3 interfaces bound to 3 IP addresses EU @IP_outer(i), (i in {1, 2, 3}).

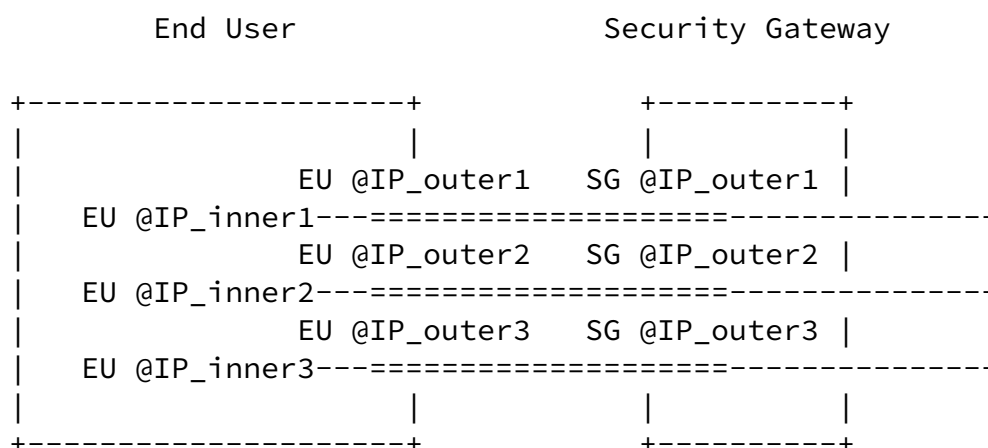


Figure 1: VPN with Multiple Interfaces

[3.1.](#) Initial MIF IPsec Configuration

[3.1.1.](#) Description

This section details how the End User with its three interfaces set (EU @IP_outer(i), i in {1, 2, 3}) can set an IPsec configuration as represented in figure 1. We consider the IPsec configuration is set using IKEv2, and that the End User uses only a single IKEv2 channel. In other words, each interface MUST NOT be considered independently from each other with its own IKEv2 channel and own Security Associations.

One of these End User IP addresses is used to set the IKEv2 channel. This IP address is used to set the IKE_SA as well as for all IKEv2 exchanges. Suppose EU @IP_outer1 is used for the IKE_SA.

Using the IKEv2 channel, the End User requests the inner IP addresses EU @IP_inner(i), i in {1, 2, 3}. If the Security Gateway has multiple interfaces, it advertises the End User, what are the available interfaces.

Once the End User has inner and outer IP addresses, it starts negotiating via the IKEv2 channel the different Security Associations. For each Security Association, the End User and the Security Gateway SHOULD be able to agree on the Traffic Selectors (i.e. the inner IP addresses) as well as the outer IP addresses used for the Tunnel.

[3.1.2.](#) Problem Statement

This section positions the current IKEv2 specifications toward the scenario described in [Section 3.1.1](#)

To request multiple inner IP addresses, the End User can use the IKEv2 with multiple INTERNAL_IP*_ADDRESS Configuration Attributes in the CFG Payload ([Section 3.15 \[RFC5996\]](#)).

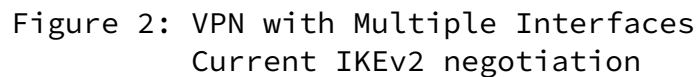
Currently IKEv2 does not provide ways for the Security Gateway to announce the End User the available outer IP addresses - SG @IP_outer1, SG @IP_outer2 and SG @IP_outer3. [\[I-D.arora-ipsecme-ikev2-alt-tunnel-addresses\]](#) details how this could

be mitigated. Note that in the VPN use case, the initiator – that is to say the End User – is more likely to request the Security Gateway outer IP addresses, then the reverse. In other words, there seems very few interest for the responder to know the different outer IP addresses of the End User. However, as detailed in [Section 5](#) the more general case SHOULD consider that both initiator and responder can advertise the available interface when the IKEv2 negotiation is initiated.

IKEv2 makes possible the negotiation of the Security Associations associated to each of the EU @IP_inner(i) IP addresses using a Traffic Selector Payload with one or multiple Traffic Selectors ([section 3.13 \[RFC5996\]](#)). IKEv2 even enables the simultaneous negotiation of Security Associations. However, currently the Security Association negotiation does not specify the outer IP addresses. The outer IP addresses are those used for the IKEv2 channel. In other words, current IKEv2 only considers a single working IP address for both the End User and the Security Gateway. Figure 2 illustrates current IKEv2 capabilities in the VPN use case with different Traffic Selectors associated to a single outer IP address. While negotiating a Security Association, IKEv2 SHOULD be able to specify the source and destination IP addresses.

Note that the benefits of specifying the outer IP addresses provides the End User or Initiator the ability to use simultaneously multiple interfaces. In the specific case of figure 1, the Security Gateway will most likely have a single IP outer IP address. We considered multiple IP addresses on the Security Gateway for the more general case.

Currently, IKEv2 does not provide the ability to negotiate the outer IP addresses of the Tunnel. By default, the outer IP addresses of the Child Security Associations are those used for the IKEv2 channel. This results in the configuration as represented in figure 2. The configuration of figure 1 does not result from an IKEv2 negotiation.



case where, for example, the End User decides to use EU @IP_outer4 instead of EU @IP_outer3 on the same hardware network interface. Other mobility use cases may also consider the EU @IP_outer4 may be associated to a different network hardware, including the one associated to EU @IP_outer(i), i in $\{1, 2\}$. Then, EU @IP_outer4 is different from EU @IP_outer3 but may be one of the EU @IP_outer(i), i in $\{1, 2\}$.

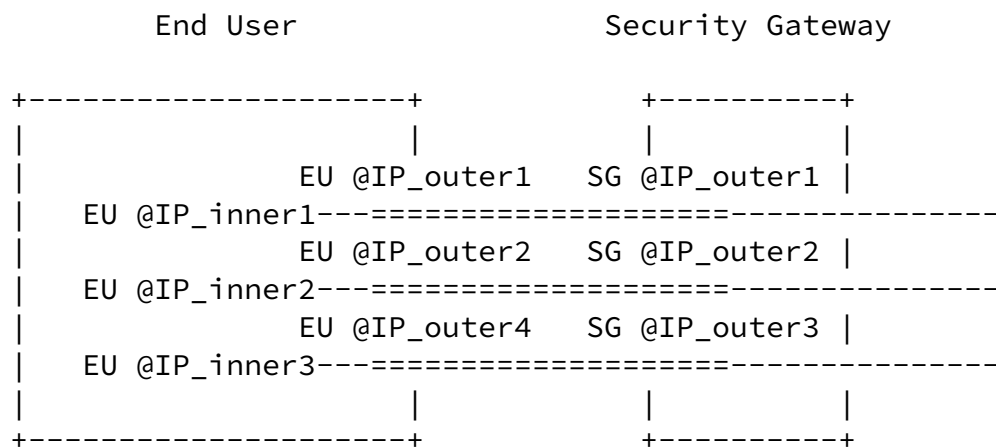


Figure 3: VPN Mobility

3.2.2. Problem Statement

Currently IKEv2 proposes different alternative to update a Security Association, and modify the outer IP address of the Tunnel. However none of them really address the description provided in [Section 3.2.1](#)

3.2.2.1. MOBIKE

MOBIKE [[RFC4555](#)] provides an UPDATE_SA_ADDRESSES exchange that updates the outer IP address of the tunnel. As explained in this section MOBIKE cannot be used in the general case described in figure 3 because the updated IP address is necessarily the one associated to the IKEv2 channel. This limitation is due to the fact that MOBIKE has been designed for a single interface.

MOBIKE does not explicitly specify in its message the IP address that has to be updated and the new value for this IP address. The IP address to be updated is the one used by the IKEv2 channel, and the new IP address to consider is the IP address used in the IP header of the UPDATE_SA_ADDRESSES message.

If EU @IP_outer1 is equal to EU @IP_outer3, then sending an UPDATE_SA_ADDRESSES would update the outer tunnel IP address of the

Security Associations using the IP address of the IKEv2 channel, that is at least EU @IP_outer1 and EU @IP_outer3, with EU @IP_outer4.

This case is only a specific case and is not applicable when the outer IP address to update is different from the IP address used for the IKEv2 channel.

If EU @IP_outer3 is different from EU @IP_outer1, then, the only way to use MOBIKE is to move the IKEv2 channel to EU @IP_outer3, that is updating EU @IP_outer1 by EU @IP_outer3, and then updating EU @IP_outer3 by EU @IP_outer4. This is not convenient because all traffic on EU @IP_outer1 has been transferred to EU @IP_outer3, and then to EU @IP_outer4. Furthermore, it is only possible for managed mobility, because we need EU @IP_outer3 to be a valid interface until IKEv2 uses EU @IP_outer3. In other words, if EU @IP_outer3 fails suddenly, moving the IKEv2 channel to EU @IP_outer3 is not possible anymore.

As a result MOBIKE cannot be used to handle the mobility described in [Section 3.2.1](#).

[3.2.2.2](#). CREATE_CHILD_SA

A second alternative is to renegotiates a new Security Association between the End User and the Security Gateway. IKEv2 provides the CREATE_CHILD_SA Exchange ([Section 1.3 \[RFC5996\]](#)) to create a new Security Association. Similarly [Section 3.1.2](#) this exchange does not specify the outer IP address of the Tunnel. By default, the outer IP address of the Tunnel is the IP address used for the IKEv2 channel. This does not address the use case described in [Section 3.2.1](#).

If requirements of [Section 3.1.3](#) were fulfilled, that is to say even if the CREATE_CHILD_SA would enable to negotiate the outer IP addresses of the Tunnel, then, using the CREATE_CHILD_SA exchange would be an alternative. However, this alternative would still suffer from several drawbacks:

- Not Mandatory: The CREATE_CHILD_SA is not a mandatory IKEv2 feature, especially for light implementations. For these implementation, an non reachable interface would require re-negotiating both the IKE_SA and the new Security Association. Furthermore, there is currently no way to advertise whether the implementation supports or not this exchange.

- Resource Consuming Exchange: The CREATE_CHILD exchange creates a Security Association from scratch and requires all parameters of the Security Association to be specified. This results in a quite complex exchange, which does not take advantage of the already negotiated parameters, like nonces, Keys, Traffic Selectors, Nonces, SPIs. Instead it requires all these parameters to be renegotiated, generation of nonces, keys, as well as multiple interactions with IPsec databases which requires more resources than updating a single parameter within

a Security Association.

- Two-Successive Exchange: The CREATE_CHILD exchange creates a new Security Association, however, the previously used Security Association has not been removed from the IPsec databases. As a result, once the new Security Association has been created, a new exchange SHOULD be performed to delete the previous Security Association with the Delete Payload ([Section 3.11 \[RFC5996\]](#)). The Delete Payload specifies the Security Associations to Delete.
- Per Security Association Exchange: The CREATE_CHILD_SA exchange creates a specific Security Association, which means that there are as many CREATE_CHILD_SA exchanges as Security Association to update. In our case, multiple Security Associations may be bound to a single interface, so the Security Association granularity is not convenient for interface management. Updating an interface implies that all Security Association bound to this interface MUST be updated. In the use case illustrated by figure 3, the End User a single Security Association per interface, so interface and Security Association management have similar granularity. On the other end, for the Security Gateway with a single interface, i.e. (all SG @IP_outer(i), i in{1, 2, 3} are the same), interface and Security Association do not have the same granularity. Note that with a single interface the Security Gateway would be able to use MOBIKE, but not with two interface (i.e. is SG @IP_outer2 and SG @IP_outer3 would be the same).

[3.2.2.3](#). One IKE channel per Interface

A fourth alternative consists renegotiating an complete independent IKEv2 channel and a new Security Association. This is out of the scope of this document. This may result as having a IKEv2 channel

per interface. Furthermore, independent IKEv2 channels may not simplify IPsec configuration and may result in multiple Security Associations matching a given Traffic Selector, which may cause trouble at least for outbound traffic. Furthermore, in this case, the End User and the Security Gateway must proceed to an authentication.

3.2.3. Requirements

In order to make the End User set its IPsec configuration as represented in figure 3, IKEv2 SHOULD make possible:

- 1. To update the outer IP address of the tunnel with a IP address that differs from those used for the IKEv2 channel. The Update is not a per security Association negotiation but SHOULD replace all Security Association associated to the old IP address. For all these Security Associations, the old IP

address is replaced by the new IP address. This consists in extending MOBIKE UPDATE_SA_ADDRESSES exchange.

3.3. Multihoming

3.3.1. Description

This section considers how a node can take advantage of multiple interfaces with multihoming. In case one of these interface fails, then another interface can be used instead. Moving the traffic from one interface to the other is called mobility. This section deals with multihoming, that is the two peers agree that in case an interface fails, a mobility should be triggered on the agreed interface.

Suppose, as represented in figure 4, EU @IP_outer3 is not reachable anymore. Applications that are multiple interfaces aware, and also bound to the others EU @IP_inner(i) (i in {1, 2}) IP addresses may handle EU @IP_outer3 non reachability. On the other hand non multiple interfaces aware applications (like regular TCP connections) bound to EU @IP_outer3 are stalled and cannot use the other interfaces.

One way to recover the EU @IP_inner3 unreachability is to reconfigure the Security Association and replace EU @IP_outer3 by EU @IP_outer(i)

($i \in \{1, 2\}$). Figure 5 shows that EU @IP_outer3 is replaced by EU @IP_outer2. EU @IP_outer2 has been provided as an Alternate IP address of EU @IP_outer3. This means that when one or the other peer notice EU @IP_outer3 is down, it can trigger a mobility with the appropriated outer IP address. More specifically, the Security Gateway can overcome the failure of EU @IP_outer3, if it detects the failure before the End User. The End User and the Security Gateway can also agree on an ordered list of Alternate IP addresses.

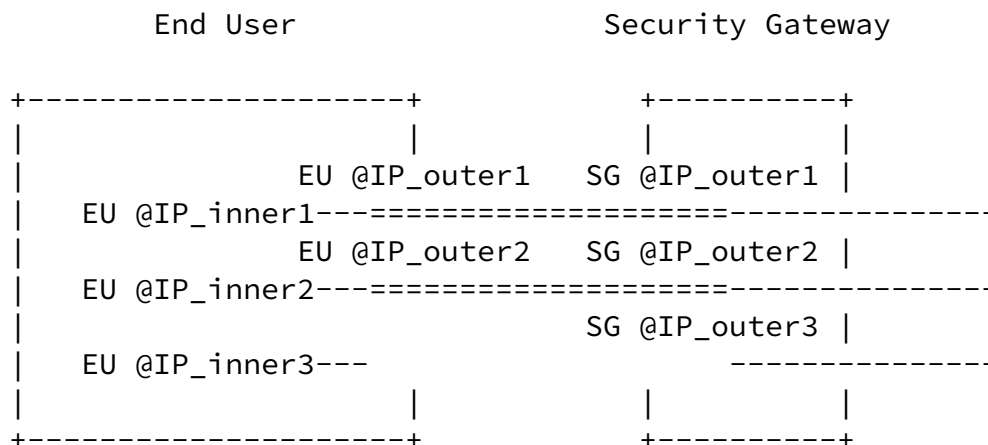


Figure 4: VPN with Mobility/Multihoming between

Multiple Interfaces: EU @IP_outer3 unreachable

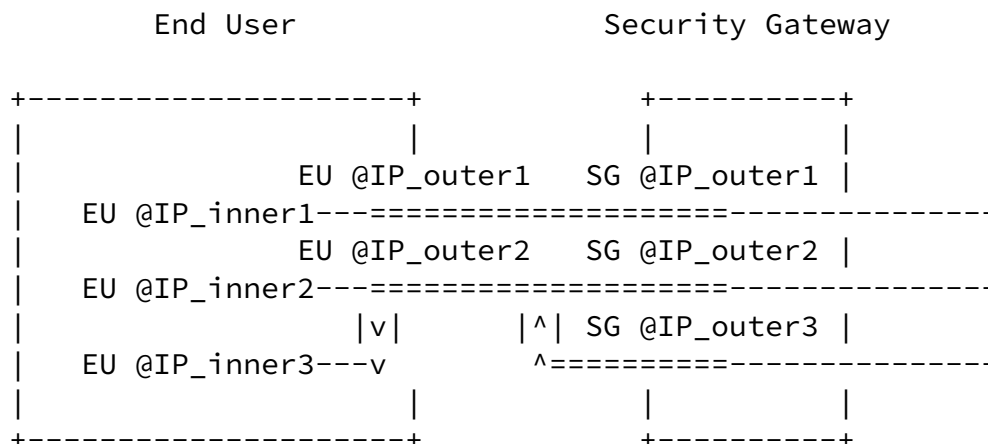


Figure 5: VPN with Mobility/Multihoming between
Multiple Interfaces: EU @IP_outer2

replaces EU @IP_outer3

[3.3.2.](#) Problem Statement

Currently Multihoming is handled by MOBIKE with the ADDITIONAL_IP*_ADDRESS Notify Payloads. As with mobility, these payloads are only provided for the interface used by the IKEv2 channel. The main reason is that MOBIKE has been designed for a single interface. In our case, MOBIKE would only make possible to provide Alternate IP addresses to EU @IP_outer1.

What happens to packets when the Security Gateway performs Multihoming and the End User has not updated its Security Association? Both End User and Security Gateway Security Associations are configured to use the EU @IP_outer3 IP address. When the Security Gateway notices EU @IP_outer3 is not reachable it updates its Security Association, triggers a mobility exchange and may start sending packets to EU @IP_outer2 before the End User has proceeded to the update of its Security Associations. The End User receives this packet and performs a Security Association match. Outer IP addresses will not perform a match, and the match occurs with the Security Policy Index (SPI). The packet is checked against the Security Policy Databases Selectors. These selectors are based on the inner IP addresses and have not been modified. As a result, packets will not be discarded.

[3.3.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 3, IKEv2 SHOULD make possible:

- 1. To provide Alternate IP addresses for IP addresses that are different from the one used by the IKEv2 channel. This extends the Multihoming features of MOBIKE to multiple interfaces.
- 2. Reduce the complexity of Multihoming. Although a node MUST be able to provide Alternate IP address for a given IP address, it should also be able to provide all its interfaces, and if multihoming is supported on both side, a multihoming rule should be derived by default from this list.

[3.4.](#) Adding an Interface

3.4.1. Description

Nodes with multiple interfaces may have some interfaces supporting the VPN whereas other interfaces have not been assigned an IP address. When this interface has been assigned an IP address, the current VPN communication may take advantage of this newly available interface. This section is concerned on how a given communication can take advantage of a newly available interface and set its IPsec settings in an optimal way.

Figure 6 represents the End User with multiple interfaces connected to the Security Gateway. We only represented a single interface for the Security Gateway but more interfaces may be also considered. In figure 7, the Security Gateway has an additional interface that becomes active, it advertises the End User this interface is available. The End User may perform some latency and Round Trip Time measurements and decide to use it. In the figure 7, the End User moves the traffic associated to its interface EU @IP_outer3 to the newly available interface SG @IP_outer2 of the Security Gateway. Moving the traffic is performed through a mobility operation as described in [Section 3.2](#).

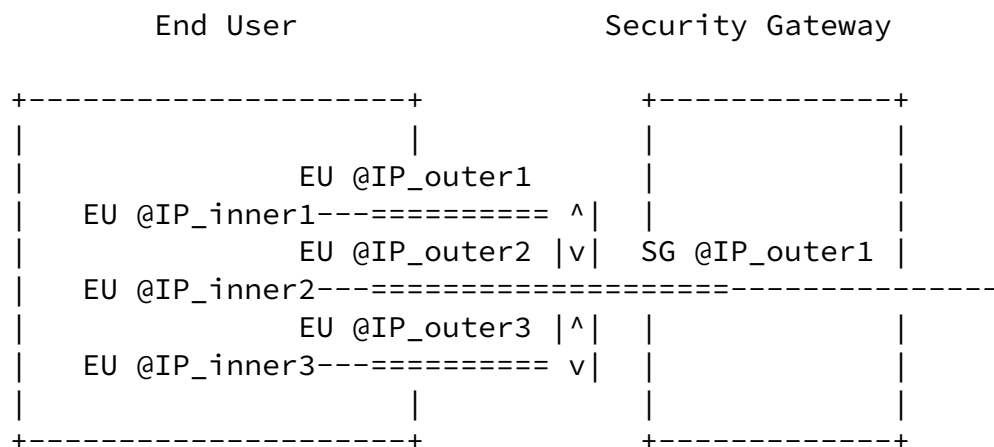
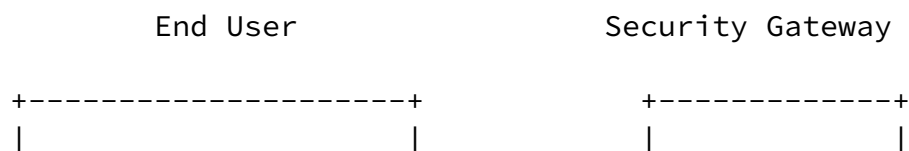
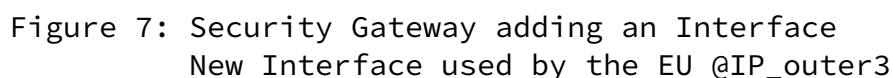


Figure 6: Security Gateway with a single Interface





```

      End User                                     Security Gateway
+-----+-----+                               +-----+-----+
|                                     |               |               | | |
|                                     |               |               |
|          EU @IP_outer1            |               |               |
| EU @IP_inner1-----^            |               |               |
|          EU @IP_outer2 |v|        | SG @IP_outer1 |               |
| EU @IP_inner2-----+-----+-----+-----+-----+-----+-----+
|                                     |               |               |
| EU @IP_inner3---                  |               |               |
|                                     |               |               |
+-----+-----+                               +-----+-----+

```

[Page 15]

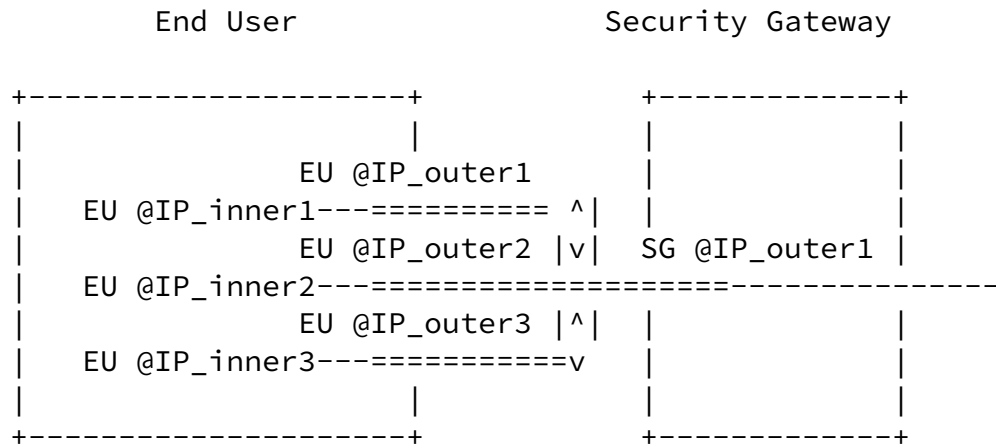


Figure 8: End User with a newly active interface EU @IP_outer3. All traffic associated to EU @IP_outer1 and EU @IP_outer2 is able to use EU @IP_outer3

In our case, the End User already had a specific inner IP address associated to the newly available interface EU @IP_outer3. This makes possible the End User to generate the new IPsec Security Associations and new Security Policies associated to EU @IP_outer3. When the Security Gateway receives the request to add the newly available interface, it may set the newly Security Policies and Security Associations. However, the End User may not have an inner IP address EU @IP_inner3, and may combine the request to the Security Gateway to add the new interface, with a request for a EU @IP_inner3 address. In that case, the Security Gateway first sets the IPsec databases, and the End User sets the IPsec databases when it receives the inner IP address.

When an interface is added, unless otherwise specified, the End User wants that all services, except IKEv2 using the available outer IP addresses (EU @IP_outer1 and @IP_outer2 addresses) may also be configured to use the newly available IP address EU @IP_outer3. By adding an interface the End User is not using a finer granularity than the interface granularity. In other words, it does not want to specify how Security Associations are derived. They should be derived in an automatic way. In return, deriving Security Associations and Security Policies is expect to optimize their creation as opposed to using CREATE_CHILD_SA.

In the example of figure 7 and 8, the End User is likely to create Security Associations derived from those established with the interfaces EU @IP_outer1 and EU @IP_outer2. All services using EU @IP_outer1 or EU @IP_outer2 will be able to use EU @IP_outer3 with the inner IP address EU @IP_inner3.

Internet-Draft

IPsec MIF Problem Statement

November 2012

The idea is to copy the Security Association associated with EU @IP_outer1 replace EU @IP_outer1 by EU @IP_outer3 and EU @IP_inner1 by EU @IP_inner3. SPIs MUST also be changed since there are unique for the Security Association. Then we perform the same with EU @IP_outer2.

Note that it is important to specify an ordered list of EU @IP_outer address from which the new SAs are derived, so to guarantee that these new Security Associations are derived the same way on both peers. Then the new Security Association MUST be created only if there are no already existing matching SPD selectors.

In the most basic case of VPN, we only have one Security Association per interface. All services using EU @IP_inner(i) are tunneled to EU @IP_outer(i) $i \in \{1,2\}$. Adding EU @IP_outer3 only requires to derive Security Association from one interface EU @IP_outer1 and EU @IP_outer2. Then, the End User needs to specify the inner and outer IP addresses EU @IP_inner3, EU @IP_outer3 and in the specific case represented on figure 7 the outer IP address of the Security Gateway SG @IP_outer3. The resulting exchange may look something like the exchange represented in figure 10. The mandatory parameters are the IP address used for the traffic selectors, and the outer IP address for the Tunnel on the End User. The destination outer IP address of the Tunnel is optional and, if not specified may be the one used by the IKEv2 channel. The list of interfaces from which are derived the Security Associations and the Security Policies may also be optional. A default value for this list may be the ordered list of associated outer IP addresses of the End User. The nonce may be used to create SPIs.

	End User	Security Gateway
request	Add Interface (EU @IP_inner3, ---> EU @IP_outer3, [outer-destination] [interface-list] [nonce])	
normal case		<--- N()
error case		<--- N(error)

Figure 10: Principle of the Adding Interface exchange

[3.4.2.](#) Problem Statement

Currently IPsec does not provide any means for a peer to advertise a new interface is available. MOBIKE makes possible to advertise a Alternate IP address is available. However Alternate IP addresses

are only intended to be use in case the Primary Interface is down. In our case, the interface is ready for use. This issue is similar to the one detailed in [Section 3.1.2](#). However, here the announcement corresponds to a dynamic changes, and the list of available IP address does not occurs during the IKE_INIT exchange, but in a regular information exchange.

Currently the only way IKEv2 provides to create new Security Associations is the CREATE_CHILD_SA exchange. Disadvantages of this exchange have been described in [Section 3.2.2](#). The key advantage of adding an interface is to provide an optimized interface management exchange instead of a Security Association management exchange.

[3.4.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 1, IKEv2 SHOULD make possible:

- 1. Make possible the Responder and Initiator to announce its interfaces outside the IKE_INIT exchange. This requirements is similar to the one of [Section 3.1.3](#)
- 1. Make possible the Responder and Initiator to automatically derive Security Associations and Security Policies from the existing interface.

[3.5.](#) Deleting an Interface

[3.5.1.](#) Description

Nodes with multiple interfaces in dynamic environment may have interfaces that are not reachable anymore. This may trigger mobility or multihoming actions. However, the node may also want to delete the Security Associations bound to this interface either as a Tunnel outer IP address or as a Traffic Selector.

[3.5.2.](#) Problem Statement

Currently IKEv2 does not make possible to delete an interface from multiple Security Associations. IKEv2 provides a Delete Payload ([Section 3.11 \[RFC5996\]](#)) that deletes one or multiple specific Security Associations, identified by their SPI.

[3.5.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 3, IKEv2 SHOULD make possible:

- 1. Delete an interface, that is to say all Security Associations associated to that interface.

[4.](#) Use Case 2: MIF applications and IPsec Tunnel mode

This section considers applications that can deal with multiple interfaces. This ability can be done with transport layer protocols like MPTCP or SCTP or with applications using one or multiple UDP / TCP connections over the various interfaces, and that manages how to send the data.

The difference between multiple interfaces aware applications and the VPN use case is that the tunnels are established per services, whereas the VPN tunnel all traffic is tunneled to a unique Security Gateway. This may increase the number of Security Associations between the End User and the Security Gateway. This section details motivation for using the IPsec Tunnel mode with multiple interfaces aware applications and position it to the VPN use case of [Section 3](#).

Applications may use the tunnel mode for end-to-end security and to benefit from the Mobility features provided by the Tunnel mode. More specifically, using the Tunnel mode provides Mobility without breaking the connectivity, if upper layer is not mobility aware.

Other motivations for using the Security Gateway is that the End User

chose not to tunnel all its traffic to the Security Gateway, but only the traffic that worth being protected. For example, an End User may chose not to tunnel its "youtube" traffic, as well as some of its "https" traffic (as well as it application layer protected traffic). On the other hand, it may want to tunnel all non-protected "http" (as well as other non protected communications).

If each service proposes different Security Gateways, the use case is very similar to the VPN use case, for each service. The main difference is that Security Association are established with different Traffic Selectors.

If multiple services are using the same Security Gateway, this will result for each interface, in multiple Security Associations established with the same Security Gateway - one per service. This case is very similar to the VPN use case but with multiple Security Associations. If "s" is the number of Services connected on the Security Gateway the number of Security Associations is at least "s" (5services are considered independent). If some applications are using multiple flows, then this number may be even larger. In that case, adding an interface results in at least negotiating "s" new Security Associations. Using the CREATE_CHILD_SA exchange may

require "s" exchanges whereas using the Adding interface exchange requires only one exchange. This use case is represented in figure 11.

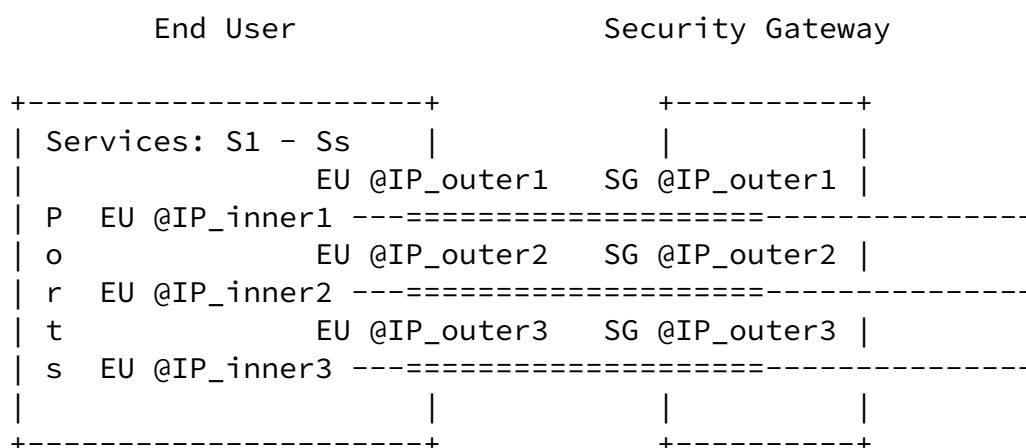


Figure 11: MIF aware applications

Requirements of this use case have already been mentioned in the VPN use case.

5. Use Case 3: MIF aware applications with Transport mode

This Use Case is very similar to the Use Case 2 except that the Transport mode is used instead of the Tunnel mode. The Use Case is illustrated with figure 12.

Unlike in the VPN use case in [Section 3](#) or for multiple interfaces aware applications described in [Section 4](#) using IPsec tunnel mode, the IPsec Transport mode does not involves inner IP addresses.

With Transport mode, we may consider two types of applications. The applications that can handle multiple interfaces. This can be done with transport protocols like MPTCP or SCTP or with a connection manager at the application layer. These applications may have Security Associations on all interfaces. Other Applications with a single using TCP/UDP and without specific connection managers may only deal with a single interface and may only have an Security Association associated to this interface.

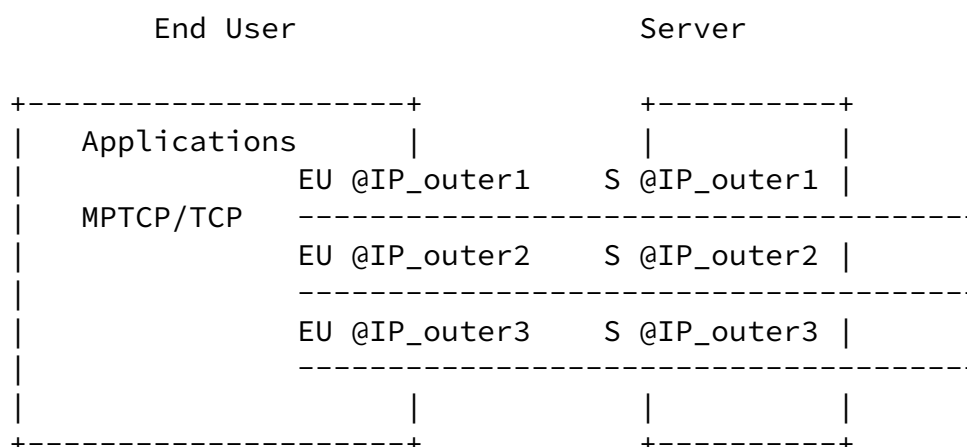


Figure 12: MIF aware applications with the Transport mode

[5.1.](#) Initial MIF IPsec Configuration

[5.1.1.](#) Description

In Figure 12, the End User initiates an IKEv2 negotiation using EU @IP_outer1 and S @IP_outer1. The Server provides the End User the available interfaces (S @IP_outer1 i in {1, 2, 3}). Then the End User negotiates Security Associations between the EU @IP_outer(i) and S @IP_outer(i) i in {1,2,3} using different Traffic Selectors.

[5.1.2.](#) Problem Statement

Currently IKEv2 does not make possible a node to announce its available interfaces.

The Transport mode, does not involve tunnel outer IP addresses. Current Security Association exchange enables Traffic Selectors negotiation. These Traffic Selectors are used both for the Security Policy Index (Traffic Selectors) for outgoing traffic and for the Security Association Index for incoming traffic. Current IKEv2 specification enables to set IPsec as described in figure 11.

[5.1.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 1, IKEv2 SHOULD make possible

- 1. Make possible the Responder and Initiator to announce its interfaces. This requirement is similar to the requirements for VPNs.

[5.2.](#) Mobility

With regular TCP connection a change of the IP address breaks the connection. Applications may use mobility with the Transport mode with transport protocols that handles with multiple interfaces (like

MPTCP or SCTP for example), with multiple independent TCP/UDP connections on the different interfaces. The application manages its connections at the application layer.

Mobility with Transport mode MUST be understood as updating an existing Security Association. The purpose of the IPsec Mobility and the Transport mode is to avoid to create a new Security Association when the IP address of an interface is changing. IPsec configures the layer so that the application can securely go on with its communications. TCP connections are restarted, since changing the IP address will most likely break the existing connection. UDP will start sending on the other interface. Mobility is intended to reduce the time IPsec requires to configure its Security Associations.

With the Tunnel mode, IPsec was in charge of securing and transporting IP datagrams. With the Transport mode, IPsec only secures the communication. Transport of the IP datagrams is shared between the application and the transport layer. Application and IPsec layers are independent and have their own way to handle with mobility. Synchronization between these two layers MUST be performed to avoid that the application moves the traffic on an interface whereas IPsec DISCARD this traffic. Although we do not intend to provide a complete list of how to synchronize these two layers, the list below provides some example where these two layers are synchronized:

- 1. For End Users with two interfaces. In that case, the interface the application may use is determined.
- 2. For applications that are configured with two interfaces.
- 3. For applications that we know the interface they will choose. Like those setting priority to interfaces. This could be set by using Multihoming and ordering the Alternate IP addresses.
- 4. If the Mobility exchange is triggered by the new socket, new packet sent. This case reduces the latency over a CREATE_CHILD_SA exchange, but does not anticipate the decision of the application.

[5.2.1.](#) Description

The mobility scenario we consider in this section is an application using a single interface EU @IP_outer3 for example. As represented in figure 13, this interface is down. Then the End User get assigned a new IP address EU @IP_outer4 and uses this interface as represented in figure 14. Both End User and Server MUST update Security Policies

and Security Associations that used EU @IP_outer3 and replace the value with EU @IP_outer4. Unlike the Tunnel mode, Traffic Selectors also need to be updated.

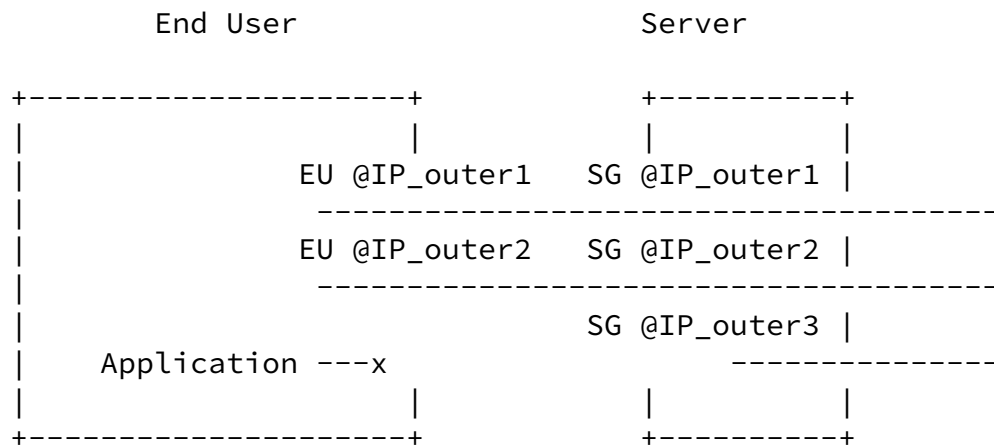


Figure 13: Mobility with Transport mode and Multiple Interfaces: EU @IP_outer3 unreachable.

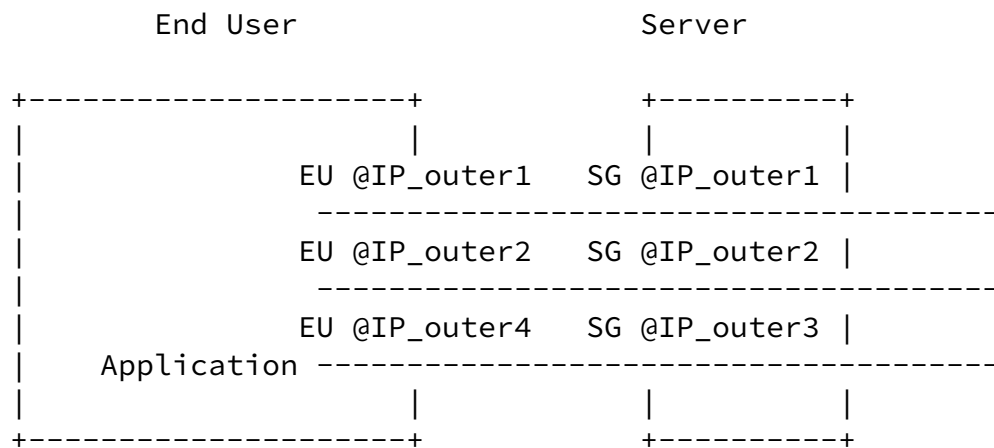


Figure 14: Mobility with Transport mode and Multiple Interfaces: EU @IP_outer4 replaces EU @IP_outer3.

5.2.2. Problem Statement

Currently IKEv2 does not provide extension that perform any mobility operation.

MOBIKE has only been designed for the Tunnel mode.

The CREATE_CHILD_SA suffers for limitations exposed in [Section 3.2.2](#): It is not mandatory in IKEv2 implementation, the exchange requires

Internet-Draft

IPsec MIF Problem Statement

November 2012

much resources as updating the Security associations. Most of the time, it requires an addition Delete exchange and is a per Security Association exchange. However, because no tunnel IP address requires to be negotiated, the CREATE_CHILD_SA can set the Security Associations and Policies as described in figure 14.

[5.2.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 1, IKEv2 SHOULD make possible

- 1. Extend MOBIKE to the Transport mode
- 2. Extend MOBIKE with Transport mode to multiple interfaces requirements described in [Section 3.2.3](#).

[5.3.](#) Multihoming

Multihoming consists in providing Alternate Interfaces in case a running interface is down, so peers are aware of the parameters to update. Multihoming can be seen as pre-configuring an mobility operation.

[5.3.1.](#) Description

With Multihoming, when the End User sets its IPsec configuration as illustrated in figure 12, the End User also specifies for each interface the corresponding Alternate IP address. Although this can be done on a per interface value, we suggest that when multiple interfaces are provided, Alternate IP addresses can be derived automatically and assigned to each interface without being explicitly mentioned. Suppose that in the case of figure 13, for example EU @IP_outer2 is provisioned as the Alternate IP address of EU @IP_outer3.

When EU @IP_outer3 is down, then the End User or the Server triggers a mobility exchange as described in section [Section 5.2.1](#).

[5.3.2.](#) Problem Statement

Currently IKEv2 does not make possible to provision Alternate IP addresses for the Transport mode. MOBIKE has only been designed for the Tunnel mode, then as mentioned in [Section 3.3.2](#), MOBIKE only assigns the Alternate IP address for the IP address used by the IKEv2

channel. This is because MOBIKE has been designed for a single interface.

Note that with the Transport mode, the Alternate Address is provided to the outer IP address that is also used as a Traffic Selector, whereas in the Tunnel mode, the Alternate IP address is provided for

the tunnel outer IP address.

Note also that the IKEv2 channel is a special case where Alternate Address is associated to the Transport mode. In fact the IKEv2 channel uses Transport mode, not the Tunnel mode.

[5.3.3.](#) Requirements

In order to make the End User set its IPsec configuration as represented in figure 1, IKEv2 SHOULD make possible to:

- 1. Extend MOBIKE Multihoming to the Transport mode
- 2. Extend MOBIKE with Transport mode to multiple interfaces requirements described in [Section 3.3.3](#). Alternate IP address should be assigned to any interface and can be automatically be derived. Alternate IP address concerns Traffic Selectors and Security Association Indexes.

[5.4.](#) Adding an Interface

Adding an interface works exactly as described in [Section 3.4](#). The only difference is that when an interface is added with the Transport mode, Traffic Selectors will automatically be associated to this newly added interface, which was not necessarily the case with the Tunnel mode.

[5.5.](#) Delete an Interface

Similarly to the addition of a new interface, Deleting an interface works exactly as described in [Section 3.5](#). The only difference is that with the Transport mode, Security Associations and Security Policies to delete are these where the specified interface appears as a Traffic Selector rather than as an outer tunnel IP address.

[6.](#) Security Considerations

The whole document sets MIF requirements for a security protocol.

[7.](#) IANA Considerations

There is no IANA consideration here.

[8.](#) Acknowledgment

We would like to thank Daniel Palomares, Pierrick Seite, Brian Carpenter, Hui Deng, Jong-Hyoun Lee, Juan Carlos Zuniga and

Migault & Williams

Expires May 7, 2013

[Page 25]

Internet-Draft

IPsec MIF Problem Statement

November 2012

Konstantinos Pentikousis for their useful comments.

[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.
- [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.
- [RFC4960] Stewart, R., "Stream Control Transmission Protocol", [RFC 4960](#), September 2007.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 5996](#), September 2010.

[9.2.](#) Informational References

- [Cisco] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015", February 2011.

- [I-D.arora-ipsecme-ikev2-alt-tunnel-addresses]
Arora, J. and P. Kumar, "Alternate Tunnel Addresses for IKEv2", [draft-arora-ipsecme-ikev2-alt-tunnel-addresses-00](#) (work in progress), April 2010.
- [RFC6182] Ford, A., Raiciu, C., Handley, M., Barre, S., and J. Iyengar, "Architectural Guidelines for Multipath TCP Development", [RFC 6182](#), March 2011.
- [Raiciu] Arora, C., Barre, S., Plunkte, C., Greenhalgh, A., Wischik, D., and M. Handley, "Improving datacenter performance and robustness with multipath TCP", SIGCOMM 2011 Toronto, Canada, August 2011.

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

Carl Williams
MCSR Labs
Philadelphia, PA 19103
USA

Phone: 650-279-5903
Email: carlw@mcsr-labs.org

